



América Latina

<http://www.cioal.com/2016/10/18/javelin-networks-crea-escudo-seguridad-ia/>

Javelin Networks crea un escudo de seguridad con IA

18/10/16

Share



La startup [Javelin Networks](#) utiliza la Inteligencia Artificial (IA) para lograr que las intrusiones de ciberatacantes sean inofensivas para las empresas e inútiles para los hackers.

CIO América Latina | Por: Elibeth Eduardo | @ely_e

Sí usted es un CIO quizás le preocupen las voces agoreras que señalan que el mundo, en general, está perdiendo la guerra contra los hackers y las empresas tienen muy poca capacidad para defenderse a la velocidad que los delincuentes innovan.

Y es que las cifras son demoledoras: de acuerdo a los estudios de HBS, la seguridad de nueve de cada diez empresas ha sido comprometida, ya sea mediante el acceso remoto por robo de credenciales, debido a intrusión a través de conexiones de red de terceros o a malware que aprovechan exploit y otras vulnerabilidades de API.

Afortunadamente, apenas saliendo del stealth mode en Silicon Valley, la startup [Javelin Networks](#) presenta al mercado una alternativa de protección innovadora con su producto Javelin ZeroMove que permite una alternativa diferente para la detección y prevención de ataques.

¿Lo más importante? Aunque los hackers hayan logrado ingresar a su servidor o computadora, la solución de software de Javelin Networks inutiliza la intrusión, impidiendo que se extienda por la organización y haciéndola – prácticamente – inofensiva.



“Nuestra solución automatiza la detección del atacante y detiene su posterior movimiento”, explicó el CEO de Javelin Networks, Roi Abutbul.

Trampa inteligente

El software de [Javelin ZeroMove](#) utiliza una solución de inteligencia artificial para generar una especie de máscara o telaraña que enmascara la topografía interna de los sistemas de la compañía, creando una trampa virtual que inutiliza los avances de los atacantes, haciendo que los (aparentes) que estos logran con la intrusión generen información falsa y, por tanto, inútil.

“El personal de TI están buscando constantemente y en forma manual atacantes en computadores y redes. Es imposible hacerlo de manera adecuada y precisa con la tecnología y los procesos utilizado en la actualidad. Fue en eso donde vimos una oportunidad, enfocándonos en la necesidad de lograr la detección de ataques post breach que pudiera ser proactiva, autónomo y sin fisuras. Nuestra solución automatiza la detección del atacante y detiene su posterior movimiento”, explicó el CEO de Javelin Networks, Roi Abutbul.