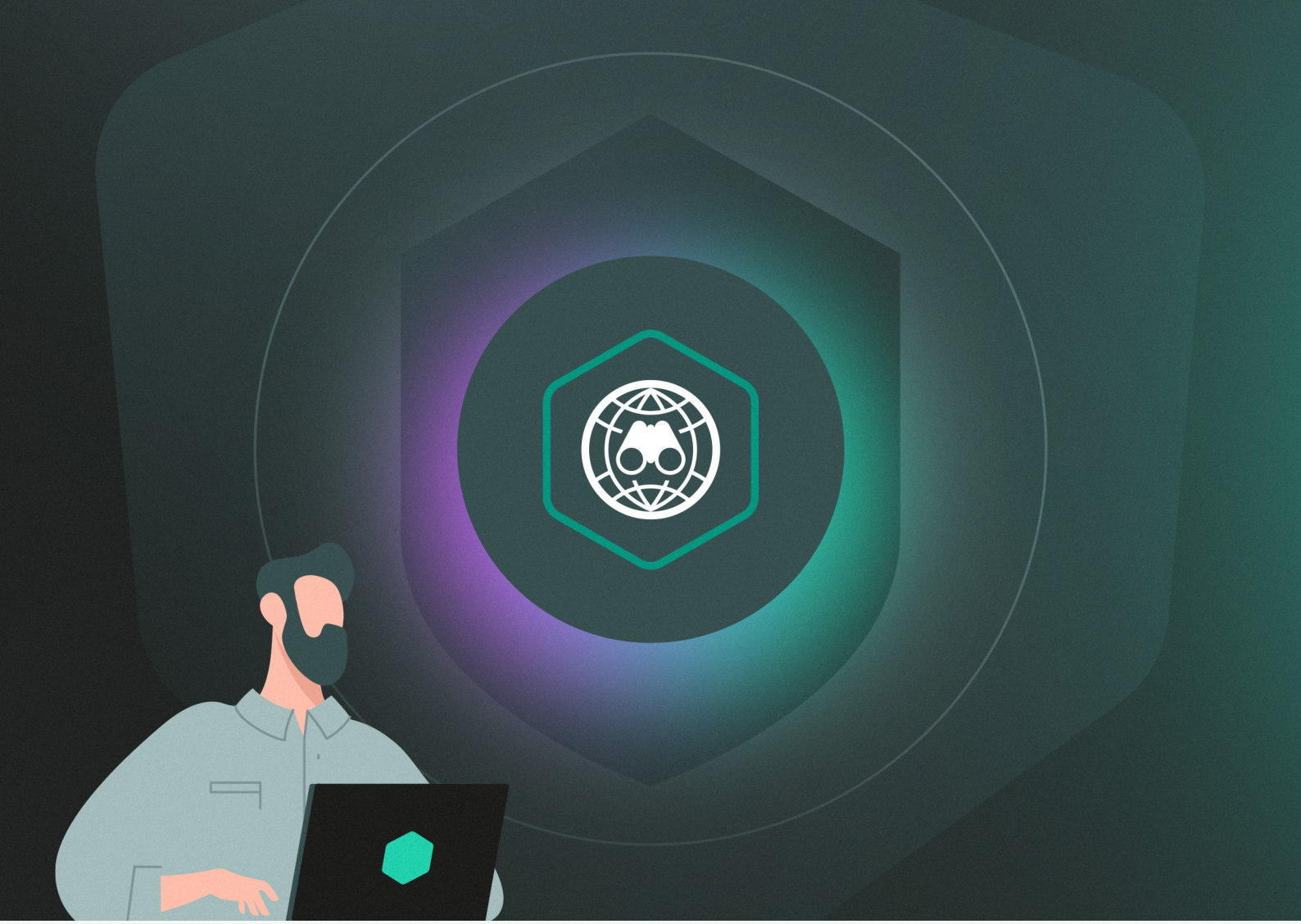

Kaspersky Threat Intelligence

Evaluación de fuentes de inteligencia frente a amenazas

kaspersky PREPARADOS PARA EL FUTURO

Obtenga más información en kaspersky.es
#bringonthefuture

Introducción

Con la superficie de ataque en expansión y la creciente sofisticación de las amenazas, no basta con reaccionar ante un incidente. Los entornos cada vez más complejos ofrecen múltiples oportunidades para los atacantes. Cada sector y organización debe proteger sus datos únicos y utilizar su propio conjunto de aplicaciones, tecnologías, etc. Todo esto introduce una enorme cantidad de variables en los posibles métodos de ejecución de un ataque, de los que surgen variaciones nuevas a diario.

En estos últimos dos años, hemos observado que los límites entre los distintos tipos de actores de amenazas se volvieron más difusos. Los métodos y las herramientas que antes suponían una amenaza para un número limitado de organizaciones se han extendido al mercado en general. Un caso de este tipo fue el volcado de código de Shadow Brokers, que puso exploits avanzados a disposición de grupos delictivos que, de otro modo, no habrían tenido acceso a un código de tal sofisticación. Otro ejemplo es la aparición de campañas de amenazas persistentes avanzadas (APT) centradas no solo en el ciberespionaje, sino en el robo de dinero para financiar otras actividades en las que participa el grupo de APT. Y la lista sigue.

Se necesita un nuevo enfoque

Los métodos y las herramientas que antes suponían una amenaza para un número limitado de organizaciones se han extendido al mercado en general.

Habida cuenta del número cada vez mayor de empresas que caen víctimas de ataques avanzados y dirigidos, es evidente que una defensa satisfactoria exige nuevos métodos. Para protegerse, las empresas deben adoptar un enfoque proactivo y adaptar constantemente sus controles de seguridad al cambiante entorno de las amenazas. La única forma de mantenerse al día de estos cambios es crear un programa eficaz de inteligencia frente a amenazas.

La inteligencia frente a amenazas ya se ha convertido en un componente clave de las operaciones de seguridad establecidas por empresas de distintos tamaños en todos los sectores y áreas geográficas. Se ofrece en formato legible por personas y por máquinas, para ayudar a los equipos de seguridad con información significativa durante todo el ciclo de gestión de incidentes y orientar la toma de decisiones estratégicas (Figura 1).

Sin embargo, la creciente demanda de inteligencia frente a amenazas externas ha dado lugar a una gran cantidad de proveedores de este servicio, cada uno con una oferta diferente. Un mercado amplio y competitivo con innumerables y complejas opciones puede hacer que escoger la solución correcta para su organización sea una tarea confusa y enormemente frustrante.

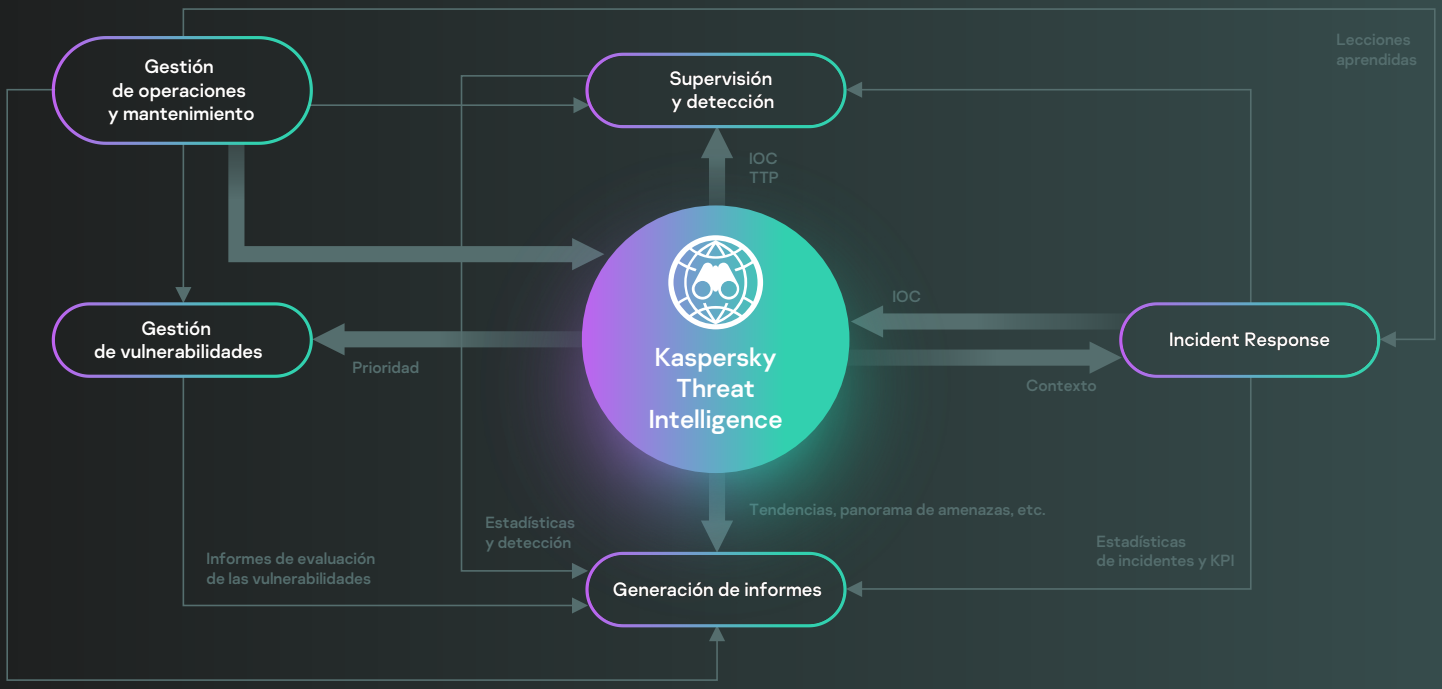

Figura 1

Operaciones de seguridad basadas en inteligencia frente a amenazas

La inteligencia frente a amenazas que no se ajusta a los detalles específicos de su empresa puede agravar la situación. En muchas empresas actuales, los analistas de seguridad dedican más de la mitad de su tiempo a descartar los falsos positivos en lugar de a la búsqueda y respuesta proactivas a las amenazas, lo que aumenta de forma significativa los tiempos de detección. Basar sus operaciones de seguridad con inteligencia irrelevante o inexacta multiplicará el volumen de alertas falsas y supondrá un impacto grave y negativo en sus capacidades de respuesta, así como en la seguridad general de la empresa.

Dónde reside la mejor inteligencia...

Entonces, ¿cómo puede evaluar las numerosas fuentes de inteligencia frente a amenazas, identificar las que son más relevantes para su organización y ponerlas en funcionamiento con eficacia? ¿Cómo puede desenvolverse entre el ingente volumen de marketing sin sentido en el que casi todos los proveedores afirman que su inteligencia es la mejor?

Estas preguntas, si bien son válidas, no son las primeras que debe plantear. Muchas organizaciones, atraídas por mensajes deslumbrantes y nobles promesas, creen que un proveedor externo puede proporcionarles algún tipo de visión de rayos X superpotentes, ignorando por completo que la inteligencia más valiosa reside dentro del perímetro de sus propias redes corporativas...

Los datos de los sistemas de detección y prevención de intrusiones, firewalls, registros de aplicaciones y registros de otros controles de seguridad pueden revelar mucha información acerca de lo que sucede dentro de la red de una empresa. Pueden identificar patrones de actividad maliciosa específicos de la organización. Pueden diferenciar entre el comportamiento normal de un usuario y la red, así como ayudar a mantener un registro de la actividad de acceso a los datos.

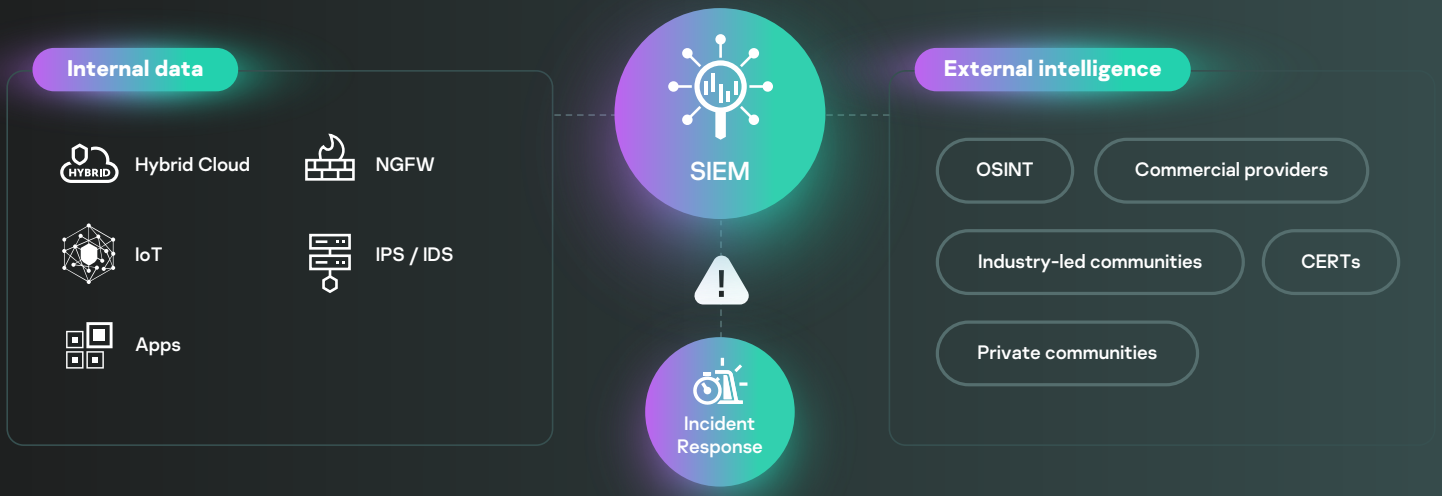

Figura 2

Poner en funcionamiento la inteligencia frente a amenazas externas

Piense como un atacante

Para crear un programa eficaz de inteligencia frente a amenazas, las empresas, también las que cuentan con centros de operaciones de seguridad consolidados, deben pensar como un atacante, para identificar y proteger los objetivos más probables. Obtener auténtico valor de un programa de inteligencia frente a amenazas requiere entender claramente cuáles son los activos clave y qué conjuntos de datos y procesos empresariales resultan vitales para lograr los objetivos de la organización. Identificar estas "joyas de la corona" permite a las empresas establecer puntos de recopilación de datos a su alrededor correlacionar en mayor medida los datos recopilados con información sobre amenazas disponible externamente. Teniendo en cuenta los recursos limitados de los que suelen disponer los departamentos de seguridad de la información, obtener el perfil de una organización completa constituye una tarea de gran envergadura. La solución pasa por adoptar un enfoque basado en el riesgo, centrado, en primer lugar, en los objetivos más susceptibles.

Una vez que se definan e implementen las fuentes de inteligencia frente a amenazas internas, la empresa podrá comenzar a pensar en añadir información externa a sus flujos de trabajo existentes.

Es una cuestión de confianza

Las fuentes de inteligencia frente a amenazas externas varían en cuanto a niveles de confianza:

Las fuentes abiertas están disponibles de forma gratuita, pero a menudo carecen de contexto y devuelven una gran cantidad de falsos positivos.

Las fuentes de inteligencia frente a amenazas comerciales son mucho más fiables, aunque el acceso puede resultar costoso.

Una buena opción para empezar es acceder a las comunidades de intercambio de inteligencia específicas de sectores, como el Centro de Intercambio y Análisis de Información de Servicios Financieros (FS-ISAC). Estas comunidades proporcionan información de valor incalculable, aunque a menudo son de carácter privado y es necesario ser miembro para obtener acceso.

El principio fundamental para elegir fuentes de inteligencia frente a amenazas externas es que debe prevalecer la calidad sobre la cantidad. Algunas organizaciones pueden considerar que cuantas más fuentes de inteligencia frente a amenazas puedan integrar, mejor visibilidad tendrán. Esto puede ser cierto en algunos casos, por ejemplo, cuando se trata de fuentes muy fiables, como las comerciales, que proporcionan inteligencia frente a amenazas adaptada al perfil de amenazas específico de la organización. De lo contrario, existe un riesgo importante de sobrecargar las operaciones de seguridad con información irrelevante.

Es probable que la información suministrada por los proveedores de inteligencia frente a amenazas especializada se solape muy poco. Gracias a que sus fuentes de inteligencia y métodos de recopilación varían, los conocimientos que proporcionan serán únicos en ciertos aspectos. Por ejemplo, un proveedor que cuente con una presencia importante en una región específica proporciona más detalles sobre las amenazas que surgen de dicha región, mientras que otro proporciona más detalles sobre tipos específicos de amenazas. Por lo tanto, obtener acceso a ambas fuentes puede ser beneficioso; al combinarlas, pueden ayudar a mostrar un panorama más amplio y guiar misiones más eficaces en la búsqueda de amenazas y la respuesta ante incidentes. Sin embargo, tenga en cuenta que estos tipos de fuentes de confianza también requieren una cuidadosa evaluación previa para garantizar que la inteligencia proporcionada sea adecuada para las necesidades específicas y los casos de uso de su organización, como las operaciones de seguridad, las respuesta a incidentes, la gestión de riesgos, la gestión de vulnerabilidades, el Red Teaming, etc.

Cuestiones que se deben considerar al evaluar las ofertas de inteligencia frente a amenazas comerciales

Aún no disponemos de criterios comunes para evaluar diferentes ofertas de inteligencia frente a amenazas comerciales, pero aquí hay algunos factores que se deben tener en cuenta al hacerlo:

Se supone que su empresa ya ha implementado algunos controles de seguridad y definido los procesos correspondientes, y que es importante que utilice la inteligencia de amenazas haciendo uso de las herramientas con las que ya está familiarizado. Por lo tanto, busque métodos de entrega, mecanismos de integración y formatos que sean compatibles con la integración fluida de la inteligencia de amenazas en sus operaciones de seguridad existentes.

Busque inteligencia con alcance global. Los ataques no tienen fronteras: un ataque dirigido a una empresa de Latinoamérica puede iniciarse desde Europa y viceversa. ¿Dispone el proveedor de información a nivel global y unifica actividades aparentemente dispares en campañas cohesionadas? Este tipo de inteligencia le ayudará a tomar las medidas apropiadas.

El contexto genera inteligencia a partir de los datos. Los indicadores de amenazas sin contexto no ofrecen ningún valor. Debe buscar proveedores que ayuden a responder a una pregunta clave: ¿por qué es esto importante? El contexto de las relaciones (por ejemplo, los dominios asociados con las direcciones IP o URL detectadas desde donde se descargó el archivo específico, etc.) aporta un valor adicional, lo que impulsa la investigación de incidentes y facilita una determinación del alcance del incidente a través de unos indicadores de compromiso en la red relacionados y recién adquiridos.

Si busca contenido más estratégico para orientar su planificación de seguridad a largo plazo, como, por ejemplo:

- Visibilidad de alto nivel de las tendencias de ataque
- Técnicas y métodos utilizados por los atacantes
- Motivaciones
- Atribuciones, etc.

Busque un proveedor de inteligencia frente a amenazas con una trayectoria demostrada de detección e investigación continuas sobre amenazas complejas en su región o sector. También es fundamental que su proveedor sea capaz de adaptar sus capacidades de investigación a las características específicas de su empresa.

Conclusión

En Kaspersky, llevamos dos décadas centrados en la investigación de amenazas. Con los petabytes de datos de amenazas que se pueden extraer, las avanzadas tecnologías de aprendizaje automático y un conjunto exclusivo de expertos globales, trabajamos para respaldarle con la inteligencia frente a amenazas más reciente de todo el mundo y ayudarle a mantener la inmunidad incluso ante ciberataques desconocidos.

Kaspersky Threat Intelligence

Más información

www.kaspersky.es

© 2022 AO Kaspersky Lab.
Las marcas comerciales y de servicios registradas pertenecen a sus respectivos propietarios.