IBM **Security**

5 leyendas urbanas sobre SIEM

¿Ha estudiado las soluciones SIEM últimamente?
Porque las cosas han cambiado.

IBM®

Introducción

Los rumores dicen que las soluciones SIEM son difíciles de manejar, complejas, y que, por lo tanto, son solo para grandes organizaciones. Es cierto que algunas SIEM encajan en el segmento exclusivo de empresas, pero esta creencia pasa por alto las soluciones SIEM más progresivas diseñadas para empresas de todos los tamaños.

No es ningún secreto que la industria de la ciberseguridad se enfrenta a una gran escasez de habilidades. Las soluciones de seguridad, SIEM o de otro tipo, deben estar diseñadas para permitirle ser eficaz en su trabajo, a pesar de sus recursos (probablemente) limitados.

Abordaremos los cinco principales mitos sobre SIEM e investigaremos qué debe esperar actualmente de una SIEM.

Mito nº 01

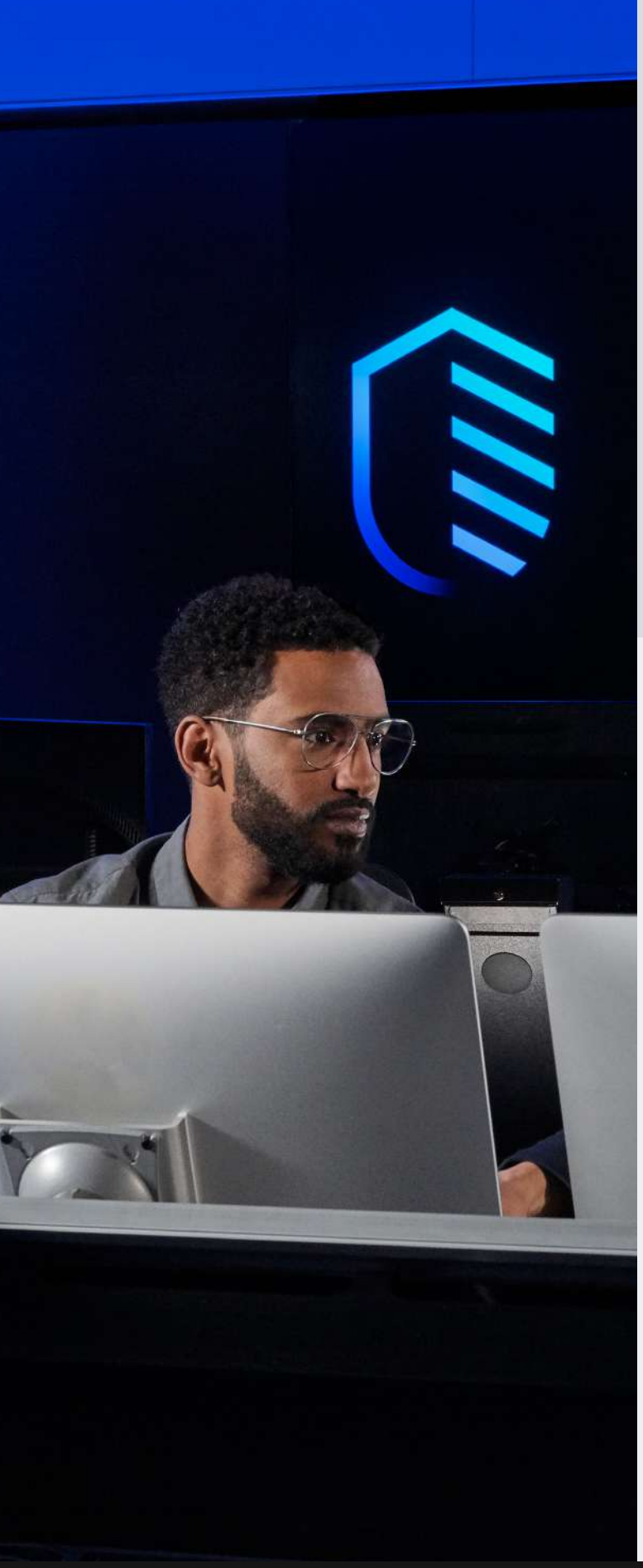
Una SIEM solo puede detectar amenazas conocidas. No es útil frente a amenazas desconocidas.

Las soluciones SIEM solo usan reglas para detectar amenazas, y para escribir una regla efectiva, primero debe saber qué buscar.

La Verdad

Las SIEM efectivas utilizan una combinación de reglas, detección de anomalias, aprendizaje automático y análisis de comportamiento para encontrar amenazas conocidas y desconocidas

También usan correlación avanzada para conectar los puntos y comprender las actividades de amenazas relacionadas. Cuando una combinación de análisis y reglas avanzadas se preconfigura en su SIEM, se pueden aplicar de manera inmediata a la actividad de la red los activos, los usuarios y las aplicaciones para que pueda ir mucho más allá de las amenazas conocidas e identificar también actividades anómalas que pueden indicar amenazas desconocidas.



Mito nº 02

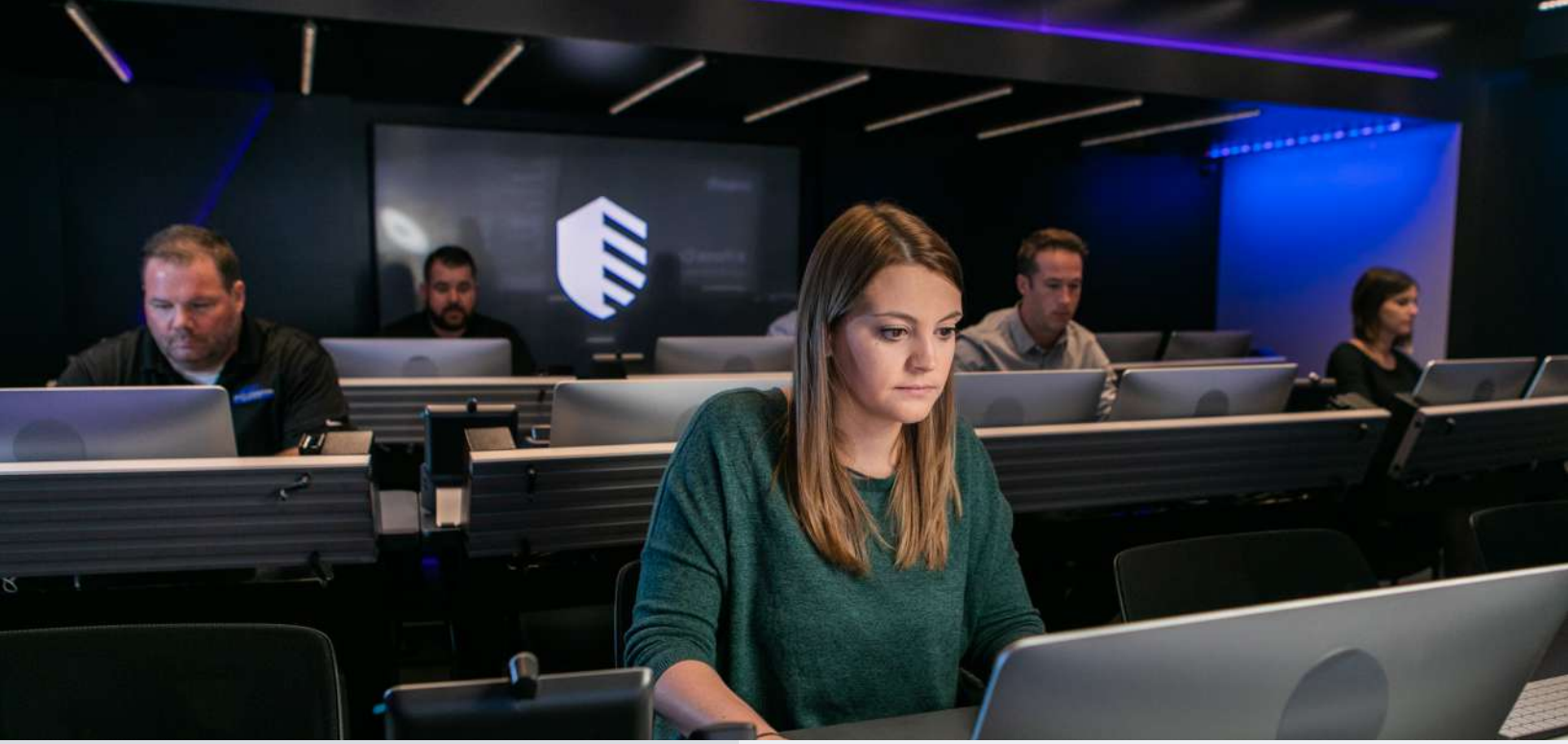
Las SIEM son solo para grandes empresas con equipos de securidad avanzados

La sabiduría popular dice que como las mejores soluciones SIEM en el mercado pueden escalarse para soportar las organizaciones más grandes, solo están destinadas a estas.

La Verdad

Las mejores soluciones SIEM se dirigen a una amplia variedad de organizaciones, independientemente de si son un negocio en crecimiento que recién comienza con el monitoreo de seguridad o si son una empresa global de Fortune 20 que necesita casos de uso avanzados.

Lo cierto es que, si bien muchos equipos de seguridad avanzados prefieren todas las opciones y extras para admitir casos de uso avanzados y especializados, una buena SIEM no requiere todas las opciones y extras para agregar valor. Una solución ideal lo ayuda a comenzar con casos de uso estándar, como detección de amenazas, monitoreo en la nube e informes de cumplimiento, listos para usar. A medida que su práctica madure y su negocio crezca, su SIEM debería escalar para soportar más entornos, múltiples geografías y casos de uso avanzados, como la inspección profunda de paquetes, análisis de DNS y una orquestación de respuesta a incidentes estrechamente integrada.



Mito nº 03

Las SIEM requieren una gran cantidad de datos y el costo de recopilar todos esos datos es extremadamente alto.

Debido a que ciertos proveedores en el mercado son conocidos por volverse prohibitivamente caros muy rápidamente, algunos equipos de seguridad suponen que todas las SIEM también son así.

La Verdad

Si está considerando proveedores que cobran en función de la cantidad de datos almacenados, puede ser muy costoso y rápido. Pero diferentes proveedores valoran sus soluciones de manera diferente.

Antes de comprometerse con algo, piense en los problemas que está tratando de resolver: ¿Es un minorista con datos de tarjeta de pago para proteger? ¿Está su negocio migrando a Amazon Web Services y necesita visibilidad en ese nuevo entorno? Los datos que recopila para fines de seguridad deberían ayudarlo a abordar sus casos de uso únicos. No se deje llevar y analice todo si no lo necesita. Dicho esto, si también tiene requisitos de retención de datos debido a regulaciones o políticas organizacionales, su proveedor SIEM debe ser capaz de proporcionar una opción de bajo costo para almacenamiento, búsqueda e informes solamente. Al analizar solo lo que es importante para su organización y enviar el resto de sus datos de registro y eventos a un almacenamiento de bajo costo, puede asumir un proyecto SIEM sin que consuma todo su presupuesto.

Mito nº 04

Necesita un equipo de científicos de datos a tiempo completo para que una SIEM sea efectiva.

A menudo dicen que para que una SIEM sea efectiva, necesitará un científico de datos de tiempo completo (o un equipo de ellos) para desarrollar todas las reglas y analítica desde cero.

La Verdad

Si no puede (o no quiere) encontrar y pagar un equipo de científicos de datos que también comprenda la seguridad, busque un proveedor que proporcione contenido empaquetado previamente listo para usar.

Algunos proveedores adoptan el enfoque de que, dado que la solución probablemente se personalizará de todos modos, ¿por qué no comenzar con una hoja en blanco? En la práctica, los equipos de seguridad de hoy simplemente no tienen los recursos para asumir un proyecto tan masivo que requiera habilidades tan especializadas. Con cualquier solución SIEM, usted deberá proporcionarle información sobre su red, pero una vez hecho esto, podrá aprovechar las reglas preescritas, la analítica y las políticas de correlación para comenzar a detectar amenazas de inmediato. No debería necesitar comenzar con una hoja en blanco. Y si todavía está preocupado, muchos proveedores de SIEM se asocian con proveedores de servicios de seguridad administrados (MSSP) para que pueda obtener todos los beneficios de una SIEM progresiva con el beneficio adicional de contar con la ayuda de expertos en operaciones de seguridad.

Mito nº 05

Las SIEM son difíciles de integrar con otras soluciones en mi entorno.

Las SIEM tienen la reputación de ser difíciles de integrar con otras soluciones, a pesar de que dependen de los datos de otras soluciones para proporcionar valor.

La Verdad

Las soluciones líderes de SIEM deben ser fáciles de integrar (y afortunadamente muchas lo son).

Las primeras SIEM que llegaron al mercado hace una década y no evolucionaron con las necesidades cambiantes y la tecnología en evolución son difíciles de integrar. Sin embargo, esos jugadores han desaparecido por completo o están en crisis ahora. Las soluciones líderes de hoy ofrecen cientos de integraciones listas para usarse con tecnologías comerciales de TI y OT, además, ofrecen conectores simples para integrar y analizar registros de aplicaciones personalizadas. Si tiene curiosidad acerca de qué integraciones existen, y son totalmente compatibles con los proveedores, consulte los sitios web de atención al cliente de los diferentes proveedores o explore sus intercambios de aplicaciones.

Conclusión

Los estereotipos que existen hoy tienden a basarse en tecnología obsoleta. Si evaluó una solución SIEM hace diez años, o incluso hace cinco, muchos de los principales mitos eran ciertos. Pero en la misma medida que la tecnología y el panorama de amenazas han evolucionado, también lo han hecho las SIEM.

Si tiene dificultades para detectar amenazas o dar sentido a los registros en su administrador de registros, hoy puede ser el día para volver a analizar soluciones SIEM y descubrir por sí mismo cuánto han cambiado.

Acerca de IBM QRadar

IBM QRadar Security Intelligence Platform es una solución flexible que proporciona visibilidad centralizada de los datos de seguridad de toda la empresa y proporciona información procesable sobre las amenazas de mayor prioridad.

La solución se basa en QRadar SIEM, que incluye cientos de reglas y analítica configurada electrónicamente, así como inteligencia de amenazas IBM X-Force. Con más de 500 integraciones listas para usarse y más de aplicaciones, los clientes pueden levantarse rápidamente y contar fácilmente con nuevos casos de uso de seguridad y conformidad. Los componentes opcionales totalmente integrados para el almacenamiento de registros, la analítica del comportamiento del usuario, la inspección de paquetes de red, la gestión de vulnerabilidades y las investigaciones de amenazas basadas en inteligencia artificial se pueden agregar y administrar fácilmente desde una única interfaz, lo que permite a los clientes comenzar de forma tan pequeña o grande como elijan y escalar fácilmente hacia arriba o hacia abajo a medida que cambian sus necesidades.

Obtenga más información en: IBM QRadar