

IBM QRadar

Perciba y detecte las amenazas modernas con la más sofisticada plataforma de analítica de seguridad



Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

- Analizar datos de cargas de trabajo
- Comprender el contexto
- Perfilar usos

Casos de uso

- Detección avanzada de amenazas
- Protección de datos críticos
- Monitorización de amenazas internas
- Gestión de riesgos y vulnerabilidades
- Detección de tráfico no autorizado
- Investigación forense y persecución de amenazas

¿Por qué IBM?

- Su panel de control de seguridad
- Potencia para actuar a cualquier escala
- IBM Security App Exchange
- Plataforma única, visibilidad global

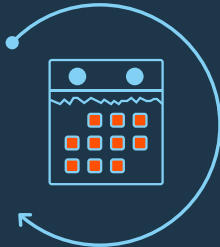
Para obtener más información

Conquiste lo desconocido

Los profesionales de la seguridad viven en un mundo de incertidumbre constante. Las amenazas y ataques golpean su organización desde todos los ángulos, a cada minuto de cada día. Cuando un atacante persistente consigue entrar, se mueve lentamente y en silencio. Busca datos valiosos y cubre sus huellas. De hecho, un estudio reciente descubrió que el tiempo medio para identificar un ataque

era de 156 días, y el tiempo medio para contenerlo, de 82 días.¹ En consecuencia, la vida en un Centro de operaciones de seguridad (SOC) es muy estresante; muchos equipos simplemente ignoran lo que no quieren saber.

Han pasado a la historia los tiempos en que la tarea de los equipos de seguridad se limitaba a asegurar el perímetro, bloquear distintas formas de acceso a Internet y apagar los últimos fuegos. En la actualidad, las organizaciones exigen conectividad mas ubicua para mantener a la empresa en funcionamiento y a la vez detener amenazas avanzadas, identificar fraudes y peligros internos, todo ello garantizando el cumplimiento continuo de la normativa. Los nuevos requisitos exigen analizar el máximo de información posible para detectar actividades amenazadoras ocultas bajo la superficie y dar una respuesta más rápida. Los analistas de SOC han de perfeccionar la capacidad de detectar desviaciones de la actividad normal y las soluciones que escojan deberán poder escalarse para llegar hasta el último rincón de la empresa con una misma plataforma cohesiva.



Los atacantes pueden estar al acecho en una organización durante
De 8 a 9 meses
antes de ser descubiertos.¹

¹ "2015 Cost of a Data Breach Study: Global Analysis" (Estudio sobre el coste de las filtraciones de datos: Análisis global), Ponemon Institute Research Report, mayo de 2015.



Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

- Analizar datos de cargas de trabajo
- Comprender el contexto
- Perfilar usos

Casos de uso

- Detección avanzada de amenazas
- Protección de datos críticos
- Monitorización de amenazas internas
- Gestión de riesgos y vulnerabilidades
- Detección de tráfico no autorizado
- Investigación forense y persecución de amenazas

¿Por qué IBM?

- Su panel de control de seguridad
- Potencia para actuar a cualquier escala
- IBM Security App Exchange
- Plataforma única, visibilidad global


Para obtener más información

Detecte las amenazas y actúe

Para mantenerse por delante, las organizaciones han de ser capaces de ‘percibir’ cadenas de actividades maliciosas de la misma forma que las personas perciben el peligro cuando ven, escuchan, huelen o sienten un entorno conflictivo. Necesitan una plataforma de seguridad capaz de:

- desplegarse rápidamente en toda la red, incluyendo recursos basados en el cloud
- detectar sutiles diferencias en el entorno, como intrusos latentes o infiltrados
- descubrir ataques sin depender de un número limitado de personas con formación muy especializada
- recopilar, normalizar y correlacionar miles de millones de eventos, dando prioridad a un pequeño número de cuestiones
- identificar las principales vulnerabilidades y riesgos para evitar intrusiones

El aspecto positivo es que los actuales analistas de SOC ya no están solos. De la misma manera que los atacantes se han agrupado para compartir sus conocimientos y técnicas, la comunidad de seguridad ha respondido compartiendo sus recursos. La emergencia de esta nueva inteligencia sobre amenazas y recursos para compartir aplicaciones contribuye a limitar la efectividad del nuevo malware y exploit kits, así como el impacto de las vulnerabilidades día cero o día uno. Sin embargo, muchos analistas de SOC siguen limitados por sistemas anticuados de gestión de registros o soluciones básicas de información de seguridad y gestión de eventos (SIEM) que generan un número excesivo de alertas utilizando una única instancia de comportamiento sospechoso.



Dar sentido a millones de eventos relacionados con la seguridad es casi imposible sin herramientas SIEM básicas.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Uso de la analítica para eliminar amenazas

Las vulneraciones de la seguridad más graves no comienzan con una gran explosión. Por el contrario, los ciberdelincuentes lanzan ataques ‘lentos y de baja intensidad’ que pueden prolongarse durante meses. ¿No sería estupendo poder identificar cambios en el entorno sutiles y relacionados y alertar a los equipos de seguridad cuando comiencen a pasar cosas raras?



IBM® QRadar® Security Intelligence Platform es la única solución de seguridad alimentada por IBM Sense Analytics, y que puede:

- desarrollar perfiles de usuarios y recursos según actividades de base legítimas
- detectar conductas anormales en personas (personal interior, colaboradores, clientes, invitados), redes, aplicaciones y datos
- relacionar las actividades sospechosas actuales e históricas para aumentar la precisión de los incidentes identificados
- recuperar y reproducir la actividad de la red e investigar el contenido de los paquetes en su forma original
- descubrir y priorizar puntos débiles antes de que sean explotados.

Los productos aislados que realizan análisis de un momento en el tiempo son poco fiables; no pueden asociar la nueva actividad en la red con los usuarios ‘de riesgo’, como pueden ser los que han visitado anteriormente sitios web de mala reputación. Sense Analytics contribuye a eliminar las amenazas relacionando comportamientos de usuarios con eventos registrados, flujos de la red, inteligencia sobre amenazas, vulnerabilidades y el contexto empresarial. Permite a las organizaciones centrarse en las amenazas más inmediatas y peligrosas buscando señales claras entre el ruido, y las orienta en sus esfuerzos de remediación para minimizar daños potenciales.

Inicio

Conquite lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

- Analizar datos de cargas de trabajo
- Comprender el contexto
- Perfilar usos

Casos de uso

- Detección avanzada de amenazas
- Protección de datos críticos
- Monitorización de amenazas internas
- Gestión de riesgos y vulnerabilidades
- Detección de tráfico no autorizado
- Investigación forense y persecución de amenazas

¿Por qué IBM?

- Su panel de control de seguridad
- Potencia para actuar a cualquier escala
- IBM Security App Exchange
- Plataforma única, visibilidad global

Para obtener más información

¿Cómo funciona Sense Analytics?

Sin datos, la analítica es inútil; sin muchos datos, resulta simplemente insuficiente. Algunos de estos datos provienen de su red, otros están almacenados en aplicaciones, otros se derivan de análisis anteriores y otros provienen de una fuente externa. QRadar recopila datos de seguridad en bruto de todos los dispositivos, aplicaciones y usuarios de la red, tanto en las instalaciones de la organización como alojados en un entorno de cloud.

Sense Analytics puede:

- [analizar datos de cargas de trabajo](#)
- [comprender el contexto](#)
- [perfilar usos](#)

Una vez recopilados los datos, los appliances de QRadar realizan análisis en tiempo real para buscar señales inmediatas de peligro y posteriormente impregnan los resultados con otros datos de inteligencia almacenados acerca de la red, usuario o metadatos de archivo. QRadar permite a los equipos de seguridad comprender de qué manera están relacionadas las actividades actuales con lo que ha ocurrido en el pasado y un elemento fundamental para detectar el cambio es disponer de los parámetros adecuados para la actividad de base.



Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Analizar datos de seguridad para detectar amenazas

QRadar con Sense Analytics utiliza análisis avanzado basado en estados para transformar los actuales datos de seguridad en información útil y significativa. Los equipos de seguridad pueden definir múltiples tipos de condiciones que les ayudan a detectar actividad potencialmente maliciosa, como:

- cambios conductuales para detectar desviaciones de los patrones regulares
- anomalías que pueden descubrir nuevo tráfico en la red o tráfico que cesa repentinamente
- violaciones de umbral para descubrir ocurrencias de una actividad que superan un nivel definido.

Un cambio en el comportamiento normal de los usuarios o identidades suele ser una de las primeras señales de que se ha vulnerado la red y de que tal vez se hayan comprometido las credenciales de alguna persona. Sense Analytics no solo compara la actividad en tiempo real-con patrones históricos, sino que también detecta nuevos usos de las aplicaciones, nuevas visitas al sitio web y nuevas actividades de transferencia de archivos. También puede ayudar a descartar falsos positivos utilizando datos de sistemas de identidades de la organización, permitiendo a los analistas de SOC ver informes recientes de cambios de puesto de personas concretas.



Utilizando QRadar, una compañía internacional del sector eléctrico puede analizar

dos mil millones de eventos diarios—
correlacionando datos en tiempo real, para identificar los 20-25 potenciales ataques que plantean más riesgo.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Comprender el contexto analizando los eventos correspondientes a flujos y paquetes

Una fuente de contexto de gran potencia y que con frecuencia se pasa por alto pueden ser los datos nativos del flujo de la red (los datos que identifican direcciones IP, puertos, protocolos e incluso aplicaciones o contenidos de 'carga útil' que recorren la red) captados mediante inspecciones Deep Packet inmediatas, o la recuperación de paquetes completos con posterioridad al incidente. Esto permite a los equipos de seguridad:

- perfilar el tráfico de red 'normal' y obtener alertas al cambiar las condiciones
- encontrar hosts nuevos o comprometidos que se comunican con IPs maliciosas
- detectar nuevas amenazas a la seguridad sin el uso de firmas
- reproducir paso a paso las acciones de un intruso o usuario malicioso detectado
- obtener visibilidad de la capa de aplicaciones y detectar contenidos sospechosos o usos inadecuados.

Sense Analytics utiliza datos de la red para proporcionar contexto para cada evento, incidente o ataque correlacionado. Puede detectar si un servidor web deja de responder a las comunicaciones, identificar un cambio importante en el nivel de actividad de los servicios habitualmente utilizados y generar alertas si aparecen en la red nuevos servicios o protocolos. Este análisis también revela tipos de aplicaciones e identifica desajustes entre puertos y protocolos, lo que puede contribuir a acelerar las investigaciones.



Utilizando QRadar, una importante empresa de servicios de salud detectó

la transmisión de datos de pacientes sin cifrar

al exterior. Gracias a la detección rápida, no tardó en remediar el riesgo y evitar posibles sanciones.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Cree perfiles de uso para almacenar información útil y contribuir a gestione el riesgo

Una solución de seguridad diseñada para buscar rápidamente entre datos en tiempo real pasará por alto muchos incidentes que requieren un conocimiento previo de las aplicaciones clave, las personas que las utilizan, sus niveles de rendimiento típicos, sus hosts asociados y cómo experimentan periodos de mayor y menor actividad. El conocimiento de estos parámetros es crucial para obtener inteligencia sobre la que actuar.



QRadar puede ayudar a una empresa de tarjetas de crédito a proteger sus datos críticos

e infraestructura contra amenazas avanzadas, y a la vez conseguir ahorros de hasta el 50 por ciento en despliegue, ajuste y mantenimiento.

La posibilidad de almacenar conocimientos mediante perfiles de recursos y personas es una de las características en las que se basa Sense Analytics. QRadar descubre automáticamente recursos y crea perfiles de recursos utilizando datos de flujo de la red y detección de vulnerabilidades. Los perfiles definen qué es cada recurso, identifican cómo se comunica con otros recursos, crea una lista de aplicaciones permisibles y señala la presencia de vulnerabilidades conocidas. A continuación, QRadar utiliza todo este contexto para reducir el ruido y presentar los incidentes con gran precisión.

Igualmente valioso para la detección de ataques y vulneraciones es crear información sobre lo que están haciendo los usuarios de la red. QRadar puede hacer seguimiento de direcciones IP y MAC, identidades de correo electrónico y nombres de usuario de chat, por ejemplo, y puede utilizar otros programas de gestión de identidades y acceso de IBM o de terceros para ofrecer un valioso contexto para las investigaciones de incidentes. Puede utilizar todas estas asociaciones para cualificar el ámbito de la analítica e incluir o excluir personas o identidades asociadas con actividades sospechosas, que estén sucediendo en este momento o que se hayan observado en el pasado.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Explore casos de uso que demuestran la potencia de Sense Analytics

En muchos entornos, la despreocupación y distracciones en las prácticas de seguridad hacen que algunos recursos críticos no tengan necesariamente la seguridad que podrían o deberían tener. Las organizaciones necesitan limitar los aspectos negativos de una inevitable intrusión. Necesitan soluciones que abarquen todo el entorno, sin puntos ciegos.

Desde el momento que se instala, QRadar comienza a crear inteligencia de seguridad inmediatamente útil que puede reforzar las defensas de la organización. Algunos de los casos de uso en los que la solución ofrece valor rápido son:

- [Detección avanzada de amenazas](#)
- [Protección de datos críticos](#)
- [Monitorización de amenazas internas](#)
- [Gestión de riesgos y vulnerabilidades](#)
- [Detección de tráfico no autorizado](#)
- [Investigación forense.](#)



QRadar elimina

el misterio de las investigaciones de seguridad,

y ayuda a los equipos de seguridad a identificar a los atacantes, sus tácticas y dónde se produjo la intrusión inicial.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Casos de uso:

Detección avanzada de amenazas

Utilizando analítica en tiempo real, los equipos de seguridad pueden detectar si un host visita un dominio potencialmente malicioso, pero es posible que no se requiera una alerta si se trata una sola visita. Sin embargo, si el mismo host comienza a mostrar comportamiento diferente, detectado mediante el uso de análisis histórico a largo plazo, y también comienza a transferir un volumen de datos anormalmente elevado que se desvía de sus líneas habituales de comportamiento, la combinación de estas tres condiciones permite a QRadar producir una única alerta de elevada intensidad.

QRadar también puede detectar un cambio repentino en el tráfico de la red, como puede ser la aparición de una nueva aplicación en un host o la finalización de un servicio habitual, y lo considera una condición anómala. Las anomalías no son fáciles de detectar por los equipos de seguridad buscando en registros de sistema, a diferencia de las firmas del malware u otros ataques definidos contra vulnerabilidades conocidas. Una anomalía es, por definición, una rareza que solo es posible descubrir mediante una solución de seguridad que monitorice y profile las acciones de todos los usuarios y entidades.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Casos de uso:

Protección de datos críticos

De un día a otro, una nueva aplicación comienza a funcionar en un host de la red. Esta actividad puede ser resultado de un nuevo requisito del negocio o, simplemente, de que alguien instala una aplicación de chat. Pero si este host tiene acceso a datos críticos y también tiene asociada una vulnerabilidad conocida, QRadar puede crear una alerta de alta prioridad para que los equipos de seguridad investiguen rápidamente el incidente.

QRadar detecta rápidamente cuándo el tráfico de un evento supera un nivel de actividad específico y genera una alerta. El umbral o límite puede basarse en cualquier dato recopilado en QRadar, como configuraciones de dispositivos en la red, servidores, telemetría del tráfico de red y aplicaciones, además de usuarios finales y sus actividades. Y como cambio o anomalía conductual, QRadar puede ampliar los datos de la alerta con el contexto de las identidades de los usuarios, puertos y protocolos en uso, reputaciones de IP y actividades de amenaza denunciadas para proporcionar a los equipos de seguridad una perspectiva más profunda del incidente.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Casos de uso:

Monitorización de amenazas internas

Un representante de atención al cliente comienza repentinamente a descargar el doble de datos de lo habitual desde un sistema de información sobre clientes, lo que podría formar parte de una nueva actividad de análisis de ventas. Pero si QRadar sabe que este representante visitó recientemente un sitio web potencialmente sospechoso y ahora comprueba que se envían pequeñas cantidades de datos al sitio web de una empresa competidora, el personal de seguridad será informado antes de que se filtre gran cantidad de información.

QRadar se diferencia de otros productos de seguridad por los perfiles de entidades y personas. La combinación de un exhaustivo conjunto de datos, contexto empresarial e inteligencia sobre amenazas, junto con la capacidad de detectar desviaciones del comportamiento normal y reconocer qué comportamiento no está permitido o no es apropiado, ofrece una capacidad de detección de incidentes extremadamente potente.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Casos de uso:

Gestión de riesgos y vulnerabilidades

Cuando aparece una nueva entidad en la red, QRadar detecta automáticamente su existencia mediante el perfilado pasivo de registros y datos de flujo. Con su detector de vulnerabilidades perfectamente integrado, QRadar puede activar un examen de esta nueva entidad para descubrir si tiene alguna vulnerabilidad urgente o de elevado riesgo que esté expuesta a potenciales fuentes de amenazas.

Por ejemplo, cuando se añade un nuevo servidor a la red, QRadar puede detectar si carece de parches críticos o si tiene las credenciales administrativas predeterminadas. QRadar puede notificar al equipo correspondiente para remediar el problema y/o programar un parche, y escalar el problema si la tarea no se lleva a cabo con rapidez.

Y, sobre todo, las nuevas vulnerabilidades descubiertas se correlacionan automáticamente con los datos existentes sin necesidad de volver a hacer una detección, lo que contribuye a aumentar la velocidad y precisión de la detección. Los ahorros operativos resultantes también permiten a los analistas de seguridad dedicar más tiempo a tácticas proactivas, como análisis de riesgos y actividades de parcheado de vulnerabilidades.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Casos de uso:

Detección de tráfico no autorizado

En un momento en el que la mayoría de las organizaciones permiten a sus empleados utilizar dispositivos propios (BYOD), los equipos de seguridad asisten a un aumento del tráfico asociado con las aplicaciones de redes sociales. Los usuarios suelen acceder a sus sistemas de correo electrónico corporativo y se mantienen conectados con los amigos mediante Facebook, LinkedIn, Twitter y otros servicios, todo ello desde el mismo dispositivo. QRadar recopila y analiza estos datos y advierte si, por ejemplo, las sesiones de chat comienzan a conectarse a través del puerto 80, el puerto normalmente reservado para el tráfico HTTP. Nuevas conexiones con servidores de botnet conocidos permiten comprobar rápidamente la entrada de malware y advierten al equipo de seguridad para que emprenda acciones.

QRadar recopila y analiza datos de dispositivos móviles y BYOD tanto de la capa de red como de sistemas de gestión de puntos de conexión. Puede detectar amenazas potenciales, como dispositivos con jailbreaking, aplicaciones sospechosas instaladas en un dispositivo o comunicaciones de Internet potencialmente maliciosas, y poner el dispositivo en cuarentena y/o escalar el problema al equipo de seguridad apropiado.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Casos de uso:

Investigación forense y persecución de amenazas

Durante la investigación de un delito, un analista de seguridad descubre que uno o varios empleados han sido víctimas de un engaño de phishing y que el atacante se ha introducido en un servidor interno. El patrón corresponde a uno de los identificados por X-Force y se conoce que inyecta software troyano de acceso remoto (RAT), difícil de detectar.

Con pocos clics del ratón, QRadar recupera todos los paquetes de red asociados con el incidente y reconstruye los movimientos paso a paso, indicando al analista de seguridad con total claridad exactamente dónde y cuándo se instaló el software de RAT. El flujo de trabajo forense permite al analista crear rápidamente un completo perfil del software malicioso e reconstruye las rutas de infección mediante análisis de enlaces para identificar al 'paciente cero' y otros infectados. El resultado es que el equipo de seguridad puede remediar rápidamente los daños y minimizar las recurrencias.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

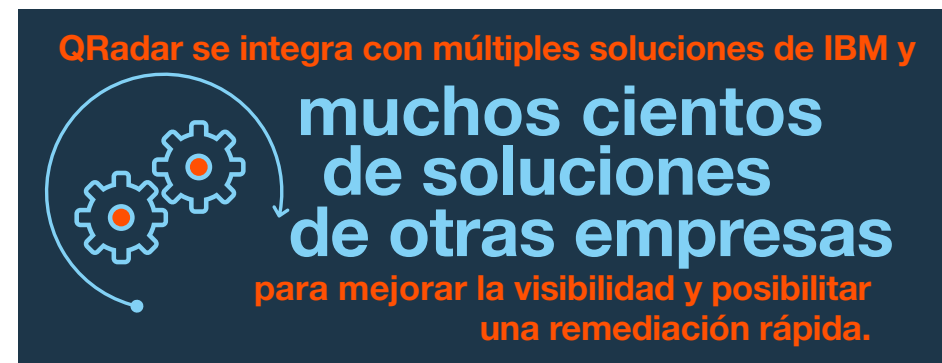
IBM proporciona inteligencia práctica para adoptar una defensa activa y reforzar la defensa

La seguridad de la información es una de las prioridades de cualquier consejo de administración, pero muchas organizaciones siguen dependiendo de docenas de productos aislados para obtener información sobre momentos en el tiempo. Empleados con elevado nivel de preparación utilizan motores de búsqueda para peinar montañas de datos, pero cada vez con más frecuencia, los atacantes evitan ser detectados mediante cambios de IP, protocolos, puertos y aplicaciones en las que introducirse, ampliarse y recopilar datos de gran valor, una vez realizada la intrusión.

IBM QRadar es diferente. Se despliega rápidamente, independientemente de la escala de la red, y comienza a ofrecer resultados en cuestión de horas. Sus capacidades, similares a las cognitivas, y la inteligencia almacenada pueden asociar ataques relacionados procedentes del mismo lugar o correspondientes a los mismos datos atacados. QRadar proporciona estas informaciones inmediatamente útiles para satisfacer las necesidades actuales y futuras, desde detección avanzada de amenazas hasta monitorización de amenazas internas, detección de fraude, gestión de riesgos y vulnerabilidades, investigaciones forenses y gestión de informes de cumplimiento.

Entre las principales razones por las que los líderes en seguridad eligen QRadar destacan:

- [Un panel de control de seguridad fácil de utilizar](#) que destaca las amenazas más importantes y apoya un flujo de trabajo rápido y eficaz para investigación y remediación
- [Escalabilidad casi ilimitada](#), respaldada por inteligencia sobre amenazas X-Force y la potencia colaborativa de IBM X-Force Exchange
- [IBM Security App Exchange](#), con aplicaciones (apps) desarrolladas por IBM y otras empresas que amplían las capacidades de QRadar sin hacerlo más complejo
- [Una plataforma integrada única con visibilidad global](#), que proporciona información útil sobre la actividad de la red, aplicaciones y usuarios.



Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

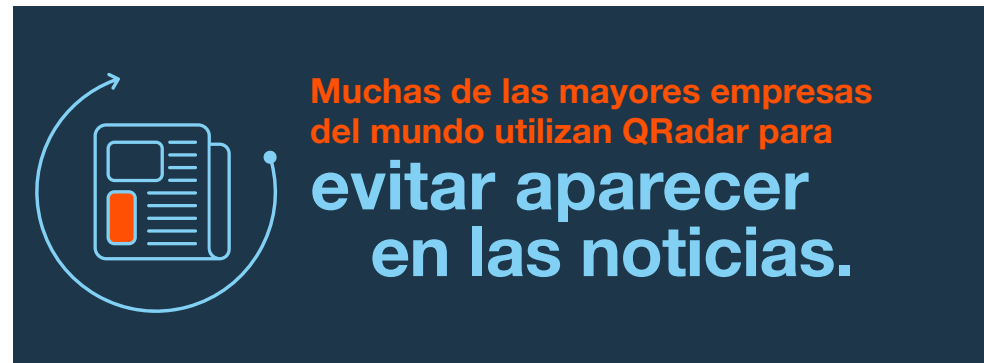
Para obtener más información

Presenta nítidamente las amenazas más importantes

Una vez detectada la amenaza, ataque o intrusión, es el momento de pasar a la acción. QRadar capacita a los equipos de seguridad con una interfaz de usuario basada en web que tiene un mismo aspecto para toda la plataforma. Pasar de monitorizar el registro de actividad a vigilar la actividad en la red, revisar incidentes relacionados, ejecutar análisis de riesgo y vulnerabilidad o realizar un análisis forense es tan

sencillo como hacer clic en una pestaña y visualizar una pantalla con toda la información en forma de panel de control. Cada panel de control contiene abundante información de inteligencia de seguridad organizada en visualizaciones gráficas de la actividad reciente, que se investiga con solo unos clics del ratón.

Dedique algunos minutos a ver los picos o examine todos los detalles de un incidente. Los equipos de seguridad pueden comprender rápidamente la naturaleza del problema resaltado, las vulnerabilidades que se han explotado, la entrada de algún botnet, RAT u otro programa de malware y el alcance de los datos perdidos. Es el momento de actuar antes de que se produzca un daño real.



Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Consiga la potencia necesaria para actuar a cualquier escala

Utilizando la plataforma QRadar completa, los equipos de seguridad pueden comprender con claridad y rápidamente qué ha sucedido y qué riesgo se corre si no se actúa. Las funciones clave, como monitorización de amenazas, gestión de riesgos y vulnerabilidades e informes de cumplimiento están al alcance de un clic y pueden pasarse información entre sí. Además, QRadar incluye plena integración con la inteligencia sobre amenazas de X-Force para disponer de actualizaciones cada hora sobre técnicas de ataques globales y cepas de malware.



En caso de intrusión, la tecnología forense integrada en QRadar proporciona a los analistas de SOC datos de los paquetes correspondientes al incidente, detallando paso a paso las acciones de los intrusos con claridad y exactitud. Para desactivar algunas amenazas basta con bloquear las comunicaciones con una dirección IP externa, pero con frecuencia se precisa la movilización de los equipos de respuesta a situaciones de emergencia para aislar y reconfigurar hosts, deshabilitar el malware y parchear las vulnerabilidades. Pero, ¿y si si equipo no sabe exactamente qué hacer? Es el momento de pedir ayuda, colaborar con otros, buscar una solución o incluso contratar los servicios de un equipo profesional.

El marco de trabajo abierto de QRadar y el [IBM Security App Exchange](#) facilitan una mayor integración con soluciones de IBM y otras empresas. Por ejemplo, una de las apps del sitio pasa los datos del incidente de QRadar a Incident Response Platform de Resilient Systems para actuar inmediatamente. Otra app proporciona una capacidad similar para compartir datos con la solución de gestión de puntos de conexión Carbon Black Enterprise Response.

Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Amplíe sus capacidades con el IBM Security App Exchange

El [IBM Security App Exchange](#) amplía exponencialmente la flexibilidad de QRadar. Este centro de colaboración permite a clientes, desarrolladores y socios comerciales compartir apps, extensiones de apps de seguridad y mejoras para los productos de IBM Security.

Con el IBM Security App Exchange, las organizaciones pueden:

- conseguir apps que amplían las capacidades de las soluciones de seguridad de IBM
- compartir mejores prácticas y aprender de otros
- encontrar soluciones y casos de uso que aumentan el valor estratégico de las operaciones de seguridad.

IBM comprueba determinados criterios establecidos en todo el código antes de que aparezca en el sitio. Y los equipos de seguridad pueden descargar e instalar las soluciones independientemente, al margen de los ciclos de actualizaciones oficiales de los productos. De esta manera, pueden aplicar nuevos casos de uso de seguridad sin aumentar innecesariamente la complejidad de la solución.

En concreto, los usuarios de QRadar pueden descargar contenido para sectores, amenazas, dispositivos y de proveedores específicos desde el IBM Security App Exchange. Además, pueden acceder a informes personalizados, paneles de control, análisis especializados e información sobre amenazas.



Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

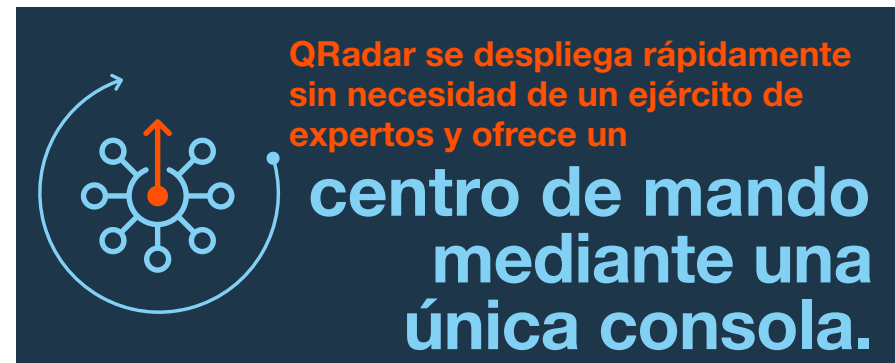
Para obtener más información

Despliegue una sola plataforma con visibilidad global

Los actuales entornos de seguridad tienen un exceso de complejidad: es frecuente que los datos de seguridad estén distribuidos entre múltiples productos de distintos proveedores, con interfaces y formatos de almacenamiento diferentes. Para detectar eficazmente las amenazas existentes y emergentes, los equipos de seguridad necesitan una vista consolidada de estos datos, junto con

completos análisis para detección de amenazas y capacidades de respuesta. QRadar utiliza una única base de datos federada para todos los datos de seguridad, diseñada específicamente para la recogida de datos escalable desde sistemas locales o en la nube, almacenamiento, creación de informes y elevada velocidad de búsqueda. Asimismo, QRadar está optimizado para análisis de incidentes históricos y en tiempo real y detectar incidentes pocos segundos después de que se produzcan, en vez de horas, días o semanas.

QRadar también ofrece un conjunto muy integrado de casos de seguridad, más otros disponibles a través de IBM Security App Exchange. Los equipos de seguridad pueden utilizar una única consola con paneles de control para todas las funciones, como monitorización de la seguridad en tiempo real, gestión proactiva de riesgos y vulnerabilidades y detección, análisis forense y remediación de incidentes. Este centro único para las operaciones de seguridad y respuesta aúna inteligencia de productos de IBM y otros fabricantes, con el respaldo de una interfaz de usuario y flujo de trabajo siempre similar, lo que aumenta en muy gran medida la efectividad de sus operaciones de seguridad.



Inicio

Conquiste lo desconocido

Detecte las amenazas y actúe

QRadar Sense Analytics

¿Cómo funciona?

Analizar datos de cargas de trabajo

Comprender el contexto

Perfilar usos

Casos de uso

Detección avanzada de amenazas

Protección de datos críticos

Monitorización de amenazas internas

Gestión de riesgos y vulnerabilidades

Detección de tráfico no autorizado

Investigación forense y persecución de amenazas

¿Por qué IBM?

Su panel de control de seguridad

Potencia para actuar a cualquier escala

IBM Security App Exchange

Plataforma única, visibilidad global

Para obtener más información

Más información

Para obtener más información sobre [IBM QRadar Security Intelligence Platform con Sense Analytics](#), póngase en contacto con su representante o Business Partner de IBM, o bien visite: ibm.com/security

Acerca de IBM Security

IBM Security ofrece una de las gamas más avanzadas e integradas de productos y servicios de seguridad empresarial. La cartera, respaldada por el desarrollo y la investigación de prestigio internacional de X-Force, proporciona inteligencia en seguridad para ayudar a las organizaciones a proteger de forma global a sus empleados, infraestructuras, datos y aplicaciones, ofreciendo soluciones para la gestión de accesos e identidades, seguridad de bases de datos, desarrollo de aplicaciones, gestión de riesgos, gestión de puntos finales y seguridad de las redes, entre otras opciones. Estas soluciones permiten a las organizaciones gestionar los riesgos de forma eficaz e implementar una seguridad integrada para entornos móviles, nube, redes sociales y otras arquitecturas empresariales. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más extensas del mundo; monitoriza 15 000 millones de eventos de seguridad al día en más de 130 países y posee más de 3000 patentes de seguridad.

IBM Security
Route 100
Somers, NY 10589

El sitio web de IBM está disponible en ibm.com/es

IBM, el logotipo de IBM, ibm.com, QRadar, Sense Analytics y X-Force son marcas comerciales de International Business Machines Corp. registradas en numerosas jurisdicciones de todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras compañías. Bajo el epígrafe "Información sobre Copyright y marcas comerciales" puede consultar la lista actualizada de las marcas comerciales de IBM en la página web www.ibm.com/legal/copytrade.shtml.

Este documento está actualizado en la fecha de publicación original y puede ser modificado por IBM en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

LA INFORMACIÓN DE ESTE DOCUMENTO SE PROPORCIONA "TAL CUAL", SIN NINGUNA GARANTÍA, NI EXPLÍCITA NI IMPLÍCITA, INCLUYENDO LAS GARANTÍAS DE COMERCIABILIDAD, IDONEIDAD PARA UN FIN DETERMINADO Y NO INCUMPLIMIENTO. Los productos IBM están garantizados de acuerdo con los términos y condiciones de los acuerdos en virtud de los cuales se proporcionen.

El cliente es responsable de asegurarse del cumplimiento de las leyes y normas que sean de aplicación. IBM no proporciona asesoramiento legal ni declara o garantiza que sus productos o servicios asegurarán que el cliente cumpla alguna ley o norma determinada.

Declaración de buenas prácticas de seguridad: La seguridad de un sistema de TI implica proteger los sistemas y la información mediante prevención, detección y respuesta ante accesos indebidos desde el interior y el exterior de su empresa. El acceso inadecuado puede dar como resultado la alteración, destrucción o uso o apropiación indebidos de la información, o bien provocar daños en sus sistemas o un uso indebido de ellos, incluidos ataques a otras organizaciones. No existe ningún sistema o producto de TI que se pueda considerar totalmente seguro, ni existe ningún producto, servicio o medida de seguridad que sea completamente eficaz en la prevención del acceso o uso indebido. Los sistemas, productos y servicios IBM están diseñados para formar parte de un enfoque de seguridad global y respetuoso con la legalidad, lo que necesariamente implica procedimientos operativos adicionales, y pueden requerir otros sistemas, productos o servicios para ser más efectivos. IBM NO GARANTIZA QUE UN SISTEMA, PRODUCTO O SERVICIO SEA INMUNE O PUEDA INMUNIZAR A SU EMPRESA CONTRA LA CONDUCTA MALICIOSA O ILEGAL DE NINGUNA PERSONA U ORGANIZACIÓN.

© Copyright IBM Corporation 2017