Contacto de prensa:
Pablo Bou Guirola
Tel: +52 55 5980 3665
Celular: (044) (55) 35236064
E Mail: Pablo.bou@pprww.com

69% de las empresas consideran que no serán capaces de responder a las amenazas en ciberseguridad sin ayuda de Inteligencia Artificial

Para 2020 dos de cada tres organizaciones planean establecer IA para reforzar sus sistemas de defensa.

París, Julio, 2019 – las empresas están acelerando el paso en su inversión en Inteligencia Artificial (IA) para defenderse ante la nueva generación de ciberataques, de acuerdo con un nuevo estudio realizado por el Instituto de Investigación de Capgemini. Dos terceras partes de las compañías (69%) reconocen que no serán capaces de responder a las amenazas críticas sin IA. Con el número de dispositivos de usuario final, las redes y las interfaces de usuario creciendo como resultado de los avances en la Nube, Internet de las Cosas (IoT[1]), 5G y tecnologías de la interfaz conversacional, las compañías enfrentan la urgente necesidad de aumentar y mejorar continuamente su ciberseguridad.

El estudio "Reinventando la ciberseguridad con Inteligencia Artificial: la nueva frontera en seguridad digital" encuestó a 850 ejecutivos senior de TI en seguridad de la información, ciberseguridad y operaciones TI en 10 países y siete sectores de negocios, así como también realizó entrevistas a profundidad a expertos de la industria, startups de ciberseguridad y académicos.

El estudio reveló lo siguiente:

La ciberseguridad basada en la IA es indispensable: cerca de la mitad (56%) de los ejecutivos dijeron que sus analistas de ciberseguridad se ven abrumados por la gran cantidad de datos que tienen que monitorear para detectar y prevenir intrusiones. Además, el tipo de ciberataques que requieren atención inmediata o que no pueden ser resueltos lo suficientemente rápido por los analistas, han incrementado notablemente, incluyendo:

- Ciberataques que afectan las aplicaciones sensibles al tiempo (42% dice que ha aumentado en un promedio de 16%).
- Ataques automatizados a una velocidad que solo una máquina puede alcanzar y que mutan a un ritmo que no se pueden neutralizar con sistemas de respuesta tradicionales (43% reportó un incremento de 15% en promedio).

Ante las nuevas amenazas, la mayoría de las compañías (69%) creen que no serán capaces de responder a los ciberataques sin el uso de IA, mientras que el 61% dijo que requieren IA para identificar las amenazas críticas. Uno de cada cinco ejecutivos experimentó una violación de ciberseguridad en 2018, de las cuales al 20% le costó a su organización más de $50 millones de dólares.

[1] *IoT – internet de las cosas*

Los ejecutivos aceleran la inversión en ciberseguridad con IA: la mayoría de los ejecutivos reconocen que la IA es fundamental para el futuro de la ciberseguridad.

- El 64% dice que reduce los costos en la detección de las brechas de seguridad y resolverlas, en un promedio de 12%.
- 74% dice que permite brindar una respuesta rápida: reduce el tiempo que toma detectar amenazas, resolver la fractura e implementar parches en un 12%.
- 69% dijo que la AI mejora la precisión para detectar brechas, y 60% dijo que incrementa la eficiencia de los analistas en ciberseguridad, reduce el tiempo que gastan analizando falsas amenazas y mejora la productividad.

En consecuencia, casi la mitad (48%) dijo que los presupuestos para ciberseguridad en IA van a incrementar en 2020 en casi un tercio (29%). En términos de despliegue, 73% están probando casos de uso para IA en ciberseguridad. Solo una de cinco organizaciones utiliza IA desde antes de 2019, pero se espera una mayor adopción: casi dos de tres organizaciones (63%) planean implementar IA para reforzar su defensa.

"*Las ofertas de IA son una gran oportunidad para la ciberseguridad*" dijo Oliver Scherer, Director de Seguridad de la Información de Grupo MediaMarktSaturn Retail, líder europeo en distribución minorista en electrónica de consumo. *"Esto es porque te permite pasar de la detección, reacción y solución manual a un sistema automático de reparación, algo que las organizaciones quisieran alcanzar en los próximos tres a cinco años".*

Sin embargo, existen barreras para la implementación de IA a escala: el mayor reto para integrar ciberseguridad en IA es la falta de entendimiento de cómo transformar las pruebas de concepto a un despliegue completo en todos los niveles de la organización. 69% de los encuestados admite tener dificultades en esta área.

Gert Van der Linden, responsable del área de ciberseguridad en Grupo Capgemini dijo que "*Las organizaciones se enfrentan a un volumen incomparable y complejo de ciber-amenazas y se han dado cuenta de la importancia de la IA como primera línea de defensa. Los analistas de seguridad están agobiados, cerca de una cuarta parte de ellos declararon no ser capaces de investigar exitosamente todos los incidentes identificados, por lo que es importante que las organizaciones incrementen la inversión y el enfoque en los beneficios que IA puede otorgar al negocio en términos de refuerzo en la ciberseguridad".*

Además, la mitad de las empresas encuestadas señalaron los retos de la integración con su infraestructura, sistemas de datos y contexto de aplicaciones actuales. Aunque la mayoría de los directivos contestaron que saben lo que quieren alcanzar con la ciberseguridad basada en IA, solo la mitad (54%) identificó las series de datos que se requieren para hacer operativos los algoritmos de IA.

Anne-Laure Thieullent, responsable de IA y Analítica de Capgemini concluyó que "*las organizaciones deben dirigir primero sus esfuerzos para resolver los problemas subyacentes de implementación que impiden que la IA alcance todo su potencial de ciberseguridad. Esto significa crear un mapa para eliminar las principales barreras y centrarse en los casos de uso que puedan aplicarse en toda la organización fácilmente y que ofrezcan los mejores resultados. Solo siguiendo estos pasos las empresas estarán preparadas para hacer frente a las amenazas de ciberataque de rápida evolución. De esa forma, ahorrarán dinero y reducirán la probabilidad de una violación devastadora en la seguridad de sus datos".*

El reporte se puede descargar aquí.

Metodología de Investigación

El reporte consultó a 850 ejecutivos senior de niveles directivos y superiores, de siete sectores: productos de consumo, retail, banca, seguros, automotriz y telecom. Una quinta parte de los ejecutivos son CIOs y uno de cada 10 son CISOs[2] en sus respectivas organizaciones. Pertenecen a compañías con sedes en Francia, Alemania, Reino Unido, Estados Unidos, Australia, Países Bajos, India, Italia, España y Suecia. Capgemini también realizó entrevistas a líderes de la industria y académicos, para conocer el estado actual y el impacto de IA en ciberseguridad.

Acerca del Instituto de Investigación de Capgemini

El Instituto de Investigación de Capgemini es el grupo interno de expertos en investigación en todo el ámbito digital. El Instituto publica investigaciones sobre el impacto de las tecnologías digitales en las grandes compañías tradicionales. El equipo se apoya en la red mundial de expertos de Capgemini y trabaja con los socios académicos y tecnológicos. El instituto cuenta con centros de investigación especializados en Estados Unidos, Reino Unido e India. Recientemente ha sido reconocido como líder por la calidad de sus informes por analistas independientes.

Acerca de Capgemini

Líder global en consultoría, servicios de tecnología, y transformación digital, Capgemini está a la cabeza de la innovación para enfrentar las oportunidades de nuestros clientes en el cambiante mundo de la nube, digital y plataformas. Basándose en su sólida herencia de 50 años y profunda experiencia específica de las industrias, Capgemini habilita a las organizaciones a alcanzar sus ambiciones de negocio a través de un conjunto de servicios que van desde la estrategia hasta las operaciones. Capgemini se impulsa por la convicción que el valor de negocio de la tecnología viene de y a través de las personas. Es una compañía multicultural con 200,000 miembros del equipo en más de 40 países. El Grupo reportó ingresos globales de 13.2 miles de millones de Euros en 2018.
Visítanos en www.capgemini.com/mx-es/. *People matter, results count.*

###

[2] CISO - director de seguridad de la información