'Big data', una oportunidad para mejorar la ciberseguridad

LAS HERRAMIENTAS DE ANALÍTICA DE 'BIG DATA' ESTÁN EN PRIMERA LÍNEA DE DEFENSA PARA CONSTRUIR MODELOS QUE AYUDEN PREDECIR EL COMPORTAMIENTO Y LOS PATRONES DE ACTUACIÓN DE LOS CIBERCRIMINALES.

Toñi Herrero Alcántara

No cabe duda que *big data* ha supuesto un nuevo capítulo en la revolución digital, convirtiendo grandes volúmenes de datos en información de valor. En cualquier caso lo fundamental de esta ingente cantidad de datos es su procesamiento, pues es este lo que los convierte en el activo tangible más valioso y con más potencial para las empresas e instituciones. El tratamiento de toda esa información digital –en la que hay muchos datos corporativos pero también personales de los propios usuarios– requiere de unas grandes medidas de seguridad para mantener la privacidad y seguridad de los mismos.

En el mundo de la seguridad, donde cada vez los ataques se cometen en menos tiempo y surgen amenazas nuevas en cuestión de segundos, es imprescindible contar con herramientas potentes que ayuden a gestionar y analizar toda esa información nueva para detectar posibles ataques en tiempo real. "En general, lo que nos debe preocupar del *big data* es la cantidad de información que se genera y almacena y, en muchas ocasiones, de carácter crítico. Si cuidamos la seguridad de la información que almacenamos en nuestra empresa, debemos ser aún más cuidadosos y estrictos con el gran volumen de datos que se aloja en un entorno *big data*. No hay que olvidar que ese volumen ingente de datos dispersos, una vez procesado, tiene gran valor... lo que puede hacer que se produzcan fugas de datos o robos de información empleado distintas técnicas. En lo que se refiere a la protección del dato en sí mismo, una buena solución de cifrado puede dar respuesta a esta situación", comenta Álvaro Roldán, responsable de Canal y Alianzas de Trend Micro Iberia, que remarca que la necesidad de tener en cuenta la naturaleza de los datos donde por cuestiones de privacidad o propiedad intelectual sea especialmente crítico el uso que se hace de la información.

Pero el *big data* también tiene otra aproximación al entorno de la seguridad, en concreto de la ciberseguridad, un área en constante cambio. Según señala IDC en su informe 'Big Data y Analítica Predictiva: Sobre la Línea de la Ciberseguridad', elaborado en 2015 para SAS, el número de ataques continúa aumentando, los tipos de actores

El 'big data' y su capacidad de procesamiento son una herramienta de inteligencia en las estrategias de ciberseguridad

de amenazas han aumentado, y las vías de ataque han crecido y se han diversificado en sofisticadas amenazas persistentes, ataques internos, fraude y delitos informáticos. Las soluciones de seguridad tradicionales no son suficientes para hacer frente a este nuevo concepto de amenaza y nuevo panorama de ataques. La mayoría de las amenazas de ciberseguridad actuales van desde ataques DDoS, robo de datos internos a ataques de troyanos, *phishing*... y los atacantes pueden ser desde accidentales e internos, un oportunistas, *hacktivistas*, criminales profesionales, etc. Aunque las bases de datos y sitios web siguen siendo objetivos tradicionales, IDC apunta amenazas y vulnerabili-

dades en varias áreas nuevas, incluyendo ataques a redes sociales y dispositivos móviles, dispositivos propiedad de los empleados (BYOD), nubes privadas, públicas o híbridas y el Internet de las cosas (IoT), donde una amplia variedad de dispositivos están conectados a Internet. El informe de IDC recoge que la propagación de vectores de ataque y los agentes de amenaza contra un conjunto cada vez mayor de áreas objetivo se ha traducido en un crecimiento exponencial del nivel de complejidad de la seguridad cibernética para el CISO y el CIO. El resultado es que la mitigación proactiva de estas amenazas con las tecnologías actuales es casi imposible si no se aplica un nuevo enfoque. Y en este punto es donde interviene el *big data* y sus herramientas. Para tener una idea de la cantidad de datos que necesita ser procesada, una red de tamaño mediano con 20.000 dispositivos (ordenadores portátiles, teléfonos inteligentes y servidores) transmitirá más de 50 TB de datos en un periodo de 24 horas. Eso significa que más de 5 Gbits deben ser analizados cada segundo para detectar ataques cibernéticos, las posibles amenazas y malware atribuidos a los hackers. Hacer frente a tales volúmenes de datos en tiempo real plantea retos difíciles. Además para el análisis de grandes volúmenes de datos es necesario crear modelos en la ciencia de datos que puedan detectar ataques cibernéticos, mientras minimizan los falsos positivos (falsas alarmas) y falsos negativos (en su defecto para detectar amenazas reales). No en vano, "una de las ciberarmas más interesante viene de la mano del *big data*, mediante la cual podemos construir modelos para predecir el comportamiento y los patrones de actuación de los cibercriminales", señala José Antonio Rubio, presidente del Digital Trust Think Tank de IDG.

> Hace tiempo que la tecnología de 'big data' forma parte de las soluciones de seguridad y los principales antivirus lo incorporan

Ciberseguridad y 'big data'

El *big data* y su capacidad de procesamiento son una herramienta de inteligencia en las estrategias de ciberseguridad ante la creciente proliferación de acciones delictivas en el ciberespacio. Y es que en la esencia del *big data* subyace la muy alta capacidad para procesar ingentes cantidades de datos de distinto tipo (estructurados, semiestructurados y no estructurados) y desarrollos de modelos que sirven a los fines definidos por las organizaciones. Como se apunta desde la Fundación Big Data, la capacidad de prevención se puede incrementar mediante la captura de los datos de acceso y su proceso en tiempo real que permita su comparación con modelos de comportamiento no seguros permitiendo la detección de las ciberamenazas. "La importancia del *big data* aplicado a la ciberseguridad queda resaltada en la necesidad de incrementar las capacidades de detección y análisis de las ciberamenazas a las Administraciones Públicas, las infraestructuras críticas y otros sistemas de interés nacional", apunta Francisco Javier Antón, presidente de la Fundación Big Data. La recopilación y tratamiento de grandes cantidades de

La ciberseguridad es una de esas áreas en la que un análisis de alto rendimiento y en tiempo real de 'big data' es imprescindible

datos puede ayudar a manejar el elevado número de amenazas al que nos enfrentamos hoy en día. De esta forma, se pueden categorizar las amenazas y, gracias al *big data*, mejorar los mecanismos de detección para que sean más eficaces. "Con la cantidad de datos que existen actualmente y los que se incorporarán con la evolución del IoT o los *wearables*, los sistemas serán capaces de detectar comportamientos anómalos para poderlos analizar de forma detallada y poder lanzar alarmas y/o sistemas preventivos", indica Pere San Martín, director de Arvato Consulting.

Por tanto *big data* y seguridad mantienen una relación muy estrecha y son mutuamente importantes para sus respectivos futuros. "Desde hace años, parte de la industria de la seguridad, y compañías como G DATA, están usando el *big data* para la protección de sus clientes. El *big data* desempeña un papel esencial en todos esos servicios que, basados en la reputación, nos están permitiendo bloquear en tiempo real las nuevas amenazas sin necesidad de detallados análisis previos. El *big data* nos ayuda a saber de dónde proceden las amenazas y a afinar y optimizar nuestras tecnologías en el futuro. Y Big Data también es el intercambio de millones de muestras de malware que hacemos diariamente la industria de seguridad TI", señala Eddy Willems, experto en Ciberseguridad en G DATA Software**.**

Una de las grandes aportaciones del *big data* es poder analizar mucha información y tener respuesta en tiempo real. También permite montar arquitecturas para analizar toda esa información y buscar objetivos o riesgos de una manera rápida. "El *big data* facilita poner foco, bajar a mucho nivel de detalle y descubrir objetivos, y de un riesgo concreto poder ver toda la información que hay alrededor: quién lo está haciendo, dónde está localizado, con quién está trabajando, el riesgo que puede tener, cómo puede afectar y a quién. Facilita una intervención rápida, de una acción más operativa para atajar ese riesgo", señala Enrique Serrano, director general de Tinámica.

Watson contra el cibercrimen

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% 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 comprender la naturaleza vaga e imprecisa del lenguaje humano en datos no estructurados. Como resultado, Watson for Cyber Security ofrecerá información de las amenazas emergentes, dará recomendaciones sobre cómo frenarlas, proporcionando mayor velocidad y más capacidades a los profesionales de seguridad. La compañía 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. A partir de otoño, IBM tiene previsto colaborar con ocho universidades –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– 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.

Y es que, a medida que el perímetro de una organización se ha vuelto más difuso (a razón de la flexibilidad del trabajo, del incremento del teletrabajo, del uso de múltiples dispositivos) las organizaciones necesitan de un enfoque diferente en la seguridad. "Un nuevo modelo basado en la agilidad, en el contexto y con capacidades de predicción y prevención del riesgo. En este sentido, las tecnologías de *big data* y *analytics* se vuelven fundamentales para capturar las crecientes señales en este perímetro más difuso que inciden en la seguridad. Es decir, para poder evaluar correctamente los riesgos y defenderse de forma adecuada ante ello", indica Josep Curto, director general de Delfos Research. "Estamos hablando por lo tanto de que transforma profundamente todas las capas en las que la seguridad está implicada: SIEM, network monitoring, autentificación y autorización de usuarios, gestión de identidades, gestión del fraude, y gobernanza, riesgo y cumplimiento". Inicialmente todas las componentes tecnológicas de *big data* son susceptibles de ayudar a la mejora de la seguridad. Según indica Curto, los principales usos que se están haciendo incluyen técnicas de reconocimiento facial, que se han usado para la identificación de perfiles de riesgo en eventos importantes y con grandes congregaciones de personas; y técnicas de almacenamiento y análisis de grafos, que se están usando para detectar patrones de comportamiento en fraude, en el que se diluye la acción mediante una red de personas.

Queda claro que la ciberseguridad es una de esas áreas en la que un análisis de alto rendimiento y en tiempo real de *big data* es imprescindible. Las compañías necesitan poder controlar en tiempo real y de manera integral todas las conexiones, interacciones y relaciones entre los activos de la red. Esto es posible gracias a la aplicación de técnicas de análisis de comportamiento a toda la actividad que diariamente se rastrea con aprendizaje automatizado (*machine learning*), pudiendo discernir lo que se considera 'normal' de lo que debe ser analizado como conducta irregular haciendo posible la priorización de potenciales incidencias para su investigación. Además, al conectarse herramientas de seguridad aisladas, se dispone de un contexto informacional del entorno del

negocio que enriquece el conjunto de datos. Así, la información finalmente disponible es más precisa, consistente, útil e inmediata, lo que permite la toma de decisiones más estratégicas y rápidas. "Esto, en el ámbito de la ciberseguridad, constituye una gran ventaja para la detección temprana de amenazas, la prevención o la respuesta inmediata a ciberataques, así como para estar al día de la evolución de las amenazas cibernéticas, ejercicio obligatorio para una defensa completa y constantemente eficaz. Es decir, convertir sus sistemas internos en verdaderas plataformas de inteligencia de seguridad", apunta Marcos Carrascosa, director de preventas en SAS España. Ahora, a través del uso de ciberanalítica, las empresas pueden predecir el comportamiento inusual y detectar una amenaza interna activa por la detección de anomalías en el comportamiento de interacción, tales como el acceso a una base de datos y descarga de un conjunto de archivos. A menos que una organización tenga la capacidad de modelar el comportamiento normal y anómalo de las personas y los activos de la red, será incapaz de detectar estos nuevos tipos de ata-

ques. Y como señala Enrique Serrano de Tinámica, la principal herramienta es el análisis predictivo. “No se trata solo de analítica para detectar, es analítica también para ver el futuro, para predecir, en el sentido de que puedes prevenir en función de una serie de variables lo que puede ocurrir”.

Analítica predictiva y soluciones

Como se detalla en el informe de IDC, la analítica presenta retos importantes para las operaciones de seguridad, incluyendo la escalabilidad, pues el análisis de comportamiento requiere una rápida ingestión continuada de datos de múltiples fuentes. Impedir ciberataques sofisticados demanda un mejor entendimiento del *big data* con más analítica proactiva. Las organizaciones necesitan cambiar de estrategias reactivas a proactivas que busquen entender una amenaza antes de que un atacante pueda causar daño. Esto requiere un monitoreo constante del comportamiento de red para que la actividad inusual pueda distinguirse del comportamiento normal. Aplicar analítica predictiva y de comportamiento a todos los datos empresariales y externos disponibles puede ayudar a las organizaciones a evaluar potenciales amenazas, detectar posibles ataques y reunir mayor información. Esta analítica necesita ejecutarse en tiempo real para que las amenazas puedan mitigarse de forma proactiva antes de que ocurra una pérdida significativa. En un primer estudio del Instituto Ponemon, el 86% de los entrevistados dijeron que detectar ciberataques lleva demasiado tiempo, y el 85% no estaban priorizando los incidentes. Mientras tanto, un 40% dijo que sus productos de seguridad no importan información de amenazas desde otras fuentes.

“La analítica predictiva aplicada a la ciberseguridad es fundamental por los ahorros que ello conlleva. Para poder trabajar sobre patrones de ataque hay que analizar todo lo que ya ha ocurrido, y sobre millones de variables y sobre millones de datos, poder intuir que efectivamente eso es un ataque que se está produciendo en un sitio. Todas las empresas tecnológicas que tienen sus centros de contingencia, están actuando bajo la misma filosofía”, comenta Francisco Javier Antón, presidente de la Fundación Big Data.

Los usos concretos de la analítica predictiva, en lo que respecta a grandes empresas, pueden pasar por la detección de patrones de comportamiento de sus empleados. Por ejemplo, una empresa de distribución con pérdidas por tema de hurtos en sus almacenes puede ayudarse de la analítica predictiva para detectar pues puede ayudar a detectar qué personas potencialmente pueden comportarse de esa manera. “Por un lado hay una mayor vulnerabi-

Datos oscuros, a la luz

Según IDC, más del 90% del big data son datos ocultos (dark data) y, en muchas ocasiones, esta información “escondida” es tan relevante a nivel empresarial como lo pueden ser los datos recogidos proactivamente. De hecho, Gartner define el dark data como “los activos de información que recopilan, tratan y almacenan las organizaciones durante sus actividades empresariales habituales, pero que no suelen utilizar para otros fines”. Una solución desarrollada por la startup Datumize se encarga de identificar y convertir en útiles estos datos. Datumize Data Collector facilita la localización de todos estos datos no accesibles a priori para convertirlos en información relevante que permite comprender mejor los procesos internos e incrementar los beneficios mediante la optimización del negocio. “Nuestra tecnología puede implementarse en diferentes sectores verticales e integrarse en cualquier sistema, capturando datos a tiempo real y en el momento adecuado. Industrias como las del big data, internet de las cosas (IoT), energía, comercio electrónico, ocio, automoción o el retail son algunos de nuestros principales focos y en los que estamos viendo que la gestión del llamado dark data puede dar los mayores beneficios”, explica Nacho Lafuente, cofundador y CEO de Datumize. Incluso se puede usar esta información para mejorar la seguridad. “Hemos estudiado el caso de un cliente en que el análisis del tráfico que generan sus miles de usuarios, que son datos oscuros, puede ser utilizado por la empresa para configurar mejor los controles de acceso a sus sistemas internos y externos”.

lidad porque hay más datos y los datos pues tienen una tendencia a concentrarse. Pero por otro lado también te ayuda a detectar esas vulnerabilidades y actuar en tiempo real. Hay más riesgos pero también hay más oportunidades de solventarlos", señala el director general de Tinámica.

Hace tiempo que el *big data* forma parte de las soluciones de seguridad y los principales antivirus incorporan algún sistema basado en estas tecnologías que permite recopilar y analizar grandes cantidades de ficheros y enlaces sospechosos. Concretamente, todos los mecanismos de recolección de muestras o de análisis de comportamiento incorporan el *big data* de alguna forma. "En ESET, por ejemplo, hace ya años que nuestras soluciones de seguridad incorporan un mecanismo automático de recolección de muestras que ayudan a detectar nuevas amenazas reduciendo al mínimo la ventana de exposición al malware. Contamos con ESET Live Grid, un sistema de recopilación y análisis de amenazas a gran escala", comenta Josep Albors, director del laboratorio de ESET. De hecho tradicionalmente la analítica ya ha sido importante en la creación de patrones y en el análisis. "Ahora ya no es posible imaginar una solución de seguridad que no tenga presente o vaya a incluir en el futuro capacidades fundamentadas en las tecnologías de *big data* ", indica el director general de Delfos Research. Igualmente destaca la facilidad que existe para montar soluciones a medida, basadas en la utilización de Hadoop o Spark con analítica que normalmente lo hacemos con lenguaje de programación R o con Phyton y de sistemas en la nube. Según describe José Antonio Rubio, del Digital Trust Think Tank de IDG, el conjunto de herramientas estaría formado por la tecnología estadística que permite que *big data* sea una realidad, como las reglas de inducción, los algoritmos genéticos o las redes neuronales artificiales. Y por otro lado con los sistemas que permiten el almacenamiento masivo de datos. De ese binomio surgen modelos como MapReduce, Apache Hadoop, Apache Spark o las bases de datos NoSQL. Para el procesado de estos volúmenes ingentes de datos se han desarrollado a su vez lenguajes de programación de alto nivel, infraestructuras *data warehouse* o sistemas de ficheros que están a nuestra disposición para hacer del *big data* una realidad en el día a día de las organizaciones.

> Las empresas ahora tienen mejores medios tecnológicos para identificar y responder al cambiante panorama de amenazas

Desde Blue Coat, las soluciones de análisis de seguridad tienen que hacer frente a siete importantes casos de uso del mundo real: conocimiento de la situación, seguimiento continuo, respuesta y resolución a incidentes de seguridad, detección avanzada de malware, monitorización y análisis de pérdida de datos, monitorización y análisis de tráfico web y gobierno de TI, gestión de riesgos y cumplimiento. Algunas de las soluciones que están ahora en el mercado son SAS Cybersecurity, que emplea analítica de alto desempeño para procesar y evaluar miles de millones de transacciones diarias de redes en tiempo real, reduciendo el tiempo para detectar eventos de seguridad y mejorando la eficiencia de operaciones de seguridad. La herramienta de Blue Coat Security Analytics ofrece un análisis forense de red y la solución de respuesta a incidentes para que las empresas puedan responder con rapidez a cualquier incidencia de seguridad. Actúa como una cámara en la red, ya que aporta inteligencia clara y práctica sobre las amenazas de seguridad de aplicaciones, archivos y contenido web. Con ese panorama retrospectivo del tráfico de la red, puede identificar rápidamente los ataques avanzados y específicos que escapan a las herramientas de seguridad preventivas tradicionales. Mientras IBM cuenta con Qradar Security Intelligence Platform que ofrece una arquitectura unificada en la que se integran la gestión de sucesos e información de seguridad, la gestión de registros, la detección de anomalías, la investigación de incidentes y la gestión de la configu-

ración y de las vulnerabilidades. Por su parte Trend Micro cuenta con Smart Protection Network, una infraestructura de seguridad inteligente en la nube de Trend Micro que recopila datos de forma continua en todo el mundo para asegurar una protección ininterrumpida.

Principales beneficiados

Los gobiernos son uno de los principales sectores beneficiados del uso del *big data* y en concreto de la analítica predictiva para combatir las ciberamenazas. Los cuerpos de seguridad nacional ya están trabajando con técnicas de *big data* para perseguir todo este tipo de delitos y para descubrir delincuentes que están ocultos en la red. "El *big data* está siendo decisivo en la persecución de la pornografía infantil en la red, ya que estos delincuentes utilizan sistemas complejos de almacenamiento y distribución de los datos que hasta la fecha era muy difícil procesar", indica Pere San Martín, de Arvato Consulting.

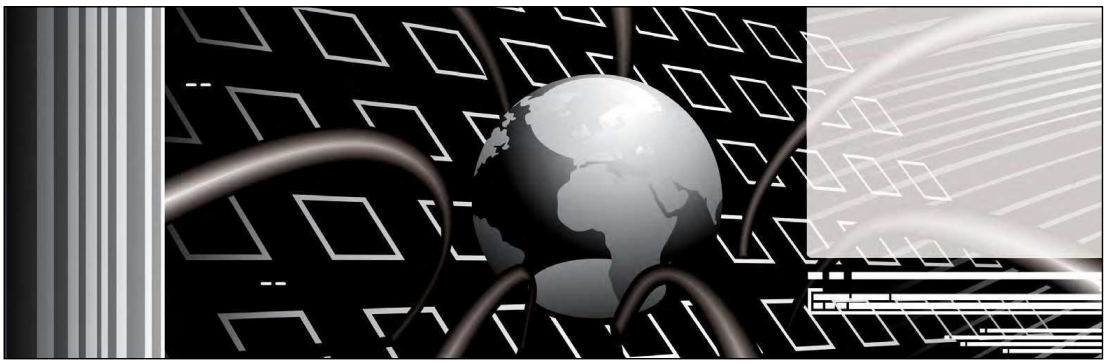
Otro de los sectores donde la analítica predictiva tiene una gran aplicación es el de los servicios financieros, para combatir el fraude y mitigar los riesgos. "Trabajamos mucho con los grandes bancos para tratar de adelantar riesgos: clientes de riesgo que pueden defraudar, riesgos con transacciones telemáticas, riesgos con medios de pago como tarjetas... Por ejemplo, cada vez más el *big data* ayuda a anticipar ese riesgo, hay algoritmos que permiten que cruzando datos y dependiendo de la transaccionalidad del histórico de transacciones y el comportamiento que tiene una persona sea bastante predecible lo que va a hacer, entonces cuando hay una transacción que se sale de su patrón el sistema te avisa", explica Enrique Serrano, de Tinámica, quien señala la posibilidad de personalización que ofrece el *big data*. "Es el análisis de patrones que antes se hacían con *clusters*, con lo cual se agrupaba, y ahora lo que haces es que el análisis de patrones sea individual". Otra tipología de empresas beneficiadas del uso de la analítica predictiva para mejorar la ciberseguridad son las grandes empresas que cuentan con grandes centros de datos. En la industria de servicios públicos y energía, la investigación de IDC encontró que la analítica avanzada y predictiva es crítica para promover una amplia variedad de cibermandatos, incluyendo el cumplimiento regulatorio.

Y es que con tantos datos, hay más riesgos pero también hay más oportunidades de solventarlos. "Todo lo que está ocurriendo, por ejemplo, papeles de Panamá, todo eso va a ir a más. Un fallo personal, deliberado o no, da lugar a fugas de información y cada vez va a haber más ataques desde fuera para intentar acceder a los datos de las compañías y de las personas por parte de los competidores, de terceras personas que van a ofrecer servicios bloqueando la ley o traspasándola en cuanto a poder acceder a datos de otros. El valor del dato, del smart data, cada vez va a ser mayor", comenta Serrano.

Más tecnologías innovadoras

Los adversarios transforman constantemente sus ataques y encuentran formas creativas para penetrar las defensas. Lo que las organizaciones necesitan es la capacidad de detectar el más sutil cambio en la actividad y analizarla teniendo en cuenta el contexto. Pero el mundo digital produce más de 2,5 trillones de bytes de datos de todos los días, y el 80% de ella es no estructurado. Esto significa se expresa en lenguaje natural –hablado, escrito o visual– que un ser humano puede entender fácilmente, pero los sistemas de seguridad tradicional no pueden.

"Desde el punto de vista de la seguridad, monitorizar un entorno es necesario porque ataques de seguridad va a haber siempre. La clave está en el tiempo de respuesta: cuando se detecta ese posible ataque, si reacciona rápidamente el impacto será mucho menor. Y eso se hace teniendo más contexto, casi en tiempo real", remarca Emmanuel Roeseler, director de Sistemas de Seguridad de IBM. Por eso uno de los retos pasa por la incorporación de tecnologías de aprendizaje automático (machine learning) y de procesamiento del lenguaje natural, lo que da paso a una nueva era de ciberseguridad, la cognitiva, que usa tecnología que es capaz de comprender, razonar y aprender. Con la gran ventaja de que un sistema cognitivo comprende y procesa la nueva información a una velocidad que está muy por encima de cualquier ser humano. Y un ejemplo paradigmático es Watson for Cyber Security, una nueva versión en cloud de la tecnología cognitiva de IBM, entrenada en el lenguaje de la seguridad, fruto de un proyecto de investigación de un año. "Hay mucha información que puede ser útil para acortar ese tiempo de respuesta. A día de hoy no se podía utilizar tecnológicamente pero con Watson será posible porque Watson aprende mucho más rápido que el ser humano, consigue procesar mucha más información que el ser humano", explica el director de sistemas de seguridad de IBM. "Pero no tiene la inteligencia de un ser humano, no aplica el sentido común, no va a poder generalizar. Va a servir para apoyar a los analistas de seguridad de las empresas para que tomen las decisiones adecuadas cuando toque tomar esas decisiones". Por tanto con sistemas como Watson se podrá procesar mucha más información y en un tiempo mucho más que razonable. "La principal ventaja de usar sistemas más avanzados es el tiempo de respuesta y el contexto. Cuanto más contexto, más fácil va a ser la decisión y con más contexto procesado vas a poder reducir el tiempo de respuesta".



Conclusión

A medida que la amenaza cibernética aumenta y evoluciona, las organizaciones se están dando cuenta de que uno de sus recursos más fuertes para luchar contra esta amenaza radica en el creciente volumen de datos a su disposición –y el poder creciente de las tecnologías para actuar sobre estos datos–. Todos estos datos contienen pistas vitales de comportamiento para identificar las amenazas y los riesgos internos y externos. Con las crecientes capacidades de analítica avanzada y predictiva, las empresas ahora tienen mejores medios tecnológicos para identificar y responder al cambiante panorama de amenazas. No cabe duda de que en el futuro, grandes herramientas de análisis de datos estarán en la primera línea de defensa, que combina el aprendizaje automático, minería de texto y el modelado de ontologías para proporcionar programas integrales e integrados de predicción, detección y disuasión y de prevención de amenazas de seguridad, de acuerdo con las últimas predicciones por el Instituto Internacional de Analytics (IIA). **cso**