



SALTO BASE

Manolo, mucho ojo, poca vista y escaso atisbo para ser ‘Domador de IAs’

Decía **Antoine de Saint-Exupéry** que lo “esencial es invisible a los ojos”. Y buen ejemplo de que no se trata de tener vista sino de saber mirar es Manolo. Un prodigio anatómico, que ha paseado por el último congreso de ciberseguridad de Andalucía, con una gigantesca cabeza coronada por un único ojo descomunal... incapaz de dar dos pasos sin caerse sin que alguien le llevara del brazo. El ideal de la visibilidad total... con la movilidad de un bonsái y, seguramente, un perfecto ejemplo de la ciberseguridad esperpéntica que a veces vivimos. Y es que el exceso de visibilidad, sin criterio, se ha convertido en una forma sofisticada de ceguera. Así se ha evidenciado en la última edición de



Muchas organizaciones están integrando modelos complacientes en procesos críticos sin tener muy claro si compensa el riesgo asumido

Espacio TiSEC, donde la observabilidad, la de verdad, se considera más que una cuestión técnica “un motivo de supervivencia” fruto de una verdad incómoda: vemos más que nunca, pero, posiblemente, entendemos menos que siempre. Y en este festival de ciberfuegos artificiales la IA se alza como hidra poderosa. O mejor dicho, *las IA*. Bajo el ‘bálsamo de fierabrás’ que tanto se oye prometiendo automatizarlo todo surge el apocalipsis de desplegar todo tipo de sistemas sin el menor control donde el usuario ha dejado de ser ‘el tonto útil’ tan cacareado durante décadas. El que hace clic donde no debe, el que reutiliza contraseñas, el que confunde urgencia con legitimidad. Un relato que ha permitido mantener intacta la fe en arquitecturas, productos y procesos considerando que él siempre es el eslabón débil de la cadena.

Ahora, gracias a la IA, muchos incidentes de alto impacto no requieren ni clic, ni error humano. Porque la IA está pensada para complacer y esa que es una de sus virtudes, se torna como una de sus grandes debilidades en ciberseguridad. Buena prueba son los denominados ataques *zero click*, sin intervención alguna de la persona.

El sistema procesa, interpreta y ejecuta sin necesidad del usuario demandando, más que nunca, profesionales que sean capaces de ser ‘Domadores de IA’, como mostré en la última edición de **RootedCON**, en una ponencia muy ilustrativa, junto a la siempre incisiva **Carmen Torrano**, sobre la ciberseguridad que se aplica a los algoritmos de IA antes de salir a producción.

Si algo puede salir mal...

Y, como enunciaba, el ingeniero **Edward A. Murphy Jr.**, en los años 40, “todo lo que pueda ir mal, irá mal”. Buena prueba de ello, es el tan esperado –pero seguramente inexistente– impacto en la ciberseguridad europea de la tan cacareada Directiva NIS2, de obligado cumplimiento desde octubre de 2024, pero aún sin transponer por media docena de países. Una cibertorre de Babel, que la **Comisión** ha querido ‘domar’ proponiendo modificaciones específicas de NIS2 (Directiva (UE) 2022/2555) a través de lo que se denomina ‘*cyber posture*’. Con ellas se busca aumentar la claridad jurídica mediante la simplificación de las normas jurisdiccionales, la agi-

lización de la recopilación de datos sobre ataques de *ransomware* y facilitar la supervisión de las entidades transfronterizas con el papel de coordinación reforzado de Enisa. En definitiva, se aspira a homogeneizar el mosaico de realidades nacionales que ha generado esta directiva, permitiendo certificar una postura. Un cambio notable y toda una declaración de intenciones.

La ciberseguridad no necesita ojos más grandes, como el de Manolo, sino miradas más entrenadas. Porque al final, proteger no es vigilarlo todo, sino saber qué no puede fallar. Lo que marca la diferencia no es cuánto vemos, sino cuánto entendemos. Y eso, por desgracia, no se compra con licencias.



José Manuel Vera
Redactor
Revista SIC