IBM lleva Watson for CyberSecurity a los centros de operaciones de seguridad

- **Entre las novedades se incluye un chat bot con tecnología Watson y un asistente de seguridad que funciona por voz**

CAMBRIDGE, MA - 13 feb 2017: IBM Security ha anunciado que los Centros de Operaciones de Seguridad (en inglés SOCs) ya pueden utilizar Watson for Cyber Security. Durante el último año, Watson ha sido entrenado en el lenguaje de la ciberseguridad, asimilando cerca de un millón de documentos de seguridad.

Según estudios de IBM, los equipos de seguridad examinan una media de 200.000 eventos de seguridad al día, utilizando más de 20.000 horas al año buscando falsos positivos. La introducción de tecnologías cognitivas en los centros de operaciones de seguridad resultaba imprescindible para afrontar la duplicación del número de incidentes de seguridad en los próximos cinco años y de la regulación a nivel global1.

Watson for Cyber Security se integrará en una nueva plataforma cognitiva de IBM en los centros de operaciones de seguridad, uniendo tecnologías cognitivas avanzadas con operaciones de seguridad y ofreciendo la capacidad de responder a las amenazas a través de puntos de acceso, redes, usuarios y cloud. La pieza central de esta plataforma es *IBM QRadar Watson Advisor*, una nueva app disponible en *IBM Security App Exchange*, que es la primera herramienta que saca provecho del corpus de información sobre ciberseguridad de Watson.

La app *IBM QRadar Advisor with Watson* ofrece capacidades cognitivas para ayudar a los analistas de seguridad en sus investigaciones y soluciones por medio de la plataforma inteligente de seguridad de IBM QRadar. La solución ayuda en la investigación de potenciales amenazas correlacionando el contenido en lenguaje natural de los blogs de seguridad, webs e informes de investigación con otras fuentes y con datos de incidentes de seguridad de QRadar, acortando las respuestas a incidentes de seguridad de semanas o días, a minutos. La app ya está siendo utilizada por Avnet, la Universidad de New Burnswich y otros 40 clientes a nivel global.

Con el fin de extender la capacidad del SOC cognitivo a los puntos de acceso, IBM Security ha anunciado también una nueva solución de detección y respuesta denominada *IBM BigFix Detect*, que permite tener visibilidad completa del panorama de puntos de acceso mientras reduce el tiempo entre la detección de la amenaza y la solución.

Servicios de seguridad cognitivos

Dado el enorme crecimiento de incidentes de seguridad, IBM ha decidido invertir en investigación para ofrecer herramientas cognitivas en su red global *X-Force Command Center*. Una de ellas es un chat bot con tecnología Watson para clientes de servicios gestionados de seguridad. Los clientes pueden preguntar a Watson vía mensajería instantánea sobre su posición de seguridad o configuraciones de red.

El otro proyecto de investigación, cuyo nombre clave es Havyn, es un asistente de seguridad pionero en esta área que funciona por voz y que utiliza la tecnología de conversación de Watson. Havyn aprovecha las APIs de Watson, BlueMix e IBM Cloud para ofrecer respuesta en tiempo real a peticiones y órdenes verbales de los analistas de seguridad, mediante el acceso a datos open source de inteligencia de seguridad, incluyendo *IBM X-Force Exchange*, así como a datos históricos del cliente y de sus herramientas de seguridad.

IBM ayudará también a sus clientes a diseñar, construir y gestionar los centros de operaciones de seguridad cognitivos a nivel global mediante *IBM Managed Security Services*. En los últimos 5 años, IBM ha construido cerca de 300 centros de operaciones de seguridad para clientes de docenas de industrias, incluyendo retail, banca y educación. Los clientes pueden elegir si IBM les construye un SOC cognitivo en sus instalaciones o lo tienen de forma virtual en IBM Cloud como parte de la red *IBM X-Force Command Center*.

- IBM 2016 Cyber Security Intelligence Index analysis
-