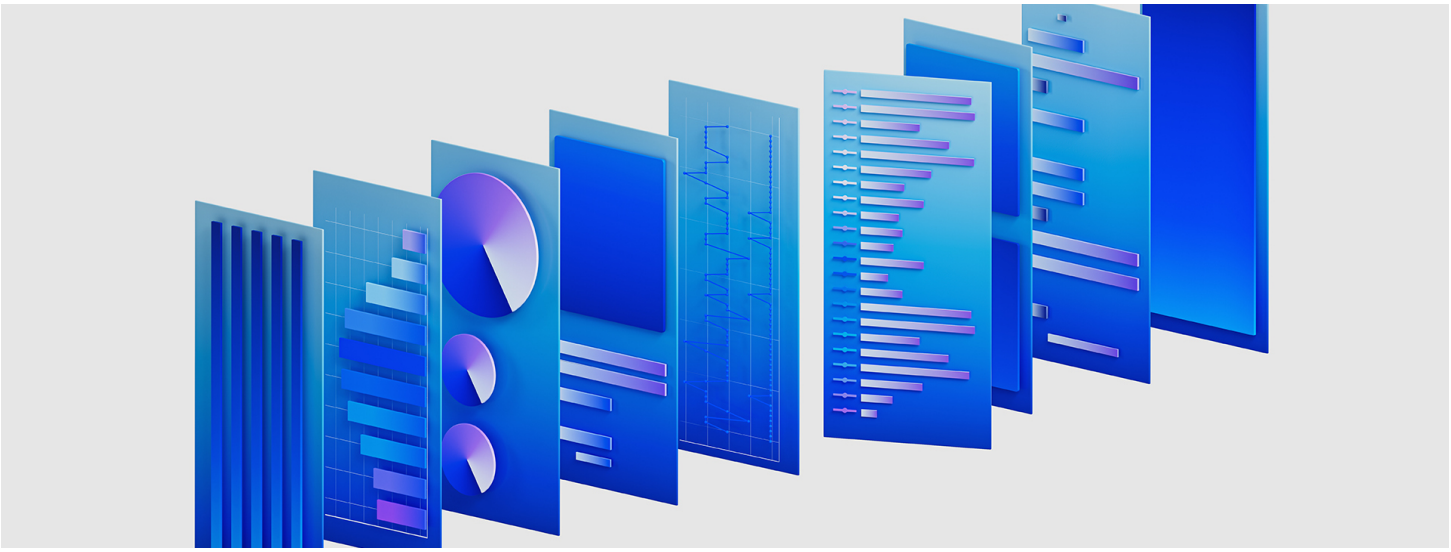
Anuncios

IBM presenta un SIEM nativo en la nube diseñado para maximizar el tiempo y el talento de los equipos de seguridad

Permite a los analistas de seguridad y a la IA trabajar codo con codo de forma más eficaz con una base modernizada y una experiencia de usuario rediseñada



ARMONK, Nueva York, 7 de noviembre de 2023 - IBM ha anunciado hoy una importante evolución de su producto insignia IBM QRadar SIEM: rediseñado sobre una nueva arquitectura nativa en la nube, construida específicamente para la escala, velocidad y flexibilidad de la nube híbrida. IBM también ha desvelado planes para ofrecer capacidades de IA generativa dentro de su portfolio de detección y respuesta a amenazas, aprovechando watsonx, la plataforma de datos e IA de la compañía preparada para empresas.

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

El nuevo SIEM QRadar nativo en la nube está construido para maximizar la potencia de los equipos de seguridad actuales. Está diseñado para aumentar y elevar el nivel del trabajo diario de los analistas de seguridad, aprovechando la IA para gestionar tareas repetitivas y que consumen mucho tiempo, a la vez que capacita a los analistas de seguridad para encontrar y responder a incidentes de seguridad de alta prioridad con mayor eficacia.

"Nuestro nuevo SIEM nativo de la nube es un elemento central de la misión de IBM para marcar el comienzo de la próxima generación de operaciones de seguridad, construidas para la era de la nube híbrida y la IA", dijo Kevin Skapinetz, Vicepresidente de Estrategia y Gestión de Productos de IBM Security. "En lugar de obligar a los analistas a trabajar en torno a la

> *“ Nuestro nuevo SIEM nativo de la nube es un elemento central de la misión de IBM para marcar el comienzo de la próxima generación de operaciones de seguridad, construidas para la era de la nube híbrida y la IA. 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 - eliminando el ruido, simplificando la experiencia del usuario y empoderando a los analistas para hacer frente a las amenazas urgentes con mayor velocidad y confianza. ”*

complejidad de las tecnologías de seguridad, estamos diseñando la tecnología para eliminar la complejidad - eliminando el ruido, simplificando la experiencia del usuario y empoderando 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 de mercado de QRadar y en el reconocimiento de los analistas[2] por su profunda analítica de seguridad, con una arquitectura rediseñada para una ingestión de datos altamente eficiente, búsqueda rápida y analítica a escala. Construida sobre una base abierta, es la última incorporación a QRadar Suite, la cartera integrada de software de detección y respuesta a amenazas de IBM.

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

Abierto en su núcleo

Construido sobre Red Hat OpenShift, QRadar SIEM está diseñado para ser abierto a nivel fundacional, lo que permite una interoperabilidad más profunda con herramientas y nubes de múltiples proveedores. Aprovecha el código abierto y los estándares abiertos para las funciones básicas, incluyendo las reglas de detección y el lenguaje de búsqueda, lo que le permite funcionar en las stacks tecnológicas y de seguridad más amplias de las empresas.

- Detecciones comunitarias de Harness Security: aprovecha **el lenguaje común y compartido para las reglas de detección (SIGMA**), lo que permite a los clientes importar rápidamente nuevas detecciones de crowdsourcing directamente desde la comunidad de seguridad a medida que evolucionan las amenazas.
- Investigación en todas las fuentes de datos: ofrece capacidades únicas **de búsqueda federada y caza de amenazas** basadas en tecnologías de código abierto, lo que permite a los analistas buscar e investigar de forma proactiva amenazas en fuentes de datos en la nube y locales de una forma única y unificada, sin mover los datos de su fuente original.
- Profunda red de partners: se basa en el ecosistema **QRadar, una de las mayores redes de socios** del sector con más de 700 integraciones preconfiguradas.

Suite completa para una respuesta de seguridad conectada y proactiva

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 proactivas a través de conjuntos de herramientas. Con QRadar Suite, las organizaciones pueden obtener visibilidad de sus activos expuestos a través de las funciones de gestión de la superficie de ataque (ASM), buscar amenazas en todos los toolsets, proteger en el punto final con EDR (Endpoint Detection and Response)y conectarse a guías automatizadas para acelerar la respuesta (SOAR). QRadar SIEM ofrece a los usuarios información compartida y acciones automatizadas en sus principales toolsets, a las que se accede directamente desde su interfaz de usuario principal, sin necesidad de cambiar de herramienta.

La IA de nivel empresarial acelera 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 han sido preentrenadas en millones de alertas de la vasta red de clientes de IBM y se perfeccionan aún más después de la implementación para tener en cuenta el entorno único de cada cliente. Por ejemplo:

- **Reducir el ruido y mejorar las alertas:** las capacidadesd de priorización de alertas utilizan la IA para priorizar automáticamente las alertas de baja intensidad, al tiempo que que agrupan, contextualizan y escalan automáticamente las alertas de alta prioridad, teniendo en cuenta el contexto de riesgo de la inteligencia de amenazas en curso y los patrones de respuesta de los analistas. Esta capacidad permitió a IBM Consulting Cybersecurity Services automatizar el 85% de la gestión de alertas para los clientes[3] y acelerar sus plazos de triaje de amenazas en un 55% en el primer año de uso[4].
- **Investigaciones inmediatas:** capacidad de IA que ejecuta automáticamente búsquedas federadas a través de sistemas conectados, generando una línea de tiempo visual del ataque, mapeos MITRE ATT&CK y acciones recomendadas - dando a los analistas una ventaja significativa en las tareas de investigación.
- **Actualización automática de las detecciones:** los análisis de QRadar SIEM se actualizan automáticamente con nuevas reglas de detección e inteligencia de amenazas de forma continua, para seguir el ritmo de las amenazas en evolución.

Las funciones de seguridad de IA de IBM están integradas de forma nativa en la interfaz de analista de QRadar Suite, lo que pone al alcance de los analistas información contextual y les ayuda a aprovechar la IA de forma más intuitiva en sus flujos de trabajo habituales.

IA generativa para mejorar la productividad de los SOC

IBM también tiene previsto lanzar capacidades de seguridad de IA generativa (GAI) para QRadar Suite a principios de 2024, basadas en watsonx, la plataforma de IA y datos de la empresa. IBM está diseñando GAI para ayudar a optimizar el tiempo y el talento de los equipos de seguridad mediante la gestión de ciertas tareas tediosas en nombre de los analistas, al tiempo que les facilita la realización de trabajos más desafiantes y de mayor valor. Por ejemplo

- **Automatizar la elaboración de informes:** crear resúmenes sencillos de casos e incidentes de seguridad que puedan compartirse con diversas partes interesadas con un solo clic.
- **Acelerar la caza de amenazas**: generar automáticamente búsquedas para detectar amenazas basadas en descripciones en lenguaje natural de comportamientos y patrones de ataque, lo que ayuda a acelerar la respuesta a las nuevas campañas de amenazas.
- **Interpretar datos generados por máquinas**: ayudar a los analistas a comprender rápidamente los datos de registro de seguridad proporcionando explicaciones sencillas de los eventos que han tenido lugar en un sistema, reduciendo las barreras técnicas y agilizando sus investigaciones.
- **Curar inteligencia sobre amenazas:** interpretar y resumir la inteligencia sobre amenazas de gran relevancia, 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 IA generativa que se entrenarán para crear respuestas activas que se optimicen con el tiempo, por ejemplo, ayudando al equipo de seguridad a encontrar incidentes similares,

actualizar los sistemas afectados y parchear el código vulnerable.

Más allá de estos casos de uso, IBM planea integrar la IA generativa en su portafolio más amplia 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 en conjuntos de datos curados y específicos del dominio, 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 más información sobre AI for Security, visite: https://www.ibm.com/security/artificial-intelligence

Las declaraciones relativas a la futura dirección e intención 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. Miles de organizaciones confían en IBM 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] Global Security Operations Center Study, 2022 realizado por Morning Consult, patrocinado por IBM.

[2] QRadar ha sido identificado como líder del mercado de SIEM en múltiples informes de analistas externos durante los últimos 13 años, incluidos informes de Gartner, Forrester, KuppingerCole, IDC y Omdia.

[3] Basado en el análisis interno de IBM de los datos de rendimiento agregados observados a partir de compromisos con más de 340 clientes en julio de 2023. Hasta el 85% de las alertas se gestionaron mediante automatización utilizando las capacidades de IA que forman parte de QRadar SIEM. Los resultados reales variarán en función de las configuraciones y condiciones de los clientes y, por lo tanto, no se pueden ofrecer resultados esperados generales.

[4] Basado en el análisis interno de IBM de los datos de rendimiento agregados observados de los compromisos 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 las capacidades de IA y automatización que forman parte de QRadar SIEM. Los resultados reales variarán en función de las configuraciones y condiciones del cliente y, por lo tanto, no se pueden proporcionar resultados

esperados en general

For further information: Camila Cuetos. Dpto. Comunicación. camila.cuetos2@ibm.com