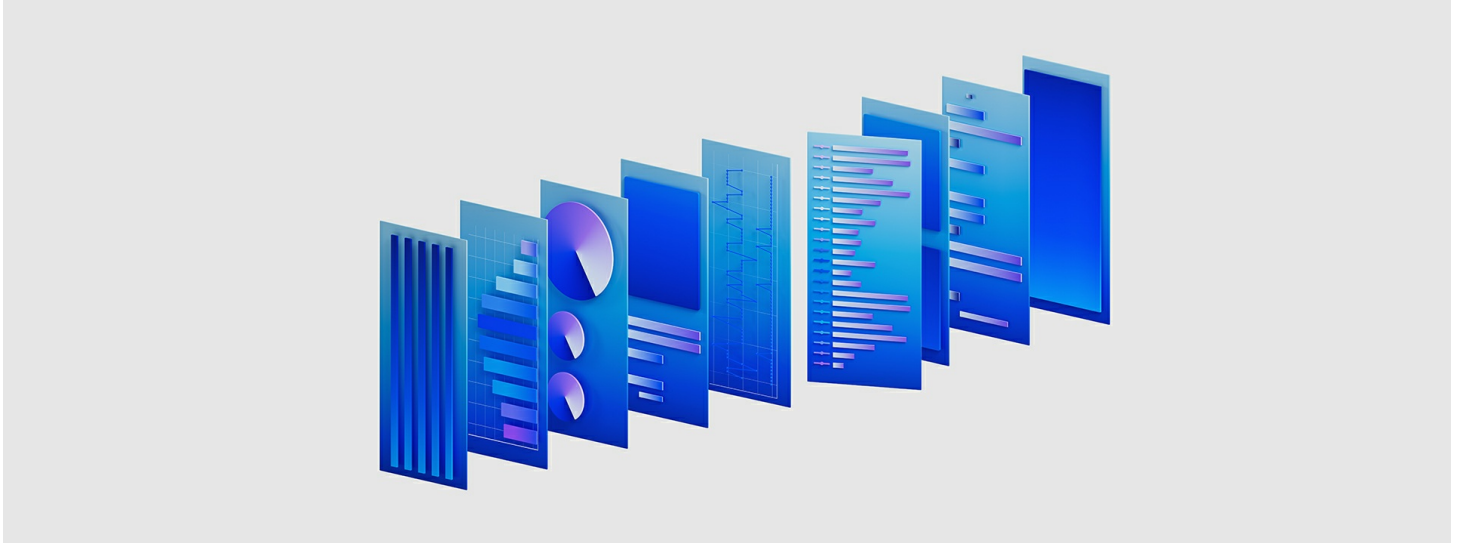


IBM lanza la nueva QRadar Security Suite para acelerar la detección y respuesta de amenazas

-La interfaz modernizada y unificada agiliza la respuesta de los analistas en todo el ciclo de vida del ataque.

-Capacidades sofisticadas de IA y automatización muestran que aceleran el triage de alertas en un 55%.



ARMONK, NY, 25 de abril de 2023 - IBM presentó su nueva suite de seguridad diseñada para unificar y acelerar la experiencia de los analistas de seguridad durante todo el ciclo de vida de los incidentes. La [IBM Security QRadar Suite](#) representa una gran evolución y expansión de la marca QRadar, abarcando todas las tecnologías principales de detección, investigación y respuesta de amenazas, con una inversión significativa en innovaciones en todo el portafolio.

Entregada como un servicio, IBM Security QRadar Suite está construida sobre una base abierta y diseñada específicamente para las necesidades de la nube híbrida. Cuenta con una interfaz de usuario única y modernizada en todos los productos, integrada con IA avanzada y automatización para empoderar a los analistas para que trabajen con mayor velocidad, eficiencia y precisión en sus herramientas principales.

Los equipos de los Centros de Operaciones de Seguridad (SOC) están protegiendo una huella digital en rápida expansión que se extiende a través de entornos de nube híbrida, creando complejidad y haciendo difícil seguir el ritmo de las velocidades aceleradas de los ataques. Estos equipos desaceleran con las investigaciones de las alertas y los procesos de respuesta laboriosos, uniendo manualmente *insights* y buscando entre datos, herramientas e interfaces desconectadas. Los profesionales de los SOC dicen que pasan alrededor de 1/3 de su día investigando y validando incidentes que terminan no siendo amenazas reales, según una encuesta reciente^[1].

Construida sobre el liderazgo existente de la compañía en 12 categorías de seguridad, IBM rediseñó su portafolio de detección y respuesta de amenazas líder en el mercado para la máxima velocidad, eficiencia y las necesidades actuales específicas de los analistas de seguridad. La nueva QRadar Suite incluye EDR/XDR, SIEM, SOAR y una nueva capacidad de gestión de *logs* nativa de la nube, todo creado en torno a una interfaz de usuario común, *insights* compartidos y flujos de trabajo conectados, con los siguientes elementos de diseño en el core:

- **Experiencia unificada para analistas:** refinada en colaboración con cientos de usuarios del mundo real, la suite cuenta con una interfaz de usuario común y modernizada en todos los productos: diseñada para aumentar drásticamente la

velocidad y la eficiencia de los analistas en toda la cadena de ataque. Está integrada con capacidades de IA y automatización de nivel empresarial que demostraron acelerar la investigación y triage de alertas en 55% en el primer año, en promedio [2].

- **Entrega en la nube, velocidad y escala:** entregados como servicio en AWS, los productos de la QRadar Suite permiten una implementación, visibilidad e integración simplificados entre entornos de nube y fuentes de datos. La suite también incluye una nueva capacidad de gestión de registros o logs, nativa en la nube y optimizada para una ingesta de datos altamente eficiente, la búsqueda rápida y la analítica a escala.
- **Fundamento abierto, integraciones preconstruidas:** La suite reúne las principales tecnologías necesarias para la detección, investigación y respuesta de amenazas, construidas alrededor de una base abierta, un amplio ecosistema de socios y más de 900 integraciones preconstruidas que proporcionan una interoperabilidad sólida entre los conjuntos de herramientas de IBM y terceros.

"Ante la creciente superficie de ataque y tiempos de ataque cada vez menores, la velocidad y la eficiencia son fundamentales para el éxito de los equipos de seguridad con recursos limitados", dijo Mary O'Brien, Gerente General de IBM Security. "IBM ha diseñado la nueva QRadar Suite en torno a una experiencia de usuario única y moderna, integrada con IA sofisticada y automatización para maximizar la productividad de los analistas de seguridad y acelerar su respuesta en cada etapa de la cadena de ataque".

Co-innovación para las demandas de seguridad del mundo real

QRadar Suite es la culminación de años de inversión, adquisiciones e innovaciones de IBM en la detección y respuesta de amenazas. Cuenta con decenas de capacidades maduras de IA y automatización refinados con el tiempo con usuarios y datos del mundo real, incluyendo la experiencia de IBM Managed Security Services con más de 400 clientes. También incluye innovaciones desarrolladas en colaboración con IBM Research y la comunidad de seguridad de código abierto.

Estos recursos basados en IA han demostrado mejorar la velocidad y la precisión de las operaciones SOC: por ejemplo, permitiendo que IBM Managed Security Services automatice más del 70% de los cierres de alertas y reduzca sus plazos de triage de alertas en 55% en promedio en el primer año de implementación.

Al reunir estas capacidades a través de la experiencia unificada de analistas, QRadar Suite contextualiza y prioriza automáticamente las alertas, muestra datos en formato visual para consumo rápido y brinda *insights* compartidos y flujos de trabajo automatizados entre productos. Este enfoque puede reducir drásticamente la cantidad de pasos y pantallas necesarias para investigar y responder a las amenazas.

Al ayudar a los analistas a responder con más rapidez y eficiencia, QRadar Suite también puede ayudar a los equipos de seguridad a mejorar su productividad y liberar tiempo para trabajos de mayor valor.

Suite de seguridad abierta, conectada y modernizada

QRadar Suite aprovecha tecnologías y estándares abiertos en todo el portafolio, junto con cientos de integraciones preconstruidas con los socios de los ecosistemas de IBM Security. Este modelo permite compartir *insights* más profundos y acciones automatizadas en nubes de terceros, productos puntuales y 'lagos' de datos, lo que reduce los tiempos de implementación e integración de meses a días o semanas.

IBM Security QRadar Suite incluye los siguientes productos principales, inicialmente entregados como SaaS y actualizados con

la nueva experiencia de analista unificada: QRadar Log Insights, QRadar EDR, QRadar XDR, QRadar SOAR y QRadar SIEM. QRadar Suite ya está disponible a través de ofertas individuales de SaaS. Para más información, visite: ibm.com/qradar

Acerca de IBM Security

IBM Security ayuda a proteger a las empresas y los gobiernos más grandes del mundo con un portafolio integrado de productos y servicios de seguridad, impulsados con capacidades de IA dinámica y recursos de automatización. El portafolio, respaldado por la investigación de renombre mundial de IBM Security X-Force®, permite a las organizaciones prever las amenazas, proteger los datos a medida que se mueven, y responder con rapidez y precisión sin frenar la innovación empresarial. Miles de organizaciones confían en IBM como su socio para evaluar, diseñar estrategias, implementar y gestionar transformaciones de seguridad. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo, monitorea más de 150 mil millones de eventos de seguridad por día en más de 130 países y ha recibido más de 10.000 patentes de seguridad en todo el mundo.

[1] [Encuesta global](#) de 1.000 profesionales de centros de operaciones de seguridad, realizado por Morning Consult, patrocinado por IBM, marzo de 2023

[2] Basado en el análisis interno de IBM de los datos de rendimiento agregados observados a partir del trabajo de Managed Security Services con +400 clientes. El tiempo promedio de triaje de alerta se redujo en 55% durante el primer año utilizando las capacidades de IA y automatización que ahora forman parte de QRadar Suite.
