Abril de 2016

Seguridad cognitiva

Desarrolle sus defensas con la seguridad que comprende, razona y aprende

IBM Security

Contenido

El nuevo imperativo

Llevamos casi un siglo programando ordenadores para resolver problemas complejos. Podemos simular el tiempo, secuenciar genomas y compartir datos al instante por todo el mundo, pero pedir a un ordenador que realice alguna tarea que el ser humano realiza a diario, como reconocer una imagen, leer un libro o explicar el significado de una poesía, ya es otra historia. Los sistemas tradicionales se quedan cortos.

Ocurre lo mismo con la seguridad. Durante décadas hemos programado ordenadores para que reconozcan virus, malware y ataques, ajustándolos continuamente para que ganen precisión, pero nunca es suficiente. Los adversarios transforman constantemente sus ataques y encuentran formas creativas para traspasar las defensas. Las organizaciones tienen que ser capaces de detectar el cambio más sutil en la actividad y analizarlo con el máximo contexto posible para distinguir y eliminar nuevas amenazas.

80 % de los datos del mundo ha sido invisible.

Hasta ahora.

Detectar ataques y comportamientos anómalos antes de que causen daños requiere supervisión constante y el máximo uso de los datos. Pero el mundo genera más de 2,5 quintillones de bytes de datos a diario, y el 80 % de ellos no está estructurado. Esto significa que están expresados en lenguaje natural – hablado, escrito o visual – que un humano puede comprender fácilmente pero los sistemas de seguridad tradicionales no. La realidad es que a diario se publican miles de blogs sobre seguridad con información detallada sobre amenazas, pero para un analista de seguridad es imposible conocer todo su contenido, y la seguridad tradicional no es capaz de analizar y aplicar dicho conocimiento como lo hace un analista.

Este es el motivo por el cual los problemas de seguridad más complicados aún requieren la intervención de personas que tomen decisiones sobre dónde actuar y qué es una falsa alarma. De hecho, los mejores profesionales de seguridad amplían su base de conocimientos a diario mediante la experiencia, hablando con compañeros, asistiendo a conferencias y siguiendo las investigaciones.

En IBM Security, estamos entrenando una nueva generación de sistemas para que comprenda, razone y aprenda sobre las amenazas de seguridad, en constante evolución. Estamos empezando a crear instinto de seguridad y experiencia en nuevas defensas que analizan informes de investigación, texto web, datos de amenazas y otros datos sobre seguridad, estructurados y sin estructurar – como hacen los profesionales de seguridad a diario – pero a una escala sin precedentes. Esta es la esencia de la seguridad cognitiva.

El resultado: los analistas recurrirán a los sistemas cognitivos para aumentar, e incluso automatizar, la comprensión de una amenaza. De esta manera, conocerán mejor los últimos ataques, y dispondrán de más tiempo para centrarse en otras cuestiones importantes.

¿Qué es la seguridad cognitiva?

Los sistemas cognitivos son sistemas de autoaprendizaje que utilizan minería de datos, aprendizaje de máquina, procesamiento del lenguaje natural e interacción ser humano–ordenador para imitar el funcionamiento del cerebro.

La seguridad cognitiva es la implementación de dos amplias funcionalidades relacionadas:

- El uso de sistemas cognitivos para analizar las tendencias de seguridad y convertir grandes volúmenes de datos estructurados y sin estructurar en información y después en conocimiento aplicable para habilitar la seguridad continua y mejorar el negocio
- El uso de tecnologías, técnicas y procesos de seguridad automatizados y basados en datos que den soporte a los sistemas cognitivos con el máximo nivel de contexto y precisión

De lo normativo a lo cognitivo

Desde la época de las primeras redes y los hackers que aparecieron poco después, la tecnología de seguridad ha ido evolucionando para detener ataques. Hasta el momento, se pueden distinguir dos eras de ciberseguridad: controles de perímetro e inteligencia en seguridad. Ambas forman los cimientos para la tercera era que está entrando—seguridad cognitiva.

Controles de perímetro: seguridad que delimita (antes del 2005)

Empezamos con defensas estáticas para proteger o limitar el flujo de datos, incluyendo cortafuegos, software antivirus y pasarelas web. La evolución de la seguridad de la información empezó como un ejercicio de conformidad normativa con el objetivo de bloquear y restringir el acceso a información sensible mediante contraseñas y un rango de estrategias de control de acceso. El éxito consistía en pasar una auditoría. Aunque las defensas de perímetro aún se aplican, por sí solas no son suficientes en el entorno actual.

Inteligencia en seguridad: seguridad que le ayuda a pensar (a partir del 2005)

Con el tiempo hemos avanzado hacia sistemas de supervisión sofisticados que recopilan y peinan grandes cantidades de datos para descubrir vulnerabilidades y priorizar ataques potenciales. Este método se centra en información en tiempo real para detectar actividad sospechosa. Actualmente, la inteligencia en seguridad engloba la recopilación en tiempo real, la normalización y el análisis de datos estructurados, generados por usuarios, aplicaciones y la infraestructura.

La inteligencia en seguridad utiliza analítica para detectar desviaciones de patrones regulares, descubrir cambios en el tráfico de red e identificar actividades que superan los niveles definidos. En una infraestructura de inteligencia en seguridad, la analítica se aplica a grandes cantidades de información a fin de comprender los datos de la empresa en contexto y priorizar tareas rutinarias. Al determinar las desviaciones importantes, la inteligencia en seguridad no solo ayuda a acelerar la detección de puntos comprometidos, sino que también reduce los falsos positivos para ahorrar tiempo y recursos.

Seguridad cognitiva: seguridad que comprende, razona y aprende a escala (a partir del 2015)

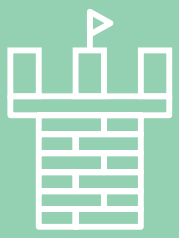
Basada en inteligencia en seguridad, que aplica la analítica de big data, la seguridad cognitiva se caracteriza por su tecnología capaz de comprender, razonar y aprender. Los sistemas cognitivos habilitan el acceso a una cantidad muy superior de datos de seguridad relevantes, y pueden procesar e interpretar el 80 % de los datos actuales no estructurados, como el lenguaje escrito y hablado.

Tras ingerir un corpus de conocimiento, tratado por expertos en una materia concreta, un sistema de seguridad cognitiva se entrena introduciéndole pares de pregunta-respuesta. Los profesionales de la seguridad mejoran este “conocimiento” de máquina interactuando con el sistema, con feedback sobre la precisión de las respuestas del sistema. Una diferencia clave: un sistema cognitivo comprende y procesa nueva información a una velocidad muy superior a la de cualquier ser humano. Por tanto, ahora se pueden entrenar las defensas técnicas para que analicen miles de informes de investigación, material de conferencias, artículos académicos, noticias, publicaciones de blogs y alertas del sector—a diario.

La observación de sucesos y comportamientos por parte de los sistemas cognitivos —distinguiendo los buenos de los malos—refuerza cada vez más la capacidad de utilizar las defensas integradas para bloquear nuevas amenazas. La seguridad cognitiva ayuda a que los analistas de seguridad sean más efectivos y acelera la respuesta ante amenazas emergentes, además de cubrir las carencias en las competencias de seguridad actuales, con mayores niveles de confianza y control de riesgos. Vea la figura 1.

Cronología de la historia de la seguridad

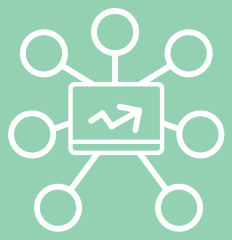
Controles de perímetro



Antes del 2005

- Defensas estáticas
- Protecciones de contraseña
- Centrada en la conformidad
- Éxito = pasar una auditoría

Inteligencia en seguridad



A partir del 2005

- Observación de la actividad en tiempo real
- Centrada en desviaciones de patrones conocidos
- Capacidad para priorizar posibles amenazas
- Reactiva y basada en reglas

Seguridad cognitiva

A partir del 2015

- Razonamiento que simula el pensamiento humano
- Capacidad para analizar datos estructurados y sin estructurar para comprender comportamientos y significados
- Aprendizaje automatizado basado en inteligencia continua sobre amenazas
- Foco proactivo mediante relaciones

Figura 1

En definitiva, los sistemas cognitivos se integran en una infraestructura basada en los fundamentos de la seguridad tradicional. La inteligencia en seguridad se mantiene como pilar de la seguridad cognitiva, la cual nos proporciona un modo de clasificar la detección y la inteligencia de amenazas, así como información aplicable, a una velocidad y escala sin precedentes.

Figura 2

Como la inteligencia en seguridad y la analítica de big data normalmente no están estructurados, el elemento cognitivo aporta un nivel adicional de comprensión importante para conocer qué sucede y cómo actuar. Gracias a esta combinación, contará con la máxima protección disponible para su entorno de seguridad. Vea la figura 2.

La ventaja de la seguridad cognitiva

Los sistemas de seguridad programables tradicionales responden a solicitudes, toman determinaciones y analizan datos según unos parámetros predefinidos. Los sistemas cognitivos interpretan datos, añaden a su base de conocimiento prácticamente todas las interacciones, sopesan probabilidades en base al conocimiento y le ayudan a tomar medidas teniendo en cuenta variables relevantes.

Mientras que la generación actual de sistemas es reactiva—detectan y responden a anomalías o ataques— la seguridad cognitiva es proactiva. De carácter progresivo y multitarea, los sistemas cognitivos peinan en busca de vulnerabilidades, conectan puntos, detectan discrepancias y rebuscan en miles de millones de sucesos para alimentar la base de conocimiento aplicable.

Las soluciones cognitivas no solo generan respuestas, sino también hipótesis, razonamiento basado en pruebas y recomendaciones. Ahora se ha habilitado la capacidad de interpretar el 80 % de los datos no estructurados, que antes eran inaccesibles para los sistemas existentes, e integrarlos con datos estructurados procedentes de infinidad de orígenes y ubicaciones. En una economía global en la que el valor reside cada vez más en la información, los datos son una de las materias primas más abundantes, valiosas y complejas del mundo. Ahora ya disponemos de los medios para analizar datos estructurados y sin estructurar, y de las características y patrones de extracción continua para proporcionar contexto en tiempo real que permite mejorar la toma de decisiones.

Los tres pilares de la seguridad cognitiva sobre los que se basan los patrones de pensamiento como el ser humano consisten en:

1. **Comprender** y dar sentido a datos no estructurados y texto en lenguaje natural. Esto incluye la capacidad de ingerir y procesar información a partir de la "lectura" de libros, informes, blogs y datos relevantes del sector, la "visualización" de imágenes y la "escucha" del habla natural en su contexto.
2. **Razonar** en base a la capacidad de interpretar y organizar información y ofrecer explicaciones de qué significa, junto con una base lógica para realizar conclusiones.
3. **Aprender** de forma continua de los datos acumulados y los conocimientos extraídos de las interacciones.

Mayor alcance y profundidad

Una estrategia centrada en detectar malware, amenazas maliciosas, valores atípicos y anomalías tiende a generar demasiados falsos positivos. Esta es la ventaja que presenta el enfoque multidimensional que aplican los sistemas cognitivos.

En el entorno actual, la capacidad de distinguir entre blanco y negro es solo uno de los aspectos de la experiencia que exige una infraestructura de seguridad integrada. El área "gris" es cada vez mayor, y es donde entran en juego los sistemas cognitivos.

Reforzados con altos niveles de intuición, inteligencia y conocimiento, los sistemas cognitivos están diseñados para ser mejorados de forma continua con datos que ayuden a distinguir comportamientos aceptables de variaciones sutiles que podrían indicar amenazas emergentes. El resultado es una perspectiva más amplia con un enfoque general más proactivo.

Cubrir las carencias de habilidades

No son solo nuestros sistemas los que afrontan el reto de mantener el entorno de seguridad actual, sino que el personal también es responsable. Se estima que el número de puestos vacantes en seguridad de la información asciende a 208.000 y se espera que alcance los 1.500 millones en 2020. La seguridad cognitiva puede ayudar.

Los sistemas cognitivos, como recurso escalable para dar soporte a la capacidad humana, funcionan como extensiones de los departamentos de seguridad, con frecuencia escasos de personal. Esta nueva dimensión resulta vital, porque ya no basta con vigilar atentamente lo que ocurre en nuestro sistema. Es necesario supervisar las amenazas a escala global para prepararse ante posibles ataques. Los sistemas cognitivos pueden acceder a redes de intercambio globales que analizan cientos de miles de sucesos por segundo, para miles de clientes de todo el mundo.

Los sistemas cognitivos facilitan el trabajo de los analistas de seguridad, proporcionando comunicaciones centradas en el ser humano, como visualizaciones avanzadas, análisis de vulnerabilidades interactivo, evaluación de riesgos, reparación y posible asignación. Asimismo, los sistemas cognitivos serán capaces de detectar anomalías y lógica deficiente, además de proporcionar razonamiento basado en pruebas. Esto permite a los analistas analizar resultados alternativos y mejorar la toma de decisiones.

Casos de uso:

Sistemas cognitivos activados

Mejore la capacidad de los analistas del SOC

Los sistemas cognitivos comprenden una gran cantidad de datos estructurados y sin estructurar, lo que ayuda a incrementar rápidamente el valor de un analista junior del nivel 1 al 2 o 3. Los sistemas cognitivos automatizan la ingesta de información – como informes de investigación y mejores prácticas – para generar resultados en tiempo real. Antes, este conocimiento solo podía obtenerse con años de experiencia.

Acelere la respuesta con inteligencia externa

Cuando aparezca la nueva vulnerabilidad Heartbleed, se publicarán artículos sobre cómo protegerse de ella. Aunque aún no haya ninguna firma disponible, existe un lenguaje natural online que le ayudará a responder a esta pregunta. Los sistemas cognitivos pueden avanzar rápidamente para descubrir cómo protegerse ante el próximo ataque.

Identifique amenazas con analítica avanzada

Los sistemas cognitivos pueden utilizar métodos de análisis como el aprendizaje de máquina, la agrupación en clúster, la minería de gráficos y el modelado de relaciones de entidades para identificar amenazas potenciales. Aceleran la detección de comportamientos de riesgo de los usuarios, la exfiltración de datos y la detección de malware antes de que produzcan daños.

Refuerce la seguridad de las aplicaciones

Los sistemas cognitivos comprenden el contexto semántico de su analítica y datos, analizando a su vez código y estructuras de código. Pueden detectar miles de vulnerabilidades y refinar los resultados hasta reducirlos a un conjunto pequeño de elementos procesables– y conducirle hasta las ubicaciones del código donde poder corregirlos.

Mejore el riesgo empresarial

En el futuro, los sistemas cognitivos podrían analizar corpus de interacciones, la naturaleza de estas interacciones y su susceptibilidad a desarrollar perfiles de riesgo para las organizaciones, acciones corporativas, formación y reeducación. Los sistemas cognitivos podrían utilizar el procesamiento del lenguaje natural para encontrar datos sensibles de una organización y clasificarlos.

El futuro: revertir la economía de la ciberdelincuencia

Los sistemas cognitivos pueden analizar las características de grandes conjuntos de software malicioso —conocido como malware— para detectar similitudes sutiles. Esta acción es clave porque aunque existe una gran diversidad de software malicioso, los grupos de ciberdelincuencia evolucionan su código, es decir, gran parte del malware activo está relacionado con malware anterior. Gracias a los sistemas cognitivos, podemos analizar miles de características de un archivo ejecutable sospechoso y agruparlas en clústeres para revelar patrones, e incluso sin que una persona llegue a saber qué características eran o cómo o por qué eran similares, el sistema puede identificar un patrón que ayude a descubrir y clasificar nuevas variantes de malware.

A medida que crece la comunidad de seguridad cognitiva, y se reduce la viabilidad de nuevos ataques, la ciberdelincuencia va entrando en una nueva realidad económica. Desarrollar malware que eluda la detección resultará cada vez más complejo y costoso. De acuerdo con el estudio de 2015 sobre los costes de las filtraciones de datos realizado por Ponemon Institute, 256 días es el promedio de tiempo que tardan las organizaciones en detectar amenazas persistentes avanzadas; y 6,5 millones de dólares es el coste medio estimado de una filtración de datos en Estados Unidos. La seguridad cognitiva permitirá a los analistas de seguridad detectar avisos tempranos de posibles ataques y acelerar su detección. Los ciberdelincuentes cada vez lo tendrán más difícil para obtener beneficios.

La informática cognitiva está impulsando un cambio transformacional al utilizar no solo los datos, sino el significado, el conocimiento, los flujos de procesos y la progresión de la actividad a una gran velocidad y alcance. Las organizaciones que adopten funcionalidades cognitivas gozarán de una importante ventaja competitiva.

Integración y experiencia para un ecosistema cognitivo

La integración y la experiencia son dos aspectos esenciales para la seguridad. Se aplican demasiadas prácticas de seguridad basadas en una recopilación de productos específicos que no están integrados y no proporcionan la visibilidad y la inteligencia aplicable necesarias para responder rápidamente.

La integración no es completa hasta que las funcionalidades de dominio interactúan y se comunican entre ellas en todo su entorno de TI híbrido, extendiendo su alcance más allá de su empresa, a través de todo el ecosistema. Una buena integración le permitirá obtener la visibilidad que necesita para responder con rapidez a los incidentes de seguridad cuando se produzcan. La integración le permite hacer más con menos, lo que resulta clave para cubrir las carencias de habilidades en seguridad.

Cada día se descubren nuevas amenazas, por lo que compartir la inteligencia de amenazas y la experiencia en seguridad es de vital importancia. Si no dispone de una buena contribución de expertos en un conjunto de soluciones cognitivas, pronto se quedará rezagado. IBM X-Force Exchange actualmente cataloga información sobre más de 88.000 vulnerabilidades, más de 25.000 millones de páginas web y datos de 100 millones de puntos finales—posibilitando una cobertura global y en tiempo real de experiencia aplicable al momento.

Cómo puede ayudarle IBM

La era cognitiva está solo en sus inicios, pero IBM dispone de la fuerza intelectual y financiera para liderar esta revolución con seguridad. Más de 7.500 profesionales de IBM Security, en 36 centros de seguridad de todo el mundo, supervisan 133 países y 35.000 millones de sucesos a diario. La inversión de IBM en tecnologías cognitivas se remonta unas décadas atrás, pero se ha percibido una gran progresión en los últimos cinco años —la capacidad de procesar el lenguaje natural, la capacidad de procesar voz e imágenes y la capacidad de convertir datos no estructurados en herramientas como gráficos de conocimiento fácilmente consultables. IBM adoptará la tecnología cognitiva para mejorar los casos de uso de seguridad de forma continua y aportar información a los analistas de seguridad.

IBM Security ya integra funcionalidades cognitivas en soluciones actuales. El aprendizaje de máquina se utiliza para incrementar la precisión en la detección de vulnerabilidades y priorizar las vulnerabilidades para acelerar la capacidad de respuesta. El aprendizaje de comportamientos se utiliza para anticipar y detectar proactivamente anomalías en torno a amenazas que se producen en la red.

IBM Security ofrece protección completa y un enfoque de inmunidad que abarca analítica detallada, identidad y acceso, fraude avanzado, datos, aplicaciones, red, puntos finales, cloud, móviles e investigación. Cada una de estas plataformas se beneficiará de las funcionalidades cognitivas de IBM. Si le interesan los beneficios que aporta la seguridad cognitiva, considere la adopción de las plataformas de IBM, que se innovarán e implementarán tecnologías cognitivas.

3 pasos a seguir

1. Conozca mejor cómo aplicar funcionalidades cognitivas para superar amenazas.

2. Desarrolle una hoja de ruta para mejorar la seguridad y prepararse para la era cognitiva.

3. Promueva la integración en su infraestructura de seguridad.

Información adicional

Póngase en contacto con su representante de IBM o IBM Business Partner, o bien visite http://www-03.ibm.com/security/es/es/

Acerca de IBM Security

IBM Security ofrece uno de los portfolios más avanzados e integrado de productos y servicios de seguridad empresarial. El portfolio, con el apoyo del desarrollo y la investigación de IBM X-Force de renombre internacional, proporciona inteligencia en seguridad para ayudar a las organizaciones a proteger globalmente a sus trabajadores, infraestructuras, datos y aplicaciones, con soluciones para la gestión de acceso e identidades, seguridad de bases de datos, desarrollo de aplicaciones, gestión de riesgos, gestión de puntos finales, seguridad de red, etc. Estas soluciones permiten a las organizaciones gestionar e implementar de forma efectiva la seguridad integrada para móviles, cloud, contenido de redes sociales y otras arquitecturas de negocio de la empresa. IBM dirige una de las mayores organizaciones de investigación, desarrollo y distribución de seguridad, supervisa 35.000 millones de sucesos de seguridad al día en 133 países y cuenta con más de 3.700 patentes de seguridad.

Además, IBM Global Financing puede ayudarle a adquirir las funcionalidades de software que necesite su negocio del modo más rentable y estratégico posible. Nos asociamos con clientes con crédito positivo para personalizar una solución financiera que se adapte a sus objetivos de negocio y desarrollo, permita una gestión de efectivo eficiente y mejore el coste total de propiedad. Financie su inversión en TI e impulse su negocio con IBM Global Financing. Para obtener más información, visite ibm.com/financing.

IBM Security
Route 100
Somers, NY 10589

Producido en los Estados Unidos
Abril de 2016

SEW03134ESES-00