Simplificando la migración de SIEM

IBM Security

IBM

Índice

Introducción

Usted sabe que sus datos están en riesgo en cualquier lugar, tanto on premises como en la nube. Y si su equipo está conformado en un 70 % por centros de operación de seguridad (SOC), probablemente dependa de un software de información de seguridad y gestión de eventos (SIEM) para detectar y analizar amenazas.[1] Dado el cambiante panorama de amenazas, nuevos entornos y fuentes de datos, es fundamental que su solución SIEM pueda monitorear sin inconvenientes toda la infraestructura de su organización, inclusive a medida que su empresa crece.

Si está leyendo este libro electrónico, probablemente esté pensando en migrar a la solución SIEM de última generación, y sabe que una migración SIEM no es una tarea sencilla. Una migración SIEM exitosa comienza con la elección del proveedor de servicios de TI adecuado, el cual pueda ofrecerle una sólida experiencia en migración.

La plataforma IBM Security™ QRadar® es una solución SIEM integral que puede ayudarlo a detectar y priorizar posibles amenazas a su negocio. Los especialistas de IBM Security han ayudado a muchas empresas a migrar sus soluciones tradicionales SIEM. IBM tiene la experiencia, las habilidades, la tecnología y los recursos para ofrecerle un recorrido de migración sin sobresaltos.

En promedio, las empresas demoran

279 dias

en detectar y contener una filtración de datos.[2]

Beneficios de actualizar a una plataforma de SIEM de última generación

¿Por qué elegir QRadar?

Incorpora grandes cantidades de datos de fuentes on premises y en la nube

Ofrece visibilidad profunda y análisis de flujo de tráfico de red y metadatos

Incluye acceso a la Inteligencia de Amenazas de IBM Security X-Force® sin costo adicional.

Aplica analítica integrada para detectar amenazas en forma precisa

Permite investigaciones asistidas por inteligencia artificial (IA) y priorización de incidentes

Fomenta un ecosistema al ofrecer más de 500 integraciones listas para usar

Permite la implementación on premise o en la nube mediante una arquitectura flexible

Compara actividades relacionadas para priorizar incidentes

Ofrece integración de la infraestructura MITRE ATT&CK para la detección de amenazas, la investigación y los procesos de respuesta

Incluye modelos de comportamiento abiertos y personalizables de elaboración de perfiles de usuarios y activos

Elimina tareas manuales al analizar datos y normalizar registros automáticamente

Ofrece visibilidad integral y centralizada

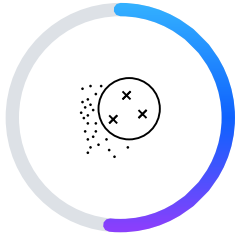
La plataforma QRadar ofrece una solución SIEM de última generación para monitorear y detectar amenazas entre aplicaciones, usuarios, contenedores, terminales, redes y entornos de nube en tiempo real.

La plataforma QRadar SIEM fue diseñada para ofrecer a los equipos de seguridad una visibilidad centralizada para identificar amenazas y anomalías de manera precoz en el ciclo de vida del ataque. A medida que se incorporan datos, la solución aplica inteligencia y analítica de seguridad en tiempo real para detectar y priorizar amenazas en forma rápida y precisa. Su equipo SOC obtendrá una vista centralizada de los registros, flujos y eventos en entornos on premises, de software como servicio (SaaS) e infraestructura como servicio (IaaS).

"Utilizar IBM QRadar SIEM es como tener ojos en la nuca. Anteriormente, siempre sentimos que estábamos en la retaguardia en relación con la seguridad, pero ahora, somos mucho más proactivos".

Michael Warrer
Gerente General de Información, NRGi

Lea el caso de estudio →



QRadar aumenta la capacidad de detectar con precisión ataques reales en un

51 %[3]

Cuenta con analítica integrada para detectar amenazas en forma precisa

La solución QRadar analiza los datos de amenazas para detectar de manera precisa amenazas conocidas y desconocidas que otros no detectan. La analítica integrada permite disminuir el tiempo de obtención de valor sin requerir experiencia en la ciencia de datos.

QRadar está diseñada para correlacionar la actividad en toda la red y aplicar una variedad de métodos de detección basados en firma y comportamiento para identificar amenazas conocidas y desconocidas.

Las décadas de experiencia en SIEM del equipo de IBM Security se han incorporado directamente en QRadar
a través de una vasta biblioteca de reglas basadas en firmas y elaboradas de forma experta. La solución utiliza modelado comportamental para crear la base de referencia de la actividad del usuario, habilitada a través de integraciones con Lightweight Directory Access Protocol (LDAP) o Microsoft
Active Directory.

QRadar puede detectar anomalías de comportamiento y comportamiento riesgoso que indica que un malware se apoderó de una cuenta de usuario, que hay credenciales en riesgo o actividad malintencionada del personal interno. Los analistas de seguridad pueden identificar usuarios rápidamente con puntuaciones de riesgo elevadas y crear listas de vigilancia priorizadas para usuarios privilegiados, ejecutivos o cuentas de máquinas. QRadar permite que los equipos SOC escalen rápidamente los programas de amenazas internas con modelos de detección de comportamiento personalizados a través de un desarrollador de modelos de aprendizaje automático (ML) integrado.

Solución IBM Security QRadar SIEM

- Correlación en tiempo real y detección de anomalías de comportamiento
- Inteligencia de amenazas e insights de vulnerabilidad
- Aprendizaje automático, servicio y creación de perfil de usuario

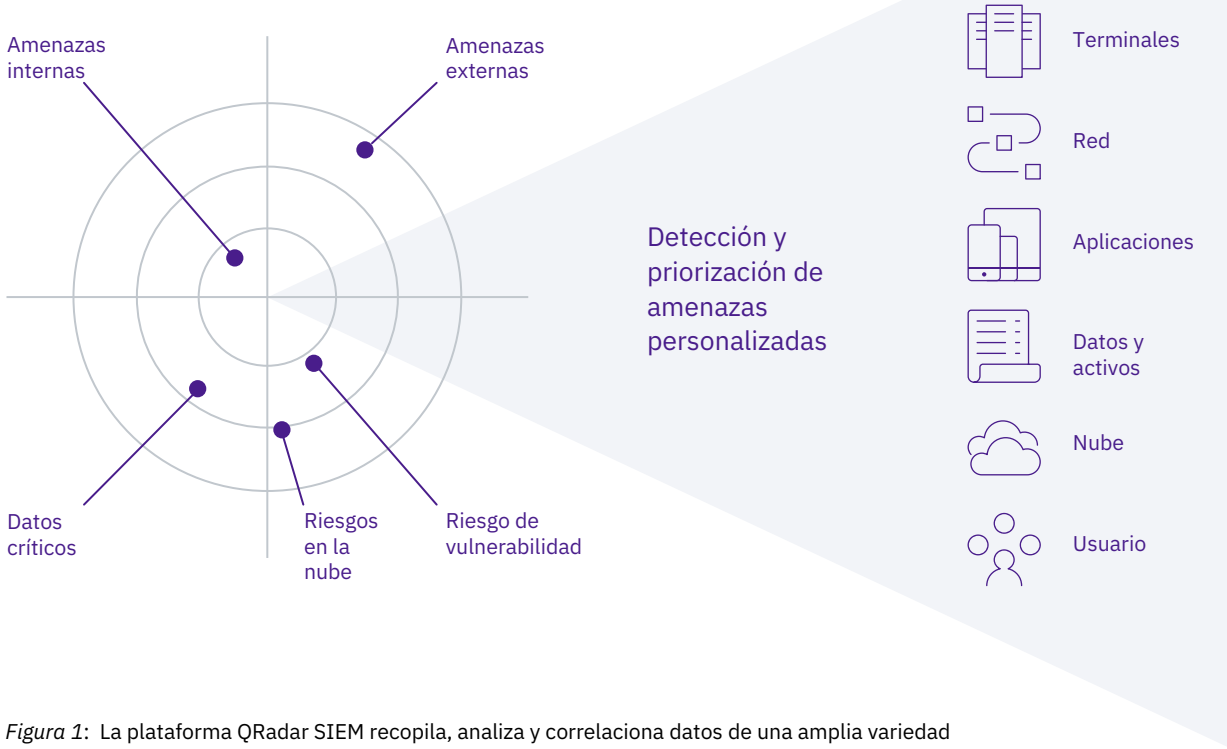


Figura 1: La plataforma QRadar SIEM recopila, analiza y correlaciona datos de una amplia variedad de fuentes para detectar y priorizar las amenazas más críticas que requieren investigación

Cuenta con analítica integrada para detectar amenazas en forma precisa

Continuación

Asimismo, QRadar emplea análisis de red avanzado para detectar un cambio en el tráfico de red, como la aparición de un nuevo host o comunicaciones anormales entre hosts existentes. El análisis de red otorga a los analistas de seguridad una comprensión más profunda del sistema, la aplicación y el tráfico de red. QRadar puede detectar tráfico de este a oeste, el cual puede indicar movimiento lateral, identificar amenazas avanzadas a medida que recorren la red y localizar intentos de exfiltración de datos confidenciales. La telemetría de red adicional recolectada reduce falsos positivos y asiste a aquellos que abordan incidentes y buscan amenazas, quienes identifican rápidamente los hosts afectados para comenzar con la corrección.

El motor de analítica de la plataforma QRadar incluye encadenamiento de infracciones, que vincula alertas relacionadas en una única infracción consolidada. El encadenamiento de infracciones presenta menos alertas de mayor fidelidad y reduce falsos positivos, lo que permite a los analistas realizar la clasificación con confianza. Debido a que toda la información está disponible en una única pantalla, para el usuario es sencillo ver una descripción general de la actividad sospechosa relacionada que se detectó. A medida que surgen nuevos eventos, la aplicación IBM QRadar Advisor con WatsonTM ayuda a priorizar infracciones y se actualiza automáticamente con nuevos datos.

.

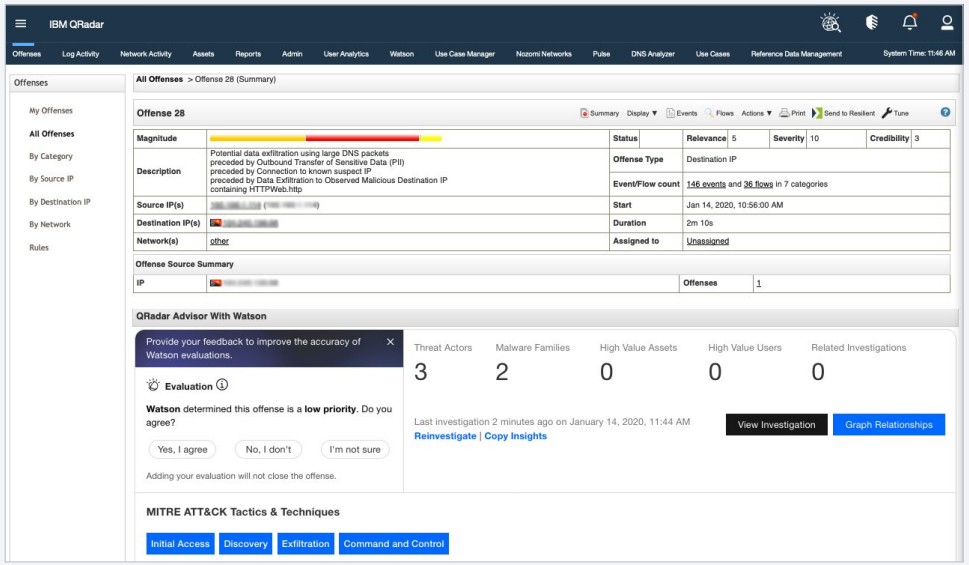


Figura 2: Reglas e infracciones personalizadas

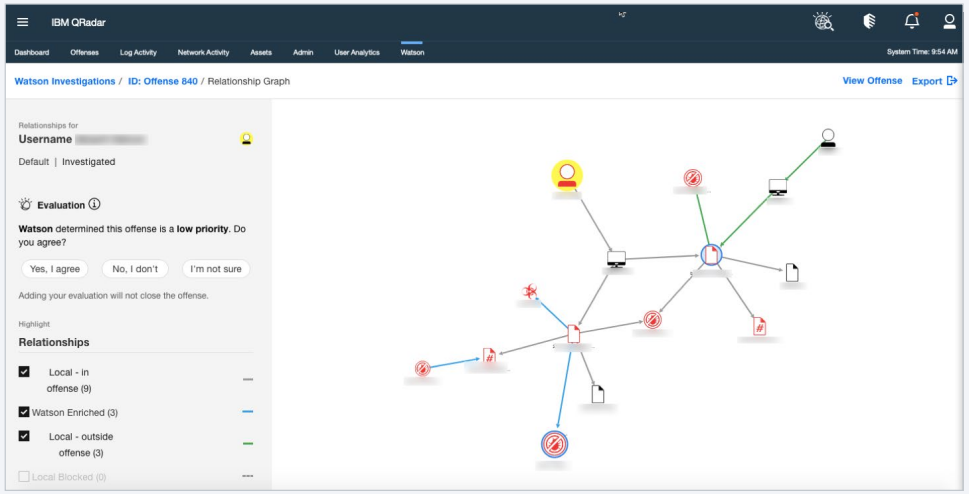


Figura 3: Ejemplo de investigación de IBM QRadar Advisor con Watson

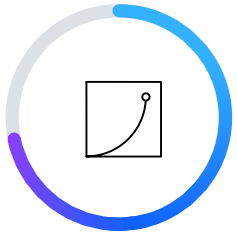
Ofrece sólidas funciones listas para usar

La solución QRadar incluye más de 500 Módulos de Soporte de Dispositivos (DSM) predefinidos que ofrecen integraciones de configuración predeterminadas con tecnologías comerciales listas para usar.

Su equipo de SOC puede simplemente señalar registros a QRadar y la solución puede detectar automáticamente el tipo de fuente de registro y aplicar el DSM correcto para analizar y normalizar los datos del registro. Como resultado, su organización puede comenzar a funcionar más rápidamente que las organizaciones con soluciones alternativas. QRadar también ofrece DSM Editor con una interfaz de usuario gráfica (GUI) diseñada para ser sencilla de usar y permitir a los equipos de seguridad definir fácilmente cómo analizar registros de aplicaciones personalizadas.

54 %

de los encuestados afirma que es muy sencillo ingresar registros en QRadar para correlación y análisis.[3]



70 %

de los encuestados afirma que las reglas de correlación listas para usar de QRadar son valiosas.[3]

Ofrece una arquitectura flexible on premises o en la nube

La solución QRadar SIEM se puede entregar como hardware, software o máquinas virtuales (VM) para entornos on premises o de IaaS. Comience por una solución todo en uno o escale a un modelo ampliamente distribuido en varios segmentos de red y geografías.

Asimismo, la solución permite la integración con servicios en la nube, como Amazon Web Services (AWS), Microsoft Azure, SalesForce.com, Office 365 e IBM Cloud™, para que los analistas puedan detectar y responder mejor a amenazas, independientemente de dónde ocurran.

La plataforma QRadar permite la integración con servicios en la nube, como ser:

- AWS
- Azure
- SalesForce.com
- Office 365
- IBM Cloud™

Usa la infraestructura MITRE ATT&CK

Organizaciones alrededor del mundo están adoptando la infraestructura MITRE ATT&CK como base para el desarrollo de modelos de amenazas y metodologías específicos en el sector privado, el gobierno y la ciberseguridad. MITRE es una organización sin fines de lucro que ha desarrollado el modelo después de años de observar cómo funcionan los grupos adversarios reales.

El software QRadar SIEM permite la integración con IBM QRadar Advisor con Watson, que asigna automáticamente las tácticas y técnicas de MITRE ATT&CK para mejorar el incidente al ofrecer información de primera mano sobre las tácticas y etapas de un ataque que posiblemente esté empleando un actor malintencionado. Este proceso reduce significativamente el tiempo de investigación, ya que los analistas obtienen una comprensión inmediata de las tácticas empleadas por actores malintencionados, lo cual a su vez, acelera la respuesta y contención de amenazas. Menores tiempos de permanencia también disminuyen los costos de brechas de seguridad.

El Administrador de Casos de Uso de IBM QRadar configura la Aplicación Cibernética de Asignación de Infraestructura de Adversarios para invalidar las asignaciones predeterminadas y asignar sus reglas personalizadas a las tácticas y técnicas de MITRE ATT&CK. Al poder visualizar la cobertura de amenazas en la infraestructura MITRE ATT&CK, los analistas de seguridad no solo pueden detectar amenazas en base al comportamiento del adversario, sino que también pueden identificar en forma proactiva brechas y áreas de cobertura de seguridad inadecuada, ver asignaciones de tácticas y técnicas predefinidas, y añadir sus propias asignaciones personalizadas para mejorar la cobertura de seguridad.

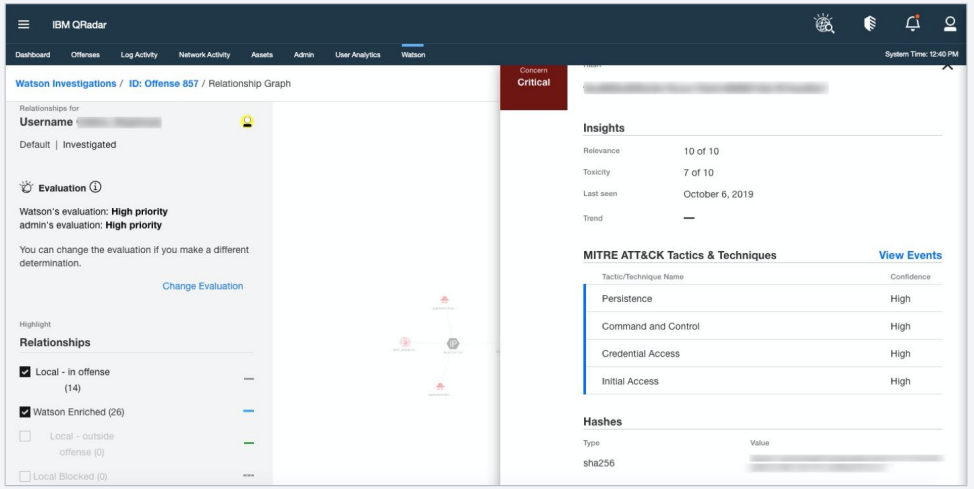


Figura 4: La aplicación QRadar Advisor con Watson asigna automáticamente tácticas y técnicas de MITRE ATT&CK al Motor de Reglas Personalizadas (CRE).

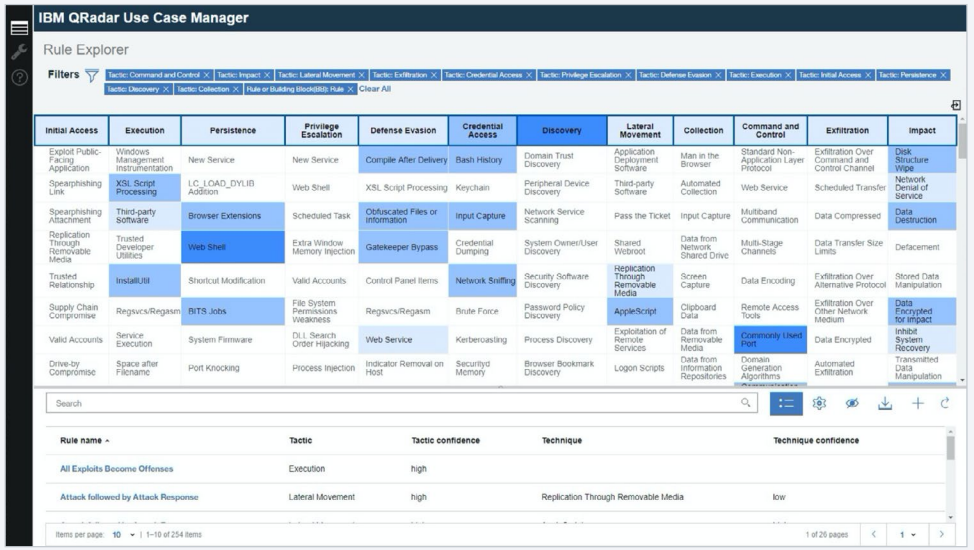


Figura 5: Gestor de Casos de Uso de QRadar

Resuelve la brecha de habilidades con IA

IBM QRadar Advisor con Watson ayuda a los analistas a obtener insights más profundos más rápidamente en relación con infracciones para tomar decisiones más informadas. La solución puede aprovechar datos no estructurados y ofrecer un gráfico de información visual que muestra el alcance completo de la amenaza en el entorno. Estos insights mejorados ayudan a reducir el tiempo dedicado a investigaciones y permiten que los analistas tomen decisiones más informadas más rápidamente.

Impulse a su equipo SOC con QRadar Advisor con Watson →

"IBM QRadar Advisor con Watson es un verdadero avance para nosotros y nuestros clientes. Mediante Watson, nuestros analistas pueden realizar tareas un 50 % más rápidamente que aquellos sin la solución Watson. Al incorporar la experiencia de primer nivel de Sogeti e IBM junto con una innovación superior, ayudamos a nuestros clientes a mejorar y fortalecer su ciberseguridad".

Vincent Laurens
Vicepresidente y ejecutivo de prácticas de ciberseguridad, Sogeti Luxembourg

Lea el caso de estudio →

Aborda los requisitos de conformidad

Con contenido, reglas e informes preconfigurados, QRadar SIEM ofrece la transparencia y la responsabilidad necesarias para ayudar a las organizaciones a abordar los requisitos de conformidad del sector. La solución ofrece paquetes de conformidad listos para usar con respecto al Reglamento General de Protección de Datos (RGPD), la Ley Federal de Gestión de la Seguridad de la información (FISMA), la Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA), ISO 27001, el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) y más. Estos paquetes se incluyen con una licencia de QRadar SIEM y están disponibles en IBM Security App Exchange.

Logre que su organización esté en conformidad con las normas →

75 %
de las organizaciones

afirma que la privacidad de datos es un imperativo estratégico para ellos. Gracias a normas como el RGPD, los clientes son más conscientes de sus derechos a la privacidad.[4]

Impulsa la respuesta ante incidentes con coordinación de seguridad

QRadar ofrece una integración fluida con la plataforma de Orquestación, Automatización y Respuesta ante Incidentes de Seguridad de IBM Resilient (SOAR), la cual aporta mejoras significativas a la manera en que su organización responde a ataques cibernéticos al automatizar y organizar personas, procesos y tecnología.

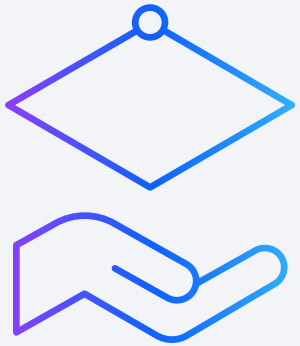
Al combinar la plataforma Resilient SOAR con una implementación existente de QRadar, sus analistas de seguridad pueden reducir el tiempo de corrección de incidentes al escalar infracciones sospechosas de manera rápida y eficiente de QRadar a Resilient, activar mejoras automatizadas adicionales e impulsar procesos de investigación completos. A medida que los incidentes evolucionan, toda la información se sincroniza entre QRadar y Resilient, lo cual garantiza una completa integridad de datos y un ciclo de retroalimentación continuo para mejorar la precisión de detección de amenazas.

Explore IBM Security Resilient →

Ayuda a maximizar sus inversiones en seguridad con IBM Security App Exchange

Explore IBM Security App Exchange y descubra más de 200 aplicaciones, integraciones, extensiones y paquetes de contenido validados de IBM y nuestro ecosistema de asociados. Conozca nuevos casos de uso e integraciones, y amplíe sus capacidades existentes para defender mejor su empresa.

Descubra nuevas aplicaciones y extensiones para mejorar QRadar →



Proceso de migración

No caben dudas de que migrar a una solución SIEM de última generación puede aumentar su eficiencia de SOC, permitirle proteger mejor su organización, gestionar incidentes y observar las normas de conformidad.

Según los requisitos de su empresa, su enfoque sobre la migración será diferente. En forma similar, la línea de tiempo y los hitos de migración también pueden ser diferentes. La situación más simple se da cuando una organización retira su SIEM tradicional y pasa a la plataforma IBM QRadar SIEM. Otra situación se da cuando la empresa A, que prefiere una plataforma SIEM más moderna, adquiere la empresa B, retira sus viejos sistemas e implementa QRadar. En cualquiera de estas situaciones, la migración es la elección lógica.

IBM Security recomienda un proceso de migración de tres pasos para que su organización pase a una solución de SIEM de última generación. Es un enfoque en fases que incluye procesos de planificación, migración y optimización, y cada fase se desarrolla en base a la anterior. El equipo de IBM Security, con sus décadas de experiencia y procedimientos recomendados, ofrece la orientación y experiencia necesarias para cada uno de estos pasos en el recorrido de migración.

Cambio instantáneo a QRadar	**Estrategia de migración** a QRadar
Active QRadar	
Recorte fuentes de registros	Canal de la SIEM actual a QRadar
Migre reglas y paneles de instrumentos	
Dé de baja la SIEM actual y mantenga la conformidad	Conserve la SIEM actual para informes limitados
Opciones de implementación pequeñas, medianas y grandes	Amplíe los insights con capacidades nativas
Consultoría de expertos de seguimiento y **migración de trespasos →**	

Tabla 1: Dos estrategias de migración

Ahora, revisemos el proceso de migración de tres pasos:

Evalúe y planifique

Migre

Optimice

Evalúe y planifique

En primer lugar: conozca sus metas y su plan. ¿Cuáles son sus desafíos comerciales? ¿Planea que la plataforma SIEM esté on premises o en una nube pública o híbrida? Sea cual fuere el modelo de implementación, el equipo de IBM QRadar puede trabajar con su organización para lanzar el proyecto y definir requisitos.

El entregable de esta etapa de planificación es un plan de migración de QRadar que describe cómo se configurará QRadar y cómo el equipo migrará los datos de eventos históricos existentes, si está dentro del alcance. El plan también incluirá qué casos de uso, informes, aplicaciones, paneles de instrumentos y alertas se implementarán en QRadar una vez que esté en funcionamiento.

El equipo de IBM guiará a su equipo de seguridad por el taller de planificación de migración o más, según se requiera. Este proceso incluirá revisar y obtener requisitos comerciales y técnicos necesarios para la migración. Por último, se creará un plan de migración. Se necesita experiencia, tanto de usted como del equipo de IBM, como parte de la revisión y obtención de requisitos.

Estos son algunos de los pasos que puede tener que realizar:

Revisión de los requisitos comerciales evaluando:

- Qué casos de uso existentes necesitan replicarse en QRadar
- Casos de uso adicionales de inteligencia de seguridad, recomendados por IBM o deseados por el cliente
- Conformidad y auditoría de necesidades de informes
- Presentación de informes y requisitos de panel de instrumentos
- Sistemas de gestión de vulnerabilidades:
- Integración con la respuesta a incidentes y herramientas de creación de tickets
- Modelos de recuperación ante desastres
- Gestión de SIEM posterior a la migración
- Desarrollo de capacidades de QRadar

Determinar los requisitos técnicos, como ser:

- Información detallada de fuentes de registros y flujos, incluida la jerarquía de red y la información de dispositivos y aplicaciones
- Requisitos de Módulos de Soporte de Dispositivos Universales (uDSM) personalizados
- Cómo trasladar la recopilación de datos de otra SIEM a QRadar
- Consideraciones de infraestructura de red, como firewalls y puertos
- Roles de usuario y acceso
- Migración de datos de eventos históricos existentes

Prepare un plan de migración que incluya:

- Detalles de los requisitos comerciales y técnicos obtenidos durante las sesiones de recopilación de requisitos
- Diagramas de arquitectura y diseño
- Procedimientos obligatorios para la migración, incluidos los de migración de datos y traslado de fuentes de registros
- Requisitos de personalización e integración o recomendaciones, de haber alguna

Migre

Durante esta fase, los especialistas de IBM implementarán la solución QRadar y migrarán datos y elementos de configuración de la SIEM de terceros. El ajuste le permitirá aislar resultados de infracciones priorizadas, de manera que pueda centrarse en lo que realmente demanda su atención. El último entregable de esta fase es una Guía de arquitectura e implementación de IBM QRadar, la cual se entregará al equipo del cliente después de la migración.

Esta actividad incluye las siguientes tareas:

- Configure y pruebe los dispositivos QRadar, las VM, las aplicaciones basadas en la nube o los nodos de software para esta participación mediante la lista de verificación de implementación detallada.
- Replique los elementos de configuración de la SIEM de terceros a QRadar.
- Realice la recopilación de registros de traslado de la SIEM de terceros a QRadar. En la fase de planificación, se establecerá un procedimiento detallado para este proceso.
- Aborde problemas con la ingesta y el análisis de datos.
- Cree módulos personalizados de soporte de dispositivos para analizar datos de registro de fuentes de registro no compatibles con la aplicación QRadar disponible para la compra (OTB).
- Si se requiere, migre datos de eventos históricos existentes a QRadar.
- Configure la retención de datos y copias de seguridad.
- Verifique la recolección de eventos y flujos de la implementación existente a nuevos dispositivos.
- Verifique el estado de la implementación y las configuraciones de rendimiento.
- Por último, prepare una guía detallada de implementación y arquitectura de QRadar que indique todas las facetas de la implementación de QRadar.

Optimice

Después de la migración, las reglas y la analítica se personalizarán para abordar las necesidades únicas de su entorno. El equipo de QRadar ofrecerá capacitación y tutoría prácticas para que su equipo pueda admitir su nueva solución de manera eficaz y continua. Este enfoque se ejecutará a un ritmo adecuado para clientes individuales, ya sea un enfoque “big bang” o un enfoque paralelo en fases.

A medida que realiza estos pasos, podrá desactivar el sistema antiguo y trabajar en su nueva base de SIEM, para evolucionar en forma gradual hacia un nuevo modelo operativo. El equipo de IBM es el que suele decidir si se deben realizar actualizaciones a la Guía de arquitectura e implementación de QRadar.

Si aún no ha comenzado a trabajar en la migración de SIEM, no espere más. Como puede ver, una migración de SIEM puede presentar importantes desafíos No obstante, al adoptar un enfoque estratégico y en fases, conforme recomienda IBM Security, debería poder pasar sin inconvenientes a un estado estable.

Por último, al migrar a una plataforma SIEM de última generación, coloca a su organización en la senda del éxito. La solución SIEM puede mejorar la capacidad de su equipo de identificar amenazas en forma proactiva, defenderse contra posibles brechas y hacer más eficiente su SOC.

Esta actividad incluye los siguientes pasos principales:

Configure QRadar para admitir los requisitos comerciales documentados. Este proceso incluye la configuración:

- Reglas y casos de uso personalizados
- Informes, alertas y paneles de instrumentos
- Canales de amenazas
- Aplicaciones de QRadar, incluida, entre otras, la analítica de comportamiento de usuarios, la inteligencia de implementación de QRadar y el pulso.

Realice ajustes para reducir el ruido blanco y los falsos positivos, y mejorar el rendimiento.

Integración con la respuesta a incidentes y herramientas de creación de tickets.

Proporcione el desarrollo de capacidades de QRadar a los recursos requeridos del cliente.

Transición de la solución de estado estable al equipo SOC del cliente o el proveedor de servicios gestionados.

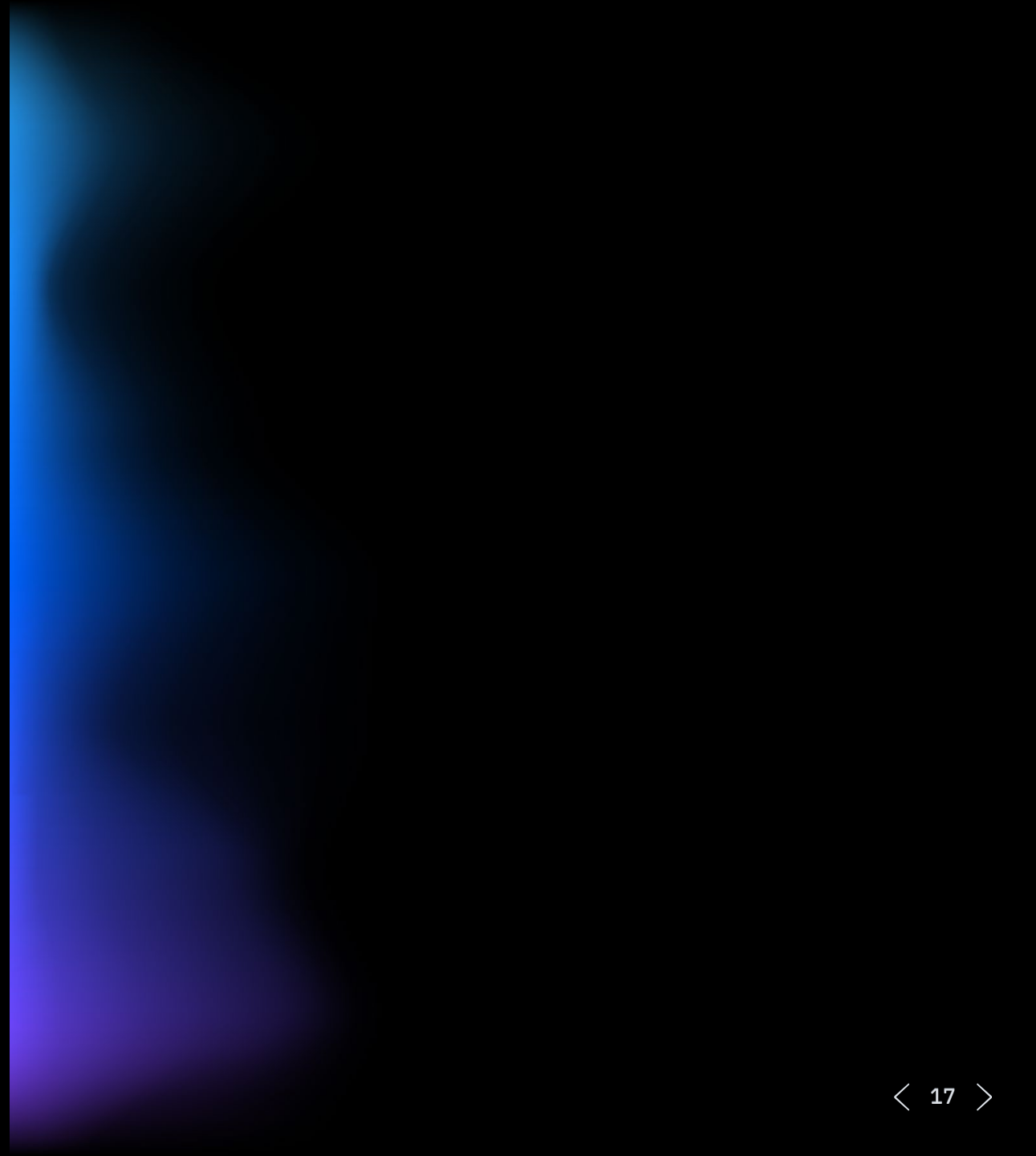
¿Y después?

IBM QRadar puede ayudarle a reducir las complicaciones causadas por soluciones desactualizadas y abordar problemas de seguridad, sin importar dónde implementa aplicaciones, ya sea en un modelo on premises, híbrido o SaaS.

Desde obtener visibilidad completa de datos hasta detectar rápidamente posibles amenazas mientras observa la conformidad, QRadar ofrece analítica, reglas de correlación y paneles de instrumentos listos para usar, para que se mantenga a la vanguardia del panorama SIEM.

Otorgue a su equipo de seguridad las herramientas adecuadas.

Actualice a una plataforma SIEM de última generación. →



¿Por qué IBM?

IBM Security ofrece uno de los portafolios de productos y servicios de seguridad empresarial más avanzados e integrados. Este portafolio, que cuenta con el respaldo de la mundialmente reconocida investigación de X-Force, proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger holísticamente sus infraestructuras, datos y aplicaciones. Ofrece soluciones para la gestión de la identidad y del acceso, la seguridad de bases de datos, el desarrollo de aplicaciones, la gestión del riesgo, la gestión de terminales, la seguridad de la red y más.

Estas soluciones permiten que las organizaciones gestionen el riesgo de manera efectiva e implementen una seguridad integrada para dispositivos móviles, nubes, redes sociales y otras arquitecturas de negocios empresariales. IBM opera una de las mayores organizaciones de investigación, desarrollo y entrega de seguridad del mundo, supervisa 15 mil millones de eventos de seguridad diarios en más de 130 países y posee más de 3.000 patentes de seguridad.

Además, IBM Global Financing ofrece diversas formas de pago para ayudarlo a adquirir la tecnología que necesita para hacer crecer su empresa. IBM ofrece la gestión completa del ciclo de vida de los productos y servicios de TI, desde su adquisición hasta su desecho. Para obtener más información, visite ibm.com/financing.

Para obtener más información sobre la plataforma de inteligencia de seguridad IBM QRadar, comuníquese con su representante de IBM o socio comercial de IBM, o visite: ibm.com/mx-es/products/hosted-security-intelligence.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Producido en los Estados Unidos de América en mayo de 2020

Este documento se actualizó por última vez en la fecha de su publicación y puede ser modificado por IBM en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

1 Jon Oltsik. "Big Changes Are Coming to Security Analytics and Operations." *Dark Reading*, 11 de diciembre de 2019. www.darkreading.com/cloud/big-changes-are-coming-to-security-analytics-and-operations/a/d-id/1336565

2 "Cost of a Data Breach Report highlights." *IBM*. ibm.com/security/data-breach

3 "QRadar Security Intelligence Client Study." *Ponemon Institute*, diciembre de 2018. ibm.com/downloads/cas/M9YRMAKZ

4 "Data Privacy Is The New Strategic Priority." Forrester Opportunity Snapshot: A custom study commissioned by IBM, julio de 2019. ibm.com/account/reg/us-en/signup?formid=urx-39964

WGW03245-USEN-01