IBM Security

IBM

IBM QRadar on Cloud

Detecta rápidamente las amenazas y cumple con las regulaciones con una solución Saas flexible y altamente escalable

Introducción

A medida que evoluciona el panorama de amenazas, las organizaciones ya no pueden confiar en las auditorías de cumplimiento de normas establecidas. En cambio, necesitan una visibilidad integral de las amenazas y los riesgos dentro de su entorno para poder proteger mejor los datos confidenciales y los activos de los atacantes más experimentados. Y necesitan lograr esto a pesar de la reducción del talento de seguridad cibernética. Las soluciones de inteligencia de seguridad más importantes pueden ayudar a las organizaciones a obtener una visión de seguridad *end-to-end* en entornos locales y basados en la nube, sin requerir meses de servicios profesionales o grandes inversiones en personalización. Cuando se entregan desde la nube, estas soluciones también pueden ofrecer una configuración y escalado más rápidos, acceso a recursos dedicados de DevOps, un menor costo de propiedad y resistencia y redundancia incorporadas.

IBM® QRadar® on Cloud es una solución altamente escalable de Información de Seguridad y Gestión de Eventos (SIEM) que consolida los datos de registro, eventos y flujo de miles de dispositivos distribuidos en redes locales y basadas en la nube, realizando correlaciones y análisis inmediatos para distinguir amenazas reales de falsos positivos. QRadar on Cloud ayuda a los equipos de seguridad a detectar y priorizar con precisión las amenazas, y proporciona información inteligente que permite a los equipos responder rápidamente para reducir el impacto de los incidentes.

Esta publicación explora las ventajas de utilizar una solución de inteligencia de seguridad preparada para la empresa, proporcionada desde IBM® Cloud™ con capacidades opcionales de monitoreo de amenazas proporcionadas por los Servicios de IBM o por un Proveedor de Servicios de Seguridad Administrada (MSSP). Analizará cómo IBM QRadar on Cloud, una oferta de Seguridad como Servicio (SaaS), permite a las organizaciones mantenerse a la vanguardia de las últimas amenazas con tecnología líder en la industria combinada con la experiencia confiable de IBM, lo que resulta en una mayor flexibilidad, rentabilidad y tranquilidad.

La inteligencia de seguridad es vital en los entornos actuales de nube híbrida

Para mantenerse al frente de los atacantes, los equipos de seguridad necesitan información procesable sobre las amenazas más críticas que ocurren en sus entornos.

Las herramientas de análisis e inteligencia de seguridad adecuadas pueden ayudar a:

- Reducir una gran cantidad de eventos de seguridad a una pequeña cantidad de delitos procesables
- Disminuir falsos positivos
- Informar a los equipos de seguridad sobre lo que ha sido explotado y qué actividad maliciosa ha tenido lugar como resultado, por ejemplo pérdida de datos, robo o fraude.
- Proporcionar una detección de amenazas más rápida y acelerar la respuesta a incidentes.

Las soluciones de inteligencia de seguridad utilizan analítica de seguridad avanzados y automatización para proporcionar evaluaciones más precisas sobre las amenazas. Estas soluciones están diseñadas para recopilar, normalizar, correlacionar y condensar grandes cantidades de datos, incluidos el tráfico de red, los registros, el comportamiento del usuario, las configuraciones del sistema, los informes de vulnerabilidad y otros, en alertas accionables y priorizadas que notifican a los equipos de seguridad, tanto sobre amenazas conocidas como desconocidas.

Las actividades del sistema y de la red de entornos locales y en la nube se pueden recopilar y analizar utilizando un enfoque coherente e integrado. Con la expectativa de que la TI local y la TI en la nube deben coexistir, es importante implementar una solución de inteligencia de seguridad que sea lo suficientemente flexible como para adaptarse a un entorno mixto en la nube y local y manejar las fuentes de datos a través de una amplia gama de infraestructuras.

IBM ofrece inteligencia y analítica de seguridad avanzadas, alojadas en la nube

La dura realidad es que las organizaciones de TI de hoy deben trabajar con presupuestos cada vez más limitados. En lugar de desplegar otra solución puntual, necesitan una plataforma integrada que pueda proporcionar inteligencia de seguridad avanzada con un tiempo de valor rápido, a la vez que proporciona la escalabilidad y la funcionalidad necesarias para cumplir de manera rápida y fácil los nuevos requisitos.

Visibilidad integrada end-to-end

IBM QRadar on Cloud proporciona una forma rápida, fácil y rentable de satisfacer las necesidades cambiantes de inteligencia y analítica de seguridad. La solución ofrece capacidades SIEM listas para el mercado como una solución SaaS, eliminando la necesidad de administración de infraestructura.

Con IBM QRadar on Cloud, los clientes pueden pasar hasta el 100 por ciento de su tiempo disponible monitoreando eventos de seguridad en su entorno, investigando incidentes potenciales y desarrollando conocimiento sobre actividades normales versus actividades sospechosas. QRadar on Cloud está diseñado para ofrecer resistencia y ayudar a proteger su organización contra fallas de hardware. También se beneficia de la alimentación de datos de IBM X-Force® Threat Intelligence para proporcionar las últimas ideas sobre amenazas y ataques recientemente descubiertos.

Las principales capacidades de la oferta de IBM QRadar on Cloud incluyen:

- Una arquitectura única para analizar eventos, registros, flujos, vulnerabilidad, datos de usuarios y activos
- Correlación casi en tiempo real y detección de anomalías de comportamiento para identificar amenazas de alto riesgo
- Detección de incidentes de alta prioridad entre miles de millones de puntos de datos
- Información y visibilidad de la red, la aplicación y la actividad del usuario.
- Cumplimiento normativo optimizado con capacidades de recopilación, correlación e informes listos para usarse

QRadar on Cloud ofrece las capacidades clave de IBM QRadar SIEM configuradas según las especificaciones del cliente y desplegadas dentro de un entorno de nube privada exclusiva. La solución está alojada por IBM dentro de los centros de datos seguros de IBM Cloud con resistencia integrada y una infraestructura de soporte de respaldo.

Cómo funciona

QRadar on Cloud es un componente de la Plataforma de inteligencia de seguridad de IBM QRadar, que ofrece capacidades integradas para la gestión de registros, SIEM, gestión de riesgos y vulnerabilidades, análisis de comportamiento del usuario e inspección de paquetes de red. Los equipos de seguridad pueden acceder a las capacidades de QRadar SIEM desde un navegador web, tal como lo harían si la infraestructura se implementara en las instalaciones. Pero los expertos de IBM administran la infraestructura, el mantenimiento continuo, la recuperación ante desastres y el soporte técnico.

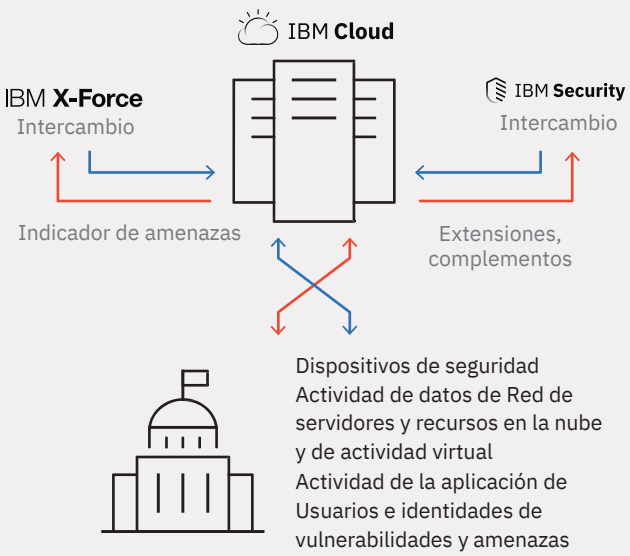
Los clientes pueden comenzar con la administración básica de registros y los informes de cumplimiento y, luego, agregar a lo largo del tiempo más capacidades y servicios, a medida que su equipo crece. Las soluciones competitivas más simples carecen de la capacidad de agregar gestión de vulnerabilidades, analítica de comportamiento del usuario (UBA) o inspección de paquetes de red, lo que puede dar lugar a inversiones desactualizadas que pueden caerse cuando ocurre un ciberataque real.

Opcionalmente, IBM Global Security Services o uno de los socios MSSP de IBM Security pueden ofrecer una amplia gama de servicios complementarios de monitoreo de amenazas para cubrir casos de uso esenciales o avanzados, o pueden ayudar por separado con servicios de respuesta de emergencia para remediar las fallas de red confirmadas.

QRadar on Cloud está diseñado para:

- Recopilar y correlacionar más de 400.000 eventos por segundo de fuentes locales y basadas en la nube para detectar patrones de comportamiento malicioso y permitir una respuesta más rápida a amenazas críticas
- Escale hacia arriba y hacia abajo para satisfacer necesidades comerciales dinámicamente cambiantes
- Ayuda a asegurar la resistencia y disponibilidad de la empresa con personal experto que supervisa el estado del servidor, instala parches críticos y actualiza el software
- Está alineada con el modelo de presupuesto de gastos operativos de una organización presentando facturación mensual y opciones de pago flexibles, en oposición al presupuesto tradicional basado en grandes gastos de capital iniciales
- Ayuda a atender la escasez de habilidades al reducir el tiempo de implementación y los gastos generales asociados con la administración de dispositivos
- Incluye inteligencia integral sobre amenazas de investigación y desarrollo de IBM X-Force, uno de los equipos de investigación de seguridad comercial más respetados

Modelo de implementación de IBM QRadar on Cloud



- Oferta basada en la nube de la solución de inteligencia de seguridad n.° 1
- Recopila datos de recursos locales y en la nube
- Aprovecha la inteligencia de amenazas en tiempo real de X-Force
- Incluye acceso a funciones de valor agregado desde App Exchange

Comience su viaje hacia una solución SIEM alojada basada en la nube

QRadar on Cloud proporciona a las organizaciones un acceso rápido a la tecnología SIEM líder en el mercado, la flexibilidad para satisfacer necesidades cambiantes y la confianza de un equipo de servicio de clase mundial. Además, la oferta de IBM permite a las organizaciones adoptar un enfoque gradual de los servicios de seguridad alojados en la nube. Las organizaciones pueden comenzar subcontratando la infraestructura central de SIEM y, opcionalmente, agregar servicios o migrar a un compromiso de servicios administrados aún más integral con el tiempo.

Flexibilidad

QRadar on Cloud está diseñado para admitir una amplia variedad de casos de uso de seguridad. Las organizaciones no tienen que preocuparse por los grandes gastos de capital iniciales, la implementación y administración de infraestructura onerosa o los gastos de mantenimiento de TI; simplemente pueden planificar los gastos operativos a través de la facturación periódica.

Al mismo tiempo, QRadar on Cloud permite a las organizaciones personalizar el servicio para satisfacer sus necesidades específicas. Para ayudar a los clientes a ponerse en marcha rápidamente, la solución ofrece más de 450 integraciones listas para usarse con productos comerciales, así como un editor de módulo de seguridad de dispositivo (DSM) personalizado para recopilar y analizar fácilmente fuentes de registro personalizadas.

Una vez que se despliega la solución, los clientes pueden aprovechar más de 150 aplicaciones desarrolladas previamente y paquetes de contenido de IBM Security App Exchange para agregar nuevas integraciones, reglas, analítica, búsquedas, paneles e informes. Las API abiertas y un SDK permiten a los clientes y socios desarrollar opcionalmente sus propias aplicaciones para atender casos de uso personalizados y ampliar el valor de las soluciones existentes. Con QRadar on Cloud, las organizaciones obtienen la flexibilidad para adaptarse a sus propios requisitos, con la seguridad de que la infraestructura subyacente está configurada de acuerdo con las mejores prácticas de seguridad.

Confianza

En lugar de lidiar con el alto costo de capital y la complejidad de una infraestructura local, las empresas que utilizan QRadar on Cloud cuentan con la ayuda de expertos de IBM por un costo predecible que se alinea con sus

presupuestos de operaciones. La solución se usa hoy y las organizaciones líderes de todo el mundo confían en ella, entre ellas:

- Una compañía energética líder que redujo dos mil millones de registros y eventos por día a 25 delitos de alta prioridad.
- Un proveedor de información financiera que rastreó 250 líneas de base de actividad y ahorró del 50 al 80 por ciento en personal
- Un banco global que identificó y bloqueó más de 650 incidentes sospechosos en los primeros seis meses de operaciones de seguridad.

Conclusión

IBM QRadar permite a los equipos de seguridad recopilar, correlacionar y analizar información de los silos de datos, incluida la nube, para detectar y priorizar automáticamente las amenazas. Y ahora, QRadar on Cloud ofrece a las organizaciones una forma de acceder a las capacidades de QRadar sin tener que administrar la infraestructura por sí mismas.

QRadar on Cloud proporciona a las organizaciones un punto de partida para la inteligencia de seguridad entregada en la nube, pero es un punto de partida que proviene de un proveedor confiable, que ofrece tecnología SIEM líder en la industria, respaldada por servicios y soporte expertos. Con el tiempo, las organizaciones pueden continuar opcionalmente la migración a una solución totalmente externalizada. Con una visibilidad profunda tanto de la infraestructura en la nube como local, QRadar on Cloud puede ayudar a las organizaciones a estar un paso al frente de las amenazas más recientes.

Para obtener más información

Para obtener más información sobre la plataforma de inteligencia de seguridad de IBM QRadar, comuníquese con su representante de IBM o socio comercial de IBM, o visite: ibm.com/qradar

Acerca de las soluciones de seguridad de IBM

IBM Security ofrece uno de los catálogos de productos y servicios de seguridad empresarial más avanzados e integrados. La cartera, respaldada por la renombrada investigación y desarrollo de X-Force, proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger de manera integral a sus personas, infraestructura, datos y aplicaciones, ofreciendo soluciones para la gestión de identidad y acceso, seguridad de bases de datos, desarrollo de aplicaciones, gestión de riesgos, administración de puntos finales, seguridad de 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 organizaciones de investigación, desarrollo y oferta de seguridad más amplias del mundo, supervisa más de 60.000 millones de eventos de seguridad por día en más de 130 países y posee más de 3.700 patentes de seguridad.

Además, IBM Global Financing ofrece diversas formas de pago para ayudarle a adquirir la tecnología que necesita para hacer crecer su empresa. Proporcionamos una gestión de todo el ciclo de vida de los productos y servicios de TI, desde su adquisición hasta su eliminación. Para obtener más información, visite: ibm.com/financing

IBM Security
Route 100
Somers, NY 10589

Producido en los Estados Unidos de América,
enero de 2019.

1 "Las 10 predicciones de computación en la nube de Forrester para 2018". Louis Columbus. Forrester Noviembre de 2017. https://www.forbes.com/sites/louiscolumbus/2017/11/07/forresters-10- cloud-computing-predictions-for-2018/#8e9bc914ae18

2 "El Estudio Global de la Fuerza Laboral de Seguridad de la Información 2017: Mujeres en la ciberseguridad". Frost & Sullivan. Marzo de 2017. https://iamcybersafe.org/wp-content/uploads/2017/03/ WomensReport.pdf