Plataforma de Inteligencia de Seguridad IBM QRadar

Proporcionar inteligencia accionable para seguridad y cumplimiento empresarial

Destacado

- Integre información de seguridad y administración de eventos (security information and event management, SIEM), detección de anomalías, administración de registros, administración de vulnerabilidad, administración de riesgos y análisis de incidentes en una solución unificada.
- Aproveche una única arquitectura para analizar datos de registros, flujo, vulnerabilidades, usuarios y activos.
- Use correlación en tiempo real y detección de anomalías en el comportamiento para identificar amenazas sofisticadas.
- Identifique incidentes de alta prioridad en miles de millones de puntos de datos.
- Obtenga una visibilidad 360º de la actividad de red, aplicaciones y atacantes.
- Automatice las actividades de recopilación, correlación e informes.

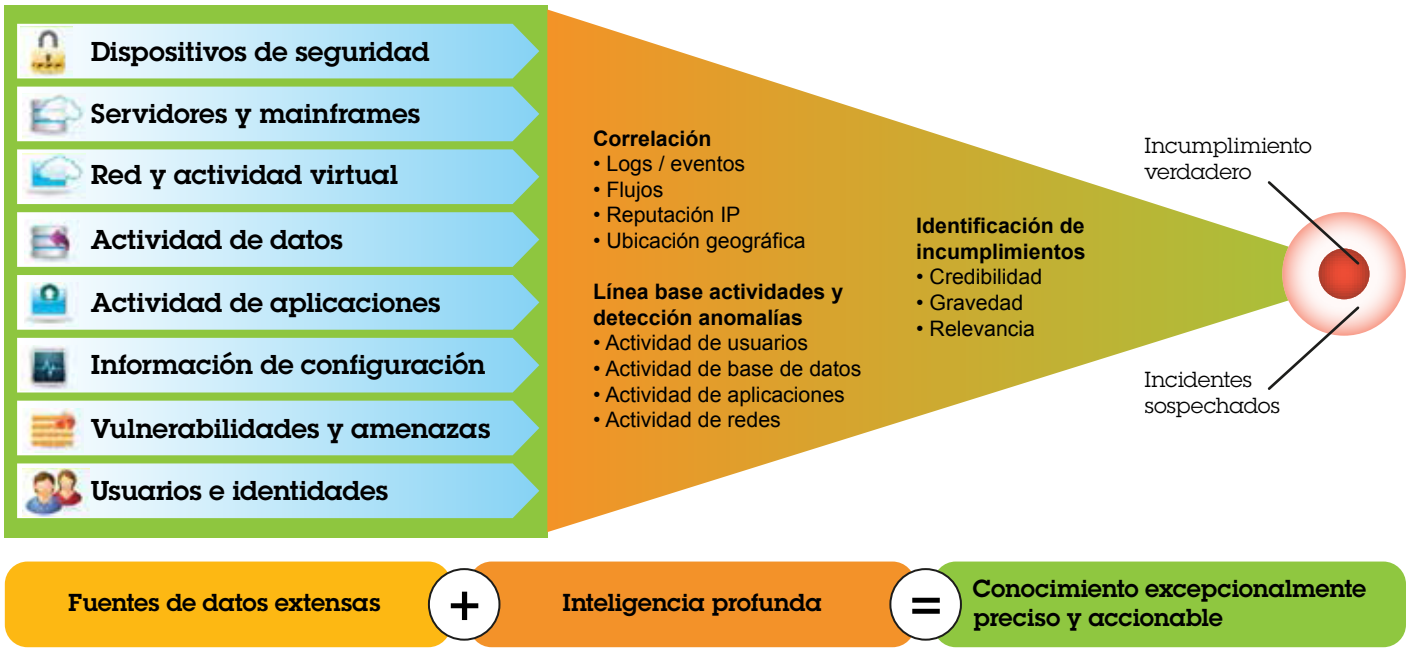
La Plataforma de Inteligencia de Seguridad IBM® QRadar® integra SIEM, administración de registros, detección de anomalías, administración de vulnerabilidades, administración de riesgos y análisis de incidentes en una solución unificada. Como utiliza inteligencia, integración y automatización para proporcionar una visión de la seguridad de 360 grados, esta solución se traduce en una detección de amenazas superior, mayor facilidad de uso y potencialmente menor costo de propiedad.

La Plataforma de Inteligencia de Seguridad QRadar usa inteligencia, integración y automatización para ofrecer beneficios de seguridad y cumplimiento que son invalorables en el mundo inteligente de hoy, en el que las empresas instrumentadas, interconectadas e inteligentes recopilan, procesan, usan y almacenan más información que nunca antes.

Las organizaciones hoy están expuestas a un mayor volumen y variedad de ataques que en el pasado. Los atacantes avanzados son inteligentes y pacientes, y apenas dejan rastro de su presencia. La Plataforma de Inteligencia de Seguridad QRadar constituye una familia de productos integrados que puede ayudar a detectar amenazas que otros sistemas pasan por alto. Ayuda a detectar y defenderse contra amenazas aplicando analítica sofisticada a una mayor cantidad de tipos de datos. Al hacerlo, contribuye a identificar incidentes de alta prioridad que de otro modo podrían pasar inadvertidos.

La Plataforma de Inteligencia de Seguridad QRadar puede ayudar a resolver una serie de problemas de negocio, entre otros:

- Consolidar silos de datos en una solución integral
- Identificar robo y fraude dentro de la organización
- Administrar vulnerabilidades, configuraciones, cumplimiento y riesgos
- Investigar incidentes y violaciones
- Abordar requisitos regulatorios



Ofrecer inteligencia, integración y automatización

La Plataforma de Inteligencia de Seguridad QRadar usa inteligencia, integración y automatización, con el objetivo de ofrecer beneficios de seguridad y cumplimiento que son invalorables en el mundo inteligente de hoy, en el que las empresas instrumentadas, interconectadas e inteligentes recopilan, procesan, usan y almacenan más información que nunca antes.

Consolidar silos de datos

Si bien existe un gran cúmulo de información en los datos de registro, flujo de red y procesos de negocio de una organización, esta información a menudo se encuentra aislada en silos, ignorada o subutilizada. QRadar permite la convergencia de vistas de red, seguridad y operaciones en una única solución flexible. Derriba los tabiques entre los silos mediante la correlación de registros con flujos de red y una multitud de otros datos, presentando virtualmente toda la información relevante en una sola pantalla. Esto contribuye a habilitar una detección de amenazas superior y una visión mucho más rica de la actividad empresarial.

Detectar fraude interno

Algunas de las amenazas más graves a la seguridad de una organización provienen de su interior, pero las organizaciones a veces carecen de los dispositivos inteligentes necesarios para detectar fuentes maliciosas internas o externas que ponen en peligro sus cuentas. Al combinar la supervisión de aplicaciones y usuarios con visibilidad de red al nivel de las aplicaciones, las organizaciones pueden estar mejor preparadas para detectar desviaciones significativas de la actividad normal, lo cual ayuda a detener un ataque antes de que se concrete.

Predecir y remediar riegos y vulnerabilidades

Los equipos de seguridad, red e infraestructura se esfuerzan por administrar el riesgo identificando vulnerabilidades y priorizando la remediación antes de que se produzca una violación. La Plataforma de Inteligencia de Seguridad QRadar integra la gestión de riesgos, configuraciones y vulnerabilidades con capacidades SIEM, que incluyen analítica de flujo de red y correlación, para proporcionar mejor conocimiento de las vulnerabilidades críticas. Como resultado, las organizaciones pueden remediar riesgos con más eficiencia y eficacia.

Realizar analítica forense

La analítica forense integrada de QRadar ayuda a los equipos de seguridad de TI a reducir el tiempo que dedican a investigar incidentes de seguridad, y elimina la necesidad de capacitación especializada. Expande las búsquedas de datos de seguridad para incluir capturas de paquetes completos y documentos de texto, voz e imagen digitalmente almacenados. Ayuda a presentar claridad sobre qué pasó y cuándo pasó, quién intervino y qué datos fueron visualizados o transferidos en un incidente de seguridad. Como resultado, ayuda a remediar una violación en las redes y puede ayudar a prevenir que se produzcan nuevamente.

Abordar mandatos de cumplimiento regulatorio

Muchas organizaciones se enfrentan al desafío de aprobar auditorías de cumplimiento y al mismo tiempo tener que realizar recopilación, supervisión e informe de datos con recursos cada vez más limitados. Para automatizar y simplificar las tareas de cumplimiento, QRadar proporciona recopilación, correlación e informes sobre actividades relacionadas con cumplimiento, con el respaldo de numerosas plantillas de información listas para usar.

Aprovechar analítica de seguridad fácil de usar

La Plataforma de Inteligencia de Seguridad QRadar ofrece una arquitectura unificada para almacenar, correlacionar, consultar e informar sobre datos de registros, flujos, vulnerabilidades, activos y usuarios maliciosos. Combina analítica sofisticada con reglas, informes y dashboards listos para usar. Mientras que es potente y escalable para empresas Fortune 500 y organismos gubernamentales, también es intuitivo y flexible para pequeñas y medianas organizaciones. Los usuarios se benefician con una obtención de valor potencialmente superior, menor costo de propiedad, mayor agilidad y mayor protección ante riesgos de seguridad y cumplimiento.

Inteligencia

Al analizar más tipos de datos y usar más técnicas analíticas, QRadar a menudo puede detectar amenazas que otras soluciones no detectan, y ayudar a elevar la visibilidad de la red, a diferencia de otras soluciones.

Integración

Con una plataforma común de aplicaciones, base de datos e interfaz de usuario, esta plataforma ofrece una escala masiva de administración de registros, sin comprometer la inteligencia en tiempo real de SIEM y analítica de comportamiento de red. Proporciona una solución común para todas las funciones de búsqueda, correlación, detección de anomalías y reporte. Una única interfaz intuitiva proporciona acceso sin interrupciones a todas las funciones de administración de registros, análisis de flujo, análisis forense, dashboards e informes.

Automatización

La Plataforma de Inteligencia de Seguridad QRadar es simple de implementar y administrar, y ofrece amplios módulos de integración pre-configurados y contenido de inteligencia de seguridad. Como automatiza muchas funciones de descubrimiento de activos, normalización de datos y sincronización, y ofrece reglas e informes listos para usar, la solución está diseñada para reducir la complejidad que a menudo inmoviliza a otros productos.

¿Por qué IBM?

IBM tiene la organización más extensa del mundo para investigación, desarrollo y entrega de seguridad. Incluye 10 centros de operaciones de seguridad, 9 centros IBM Research, 11 laboratorios de desarrollo de seguridad de software y un Instituto para Seguridad Avanzada, con capítulos en EE.UU., Europa y Asia Pacífico. Las soluciones de IBM habilitan a las organizaciones a reducir sus vulnerabilidades de seguridad y a enfocarse más en el éxito de sus iniciativas estratégicas. Estos productos capitalizan la especialización en inteligencia de amenazas del equipo de investigación y desarrollo de IBM X-Force® para proporcionar un enfoque preventivo de la seguridad. Como asesor de confianza en seguridad, IBM ofrece las soluciones para mantener toda la infraestructura empresarial, incluso en la nube, protegida de los últimos riesgos de seguridad.

Más información

Para conocer más sobre la Plataforma de Inteligencia de Seguridad IBM QRadar, contacte a su representante IBM o Asociado de Negocio IBM, o visite: ibm.com/security

Si quiere que un especialista de IBM lo contacte, **haga click aquí** y complete sus datos.

IBM Corporation

Software Group Route 100

Somers, NY 10589

Producido en EE.UU.

Septiembre 2014

Por favor recicle

WGD03019-COES-02