

“La inteligencia artificial no inventa el ciberdelito pero lo industrializa”

Carles Flamerich CEO de Apolo Cybersecurity

La tecnología es una pieza crítica para cualquier organización. Fábricas, cadenas logísticas, dispositivos y proveedores forman ecosistemas más conectados y expuestos. Apolo Cybersecurity plantea que la respuesta debe ir más allá de prevenir: hay que comprender las amenazas, reaccionar con rapidez y garantizar que la empresa siga operando. “La ciberseguridad es continuidad de negocio, reputación, competitividad y confianza”, resume Carles Flamerich, CEO de Apolo Cybersecurity.

¿Estamos realmente ante un aumento del riesgo de ciberseguridad o existe también cierto alarmismo?

Estamos ante un aumento real. Crece el número de ataques y cambian su capacidad, velocidad y sofisticación. En la industria, la dependencia tecnológica incluye fábricas, sensores, maquinaria conectada, IoT, sistemas OT, cloud y cadenas de suministro.

Por ello, un ciberataque ya no supone únicamente el riesgo de perder información. Puede detener una empresa, paralizar una planta o interrumpir una cadena logística. La superficie de ataque crece más rápidamente que nuestra capacidad humana para vigilarla.

¿Qué está cambiando la inteligencia artificial en manos de los ciberdelincuentes?

Está reduciendo las barreras de entrada. Los atacantes no son necesariamente mejores, pero pueden operar con mucha más rapidez, productividad y escala.

La IA permite automatizar el reconocimiento, elaborar campañas de phishing convincentes y personalizadas, traducir mensajes, crear voces o imágenes falsas, analizar vulnerabilidades

e incluso ayudar a generar código malicioso. Antes, preparar un engaño sofisticado exigía tiempo y conocimientos; hoy una parte importante puede automatizarse. La inteligencia artificial no inventa el ciberdelito, pero lo industrializa.

Pero la inteligencia artificial también puede reforzar la defensa. ¿Cómo cambia el trabajo de un SOC?

Una empresa genera millones de eventos que ningún equipo humano puede analizar en tiempo real. La IA permite correlacionar información, detectar comportamientos anómalos, reducir falsos positivos, priorizar alertas y proporcionar contexto al especialista.

El SOC tradicional se basaba principalmente en reglas y alertas. Ahora debe evolucionar hacia un sistema capaz de comprender mejor qué ocurre y ayudar a decidir qué hacer. La IA automatiza el trabajo repetitivo para que los especialistas puedan investigar, interpretar el contexto y tomar decisiones.

¿Qué diferencia el modelo que está desarrollando Apolo Cybersecurity?

Nuestro modelo combina inteligencia artificial, contexto y talento humano. La tecnología procesa millones de señales, pero lo importante es el equipo que las interpreta y decide cómo actuar.

También resulta esencial la convergencia entre IT, IoT y OT.



Muchas organizaciones utilizan soluciones distintas para proteger ordenadores, servidores, dispositivos conectados e instalaciones industriales, pero la amenaza no respeta esas fronteras. Un atacante puede entrar por un ordenador corporativo y terminar afectando a una fábrica. El atacante no distingue entre IT, IoT y OT; la defensa tampoco debería hacerlo.

¿Por qué preocupa especialmente la ciberseguridad industrial?

Industria 4.0 conecta fábricas, máquinas, robots, sensores y sistemas logísticos. Mejora la productividad, pero crea nuevas superficies de ataque. Muchos sistemas industriales fueron diseñados para ofrecer disponibilidad y durabilidad, no para permanecer conectados.

Ahora IT y OT convergen. Por eso, la ciberseguridad debe incorporarse desde el diseño de cualquier proceso de transforma-

ción industrial y no añadirse al final como una capa adicional. Estamos digitalizando el mundo físico y un incidente puede tener consecuencias operativas.

¿Cómo pueden afrontar este escenario las empresas medianas?

Es difícil que una compañía mediana disponga internamente de todos los especialistas y tecnologías necesarios para mantener una vigilancia permanente. Ahí está el valor de los servicios gestionados y los SOC compartidos: hacer accesibles capacidades avanzadas que antes estaban reservadas a grandes corporaciones.

La regulación europea aumenta las obligaciones, pero la ciberseguridad no debería contemplarse únicamente como cumplimiento normativo. Cumplir es importante; mantener funcionando el negocio lo es todavía más.

“El atacante no distingue entre IT, IoT y OT; la defensa tampoco debería hacerlo.”

“DFactory nos permite estar donde se está creando la industria que tendremos que proteger mañana.”

¿Qué aporta a Apolo formar parte del ecosistema de DFactory Barcelona?

Nos permite estar cerca de donde se diseña la nueva industria: automatización, robótica, IoT y fabricación avanzada. Estamos muy satisfechos de formar parte de un entorno donde empresas tecnológicas e industriales comparten conocimiento y proyectos.

Para Apolo es una oportunidad para comprender mejor los riesgos reales e incorporar la ciberseguridad desde el diseño. DFactory nos permite estar donde se está creando la industria que tendremos que proteger mañana.

¿Qué deberían hacer hoy las empresas para prepararse para las amenazas de los próximos años?

Primero, asumir que no podremos impedir todos los ataques y evolucionar desde una cultura exclusivamente preventiva hacia otra basada también en la resiliencia. La pregunta es cuánto tardaremos en detectar un incidente, reaccionar y volver a operar.

Hay cinco elementos básicos: conocer los activos y dependencias; proteger las identidades; disponer de monitorización y respuesta continua; incorporar inteligencia para anticiparse y priorizar amenazas; y practicar la respuesta ante incidentes. Un plan de crisis que nunca se ha probado es solamente un documento.

“Lo verdaderamente importante es el equipo que interpreta la tecnología y decide cómo actuar.”

