La perspectiva de un CISO sobre IA

Por Harold Rivas*

Muchos de los líderes en ciberseguridad con los que platico, expresan una mezcla de incertidumbre y entusiasmo por las nuevas capacidades de IA generativa (GenAI). Estamos pensando en cómo la IA afecta nuestra capacidad para proteger nuestras organizaciones y cómo podemos adelantarnos a los riesgos que plantea. Al mismo tiempo, esperamos utilizarlo para ser más adaptables y más rápidos a la hora de detectar y remediar amenazas. A medida que comenzamos el año 2024, esta es mi opinión sobre dónde los directores de Información y Seguridad (CISO) verán mayores amenazas (y oportunidades) de la IA.

La IA permite nuevas ciber amenazas

Proteger a una organización de una amplia gama de amenazas nunca ha sido tan desafiante. Los ciberdelincuentes pueden utilizar la IA para ocultar códigos maliciosos, crear malware capaz de imitar sistemas confiables y redactar correos electrónicos de phishing convincentes.

Y ya hemos visto a atacantes utilizar pruebas de penetración de IA. Todo lo que los ciberdelincuentes tienen que hacer es crear el mensaje correcto, utilizando la herramienta que elijan, para penetrar un sistema.

En esencia, la ciberseguridad se ha convertido en una carrera armamentista en la que los atacantes aprovechan la IA para superar los mecanismos de defensa tradicionales. El gran volumen de amenazas potenciales y la velocidad a la que evolucionan hacen imposible que los operadores humanos, por sí solos, puedan seguir el ritmo.

GenAI también puede aumentar el riesgo de amenazas internas. Los empleados que utilizan ChatGPT pueden filtrar inadvertidamente información confidencial fuera de la organización. Incluso si estas acciones no son maliciosas, pueden causar daños importantes.

Cómo los CISO pueden integrar GenAI en su postura de ciberseguridad

Como CISO, debemos informar a nuestras partes interesadas sobre los riesgos de los ataques asistidos por IA y ayudarlos a comprender lo desafiante que se ha vuelto esto.

Un punto importante que podemos destacar es que el ritmo de los ataques se está acelerando. A medida que los atacantes operan más rápido, los defensores tienen que operar aún más rápido, lo que significa utilizar IA para actividades defensivas. GenAI puede ser un poderoso aliado para recopilar información crítica rápidamente. Por ejemplo, disfruto usando Grok de X para aprender en tiempo real lo que el mundo publica sobre las últimas vulnerabilidades de día cero o las amenazas recién descubiertas.

Como CISO, podemos utilizar la IA para ayudar a nuestras organizaciones a pasar de un enfoque reactivo a uno más adaptativo y basado en riesgos. La IA puede ayudar a conectar los puntos para que pueda pasar de un mar de datos sobre indicadores de compromiso (IOC) a aplicar inteligencia contextual. Con un poco de personalización, podrá comprender mejor a quién quiere atacar a su organización, sus técnicas y los indicadores que le ayudan

a demostrarlo. Esta inteligencia brinda a los CISO información valiosa que puede ayudarlo a fortalecer aún más las defensas de su organización y guiar sus conversaciones con otros ejecutivos.

Usando IA para pasar de reactivo a adaptativo

Como Cliente Cero de la tecnología Trellix, puedo probar nuestras últimas innovaciones. Y tenemos algunos desarrollos nuevos e interesantes con la IA. Por ejemplo, nuestro reciente anuncio de Trellix GenAI, construido en Amazon Bedrock, ayudará a los equipos de SecOps a acelerar más rápidamente desde la detección hasta la investigación y la respuesta, y ayudará a los analistas de seguridad restringidos a ser más eficientes.

Normalmente los CISO no suelen participar directamente en el combate cibernético diario, pero podemos utilizar la IA para comprender las mayores amenazas a nuestras organizaciones y abordar los principales desafíos que enfrentan nuestros equipos.

Aquí algunos ejemplos de cómo puede hacerse:

Aceleración de *insights*: la IA reduce el tiempo de análisis de datos al ayudar a formular consultas más enfocadas y relevantes. Los CISO pueden tomar decisiones más rápidas y precisas basadas en datos, lo cual es crucial en un panorama de amenazas que evoluciona rápidamente.

Correlación de información: la IA puede correlacionar datos de múltiples fuentes con la información interna de una organización, destacando posibles vulnerabilidades y debilidades. Por ejemplo, si una organización similar experimenta una brecha debido a una vulnerabilidad particular, la IA puede señalarla para recibir atención inmediata, lo que permite una mitigación más estratégica.

Aumento de los esfuerzos humanos: la IA actúa como un analista de seguridad vigilante las 24 horas del día, los 7 días de la semana, monitoreando continuamente una organización en busca de signos de actividad maliciosa y tomando medidas proactivas. Podemos utilizar investigaciones guiadas por IA para acelerar las respuestas, reducir la carga de trabajo de los analistas y, esencialmente, ayudar a un analista de SOC junior a ser 10 veces más eficaz, apoyándolo y brindándole el contexto y el color que son fundamentales para su capacidad de respuesta. La IA también puede desarrollar rápidamente manuales de respuesta, lo que lleva a una disminución general de las acciones de mitigación y orquestación, aumentando al mismo tiempo la madurez de la seguridad.

La IA en ciberseguridad es un arma de doble filo. Tiene un inmenso potencial para fortalecer nuestras posturas de seguridad, pero los ciberdelincuentes también pueden utilizarlo en nuestra contra. Los CISO deberían planificar de forma proactiva el papel de la IA en la estrategia de seguridad de su organización lo antes posible.

Obtenga más información en el seminario web "**Conectando los puntos y aprovechando la IA: cómo pasar de operaciones de seguridad reactivas a operaciones de seguridad adaptativas**", disponible el 31 de enero en América, Europa, Medio Oriente y África y Asia-Pacífico y Japón.

---

*Harold Rivas dirige las iniciativas globales de Trellix en seguridad y cumplimiento, permitiendo a la compañía protegerse mejor contra las amenazas, gestionar sus necesidades de cumplimiento y riesgos de terceros, así como implementar las mejores prácticas de la industria. Harold tiene más de dos décadas en ciberseguridad, antes de llegar a Trellix fue CISO en loanDepot y antes lo fue para varias empresas, incluyendo Santander Consumer y Fujitsu America. También dirige programas de ciberseguridad en Citigroup. Tiene una licenciatura en Ciencia de Administración de Empresas, Maestría en Administración de Empresas y mantiene varias certificaciones de la industria, incluyendo Profesional Certificado en Sistemas de Seguridad en la Información (CISSP). También es conferencista y miembro de la InfraGard del Buró Federal de Investigaciones (FBI).