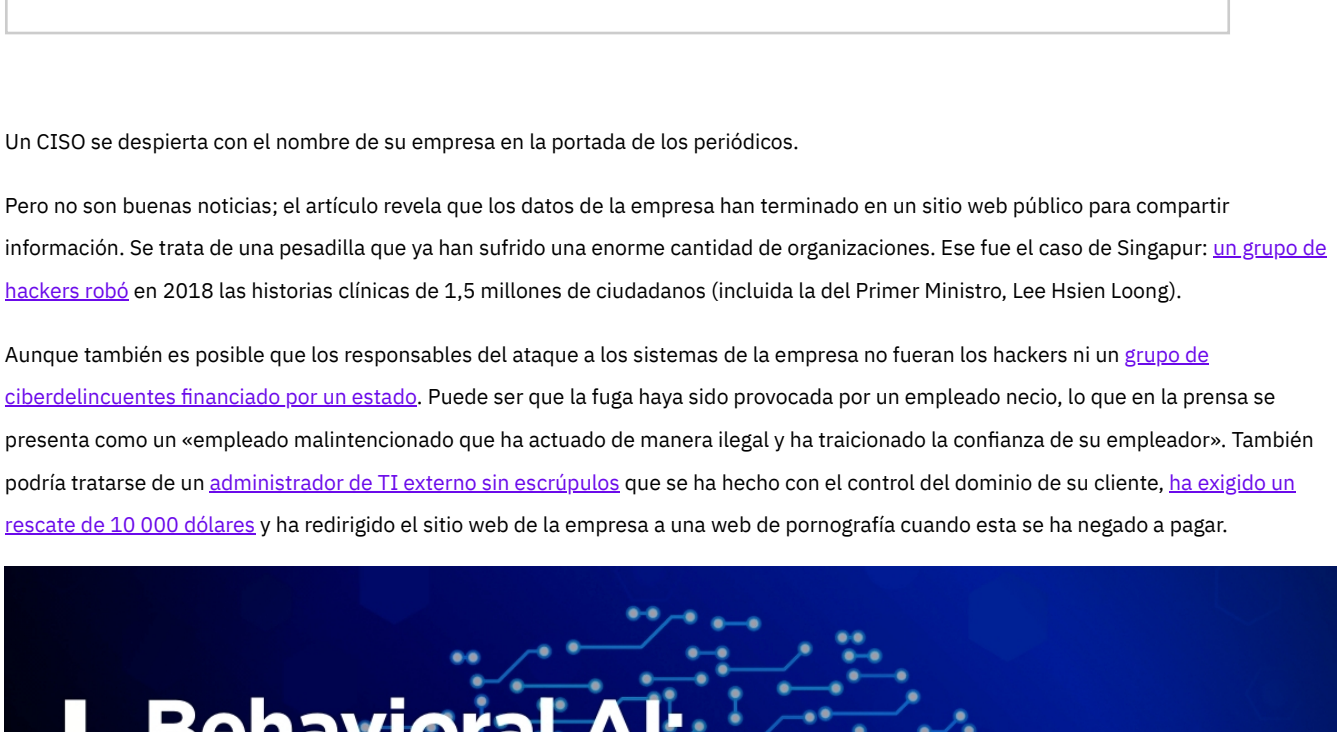


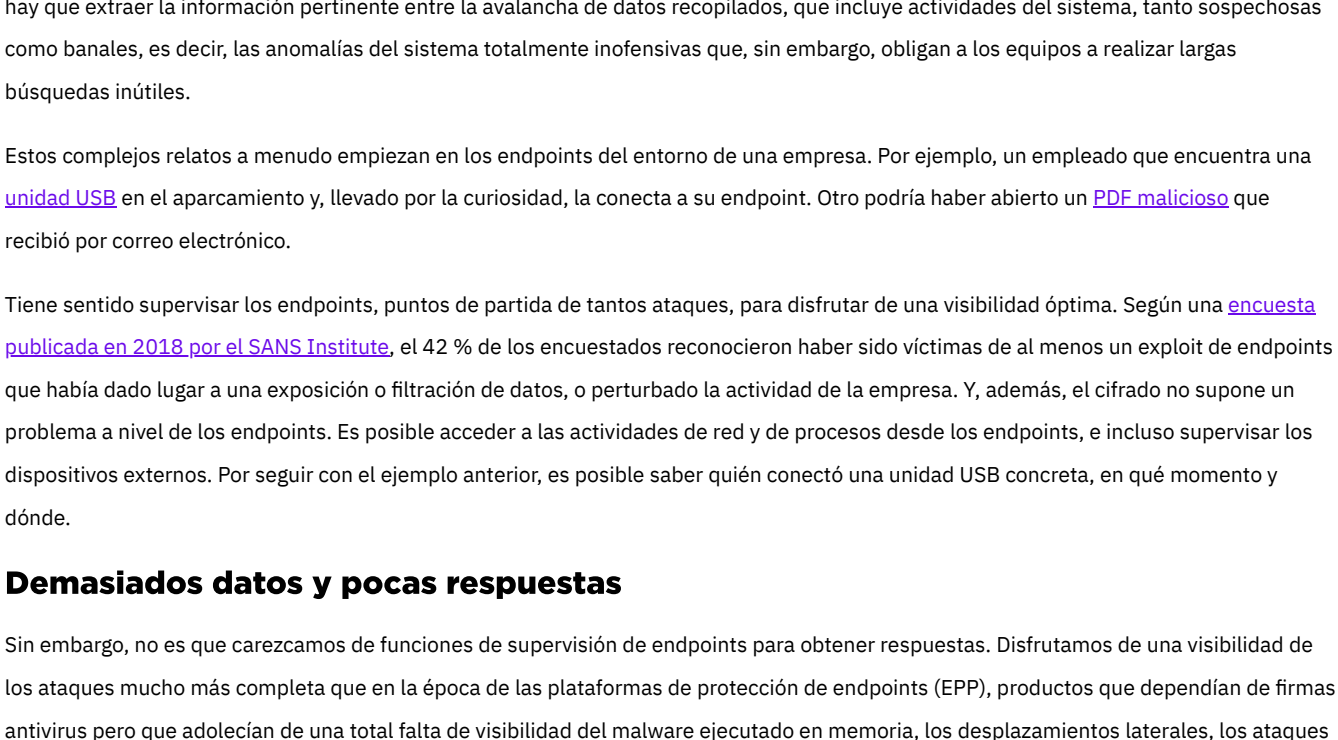
Inteligencia artificial basada en el comportamiento: posibilidades ilimitadas a la hora de proteger a las empresas

agosto 3, 2020
by Lisa Vaas

Un CISO se despierta con el nombre de su empresa en la portada de los periódicos.

Pero no son buenas noticias; el artículo revela que los datos de la empresa han terminado en un sitio web público para compartir información. Se trata de una pesadilla que ya han sufrido una enorme cantidad de organizaciones. Ese fue el caso de Singapur: un grupo de hackers robó en 2018 las historias clínicas de 1,5 millones de ciudadanos (incluida la del Primer Ministro, Lee Hsien Loong).

Aunque también es posible que los responsables del ataque a los sistemas de la empresa no fueran los hackers ni un grupo de ciberdelincuentes financiado por un estado. Puede ser que la fuga haya sido provocada por un empleado necio, lo que en la prensa se presenta como un «empleado malintencionado que ha actuado de manera ilegal y ha traicionado la confianza de su empleador». También podría tratarse de un administrador de TI externo sin escrúpulos que se ha hecho con el control del dominio de su cliente, ha exigido un rescate de 10 000 dólares y ha redirigido el sitio web de la empresa a una web de pornografía cuando esta se ha negado a pagar.



La casuística es interminable y las consecuencias son siempre desastrosas, tanto para la ciberseguridad como para la propia empresa que, muy a su pesar, sale en las noticias y con frecuencia llama la atención de las fuerzas de seguridad. Si bien los periodistas y las autoridades se interesan sobre todo por los autores del ataque, sus métodos y sus objetivos, lo más importante para el centro de operaciones de seguridad (SOC) de la empresa es conocer los antecedentes y el relato a fin de reconstruir el ataque, identificar a los responsables y aplicar las medidas correctivas necesarias para resolver el problema, si todavía no se ha hecho. Este relato es difícil de obtener porque a menudo hay que extraer la información pertinente entre la avalancha de datos recopilados, que incluye actividades del sistema, tanto sospechosas como banales, es decir, las anomalías del sistema totalmente inofensivas que, sin embargo, obligan a los equipos a realizar largas búsquedas inútiles.

Estos complejos relatos a menudo empiezan en los endpoints del entorno de una empresa. Por ejemplo, un empleado que encuentra una unidad USB en el aparcamiento y, llevado por la curiosidad, la conecta a su endpoint. Otro podría haber abierto un PDF malicioso que recibió por correo electrónico.

Tiene sentido supervisar los endpoints, puntos de partida de tantos ataques, para disfrutar de una visibilidad óptima. Según una encuesta publicada en 2018 por el SANS Institute, el 42 % de los encuestados reconocieron haber sido víctimas de al menos un exploit de endpoints que había dado lugar a una exposición o filtración de datos, o perturbado la actividad de la empresa. Y, además, el cifrado no supone un problema a nivel de los endpoints. Es posible acceder a las actividades de red y de procesos desde los endpoints, e incluso supervisar los dispositivos externos. Por seguir con el ejemplo anterior, es posible saber quién conectó una unidad USB concreta, en qué momento y dónde.

Demasiados datos y pocas respuestas

Sin embargo, no es que carezcamos de funciones de supervisión de endpoints para obtener respuestas. Disfrutamos de una visibilidad de los ataques mucho más completa que en la época de las plataformas de protección de endpoints (EPP), productos que dependían de firmas antivirus pero que adolecían de una total falta de visibilidad del malware ejecutado en memoria, los desplazamientos laterales, los ataques de malware sin archivos o de día cero.

Pero aquí está el problema: las plataformas EPP pueden proteger los endpoints, pero no ofrecen a las empresas visibilidad de las amenazas. Las herramientas EDR (Endpoint Detection and Response) de primera generación estaban diseñadas para ofrecer la visibilidad que las plataformas EPP sencillamente no proporcionaban. Esta primera generación de herramientas EDR, llamémosla EDR pasiva, era capaz de proporcionar datos, pero no contexto. Es como tener todas las piezas del rompecabezas, pero ninguna vista del conjunto.

Con ayuda de una supervisión de endpoints integrada y pasiva, por ejemplo, podríamos ver que las entradas del registro de eventos de Windows detectaron un compromiso de unidad USB, que dio lugar a la ejecución de un script PowerShell desde un teclado virtual, que el ataque pudo haber utilizado técnicas avanzadas, como el borrado de registros, que instaló una puerta trasera para asegurar la persistencia, que continuó con el robo de credenciales y su posterior uso para conectarse, que, en un momento dado, no pudo iniciar sesión, que escaló los privilegios, borró los registros, añadió un nuevo usuario local y después lo admitió en el grupo de administradores, y así sucesivamente. ¡Buena suerte al intentar resolverlo!

Una solución así puede parecer fantástica en una demostración, pero ¿qué pasa con el uso diario? ¿Quién es capaz de entender toda esta información? Sin duda, muy pocos analistas de seguridad especializados y cualificados. Y, desafortunadamente, no abundan. Además, los pobres también tienen derecho a dormir de vez en cuando. Dicho de otra forma, cuando un ataque se produce de madrugada, los ciberdelincuentes disfrutan de mucho más tiempo de permanencia hasta que los analistas se ponen a trabajar, consiguen descifrar los eventos y determinar los objetivos, el responsable del ataque y el método utilizado.

Lo que interesa a los CISO no es disponer de todos y cada uno de los datos inconexos sobre el ataque. Más bien se parecería a una partida de Cluedo: ¿es el culpable el Coronel Mostaza en la habitación de estudio, un contratista utilizando una unidad USB o un grupo de ciberdelincuentes financiado por un estado? ¿Se ha neutralizado ya la amenaza? Y, de ser así, ¿cuánto tiempo ha estado activa? ¿Cuál de los escasos analistas con los que cuenta un SOC está analizando ese tsunami de datos que recopila la solución EDR pasiva?

¿Qué es la «inteligencia artificial basada en el comportamiento» y cómo puede ayudar?

¿Qué ocurre tras un ataque? El relato puede desarrollarse de dos maneras. En el primer caso (y más problemático) los analistas de seguridad tienen que examinar cuidadosamente todas las alertas y anomalías generadas por la solución EDR pasiva. Esas investigaciones requieren tiempo y exigen un cierto nivel de experiencia: un bien escaso, si tenemos en cuenta lo difícil que es encontrar, formar y retener personal que tenga las competencias necesarias para utilizar las plataformas de seguridad y los conocimientos para separar el grano de la paja o, lo que es lo mismo, los verdaderos exploits de los errores aleatorios.

El segundo caso consiste en reconstruir el ataque: la contextualización de todos los datos dispares para hacer una narración lógica y coherente. En SentinelOne, este enfoque lo encarna la tecnología ActiveEDR. Este modelo de inteligencia artificial basada en comportamientos evita a la empresa tener que depender exclusivamente de las competencias de analistas, a menudo escasos, y, además, actúa ininterrumpidamente, grabando y poniendo en contexto todo lo que ocurre en cada dispositivo que se conecta a la red.

El motor de inteligencia artificial basada en el comportamiento de SentinelOne crea lo que llamamos relato, o reconstrucción, del incidente: una serie de huellas que permiten a una empresa rastrear los incidentes para averiguar quién es el culpable de un indicador de peligro. Es una solución EDR, pero no la EDR pasiva que posiblemente ya conoce. La función de una solución EDR tradicional consiste en buscar una actividad aislada e intentar correlacionarla con otra, y luego con otra, y así sucesivamente. Este largo y laborioso enfoque, que precisa de un personal altamente cualificado, intenta tener una imagen completa de la situación a posteriori.

Con la tecnología ActiveEDR de SentinelOne *es la máquina la que hace el trabajo,* no el analista. Para ello, rastrea y contextualiza cada evento que ocurre en el dispositivo e identifica las actividades maliciosas en tiempo real, automatizando las respuestas necesarias. Cuando, en su caso, el analista quiere intervenir, ActiveEDR le permite rastrear fácilmente las amenazas mediante búsquedas completas a partir de un solo indicador de peligro.

A diferencia de otras soluciones EDR, ActiveEDR no necesita una conexión a la nube para detectar una amenaza, lo que reduce el tiempo de permanencia hasta la ejecución. El agente inteligente instalado en cada dispositivo no necesita una conexión a la nube para tomar una decisión. Reconstruye constantemente el desarrollo de cada incidente que ocurre en el endpoint y, si detecta un comportamiento malicioso, no solo puede neutralizar los procesos y archivos maliciosos, sino también bloquear por completo el relato (e incluso revertirlo).

¿Por qué la función ActiveEDR es mejor a la hora de detener ataques con y sin archivos?

Los ciberdelincuentes actuales han encontrado la manera de dejar de depender de los archivos y no dejan ninguna huella, ya que utilizan malware sin archivos activos en memorias para eludir la mayoría de las soluciones de seguridad, excepto las más sofisticadas. Pero como ActiveEDR hace un seguimiento de todo, le ofrece la manera de detectar a los ciberdelincuentes que posiblemente ya tengan credenciales en su entorno y que utilizan las tácticas LotL (Living-off-the-land, o que aprovechan para sus ataques los recursos existentes). El término se refiere a ataques sin archivos y sin malware que emplean las herramientas nativas y legítimas de un sistema para hacer su trabajo sucio, con lo cual se camuflan en la red y se ocultan entre los procesos legítimos para abusar de los sistemas con total impunidad.

Inteligencia artificial basada en el comportamiento: un caso real

A continuación, presentamos un caso real de este tipo de ataque: la policía se pone en contacto con usted para advertirle de que las credenciales de su empresa están en un sitio web público para compartir datos, como Pastebin. Desea saber cómo han llegado ahí y efectúa una búsqueda mediante el módulo de caza de amenazas DeepVisibility. DeepVisibility es un producto optimizado por la tecnología Storyline de SentinelOne, que permite a los usuarios rastrear rápidamente las amenazas, con la posibilidad de buscar las referencias, en este caso las referencias a Pastebin.

Con Storyline, cada agente inteligente autónomo instalado en el endpoint crea un modelo de infraestructura de su endpoint y un comportamiento de ejecución en tiempo real, y le asigna un ID de Storyline, es decir, un ID atribuido a un grupo de eventos relacionados. Al buscar «Pastebin», encontrará un ID de Storyline que puede llevarle rápidamente a todos los procesos, archivos, hilos, subprocesos, eventos y otros datos relacionados que correspondan a esa búsqueda única. DeepVisibility devuelve datos contextualizados completos que le permiten comprender rápidamente el origen de una amenaza, incluido todo su contexto, relaciones y actividades.

Cada agente puede corregir los efectos del ataque del endpoint en el que está instalado, automática o manualmente; puede restaurar el sistema, desconectarlo de la red o ejecutar un shell remoto en el sistema. La operación puede realizarse automáticamente, con un simple clic. Se lleva a cabo en cuestión de segundos, no depende de la nube, y no requiere que se suban datos para que los analicen expertos. No se requiere tampoco una solución de análisis en la nube, ya que el agente se encarga de todo.

La automatización del máximo de tareas permite resolver múltiples problemas. Por un lado, al identificar los comportamientos maliciosos, la solución detecta fácilmente los ataques basados en archivos sin necesidad de utilizar firmas. Por otro, puede impedir y predecir los ataques sin archivos.

La protección de endpoints de SentinelOne funciona en la etapa anterior a la ejecución para detener un ataque antes de que se ejecute, ya se trate de un PDF o de un documento Word infectado, o de cualquier otra amenaza. El primer paso consiste en analizar la actividad para determinar si es anormal. Si lo es, la amenaza se pone en cuarentena. Si el código supera la primera prueba y empieza a ejecutarse, ActiveEDR entra en juego. Este mecanismo autónomo de caza de amenazas, que incluye funciones de detección e intervención del agente, busca comportamientos anormales. Por ejemplo, busca acciones de los usuarios, como la apertura de un archivo Word que generará un script PowerShell para recuperar algo de Internet. En la mayoría de los casos, eso no es un comportamiento normal y adecuado. ActiveEDR observa el comportamiento mientras se ejecuta y supervisa todos los eventos que ocurren en el sistema operativo como un relato, de principio a fin, tanto si se desarrollan en el espacio de un segundo, de un mes o más. La tecnología evalúa continuamente el comportamiento para determinar si en un momento dado se ha «vuelto malicioso».

El toque humano, con ayuda de la inteligencia artificial basada en el comportamiento

Esto está bien, pero no es suficiente, porque ninguna solución puede interceptarlo o detectarlo todo. Es aquí donde interviene la caza de amenazas de ActiveEDR —la función responsable de la superioridad de SentinelOne en materia de detección de ataques con o sin archivos.

Imaginemos que ha encontrado un dispositivo que se ha comunicado varias veces con Pastebin. Al hacer clic en el ID de Storyline en la consola de SentinelOne, accede al relato completo del ataque, con el contexto pertinente, un diagrama detallado del origen del ataque y una cronología arbórea de los procesos generados: apertura de un documento de Microsoft Word, seguida de la creación de un script Windows PowerShell, que a su vez generó siete procesos más. Storyline incluye incluso argumentos de línea de comandos completos, que es lo que los investigadores necesitan para comprender perfectamente el ataque. La solución ofrece el contexto íntegro del ataque, generado no por un equipo completo de respuesta a incidentes, sino, por una sola consulta.

Claramente, tener a mano un asistente basado en la inteligencia artificial (concretamente, un agente de inteligencia artificial instalado en cada dispositivo conectado a la red) le permite ahorrar un tiempo precioso, ya que evita a la empresa tener que contar exclusivamente con recursos humanos para analizar eventos que, en ocasiones, son insignificantes.

Duerma tranquilo, nosotros nos encargamos

¿No ha llegado la hora de dejar de reaccionar precipitadamente? Ahora, es posible.

La inteligencia artificial basada en el comportamiento puede configurarse para limitar automáticamente los riesgos, lo que verdaderamente marca la diferencia. La tecnología es capaz de tomar decisiones a nivel del dispositivo, sin depender de la nube ni de la intervención humana, e indicar al agente lo que hay que hacer. Si se define ActiveEDR para la «detección», recibirá advertencias contextualizadas. En cambio, si lo configura para la «protección», el documento Word infectado será sencillamente bloqueado. No es necesaria la intervención humana. Cuando un usuario intenta abrir el archivo Word, la amenaza se detecta, se bloquea y se elimina rápidamente. Si ActiveEDR se ha configurado para la protección, la reconstrucción del ataque indicará que no consiguió llegar lejos: fue bloqueado antes de que consiguiera comunicarse con el exterior.

Dado que los agentes con inteligencia artificial basada en el comportamiento se incorporan en cada endpoint, los comportamientos maliciosos pueden bloquearse inmediatamente. Más adelante, si decide que una actividad o proceso no debía bloquearse, puede restaurarlo sin ningún problema. Además, a diferencia de las personas, la inteligencia artificial basada en el comportamiento de SentinelOne, ActiveEDR, no necesita dormir y no deja de trabajar a las 5 de la tarde.

La mitigación automática de riesgos mediante la inteligencia artificial basada en el comportamiento le evita, por tanto, problemas como la filtración de datos, la publicidad desfavorable y las llamadas de las fuerzas de seguridad.

Si desea obtener más información sobre la inteligencia artificial basada en el comportamiento de SentinelOne y acerca de cómo puede ayudar a proteger su empresa, póngase en contacto con nosotros hoy mismo o solicite una demostración gratuita.

¿Te gusta este artículo? Síguenos en LinkedIn, Twitter, YouTube or Facebook para ver el contenido que publicamos.

Lee acerca de Ciberseguridad

- MITRE Manía: Su guía para comprender el posicionamiento de proveedores y su importancia