IBM Security

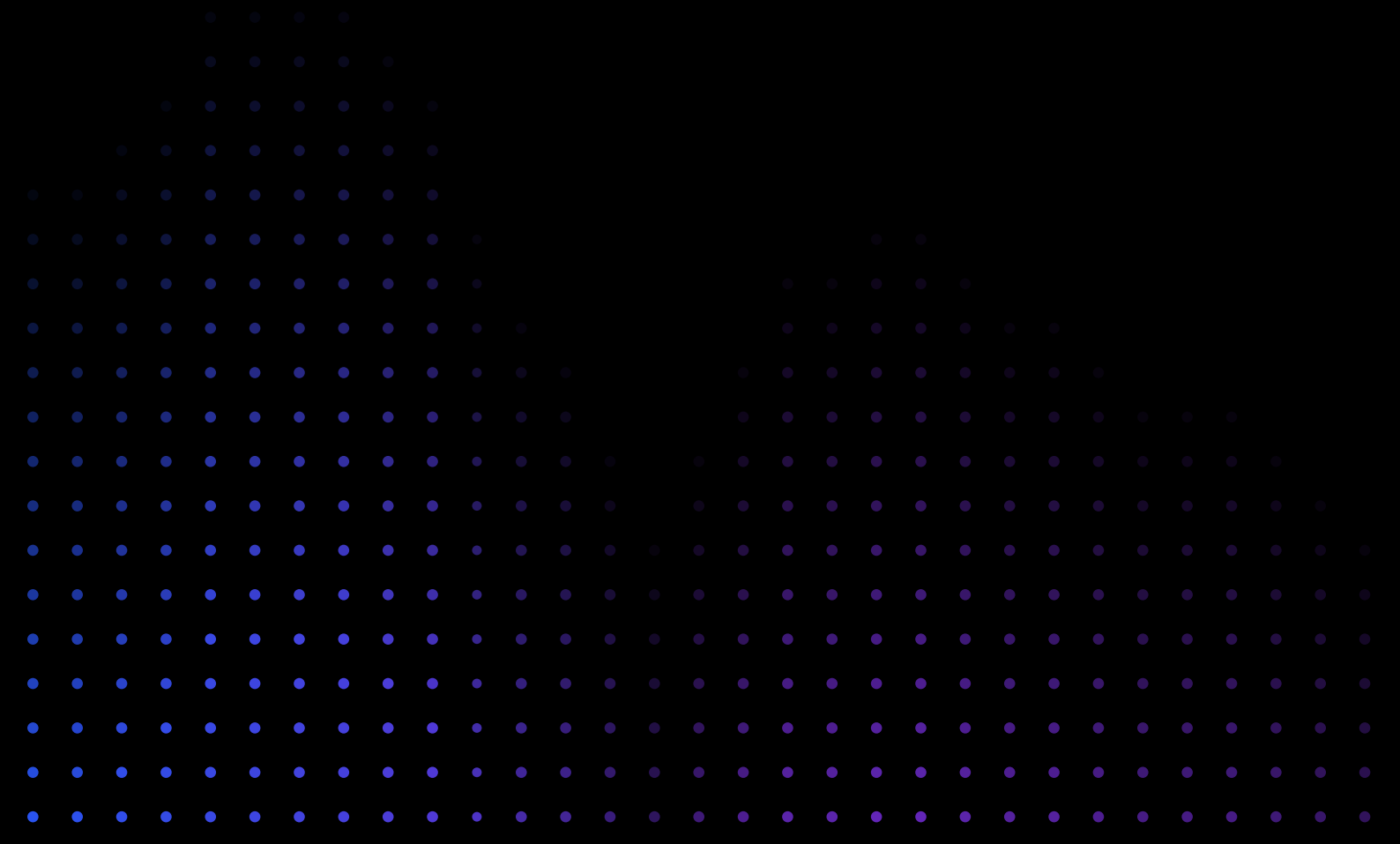
IBM

Más allá de la publicidad: IA en su SOC

Hágase estas 7 preguntas antes de adoptar una solución cognitiva de ciberseguridad

Visite nuestro sitio web →

Hable con un especialista →



01

¿Confío en nuestro balance de riesgos y seguridad?

Los responsables centrales de la seguridad informática (CISO) tienen uno de los trabajos más difíciles en el área de la tecnología: Deben permitir que los usuarios accedan a datos críticos, pero también proteger esos datos de amenazas internas, abuso de credenciales y error humano. Su trabajo es detectar y responder a todas las amenazas, incluidas las más complejas, dependiendo de un equipo que se normalmente encuentra abrumado y falto de personal.

Peor aún, los desafíos están en su punto más alto y las excusas nunca serán suficientes. Las organizaciones de sus clientes exigen seguridad. Los reguladores están vigilando. Las tarifas de seguro de ciberseguridad siguen aumentando. Los inversores no están tranquilos y los abogados están a la espera. Todos, desde el cuerpo directivo hasta los empleados de base, requieren una seguridad absoluta y hermética, mientras que ellos mismos también son un vector de vulnerabilidad.

Considere estos tres elementos de su lista de verificación:

A usted le falta personal capacitado

Los analistas de nivel 1 o de la primera línea suelen ser nuevos en la industria. Les lleva tiempo desarrollar realmente capacidades, confianza y madurez en las capacidades de investigación que usted necesita en su SOC. Según una investigación del ESG, el 51 % de las organizaciones informan haber tenido una “carencia problemática” de las capacidades de ciberseguridad durante el 2018. Desde 2017, ha aumentado en un 45%. La fatiga en un trabajo de ciberseguridad es real, según el ESG, el 38 % de los profesionales de ciberseguridad ya dicen que la carencia de capacidades los ha conducido a altos índices de desgaste y deserción de personal.

Los tiempos de expiración son demasiado prolongados y eso es un gasto para usted

Los tiempos de espera en promedio pueden varíar entre 50 y 200 días. Las empresas que identificaron una violación en menos de 100 días ahorraron más de $ 1 millón en comparación con los que demoraron más de 100 días.

Su equipo está sobrecargado de información

Es probable que su organización sufra de fatiga laboral en ciberseguridad (no se preocupe, no está solo). La organización está abrumada por el trabajo repetitivo y hay un desmoronamiento de los procesos definidos. Todo esto se suma a una mayor probabilidad de que se haya pasado por alto un importante indicador de compromiso (IoC). Y cuando usted añade nuevas soluciones puntuales para abordar las amenazas más recientes y avanzadas, solo empeora las cosas: esto crea más silos de datos, crea complejidad de integración y aumenta la cantidad de perspectivas que sus analistas deben analizar.

Es necesario un SIEM para su operación, ¿pero qué hay de la IA? ¿Qué parte es publicidad y qué parte es real?

02

¿Cómo ayuda la IA a lograr el equilibrio adecuado?

Ya habrá escuchado a los evangelistas de la IA, pero ¿cómo puede asegurarse de que la solución de IA en la que usted invierte es una solución inteligente y cognitiva que puede facilitar su trabajo? La respuesta antipublicitaria se centra en garantizar que puede aprender y puede ser proactiva. Debería automatizar sus tareas repetitivas para mitigar la fatiga y solucionar lo que podría ser su mayor desafío: las personas. Es así de simple.

03

¿Cómo hace la IA para realmente fortalecer mi posicionamiento de seguridad?

Lo cierto es que no es humanamente posible estar siempre actualizado con el escenario de amenazas que se expande constantemente, especialmente dado lo ocupado que está haciendo malabares con el liderazgo, manteniendo la posición de seguridad de su organización y las tareas diarias de poner en marcha su SOC. Se requiere un arsenal de herramientas ya disponibles para proteger su SOC.

En los últimos años, la IA ha sido publicitada y alabada en exceso. Eso lo entendemos. Pero tenga en cuenta lo siguiente: la IA adecuada, aplicada correctamente dentro de su SOC es una herramienta altamente efectiva que aprende y se actualiza sola continuamente, por sí misma. No es la cura para todos los males, pero es una parte esencial de su arsenal de armas de seguridad.

04

¿La IA remplazará a mi equipo? ¿Esta solución amenaza su subsistencia?

La IA trabaja junto a su equipo, no contra él. Maneja tareas repetitivas y le ayuda a tomar decisiones mejor informadas. La IA combina datos externos de manera proactiva (información de todos lados) y los combina con su entorno nativo para comprender cuál debería ser su próximo movimiento. En todos los casos, usted decide cuánto trabajo desea que la IA realice, desde tareas que llevan más tiempo hasta tomar decisiones rutinarias. En conclusión, la IA siempre estará allí, siempre estará aprendiendo, pero es usted quien lleva el ritmo y quien estará al mando.

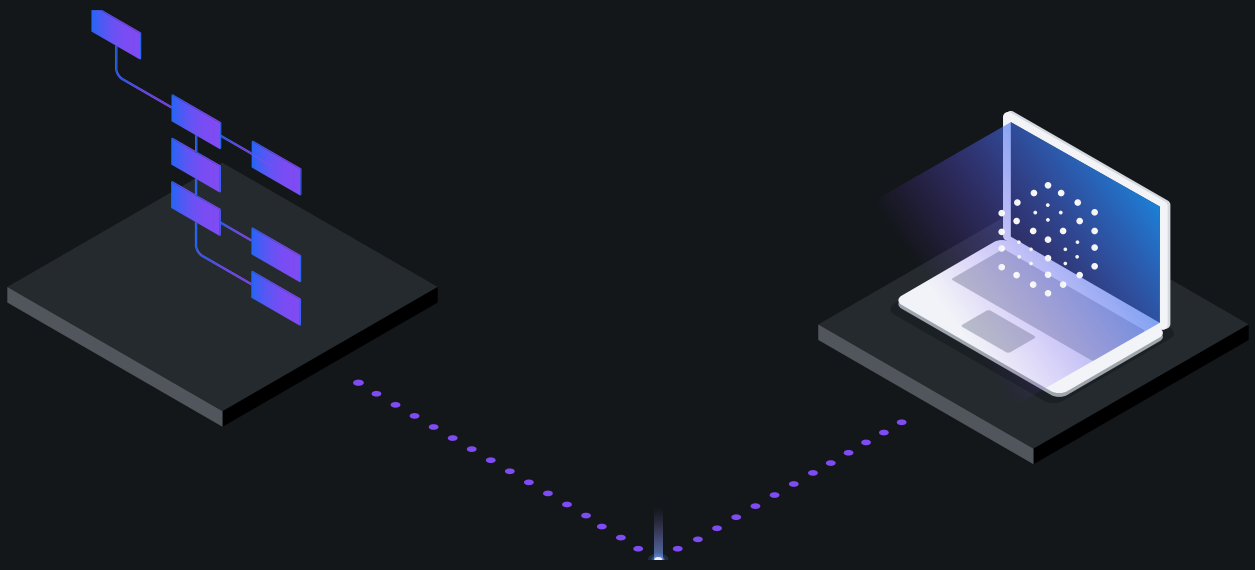
05

¿La solución para esto es la IA o el aprendizaje automático? ¿Yo sé cuál es la diferencia?

Cuando la gente usa términos como “IA” y “aprendizaje automático”, suelen usarlos de manera intercambiable. Lo que es peor, también despliegan una sopa alfabética de abreviaturas como “AA”, en lugar de “aprendizaje automático”, o dicen “inteligencia artificial”, en lugar de “IA”. Pero no deje que eso lo confunda: La IA (inteligencia artificial) y el AA (aprendizaje automático) no son lo mismo, así que no compre una solución de aprendizaje automático cuando lo que realmente desea es IA. El aprendizaje automático se centra en la capacidad de las máquinas para interactuar con los datos. Puede “aprender” e incluso cambiar un algoritmo a medida que recibe más datos, pero es allí donde se detiene ya que el aprendizaje automático es un subconjunto de la IA.

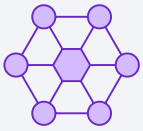
La IA tiene la capacidad cognitiva de crecer, aprender y realizar tareas con base a algoritmos. Potencia su SOC ya que continuamente obtiene más conocimiento a medida que reúne información de una variedad de fuentes prácticamente infinita, ya sea que los datos se puedan consultar perfectamente en una base de datos o se generen mediante una máquina estructurada) o artículos de revista o medios sociales (no estructurados). La IA puede aprender de los datos de su empresa, o externamente a través de blogs, informes, investigación y alertas de seguridad: desde cualquier lugar y en todas partes. Todos estos elementos separan la IA del aprendizaje automático.

Con la IA en su SOC, tiene acceso a un depósito de memoria institucional que puede proporcionar sugerencias diseñadas específicamente para su organización. La IA le permite equilibrar sus operaciones y soluciones de seguridad, por lo que es importante comprender si está comprando una verdadera solución de IA.



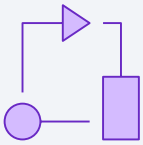
06

¿Qué avances en la postura de seguridad puedo esperar con la IA?



Encadene diferentes incidentes potenciales de forma automática.

La IA se destaca en la automatización e integración del análisis de la causa raíz. La IA detecta conexiones para conocer las amenazas y los riesgos, y no se fatiga. La IA muestra las interrelaciones que su personal puede estar pasando por alto debido a la rotación, la falta de experiencia o el paso del tiempo. Sin la IA, los analistas inexpertos podrían cerrar una alerta pensando que era una instancia única de un ataque. Encuentra puntos en común entre incidentes utilizando el razonamiento cognitivo y proporciona comentarios procesables con contexto, ya sea que los puntos en común sean de un ticket cerrado ayer o meses antes. La IA recopila información sobre amenazas externas para ayudarlo a agregar más contexto a su análisis y detectar lo que otros pueden pasar por alto.

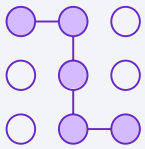


Soluciona los problemas de su personal.

La IA determina el análisis de causa fundamental y puede organizar los siguientes pasos en función del conocimiento que ha creado sobre las amenazas y su organización. No se toma vacaciones. Nunca lo deja por otro empleo. Y no debe preocuparse por reconocer un IOC significativo.

Realiza investigaciones consistentes y más profundas, todo el tiempo.

La IA puede leer tanto datos estructurados como no estructurados, más de lo humanamente posibles de leer. Aprende. Le brinda la información que necesita para reducir el tiempo promedio hasta la detección y el tiempo promedio hasta la respuesta (MTTD y MTTR, por sus siglas en inglés), con un proceso de escalación más rápido y decisivo. La IA puede ofrecerle análisis avanzados para detectar las amenazas conocidas y desconocidas. La IA ofrece investigaciones consistentes y más profundas, en todo momento, y le da el poder a sus analistas de tomar una decisión impulsada por los datos en lugar de confiar en sus instintos.



Cuenta con un flujo de trabajo sólido y automatizado de respuesta a incidentes (RI) que abarca personal, proceso y tecnología.

La IA guía a los analistas de seguridad por una respuesta rápida y completa impulsada por los datos y la evidencia. Automatiza el flujo de trabajo y la resolución de problemas. Permite que el SOC evalúe y perfeccione sus procesos de RI, de manera continua.

07

¿Cómo hace la IA para mejorar el SOC antes, durante y después de un ataque?

Antes, durante y después de una violación de datos, la IA permite que su SOC esté mejor preparado y se recupere de manera más rápida. IBM® QRadar® Security Intelligence Platform toma esta tecnología y la integra a su SOC a fin de proporcionar una solución analítica integral; todo en una sola plataforma.

Antes de un ataque	Durante un ataque	Después de un ataque
IBM® QRadar® SIEM proporciona una visibilidad completa e identifica las amenazas y las anomalías al inicio del ciclo de ataques.	IBM QRadar SIEM recopila continuamente evidencia en curso, y proporciona así un acceso fácil a los datos forenses. Establece una prioridad en función del impacto del negocio.	IBM QRadar SIEM ajusta continuamente los mecanismos de detección en función de las lecciones aprendidas.
IBM QRadar Advisor with Watson™ Investiga de manera automática todas las anomalías e identifica las conductas de ataque de alto riesgo.	IBM QRadar Advisor con Watson multiplica la fuerza de su equipo con un análisis automatizado de causa fundamental y le ayuda a comprender el alcance completo de la amenaza.	IBM QRadar Advisor with Watson adapta los modelos para responder con mayor precisión a futuras amenazas.
IBM Resilient® permite que los SOC preparen flujos de trabajo de RI sólidos y automatizados que abarquen al personal, al proceso y a la tecnología.	IBM Resilient guía a los analistas de seguridad por una respuesta rápida y completa y automatiza el flujo de trabajo y la solución de incidentes.	IBM Resilient permite que los SOC evalúen y perfeccionen de manera continua los procesos de RI.

Acerca de IBM QRadar Advisor with Watson

Con la IA, puede optimizar sus operaciones de SOC al mismo tiempo que frustra exitosamente las amenazas cibernéticas en constante crecimiento. IBM QRadar Advisor with Watson automatiza las tareas SOC de rutina, encuentra semejanzas entre las investigaciones y proporciona retroalimentación accionable para los analistas, lo que los libera para centrarse en elementos más importantes de la investigación y mejorar la eficiencia.

Más información →

Referencias

El estado de las carreras profesionales de seguridad cibernética, ESG