Permanece un paso adelante
de tus adversarios

Kaspersky Threat Intelligence

kaspersky PREPARADOS PARA EL FUTURO

Kaspersky Threat Intelligence

Threat Intelligence de Kaspersky te permite acceder a la inteligencia que necesitas para mitigar ciberamenazas, gracias a nuestro equipo de investigadores y analistas líder a nivel mundial.

El conocimiento, la experiencia y la inteligencia profunda de Kaspersky en cada aspecto de la ciberseguridad nos ha convertido en el socio de confianza de las principales agencias gubernamentales y de seguridad del mundo, como INTERPOL y las principales CERT. Kaspersky Threat Intelligence te brinda acceso instantáneo a inteligencia de amenazas táctica, operativa y estratégica.

Kaspersky Threat Intelligence ofrece una vista completa del panorama global de amenazas, al combinar fuentes de inteligencia, fuentes de datos de amenazas e investigación interna, todo bajo el análisis de nuestro equipo de expertos para ofrecer perspectivas procesables para ayudar a que las organizaciones se protejan contra las ciberamenazas.

Kaspersky Threat Intelligence te empodera

Identifica y previene amenazas de forma proactiva

Kaspersky Threat Intelligence te mantiene informado sobre las amenazas y las vulnerabilidades más recientes, y te brinda las herramientas para que puedas tomar medidas proactivas de protección de tus sistemas antes de que se produzca un ataque.

Obtén visibilidad de tu presencia digital

Kaspersky Threat Intelligence ofrece un panorama integral de tu presencia digital, incluidos todos los activos que puedan ser vulnerables a ataques o filtraciones.

Mejora tus capacidades de detección de amenazas

Kaspersky Threat Intelligence te ayuda a aumentar tus soluciones de seguridad existentes con la inteligencia de amenazas más reciente, al mejorar tu capacidad de detectar y bloquear amenazas avanzadas.

Mejora tu respuesta a incidentes

Kaspersky Threat Intelligence ofrece información en tiempo real sobre amenazas emergentes e indicadores de riesgo, para que puedas responder de manera rápida y efectiva a los incidentes.

Cumple con regulaciones y estándares

Todas las empresas están sujetas a distintos estándares y regulaciones dentro de su industria. Kaspersky Threat Intelligence permite el cumplimiento, al ayudarte a cumplir estos requisitos.

Enriquece los conocimientos de tu personal interno

El equipo de expertos de Kaspersky está compuesto por los investigadores más experimentados y respetados del sector, que aportan una enorme cantidad de conocimiento y experiencia a tus equipos de seguridad de la información.

Fuentes de datos de amenazas de Kaspersky

Se producen ciberataques todos los días. Su frecuencia, complejidad y nivel de ofuscación es cada vez mayor, ya que intentan poner en riesgo tus defensas. Los adversarios utilizan cadenas de ataques de intrusión complicadas, campañas y tácticas, técnicas y procedimientos personalizados para interrumpir las operaciones de tu empresa o dañar a tus clientes. Una protección efectiva requiere nuevos métodos, basados en inteligencia de amenazas.

Al integrar las últimas fuentes de inteligencia de amenazas, que incluyen información sobre direcciones IP, URL y hashes sospechosos y peligrosos en sistemas de seguridad como SIEM, SOAR y plataformas de inteligencia de amenazas, los equipos de seguridad pueden automatizar el proceso de triaje de alertas inicial y brindar a sus especialistas en triaje un contexto suficiente para que puedan identificar de inmediato las alertas que deben investigarse o escalarse a los equipos de respuesta a incidentes para su posterior investigación y respuesta.

Las fuentes de datos de amenazas de Kaspersky ofrecen información de inteligencia en tiempo real para que puedas proteger tus redes y sistemas contra las ciberamenazas. Las fuentes de datos incluyen información sobre malware conocido, sitios web de phishing, las vulnerabilidades y los exploits más recientes y otros tipos de ciberamenazas. Toda esta información te ayudará a bloquear tráfico malicioso, actualizar tu software de seguridad y tomar otras medidas de protección contra ciberataques.

Datos contextuales

Todos los registros de cada fuente de datos están enriquecidos con contexto procesable (nombres de amenazas, marcas de tiempo, geolocalización, direcciones IP resueltas de recursos web infectados, hashes, popularidad, etc.). Los datos contextuales ayudan a revelar el panorama general, para una mayor validación y un uso más amplio de los datos. Cuando se los coloca en contexto, los datos pueden estar más disponibles para responder las preguntas "quién, qué, dónde, cuándo", identificar a tus adversarios, ayudarte a tomar decisiones rápidas y actuar.

Cómo funciona

1

Se recopilan datos de una amplia variedad de fuentes de confianza, entre ellas Kaspersky Security Network y nuestras propias arañas, un servicio de supervisión de amenazas de botnets (que realiza un seguimiento de botnets y sus objetivos las 24 horas, todos los días), trampas de spam, datos de grupos de investigación, socios y mucho más.

2

Toda la información recopilada se comprueba y se limpia cuidadosamente en tiempo real con distintos métodos de procesamiento: entornos de prueba, análisis estadístico y heurístico, herramientas de similitud, perfiles de comportamiento y análisis a cargo de expertos.

3

Las fuentes de amenazas ayudan a recopilar información de amenazas sobre una alerta o un incidente y a profundizar en sus detalles. También ayuda a responder las preguntas "quién, qué, dónde, cuándo" y a identificar el origen de un ataque, para poder tomar decisiones rápidas que permitan proteger a tu empresa contra amenazas de cualquier complejidad.

Las entradas en las fuentes proporcionadas por Kaspersky incluyen datos contextuales que los ayudan a confirmar y priorizar amenazas rápidamente:

- Nombres de amenazas
- Direcciones IP y nombres de dominio de recursos web maliciosos
- Hashes de archivos maliciosos
- Objetos vulnerables y en riesgo
- Tácticas, técnicas y procedimientos de ataque según la clasificación de MITRE ATT&CK
- Marcas de tiempo
- Geolocalización
- Popularidad, etc.

Beneficios de las fuentes de datos de amenazas de Kaspersky

Mejora y acelera tus capacidades forenses y de respuesta a incidentes

gracias a la automatización del proceso de triaje inicial, además de ofrecer a tus analistas de seguridad contexto suficiente para que identifiquen de inmediato las alertas que deben investigarse o escalarse a equipos de respuesta a incidentes para su posterior investigación y respuesta.

Refuerza tus soluciones de seguridad,

incluidos SIEM, firewalls, IPS/IDS, proxies de seguridad, soluciones de DNS y anti APT, con indicadores de riesgo (IOC) actualizados continuamente y contexto procesable para obtener un panorama de los ciberataques y entender mejor las intenciones, las capacidades y los objetivos de tus adversarios. Ofrecemos una compatibilidad total con los principales SIEM (entre ellos ArcSight, IBM QRadar, MS Sentinel, Splunk, etc.) y plataformas de TI.

Previene la exfiltración de activos y propiedad intelectual confidenciales,

desde máquinas infectadas hacia el exterior de la organización. Detecta rápidamente activos infectados para proteger tu reputación de marca, conserva tu ventaja competitiva y obtén oportunidades comerciales.

Haz crecer tu negocio de MSSP

al ofrecer una inteligencia de amenazas líder en la industria como servicio premium para tus clientes. Como CERT, mejora y amplía tus capacidades de detección e identificación de ciberamenazas.

Kaspersky CyberTrace

El crecimiento permanente de la cantidad de fuentes de datos de amenazas y orígenes de inteligencia de amenazas disponibles hace que sea difícil para las empresas determinar qué información deben considerar relevante. Al mismo tiempo, la inteligencia de amenazas viene en muchos formatos diferentes e incluye una gran cantidad de indicadores de riesgo (IoC), lo que dificulta su digestión por parte de los SIEM y otros controles de seguridad de red.

Al integrar la última inteligencia de datos legible por máquina con controles de seguridad existentes como sistemas SIEM, los centros de operaciones de seguridad pueden automatizar el proceso de triaje inicial y ofrecer a los analistas de seguridad un contexto suficiente para que identifiquen de inmediato las alertas que deben investigarse o escalarse a los equipos de respuesta a incidentes para su posterior investigación y respuesta.

Kaspersky CyberTrace es una plataforma de inteligencia de amenazas que permite la integración eficiente de fuentes de datos de amenazas con soluciones SIEM, para ayudar a que los analistas aprovechen la inteligencia de amenazas en su flujo de trabajo de operaciones de seguridad existente de manera más efectiva. Se integra con cualquier fuente de inteligencia de amenazas (de Kaspersky, otros proveedores, OSINT o las fuentes de tus clientes) en los formatos JSON, STIX, XML y CSV, además de permitir una integración sin configuración con numerosas fuentes de registros y soluciones SIEM.

Instrumentos

Kaspersky CyberTrace ofrece un conjunto de instrumentos para operacionalizar de manera efectiva la inteligencia de amenazas:

Una base de datos de indicadores con búsqueda de texto completo y la capacidad de buscar mediante consultas avanzadas permite realizar búsquedas complejas en todos los campos de indicadores, incluido el contexto

Las estadísticas de uso de fuentes para medir la efectividad de las fuentes integradas y la matriz de intersección de fuentes sirven para elegir a los proveedores de inteligencia de amenazas más valiosos

El etiquetado de IoC simplifica su gestión Puedes crear cualquier etiqueta y especificar su ponderación (importancia) para usarla en el etiquetado manual de IoC También puedes ordenar y filtrar IoC en función de estas etiquetas y su ponderación

Un gráfico de investigación te permite explorar visualmente los datos y detecciones almacenados en CyberTrace y descubrir factores comunes entre amenazas

La función de exportación de indicadores te permite exportar conjuntos de indicadores a controles de seguridad como listas de directivas (listas de bloqueo) y compartir datos de amenazas entre instancias de Kaspersky CyberTrace o con otras plataformas de TI

La función de correlación histórica (retroanálisis) te permite analizar observables de eventos revisados anteriormente con las fuentes más recientes para encontrar amenazas detectadas previamente.

Las funciones multiempresa admiten casos de uso de MSSP y grandes empresas

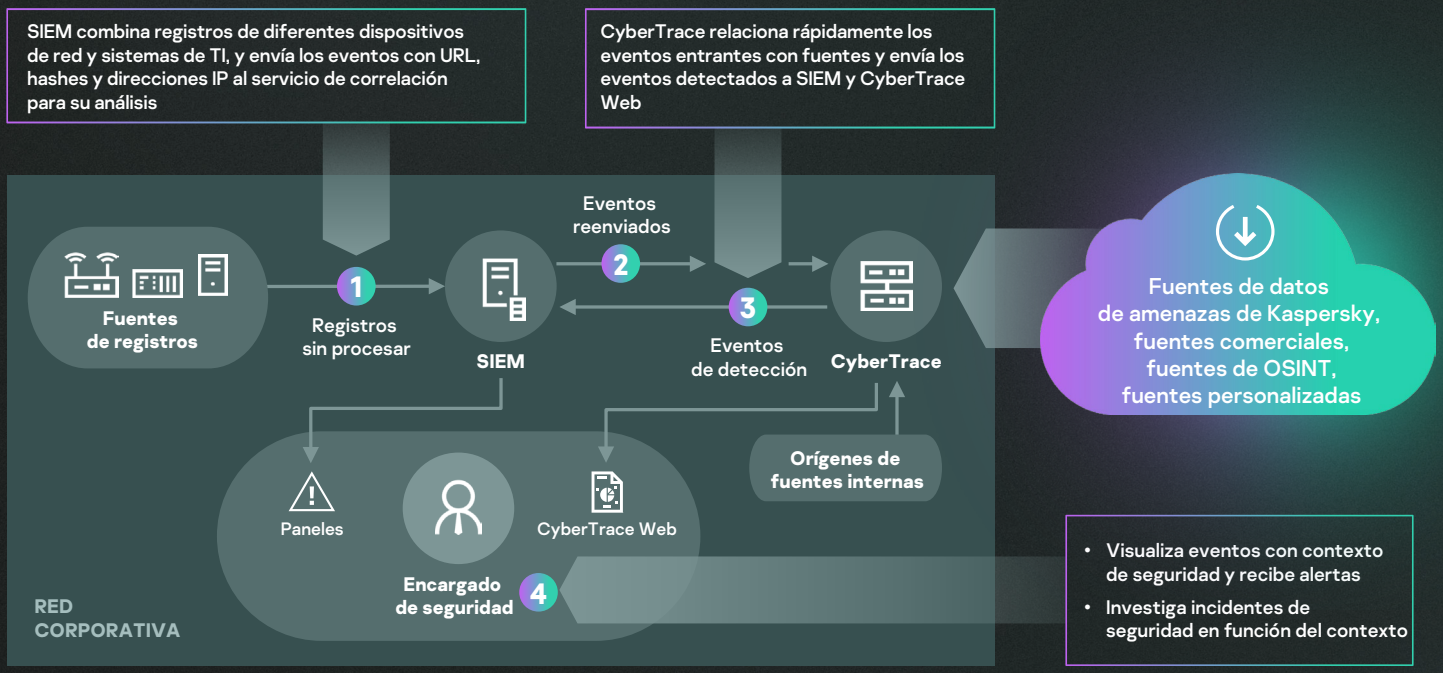
Un filtro envía eventos de detección a soluciones SIEM, lo que reduce la carga tanto en los SIEM como en los analistas

La HTTP RestAPI te permite buscar y gestionar inteligencia de amenazas

Las páginas con información detallada sobre cada indicador ofrecen un análisis aún más profundo. Cada página presenta toda la información sobre un indicador de todos los proveedores de inteligencia (deduplicación) para que los analistas puedan hablar sobre las amenazas en los comentarios y añadir inteligencia de amenazas interna sobre el indicador

La herramienta utiliza un proceso internalizado de análisis y emparejamiento de datos entrantes que reduce significativamente la carga de trabajo de SIEM. Kaspersky CyberTrace analiza los registros y los eventos entrantes, empareja rápidamente los datos resultantes con fuentes y genera sus propias alertas de detección de amenazas.

Arquitectura



Kaspersky CyberTrace y las fuentes de datos de amenazas de Kaspersky permiten que tus analistas de seguridad hagan lo siguiente:

Filtren y prioricen de manera efectiva grandes cantidades de alertas de seguridad.

Mejoren y aceleren los procesos de triaje y respuesta inicial.

Diseñen una defensa proactiva e impulsada por inteligencia.

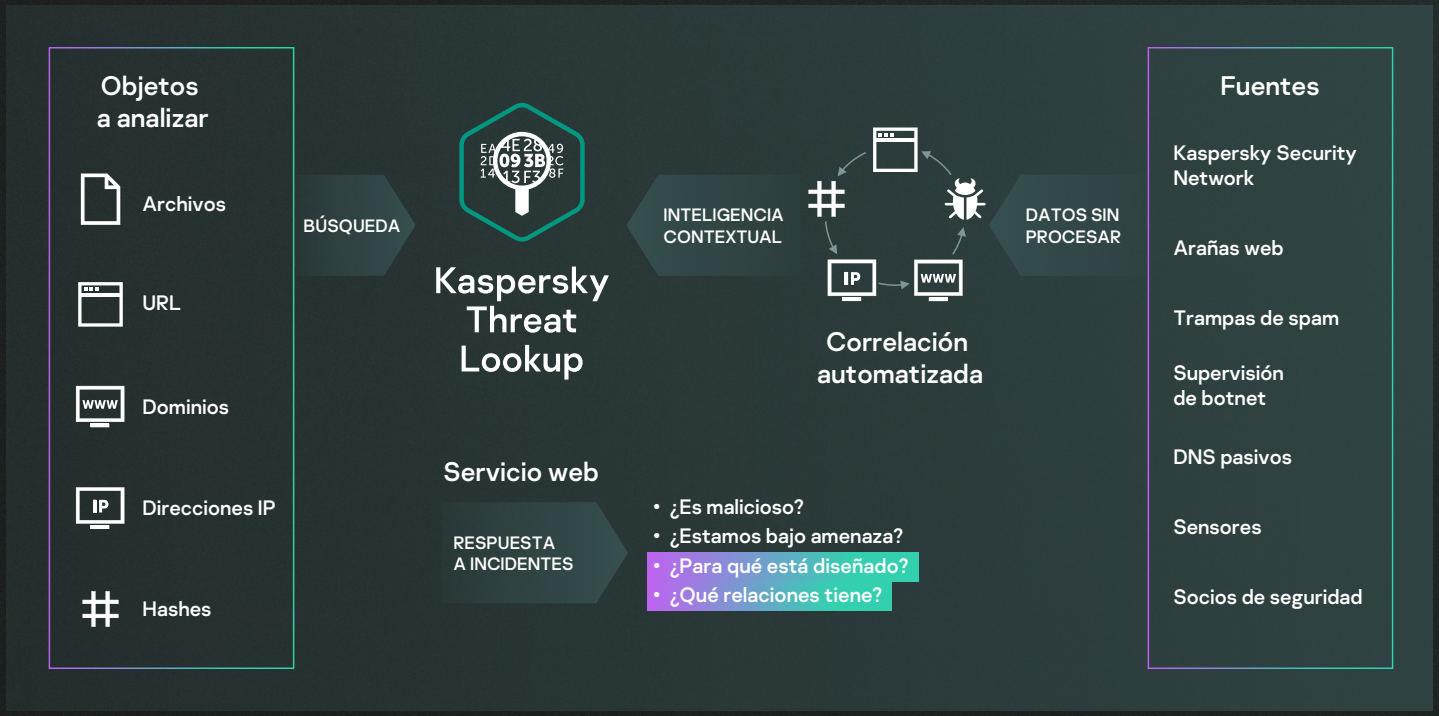
Identifiquen de inmediato las alertas críticas para tu empresa y tomen decisiones más informadas sobre cuáles deberían escalarse a los equipos de respuesta a incidentes.

Búsqueda de amenazas de Kaspersky

El ciberdelito no conoce fronteras, y las capacidades técnicas están mejorando rápidamente: observamos que los ataques son cada vez más sofisticados y que los ciberdelincuentes utilizan recursos de la dark web para amenazar a sus víctimas. La frecuencia, la complejidad y el nivel de ofuscación de las ciberamenazas es cada vez mayor, y se realizan nuevos intentos por poner en riesgo tus defensas. Los atacantes utilizan cadenas de ataque complicadas y tácticas, técnicas y procedimientos personalizados en sus campañas para interrumpir la operación de tu empresa, robar tus activos o dañar a tus clientes.

La búsqueda de amenazas de Kaspersky ofrece todo el conocimiento adquirido por Kaspersky sobre ciberamenazas y sus relaciones, combinado en un único y potente servicio web. El objetivo es que tus equipos de seguridad tengan la mayor cantidad de datos posibles y puedan prevenir los ciberataques antes de que afecten a la organización. La plataforma recopila la inteligencia de amenazas detallada más reciente sobre URL, dominios, direcciones IP, hashes de archivos, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS/DNS, atributos de archivos, datos de geolocalización, cadenas de descarga, marcas de tiempo, etc. El resultado es una visibilidad global de las amenazas nuevas y emergentes que te ayudará a proteger a tu organización y mejorar la respuesta a incidentes.

Cómo funciona



Aspectos destacados

Inteligencia de confianza

Un atributo clave de la búsqueda de amenazas de Kaspersky es la fiabilidad de nuestros datos de inteligencia de amenazas, enriquecidos con contexto procesable. Kaspersky lidera el campo en pruebas antimalware, lo que demuestra la calidad inigualable de nuestra inteligencia de seguridad para ofrecer las tasas de detección más altas, con falsos positivos cercanos a cero.

Búsqueda de amenazas

Adopta una postura proactiva para prevenir, detectar y responder ataques a fin de minimizar su impacto y frecuencia. Realiza seguimientos y elimina agresivamente los ataques lo antes posible. Cuanto antes descubras un ataque, menos daño podrá causar, más rápido se podrán efectuar reparaciones y las operaciones podrán regresar a la normalidad a la brevedad.

Interfaz web de fácil uso o

API RESTful. Usa el servicio en modo manual a través de una interfaz web (con un navegador) o accede a él a través de una API RESTful simple, la opción que prefieras

Amplia variedad de formatos de exportación

Exporta indicadores de riesgo (IOC) o contexto procesable a los formatos compartidos legibles por máquina más populares y de uso generalizado, como STIX, OpenIOC, JSON, Yara, Snort o incluso CSV, para aprovechar al máximo la inteligencia de amenazas, automatizar el flujo de trabajo operacional o lograr una integración con controles de seguridad como SIEM.

Beneficios de la búsqueda de amenazas de Kaspersky

Realiza búsquedas profundas en indicadores de amenazas con contextos altamente validados, que te permiten priorizar ataques y concentrarte en mitigar las amenazas que representan el mayor riesgo para tu empresa

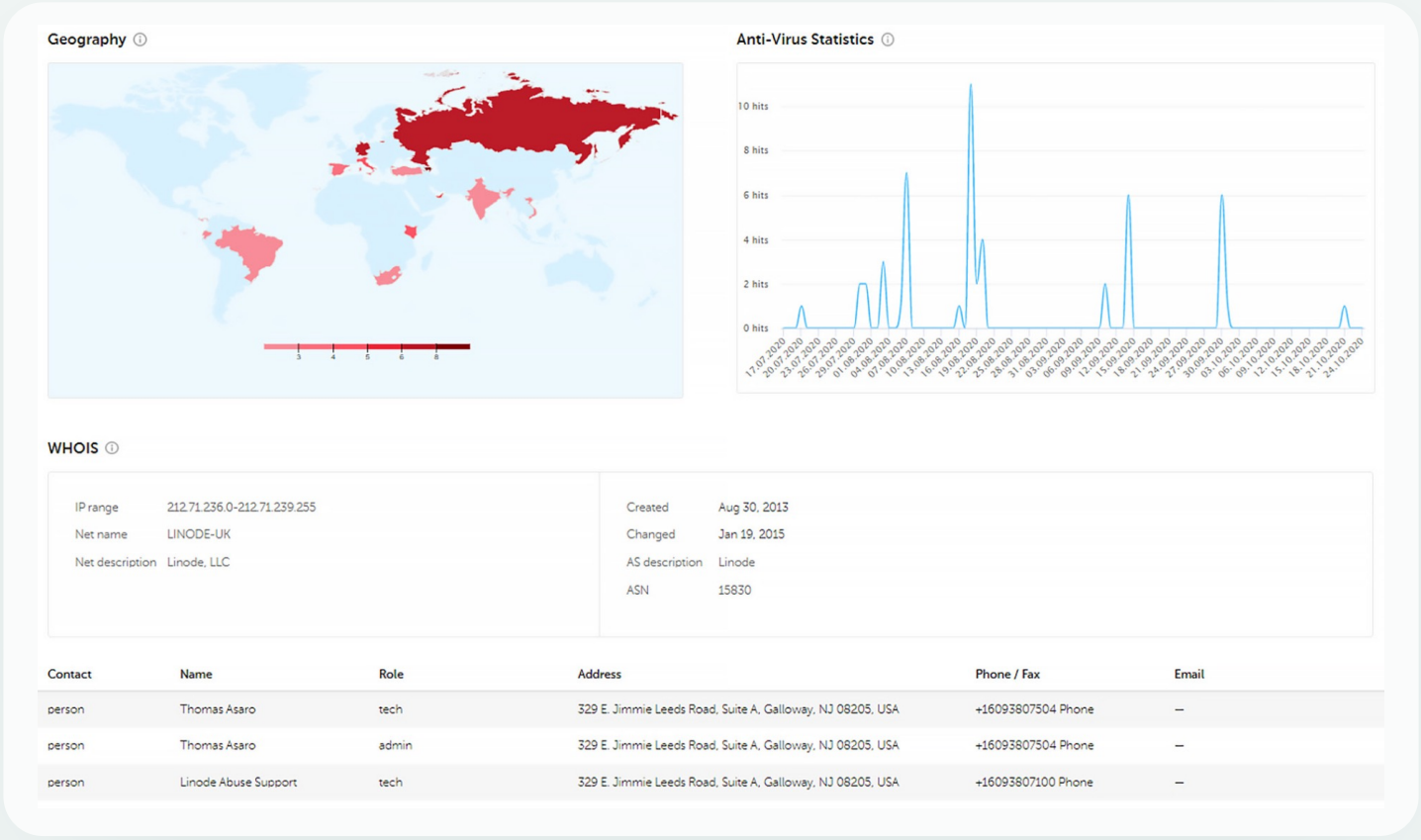
Diagnostica y analiza incidentes de seguridad en hosts y en la red de manera más eficiente y prioriza señales de sistemas internos contra amenazas desconocidas

Mejora tus capacidades de respuesta a incidentes y búsqueda de amenazas para interrumpir la cadena de ataque antes de que se pongan en riesgo sistemas y datos críticos

Busca indicadores de amenazas desde una interfaz web o a través de la API RESTful

Examina detalles avanzados como certificados, nombres de uso común, rutas de archivos o URL relacionadas para descubrir nuevos objetos sospechosos

Comprueba si el objeto detectado se ha distribuido o es único, y entiende por qué un objeto debe ser tratado como malicioso



Kaspersky Research Sandbox

Es imposible prevenir ataques selectivos solo con herramientas antivirus tradicionales. Los motores antivirus solo pueden detener amenazas conocidas y sus variantes, mientras que los actores de amenazas sofisticados utilizan una amplia variedad de técnicas para evadir la detección automática. Las pérdidas debido a incidentes de seguridad de la información siguen creciendo, y ponen de manifiesto la importancia de contar con capacidades de detección de amenazas inmediata para garantizar una respuesta rápida y la capacidad de contrarrestar las amenazas antes de que puedan causar daños.

Tomar una decisión inteligente basada en el comportamiento de un archivo, y al mismo tiempo analizar la memoria del proceso, la actividad de red, etc., es el enfoque óptimo para entender las amenazas selectivas y personalizadas más recientes y sofisticadas. Aunque los datos estadísticos pueden carecer de información sobre el malware recientemente modificado, las tecnologías de entornos de prueba son herramientas potentes que permiten investigar los orígenes de la muestra del archivo, recopilar IOC basados en análisis de comportamiento y detectar objetos maliciosos no observados anteriormente.

Kaspersky Research Sandbox te permite investigar los orígenes de la muestra del archivo, recopilar IOC basados en análisis de comportamiento y detectar objetos maliciosos no observados anteriormente. Ofrece un enfoque híbrido que combina la inteligencia de amenazas recopilada de petabytes de datos estadísticos (gracias a Kaspersky Security Network y otros sistemas patentados), análisis de comportamiento y una sólida antievasión con tecnologías de simulación del comportamiento humano, como auto clicker, desplazamiento de documentos y procesos ficticios.

Detección y mitigación de amenazas proactiva

El malware utiliza distintos métodos para ocultar su ejecución y evitar la detección. Si el sistema no cumple con los parámetros requeridos, el programa malicioso se destruirá y no dejará rastros casi en la totalidad de los casos. Para que el código malicioso se ejecute, el entorno de pruebas debe ser capaz de imitar con precisión el comportamiento normal de un usuario final.

Kaspersky Research Sandbox ofrece un enfoque híbrido que combina la inteligencia de amenazas recopilada de petabytes de datos estadísticos (gracias a Kaspersky Security Network y otros sistemas patentados), análisis de comportamiento y una sólida antievasión con tecnologías de simulación del comportamiento humano, como auto clicker, desplazamiento de documentos y procesos ficticios.

Este servicio fue desarrollado en nuestro laboratorio de entornos de pruebas interno y ha estado evolucionando durante más de una década. La tecnología incorpora todo nuestro conocimiento en comportamiento de malware, obtenido durante más de 25 años de investigación de amenazas continua. Esto nos permite detectar más de 400000 nuevos objetos maliciosos por día, para ofrecerles a nuestros clientes soluciones de seguridad líderes en el sector.

Kaspersky Research Sandbox se puede gestionar tanto desde una plataforma de administración única basada en la nube como desde una consola fuera de línea en entornos herméticos, para aprovechar la inteligencia de amenazas e incorporar análisis personalizables.

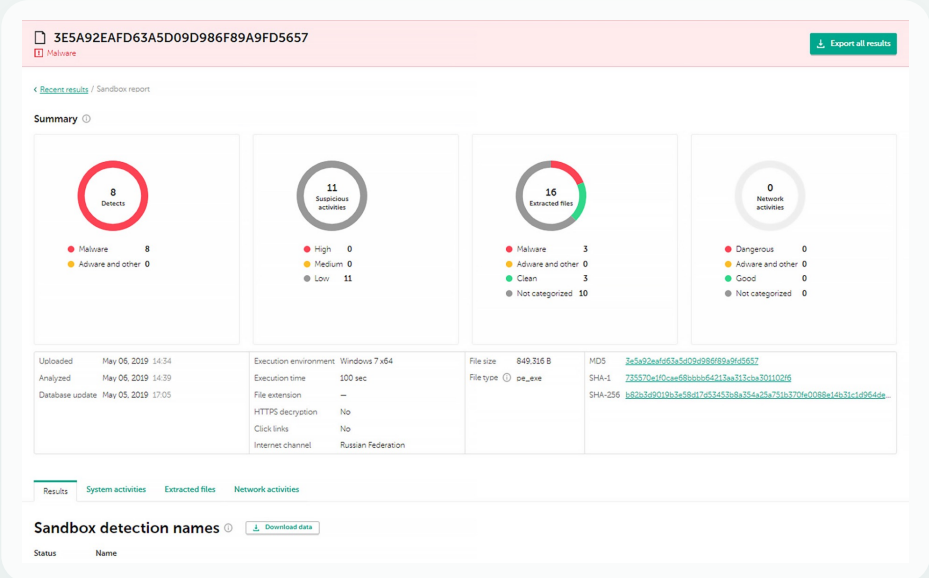
Como parte de Threat Intelligence Portal, Kaspersky Research Sandbox es el componente final en tu flujo de trabajo de inteligencia de amenazas. Mientras que la búsqueda de amenazas recupera la inteligencia de amenazas detallada más reciente sobre URL, dominios, direcciones IP, hashes de archivos, nombres de amenazas, datos estadísticos/ de comportamiento, datos de WHOIS/ DNS, etc., Research Sandbox vincula ese conocimiento con los IOC generados por el archivo analizado.

Informes integrales

- Calificación de amenazas unificada
- Actividades del sistema sospechosas con descripciones detalladas
- DLL cargadas y ejecutadas
- Archivos creados, modificados y eliminados
- Volcados de memoria de procesos y volcado de tráfico de red (PCAP)
- Extensiones mutuas (mutexes) creadas
- Claves de registro modificadas y creadas
- Procesos creados por el archivo ejecutado
- Actividades de red (SMB, SMTP, IP, TCP, UDP, DNS, SSL, FTP, IRC, POP3, sesiones de SOCKS; HTTP(s), solicitudes y respuestas)
- Inteligencia de amenazas detallada con contexto procesable para cada indicador de riesgo (IOC) revelado
- Mapa de ejecución detallada con técnicas MITRE ATT&CK destacadas
- Detecciones de YARA y reglas de IDS disparadas (incluidas las personalizadas)
- Descarga y análisis de un archivo alojado en una URL determinada
- Clics en enlaces de documentos de Microsoft Office (Word, Excel, PowerPoint, Publisher, Outlook) y Adobe Reader
- Posibilidad de exportar los datos del análisis en los formatos STIX, JSON, CSV
- Variedad de entornos, incluidos sistemas operativos móviles (Android) y capacidades de personalización de entornos
- Parámetros de ejecución de archivos personalizados
- Canales de Internet diferentes, la posibilidad de enrutar tráfico a través del canal VPN personalizado
- API RESTful
- Capturas de pantalla y mucho más

Con Kaspersky Research Sandbox, puedes realizar investigaciones de incidentes altamente efectivas y complejas, para comprender de inmediato la naturaleza de la amenaza y conectar distintos elementos a medida que profundizas para revelar indicadores de amenazas interrelacionados.

La inspección puede consumir muchos recursos, especialmente si hablamos de ataques multietapa. Kaspersky Research Sandbox mejora tu respuesta a incidentes y actividades forenses, al ofrecerte la escalabilidad para procesar archivos automáticamente sin tener que adquirir dispositivos costosos ni preocuparte por los recursos del sistema.



Kaspersky Threat Attribution Engine

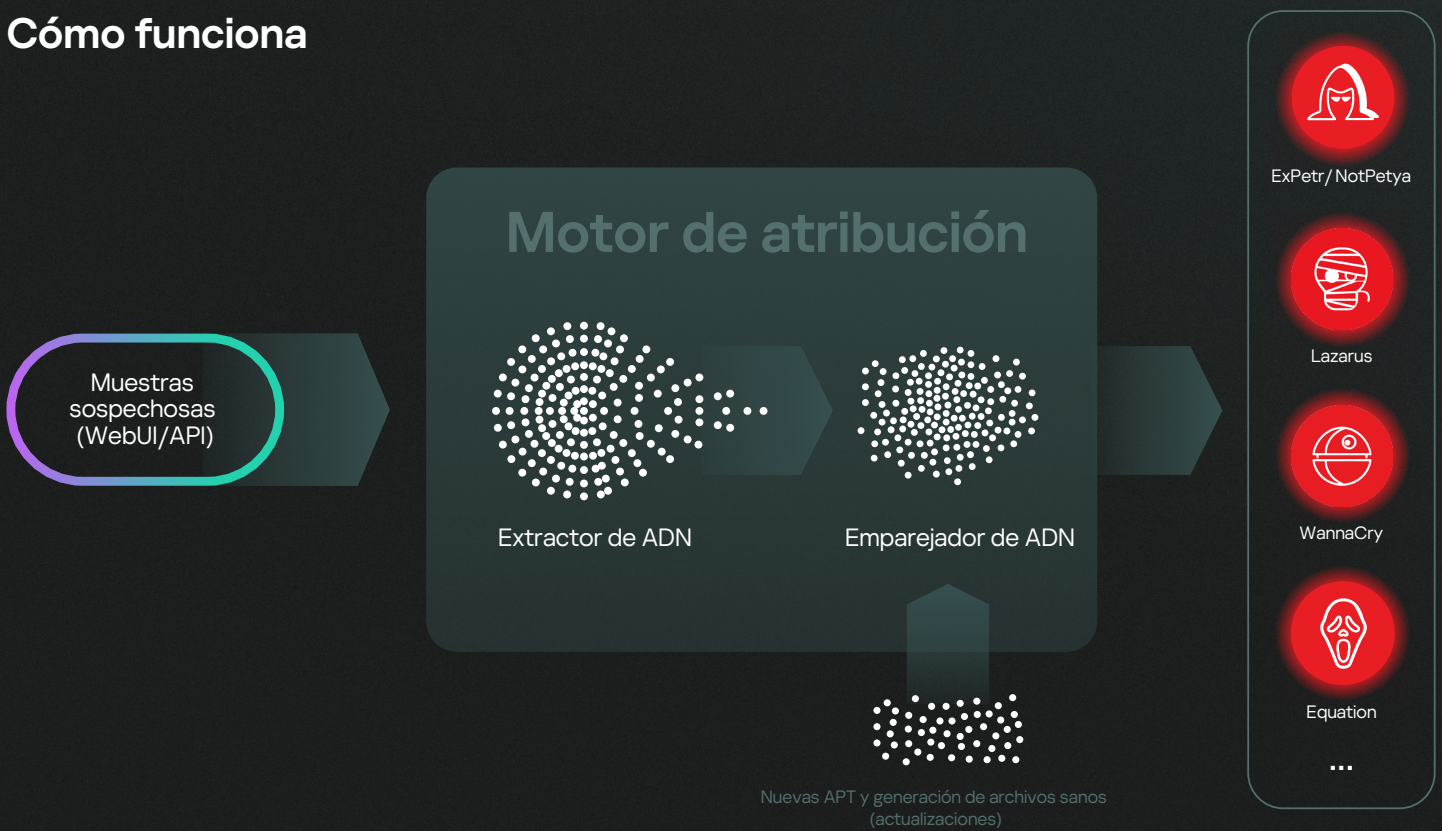
Hay un motivo de peso por el cual la atribución de amenazas tiene un papel importante en la ciberseguridad. El retraso de tiempo promedio entre la detección y la respuesta a amenazas altamente sofisticadas puede ser muy prolongado y frustrante, debido a los complejos procesos de ingeniería inversa e investigación involucrados. En muchos casos, este retraso puede darles a los atacantes el tiempo suficiente para alcanzar sus objetivos. Una atribución correcta y oportuna ayuda no solo a acortar los tiempos de respuesta de horas a minutos, sino también a reducir la cantidad de falsos positivos.

Identificar un ataque selectivo, realizar un perfil de los atacantes y crear factores de atribución para los diferentes actores de amenazas es una tarea larga y compleja, que puede llevar años. Crear una atribución que funcione también requiere una gran cantidad de datos acumulados a lo largo del tiempo, además de un equipo altamente capacitado de investigadores, con una experiencia adecuada en su trabajo. Estos investigadores normalmente se encargarán de seguir la actividad de diferentes grupos y completarán una base de datos con los diferentes datos acumulados. En lo sucesivo, esta base de datos se convertirá en un valioso recurso que puede compartirse como herramienta.

Kaspersky Threat Attribution Engine incorpora una base de datos compuesta por muestras de malware APT y archivos limpios recopilados por expertos de Kaspersky a lo largo de 25 años y más. Realizamos seguimientos a más de 1100 campañas y actores de amenazas, y publicamos más de 120 informes de inteligencia de amenazas al año. Nuestra investigación en curso incluye una colección de APT que contiene aproximadamente 83 000 archivos. Esto mejora la detección de banderas falsas y, junto con el uso de herramientas automatizadas, da como resultado niveles de atribución increíblemente precisos.

El producto ofrece un enfoque único en la comparación de muestras similares y garantiza tasas de falsos positivos cercanas a cero. Todos los ataques nuevos pueden vincularse rápidamente a malware de APT conocidos, ataques selectivos anteriores y grupos de piratas informáticos, para ayudarte a distinguir amenazas de alto riesgo de incidentes menos graves, a fin de que puedas tomar medidas de protección oportunas para evitar que un atacante acceda a tu sistema.

Cómo funciona



Para vincular el malware con entidades de atribución, Kaspersky Threat Attribution Engine utiliza un método patentado exclusivo de búsqueda de similitudes entre archivos. Este método incluye lo siguiente:

1

Análisis de la genética de una muestra mediante la extracción de los siguientes elementos del código:

- Genotipos: fragmentos distintivos de código binario.
- Cadenas: cadenas distintivas de código binario.

2

Búsqueda automática dentro de archivos analizados de genotipos y cadenas que sean similares a aquellos de muestras de APT analizadas previamente o que ya estén vinculadas a entidades de atribución.

3

Con base en genotipos y cadenas similares detectadas en muestras de APT, se ofrece un informe sobre el origen de la muestra analizada, las entidades de atribución relacionadas y cualquier similitud entre esta muestra y muestras de APT conocidas.

El producto puede implementarse en entornos herméticos y seguros, para restringir el acceso de cualquier tercero a la información procesada y los objetos enviados. Una API conecta el motor con otras herramientas y estructuras para implementar la atribución en la infraestructura existente y los procesos automatizados.

Aspectos destacados del producto

- Acceso instantáneo a un repositorio de datos curados sobre miles de actores de APT, muestras y amenazas más generales (a través del motor antivirus).
- Eficiente priorización de amenazas y triaje de alertas manual o automatizado.
- Incorporación de muestras y actores privados que entrenan al producto para que pueda detectar muestras similares a los archivos de tu colección privada.
- Cargas de muestras manuales y funcionalidad de API REST mejorada para la integración con flujos de trabajo automatizados.
- Implementación en Amazon Web Services (AWS) que permite una rápida configuración del producto y un ahorro de costes, ya que no hay necesidad de invertir en hardware por adelantado.
- Exportaciones sencillas a reglas de YARA para un posterior análisis/búsqueda de manera automatizada de archivos similares, o integración con soluciones de terceros.
- Exportaciones sencillas a formato STIX 2.1 (también se admiten los formatos TXT y JSON) para un posterior análisis automatizado de registros de seguridad, o integración con soluciones o controles de seguridad de terceros.
- Descompresión de archivos protegidos con contraseñas personalizadas.
- Acceso rápido a documentación y contrato de licencia del usuario final (CLUF) en la interfaz web.
- Envío de atributos en archivos paralelos para su análisis en una sola solicitud.

Beneficios de Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine calcula la calificación de reputación

de la muestra y revela su genética y su atribución de código. Esto ofrece un panorama sobre el origen de la muestra y puede permitir su atribución a posibles autores.

Tu equipo de seguridad puede añadir sus propias entidades de atribución privadas

y las muestras relacionadas a la base de datos de Kaspersky Threat Attribution Engine. De este modo, el equipo puede entrenar a la aplicación para que atribuya las muestras enviadas a estas muestras y entidades de atribución privadas.

El proceso de atribución lleva unos pocos segundos

Con Kaspersky Threat Attribution Engine, el proceso de atribución lleva unos pocos segundos; no los meses y años que se necesitaban en el pasado.

Kaspersky Threat Attribution Engine amplía y fortalece

la cartera de productos de Kaspersky para centros de operaciones de seguridad (SOC) y organismos de ciberseguridad nacionales, al ayudarlos a establecer un proceso de gestión de incidentes efectivo.

Kaspersky APT Intelligence Reporting

Los clientes de Kaspersky APT Intelligence Reporting reciben un acceso continuo y exclusivo a nuestras investigaciones y descubrimientos, incluidos datos técnicos completos (en distintos formatos) de cada APT en el momento de su descubrimiento y de amenazas que jamás se revelarán públicamente. Los informes contienen un resumen ejecutivo que incluye información fácil de entender, orientada a cargos ejecutivos de empresas, donde se describe la APT relacionado junto con una descripción técnica detallada la APT con los IOC y las reglas de YARA relacionados, para que los investigadores de seguridad, analistas de malware, ingenieros de seguridad, analistas de seguridad de redes e investigadores de APT cuenten con datos procesables que les permitan brindar una respuesta rápida y precisa a la amenaza.

Nuestros expertos te alertarán de inmediato ante cualquier cambio que detecten en las tácticas de los grupos de ciberdelincuentes. También podrás acceder a la base de datos de informes de APT completa de Kaspersky, otro potente componente de investigación y análisis en tus defensas de seguridad.

Más de 300
actores de amenazas

Más de 160
informes privados al año

Más de 12 000
IoC

Más de 400
campañas

Más de 700
reglas de Yara

Kaspersky APT Intelligence Reporting ofrece lo siguiente

Perfiles de actores de amenazas

Asignación a MITRE ATT&CK

Resumen ejecutivo

Información orientada a cargos ejecutivos de empresas

Análisis técnico profundo
- Métodos de ataque
- Exploits utilizados
- Descripción de malware
- Descripción de protocolos e infraestructura de mando y control
- Análisis de víctimas
- Análisis de exfiltración de datos
- Atribuciones

Conclusiones y recomendaciones

Indicadores de riesgo (IOC) y reglas de YARA

Beneficios de Kaspersky APT Intelligence Reporting

Información sobre APT no públicos

Por distintos motivos, no todas las amenazas de alto perfil se divulgan para el público en general; pero tú sí accederás a ellas

Acceso privilegiado

Recibe descripciones técnicas sobre las amenazas más recientes durante investigaciones en curso, antes de su divulgación al público en general

Análisis en retrospectiva

El acceso a todos los informes publicados previamente está disponible a través de la suscripción

Acceso a datos técnicos

Incluida una lista ampliada de IOC disponible en formatos estándar, entre ellos openIOC o STIX, además de acceso a nuestras reglas de YARA

Inteligencia sobre perfiles de actores de amenazas

Incluidos presunto país de origen y actividad principal, familias de malware utilizadas, industrias y geografías seleccionadas como objetivo y descripciones de todos los TTP utilizados, con asignación a MITRE ATT&CK

Integración y automatización eficientes

Integración y automatización eficientes de los flujos de trabajo de seguridad con API RESTful

Supervisión de campañas de APT continuas

Accede a inteligencia procesable durante investigaciones con información sobre distribución de APT, IOC, infraestructuras de mando y control, etc.

MITRE ATT&CK

Todos los TTP descritos en los informes están asignados a MITRE ATT&CK para permitir la detección y respuesta mejoradas a través del desarrollo y la priorización de los casos de uso de supervisión de seguridad correspondientes, los análisis de brechas y las pruebas de las defensas actuales contra los TTP correspondientes

Informes de inteligencia de Crimeware de Kaspersky

El ciberdelito con motivaciones económicas no está limitado a industrias específicas. Y, aunque sigue habiendo ataques a infraestructuras financieras como cajeros automáticos y dispositivos de punto de venta, todas las empresas en cada sector corren riesgo de ser víctimas de ransomware. En los últimos dos años, se han borrado las barreras entre los diferentes tipos de amenazas y los diferentes tipos de actores de amenazas. Esto incluye la aparición de campañas de amenazas persistentes avanzadas (APT) dirigidas no solo al ciberespionaje sino también al robo; es decir, a la obtención de dinero para financiar otras actividades en las que participa el grupo de ATP. La creciente sofisticación de las amenazas de crimeware no debe subestimarse.

Los informes de inteligencia de Crimeware de Kaspersky mejoran tus estrategias defensivas con información oportuna sobre campañas de malware, ataques selectivos a instituciones financieras e información sobre herramientas de crimeware utilizadas para atacar bancos, empresas de procesamiento de pagos y sus infraestructuras específicas.

Los informes de inteligencia de Crimeware de Kaspersky ofrecen lo siguiente

- Descripciones detalladas de malware popular, generalizado y altamente publicitado.
- Notas y advertencias tempranas de investigadores, incluida información sobre amenazas de malware nuevas y actualizadas.
- Información sobre campañas de malware peligrosas y generalizadas.
- Descripciones detalladas de amenazas dirigidas a infraestructuras financieras y las herramientas de ataque correspondientes que desarrollan o venden los ciberdelincuentes a través de la dark web en distintas geografías.

Beneficios de los informes de inteligencia de Crimeware de Kaspersky

Acceso privilegiado

Recibe descripciones técnicas sobre las amenazas más recientes durante investigaciones en curso, antes de su divulgación al público en general

Análisis en retrospectiva

El acceso a todos los informes publicados previamente está disponible a través de la suscripción

Integración y automatización eficientes

Integración y automatización eficientes de los flujos de trabajo de seguridad con API RESTful

Acceso a datos técnicos

, incluida una lista ampliada de IOC disponible en formatos estándar, entre ellos openIOC o STIX, además de acceso a nuestras reglas de YARA

Inteligencia sobre perfiles de actores de crimeware

Incluidos presunto país de origen y actividad principal, familias de malware utilizadas, industrias y geografías seleccionadas como objetivo y descripciones de todos los TTP utilizados, con asignación a MITRE ATT&CK

Kaspersky ICS Threat Intelligence Reporting

Kaspersky ICS Threat Intelligence Reporting ofrece inteligencia profunda y un mayor nivel de conciencia sobre las campañas maliciosas dirigidas a organizaciones industriales, además de información sobre las vulnerabilidades encontradas en los sistemas de control industriales más populares y las tecnologías subyacentes. Los informes se envían a través de Kaspersky Threat Intelligence Portal, por lo que puedes comenzar a utilizar el servicio de inmediato.

Toda la investigación de inteligencia de amenazas relacionada con ICS está a cargo de un equipo exclusivo, Kaspersky ICS CERT:

- Fundado en 2016
- El primer equipo de CERT creado por una organización comercial
- Alrededor de 20 expertos altamente cualificados en investigación de vulnerabilidades y amenazas de ICS, respuesta a incidentes y análisis de seguridad

Informes incluidos en tu suscripción

Informes de APT

Informes sobre nuevas APT y campañas de ataque de alto volumen dirigidas a organizaciones industriales, y actualizaciones sobre amenazas activas

Vulnerabilidades encontradas

Informes sobre las vulnerabilidades identificadas por Kaspersky en los productos más populares utilizados en sistemas de control industrial, la Internet de las cosas industrial e infraestructuras de distintas industrias

Análisis y mitigación de vulnerabilidades

Nuestros asesores ofrecen recomendaciones procesables realizadas por expertos de Kaspersky para ayudar a identificar y mitigar las vulnerabilidades en tu infraestructura

Evolución del panorama de amenazas

Informes sobre cambios significativos al panorama de amenazas de sistemas de control industrial, factores críticos recientemente descubiertos que afectan a los niveles de seguridad de ICS y la exposición de ICS a amenazas, incluida información específica por región, país e industria

Los datos sobre inteligencia de amenazas te permiten hacer lo siguiente

Detectar y prevenir

Amenazas informadas para proteger activos críticos, incluidos componentes de software y hardware, y garantizar la seguridad y la continuidad de los procesos tecnológicos

Evaluar vulnerabilidades

Evaluación de tus entornos y activos industriales tras un análisis preciso del alcance y la gravedad de una vulnerabilidad para tomar decisiones informadas sobre administración de parches e implementación de otras medidas preventivas recomendadas por Kaspersky

Correlacionar

Toda la actividad maliciosa y sospechosa que detectas en entornos industriales con los resultados de búsqueda de Kaspersky para atribuir tu detección a la campaña maliciosa en cuestión, identificar amenazas y responder rápidamente a incidentes

Aprovechar información

Sobre tecnologías, tácticas y procedimientos de ataque, vulnerabilidades recientemente descubiertas y otros cambios importantes en el panorama de amenazas para lograr lo siguiente:

- Identificar y evaluar los riesgos que suponen las amenazas identificadas y otras amenazas similares
- Planificar y diseñar cambios a infraestructuras industriales para garantizar una producción segura y la continuidad del proceso tecnológico
- Ejecutar actividades de concienciación en seguridad basadas en análisis de casos reales para generar escenarios de formación de personal y planificación de ejercicios de equipo rojo contra equipo azul
- Tomar decisiones estratégicas informadas para invertir en ciberseguridad y garantizar la resiliencia operativa

Kaspersky Digital Footprint Intelligence

A medida que tu empresa crece, también lo hace la complejidad y la distribución de tus entornos de TI. Eso presenta un desafío: proteger tu presencia digital de distribución amplia sin control o titularidad directa. Los entornos dinámicos e interconectados permiten que las empresas obtengan importantes beneficios. Sin embargo, una interconectividad en permanente crecimiento también amplía la superficie de ataque. A medida que los atacantes se vuelven más hábiles, no solo es vital tener una imagen acabada de la presencia en línea de tu empresa, sino también poder realizar un seguimiento de sus cambios y reaccionar ante amenazas externas que tienen como objetivo exponer activos digitales.

Las organizaciones utilizan un amplio rango de herramientas de seguridad en sus operaciones de seguridad, pero aún hay amenazas digitales al acecho que requieren capacidades muy específicas: la detección y la mitigación de filtraciones de datos, supervisión de planes y esquemas de ataques de ciberdelincuentes ubicados en foros de la dark web, etc. Para ayudar a que tus analistas de seguridad exploren la visión que tiene el adversario de los recursos de tu empresa, descubran rápidamente los potenciales vectores de ataque que tienen a su disposición y ajusten tus defensas de forma acorde, Kaspersky ha creado Kaspersky Digital Footprint Intelligence.

Kaspersky Digital Footprint Intelligence ofrece lo siguiente

Reconocimiento de red

Identificación de los recursos de red y los servicios expuestos del cliente que son un potencial punto de entrada para un ataque. Análisis personalizado de vulnerabilidades existentes, con calificación y evaluación de riesgo integral adicionales en función de la calificación base de CVSS, la disponibilidad de exploits públicos, la experiencia de pruebas de penetración y la ubicación del recurso de red (hosting/infraestructura).

Protección de marca

Supervisión y bloqueo del uso no autorizado de la marca de una empresa en Internet. Identificación de cuentas y aplicaciones de redes sociales falsas, sitios web de phishing y otras actividades fraudulentas que pueden dañar la reputación de una empresa o defraudar a clientes. Baja de cuentas de redes sociales falsas y aplicaciones falsas en mercados de aplicaciones móviles.

Supervisión de la dark web

Supervisión continua de recursos de la dark web (foros, blogs de ransomware, aplicaciones de mensajería, sitios de Tor, etc.) para detectar cualquier referencia y amenaza relacionada con tu empresa, clientes y socios. Análisis de ataques selectivos activos o ataques que están en fase de planificación, campañas de APT dirigidas a tu empresa, industria y regiones de operación.

Detección de filtraciones de datos

Detección de credenciales, tarjetas bancarias, números de teléfono y otra información confidencial en riesgo de empleados, socios y clientes, que pueden utilizarse para llevar a cabo un ataque o suponen un riesgo para la reputación de la empresa.

Recursos de inteligencia

Es esencial que tengas una idea acabada de la postura de seguridad externa de tu empresa.
Para brindar esta información, analistas de seguridad de Kaspersky recopilan y combinan información de las siguientes fuentes de inteligencia:

Tus datos sin estructurar

- Direcciones IP
- Dominios de empresas
- Nombres de marca
- Palabras clave

Inventario del perímetro de la red

Red superficial, profunda y oscura

Base de conocimientos de Kaspersky

Informes analíticos

Alertas de amenazas

10 solicitudes de baja al año

Búsqueda en tiempo real en fuentes de Kaspersky, OSINT y de las redes superficial, profunda y oscura

Cómo funciona

Configuración	Recopilación	Filtrado	Reacción
Detección de información sobre los recursos digitales de la empresa	Recopilación de datos automatizada de las redes superficial, profunda y oscura, y de la base de datos de inteligencia de amenazas de Kaspersky	Detección, análisis y priorización de amenazas a cargo de analistas	Entrega de inteligencia completa

Valores empresariales

Kaspersky Digital Footprint Intelligence ofrece beneficios importantes y un valor significativo a tu organización:

Protege tu marca

Detecta amenazas potenciales en tiempo real para proteger tu reputación de marca, preservar la confianza de los clientes, reducir el riesgo de pérdidas financieras y daños a las operaciones comerciales.

Reduce los riesgos cibernéticos

Equipa a tus actores clave (directores y miembros de la junta) con información sobre los lugares donde debe concentrarse el gasto en ciberseguridad, mediante la detección de brechas en la configuración actual y los riesgos que estas suponen.

Reacciona más rápido

El contexto adicional para alertas de seguridad mejora la respuesta ante incidentes y reduce el tiempo medio de respuesta.

Reduce la superficie de ataque

Gestiona la presencia digital de tu empresa y controla recursos de red externos para minimizar los vectores de ataques y las vulnerabilidades que pueden usarse para un ataque.

Entiende a tus adversarios

Hombre prevenido vale por dos: si sabes lo que los ciberdelincuentes están planificando y la información que están intercambiando sobre tu empresa en la red oscura, estarás preparado para ellos.

Conoce lo desconocido

Mejora tu capacidad de soportar ciberataques e identifica amenazas fuera de la jurisdicción de tus equipos de seguridad internos.

Kaspersky Takedown Service

Los ciberdelincuentes crean dominios maliciosos y de phishing que se utilizan para atacar a tu empresa y a tus marcas. La incapacidad para mitigar rápidamente estas amenazas, una vez identificadas, puede provocar pérdidas de ingresos, daños a la marca, pérdida de confianza de los clientes, filtraciones de datos y otros problemas. Pero la gestión de las bajas de estos dominios es un proceso complejo, que requiere experiencia y tiempo.

Kaspersky Takedown Service mitiga rápidamente las amenazas que suponen los dominios maliciosos y de phishing antes de que puedan dañar a tu marca y tu empresa. La gestión integral del proceso ahorra tiempo y recursos valiosos de los clientes. El servicio se ofrece en todo el mundo.

Kaspersky bloquea más de 15 000 URL de phishing/estafas y previene más de un millón de intentos de hacer clic en estas URL todos los días. Nuestra amplia experiencia en el análisis de dominios maliciosos y de phishing significa que sabemos cómo recopilar toda la evidencia necesaria para demostrar que se trata de actividades malintencionadas. Nos encargaremos de la gestión de baja y tomaremos medidas rápidas para minimizar el riesgo digital, para que tu equipo pueda concentrarse en otras tareas prioritarias.

Kaspersky ofrece a sus clientes una protección efectiva de sus servicios online y reputación. Para ello, trabaja junto con fuerzas del orden internacionales, nacionales y regionales (por ejemplo, INTERPOL, Europol, la Unidad de Delitos Digitales de Microsoft, la Unidad Nacional de Delitos Tecnológicos Complejos de la Agencia de Policía de los Países Bajos y la Policía de la Ciudad de Londres), y también con equipos de respuesta a emergencias informáticas (CERT) de todo el mundo.

Visibilidad completa

Recibirás notificaciones en cada etapa del proceso, desde el registro de la solicitud hasta la baja exitosa.

Gestión integral

Gestionamos todo el proceso de baja para que tu participación sea mínima.

Cobertura global

Más allá del lugar donde esté registrado un dominio malicioso o de phishing, Kaspersky solicitará su baja desde la organización regional ante la autoridad legal correspondiente.

Integración con Kaspersky Digital Footprint Intelligence

Kaspersky Takedown Service puede adquirirse por separado, pero su integración con Kaspersky Digital Footprint Intelligence permite aprovechar al máximo la sinergia natural entre estos servicios. Kaspersky Digital Footprint Intelligence ofrece notificaciones en tiempo real sobre dominios de phishing y malware que pueden enviarse de inmediato a Kaspersky Takedown Service para su posterior bloqueo.

Cómo funciona

Puedes enviar tus solicitudes a través de Kaspersky Company Account, nuestro portal de soporte a clientes corporativos. Prepararemos toda la documentación necesaria y enviaremos la solicitud de baja a la autoridad local/regional correspondiente (CERT, registro, etc.), que tenga los derechos legales requeridos para dar de baja el dominio. Recibirás notificaciones en cada etapa del proceso hasta que el recurso solicitado se haya dado de baja correctamente.

Protección sin esfuerzo

Kaspersky Takedown Service mitiga rápidamente las amenazas que suponen los dominios maliciosos y de phishing antes de que puedan dañar a tu marca y tu empresa. La gestión integral del proceso te permite ahorrar tiempo y recursos valiosos.

Kaspersky Ask the Analyst

Los ciberdelincuentes desarrollan formas sofisticadas de atacar a las empresas todo el tiempo. El panorama volátil y de rápido crecimiento actual incluye técnicas de ciberdelito cada vez más ágiles. Las organizaciones enfrentan incidentes complejos provocados por ataques que no son de malware, ataques sin archivos, ataques "living-off-the-land", exploits de día cero y combinaciones de todos ellos integrados en amenazas complejas, como los ataques APT y los ataques selectivos.

En una era de ciberataques que ponen de rodillas a las empresas, los profesionales de la ciberseguridad son más importantes que nunca. Pero encontrarlos y conservarlos no es fácil. Y, aunque tengas un equipo de ciberseguridad establecido, no siempre puedes esperar que tus expertos combatan amenazas sofisticadas por su cuenta. Deben tener la posibilidad de recurrir a asistencia de expertos independientes. Los expertos externos pueden echar luz sobre las rutas probables de APT y ataques complejos, y ofrecer asesoramiento procesable sobre la forma más decisiva de eliminarlos.

La investigación de amenazas continua permite que Kaspersky descubra, infiltre y supervise comunidades cerradas y foros oscuros de todo el mundo, frecuentados por adversarios y ciberdelincuentes. Nuestros analistas aprovechan este acceso para detectar e investigar proactivamente las amenazas más dañinas y prominentes, además de amenazas diseñadas para atacar organizaciones específicas.

Kaspersky Ask the Analyst amplía nuestra cartera de productos de inteligencia de amenazas y te permite solicitar asesoramiento y panoramas sobre amenazas específicas que enfrentas o son de tu interés. El servicio adapta las potentes capacidades de investigación e inteligencia de amenazas de Kaspersky a tus necesidades específicas y te permite construir defensas resilientes contra amenazas dirigidas a tu organización.

Entregables de Kaspersky Ask the Analyst (suscripción unificada a pedido)

APT y crimeware

Información adicional sobre informes publicados e investigaciones continuas (además del servicio de informes de inteligencia de APT o crimeware)

Descripciones de amenazas, vulnerabilidades e IOC relacionados

- Descripción general de una familia de malware específica
- Contexto adicional de amenazas (hashes relacionados, URL, mando y control, etc.)
- Información sobre una vulnerabilidad específica (su nivel de criticidad y los mecanismos de protección correspondientes en los productos de Kaspersky)

Solicitudes relacionadas con ICS

- Información adicional sobre los informes publicados
- Información sobre vulnerabilidades de ICS
- Estadísticas y tendencias de amenazas de ICS por región e industria
- Información de análisis de malware de ICS sobre regulaciones o estándares

Inteligencia de la dark web

- Investigación sobre determinados artefactos, direcciones IP, nombres de dominio, nombres de archivo, correos electrónicos, enlaces o imágenes de la dark web
- Búsqueda y análisis de información

Análisis de malware

- Análisis de muestras de malware
- Recomendaciones de acciones de corrección posteriores

Cómo funciona

Kaspersky Ask the Analyst puede comprarse por separado o de forma adicional a nuestros servicios de inteligencia de amenazas. Puedes enviar tus solicitudes a través de Kaspersky Company Account, nuestro portal de soporte a clientes corporativos. Te responderemos por correo electrónico, pero, si hace falta y estás de acuerdo, podemos organizar una videoconferencia o una sesión de pantalla compartida. Una vez aceptada tu solicitud, te informaremos del plazo estimado para su procesamiento.

Casos de uso

1. Aclarar cualquier detalle en informes de inteligencia de amenazas publicados previamente
2. Obtener inteligencia adicional de IoC ya proporcionados
3. Accede a detalles sobre vulnerabilidades y recomendaciones para protegerte contra su explotación
4. Recibir más detalles sobre las actividades específicas de la red oscura que te interesan
5. Acceder al informe general de un malware que incluye el comportamiento del malware, su potencial impacto y detalles sobre cualquier actividad relacionada observada por Kaspersky
6. Prioriza de manera efectiva alertas e incidentes con información contextual detallada y categorización de los IOC relacionados a través de informes breves
7. Solicitar ayuda para identificar si una actividad inusual está relacionada con un actor de crimeware o APT
8. Envía archivos de malware para su análisis integral, que permitirá entender el comportamiento y la funcionalidad de las muestras proporcionadas

Beneficios de Kaspersky Ask the Analyst

Amplía tus conocimientos

Obtén acceso a pedido a expertos de la industria sin necesidad de realizar búsquedas e invertir en la contratación de especialistas de tiempo completo, algo muy difícil de lograr

Acelera investigaciones

Evalúa el alcance de los incidentes y priorízalos de forma efectiva en función de información contextual personalizada y detallada

Responde rápido

Responde a amenazas y vulnerabilidades con rapidez, gracias a nuestro asesoramiento para bloquear ataques a través de vectores conocidos

Amplía tus conocimientos y recursos

Kaspersky Ask the Analyst te permite acceder a un grupo central de investigadores de Kaspersky caso por caso. El servicio ofrece una comunicación detallada entre expertos para que puedas ampliar tus capacidades existentes gracias a nuestros conocimientos y recursos exclusivos.

Conclusión

Contrarrestar las ciberamenazas actuales requiere un panorama integral de las tácticas y herramientas utilizadas por actores de amenazas. Generar esta inteligencia e identificar las medidas correctivas más efectivas requiere una dedicación constante y altos niveles de especialización. Con petabytes de datos complejos que pueden minarse, tecnologías de aprendizaje automático avanzadas y un conjunto único de expertos mundiales, trabajamos para asistir a nuestros clientes de todo el mundo con el objetivo de que logren mantenerse inmunes incluso a ciberataques previamente desconocidos.

Beneficios clave

Permite una visibilidad de amenazas global, una detección oportuna de ciberamenazas, la priorización de alertas de seguridad y una respuesta efectiva a incidentes de seguridad de la información

Los panoramas exclusivos de las tácticas, las técnicas y los procedimientos utilizados por los actores de amenazas entre diferentes industrias y regiones permiten una protección proactiva contra amenazas selectivas y complejas

Un panorama integral de tu postura de seguridad con recomendaciones procesables sobre estrategias de mitigación te permitirá concentrar tu estrategia de defensa en áreas identificadas como objetivos de ciberataques principales

Evita el agotamiento de los analistas y ayuda a que tu fuerza de trabajo pueda concentrarse en amenazas genuinas

La respuesta a incidentes mejorada y acelerada, además de las capacidades de búsqueda de amenazas, ayuda a reducir el "tiempo de permanencia" del ataque y a minimizar significativamente los posibles daños

Kaspersky Threat Intelligence

Más información

www.kaspersky.es

#kaspersky
#bringonthefuture