IBM Security

QRadar: Detecte amenazas a medida que su empresa crece

IBM

QRadar está preparado para crecer a medida que lo hace su empresa

¿Cuál de los siguientes escenarios describe mejor su empresa?

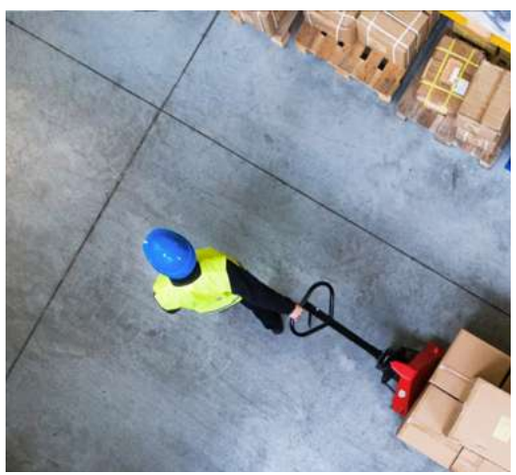
IBM QRadar le permite atender los más importantes desafíos a la seguridad, sin importar el tamaño de su empresa. Elija el tamaño de empresa que coincida con la suya para descubrir de qué manera IBM QRadar puede serle útil a su empresa.

El activista de la pequeña empresa →

Somos una pequeña empresa con orgullo; no obstante, la seguridad no es una gran prioridad, ya que contamos con un personal de TI limitado o inexistente para establecer una infraestructura de seguridad.

La empresa mediana preparada para escalar →

Somos una empresa mediana con un equipo de operaciones de seguridad comprometido, pero nuestra configuración no está personalizada para nuestra empresa.

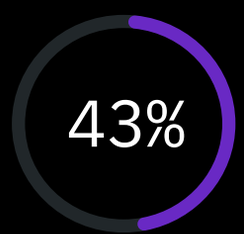


La empresa establecida →

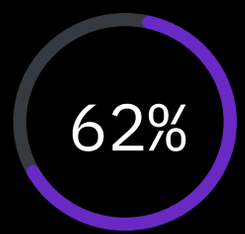
Contamos con un equipo de operaciones de seguridad avanzado; no obstante, nuestro programa de seguridad es demasiado complejo y queda rápidamente desactualizado.

El activista de la pequeña empresa

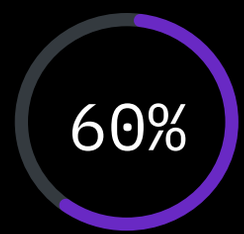
Tener una pequeña empresa no implica tener pocas necesidades de seguridad.



De las violaciones de 2019 involucró a víctimas de pequeñas empresas [1]



De los ataques cibernéticos se dirigió a pequeñas empresas [2]



De las pequeñas empresas cesa sus actividades 6 meses después de las violación [3]

No deje que el desconocido mundo de la seguridad impida que su empresa avance. IBM QRadar puede ayudar.

“ "Quiero implementar los protocolos de seguridad adecuados que me permitan proteger a mis clientes y a mi empresa en expansión".

Las dificultades son reales para las pequeñas empresas

Nuevas normas disponen supervisión, detección e informes de seguridad, pero, en una organización pequeña con personal de TI limitado, esto es difícil de gestionar. No crea el mito de que una SIEM no puede facilitar las tareas.

5 preguntas que debe plantearse antes de actualizar a una SIEM moderna →

- Nuevas normas disponen supervisión, detección e informes de seguridad
- Existe una mayor presión de los clientes que intentan gestionar el riesgo de terceros; el control proactivo de seguridad se está volviendo un requisito para mantener o hacer crecer la empresa
- Un personal de seguridad capacitado y dedicado limitado (o inexistente) a)

Necesita una visibilidad clara de su seguridad

A medida que crece su empresa, necesitará supervisar los activos en forma continua, de cumplimiento regulatorio con el aumento de normas. Sí, una SIEM puede escalar a un nivel empresarial, pero también puede ofrecerle la visibilidad que necesita en toda la empresa, independientemente de su tamaño.

5 preguntas que debe plantearse antes de actualizar a una SIEM moderna →

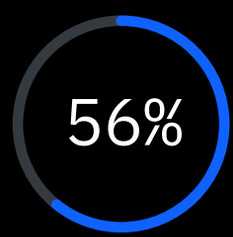
QRadar puede escalar junto con su empresa

Al aprovechar el poder de una SIEM en toda la empresa, QRadar puede ayudarlo a atender los casos de uso de seguridad más urgentes, sin necesitar esfuerzos significativos de personalización.

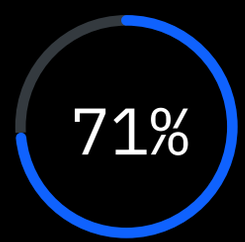
5 preguntas que debe plantearse antes de actualizar a una SIEM moderna →

La empresa mediana preparada para escalar

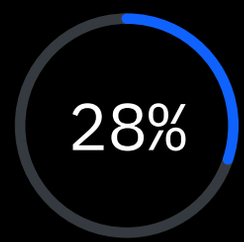
La necesidad de una mayor visibilidad



De las violaciones de 2019 demoró meses o más en detectarse [1]



De las violaciones de 2019 tenía una motivación financiera [1]



De las violaciones de 2019 implicó el uso de credenciales robadas [1]

Asegúrese de que el programa de operaciones de seguridad sea personalizado para adaptarse a su empresa y prioridades.

“ Necesitamos que nuestro equipo de seguridad pueda priorizar la actividad, mantener el cumplimiento de normas y aumentar la eficacia a la hora de atender problemas".

Ofrezca a su equipo limitado más capacidad de seguridad

Si bien puede contar con un equipo de operaciones de seguridad comprometido, las alertas continuas de diferentes detecciones de alertas que pueden no ser relevantes para su empresa pueden disminuir su capacidad.

Actualización a una SIEM inteligente →

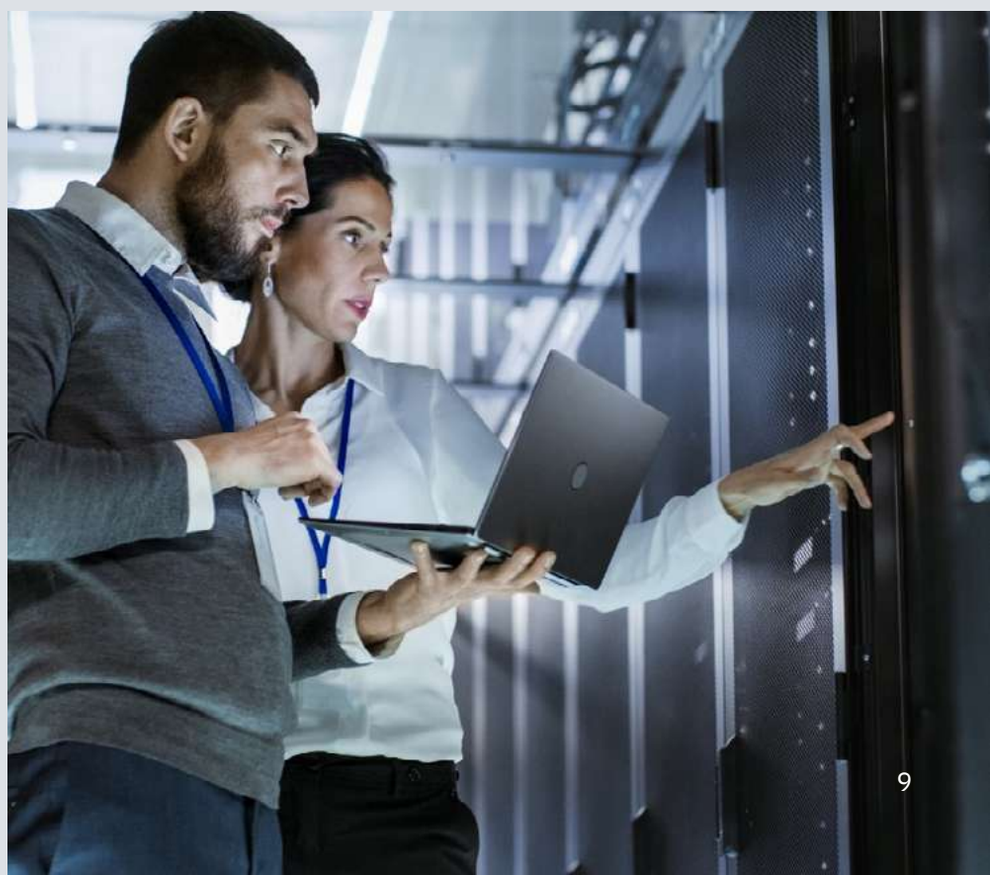
- Se necesitan casos de uso de detección de amenazas personalizables y listos para usar, los cuales sean a la medida de su empresa
- Se necesita atender e informar sobre la norma
- Debe contar con un pequeño equipo de seguridad comprometido que requiera automatización y facilidad de uso para gestionar las operaciones de seguridad de manera eficaz
- Un limitado (o inexistente) personal de seguridad capacitado y comprometido

Obtener insights prácticos sobre amenazas

Necesita herramientas que le otorguen visibilidad sobre lo que ocurre en toda la red y activar a su equipo cuando sea necesario. A medida que su equipo crece, debe considerar la automatización para poder gestionar de manera eficaz sus operaciones de seguridad.

Actualizar a una SIEM inteligente →

- Visibilidad y supervisión de los entornos en las instalaciones y en la nube
- Un proceso de detección automatizada para ofrecer insights prácticos en tiempo real sobre las amenazas
- Almacenamiento de datos de bajo costo para permitir investigaciones exhaustivas



Afiance las fortalezas de un equipo reducido

IBM Qradar le ayuda a detectar amenazas conocidas y desconocidas, a mirar más allá de las alertas individuales y a priorizar posibles incidentes, así como a aplicar IA para acelerar los procesos de investigación en un 50 %.

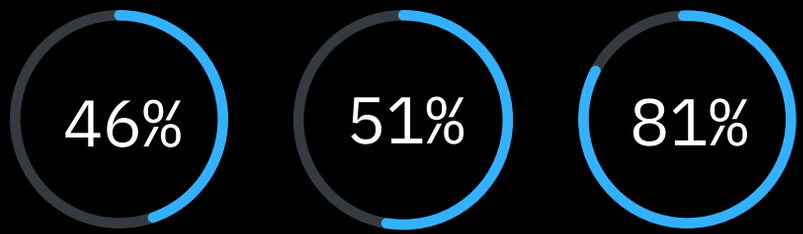
Actualización a una SIEM inteligente →

- Descubre tipos de fuentes de registros de forma autónoma e incluye más de 450 integraciones listas para usar, para analizar y normalizar registros en todo el entorno.
- Incluye más de 1.600 reglas preconstruidas y algoritmos de detección de anomalías listos para usar, para atender casos de uso rápidamente
- Correlación en tiempo real para detectar amenazas en el momento en que suceden; conectar de forma automática la actividad relacionada a amenazas y priorizar alertas basadas en la criticidad.

La empresa establecida

> “ Siempre estamos intentando detectar posibles amenazas que pueda afrontar nuestra empresa y necesitamos estar preparados para reaccionar con celeridad".

Contamos con suficientes datos, pero no con los insights suficientes

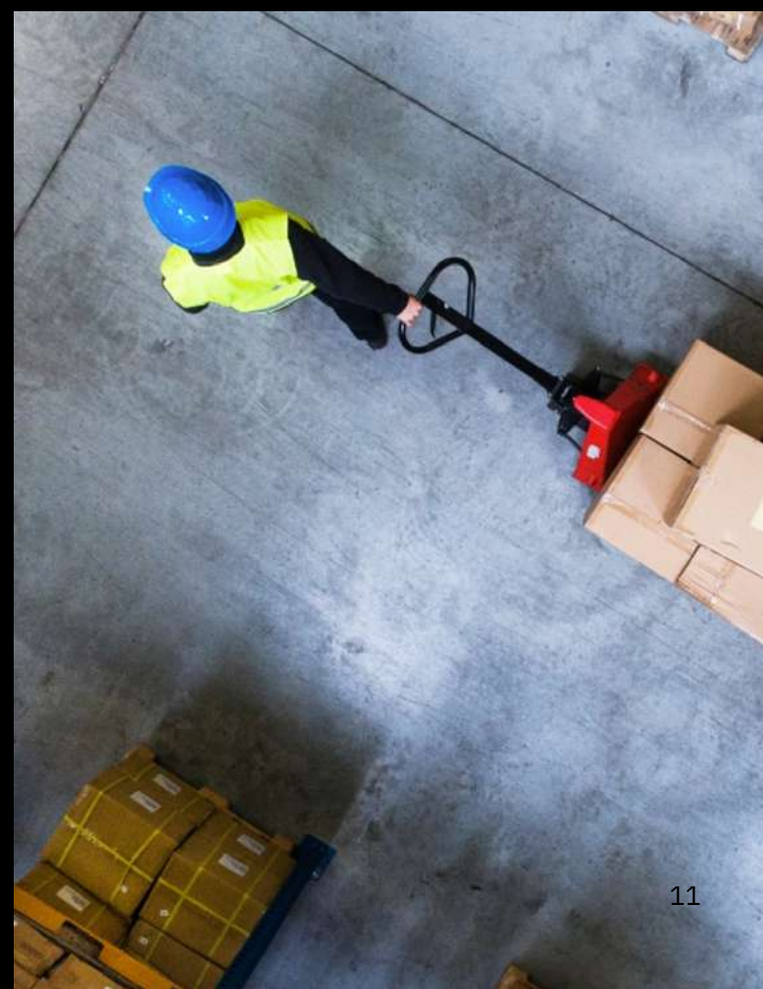


De las alertas de detección de amenazas no se investiga [4]

De las alertas de amenazas legítimas que pueden afectar a la empresa no se investiga [4]

De los CISO les preocupa que no se atiendan las violaciones [5]

Combinar la automatización y el conocimiento del sector para atender la complejidad y la dimensión de la seguridad.



Colocar las herramientas correctas al servicio de su equipo

Inclusive con un amplio equipo de seguridad, investigar y detectar los eventos de seguridad correctos puede ser un desafío. Necesita una plataforma que le otorgue a su equipo los insights que necesita para priorizar las medidas que deben implementarse y cuándo implementarlas.

Automatice su SOC con IA →

- Actualmente, probablemente estamos utilizando una solución de SIEM desactualizada y compleja
- Los continuos costos de administración son elevados y la complejidad intrínseca hace difícil el ajuste y la personalización
- Debe atender los casos de uso asociados con la nube, pero es difícil visualizar, supervisar y analizar los datos de multicloud híbrida
- Necesita insights prematuros sobre amenazas avanzadas, sigilosas y desconocidas

Se debe exigir escalabilidad y flexibilidad

Necesita una solución que pueda escalar fácilmente para dar soporte a varios entornos sin necesitar gastos generales adicionales. Al mismo tiempo, su equipo necesita una plataforma flexible que pueda dar soporte una amplia variedad de casos de uso.

Automatice su SOC con IA →

- Almacenamiento de datos de bajo costo para admitir lagos de datos, utilizados para la generación de informes, la detección de amenazas y un análisis personalizado
- Inteligencia automatizada para que los analistas tomen mejores decisiones, aceleren los procesos de clasificación y respondan a las amenazas de manera más precisa
- Análisis automatizado, visibilidad de flujos de red, correlación y priorización de amenazas para detectar las amenazas más serias al tiempo que se filtra el ruido.
- Necesita insights prematuros sobre amenazas avanzadas, sigilosas y desconocidas

Afrontar las alertas de amenazas a escala

QRadar le permite escalar la seguridad al correlacionar millones de puntos de datos para identificar una lista controlable de alertas priorizadas para que su equipo vuelva a contar con la capacidad para tomar las decisiones correctas.

Automatice su SOC con IA →

- Recopila, analiza y correlaciona una serie de datos, incluidos registros de terminales, datos de activos, flujos de red, la actividad del usuario, información de vulnerabilidad e inteligencia de amenazas
- IA para ofrecer insights más exhaustivos y personalizados de amenazas activas, comprender mejor las relaciones entre amenazas y entender cómo los analistas suelen responder a ciertos tipos de amenazas para llevar a cabo procesos de respuesta más precisos y consistentes
- Mejora la precisión de la detección de amenazas en un 51 % y genera un 50 % menos de falsos positivos que las SIEM competitivas

Para obtener más información sobre IBM Security:

Visite nuestro sitio web →

Dé el próximo paso
Entre en contacto con nuestro especialista que le ayudará a superar los desafíos de ciberseguridad .

Hable com un especialista →

Fontes

1. Verizon, 2019 Data Breach Investigations Report, mayo de 2019
2. Inc, 60 Percent of Small Business Fold Within 6 Months of a Cyber Attack, Joe Galvin, mayo de 2018
3. Seattle Times, Interest in cyberinsurance grows as hackers target small business, Marissa Lang, septiembre de 2017
4. Cisco, 2018 Cisco Cybersecurity Report: Special Edition SMB, julio de 2018
5. ServiceNow, The Global CISO Study, 2019

IBM