Analítica de seguridad para sus despliegues multicloud

Solución SIEM de IBM Security QRadar

Contenido

01

La revolución multicloud está ganando impulso

La empresa moderna necesita seguridad inteligente

La adopción del multicloud híbrido no para de aumentar y, con ella, un número cada vez mayor de datos, aplicaciones y cargas de trabajo se mueven hacia el cloud. Ante el mayor número de empleados que trabajan desde casa y que las interacciones personales se realizan en línea, se espera que el uso del cloud alcance un nuevo máximo.[1]

Gartner estima que el sector de los servicios de cloud público crecerá exponencialmente hasta 2022. El segmento de mercado cloud con un crecimiento más rápido será el de Infraestructura como Servicio (IaaS), en el que Gartner pronostica un crecimiento de 76 600 millones de dólares hasta 2022.[2]

La seguridad debe situarse en el centro de estas iniciativas cloud. Las brechas de seguridad cloud pueden costar a las compañías más de 50 000 dólares en menos de una hora.[3] Las organizaciones que dependen de IaaS deben proteger proactivamente sus sistemas operativos, gestionar las configuraciones de red y, evidentemente, proteger los datos que circulan por dichos sistemas.

Para mantener la seguridad de la información crítica de negocio, los analistas de seguridad necesitan tener una completa visibilidad de todo el ecosistema TI – redes, aplicaciones y actividades – que se ejecuta localmente y en cloud. Necesitan tener la capacidad para detectar amenazas en tiempo real, identificar el uso de servicios cloud no autorizados y tener una clara visibilidad de si las cuentas y recursos del cloud están correctamente configurados para mantener la seguridad.

Más de mil millones de registros perdidos

La configuración incorrecta de entornos cloud fue la causa de la pérdida de más de mil millones de registros en 2019.[3]

Pérdidas de más de 50 000 dólares en menos de una hora

Las brechas de seguridad cloud pueden costar a las compañías más de 50 000 dólares en menos de una hora.[3]

02

Liberar el potencial de las soluciones IBM Security QRadar

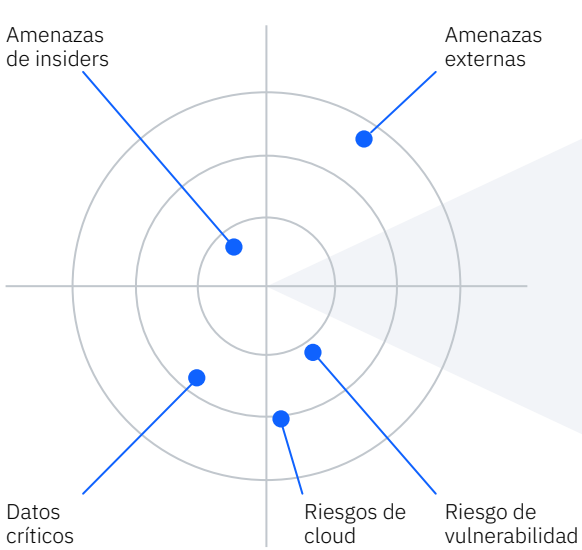
Consiga una completa visibilidad de los servicios cloud

La solución de información y gestión de eventos de seguridad (SIEM) de IBM Security QRadar se integra con múltiples servicios cloud, tales como Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Salesforce.com, Microsoft Office 365, IBM Cloud, etc.

Recopilando y normalizando información de seguridad de entornos tanto locales como en cloud, la solución QRadar aplica analítica avanzada para clasificar automáticamente millones de eventos. La solución ayuda a identificar las amenazas más críticas y proporciona alertas priorizadas y significativas de las incidencias potenciales, para proteger los entornos híbridos locales y multicloud.

Es más, la solución ofrece a los analistas de la seguridad una interfaz unificada en la que pueden ver las amenazas más críticas, revisar la cadena cronológica de eventos que han motivado cada una de las alertas y obtener información inmediata de los ataques potenciales. Sus sólidas funciones listas para usar garantizan un despliegue rápido y escalabilidad en los entornos soportados.

Obtenga más información sobre cómo la solución QRadar puede ayudarle a proteger su entorno cloud →



Detección y priorización automatizada de las amenazas

La solución SIEM de IBM Security QRadar recopila, analiza y correlaciona datos de una amplia variedad de orígenes para detectar y priorizar las amenazas más críticas que requieren investigación.

03

Integrar la solución QRadar con Amazon Web Services (AWS)

Amplíe la visibilidad en AWS para mejorar el estado de la seguridad

Aproximadamente el 76 % de las organizaciones utilizan AWS en alguna capacidad.1 Puesto que esta transición de la informática local y tradicional a la informática basada en cloud no cesa, los equipos de seguridad necesitan tener visibilidad de la infraestructura basada en cloud, aplicaciones y datos – como si estuvieran en un entorno local.

Identificar riesgos que puedan exponer a los datos
Algunas de las mayores brechas de los últimos años no las causaron atacantes maliciosos. Al contrario, fueron el resultado de configuraciones incorrectas en los “buckets” de Amazon Simple Storage Service (Amazon S3), que exponían los datos confidenciales al público.

Por medio de la solución QRadar, los equipos de seguridad pueden explorar proactivamente sus entornos AWS, ya sea de forma puntual o formando parte de un programa de exploración periódico, para buscar activamente dichas configuraciones incorrectas y alertar de ello a los analistas. Con estas alertas, los equipos de seguridad pueden comenzar el proceso de respuesta para cerrar brechas y proteger sus datos.

Detectar amenazas en los datos y flujos de trabajo de cloud
Ante el aumento de los datos confidenciales y activos críticos de negocio que se mueven al cloud, AWS empieza a ser uno de los objetivos principales de los atacantes. Si las cuentas de AWS se ven comprometidas, ya sea directamente mediante phishing o en el curso de un movimiento lateral, los datos y cargas de trabajo AWS podrían acabar bajo el control de un atacante. Para evitar daños, es crítico contar con advertencias rápidas y unificadas de las amenazas. La solución QRadar lleva los datos de seguridad de AWS, incluidos AWS CloudTrail, AWS CloudWatch y AWS Virtual Private Cloud (VPC) Flow Logs, a una solución de analítica de seguridad centralizada que los equipos de operaciones de seguridad pueden utilizar para monitorizar las amenazas tanto externas como de insiders, desde un único cuadro de mandos.

La solución QRadar puede recopilar eventos de sus productos de seguridad por medio de un archivo complementario denominado **Módulo de Soporte de Dispositivo**.

Mediante protocolos soportados y Módulos de Soporte de Dispositivo (DSMs), la solución QRadar se integra con los siguientes componentes AWS para facilitar el análisis de seguridad avanzada:

AWS CloudTrail. La integración de QRadar ofrece visibilidad de la actividad del usuario registrando las acciones realizadas en la cuenta. Admite sucesos de auditoría que se recopilan de los buckets de Amazon S3 y de un grupo de registros de AWS CloudWatch Logs.

AWS Security Hub. Esta integración utiliza un sistema integrado de analíticas y defensas en tiempo real para ofrecer a los equipos de seguridad una mayor visibilidad de las alertas de seguridad de alta prioridad y comprobaciones automatizadas del cumplimiento normativo, en un único cuadro de mandos del centro de operaciones de seguridad (SOC). Mediante la integración con AWS Security Hub Amazon Findings Format (AFF), la solución QRadar puede optimizar la agregación de eventos de múltiples capacidades de seguridad AWS, instancias y soluciones de seguridad AWS Partner Network (APN) para mejorar el análisis de seguridad.

Amazon GuardDuty. Con esta integración, los usuarios pueden analizar flujos continuos de metadatos generados en su cuenta y su actividad en la red, que se encuentran en los eventos de AWS CloudTrail, Amazon VPC Flow Logs y registros del servidor de nombres de dominio (DNS).

Amazon VPC Flow Logs. Esta integración permite a los clientes recopilar, almacenar y analizar registros de flujos de red. Se puede utilizar para monitorizar y resolver problemas de conectividad y de seguridad, para asegurarse de que las reglas de acceso a la red funcionan según lo previsto.

Amazon AWS Content Extension. Esta extensión de contenidos añade un nuevo análisis de datos de eventos encima del AWS incorporado en la solución QRadar y acelera el análisis de datos de eventos críticos. Los datos, tales como el ID de instancia, nombre de archivo, nombre de rol, nombre de almacenamiento, etc. se ponen a disposición de los usuarios para que puedan monitorizar los cambios y crear informes de la seguridad relativa de sus entornos cloud.

App IBM Security QRadar Cloud Visibility. Esta app proporciona cuadros de mandos y mejoras específicas de AWS, tales como:

- Gestión simplificada de orígenes de registros
- Gestión de identidad y acceso (IAM) de cuentas, usuarios y roles IAM
- Llenado automático de la jerarquía de redes de QRadar
- Visualización de Amazon VPC Flow Log
- Integración con AWS Security Hub y Amazon Detective

¿Por qué utilizar la solución QRadar para monitorizar entornos AWS?

- Ofrece visibilidad centralizada de los riesgos y amenazas de los despliegues cloud
- Permite a los analistas de seguridad buscar proactivamente configuraciones incorrectas que requieran una respuesta
- Elimina los silos para comprender mejor toda la cadena de eventos relacionados con una incidencia
- Utiliza el aprendizaje automático para identificar usuarios de alto riesgo y detectar amenazas de insiders más rápidamente

Obtenga más información sobre IBM Security QRadar Amazon AWS Content Extension →

04

Integrar la solución QRadar con Microsoft Azure

Aumente la visibilidad y procese los eventos de millones de dispositivos

La adopción de Microsoft Azure ha aumentado constantemente con el paso del tiempo y el 61 % de las organizaciones indicaban su uso del servicio.[1] A medida que más datos y cargas de trabajo se mueven a Azure, las prácticas de seguridad deben adaptarse para proteger los activos de este nuevo entorno. La solución QRadar proporciona sólidas características listas para usar, que llevan los datos de seguridad de Azure a un programa de analítica de seguridad de nivel empresarial.

Mediante protocolos soportados y DSMs, la solución QRadar se integra con los siguientes componentes de Azure para facilitar el análisis de seguridad avanzada:

Registros de actividad de Azure El servicio de recopilación de eventos nativo de Azure ingiere un gran volumen de datos de telemetría y eventos. Esta información se puede enviar fácilmente a la solución QRadar para que los equipos de seguridad puedan extraer información detallada de los riesgos y amenazas potenciales de los entornos Azure.

Azure Active Directory. La integración de la solución QRadar con Azure Active Directory ofrece a los equipos de seguridad la capacidad para monitorizar la identidad, la gestión de accesos y los eventos de seguridad de recursos externos, tales como Microsoft Office 365 y Microsoft Azure.

Microsoft Graph Security API. Con el protocolo QRadar Microsoft Graph Security API, las organizaciones pueden ingerir alertas de Microsoft Graph Security API, lo que permite a los analistas de seguridad investigar rápidamente los delitos.

App QRadar Cloud Visibility. La solución QRadar puede detectar problemas potenciales de los entornos Azure y resolver los casos de seguridad. Cuando se crean delitos, la app QRadar Cloud Visibility ayuda a los usuarios a gestionarlos en el cuadro de mandos de AzureOffense Overview.

El cuadro de mandos de Azure Offense Overview muestra los datos de los delitos activos en las siguientes gráficas:

- Todos los usuarios por magnitud
- Todos los usuarios por regla relacionada
- Delitos más graves
- Todos los usuarios por número de delitos
- Indicador de nivel de magnitud

IBM Security QRadar Content Extension for Azure. La extensión de contenidos Azure de QRadar añade reglas, informes y búsquedas guardadas, que se añaden a las capacidades de análisis de eventos existentes en QRadar para los despliegues de Azure.

Esta extensión de contenidos está específicamente dirigida a la gestión de seguridad de la red, la modificación de reglas de seguridad y la gestión de redes virtuales.

¿Por qué utilizar la solución QRadar para proteger y monitorizar componentes de Azure?

- Detectar patrones de comportamiento anómalo en toda la infraestructura de TI mediante reglas de seguridad.
- Monitorizar y diagnosticar tráfico de red a través de los grupos de seguridad de red de Azure.
- Gestionar redes virtuales de forma más eficaz.
- Recopilar registros de eventos y datos de seguridad de flujos de red en las pasarelas de redes locales.
- Monitorizar el rendimiento y el uso de aplicaciones web que se ejecutan en Azure.

Obtenga más información sobre QRadar Content Extension for Azure →

05

Integrar la solución QRadar con Google Cloud Platform

Detecte anomalías rápidamente y descubra amenazas en tiempo real

Google Cloud Platform es una de las principales soluciones cloud con una base de usuarios que crece al 35 %.[1] La solución ofrece una suite de servicios cloud que utiliza la infraestructura de Google. La solución IBM Security QRadar ofrece una integración avanzada con Google Cloud Platform. Proporciona visibilidad centralizada mediante la recopilación, búsqueda y análisis de cientos de datos de las cargas de trabajo que residen en los entornos. Sus equipos de seguridad podrán detectar y responder mejor a las amenazas dondequiera que se produzcan.

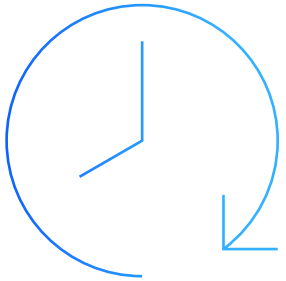
Mediante protocolos soportados y DSMs, la solución QRadar se integra con los siguientes servicios de Google Cloud Platform para facilitar el análisis de seguridad avanzada:

Informes de actividad de Google G Suite. La solución QRadar tiene visibilidad de los eventos de actividad de auditoría generados en la plataforma Google G Suite, incluidos los inicios de sesión, las cuentas de usuario, Google Drive y Google Admin.

Su equipo de seguridad podrá obtener información de los siguientes casos:

- Cuenta inhabilitada debido a una actividad sospechosa
- Información de usuario descargada como archivo de valores separados por coma (CSV)
- Privilegios administrativos revocados por el usuario
- Un actor ha cambiado la pregunta o respuesta secreta de recuperación de cuenta
- Un actor ha cambiado los permisos de compartición de usuario
- Un actor ha movido un elemento desde la carpeta de origen hasta la carpeta de destino
- El usuario ha sudo suspendido

Protocolo Google Cloud Pub/Sub. Con el protocolo de QRadar para Google Cloud Pub/Sub, los usuarios pueden tener una mayor visibilidad de todo lo que crea un “sink” en Pub/Sub, lo que permite a los equipos de seguridad actuar más rápidamente.



06

Ver en SaaS

Supervise los datos de sus aplicaciones SaaS mediante los DSMs de QRadar

Las empresas ya están utilizando aplicaciones de Software como Servicio (SaaS) para ser más ágiles, trabajar más rápido y dar soporte a proyectos que generen ingresos – y la adopción de SaaS no para de aumentar. Gartner predice que esta solución cloud basada en servicios ascenderá a los 143 700 millones de dólares en 2022.[2]

La solución QRadar ayuda a las organizaciones a tener visibilidad del uso de aplicaciones SaaS y permite a los equipos de seguridad detectar y bloquear amenazas de forma más eficaz. DSMs predefinidos permiten tener una integración sin fisuras con las demás soluciones del entorno. Los DSMs están probados y validados por el equipo de IBM Security antes de su despliegue.

La solución QRadar está diseñada para ayudar a su equipo a empezar fácilmente a monitorizar datos de sus aplicaciones SaaS, incluido Salesforce.com, Office 365, entornos Box, etc. Cuando estos datos se llevan a su programa de analítica de seguridad, su equipo podrá obtener información de amenazas potenciales y descubrir incidencias potenciales dirigidas a los datos de dichas soluciones. Sus analistas de seguridad estarán mejor dotados para detectar insiders maliciosos en las primeras etapas de su ciclo de ataque e impedirles que comprometan los datos confidenciales almacenados en dichas aplicaciones y servicios.

Obtenga más información sobre los DSMs soportados por la solución QRadar →

La solución QRadar, mediante los DSMs, se integra con diversas soluciones SaaS e IaaS populares.

- Amazon CloudTrail
- Amazon CloudWatch
- Amazon VPC Flows
- Microsoft Azure Event Hubs
- Microsoft Office 365
- Box.com
- Netskope Active
- Cloudera Navigator
- CloudPassage Halo
- Skyhigh Networks
- OpenStack
- Cisco Cloud Web Security
- VMware
- Salesforce
- Okta
- Google Cloud Platform
- Plataforma Red Hat® Ansible®

07

Dotar al equipo de seguridad de las herramientas correctas

Explore la familia de productos de QRadar

En resumen, las soluciones IBM Security QRadar se han diseñado para proporcionar la información crítica que necesita para el crecimiento de sus entornos cloud. Con el uso de esta familia de soluciones puede reunir varios silos de datos en una única plataforma para su completa visibilidad, análisis de seguridad y detección de amenazas. Puede identificar comportamientos anómalos para protegerse de las amenazas externas e internas, identificar vulnerabilidades que accidentalmente puedan poner en riesgo los datos confidenciales y descubrir el uso de servicios cloud no autorizados.

Juntas, estas capacidades ayudan a ofrecer una completa visión de la actividad del sistema, la red y los usuarios de la organización y pueden proporcionar perspectivas inteligentes para el combate proactivo de los riesgos y las amenazas.

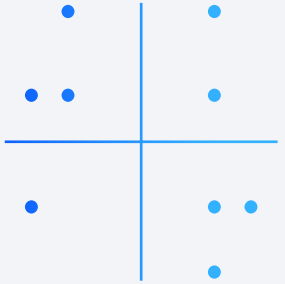
La solución QRadar recopila y analiza de forma centralizada los flujos de datos y la información de amenazas de distintas fuentes del entorno, como AWS, Azure, IBM Cloud, aplicaciones SaaS, clouds privados e infraestructuras locales tradicionales. Puede optar por desplegar hardware o software locales, desplegar máquinas virtuales en entornos IaaS o consumir la solución QRadar como servicio cloud de IBM.

Cuando avance en el camino a multicloud, puede contar con las mismas capacidades de seguridad, monitorización y analítica en toda la empresa.

Obtenga más información →

IBM ha sido nombrado líder en el último Gartner Magic Quadrant for Security Information and Event Management (SIEM) **por 11 año consecutivo.**

Lea el informe →



08

¿Por qué las soluciones de IBM Security?

IBM opera una de las organizaciones de investigación de seguridad, desarrollo y entrega más amplia del mundo.

Las soluciones de IBM Security ofrecen una de las carteras más avanzadas e integradas de productos y servicios de seguridad para la empresa. La cartera, respaldada por la investigación de IBM X-Force de fama mundial, proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger globalmente sus infraestructuras, datos y aplicaciones. Ofrece soluciones para la gestión de identidad y acceso, seguridad de bases de datos, desarrollo de aplicaciones, gestión del riesgo, gestión de puntos finales, seguridad de red, etc. Estas soluciones permiten a las organizaciones gestionar eficazmente el riesgo e implementar seguridad integrada para móviles, clouds, redes sociales y otras arquitecturas de negocio empresariales.

Asimismo, IBM Global Financing ofrece numerosas opciones de pago que le ayudarán a adquirir la tecnología que necesita para hacer crecer su negocio. IBM proporciona una gestión completa del ciclo de vida de productos y servicios de TI, desde la adquisición hasta la eliminación. Si desea obtener más información, visite ibm.com/financing.

Más información
Si desea obtener más información sobre la solución de inteligencia de seguridad de QRadar, puede ponerse en contacto con su representante de IBM o Business Partner de IBM, o bien visitar ibm.com/security/security-intelligence/qradar.

IBM supervisa **miles de millones** de sucesos de seguridad cada día, en más de **130 países**, y posee más de **3000 patentes de seguridad**.

IBM España, S.A.
Tel.: +34-91-397-6611
Santa Hortensia, 26-28
28002 Madrid
Spain

La página de inicio de IBM se encuentra en:
ibm.com

Este documento es válido en la fecha inicial de publicación y puede estar sujeto a cambios por parte de IBM en cualquier instante. No todas las ofertas están disponibles en todos los países en los que IBM opera.

Declaración de buenas prácticas de seguridad: la seguridad de sistemas TI implica la protección de sistemas e información a través de la prevención, detección y respuesta al acceso inadecuado desde el interior y exterior de la empresa. Un acceso inadecuado puede causar la alteración, destrucción, uso indebido o mal uso de la información o pueda causar daños o mal uso de sus sistemas, incluido el uso en ataques dirigidos a otros. Ningún sistema o producto TI debe considerarse completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente eficaz en la prevención de un uso o acceso inadecuados. Los sistemas, productos y servicios de IBM se han diseñado para formar parte de un enfoque de seguridad legal y completo, que necesariamente implicará procedimientos operativos adicionales y que pueden requerir que otros sistemas, productos o servicios sean lo máximo de eficaces. IBM NO GARANTIZA QUE LOS SISTEMAS, PRODUCTOS O SERVICIOS SEAN INMUNES, O HARÁN QUE SU EMPRESA SEA INMUNE, A LA CONDUCTA MALINTENCIONADA O ILEGAL DE TODAS LAS PARTES.

1 10 Key Takeaways from RightScale 2020 State Of The Cloud Report From Flexera, *Forbes*, 2 de mayo de 2020

2 Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019, *Gartner*, 2 de abril de 2019

3 Cloud Threat Landscape Report 2020, *IBM Security X-Force®* Incident Response and Intelligence Services, mayo de 2020