LITORALPRESS

Fecha: 14-07-2025
Medio: Revista Nueva Minería & Energía
Supl. : Revista Nueva Minería & Energía
Tipo: Columnas de Opinión
Título: COLUMNAS DE OPINIÓN: CÓMO LA IA CAMBIARÁ LA CIBERSEGURIDAD

Pág. : 20
Cm2: 394,4
VPE: $ 805.777

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

OPINIÓN

CÓMO LA IA CAMBIARÁ LA CIBERSEGURIDAD

Por Cristián Ojeda,
gerente general de Nubatech.

Foto: Nubatech

> En Chile, las mineras han comprendido los riesgos y han adoptado mayores capacidades y estrategias colaborativas, que podrían ser mejoradas con la misma arma que muchos entes maliciosos utilizan para explotar sus vulnerabilidades: la **inteligencia artificial.**

La incorporación de inteligencia artificial, la automatización de procesos, la operación a distancia y de tecnologías como IoT/OT en la industria minera han sido claves para mejorar su producción y competitividad, aportando eficiencia en sus operaciones y optimizando la toma de decisiones.

Todas estas ventajas vienen acompañadas del riesgo que conlleva aumentar la superficie de ataque en el mundo digital, transformando a estas empresas y a su cadena de suministro en un objetivo cada vez más apetecido por el ciberdelito.

En Chile, las mineras han comprendido los riesgos y han adoptado mayores capacidades y estrategias colaborativas, que podrían ser mejoradas con la misma arma que muchos entes maliciosos utilizan para explotar sus vulnerabilidades: la inteligencia artificial.

Así como hoy esta tecnología se está utilizando para automatizar procesos, gestionar datos, buscar minerales, hacer mantenimientos predictivos y optimizar la cadena de suministro, también puede ser aplicada en el área de ciberseguridad, debido a su alta capacidad de procesar información, correlacionar incidentes y predecir escenarios.

Para usar una analogía, pensemos en un fenómeno relacionado con la realidad sísmica de nuestro país. Todos conocemos relativamente bien lo que es un enjambre sísmico, que es cuando se registran varios temblores consecutivos de baja magnitud en un área determinada, y la mayoría de la gente tiende a pensar que es la anticipación de un evento sísmico más fuerte.

Con las amenazas cibernéticas, esta predicción casi siempre se cumple, porque antes de realizar un ataque, los ciberdelincuentes primero hacen pruebas de concepto, es decir, realizan simulaciones para asegurarse de que su estrategia va a tener éxito, lo que genera un enjambre de actividad en torno al epicentro, es decir, a su objetivo.

La única forma de adelantar estas amenazas es con inteligencia artificial, ya que un especialista o incluso un equipo de analistas no tiene la capacidad o velocidad para monitorear la red y dar una alerta oportuna.

La IA escanea en minutos toda la red a nivel mundial y detecta estos enjambres de actividad maliciosa. Luego analiza esa información, donde hay mucho ruido de fondo, separando los datos fiables de los falsos e identifica el epicentro que puede ser, por ejemplo, una minera o un proveedor en su cadena de suministro. Automáticamente, actúa para bloquear o mitigar en tiempo real las amenazas emergentes, antes que ocurra el ataque.

Esta capacidad, que solo ofrece la inteligencia artificial, podría hacer una gran diferencia en un sector crítico como la minería, para avanzar desde un enfoque reactivo a uno proactivo. Además, permitiría a la industria compartir oportunamente información valiosa sobre amenazas y vulnerabilidades, para que otras empresas bloqueen preventivamente el tráfico de red malicioso antes de que pueda causar daños, salvaguardando colaborativamente la integridad de sus cadenas de suministro y garantizando el buen funcionamiento de sus líneas de producción.