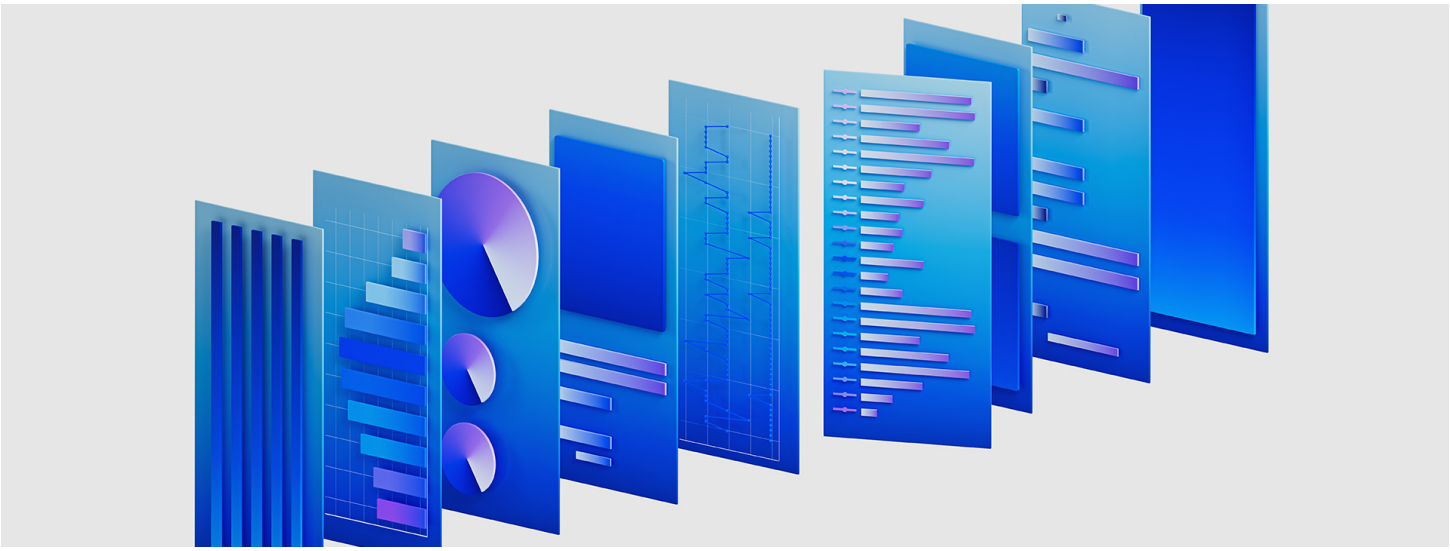
Anuncios

IBM lanza la nueva suite de seguridad de QRadar para acelerar la detección y respuesta ante amenazas

Una interfaz unificada y modernizada agiliza la respuesta de los analistas a lo largo de todo el ciclo de vida de los ataques

Las funciones sofisticadas de IA y automatización aceleran la selección de alertas en un 55%



ARMONK, NY - 24 de abril de 2023 – IBM (NYSE: IBM) ha presentado su nueva suite de seguridad diseñada para unificar y acelerar la experiencia de los analistas de seguridad a lo largo de todo el ciclo de vida de los incidentes. IBM Security QRadar Suite representa una importante evolución y expansión de la marca QRadar, que abarca todas las tecnologías básicas de detección, investigación y respuesta ante amenazas, con una importante inversión en innovaciones en todo el porfolio de productos.

Suministrada como servicio, IBM Security QRadar Suite está construida sobre una base abierta y diseñada específicamente para las exigencias de la nube híbrida. Presenta una interfaz de usuario única y modernizada en todos los productos, con IA y automatización avanzadas integradas que permiten a los analistas trabajar con mayor velocidad, eficiencia y precisión en sus principales conjuntos de herramientas.

En la actualidad, los equipos de los centros de operaciones de seguridad (SOC) protegen una huella digital que crece a un ritmo rápido y se extiende a través de entornos de nube híbrida, lo que crea complejidad y dificulta seguir el ritmo de la aceleración de los ataques. La investigación de alertas y los procesos de respuesta, que exigen mucho trabajo, pueden ralentizarlos, al igual que la recopilación manual de información y la alternancia entre datos, herramientas e interfaces desconectados. Según una encuesta reciente[1], los profesionales de los SOC afirman que dedican aproximadamente un tercio de su jornada a investigar y validar

"Ante un escenario de ataque cada vez mayor y con una frecuencia de tiempo menor, la velocidad y la eficiencia son fundamentales para el éxito de los equipos de seguridad con recursos limitados. IBM ha diseñado toda la cartera nueva de QRadar Suite en torno a una experiencia de usuario singular y modernizada, integrada con IA y automatización sofisticadas para maximizar la productividad de los analistas de seguridad y acelerar su respuesta en cada paso de la cadena

incidentes que resultan no ser amenazas reales.

de ataque. ”

Basándose en el actual liderazgo de la compañía en 12 categorías de seguridad[2], IBM ha rediseñado su cartera de productos de detección y respuesta a amenazas, líder del mercado, para ofrecer la máxima velocidad y eficiencia, y satisfacer las necesidades específicas de los analistas de seguridad actuales. La nueva IBM Security QRadar Suite incluye EDR/XDR, SIEM, SOAR y una nueva función de gestión de registros nativa de la nube. Todo ello construido en torno a una interfaz de usuario común, con información compartida y flujos de trabajo conectados, además de los siguientes elementos de diseño básicos:

- **Experiencia analítica unificada**: perfeccionada en colaboración con cientos de usuarios reales, la suite cuenta con una interfaz de usuario común modernizada en todos los productos y ha sido diseñada para aumentar significativamente la velocidad y la eficiencia de los equipos de seguridad en toda la cadena de ataque. Incorpora funciones de IA y automatización de nivel empresarial que han demostrado acelerar la investigación y clasificación de alertas en un 55% de media durante el primer año[3].
- **Desempeño en la nube, velocidad y escala:** disponibles como un servicio en Amazon Web Services (AWS), los productos QRadar Suite permiten un despliegue, visibilidad e integración simplificado a través de entornos en la nube y fuentes de datos. La suite también incluye una nueva capacidad de gestión de registros nativa en la nube optimizada para una acogida de datos altamente eficiente, búsqueda rápida y análisis a escala.
- **Base abierta, integraciones predefinidas:** la suite reúne las principales tecnologías necesarias para la detección, investigación y respuesta ante amenazas, desarrolladas sobre una base abierta, un amplio ecosistema de socios y más de 900 integraciones pre-integradas que proporcionan una sólida interoperabilidad entre IBM y conjuntos de herramientas de terceros.

"Ante un escenario de ataque cada vez mayor y con una frecuencia de tiempo menor, la velocidad y la eficiencia son fundamentales para el éxito de los equipos de seguridad con recursos limitados", ha afirmado Mary O'Brien, directora general de IBM Security. "IBM ha diseñado toda la cartera nueva de QRadar Suite en torno a una experiencia de usuario singular y modernizada, integrada con IA y automatización sofisticadas para maximizar la productividad de los analistas de seguridad y acelerar su respuesta en cada paso 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 detección y respuesta ante amenazas. Cuenta con docenas de capacidades maduras de IA y automatización que se han perfeccionado con el tiempo a partir de la actividad de los usuarios y de datos reales, incluyendo los compromisos de IBM Managed Security Service con más de 400 clientes. También incluye innovaciones desarrolladas en colaboración con IBM Research y la comunidad de seguridad de código abierto.

Se ha demostrado que estas funciones basadas en IA mejoran significativamente la velocidad y la precisión de las operaciones de los SOC: por ejemplo, permitiendo a IBM Managed Security Services automatizar más del 70% de los cierres de alertas[4] y reducir sus plazos de selección de alertas en un 55% de media durante el primer año de implementación.

Al reunir estas capacidades a través de una experiencia unificada para el analista, QRadar Suite contextualiza y prioriza automáticamente las alertas, muestra los datos en formato visual para un consumo rápido y proporciona perspectivas compartidas y flujos de trabajo automatizados entre productos. Este enfoque puede reducir drásticamente el número de pasos y pantallas necesarios para investigar y responder a las amenazas. Algunos ejemplos son:

- **Selección de alertas basadas en IA**: prioriza o cierra alertas en función del análisis de riesgos basados en IA entrenados en patrones de respuesta de analistas anteriores, junto con inteligencia de amenazas externas de IBM X-Force e informaciones más amplias procedentes de todos los conjuntos de herramientas de detección.
- **Investigación automatizada de amenazas**: identifica incidentes de alta prioridad que pueden justificar una investigación y la inicia automáticamente, obteniendo artefactos asociados y recopilando pruebas y datos en todos los entornos. El sistema utiliza estos resultados para generar una cronología y un gráfico de ataque del incidente basado en el marco ATT&CK de MITRE, y recomienda acciones para acelerar la respuesta.
- **Búsqueda acelerada de amenazas**: utiliza un lenguaje de amenazas de código abierto y capacidades de búsqueda para ayudar a los profesionales a descubrir ataques furtivos e indicadores de compromiso en sus entornos, sin mover los datos de su fuente original.

Al ayudar a los analistas a responder con mayor rapidez y eficacia, las tecnologías integradas en QRadar también pueden ayudar a los equipos de seguridad a mejorar su productividad y liberar tiempo de los analistas para que realicen tareas de mayor valor.

Suite de seguridad abierta, conectada y modernizada

QRadar suite aprovecha las tecnologías y los estándares abiertos de todo el portfolio, junto con cientos de integraciones predefinidas con socios del ecosistema de IBM Security. Este modelo permite un conocimiento compartido más profundo y acciones automatizadas a través de nubes de terceros, productos puntuales y *data lakes*, pudiendo reducir los tiempos de despliegue e integración de meses a días o semanas.

IBM QRadar Suite también incluye los siguientes productos principales, suministrados inicialmente como SaaS y actualizados con la nueva experiencia de analista unificada:

- **QRadar Log Insights:** una nueva solución de gestión de registros y observabilidad de la seguridad en la nube que proporciona una ingestión de datos simplificada, búsquedas en menos de un segundo y análisis rápidos. Está diseñada para una gestión rentable de los registros de seguridad, junto con búsquedas e investigaciones federadas.
- **QRadar EDR y XDR:** ayuda a las empresas a proteger sus terminales contra amenazas desconocidas hasta ahora, utilizando la automatización y cientos de modelos de aprendizaje y comportamientos automáticos para detectar anomalías de comportamiento y responder a los ataques casi en tiempo real. Aprovecha un enfoque único que supervisa los sistemas operativos desde el exterior, ayudando a evitar la manipulación o interferencia de los ciberdelincuentes. Para las empresas que buscan ampliar sus capacidades de detección y respuesta más allá del *endpoint*, IBM también ofrece XDR con correlación de

alertas, investigación automatizada y respuestas recomendadas a través de la red, la nube, el correo electrónico y más, así como detección y respuesta gestionadas (MDR).

- **QRadar SOAR:** esta solución, que ha recibido el premio Red Dot Design Award por su interfaz y experiencia de usuario, ayuda a las organizaciones a automatizar y orquestar los flujos de trabajo de respuesta a incidentes y a garantizar que sus procesos específicos se siguen de forma coherente, optimizada y medible. Además, incluye 300 integraciones preconfiguradas para responder a más de 180 normativas globales sobre violación de datos y privacidad.
- **QRadar SIEM:** esta solución de IBM, líder del mercado, QRadar SIEM se ha mejorado con la nueva interfaz de analista unificada, que proporciona información y flujos de trabajo compartidos con herramientas de operaciones de seguridad más amplias. Ofrece detección en tiempo real, aprovechando IA, análisis de comportamiento de red y usuario, e inteligencia de amenazas del mundo real para proporcionar a los analistas alertas más precisas, contextualizadas y priorizadas. IBM también tiene previsto que QRadar SIEM esté disponible como servicio en AWS a finales del segundo trimestre de 2023.

IBM Security QRadar Suite ya está disponible a través de ofertas SaaS individuales. Para más información, visite: https://www.ibm.com/es-es/qradar

Las declaraciones relativas a la futura dirección e intenciones de IBM están sujetas a cambios o retirada sin previo aviso, y representan únicamente metas y objetivos.

Acerca de IBM Security

IBM Security ayuda a proteger a las empresas y gobiernos más grandes del mundo con una cartera integrada de productos y servicios de seguridad, infundida con capacidades dinámicas de IA y automatización. La cartera, respaldada por la investigación de renombre mundial IBM Security X-Force®, permite a las organizaciones predecir amenazas, proteger datos en movimiento y responder con velocidad y precisión sin frenar la innovación empresarial. IBM cuenta con la confianza de miles de organizaciones como su socio para evaluar, elaborar estrategias, implementar y gestionar transformaciones de seguridad. IBM cuenta con una de las organizaciones de investigación, desarrollo y distribución de seguridad más amplias del mundo, supervisa más de 150.000 millones de eventos de seguridad al día en más de 130 países y ha obtenido más de 10.000 patentes de seguridad en todo el mundo.

---

[1] Resultados del estudio Global Security Operations Center, administrado por Morning Consult y encargado por IBM, marzo de 2023. Basado en las respuestas de 1.000 profesionales de centros de operaciones de seguridad encuestados de 10 países.

[2] Basado en evaluaciones de productos de seguridad de firmas de analistas externos, entre las que se incluyen Gartner, IDC, Forrester, KuppingerCole y Omdia, que sitúan a IBM como líder en 12 categorías de productos de seguridad: SIEM, SOAR, Plataforma de Inteligencia para la Reducción del Fraude, Autenticación Basada en el Riesgo, Gobierno y Administración de Identidades, Gestión de Accesos, Gestión de Identidades y Accesos como Servicio, Gobierno e Inteligencia de Accesos y Gobierno de Identidades, Autenticación, Gestión de Identidades y Accesos de Clientes, Seguridad de Datos, Gestión Unificada de Endpoints.

[3] Basado en el análisis interno de IBM de los datos de rendimiento agregados observados de los compromisos de Managed Security Service con más de 400 clientes de 2018-2019, que mostraron que la línea de tiempo promedio de triaje de alertas se redujo en un 55% durante el primer año utilizando AI y capacidades de automatización que ahora forman parte de QRadar. Los resultados reales variarán en función de las configuraciones y condiciones del cliente y, por lo tanto, no se pueden ofrecer resultados esperados de forma general..

[4] Informe del IBM Institute for Business Value, "AI and automation for cybersecurity", 2022. Resultados basados en el análisis de IBM de los datos de rendimiento anuales agregados observados de cientos de clientes globales que utilizan las capacidades de IA y automatización que ahora forman parte de QRadar Suite. Los resultados reales variarán en función de las configuraciones y condiciones del cliente y, por lo tanto, no se pueden ofrecer resultados esperados de forma general.

For further information: Alfonso Mateos Cadenas. Dpto. Comunicación. alfonso.mateos@ibm.com