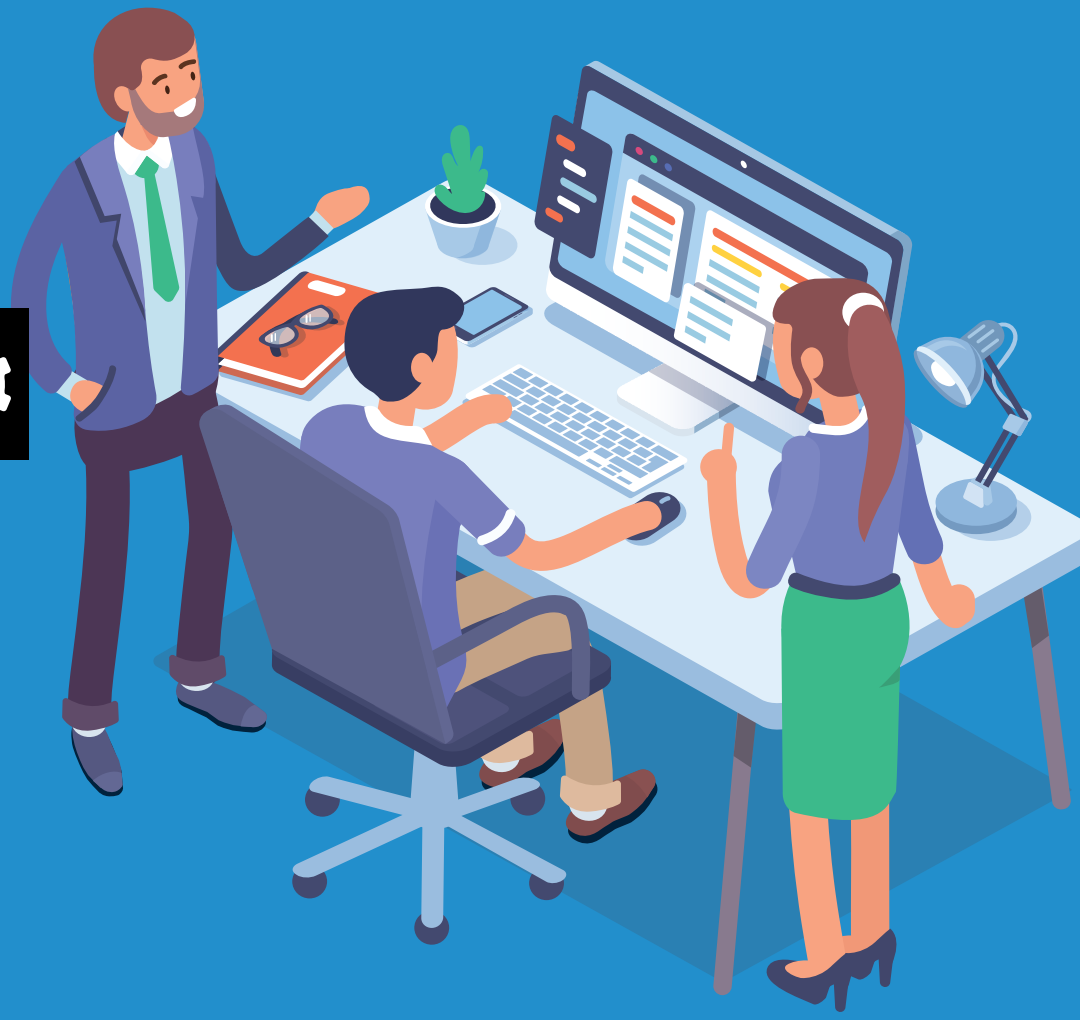
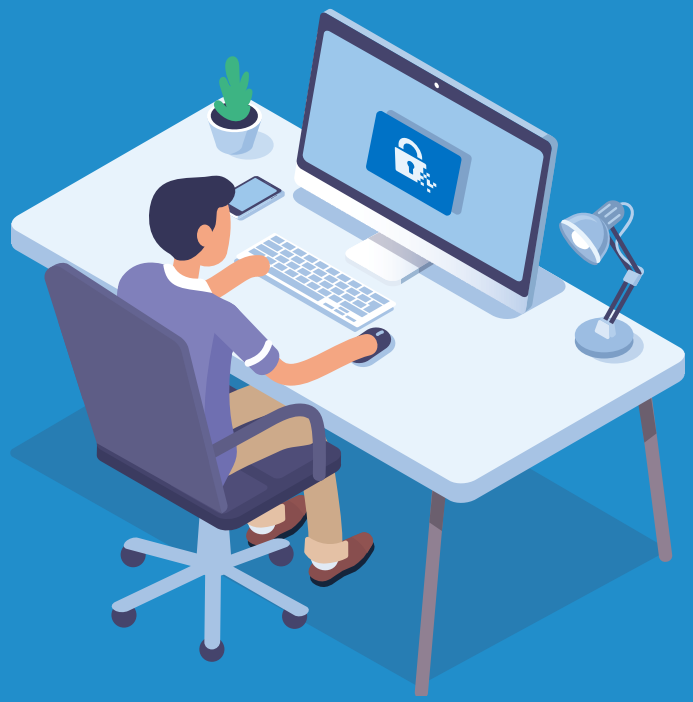
helpsystems

SIEM Buyer's Guide





SIEM Buyer's Guide

El reto de la Seguridad, hoy en día

No es ningún secreto que las amenazas en materia de Seguridad han aumentado y que éstas pueden provenir tanto de fuentes internas como externas. A las continuas amenazas de hackers, que buscan vulnerar los protocolos de Seguridad que protegen su información sensible, se suma otra creciente preocupación: los empleados que por accidente configuran erróneamente los parámetros de Seguridad y abren la puerta a los ataques. Para hacer frente a estos problemas, las organizaciones han adoptado diversos sistemas, con el objetivo de protegerse contra intentos de intrusión y un sinfín de otros riesgos.

El inconveniente de estos sistemas de protección es que generan tal cantidad de datos de seguimiento, que los equipos de IT se enfrentan al inconveniente de tener que interpretarlos en su totalidad para poder identificar los verdaderos problemas. En efecto, para los equipos de Seguridad escasos de personal, recibir un flujo importante de datos resulta inútil si éstos no pueden ser analizados y filtrados con rapidez, para generar alertas procesables. En vista de la inmensa cantidad de datos en cuestión, para las organizaciones ya no es posible recurrir al análisis manual para realizar este trabajo.

Es aquí donde interviene un software SIEM.

Introducción al concepto de SIEM

SIEM o Gestión de Eventos e Información de Seguridad *(Security Information and Event Management)* es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de Seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas. Esto es posible mediante un análisis centralizado de datos de Seguridad, obtenidos desde múltiples sistemas, que incluyen aplicaciones antivirus, firewalls y soluciones de prevención de intrusiones.

Gartner acuñó el término "SIEM" en un reporte de 2005 titulado "Mejore la Seguridad de IT con la Gestión de Vulnerabilidades". El término reúne los conceptos de Gestión de Eventos de Seguridad (SEM) con el de Gestión de Información de Seguridad (SIM), para obtener lo mejor de ambos mundos. SEM cubre el monitoreo y correlación de eventos en tiempo real, al mismo tiempo que alerta la configuración y vistas de consola relacionadas con esas actividades. Por su parte, SIM lleva estos datos a una siguiente fase, que incluye el almacenamiento, análisis y generación de reportes de los resultados.

¿Por qué es importante para las compañías hoy en día contar con un SIEM?

Con un SIEM, usted cuenta con un método efectivo para automatizar y centralizar la gestión de Seguridad, que lo ayuda a simplificar la difícil tarea de proteger su información sensible. Un SIEM lo asiste para comprender la diferencia entre una amenaza de bajo riesgo y una que podría ser perjudicial para su Negocio.

Un software SIEM transmite inteligencia procesable, que le permite gestionar vulnerabilidades potenciales de una forma proactiva, basándose en información en tiempo real. Esto protege su Negocio y a sus clientes de vulneraciones de datos que podrían ser devastadoras. Con la incidencia cada vez mayor de estos ataques, hoy en día esta tecnología es más importante que nunca.

Afine su visión

Un SIEM es una pieza esencial de su set de herramientas de IT y Seguridad. Piense en ella como en una lente que afina su visión panorámica, y lo ayuda a enfocar los esfuerzos de su equipo allí donde tienen mayor impacto. Esto es particularmente importante en situaciones que involucran amenazas que van evolucionando, cuando la rapidez de los analistas para investigar y resolver los problemas depende de la capacidad de recopilar y analizar los datos obtenidos.

Resumen de las funcionalidades clave de una solución SIEM

- Centraliza su visibilidad sobre potenciales amenazas
- Identifica aquellas amenazas que requieren remediación, y determina cuáles son inocuas
- Escala los problemas detectados a los analistas de Seguridad correspondientes, para que puedan intervenir rápidamente
- Incluye el contexto de los eventos de Seguridad, lo cual permite una remediación bien informada
- Documenta en un registro de auditoría los eventos detectados, y cómo fueron resueltos
- Cumple con las regulaciones de la industria en un formato de reporte sencillo

¿Cómo han evolucionado los SIEM en los últimos años?

Si ha evaluado una solución SIEM en el pasado, pero hace tiempo que no lo hace, puede que encuentre novedades en esta tecnología, incluyendo:

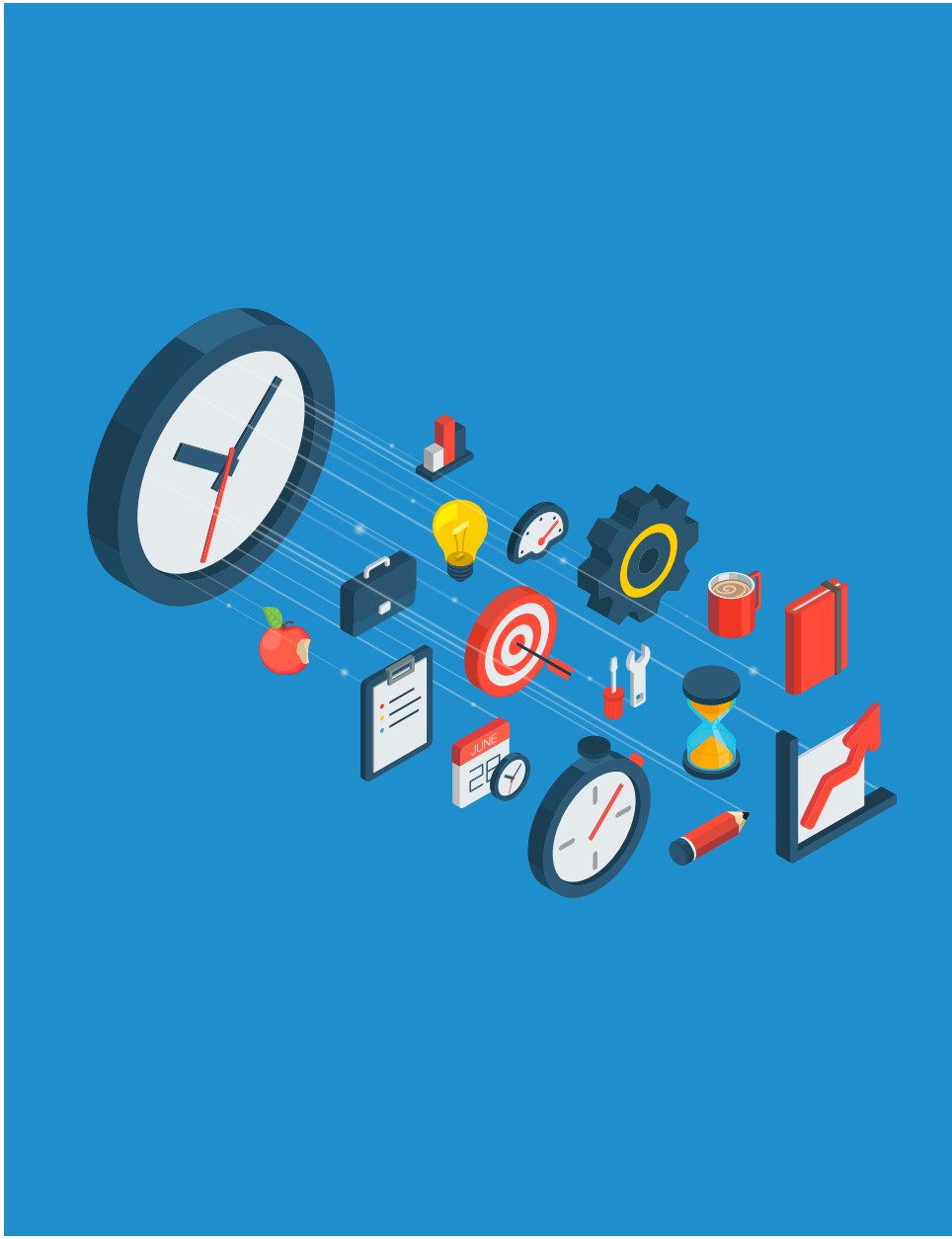
- **Integración con otras herramientas de Seguridad:** Un SIEM puede extraer datos de aplicaciones antivirus, de información de inicio de sesión y de softwares de auditoría de Seguridad, para darle una visión integral de su entorno.

- **Análisis forense:** Un SIEM le otorga información para profundizar en los detalles de un incidente de Seguridad, y poder determinar qué ocurrió exactamente y qué equipos pueden haber sido afectados.

- **Registro de auditoría:** Para cumplir con los requisitos de las normativas, se deben presentar reportes detallados con el registro de auditoría de sus prácticas y eventos de Seguridad. Las funcionalidades de reporting de un SIEM pueden darle esta información y generar estos reportes por usted.

- **Datos estandarizados:** Mantener un flujo de datos para tener una visión centralizada de su infraestructura solo es efectivo cuando estos datos pueden ser estandarizados. No importa si la información proviene de miles o millones de fuentes y sistemas distintos, un SIEM puede traducir todos esos datos a un formato común, para luego proceder a su análisis y correlación. Libera a su equipo de realizar esta tarea, y le permite contar con una mejor visión de la actividad y de los potenciales problemas.

- **Correlación:** A través de la correlación de registros o eventos individuales (por ejemplo, un nuevo usuario recientemente creado, que luego fue utilizado para acceder a información sensible), un SIEM permite esclarecer el panorama general, e identificar actividades maliciosas a medida que se producen.



Funcionalidades clave de una solución SIEM efectiva

Teniendo en cuenta la cantidad de soluciones SIEM que existen en el mercado y las funcionalidades que hemos descrito anteriormente, es conveniente analizar cuáles son las funciones que su empresa necesita. Al evaluar los diferentes softwares disponibles en el mercado, recuerde tomar en cuenta los siguientes puntos:

Establecer prioridades en los eventos de Seguridad

Es imposible anticiparse a las amenazas, si su equipo de Seguridad pierde tiempo investigando eventos de Seguridad insignificantes. Es necesario identificar los eventos más críticos y establecer cuáles tienen menor prioridad. Busque una solución que facilite el proceso de asignación de prioridades, con controles listos para usar, que puedan ser ajustados a su conveniencia.

Estandarización de fuentes de datos dispares

Las organizaciones cuentan con múltiples tecnologías para administrar su Negocio. Como consecuencia, para los equipos de Seguridad puede resultar muy difícil entender la información que procede de fuentes dispares. A través de un proceso de estandarización, un SIEM puede convertir estos datos en inteligencia procesable: los ajusta a un formato común y lo ayuda a interpretarlos. De modo que ya no es necesario que los analistas ahonden en los matices de diferentes Sistemas Operativos, aplicaciones, bases de datos, firewalls y dispositivos de red. Una solución robusta será capaz de indicarle qué significa la información de cada evento y qué hacer con ella.

Enriquecimiento de datos

Busque una solución capaz de proveer un contexto más amplio detrás de los eventos de Seguridad, para lograr una respuesta rápida y exhaustiva. El enriquecimiento de datos permite que todos los detalles del evento y el análisis forense estén al alcance de su mano. Por ejemplo, si se crea un nuevo usuario, y éste se conecta inmediatamente a un sistema crítico, el SIEM reconoce esta conducta como anormal y escala el incidente a quien corresponda, para que sea investigado.

Detección de amenazas en tiempo real

Para minimizar el impacto de una filtración de datos, usted debe ser capaz de detectar las amenazas muy rápidamente. Esto significa tener la capacidad de llevar un registro y correlacionar los eventos, dando prioridad a unos sobre otros, en tiempo real. Así, su equipo podrá resolver y mitigar amenazas, antes de que éstas deriven en una filtración de datos devastadora.

Reacción rápida ante incidentes

La solución que usted elija deberá ser capaz de escalar automáticamente los eventos a la persona indicada, y gestionar aquellos casos que pueden ser investigados posteriormente, para que su equipo sea más eficiente.

Una solución de Seguridad lista para usar

A medida que conecta nuevas fuentes de datos, como servidores Windows® o bases de datos Oracle®, asegúrese de poder aplicar automáticamente los controles y las normas de Seguridad apropiados. Contar con plantillas de controles de Seguridad listas para usar permite comenzar a operar con nuevos sistemas muy rápidamente, a la vez que le permite también ajustar la configuración en función de sus necesidades.

Reportes de Seguridad y cumplimiento

Tanto los equipos de Operaciones de IT como los de Seguridad deben presentar reportes a auditores y ejecutivos de forma periódica. Muchas organizaciones además necesitan cumplir con una serie de normativas, lo cual agrega complejidad e implica una mayor dedicación a la generación de reportes. Un SIEM que cuente con un potente motor de reportes facilita la generación de reportes con el registro de eventos y de la actividad de respuesta a incidentes. Los reportes de cumplimiento que proporciona un SIEM incluso pueden ayudarlo a mostrar cómo mejora su postura de Seguridad a lo largo del tiempo.

Haga un balance de las funcionalidades que necesita

Invierta en una solución con un nivel de funcionalidades adecuado a sus requerimientos, pero cuya complejidad no sea tal que impida a su equipo usarla fácilmente en el día a día. Usted no deseará quedarse con una herramienta complicada o costosa, pues es muy factible que esto le impida implementar otros controles críticos en su organización.

Otros puntos a considerar

Aparte de las consideraciones referidas a las funcionalidades, hay otros elementos de un SIEM que, a largo plazo, promoverán la usabilidad y el éxito de esta solución en su organización.

Soluciones de nivel empresarial vs. código abierto (Open Source)

Ciertas soluciones SIEM corresponden a la categoría empresarial. Esto significa que cuentan con un equipo de desarrollo, enfocado en proporcionar mejoras de producto y soporte al cliente. Otras opciones se basan en el modelo de código abierto (Open Source). En este caso, una vasta comunidad de desarrolladores se ocupa de proveer soporte y corregir problemas.

Las soluciones SIEM de código abierto proporcionan funcionalidades básicas que pueden ser óptimas para organizaciones pequeñas que recién están comenzando a analizar la información de sus eventos de Seguridad. Sin embargo, muchos profesionales de IT se encuentran con que un software SIEM de código abierto exige demasiado trabajo. De modo que se plantean si sigue siendo una opción viable a medida que la organización crece. Sumado a esto, algunas compañías tienen políticas que desalientan la implementación de soluciones de código abierto. Es vital que usted esté al tanto de las ventajas y desventajas de cada enfoque, y de aquello que está permitido en su organización.

Automatización

Algunas partes del proceso de un SIEM pueden ser automatizadas, para ahorrar tiempo y ganar velocidad a la hora de compartir información entre los miembros de su equipo. Se puede enviar notificaciones a la persona adecuada, en función de cuál sea la fuente de datos o eventos. Por ejemplo, si se trata de un evento de detección de virus proveniente de su entorno Linux, éste puede ser dirigido directamente al Administrador Linux. Será quien mejor sepa aislar rápidamente el sistema y remediar la infección, antes de que ésta se propague.

Implementación y capacitación

Cada proveedor de software tiene procesos distintos a la hora de implementar sus soluciones, y diferentes formas de hacer participar al equipo del cliente en la capacitación. Saber cuáles son sus opciones con relación a estos servicios es clave para estimar cuánto tiempo le llevará poner en marcha el software y empezar a ver resultados. Las soluciones más intuitivas requieren de menor tiempo de capacitación previa, lo que acelera la aparición de resultados para su organización.

Las soluciones más complejas requieren que su equipo invierta un tiempo considerable en capacitación, y conllevan la realización de ajustes periódicos en el sistema. Generalmente, los servicios profesionales incluyen integración, desarrollo y consultoría. Sepa de antemano si el proveedor que está considerando ofrece estos servicios: quizás usted no cuenta con los recursos necesarios para implementar la solución, o bien desearía que el proveedor lo ayude en el proceso de migración al nuevo software.

La capacitación debería permitirle obtener un conocimiento a fondo de la solución. Cuando solicite detalles referidos a capacitación, recuerde formular al proveedor las siguientes preguntas:

- ¿Los costos de capacitación son los mismos, prescindiendo de cuántas personas participen de la sesión?
- ¿Las actividades de capacitación son interactivas? ¿O se trata de una demostración realizada por el capacitador?
- ¿Se puede revisar un esquema del curso antes de comprar el paquete de sesiones?
- ¿Pueden personalizar el material de la capacitación?

Supporte

Evalúe las opciones de soporte al cliente que ofrece el proveedor. ¿Está disponible las 24 horas, los 7 días de la semana? Ante un problema, ¿usted puede comunicarse a través de la web, por teléfono y chat? ¿El soporte es tercerizado o se realiza localmente? Todas estas son consideraciones importantes, que usted deberá sopesar a fin de proteger la salud y utilidad de su aplicación SIEM en el tiempo.

Integraciones

El hecho de contar con un contexto complejo, donde conviven diversas soluciones de Seguridad, puede constituir un desafío a la hora de garantizar la Seguridad de su entorno. Las integraciones entre productos -como antivirus o softwares de auditoría de Seguridad - hacen generan un perfil de Seguridad más eficiente y centralizado. Esto ayuda a evaluar cualquier impacto potencial sobre la Seguridad de la información alojada *on premise*, en la nube, o en una configuración híbrida.

Costos a tener en cuenta

Licencias y métodos de implementación

Algunos proveedores licencian su software SIEM de acuerdo al volumen de datos generado o en función de cuántos sistemas gestiona la solución. Otros tienen un enfoque diferente, con una simple tarifa plana. Análogamente, los modelos de implementación pueden ser *on-premise* o en la nube. Ciertas soluciones utilizan agentes y otras no. Un agente es un código que debe ser ubicado entre los *endpoints* de los sistemas, para habilitar el envío de información del sistema monitoreado por la solución SIEM. De esta forma, es posible la estandarización y evaluación de esa actividad. Las aplicaciones desprovistas de agentes se conectan a los sistemas de forma automática, para simplificar la administración. A la hora de evaluar ofertas, sepa cómo impactarán estas diferencias en el coste global, al adquirir el producto.

ROI

La capacidad de detectar amenazas y bloquearlas redundará en un importante retorno de inversión (ROI) para su Negocio. Sin embargo, este beneficio puede ser difícil de cuantificar. Haga hincapié en cuánto se ha incrementado la eficiencia del área de IT desde la incorporación de un SIEM. Destaque el ahorro en términos de tiempo, al contar con un agregador que recopila datos de múltiples fuentes de Seguridad. Cuando llegue el momento de evaluar de qué forma lo ayuda una solución SIEM, considere lo siguiente:

- Centraliza su visión de potenciales amenazas
- Determina cuáles son las amenazas que requieren ser remediadas, y cuáles son inocuas
- Escala eventos a los analistas de Seguridad adecuados, para que intervengan rápidamente
- Incluye información de contexto de los eventos de Seguridad, para posibilitar una remediación bien informada
- Documenta en un registro de auditoría todos los eventos detectados y cómo fueron remediados
- Muestra el cumplimiento con las normativas vigentes de la industria, facilitando la generación de reportes

Repercusiones sobre el personal

Algunas soluciones requieren personal dedicado al funcionamiento del software y a la gestión de la interfaz de eventos. Otros implican una menor carga de trabajo, y es muy factible que pueda gestionarlos el staff actual de su organización. Usted debe establecer si será necesario sumar empleados a su equipo actual para la gestión diaria de la nueva aplicación SIEM. Y deberá analizar si este costo figura en su presupuesto actual.

El rol de un SIEM para el cumplimiento

Los SIEM ganaron popularidad cuando las grandes empresas empezaron a trabajar para adecuarse a la normativa PCI DSS *(Payment Card Industry Data Security Standard)*. Además, también son sumamente útiles a la hora de cumplir con el Reglamento General de Protección de Datos (RGPD), Sarbanes-Oxley (SOX) y otras normativas. Estas normativas exigen que las organizaciones dispongan de mecanismos orientados a detectar amenazas y resolverlas rápidamente. Esto implica que usted debe estar al tanto de lo que sucede en toda su infraestructura informática, que abarca entornos on-premise, en la nube y entornos híbridos.

Una solución SIEM es clave para tener la información necesaria y disponer de una visión completa, a fin de monitorear datos e intervenir rápidamente ante cualquier amenaza que sea motivo de alerta. Cuando toda esta actividad es capturada y volcada a un registro detallado de auditoría, los auditores verifican que su organización esté dando los pasos necesarios para proteger su información.

Lista de verificación de requisitos

Una vez que haya pensado detenidamente en las funcionalidades y opciones que necesita en su solución SIEM, le será de gran ayuda disponer de una lista de verificación de requisitos. Así, podrá evaluar las diversas propuestas en el mercado y ver en qué medida se ajustan a sus necesidades en particular.

A continuación, le presentamos una lista de verificación de requisitos, a modo de ejemplo, para ayudarlo a empezar.

Requisitos	Proveedor 1	Proveedor 2	Proveedor 3
La solución cuenta con controles de acceso basados en roles para la separación de funciones.			
La solución soporta las normativas de Seguridad ____ (ej.:PCI DSS, HIPAA, SOX, BCRA, FISMA), cuyo cumplimiento es obligatorio para mi organización.			
La solución recopila registros y eventos de múltiples fuentes y tipos de sistema que preciso utilizar, como _____ (ej.:Linux, AIX, Windows, IBM i, VMware, dispositivos de red, bases de datos).			
La solución correlaciona eventos de Seguridad en tiempo real.			
La solución almacena el historial de información a largo plazo, para asegurar el cumplimiento.			
La solución es viable para múltiples casos de uso, inclusive para proyectos ajenos al área de Seguridad, como Operaciones de IT.			
La solución es fácil de usar y administrar, y no requiere una programación compleja ni personal especialmente calificado.			
La solución es escalable, con costos predecibles.			
La solución cuenta con el respaldo de una compañía de probada y sólida trayectoria en la industria de software, con ulteriores mejoras de producto e inversiones en desarrollo.			
La solución no se limita a ser instalada *on-premise*, sino que soporta entornos híbridos y *cloud*.			
La solución dispone de un ecosistema abierto, que permite configuraciones de usuarios para casos de uso puntuales.			
El panel de control permite clasificar y filtrar datos con unos pocos clicks.			
Cuenta con reportes integrados y plantillas de reporte configurables.			
La solución ofrece un registro de auditoría exhaustivo de las actividades de los analistas de Seguridad.			
La solución monitorea la actividad del usuario, para localizar tentativas de vulneración y exponer usos indebidos.			
La solución establece prioridades en las amenazas de forma automática y deriva cada caso al analista correspondiente.			
La solución permite la incorporación de registros y eventos a través de un simple menú en su interfaz.			
La solución puede identificar eventos significativos, señala su gravedad y muestra su estado.			
La solución puede realizar búsquedas personalizadas de eventos y datos de registro.			
La solución toma datos provenientes de múltiples fuentes y los traduce a un formato común, para facilitar su análisis.			
La solución puede ser integrada a otras herramientas de Seguridad, como antivirus y software de auditoría.			

Ya tiene una lista acotada de proveedores - ¿Cómo proseguir?

Defina su presupuesto

A la hora de establecer cuánto desea invertir en una solución SIEM, es importante que tenga en cuenta qué incluye - y no incluye - el precio. Algunas preguntas que le sugerimos hacerle al equipo de ventas de cada proveedor son las siguientes:

- ¿Puedo solicitar una licencia para módulos puntuales?
- ¿Puedo adquirir el software mediante *leasing*?
- ¿Ofrecen licencias para un número limitado de usuarios o proveedores? ¿O el número de usuarios y proveedores es ilimitado?

Más allá de las licencias iniciales del software, cabe remarcar que muchos compradores adquieren un pack de soporte y mantenimiento anual, que les permite una actualización a la última versión del producto tan pronto como ésta se encuentre disponible. También debe considerar otras inversiones opcionales a agregar al producto, como los servicios profesionales (por ejemplo, asistencia durante el proceso de migración e implementación, o capacitación en el software) o la suma de módulos para expandir el rendimiento de su solución SIEM.

Analice los recursos que el proveedor pone a su disposición

Tómese un tiempo para explorar los recursos con que cuenta cada proveedor de soluciones SIEM. Si un proveedor tiene buenos recursos, como documentación en línea y tutoriales, es una señal de que el proveedor no solo se aboca a desarrollar un software potente, sino que también desea ayudarlo a entender todo lo que el producto puede hacer por su organización.

Solicite una demostración en vivo

Una vez que haya acotado las opciones a dos o tres que parecen cumplir con las necesidades de su organización, invite a los miembros de su equipo que intervendrán en la decisión de compra, a una demostración en vivo con el proveedor. Normalmente duran una hora y las lideran los expertos en SIEM de cada proveedor.

Prepárese para esta reunión: haga preguntas que lo ayuden a evaluar exhaustivamente cada solución y plantee todas sus inquietudes. En cada demostración, recuerde que además de analizar el producto, usted está evaluando a los representantes de su proveedor y, fundamentalmente, su profesionalismo. Ya que el proveedor colaborará con su organización en los próximos años, usted necesita sentir plena confianza en sus capacidades.

Pruebe la solución

Si una solución le atrae, decida si quiere solicitar al proveedor una prueba gratuita del software. Esto implica instalarlo en su entorno para conocer cuál es su desempeño real. Normalmente las pruebas de producto duran entre 14 y 30 días y permiten testear diferentes escenarios con todos sus parámetros en su lugar.

Acerca de HelpSystems

Organizaciones de todo el mundo confían en HelpSystems para simplificar la vida de los departamentos de IT y mantener sus negocios funcionando sin problemas. Nuestros productos y servicios monitorean y automatizan procesos, encriptan y protegen datos, y proporcionan un fácil acceso a la información que las personas necesitan.

10MLPTXSIEMBGD19