

[Anuncios](#)

IBM Watson for Cyber Security ya está disponible en versión beta para combatir el cibercrimen

Armonk, NY - 06 dic 2016: IBM Security ha anunciado que empresas líderes de sectores de banca, salud, seguros, educación y otras industrias clave se han unido al programa Beta de *IBM Watson for Cyber Security*. Sun Life Financial, el Centro Médico de la Universidad de Rochester, la Corporación SCANA, el grupo financiero Sumitomo Mitsui, la Universidad Estatal Politécnica de California, la Universidad de New Brunswick, Avnet y Smarttech se encuentran entre las 40 organizaciones que están probando la capacidad de Watson para ayudar en la lucha contra el cibercrimen.

El cibercrimen es cada vez más frecuente y complejo. Para identificar y frenar sus amenazas, se requieren herramientas con más inteligencia. *Watson for Cyber Security* utiliza tecnologías cognitivas como el aprendizaje de máquinas y el procesamiento del lenguaje natural, lo que puede ayudar a los analistas de seguridad a tomar mejores decisiones más rápidamente a partir de grandes cantidades de datos.

Un estudio reciente del *IBM Institute for Business Value* revela que casi el 60 por ciento de los profesionales de la seguridad creen que las tecnologías cognitivas emergentes serán un elemento crítico para cambiar el curso de la lucha contra el cibercrimen. (1)

El programa beta de IBM Watson for Cyber Security en marcha

Watson for Cyber Security saca el máximo partido de la tecnología cognitiva líder de IBM, y está siendo entrenado para entender el singular lenguaje de la seguridad. De esta forma los analistas de seguridad pueden tomar mejores decisiones a partir de datos estructurados pero también a partir de la enorme cantidad de datos no estructurados que hasta ahora habían sido invisibles para los sistemas de defensa de las organizaciones.

Las compañías Fortune 500 y otras organizaciones de diferentes industrias como finanzas, viajes, energía, automoción y educación están trabajando actualmente con *Watson for Cyber Security*, ayudando a perfeccionar las capacidades de ciberseguridad de Watson ante diferentes situaciones. Avnet, la Universidad Estatal Politécnica de California, la Corporación SCANA, Smarttech, Sun Life Financial, el Grupo Financiero Sumitono Mitsui, la Universidad de New Brunswick y el Centro Médico de la Universidad de Rochester están entre el primer grupo de clientes que ya trabajan en el programa *Watson for Cyber Security*. El programa beta incorporará 40 empresas en las próximas semanas.

Estos clientes beta están aprovechando las ventajas de Watson en sus entornos de seguridad en diferentes casos como:

- Determinar si una “infracción” de seguridad está o no asociada a una campaña conocida de malware o ciberdelincuencia; si es así, Watson proporciona información sobre el malware empleado, las vulnerabilidades y el alcance de la amenaza, entre otras cosas.

- Mejora la identificación de conductas sospechosas; Watson proporciona un contexto adicional a la actividad del usuario, lo que permite determinar si una actividad es o no malintencionada. Trabajando con estos clientes beta, IBM continúa mejorando la comprensión de Watson de los datos de seguridad cibernética y refinando la forma en la que Watson se integra con las operaciones de seguridad diaria.

La seguridad cognitiva está en alza

El *IBM Institute for Business Value* ha entrevistado recientemente a más de 700 profesionales de la seguridad para evaluar las perspectivas sobre los desafíos, beneficios y oportunidades para las tecnologías de seguridad cognitiva. Casi el 60 por ciento de los encuestados confía en que las tecnologías cognitivas madurarán lo bastante pronto como para frenar significativamente a los ciberdelincuentes en un futuro cercano. Mientras que solo el 7 por ciento dijo que sus organizaciones están actualmente en proceso de implementar soluciones de seguridad cognitiva, el 21 por ciento manifestó que implementaría estas soluciones en los próximos 2-3 años, lo que representa un aumento de 3 veces en la tasa de adopción.

Los profesionales de seguridad consideran que las tecnologías cognitivas, por un lado mejorarán la detección de las amenazas y por otro, optimizarán las capacidades de reacción ante incidentes (un 40 por ciento de los encuestados) puesto que en la actualidad las organizaciones tardan una media de 201 días en identificar y una media de 70 días para contenerlas (2)

La tecnología cognitiva se integra en la oferta de IBM Security

A medida que continúa el desarrollo de *Watson for Cybersecurity*, IBM sigue introduciendo capacidades analíticas y cognitivas avanzadas en otras áreas de su portfolio de soluciones de seguridad.

- Análisis de comportamiento para comprender mejor los patrones de uso de los empleados y socios y determinar si sus credenciales han sido comprometidos a través de *IBM QRadar User Behavior Analytics*.
- Uso de capacidades de análisis patentadas, aprendizaje automático y biometría de comportamiento para prevenir el fraude bancario con *IBM Trusteer Pinpoint Detect*.
- Aprendizaje automático para ayudar a los clientes a encontrar vulnerabilidades potenciales en sus aplicaciones más rápidamente con *IBM Application Security on Cloud*.
- Ayudar a los clientes a detectar y remediar las brechas antes de que se produzcan con las nuevas capacidades de detección de anomalías en todos sus datos, con *IBM Security Guardium*.

[1] IBM Institute of Business Value Study: Cybersecurity in the Cognitive Era

[2] IBM / Ponemon Cost of a Data Breach study, 2016
