IBM Watson lucha contra el cibercrimen

ARMONK, N.Y. - 10 may 2016: IBM Security (NYSE: IBM) ha anunciado *Watson for Cyber Security*, una nueva versión en cloud de la tecnología cognitiva de la compañía, entrenada en el lenguaje de la seguridad, fruto de un proyecto de investigación de un año. Para continuar este proyecto, IBM tiene previsto colaborar con ocho universidades de Estados Unidos y Canadá con el fin de ampliar en gran medida la recogida de datos de seguridad con los que IBM ha entrenado al sistema cognitivo.

Watson for Cyber Security supone un gran avance en el área de la seguridad cognitiva. IBM Watson está aprendiendo todos los diferentes matices de las investigaciones de seguridad y los patrones detectados así como ejemplos de ataques y amenazas ocultas que de otro modo se perderían. Desde el próximo otoño, IBM trabajará con ocho universidades de Estados Unidos y Canadá para continuar entrenando a Watson en el lenguaje de la ciberseguridad.

El anuncio de hoy forma parte de un proyecto pionero de seguridad cognitiva cuya finalidad es hacer frente a la brecha de capacidades de ciberseguridad que se avecina. Los esfuerzos de IBM se centran en ayudar a que los especialistas en seguridad mejoren sus capacidades mediante la utilización de sistemas cognitivos que automaticen la asociación de información, amenazas emergentes y estrategias de respuesta y resolución. IBM tiene la intención de iniciar los despliegues de producción beta de *Watson for Cyber Security* a finales de este año.

La biblioteca de investigación de vulnerabilidades X-Force será el núcleo de los materiales que nutren Watson for Cyber Security. Esta fuente de conocimiento abarca 20 años de investigación de seguridad, detalles de 8 millones de ataques spam y phishing y más de 100.000 vulnerabilidades documentadas.

IBM Watson ante la creciente necesidad de capacidades de seguridad

El volumen de datos de seguridad que deben utilizar los especialistas de seguridad está aumentando de una forma desmesurada. Las empresas manejan una media de 200.000 datos de eventos de seguridad al día1 lo que supone un gasto de 1,3 millones de dólares al año solo gestionando falsos positivos y más de 21.000 horas de trabajo2. A esto se añaden otros 10.000 documentos de investigaciones de seguridad o cerca de 60.000 blogs de seguridad publicados al mes, lo que representa un reto para los especialistas de seguridad a la hora de actuar con la información actualizada.

Diseñada en IBM Cloud, *Watson for Cyber Security* es la primera tecnología que ofrece conocimiento de datos de seguridad a gran escala utilizando la capacidad de IBM Watson para razonar y aprender de datos desestructurados -80 por ciento de todos los datos de Internet que las herramientas de seguridad tradicionales no pueden procesar, incluyendo blogs, artículos, vídeos, informes, alertas y otro tipo de datos. *Watson for Cyber Security* procesa también el lenguaje natural para para comprender la naturaleza vaga e imprecisa del lenguaje humano en datos no estructurados.

Como resultado, *Watson for Cyber Security* está diseñada para ofrecer información de las amenazas emergentes, así como dar recomendaciones sobre cómo frenarlas, proporcionando mayor velocidad y más capacidades a los profesionales de seguridad. IBM irá incorporando progresivamente otras capacidades de IBM Watson incluyendo sistemas de análisis de datos para detecciones atípicas, herramientas de representación gráfica y técnicas para encontrar conexiones entre datos relacionados en diferentes documentos. Por ejemplo, IBM Watson puede encontrar datos de un tipo de malware emergente en un boletín de seguridad online e información sobre una estrategia de defensa en un blog de un analista de seguridad.

Colaboración con Universidades para entrenar a IBM Watson for Cyber Security

IBM tiene previsto colaborar con ocho universidades que tienen algunos de los mejores programas de ciberseguridad del mundo con el fin de seguir entrenando a IBM Watson e iniciar a sus estudiantes en el aprendizaje de la computación cognitiva. Estas universidades son: California State Polytechnic University, Pomona; Pennsylvania State University; Massachusetts Institute of Technology; New York University; UMBC; University of New Brunswick; University of Ottawa y University of Waterloo.

Los estudiantes ayudarán a IBM Watson en el lenguaje de la ciberseguridad y trabajarán para construir el corpus de conocimiento de IBM Watson alimentando el sistema con informes y datos de seguridad. Los estudiantes colaborarán codo con codo con los expertos de IBM Security para aprender los diferentes matices de esos informes de seguridad inteligente y por tanto serán los primeros en adquirir experiencia en esta área emergente de seguridad cognitiva.

Más información en www.ibm.com/security/cognitive

1 IBM 2015 Cybersecurity Intelligence Index

2 The Cost of Malware Containment, del Ponemon Institute, publicado en enero de 2015