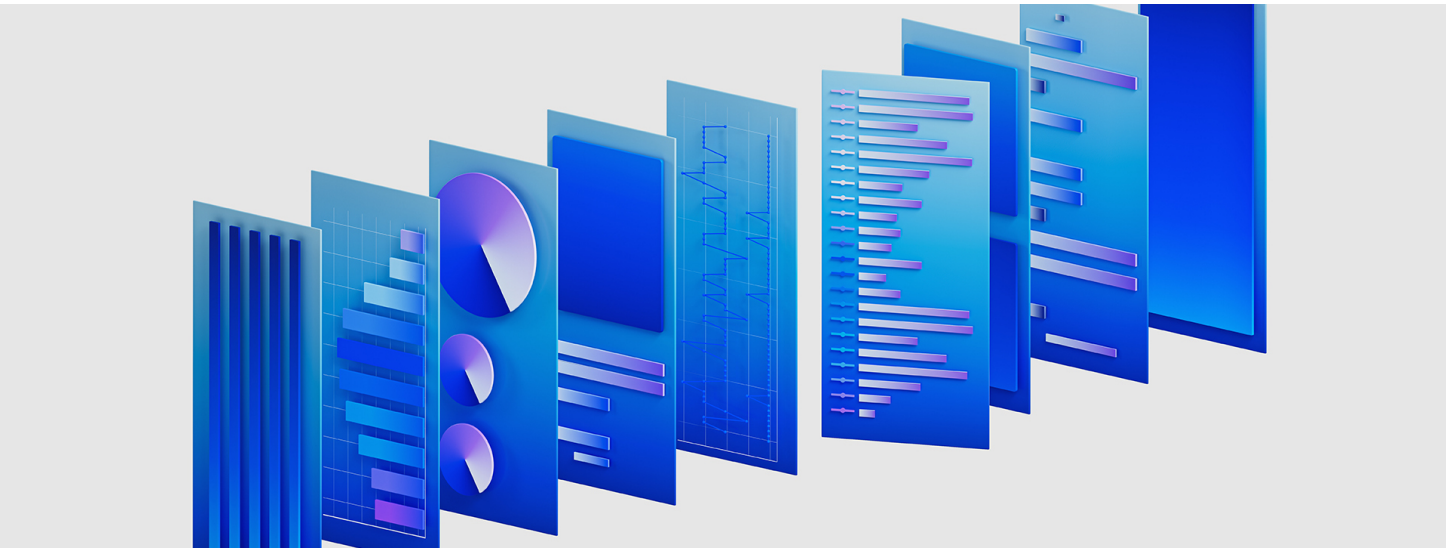
Comunicados

IBM presenta su SIEM nativo en la nube, creado para maximizar el tiempo y el talento de los equipos de seguridad

- Con una base modernizada y una experiencia de usuario rediseñada, permite a los analistas de seguridad y a la IA trabajar juntos de forma más eficaz



Bogotá, 16 de noviembre de 2023 - IBM anunció una importante evolución de su tecnología insignia IBM QRadar SIEM: rediseñada con una nueva arquitectura nativa en la nube construida específicamente para la escala, la velocidad y la flexibilidad de la nube híbrida. IBM también dio a conocer los planes para entregar capacidades de IA generativa dentro de su portafolio de detección y respuesta de amenazas, aprovechando watsonx, la plataforma empresarial de datos e IA de la compañía.

Los entornos de nube híbrida actuales están evolucionando y escalando a un ritmo exponencial, creando una superficie de ataque más grande y compleja que proteger. Esta creciente huella de TI hace que sea más difícil encontrar rápidamente las verdaderas amenazas entre el ruido, ralentizadas por tecnologías aisladas, búsquedas manuales y una sobrecarga de alertas, sin un contexto claro ni visual. De hecho, los profesionales del SOC llegan a menos de la mitad (49%) de las alertas que se supone que deben revisar dentro de un día de trabajo típico, según una encuesta global reciente [1].

"Nuestro nuevo SIEM nativo en la nube es un elemento central de la misión de IBM de marcar el comienzo de la próxima generación de operaciones de seguridad, diseñadas para la era de la nube híbrida e IA", dijo Kevin Skapinetz, Vicepresidente de Estrategia y Gestión de Productos, IBM Security. "En lugar de obligar a los analistas a trabajar en torno a la complejidad de las tecnologías de seguridad, estamos diseñando la tecnología para eliminar la complejidad: cancelando el ruido, simplificando la experiencia del usuario y capacitando a los analistas para hacer frente a las amenazas urgentes con mayor velocidad y confianza".

El SIEM nativo en la nube se basa en los 13 años de liderazgo en el mercado de IBM QRadar y en el reconocimiento de los analistas [2] para analítica de seguridad profunda, con una arquitectura rediseñada para una ingesta de datos altamente eficiente, búsquedas rápidas y análisis a escala. Construido sobre una base abierta, es la incorporación más reciente a QRadar Suite, el portafolio integrado de software de detección y respuesta de amenazas de IBM.

El nuevo IBM QRadar SIEM nativo en la nube estará disponible como SaaS en el cuarto trimestre de 2023, con planes para ofrecer software para despliegue en infraestructura local y multinube en 2024.

Abierto desde su *core*

Basado en Red Hat OpenShift, QRadar SIEM está diseñado para ser abierto desde la base, permitiendo una mayor interoperabilidad con herramientas y nubes de múltiples proveedores. Aprovecha el código y los estándares abiertos para las funciones principales, incluyendo reglas de detección y lenguaje de búsqueda, facultando su funcionamiento en los *stacks* de tecnología y seguridad de las empresas.

- **Utiliza las detecciones de la comunidad de seguridad:** aprovecha el lenguaje común y compartido para las reglas de detección (SIGMA), permitiendo a los clientes importar rápidamente detecciones colaborativas de la comunidad de seguridad a medida que evolucionan las amenazas.
- **Investiga entre fuentes de datos:** ofrece capacidades únicas de búsqueda de amenazas creadas sobre tecnologías de código abierto, habilitando a los analistas para buscar e investigar de manera proactiva amenazas en la infraestructura local y la nube, de manera simple y unificada, sin mover los datos de su fuente original.
- **Amplia red de aliados:** basado en el ecosistema de QRadar, una de las redes de aliados más grandes de la industria con más de 700 integraciones prediseñadas.

Suite completa para una respuesta de seguridad proactiva y conectada

Como parte de QRadar Suite, el nuevo SIEM nativo en la nube ofrece a los clientes acceso a un amplio conjunto de capacidades integradas que pueden permitir una detección, investigación y respuesta más proactiva a través de conjuntos de herramientas. Con QRadar Suite, las organizaciones pueden aumentar la visibilidad de sus activos expuestos a través de capacidades de gestión de superficie de ataque (ASM), buscar amenazas en conjuntos de herramientas, proteger *endpoins* con EDR y conectarse a *playbooks* automatizados para acelerar la respuesta (SOAR). QRadar SIEM empodera los usuarios con conocimiento colaborativo y acciones automatizadas a través de sus herramientas principales, a las que se accede directamente desde su interfaz de usuario principal, sin necesidad de cambiar entre herramientas.

IA de nivel empresarial para acelerar la respuesta a amenazas críticas

QRadar SIEM aplica múltiples capas de IA y automatización para mejorar la calidad de las alertas y la eficiencia de los analistas de seguridad. Estas capacidades maduras de IA se han entrenado en millones de alertas de la vasta red de clientes de IBM y se refinan aún más después de la implementación teniendo en cuenta el entorno único de cada cliente. Por ejemplo:

- **Reducir el ruido y mejorar alertas:** las capacidades de priorización de alertas usan IA para quitar automáticamente la prioridad de las alertas de baja prelación, mientras agrupan, contextualizan y escalan automáticamente las alertas de alta prelación, considerando el contexto de riesgo a partir de la inteligencia de amenazas en curso y patrones de respuesta de los analistas. Esta capacidad permitió a IBM Consulting Cybersecurity Services automatizar el 85 % de la gestión de alertas de clientes [3] y acelerar plazos de clasificación de amenazas en un 55 % durante el primer año de uso [4].
- **Iniciar investigaciones:** las capacidades de IA ejecutan automáticamente búsquedas unificadas a través

de sistemas conectados, generando una línea de tiempo visual de ataque, correlaciones con MITRE ATT&CK y acciones recomendadas, dando ventaja a los analistas en tareas de investigación.

- **Actualizar automáticamente la información sobre las detecciones:** la analítica de QRadar SIEM se actualiza automáticamente con nuevas reglas de detección e inteligencia de amenazas de forma continua para mantenerse al ritmo de las amenazas en evolución.

Las capacidades de Inteligencia Artificial en seguridad de IBM están incorporadas de forma nativa en la interfaz de QRadar Suite de los analistas, entregando conocimientos contextuales y ayudándoles a aprovechar la IA de forma más intuitiva dentro de sus flujos de trabajo habituales.

IA generativa para mejorar la productividad del SOC

IBM también planea lanzar capacidades de seguridad con IA generativa (IAG) en QRadar Suite a principios de 2024, basadas en watsonx, la plataforma de datos e inteligencia artificial de la compañía. IBM está diseñando IAG para ayudar a optimizar el tiempo y el talento de los equipos de seguridad mediante la gestión de ciertas tareas tediosas para los analistas, para facilitarles la realización de trabajos más desafiantes y de mayor valor. Por ejemplo:

- **Automatizar informes:** crear resúmenes simples de casos e incidentes de seguridad que se puedan compartir con una variedad de partes interesadas con un solo clic.
- **Acelerar la caza de amenazas:** generar búsquedas para detectar amenazas automáticamente con descripciones en lenguaje natural de los comportamientos y patrones de ataque, ayudando a acelerar la respuesta a nuevas campañas de amenazas.
- **Interpretar los datos:** ayudar a los analistas a comprender rápidamente los datos de los *logs* o registros de seguridad proporcionando explicaciones sencillas de los eventos que se han producido en un sistema, reduciendo las barreras técnicas y agilizando sus investigaciones.
- **Curar inteligencia de amenazas:** interpretar y resumir inteligencia sobre amenazas altamente relevante, centrándose en las campañas que tienen más probabilidades de afectar a los clientes en función de su perfil de riesgo único.

IBM también está desarrollando capacidades predictivas de seguridad con IA generativa que se entrenarán para crear respuestas activas que se optimicen con el tiempo, como ayudar al equipo de seguridad a encontrar incidentes similares, actualizar sistemas afectados y parchar código vulnerable.

Más allá de estos casos de uso, IBM planea incorporar la IA generativa de manera general en su portafolio de software y servicios de seguridad. Estas capacidades aprovecharán la infraestructura de watsonx, así como los modelos de IA de watsonx, que han sido entrenados con *datasets* curados, seleccionados y por especialidad, diseñados para ofrecer mayor confianza, transparencia y precisión.

Para más información sobre QRadar SIEM, visite: https://www.ibm.com/products/qradar-cloud-native-siem

Para obtener más detalles sobre IA en seguridad, visite: https://www.ibm.com/security/artificial-intelligence

Las declaraciones sobre la futura dirección e intención de IBM están sujetas a cambio o retirada sin previo aviso, y sólo representan objetivos y objetivos.

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] *Estudio global sobre los Centros de Operaciones de Seguridad, 2022 realizado por Morning Consult, patrocinado por IBM.*

[2] *QRadar ha sido identificado como un líder de mercado para SIEM en múltiples informes de terceros analistas durante los últimos 13 años, incluyendo informes de Gartner, Forrester, KuppingerCole, IDC y Omdia.*

[3] *Basado en el análisis interno de IBM de datos de rendimiento agregados observados en interacciones con más de 340 clientes en julio de 2023. Hasta el 85 % de las alertas se manejaron mediante automatización usando capacidades de IA que forman parte de QRadar SIEM. Los resultados varían según las configuraciones y condiciones del cliente y, por lo tanto, generalmente no se pueden proporcionar los resultados esperados.*

[4] *Basado en el análisis interno de IBM de datos de rendimiento agregados observados en interacciones con más de 400 clientes entre 2018 y 2019, que mostró que el cronograma promedio de clasificación de alertas se redujo en un 55 % durante el primer año utilizando capacidades de automatización e inteligencia artificial que forman parte de QRadar SIEM. Los resultados varían según las configuraciones y condiciones del cliente y, por lo tanto, generalmente no se pueden proporcionar los resultados esperados.*