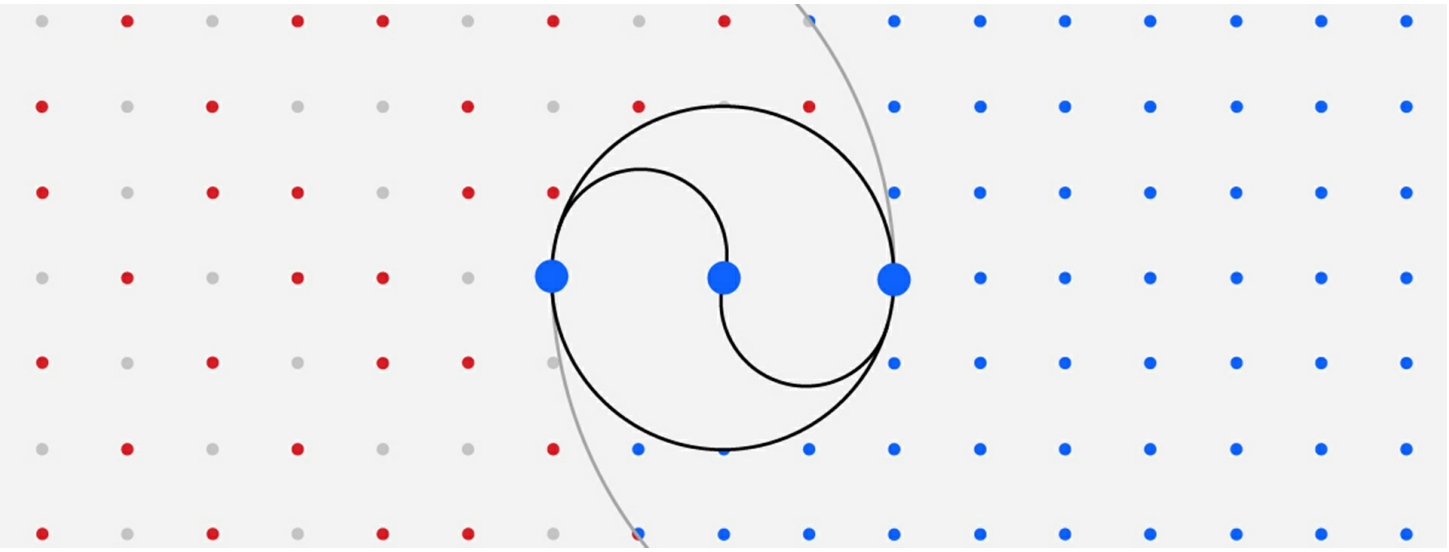
Comunicados

IBM anuncia nuevos servicios de detección y respuesta de amenazas impulsados por IA

- Ingiere y analiza datos de seguridad de un amplio ecosistema de tecnologías y proveedores.

- Ofrece monitoreo, investigación y remediación automatizada de alertas de seguridad 24/7.



ARMONK, N.Y., 5 de octubre de 2023 - IBM (NYSE: IBM) presentó hoy la próxima evolución de su oferta de servicios gestionados de detección y respuesta con nuevas tecnologías de IA, incluyendo la capacidad de escalar o cerrar automáticamente hasta el 85% de las alertas[1], ayudando a acelerar los tiempos de respuesta de seguridad para los clientes.

Los nuevos Servicios de Detección y Respuesta de Amenazas (TDR) proveen monitoreo, investigación y remediación automatizada de las alertas de seguridad de todas las tecnologías relevantes en los entornos de nube híbrida de los clientes 24x7, incluyendo las herramientas de seguridad existentes e inversiones, así como las tecnologías de nube, infraestructura local y tecnología operacional (OT). Los servicios gestionados son entregados por el equipo global de analistas de seguridad de IBM Consulting a través de la plataforma de servicios de seguridad avanzada de IBM, que aplica múltiples capas de IA e inteligencia contextual sobre amenazas de la vasta red de seguridad global de la compañía, ayudando a automatizar el ruido mientras escala rápidamente las amenazas críticas.

"Actualmente, los equipos de seguridad no sólo se ven superados en número por los atacantes, sino también por la cantidad de vulnerabilidades, alertas, herramientas y sistemas de seguridad que deben administrar en el día a día", dijo Chris McCurdy, Gerente General de IBM Consulting Cybersecurity Services a nivel global. "Al combinar análisis avanzado e inteligencia de amenazas en tiempo real con experiencia humana, los nuevos servicios de detección y respuesta a amenazas de IBM pueden aumentar las defensas de seguridad de las organizaciones con una capacidad escalable, en mejora continua y lo suficientemente sólida para las amenazas futuras".

Adaptando inteligentemente las defensas de amenazas

Los nuevos Servicios TDR están respaldados por un conjunto de tecnologías de seguridad impulsadas por IA que apoyan a miles de clientes en el mundo, monitoreando miles de millones de eventos potenciales de seguridad por día. Estas aprovechan modelos de IA que aprenden continuamente de los datos y las respuestas de los analistas de seguridad, y están diseñadas

para cerrar automáticamente alertas de baja prioridad y falsos positivos según el nivel de confianza definido por cada cliente. Esta funcionalidad también escala automáticamente las alertas de alto riesgo que requieren una acción inmediata de los equipos de seguridad y proporciona un contexto de investigación.

Los Servicios TDR de IBM están diseñados para proporcionar:

- **Reglas de detección colaborativas, alertas optimizadas.** Aprovechando los conocimientos en tiempo real del trabajo en gestión de amenazas de IBM, los nuevos servicios utilizan IA para evaluar y recomendar automáticamente las reglas de detección más efectivas, ayudando a mejorar la calidad de las alertas y la velocidad en los tiempos de respuesta. Esta capacidad ayudó a reducir las alertas SIEM de bajo valor en un 45% y a escalar automáticamente el 79% más de las alertas de alto valor que requerían atención inmediata[2]. Las organizaciones pueden aprobar y actualizar las reglas de detección con sólo dos clics a través de su portal de gestión conjunta.
- **Valoración MITRE ATT&CK.** Para mantenerse preparados para el ransomware y los ataques de wipe-out (eliminación), las organizaciones podrán ver cómo su entorno cubre las tácticas, técnicas y procedimientos del marco MITRE ATT&CK, en comparación con pares de la industria y geografía. Al aplicar la IA, los nuevos servicios están diseñados para conciliar las múltiples herramientas de detección con las políticas en vigor en una organización, brindando una visión empresarial sobre cómo detectar mejor las amenazas y evaluar las brechas para actualizar dentro del marco ATT&CK.
- **Integración continua de principio a fin.** Con un enfoque de APIs abiertas, los nuevos servicios pueden integrarse rápidamente con los activos de seguridad de las empresas, ya sea en la infraestructura local o en la nube. Las organizaciones pueden continuar accediendo a su ecosistema al mismo tiempo que tienen la opción de conectarse, colaborar y definir sus propios *playbooks* de respuesta a través de un portal de gestión conjunta. Esto permite una vista empresarial unificada, capacidades de remediación precisas y aplicación consistente de las políticas de seguridad IT y OT.
- **Soporte global 24x7.** Las organizaciones tendrán acceso 24/7 x 365 a +6.000 profesionales de IBM Cybersecurity Services en el mundo para ayudarles a mejorar los programas de seguridad. La vasta red global de IBM Consulting Cybersecurity Services atiende +3.000 clientes en el mundo, gestionando más de 2 millones de *endpoints* y 150 mil millones de eventos de seguridad por día.

"Hoy en día, los líderes de seguridad están tratando de escapar del círculo vicioso de escasez de personal, mayores amenazas y las demandas crecientes de la C-Suite para madurar su programa cibernético sin quebrar el banco. Para muchas organizaciones, cambiar las herramientas por las plataformas preferidas de un proveedor no funciona, ya que no pueden darse el lujo de cancelar inversiones anteriores en centros de operaciones de seguridad (SOC)", dijo Craig Robinson, Vicepresidente de Investigación de Servicios de Seguridad de IDC. "Servicios como el de IBM de Detección y Respuesta de Amenazas puede proporcionar la salida a esas preocupaciones, sin necesidad de eliminar las inversiones anteriores en seguridad, ayudando a transformar el capital humano en el SOC hacia un modo más proactivo".

Para apoyar la mejora continua de las capacidades de operaciones de seguridad, los Servicios TDR de IBM, que ya están disponibles, incluyen el acceso a los Servicios de Respuesta a Incidentes de IBM X-Force junto con la opción de incluir servicios adicionales de seguridad proactiva de IBM X-Force, como pruebas de penetración, simulación de adversarios o gestión de vulnerabilidades. X-Force también proporcionará orientación para ayudar a las empresas a mejorar las operaciones de seguridad a lo largo del tiempo, basándose en el panorama de amenazas actual, el entorno de TI en evolución de los clientes y los conocimientos obtenidos con miles de clientes de IBM Cybersecurity Services en todo el mundo.

Para más información de IBM TDR Services, visite https://www.ibm.com/services/threat-detection-response .

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] *Basado en el análisis interno de IBM de los datos agregados de desempeño que se observaron en los compromisos con +340 clientes en julio de 2023. Hasta el 85% de las alertas se manejaron a través de la automatización en lugar de la intervención humana, utilizando capacidades de IA que forman parte del servicio de Detección y Respuesta de Amenazas de IBM. Los resultados reales pueden variar en función de las configuraciones y condiciones de cada cliente y, por lo tanto, los resultados generalmente esperados no se pueden proporcionar.*

[2] *Basado en el análisis de IBM de los datos agregados de desempeño anual observados en 2022 con +150 clientes SIEM gestionados. Los resultados reales pueden variar en función de las configuraciones y condiciones de cada cliente y, por lo tanto, los resultados generalmente esperados no se pueden proporcionar.*
