EL MERCURIO

Fecha: 03/10/2024 Audiencia: 320.543 Sección: CONTRAPORTADA
Vpe: $6.382.719 Tirada: 126.654 Frecuencia: 0
Vpe pág: $20.570.976 Difusión: 126.654
Vpe portada: $20.570.976 Ocupación: 31,03%

DE ALCANCE GLOBAL:

Los proyectos de inteligencia artificial que destacan en ciberseguridad

Aunque se trata de un rubro en constante evolución, ya existen algunas aplicaciones y proyectos clave para que las empresas aprovechen las ventajas del uso de esta tecnología en herramientas proactivas y automatizadas de prevención y respuesta a amenazas.

Como en muchos ámbitos, el de la ciberseguridad se ha visto fuertemente impactado por el desarrollo y auge de la inteligencia artificial (IA), al permitir una detección automática, proactiva y en tiempo real de ataques, ofreciendo respuestas inmediatas y adaptativas a los incidentes y prediciendo amenazas emergentes al identificar patrones, entre otras ventajas.

Pese a que es un rubro que evoluciona minuto a minuto, ya han comenzado a surgir *rankings* con los mejores proyectos o aplicaciones de IA en ciberseguridad.

LOS MÁS RELEVANTES

Patricio Cofré, socio de Consultoría en Inteligencia Artificial y Datos de EY Chile, estima que los más destacados son "los sistemas de detección de intrusiones basados en IA, que utilizan algoritmos de aprendizaje automático para monitorizar el tráfico de red y detectar comportamientos anómalos". Son efectivos en identificar amenazas desconocidas y reducir falsos positivos, "aunque pueden requerir grandes cantidades de datos y ser vulnerables a ataques", añade.

Otros proyectos clave buscan autenticar y prevenir fraudes impulsados por IA, analizando el comportamiento de los usuarios para detectar accesos sospechosos en tiempo real, pero "pueden ser costosos y necesitar ajustes para evitar bloquear a usuarios legítimos", dice.

Finalmente, menciona las plataformas de respuesta automatizada a incidentes (SOAR con IA), que combinan IA y automatización para reaccionar en "forma eficiente, lo que permite a los equipos de seguridad centrarse en tareas estratégicas; sin embargo, su implementación puede ser compleja y requiere configuraciones detalladas para minimizar falsas alarmas", afirma.

Sebastián Ávila, jefe CSIRT de ITQ Latam, destaca la plataforma en la nube CrowdStrike, que combina IA con análisis de comportamientos para prevenir y accionar ante archivos maliciosos, actuaciones anómalas y ataques. Su mayor ventaja es la rapidez de respuesta, "dando una amplia visibilidad de amenazas gracias a su enfoque de inteligencia de amenazas". Sin embargo, su costo es alto comparado con otras soluciones y depende de "una conexión a internet constante para que los equipos se mantengan actualizados y protegidos".

En segundo lugar, resalta a Darktrace, que también utiliza la IA para detectar y responder a amenazas en tiempo real, con la ventaja de aprender el comportamiento normal de la red y detectar anomalías sin intervención humana. Un inconveniente sería la generación de falsos positivos, lo que requiere supervisión adicional.

Y en tercer término, Ávila ubica a IBM Watson, por su capacidad de analizar grandes volúmenes de datos y detectar amenazas. "Su desventaja es que requiere tiempo para su implementación y puede ser complejo de manejar a nivel de usuarios sin experiencia", explica.

PIXABAY

Cada compañía debe elegir la solución que más se adapte a su realidad y necesidades, considerando factores como costos, facilidad de uso y capacitaciones requeridas, entre otros.

SOLUCIONES *AD HOC*

Cada empresa debe elegir estas soluciones según su propia realidad y necesidades. Sebastián Ávila, de ITQ Latam, enumera cuatro consideraciones prioritarias: compatibilidad y escalabilidad respecto a las políticas y crecimiento de la empresa; costo versus beneficios; facilidad de uso, considerando la capacitación necesaria para el personal, y reputación del proveedor, de acuerdo a su experiencia y trayectoria en ciberseguridad.

Patricio Cofré, de EY, subraya que se debe evaluar la capacidad de integración armónica con los sistemas y herramientas de seguridad existentes; "revisar la calidad de los modelos de IA, su capacidad de entrenarse con datos relevantes y actualizarse continuamente para mantener la precisión en la detección de amenazas"; la facilidad de uso y el nivel de automatización, "ya que las soluciones deben ser intuitivas y reducir la carga operativa de los equipos de TI", y finalmente, "que la solución maneje los datos de manera segura, cumpliendo con las regulaciones de privacidad para proteger la información sensible de la empresa", puntualiza.