EL REVUELO GENERADO EN TORNO A LA INTELIGENCIA ARTIFICIAL, ¿ESTA PONIENDO EN RIESGO LOS NEGOCIOS?

ENJOY SAFER TECHNOLOGY™

Los medios no dejan de hablar sobre los beneficios de la Inteligencia Artificial y el Machine Learning (Aprendizaje Automático) para la seguridad informática. Cada vez más, los proveedores de next-generation acercan productos basados en Inteligencia Artificial al mercado, presentando estas tecnologías como revolucionarias dentro de la industria. Con su habilidad para detectar cualquier tipo de malware en una red de manera instantánea y mitigar los riesgos antes de que éstos ocurran, la estrategia de ventas de éstas se vuelve atractiva para las organizaciones.

Sin embargo, este discurso puede ser engañoso. Y el revuelo generado podría llevar a los negocios a enfrentar mayores riesgos.

En este documento planteamos que, mientras la tecnología de Machine Learning ha probado ser una herramienta poderosa en la detección de malware durante años, la realidad es que la verdadera Inteligencia Artificial aún no existe. Las estrategias de marketing de los proveedores next-gen solo están confundiendo el asunto todavía más para los responsables de IT, que deben construir sistemas de seguridad robustos en tiempos en que el panorama de amenazas se vuelve más precario.

ÍNDICE

Opiniones encontradas

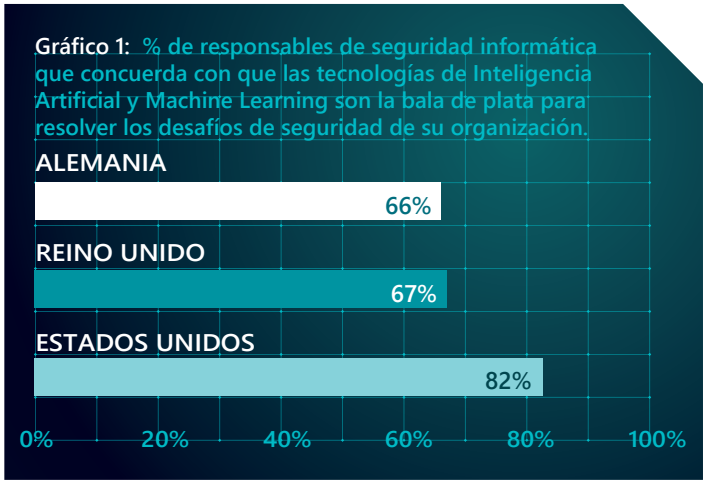
Realizamos una encuesta entre los responsables de seguridad de diversos negocios alrededor de Estados Unidos, Reino Unido y Alemania para conocer sus actitudes y abordaje de la Inteligencia Artificial y Machine Learning aplicados a la ciberseguridad, y está claro que son muchas las confusiones y opiniones encontradas.

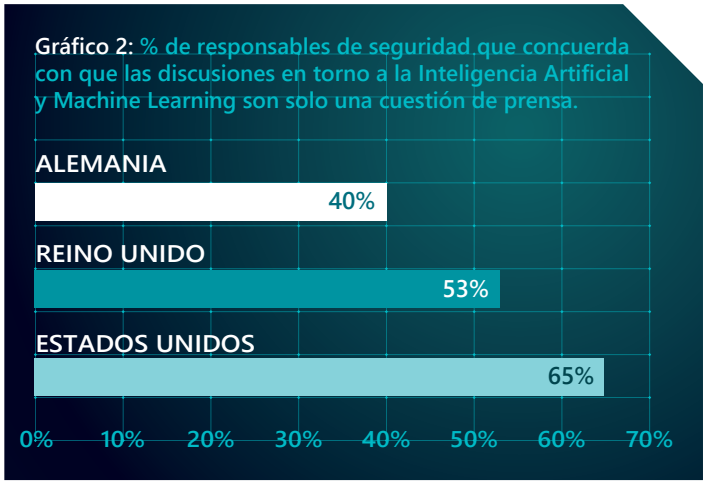
Mientras que un alto porcentaje de encuestados considera a estas tecnologías como la "bala de plata" para resolver los desafíos de seguridad de sus organizaciones, un alto número también opina que las discusiones en torno a ella no son más que una exageración. Los responsables de seguridad estadounidenses se apoyaron más sobre la idea de que esta tecnología es, efectivamente, la bala de plata para sus defensas digitales, con un 82% de acuerdo en que ellas resolverán los desafíos de seguridad informática, mientras que en Alemania éstos representaban un 66% (ver figura 1).

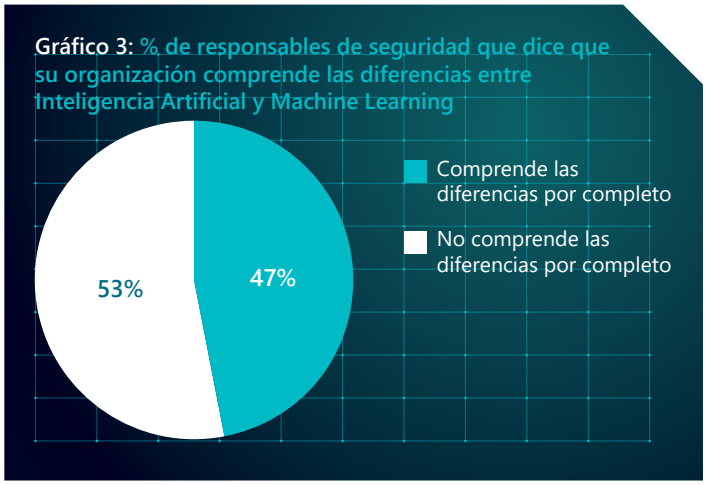
Aun así, también fueron los estadounidenses quienes mayor porcentaje registraron (65%) a la hora de considerar las discusiones en torno a la Inteligencia Artificial y Machine Learning como una cuestión de "bombo" – en comparación con el 53% del Reino Unido y el 40% de los encuestados en Alemania (ver figura 2).

¿Saben realmente los responsables de seguridad IT en qué creer?

Existe, además, una confusión sobre la terminología utilizada, ya que solo el 53% de quienes toman las decisiones dijo que su compañía comprende por completo las diferencias entre ambos términos (ver figura 3).





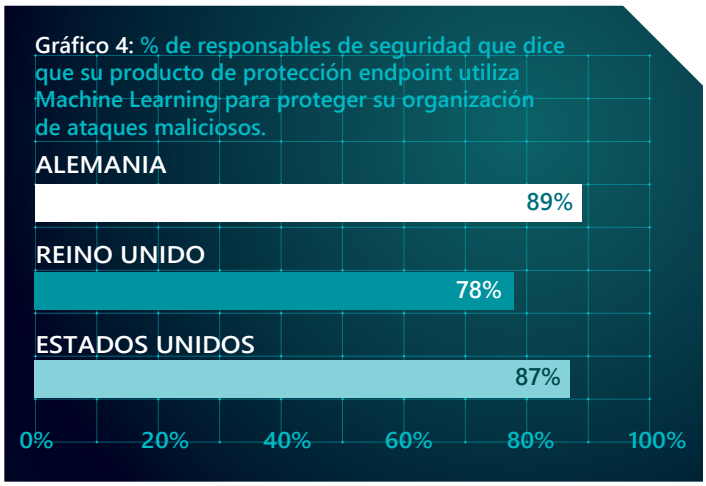


Nada nuevo

Desafortunadamente, la terminología utilizada, tanto en las actuales piezas de marketing como en los medios, suele ser confusa. En muchos casos, el término Machine Learning se cambia por el de Inteligencia Artificial erróneamente. En síntesis, la Inteligencia Artificial se da cuando las máquinas llevan a cabo tareas sin estar previamente programadas o entrenadas. En cambio, el Machine Learning depende del entrenamiento de computadoras, por medio de algoritmos, para hallar patrones entre grandes cantidades de información e identificar datos en base a reglas y a información que ya tienen. El Aprendizaje Automático no es nada nuevo; ha estado presente en la seguridad informática desde los '90.

Además, la mayoría de los responsables de seguridad encuestados ya ha implementado Machine Learningdentro de sus estrategias de seguridad, con un 89% de respuestas de Alemania, un 87% de Estados Unidos y un 78% del Reino Unido que afirman que sus productos de protección endpoint utilizan Aprendizaje Automático para proteger sus organizaciones de ataques maliciosos.

Se necesita de mayor claridad respecto a las declaraciones que están haciendo los equipos de marketing de proveedores next-gen. El panorama de amenazas se está convirtiendo en uno todavía más complejo para navegar, a medida que los atacantes buscan nuevas maneras de obtener acceso a las redes de la compañía. La conmoción en torno a la Inteligencia Artificial y Machine Learning como la bala de plata para resolver los desafíos que enfrenta la seguridad de la información ensucia el mensaje para aquellos que toman las decisiones claves a la hora de asegurar las redes e información de sus compañías.



Desafortunadamente, la terminología utilizada, tanto en las actuales piezas de marketing como en los medios, suele ser confusa.

El actual estado de las cosas

Es importante saber que la tecnología de Machine Learning es una herramienta poderosa en la guerra contra el cibercrimen, especialmente en el análisis de malware – ayudando a los usuarios en la detección de amenazas potenciales para que puedan mitigarlas proactivamente a mayor velocidad.

Machine Learning refiere a una de las tecnologías incluidas en la solución de seguridad que ha recibido grandes cantidades de muestras correctamente etiquetadas como limpias o maliciosas para poder aprender la diferencias entre el bien y el mal. Gracias a este entrenamiento, es capaz de analizar e identificar la mayoría de las amenazas potenciales y permitirles a los usuarios actuar de forma proactiva para mitigarlas.

Esta capacidad de detectar las amenazas rápidamente y mitigar el elevado número de muestras que emergen cada día es lo que hace a esta tecnología tan atractiva para los responsables de IT.

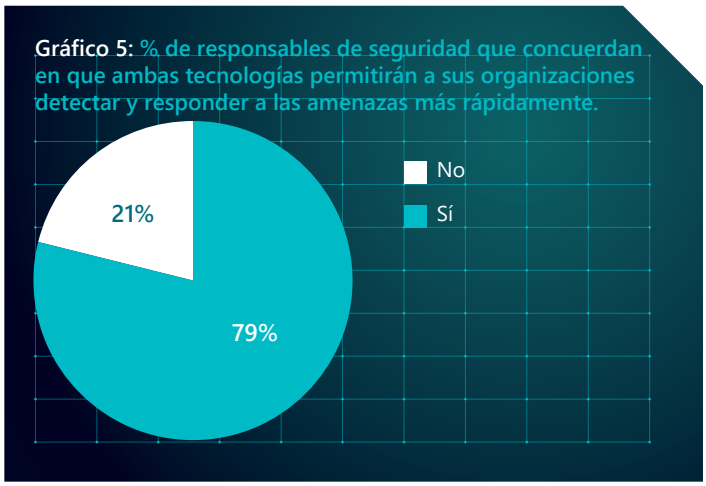
Sin embargo, el Machine Learning– si está bien implementado – viene con problemas y limitaciones que los productos de marketing parecen evadir.

1. Las máquinas requieren de entrenamiento supervisado

Por empezar, para utilizar Machine Learning necesitas de muchos inputs – y cada uno debe estar correctamente etiquetado. En una aplicación de seguridad, esto significa tener un alto número de muestras, divididas en tres grupos – maliciosa, limpia, potencialmente no deseada. En ESET, hemos pasado cerca de tres décadas reuniendo, clasificando y seleccionando data para entrenar a nuestro sistema de Aprendizaje Automático.

Además, aun cuando un algoritmo ha recibido grandes cantidades de información, no hay garantía de que éste pueda identificar correctamente las nuevas muestras que encuentre. La verificación humana sigue siendo necesaria. Sin ella, con solo un input incorrecto puede generarse el efecto de una bola de nieve y, posiblemente, arruinar la solución al punto de generar una falla total.

Hemos oído a algunos proveedores de seguridad next-gen afirmar que situaciones de ese estilo no ocurren con sus algoritmos de Machine Learning, ya que ellos pueden identificar cada una de las muestras antes de que sea ejecutada y determinar si está limpia o es maliciosa, solo haciendo las cuentas necesarias.



Pero una vez más, hay algunas fallas presentes en estas afirmaciones – fallas que simplemente confunden a los responsables de IT.

2. Las matemáticas no son suficiente

La realidad es que, incluso una máquina sin errores, no será capaz de decidir por siempre si un input desconocido, a futuro, lo guiará a comportamiento no deseado . Si un proveedor de next-gen afirma que su algoritmo de Machine Learning puede distinguir cada muestra previo a ejecutarla y decidir si está limpia o es maliciosa, entonces tendría que bloquear una enorme cantidad de ítems indecisos – llenando los departamentos de IT de las compañías con falsos positivos (errores que suceden cuando una solución de seguridad incorrectamente etiqueta como limpia a una muestra maliciosa).

Por supuesto, no todo falso positivo lleva, necesariamente, al colapso de la infraestructura IT de tu negocio. Sin embargo, sí son capaces de interrumpir la continuidad del mismo, y, en consecuencia, ser potencialmente aún más destructivo. Por lo tanto, los sistemas de Machine Learning, necesitan de la ayuda de humanos nuevamente una vez que se cruzan con algo que nunca antes han visto.

El rol humano aquí es crítico. Los sistemas de Aprendizaje Automático necesitan contar con la opción de notificar a los equipos cuando encuentran algo que nunca antes habían visto y pedir la ayuda de un humano.

[1] Conocido como el problema de la parada, probado por el matemático, científico computacional y criptoanalista inglés Alan Turing, que quebró el Código Enigma Nazi durante la Segunda Guerra Mundial.

3. Los atacantes rompen las reglas – no las máquinas

El malware está constantemente en evolución, y los cibercriminales están continuamente aprendiendo. Si quieres proteger tu negocio de intromisiones, debes mantenerte al día. El clásico discurso de ventas de los proveedores next-gen cataloga al Machine Learning como la solución adecuada para preparar a los negocios para la pelea, y el buen manejo de números permite a uno predecir cada movimiento del atacante. Pero, lamentablemente, sin importar qué tan inteligente sea el algoritmo de Aprendizaje Automático, su foco es reducido y, como dijimos, aprende de un grupo de datos y reglas específico.

El hecho es que, por contraste, los atacantes no siguen ninguna regla. Por el contrario, son capaces de modificar el campo de juego por completo sin ningún tipo de advertencia.

Un atacante puede aprender contexto y beneficios con algo de inspiración, lo que ninguna máquina ni algoritmo es capaz de predecir – sin importar qué tan sofisticado pueda ser. Quienes escriben malware son capaces de esconder el verdadero objetivo de su código "ocultándolo" por medio de cifrado o haciéndolo ininteligible.

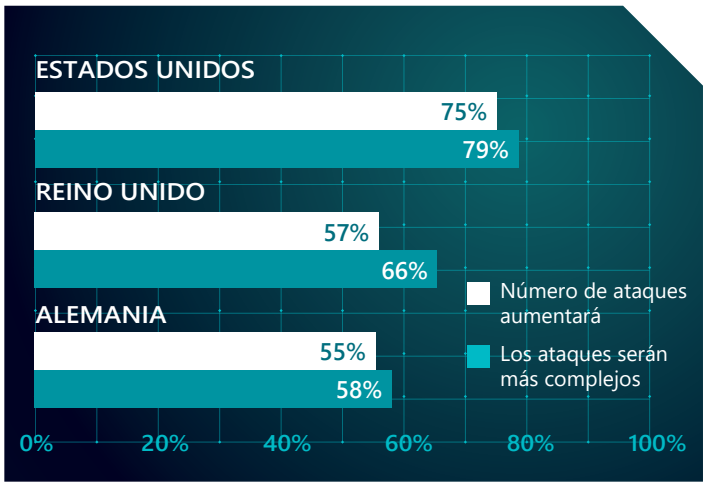
Por ejemplo, un atacante podría esconder código malicioso en los ajustes de pixeles de un archivo de imagen inocente. Podrían también dividir el malware en varias piezas y esconderlo en distintos archivos separados. Cada uno de estos archivos por sí solos parecen estar limpios – solo cuando convergen en un endpoint o red comienzan a demostrar comportamiento malicioso. Si el algoritmo de Machine Learning no es capaz de ver detrás de estas "máscaras", puede tomar una decisión incorrecta, etiquetando un ítem malicioso como limpio – causando una equivocación potencialmente peligrosa.

Por ende, máquina y humano necesitan trabajar en conjunto para prevenir y mitigar actividad maliciosa de forma proactiva.

Los atacantes no siguen ninguna regla. Por el contrario, son capaces de modificar el campo de juego por completo sin ningún tipo de advertencia.

¿Cambian el juego estas tecnologías?

Aun siendo el Machine Learning, con intervención humana, una poderosa herramienta, sin duda alguna, para la estrategia de seguridad de un negocio, los expertos e investigadores advirtieron también sobre las maneras en que los atacantes han comenzado a adoptar técnicas de Machine Learning para mejorar o automatizar actividad maliciosa. Lamentablemente, donde hay un avance tecnológico que permite asistir en la batalla contra el cibercrimen, hay también potencial para uso de los cibercriminales en el uso de estas tecnologías para avanzar con su actividad maliciosa.



En consecuencia, hay una creciente preocupación por parte de los responsables de IT sobre las maneras en que los atacantes usarán la Inteligencia Artificial. Sin embargo, nuestra investigación demuestra que, una vez más, el nivel de preocupación varía en las distintas regiones, lo que nos lleva a preguntar qué tan informados se sienten los responsables de seguridad sobre el riesgo potencial que representan los ataques impulsados por Inteligencia Artificial.

Por ejemplo, los responsables de IT de Estados Unidos están más preocupados por cómo la inteligencia artificial aumentará el número de ataques que deberán detectar y mitigar sus equipos, y tienden a creer que la Inteligencia Artificial hará estos ataques más complejos. En comparación, son menos los responsables de IT en Reino Unido y Alemania que piensan que la Inteligencia Artificial tendrá este impacto en los ataques que enfrenta su organización.

La realidad es que los atacantes podrían hacer uso de Machine Learning para establecer el perfil de sus víctimas antes de realizar el ataque. Esto incluye el análisis del equipo para corroborar si se está utilizando en un ecosistema de virtualización o se ejecuta en sitios tales como la máquina de un analista de malware. Otra pregunta recurrente es si podría aumentar este tipo de ataques en el futuro cercano.

Gracias a la escalabilidad y la creciente eficiencia de los sistemas de Machine Learning – y lógicamente, la Inteligencia Artificial que podría seguirle – puede volverse más sencillo y efectivo realizar ciberataques intensivos. Éstos, incluyen ataques que involucran ingeniería social, como el spearphishing. Al automatizar las tareas más complejas que los atacantes deben llevar a cabo previo a lanzar sus operaciones dirigidas, el futuro uso de Inteligencia Artificial puede, potencialmente, atraer más adversarios, y con menor esfuerzo para conducirlos. Los atacantes podrían también ser capaces de lanzar ataques sofisticados de spearphishing en masa, mientras que la implementación de chatbots realistas haciéndose pasar por "conocidos" puede también añadir nuevas capas a las amenazas.

Además, las mismas vulnerabilidades basadas en sistemas con Machine Learning podrían estar abiertas a ser explotadas. Por ejemplo, esto podría llevarse adelante por medio de contaminación de datos, por el cual los atacantes identifican el modo en que funcionan los algoritmos o la fuente de datos que entrenan al sistema de Aprendizaje Automático, para luego comprometer y manipular esos datos para modificar qué es reconocido como 'bueno' o 'malo'.

Máquina + Humano

El mundo de la ciberseguridad cambia constantemente, lo que hace imposible crear una solución de seguridad universal, basada únicamente en Machine Learning. Con una solución de seguridad basada 100% en esta tecnología, solo se necesitaría de un ataque exitoso por parte de actores maliciosos para que los endpoints de tu compañía queden a disposición de toda una milicia de amenazas cibernéticas.

Es por esto que deben involucrarse otras capas de seguridad, así como humanos, al implementar sistemas de Machine Learning.

En función de mantener los índices de detección elevados y el número de Falsos Positivos bajo, un grupo humano puede estar a cargo de supervisar y evaluar los ítems que se diferencian mucho de otras muestras recibidas, y, en consecuencia, son difíciles de rotular para el sistema.

Gracias al entrenamiento riguroso y la supervisión de humanos, la tecnología de Machine Learning es capaz de analizar datos, hallar patrones e identificar la mayoría de las potenciales amenazas que se presentan a las organizaciones. La automatización de estos procesos acelera la solución de seguridad y ayuda, esencialmente, a tu equipo de seguridad a administrar el creciente número de muestras que se les presentan cada día.

Más allá del revuelo

Aun queriendo creer que existe una ´bala de plata´ para resolver todos nuestros desafíos de seguridad, esto simplemente no es cierto. Independientemente de lo que digan las piezas de marketing, la verdadera Inteligencia Artificial aún no existe, y el Machine Learning no es lo suficientemente maduro para ser la única capa de seguridad que se interpone entre tu máquina y el atacante.

Las exageraciones no hacen más que confundir a los responsables de seguridad, y pueden estar poniendo en riesgo al negocio. En el panorama de negocios actual, sería poco sabio depender únicamente de una tecnología para proteger tu red y tus datos. Es importante que las empresas sepan que el Machine Learning tiene sus limitaciones para entender de qué manera asegurarse que su organización está asegurada como corresponde.

Al construir el sistema de defensa cibernético confiable y robusto, debes comprender cuáles son los desafíos que enfrenta tu negocio, para luego considerar qué soluciones serán más adecuadas para atender tus necesidades específicas. Cada negocio es único, por lo cual una solución universal no resolverá todos los problemas. Soluciones en múltiples capas, combinadas con gente talentosa y experimentada, serán la única combinación eficiente para mantenerte un paso delante de los atacantes, a medida que evoluciona el panorama de amenazas.

Si la última década nos ha enseñado algo, es que aquello que encontramos en el ciberespacio no tiene una solución sencilla – los cambios llegan rápido y el campo de juego puede cambiar en pocos minutos. En lugar de ver estas tecnologías como la solución mágica, mira más allá del bullicio y enfócate en aquello que realmente será útil para tu negocio; ¿dónde están los puntos más vulnerables y cómo puedes asegurarte que éstos no actúen como backdoors para los actores maliciosos? ¿Sabes dónde reside la información más sensible y cómo te estás asegurando que está protegida?

La tecnología de Machine Learning, por sí sola, no es la respuesta. Es indispensable para detectar malware, pero será crítico controlar las expectativas de los responsables de seguridad sobre las capacidades de la tecnología. El juego puede cambiar en cualquier momento y debes asegurarte de haber implementado y administrado tus defensas de manera adecuada para que 'los malos' queden afuera.

Independientemente de lo que digan las piezas de marketing, la verdadera Inteligencia Artificial aún no existe, y el Machine Learning no es lo suficientemente maduro para ser la única capa de seguridad que se interpone entre tu máquina y el atacante.