Anticípese a sus adversarios

Kaspersky Contra amenazas Intelligence

kaspersky preparados para el futuro

Kaspersky
Threat Intelligence

Kaspersky Threat Intelligence

Threat Intelligence de Kaspersky te proporciona acceso a la inteligencia que necesitas para mitigar ciberamenazas de la mano de nuestro equipo líder de investigadores y analistas.

Gracias a nuestros conocimientos, experiencia e inteligencia avanzada de todos los aspectos relativos a la ciberseguridad, en Kaspersky nos hemos convertido en el partner de confianza de las fuerzas del orden y los organismos gubernamentales más importantes del mundo, entre las que se incluyen la Interpol e importantes equipos CERT. Kaspersky Threat Intelligence te ofrece acceso inmediato a inteligencia de amenazas táctica, operativa y estratégica.

Además, Kaspersky Threat Intelligence ofrece una visión integral del panorama mundial de las amenazas, ya que combina fuentes de inteligencia, fuentes de datos de amenazas e investigación interna, todo ello analizado por nuestro equipo de especialistas para ofrecer información práctica que permita a las organizaciones protegerse contra las ciberamenazas.

Táctico

Información de bajo nivel y muy perecedera que respalda las operaciones de seguridad y la respuesta a incidentes. Un ejemplo de inteligencia táctica son los IOC relacionados con la ejecución de un ataque recientemente detectado.

Funciones:
- Analista de SOC

Sistemas:
- SIEM
- NGFW
- IPS
- IDS
- SOAR

Procesos:
- Búsqueda de amenazas
- Supervisión

Operativo

Este nivel suele incluir datos sobre campañas y TTP de orden superior. Puedes incluir información sobre la atribución de ciberdelincuentes específicos, así como sobre las capacidades e intenciones de los adversarios.

Funciones:
- Analista L3 de SOC
- Analista de DFIR
- Analista de IR

Sistemas:
- SIEM
- NTA
- EDR/XDR
- TIP

Procesos:
- INCIDENT RESPONSE
- Búsqueda de amenazas

Estratégico

Este nivel apoya al personal ejecutivo y a las juntas directivas en la toma de decisiones serias sobre evaluación de riesgos, asignación de recursos y estrategia de la organización. Esta información incluy e tendencias, motivaciones de los ciberdelincuentes y sus clasificaciones.

Funciones:
- CISO
- CTO
- Director de IT
- DIRECTOR EJECUTIVO

Procesos:
- Creación de una estrategia de IS
- Concienciación

Esquema de la aplicación Kaspersky Threat Intelligence

Kaspersky Threat Intelligence te da poder

Identifica y prevén amenazas de forma proactiva

Kaspersky Threat Intelligence te mantiene informado sobre las últimas amenazas y vulnerabilidades y te permite tomar medidas proactivas para proteger tus sistemas antes de que se produzca un ataque.

Obtén visibilidad de tu huella digital

Kaspersky Threat Intelligence te proporciona una visión integral de tu huella digital, e incluye cualquier activo que pueda ser vulnerable a un ataque o riesgo.

Mejore su capacidad de detección de amenazas

Kaspersky Threat Intelligence te permite aumentar tus soluciones de seguridad existentes con la inteligencia frente a amenazas más reciente, lo que mejora tu capacidad de detección y bloqueo de amenazas avanzadas.

Mejora la respuesta ante incidentes

Kaspersky Threat Intelligence ofrece información en tiempo real sobre amenazas emergentes e indicadores de peligro, para que puedas responder con rapidez y eficacia a los incidentes.

Cumple con normativas y estándares

Todas las empresas están sujetas a diversos estándares y normativas dentro de su sector. Kaspersky Threat Intelligence respalda el cumplimiento de normativas, ya que te brinda ayuda para cumplir con estos requisitos.

Mejora los conocimientos internos

El equipo de especialistas de Kaspersky se encuentra entre los investigadores con mayor experiencia y aprecio del sector, y brinda una gran cantidad de conocimientos y experiencia a sus equipos de seguridad de la información.

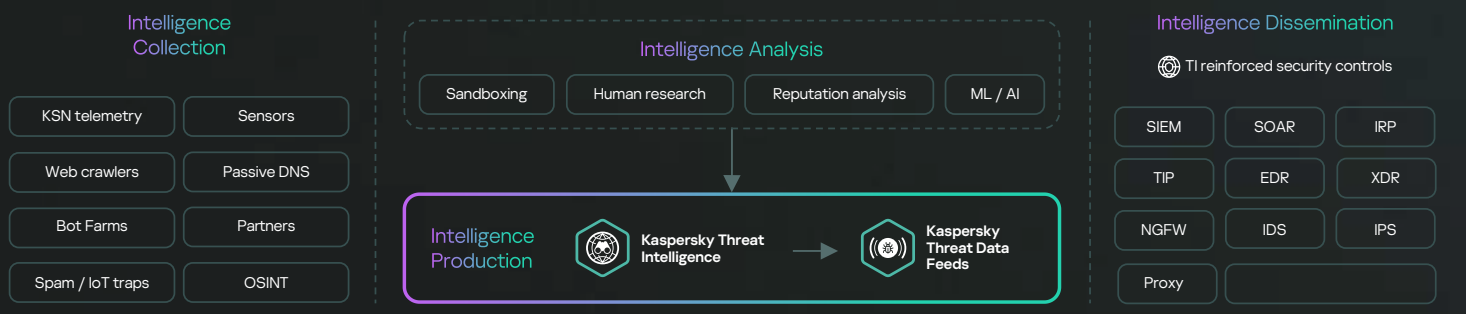
Kaspersky
Threat Data

Kaspersky Threat Data Feeds

Los ciberataques ocurren diariamente. La frecuencia, la complejidad y la ofuscación de las ciberamenazas crecen de forma constante a medida que intentan comprometer tus defensas. Los adversarios utilizan complicados esquemas de ataque de intrusión, campañas, así como tácticas, técnicas y procedimientos (TTP) personalizados para interrumpir las actividades de tu empresa o dañar a tus clientes. Se necesitan nuevos métodos de protección basados en la inteligencia de amenazas.

Mediante la integración en los sistemas de seguridad existentes, como las plataformas SIEM, SOAR y de inteligencia de amenazas de las fuentes de inteligencia de amenazas actualizadas que contienen información sobre direcciones IP, URL y hashes de archivos sospechosos y peligrosos, los equipos de seguridad pueden automatizar el proceso de análisis inicial de alertas y, al mismo tiempo, ofrecer a sus especialistas en evaluación suficiente contexto para identificar de inmediato las alertas que se deben investigar o escalar a los equipos de Respuesta a Incidentes para una mayor investigación y respuesta.

El servicio Kaspersky Threat Data Feed ofrece información sobre la inteligencia frente a amenazas en tiempo real para permitirles a las organizaciones industriales proteger sus redes y sistemas de las ciberamenazas. Las fuentes de datos incluyen información sobre malware, sitios web de phishing y las últimas vulnerabilidades y exploits conocidos, y otros tipos de ciberamenazas, e información que te permitirá bloquear el tráfico malicioso, actualizar tu software de seguridad y tomar otras medidas de protección contra los ciberataques.



1

Los datos se recopilan a partir de una amplia variedad de fuentes de confianza, como Kaspersky Security Network y nuestras propias arañas web, el servicio de supervisión de amenazas de redes de bots (rastrea redes de bots y sus objetivos las 24 horas del día, los 7 días de la semana), trampas de spam, datos de grupos de investigación, partners, y mucho más.

2

Toda la información recopilada se verifica y depura con atención y en tiempo real mediante diversos métodos de preprocesamiento: entornos de prueba, análisis estadístico y heurístico, herramientas de similitud, elaboración de perfiles de comportamiento y análisis de especialistas.

3

Las fuentes de datos permiten recopilar información sobre amenazas acerca de una alerta o incidente, y profundizar en los detalles. También ayuda a responder a las preguntas "¿Quién? ¿El qué? ¿Dónde? y ¿por qué?", y a identificar el origen de un ataque, lo que permite tomar decisiones rápidas para proteger tu empresa de amenazas de cualquier complejidad.

Datos contextuales

Los datos contextuales ayudan a revelar una "visión de conjunto", lo que mejora la validación y complementación de un uso variado de los datos. Las entradas de las fuentes proporcionadas por Kaspersky contienen los siguientes datos contextuales que te permiten confirmar y priorizar con rapidez las amenazas:

1. Nombres de amenaza
2. Direcciones IP y nombres de dominio de recursos web maliciosos
3. Hashes de archivos maliciosos
4. Objetos vulnerables y en riesgo
5. tácticas, técnicas y procedimientos de ataque según la clasificación de MITRE ATT&CK
6. Marcas de tiempo
7. Geolocalización
8. Popularidad, etc.

Fuentes de datos de amenazas de Kaspersky Beneficios

Mejora y acelera tu respuesta ante incidentes y tus capacidades de análisis forense

automatizando el proceso de evaluación inicial y proporcionando a sus analistas de seguridad el contexto suficiente para identificar inmediatamente las alertas que se deben investigar o escalar a los equipos de respuesta de incidentes para una mayor investigación y respuesta.

Refuerza tus soluciones de seguridad

como SIEM, firewalls, IPS/IDS, proxy de seguridad, soluciones DNS, protección contra APT con indicadores de compromiso (IOC) en constante actualización y contexto útil, con el fin de proporcionar información sobre ciberataques y una mayor comprensión de la intención, las capacidades y los objetivos de sus adversarios. Los principales SIEM (como ArcSight, IBM QRadar, MS Sentinel, Splunk, etc.) y las plataformas de TI son totalmente compatibles.

Evita la filtración de activos confidenciales y propiedad intelectual

de los equipos infectados fuera de tu organización. Detecta rápidamente los activos infectados para proteger la reputación de tu marca, mantener tu ventaja competitiva y asegurar las oportunidades de negocio.

Haz crecer tu empresa de MSSP

proporcionando inteligencia frente a amenazas líder del sector como servicio premium a tus clientes. Como CERT, mejora y amplía tus capacidades de identificación y detección de ciberamenazas.

Kaspersky CyberTrace

Kaspersky CyberTrace

El crecimiento continuo de la cantidad de fuentes de datos sobre amenazas y de inteligencia frente a amenazas disponibles dificulta que las empresas determinen qué información es relevante para ellas. Al mismo tiempo, la inteligencia frente a amenazas se incluye en diferentes formatos e incluye una gran cantidad de indicadores de compromiso (IOC), lo que dificulta su procesamiento por parte de los SIEM o los controles de seguridad de red.

Mediante la integración de la inteligencia frente a amenazas actualizada al minuto y legible por máquinas en los controles de seguridad existentes, como los SIEM, los centros de operaciones de seguridad pueden automatizar el proceso inicial de evaluación al tiempo que ofrecen a sus especialistas de primer nivel el contexto suficiente para identificar de inmediato las alertas que se deben investigar o escalar a los equipos de respuesta ante incidentes para una mayor investigación y respuesta.

Kaspersky CyberTrace es una plataforma de inteligencia frente a amenazas que facilita una integración perfecta de las fuentes de datos sobre amenazas con soluciones de SIEM para ayudar a los analistas a aprovechar de manera más eficaz la inteligencia frente a amenazas de su flujo de trabajo de operaciones de seguridad existente. Se integra en cualquier fuente de inteligencia de amenazas (Kaspersky, otros proveedores, OSINT o sus fuentes de clientes) en formatos JSON, STIX, XML y CSV y es compatible con la integración inmediata en varias fuentes de registro y soluciones de SIEM.

Aspectos destacados

Las páginas con información detallada sobre cada indicador proporcionan un análisis aún más acabado. Cada página presenta toda la información sobre un indicador de todos los proveedores de inteligencia frente a amenazas (desduplicación) para que los analistas puedan evaluar las amenazas en los comentarios y añadir inteligencia interna sobre cada indicador.

Las estadísticas de uso de fuentes para medir la eficacia de las fuentes integradas y de la matriz de intersección de las fuentes ayudan a elegir los proveedores de inteligencia frente a amenazas más valiosos.

El etiquetado de IoC simplifica la administración. Crea cualquier etiqueta y especifica tu peso (importancia) y úsala para etiquetar IoC manualmente. También puedes ordenar y filtrar IoC de acuerdo con estas etiquetas y sus pesos

Un gráfico de investigación permite explorar de forma visual datos y detecciones almacenados en CyberTrace y descubrir características de las amenazas

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

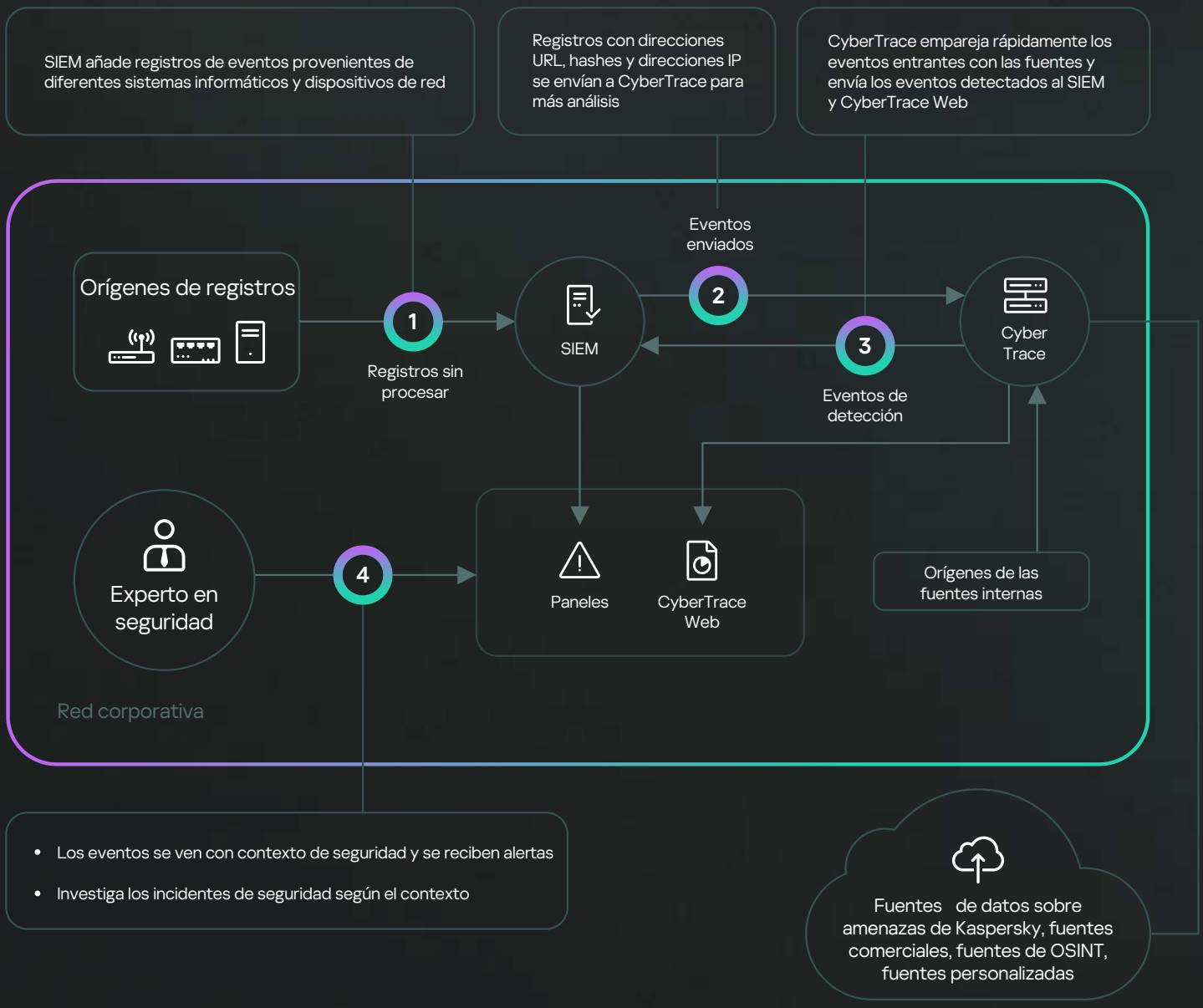
La función de correlación histórica (retroscan) te permite analizar los elementos observables de eventos previamente comprobados utilizando las fuentes más recientes para encontrar amenazas no detectadas anteriormente.

La multitenencia es compatible con los MSSP y los casos de uso de grandes empresas.

Envía eventos de detección a las soluciones de SIEM, lo que reduce tu carga y la de los analistas.

HTTP RestAPI te permite buscar y gestionar la inteligencia frente a amenazas

Funcionamiento



Kaspersky CyberTrace analiza los registros y eventos entrantes, concilia rápidamente los datos resultantes con las fuentes y genera sus propias alertas de detección de amenazas, lo que reduce de modo considerable la carga de SIEM.

Beneficios del uso de CyberTrace con las fuentes de datos de amenazas de Kaspersky

Sintetizar y priorizar eficazmente grandes cantidades de alertas de seguridad

Mejorar y acelerar los procesos de evaluación y respuesta inicial.

Formar una defensa proactiva e inteligente

Identifica inmediatamente las alertas críticas para tu empresa y comunícalas a los equipos de IR

Kaspersky
Threat Lookup

Kaspersky Threat Lookup

La ciberdelincuencia no tiene límites y sus capacidades técnicas mejoran rápidamente. Los ciberdelincuentes utilizan recursos de la Web oculta para amenazar a sus objetivos, por lo que los ataques son cada vez más sofisticados. La frecuencia, la complejidad y la confusión en torno a las ciberamenazas crecen de forma sostenida a medida que se producen nuevos intentos de poner en peligro tus defensas. Los atacantes utilizan complicadas cadenas de ataques, así como tácticas, técnicas y procedimientos (TTP) personalizados en sus campañas para interrumpir las actividades de su negocio, robar sus activos y dañar a sus clientes.

Kaspersky Threat Lookup ofrece todos los conocimientos de Kaspersky sobre las ciberamenazas y sus relaciones reunidos en un único y potente servicio web. El objetivo es proporcionar a los equipos de seguridad la mayor cantidad de datos posible, evitando los ciberataques antes de que afecten a tu organización. La plataforma recupera la inteligencia de amenazas más reciente y detallada sobre URL, dominios, direcciones IP, hash de archivos, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS y DNS, atributos de archivos, datos de geolocalización, cadenas de descargas, marcas de tiempo, etc. El resultado es una visibilidad global de las amenazas nuevas y emergentes, que te ayuda a proteger tu organización y mejorar tus índices de respuesta ante incidentes.

Funcionamiento

Objetos para analizar

Aspectos destacados

Inteligencia de confianza

un atributo clave de Kaspersky Threat Lookup es la fiabilidad de nuestros datos de inteligencia frente a amenazas, que se mejoran con contexto útil. Kaspersky está a la vanguardia de las pruebas antimalware, demostrando la calidad inigualable de nuestra inteligencia de seguridad al proporcionar los más altos índices de detección, sin apenas falsos positivos.

Búsqueda de amenazas

hay que ser proactivo en la prevención, detección y respuesta a los ataques, para minimizar su impacto y frecuencia. Se debe realizar un seguimiento y eliminar drásticamente los ataques lo antes posible. Cuanto antes se detecte una amenaza, menos daños provocará, antes será posible llevar a cabo las reparaciones necesarias y con mayor prontitud podrán volver a la normalidad las operaciones de red.

Fácil de usar

Acceso a la interfaz web o API RESTful. uso del servicio en modo manual mediante una interfaz web (a través de un navegador web) o acceso a través de una sencilla API RESTful, según las preferencias

Amplia gama de formatos de exportación

Exporta indicadores de compromiso (IoC) o contexto útil sobre los formatos de uso compartido legibles por máquina más ampliamente usados y organizados (como STIX, OpenIOC, JSON, Yara, Snort o incluso CSV) para sacar el máximo beneficio de la inteligencia frente a amenazas, automatizar el flujo de trabajo de operaciones o integrarlos en los controles de seguridad como SIEM.

Kaspersky Threat Lookupbeneficios

1

Realice búsquedas exhaustivas sobre indicadores de amenaza con un contexto de amenazas altamente validado que le permite priorizar los ataques y enfocarse en mitigar las amenazas que impliquen el mayor riesgo para su negocio.

2

Diagnostica y analiza de forma más eficiente los incidentes de seguridad de los hosts y la red, y prioriza las señales de los sistemas internos frente a amenazas desconocidas

3

Potencia tus capacidades de respuesta ante incidentes y de búsqueda de amenazas para alterar el esquema del ataque antes de que los sistemas y datos importantes se vean comprometidos

4

Buscar indicadores de amenaza desde una interfaz web o la API RESTful.

5

Examinar datos avanzados, como certificados, nombres usados habitualmente, rutas de archivos o URL relacionadas, para detectar nuevos objetos sospechosos.

6

Comprueba si el objeto detectado es común o único y comprende por qué un objeto se debe tratar como malicioso

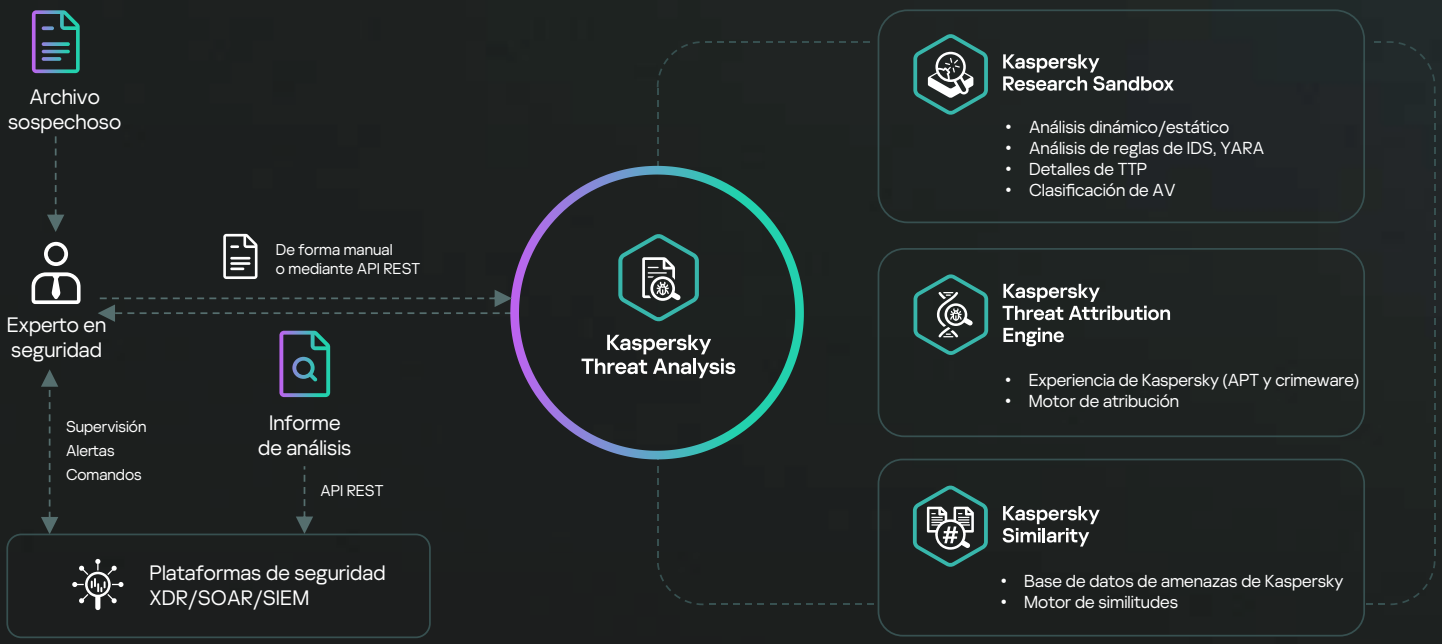
Kaspersky
Threat Analysis

Kaspersky Threat Analysis

Ante una potencial ciberamenaza, las decisiones que tomes y tu habilidad para tomarlas pueden resultar aspectos críticos. En la actualidad, es imposible evitar los ataques dirigidos con herramientas antivirus tradicionales. Los motores antivirus son capaces de detener solo amenazas conocidas y sus variaciones, mientras que los sofisticados actores de las amenazas usan todos los medios a su disposición para evadir la detección automática. La cantidad de alertas de seguridad procesadas por los centros de operaciones de seguridad (SOC) crece exponencialmente día tras día. Con la cantidad de muestras de malware que se generan cada día, resulta casi imposible priorizar, evaluar y validar con eficacia las alertas.

Para ayudar a los investigadores de seguridad a mantenerse informados acerca de las amenazas emergentes y existentes, Kaspersky proporciona un único marco resistente para automatizar los análisis de rutina de archivos sospechosos. Además de contar con herramientas de análisis de amenazas tradicionales como el sandbox, Kaspersky Threat Analysis ofrece tecnologías de atribución de última generación y otras soluciones relacionadas, un enfoque híbrido que brinda un análisis de amenazas eficiente, para poder tomar decisiones informadas y mantener la infraestructura protegida. Kaspersky Threat Analysis se proporciona a través de interfaces web unidas y RESTful.

Kaspersky Threat Analysis componentes



Kaspersky
Research Sandbox

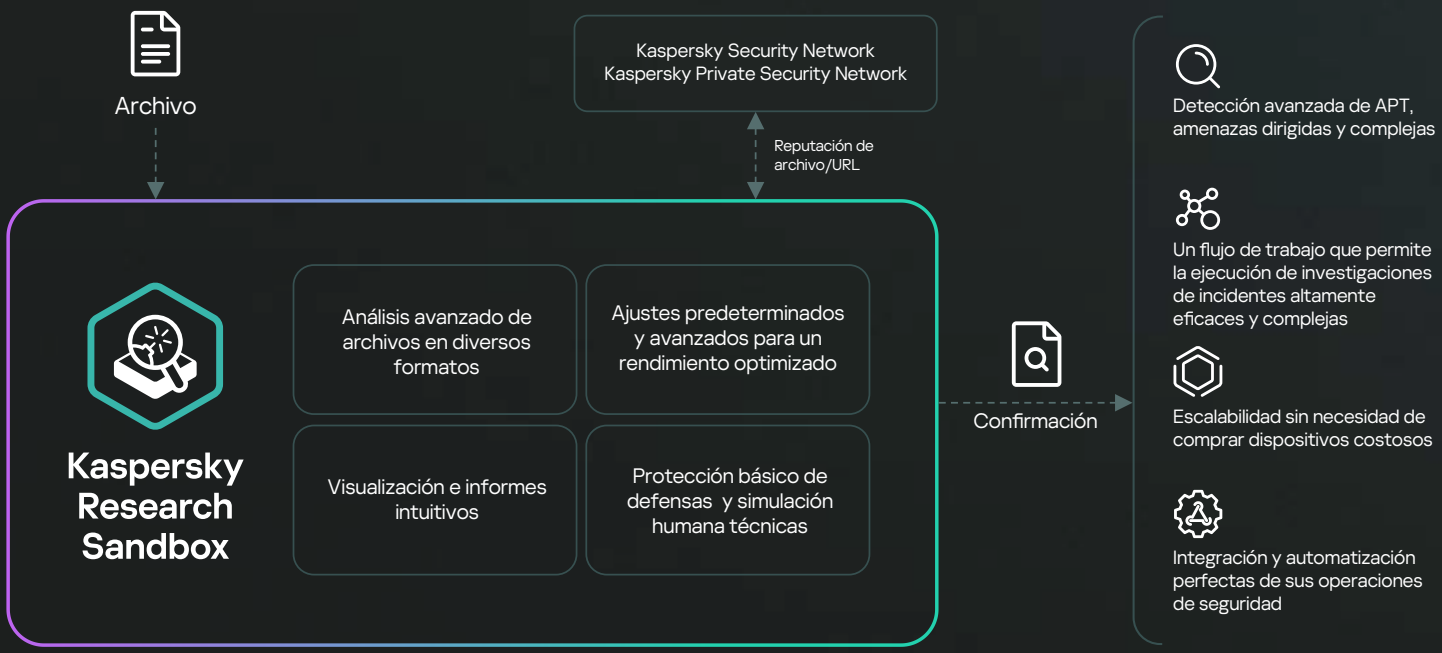
Kaspersky Research Sandbox

Kaspersky Research Sandbox se ha desarrollado directamente a partir del entorno de sandbox de nuestro laboratorio, una tecnología con más de dos décadas de evolución. Incorpora todo el conocimiento sobre los comportamientos de malware que hemos adquirido durante nuestra investigación continua de amenazas, lo que nos permite detectar más de 420 000 objetos maliciosos nuevos cada día.

Kaspersky Research Sandbox permite investigar los orígenes de las muestras de archivos, recopilar IOC basados en el análisis de comportamiento y detectar objetos maliciosos no vistos anteriormente. Ofrece un enfoque híbrido, que combina el análisis de comportamiento y las técnicas antievasión más sólidas con tecnologías de simulación humana, como el clic automático, el desplazamiento de documentos y los procesos ficticios.

Esta tecnología, que se implementa en las instalaciones, impide la exposición de datos fuera de la organización. Kaspersky Research Sandbox en las instalaciones también permite crear entornos de ejecución personalizados para análisis al adaptarlos a entornos reales, lo que aumenta la precisión de la detección de amenazas y la velocidad de la investigación.

Funcionamiento



Aspectos destacados del producto

- Tecnología patentada
- Análisis automatizado de objetos en entornos Windows, Linux y Android
- Posibilidad de analizar más de 200 tipos de archivos con informes de análisis detallados
- SOC de Kaspersky utiliza más de 700 indicadores de ataque propios que cubren el 100 % de todas las tácticas, técnicas y procedimientos (TTP) conocidos de los adversarios. Más de 1000 búsquedas únicas para la extracción de TTP mediante MITRE ATT&CK
- Técnicas antievasión y tecnologías de simulación humana avanzadas
- Puntuación de amenazas en función de métricas y datos obtenidos durante la ejecución del archivo que muestra el nivel de riesgo del objeto analizado
- Reglas de Suricata preconfiguradas para inspeccionar el tráfico de red generado durante la ejecución de archivos
- Incluye la carga de muestras manual y API REST mejorada para su integración en flujos de trabajo automatizados

Kaspersky
Threat Attribution
Engine

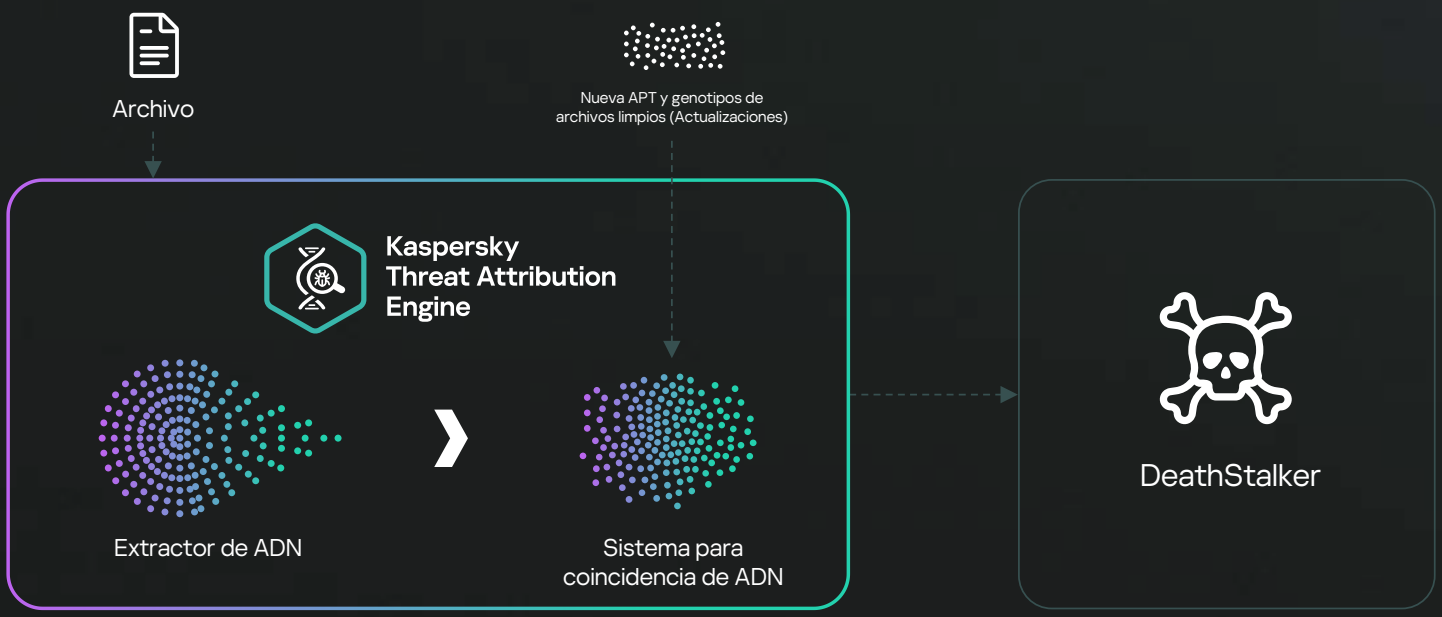
Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine es una herramienta de análisis exclusiva que proporciona información acerca del origen de malware de alto perfil y sus posibles autores. Vincula rápidamente un archivo sospechoso con amenazas persistentes avanzadas (APT), actores y campañas conocidos mediante un algoritmo único y una base de datos especial que contiene muestras de malware APT y el mayor conjunto de archivos limpios de la industria, recopilados por expertos de Kaspersky durante los últimos 25 años, y más.

Hacemos seguimiento a más de 1100 atacantes y campañas, y publicamos más de 200 informes sobre inteligencia de amenazas al año. Nuestra investigación continua respalda una recopilación de APT que contiene más de 100 000 archivos que, en combinación con el uso de herramientas automatizadas, ofrecen niveles de atribución de una exactitud sobresaliente.

El producto ofrece un enfoque único hacia la comparación de muestras similares al tiempo que garantiza índices de falsos positivos casi nulos. Todos los ataques nuevos se pueden vincular rápidamente con un malware APT conocido, grupos de hackers y ataques dirigidos anteriores, lo cual ayuda a distinguir las amenazas de alto riesgo de los incidentes menos serios, con el fin de que puedas tomar medidas proactivas a tiempo y así evitar que un atacante logre un punto de apoyo en tu sistema. Kaspersky Threat Attribution Engine se puede implementar en entornos seguros y herméticos, lo que restringe el acceso de cualquier tercero a la información procesada y a los objetos enviados. La implementación local ofrece funciones adicionales para agregar agentes y muestras propios con el fin de detectar muestras similares a archivos de tu colección privada, así como exportar reglas YARA para realizar búsquedas automatizadas de archivos similares en tu infraestructura e integrarse con soluciones de terceros.

Funcionamiento



Método debúsqueda patentado

Para vincular el malware con las entidades de atribución, Kaspersky Threat Attribution Engine utiliza un método patentado único
de búsqueda de genotipos y cadenas similares entre los archivos. Este método abarca lo siguiente:

1

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

- Genotipos: piezas distintivas de código binario.
- Cadenas: cadenas distintivas de caracteres.

2

Análisis automático de los archivos analizados en busca de genotipos y cadenas que se parezcan a los genotipos y las cadenas de muestras de APT que se hayan analizado anteriormente o que ya estén vinculados con entidades de atribución.

3

En función de genotipos y cadenas similares que se hayan encontrado en las muestras de APT, generación de un informe sobre el origen de la muestra analizada, entidades de atribución relacionadas y toda similaridad entre esta muestra y muestras conocidas de APT.

Aspectos destacados del producto

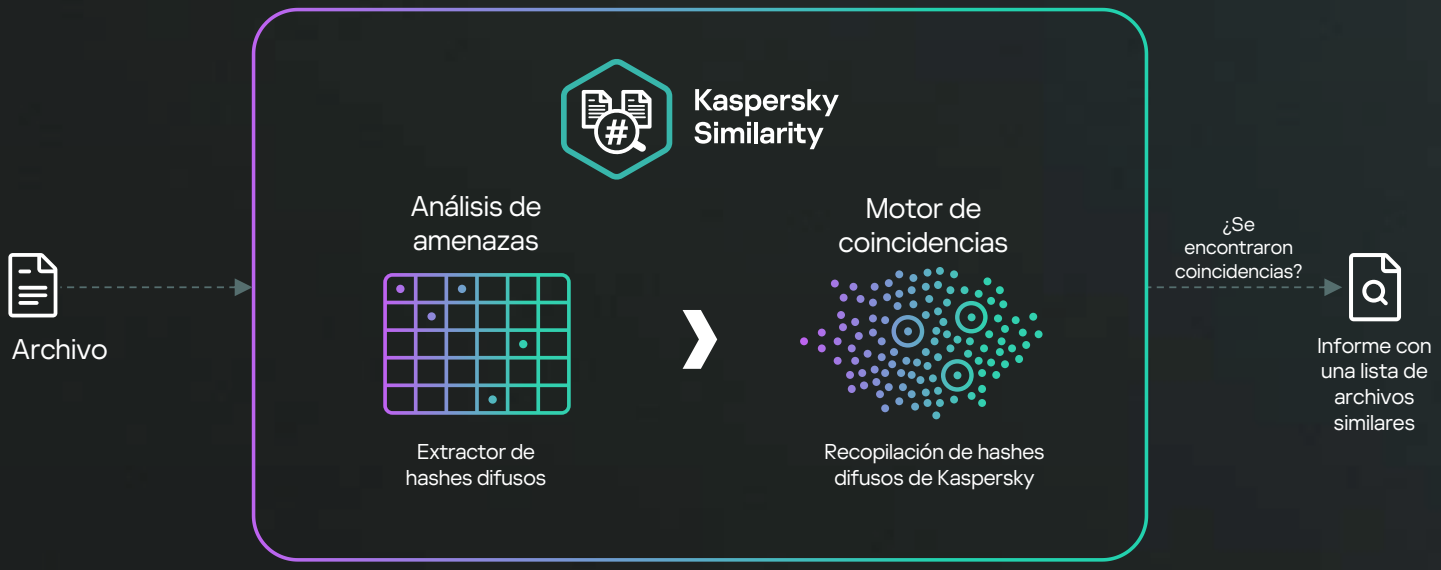
- Tecnología patentada
- Acceso instantáneo a un repositorio de datos seleccionados sobre cientos de actores, muestras y campañas de APT.
- Incluye la carga de muestras manual y API REST mejorada para su integración en flujos de trabajo automatizados
- Operatividad para descomprimir archivos protegidos con contraseña con contraseñas personalizadas
- Exportación a formato STIX 2.1 (los formatos TXT y JSON también son compatibles) para un análisis más automatizado de registros de seguridad o integración con soluciones de terceros
- Admite la implementación en infraestructuras en la nube como Amazon Web Services (AWS), lo cual permite una configuración rápida del producto y un ahorro de costes, dado que no se necesita invertir en hardware de antemano

Kaspersky Intelligence Reporting

Kaspersky Similarity

Kaspersky Similarity es una práctica herramienta para identificar archivos con funciones similares basada en la tecnología desarrollada por los expertos de Kaspersky para proteger contra amenazas desconocidas y ocultas. La tecnología utiliza más de 50 tipos únicos de hashes especiales y una base de datos de muestras de malware acumulada por Kaspersky durante más de 25 años y que contiene millones de archivos maliciosos para garantizar la máxima precisión y confianza en los resultados.

Kaspersky Similarity te permite buscar malware similar (por ej., evasivo) y buscarlo en la infraestructura para que estés seguro de que incluso un ligero cambio de la muestra, realizado por el adversario, no escapa del radar de seguridad.



Informes de similitud

Los expertos de Kaspersky han creado un conjunto de hashes para determinar la similitud entre diferentes archivos sobre la base de estos atributos.

Kaspersky Similarity permite a los usuarios enviar un archivo sospechoso, extraer sus hashes y compararlos con hashes de archivos anteriores en la base de datos de amenazas de Kaspersky. Si se encuentran coincidencias, genera una lista de hashes para los principales archivos maliciosos similares, conocidos por Kaspersky y clasificados sobre la base de la puntuación de similitud. El informe incluye el contexto adicional, con metadatos para cada archivo similar:

- Confianza de similitud
- Estado del archivo (malware, adware u otros)
- Nombre de la amenaza
- Marcas horarias de la primera y última detección
- Cantidad de coincidencias (detecciones)
- Hash de archivo
- Tipo de archivo
- Tamaño del archivo

Aspectos destacados

- Tecnología patentada
- Utiliza una de las bases de datos de archivos maliciosos y limpios más amplias de la industria, recopilada durante los últimos 25 años, lo que permite una cobertura máxima para mayor exactitud en las comparaciones.
- Incluye la carga de muestras manual y API REST mejorada para su integración en flujos de trabajo automatizados
- Los expertos de Kaspersky llevan mucho tiempo usando esta tecnología para explorar nuevas amenazas y ofrecer una protección incluso mayor en nuestros productos, lo que se demuestra de manera regular a través de las buenas calificaciones recibidas periódicamente en pruebas independientes:

Más información

Kaspersky Threat Lookupbeneficios

1

Kaspersky Research Sandbox potencia tus actividades forenses y de respuesta ante incidentes, lo que permite escalar respecto del procesamiento de archivos automático sin tener que adquirir dispositivos costosos ni preocuparse por los recursos del sistema.

2

La atribución correcta y oportuna con Kaspersky Threat Attribution Engine ayuda a definir el agente de la amenaza con la lista completa de TTP, proporcionando una visión completa del vector de ataque con pasos claros de mitigación que permiten reducir los tiempos de respuesta ante incidentes de meses a minutos.

3

Detecta amenazas evasivas gracias a Kaspersky Similarity, que permite encontrar muestras maliciosas creadas especialmente para eludir las tecnologías antimalware tradicionales y detectar así los ataques de APT más sofisticados, que pueden durar años sin ser rastreados.

Kaspersky Intelligence Reporting

Kaspersky Threat Intelligence Reporting

Contrarrestar las ciberamenazas modernas requiere una visión global de las tácticas, las técnicas y los procedimientos que utilizan los actores de amenazas. Mientras que los mandos y controles, y las herramientas que se utilizan en los ataques cambian con frecuencia, a los atacantes les resulta difícil modificar su comportamiento y métodos durante la ejecución de sus ataques. Identificar y exponer estos patrones lo antes posible ayuda a implementar mecanismos defensivos eficaces de antemano, detener a los cibercriminales e interrumpir la cadena de ataque.

La suscripción a Kaspersky Threat Intelligence Reporting proporciona un acceso continuo y exclusivo a nuestra investigación, lo que proporciona información actualizada sobre las amenazas más peligrosas, permitiéndote a ti y a tu equipo de seguridad implementar de forma proactiva una estrategia eficaz para la detección de ataques de forma oportuna, así como minimizar los daños de amenazas similares.

Si bien solo un pequeño porcentaje de nuestras investigaciones se hacen públicas, los Informes de inteligencia de Kaspersky te ofrecen un acceso privilegiado a la información más actualizada sobre las amenazas más recientes. Nuestros expertos supervisan continuamente las actividades de los ciberdelincuentes, e identifican los ataques selectivos más sofisticados y peligrosos, las campañas de ciberespionaje, las muestras de malware y cifrado, y las últimas tendencias de la ciberdelincuencia en todo el mundo.

+ 200
informes privados al año

+ 300
actores de amenazas

+ 500
spear phishing.

+ 2500
Reglas YARA

170 000+
IOC

Los informes analíticos incluyen lo siguiente:

Perfiles de actores de amenazas

Asignación a MITRE ATT&CK

Resumen ejecutivo (información orientada al nivel C)

El análisis técnico exhaustivo incluye lo siguiente:

- Métodos de ataque
- Exploits utilizados
- Descripción del malware
- Descripción de protocolos e infraestructura de C&C
- Análisis de víctimas
- Análisis de filtración de datos
- Atribuciones

Indicadores de compromiso (IOC) y reglas YARA/Suricata

Recomendaciones de los expertos de Kaspersky

Ofrecemos varias opciones de informes comerciales en función de tus necesidades y de las características específicas de tu organización:

Kaspersky APT Intelligence Reporting

Proporciona información sobre ciberamenazas sofisticadas y selectivas a largo plazo que a menudo proceden de grupos bien organizados y financiados. Incluye información sobre diversos grupos de APT de todo el mundo y sus tácticas, técnicas y procedimientos (TTP), así como los sectores y regiones a los que se dirigen. Estos informes se centran en las actividades de espionaje, desde los ataques a la cadena de suministro hasta las actividades de piratería y destrucción. Estos informes son ideales si tu organización es una gran empresa, una agencia gubernamental o una organización relacionada con infraestructuras críticas, y también son especialmente importantes para las organizaciones que poseen datos confidenciales que pueden ser objeto de interés para las entidades gubernamentales.

Kaspersky Crimeware Intelligence Reporting

Se centra en ataques y campañas cuyo objetivo principal es el beneficio económico. Incluye información sobre las últimas tendencias en ciberdelincuencia, incluidos los datos robados que se venden en la web oscura, el fraude financiero, el ransomware y el malware para cajeros automáticos y POS. Proporcionan detalles sobre nuevas variedades de crimeware, sus métodos de distribución y los tipos de datos a los que se dirigen. Estos informes son especialmente importantes si tu empresa realiza una gran cantidad de negocios en línea o si tienes en tu poder datos confidenciales de clientes, por ejemplo, si eres una entidad financiera o una plataforma de comercio electrónico.

Kaspersky ICS Threat Intelligence

Proporciona una inteligencia detallada y un mayor conocimiento de las campañas maliciosas que apuntan a las organizaciones industriales, así como información sobre las vulnerabilidades que se encuentran en los sistemas de control industrial más populares y las tecnologías subyacentes. Kaspersky ICS CERT, un equipo de más de 30 expertos altamente calificados en investigación de amenazas y vulnerabilidades de ICS, respuesta ante incidentes y análisis de seguridad, establecido en 2016, ofrece este informe. Estos informes brindan información útil y orientación para proteger los activos críticos, incluidos los componentes de software y hardware, y garantizar la seguridad y la continuidad de los procesos tecnológicos.

Puede que debas considerar los siguientes servicios relacionados de Kaspersky ICS Threat Intelligence:

ICS Threat Intelligence Reporting

Suscripción a nuestras publicaciones periódicas sobre amenazas y vulnerabilidades de la ciberseguridad industrial:

- Alertas sobre amenazas de día cero
- Informes técnicos detallados
- Revisiones mensuales
- Recomendaciones sobre las mitigaciones de vulnerabilidades
- Estadísticas y tendencias

Fuentes de datos sobre amenazas de ICS

Flujos de datos legibles por máquinas sobre las amenazas y vulnerabilidades de la ciberseguridad industrial.

Formatos simples de distribución de datos (JSON, CSV, OpenIoC, STIX) a través de HTTPS, TAXII y métodos de distribución especializados para la integración en soluciones de seguridad de la información.

Ask the Analyst

Consulta con los expertos de Kaspersky ICS CERT, que te proporcionarán asesoramiento individual sobre las amenazas y vulnerabilidades de ciberseguridad industrial, estadísticas y panorama de amenazas, normas industriales, etc. más importantes para ti.

Kaspersky Threat Intelligence Reportingte proporciona lo siguiente:

Acceso privilegiado

Por diversas razones, no todas las amenazas de alto perfil se hacen públicas. Sin embargo, proporcionamos este tipo de información exclusiva a nuestros clientes durante el proceso de investigación, incluso antes del anuncio público oficial.

Acceso a datos técnicos

Incluye una lista ampliada de IOC, disponible en formatos estándar, como openIOC o STIX y acceso a nuestras reglas YARA / Sigma / Suricata.

Perfiles de actores de amenazas

Incluye el posible país de origen y la actividad principal, las familias de malware utilizadas, los sectores y las geografías objetivo, así como las descripciones de todas las TTP utilizadas con asignación a MITRE ATT&CK.

MITRE ATT&CK

Todos los TPP descritos en los informes se asignan a MITRE ATT&CK, lo que facilita una mejor detección y respuesta mediante el desarrollo y priorización de los casos de uso de supervisión de seguridad correspondientes, la realización de análisis de brechas y la prueba de las defensas actuales contra los TPP relevantes.

Análisis retrospectivo

Acceso a todos los informes privados publicados con anterioridad durante todo el periodo de tu suscripción.

Soporte de API RESTful

Integración y automatización perfectas de tus operaciones de seguridad.

Kaspersky
Digital Footprint
Intelligence

Kaspersky Digital Footprint Intelligence

A medida que su empresa crece, la complejidad y la distribución de sus entornos de TI también lo hacen, lo que presenta el desafío de proteger una presencia digital ampliamente distribuida sin control ni propiedad directos. Los entornos dinámicos e interconectados permiten que las empresas obtengan grandes beneficios. Sin embargo, el constante aumento de la interconectividad también está ampliando el área de ataque. Dado que los atacantes son cada vez más hábiles, es vital no solo disponer de una imagen precisa de la presencia en línea de tu organización, sino también poder rastrear sus cambios y reaccionar ante amenazas externas dirigidas a los activos digitales expuestos.

Las organizaciones utilizan una amplia gama de herramientas en sus operaciones de seguridad, pero sigue habiendo amenazas digitales al acecho que requieren capacidades muy específicas: detectar y mitigar filtraciones de datos, supervisar planes y esquemas de ataque de cibercriminales ubicados en foros de la red oscura, etc. Para ayudar a los analistas de seguridad a explorar la visión que tiene el adversario de los recursos de tu empresa, detectar rápidamente los posibles vectores de ataque disponibles para ellos y ajustar sus defensas en consecuencia, Kaspersky ha creado Kaspersky Digital Footprint Intelligence.

Kaspersky Digital Footprint Intelligence proporciona lo siguiente:

Detección de amenazas

Supervisión de actividades fraudulentas que pueden dañar la reputación de una empresa o engañar a los clientes.

Reconocimiento de redes

Identificación de los recursos de red del cliente y los servicios expuestos, que son un potencial punto de entrada para un ataque. Análisis personalizado de las vulnerabilidades existentes, con una mayor puntuación y evaluación de riesgos integral basada en la puntuación base del CVSS, la disponibilidad de exploits públicos, la experiencia de pruebas de penetración y la ubicación del recurso de red (alojamiento/infraestructura).

Supervisión de la red oscura

Supervisión constante de recursos de la red oscura (foros, ransomware, blogs, sistemas de mensajería, sitios de tor, etc.), que detecta todas las referencias y amenazas relacionadas con tu empresa, clientes y partners. Análisis de ataques dirigidos activos o que se estén planificando, campañas de APT dirigidas a tu empresa, sector y regiones de operaciones.

Detección de filtraciones de datos

Detección de credenciales, tarjetas bancarias, números de teléfono y otra información confidencial de empleados, clientes y partners vulnerados, que se puede usar para realizar un ataque o que significa un riesgo para la reputación de la empresa.

Compatibilidad con tenencia múltiple

Funciones mejoradas para proveedores de servicios de seguridad gestionados MSSP y organizaciones grandes con una estructura de varias sucursales.

Fuentesde inteligencia

Es esencial que tengas una comprensión integral de la postura de seguridad externa de la empresa. Para proporcionar esta información, los analistas de seguridad de Kaspersky recopilan y añaden información de las siguientes fuentes de inteligencia:

Sus datos no estructurados

- Direcciones IP
- Dominios de empresa
- Nombres de marca
- Palabras clave
- Rangos de red
- Números de tarjetas BIN/IIN
- Información de empleados

Inventario del perímetro de la red

Búsqueda en la red oscura, profunda y superficial

Búsqueda en la base de conocimientos de Kaspersky

Alertas de amenazas

Búsqueda en tiempo real en las fuentes de Kaspersky y la red visible y oscura

Informes analíticos*

Funcionamiento

Configurar	Recopilar	Filtro	Notificación
Detección de información sobre los activos digitales de la empresa	Recopilación automatizada de datos desde la red superficial, profunda y oscura, así como la base de datos de Kaspersky	Detección de amenazas, análisis y priorización administrada por analistas	Envío de notificaciones sobre amenazas operativas en Kaspersky Threat Intelligence Portal o a través de la API

*Servicio complementario

Valores comerciales de DigitalFootprint Intelligence

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

Detección de amenazas

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

Reduce los ciberriesgos

Brinda a las partes interesadas (director de experiencia de cliente y Junta Directiva) información sobre dónde ubicar el gasto en ciberseguridad, lo que revelará las brechas de la configuración actual y los riesgos que acarrean.

Reacciona más rápido

El contexto adicional de las alertas de seguridad mejora la respuesta ante incidentes y reduce tu tiempo medio de respuesta (MTTR)

Reduce la superficie de ataque

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

Comprende a tus adversarios

Más vale prevenir que curar: debes saber lo que los ciberdelincuentes planean y hablan sobre tu empresa en la red oscura para que la empresa esté preparada.

Conoce lo desconocido

Mejora tu capacidad de resistencia ante ciberataques e identifica las amenazas externas a la jurisdicción de tus equipos de seguridad internos.

Eficiencia de la prestación de servicios

El inicio rápido y el escalamiento sencillo en el modo de tenencia múltiple ahorra tiempo a los proveedores de servicios de seguridad gestionados (MSSP) y sus clientes, además de a las organizaciones grandes de múltiples filiales.

Kaspersky Takedown Service

Kaspersky Takedown Service

Los cibercriminales crean dominios maliciosos y de phishing que se utilizan para atacar su empresa y sus marcas. La incapacidad de mitigar rápidamente estas amenazas una vez identificadas puede conducir a una pérdida de ingresos, daños a la marca, pérdida de la confianza del cliente, filtración de datos y mucho más. Pero la gestión de la eliminación de estos dominios es un proceso complejo que requiere de experiencia y tiempo.

Kaspersky Takedown Servicemitiga rápidamente las amenazas planteadas por los dominios maliciosos y de phishing antes de que causen algún daño a tu marca y empresa. La gestión integral del proceso completo ahorra tiempo y recursos valiosos a los clientes. El servicio se ofrece en todo el mundo.

Kaspersky bloquea más de 15 000 URL de phishing y estafa, y evita más de un millón de intentos de acceso a las URL cada día. Nuestra gran experiencia en el análisis de dominios maliciosos y de phishing significa que sabemos cómo recopilar toda la evidencia necesaria para comprobar que son maliciosos. Nos encargaremos de la gestión de eliminación y permitiremos actuar con rapidez para minimizar el riesgo digital, de manera que su equipo se pueda centrar en otras tareas prioritarias.

Kaspersky protege de manera eficaz los servicios online y la reputación de sus clientes mediante el trabajo colaborativo con organizaciones internacionales, organismos de seguridad nacionales y regionales (como la INTERPOL, Europol, la Unidad de Crimen Digital de Microsoft, la Unidad Nacional de Delitos de Alta Tecnología (NHTCU) de la agencia policial de los Países Bajos y la policía de Londres), así como con los equipos de respuesta ante emergencias informáticas (CERT) de todo el mundo.

Visibilidad completa

Se le notificará en cada etapa del proceso, desde el registro de su solicitud a la eliminación

Gestión integral

Gestionaremos todo el proceso de eliminación para minimizar tu participación

Cobertura global

No importa dónde se registre un dominio malicioso o de phishing, Kaspersky solicitará su eliminación de la organización regional con las autoridades legales relevantes

Funcionamiento

Puedes enviar tus solicitudes a través de Kaspersky Company Account, nuestro portal corporativo de servicio al cliente. Prepararemos toda la información necesaria y enviaremos la solicitud de eliminación a la autoridad local/regional respectiva (CERT, registro, etc.) que posea los derechos legales necesarios para desactivar los dominios. Recibirás notificaciones en cada etapa del proceso hasta que se elimine el recurso deseado.

Protección sencilla

Kaspersky Takedown Service mitiga rápidamente las amenazas planteadas por los dominios maliciosos y de phishing antes de que causen algún daño a tu marca y empresa. La gestión integral del proceso completo le ahorra tiempo y recursos valiosos.

Kaspersky
Ask the Analyst

Kaspersky Ask the Analyst

Los ciberdelincuentes desarrollan constantemente formas sofisticadas de atacar a las empresas. Actualmente, la situación volátil de las amenazas está en rápido crecimiento y presenta técnicas de ciberdelincuencia cada vez más ágiles. Las organizaciones se enfrentan a incidentes complejos provocados por ataques no relacionados con el malware, ataques sin archivos, ataques living-off-the-land, vulnerabilidades de día cero y combinaciones de todos estos ataques integrados en amenazas complejas, similares a APT y ataques dirigidos.

En una época donde los ciberataques perjudican a las empresas, los profesionales de la ciberseguridad son más importantes que nunca. Sin embargo, encontrarlos y mantenerlos no es una tarea fácil. Incluso si tiene un equipo sólido de ciberseguridad, no siempre puede esperar que sus expertos combatan solos la guerra contra las amenazas sofisticadas: es importante que puedan obtener ayuda de expertos externos. La experiencia externa puede aclarar la posible trayectoria de los ataques complejos y APT, y dar consejos útiles sobre la forma más decisiva de eliminarlos.

La investigación continua de amenazas permite a Kaspersky descubrir, supervisar e infiltrarse en comunidades y foros de la red oscura de todo el mundo y cuyo acceso está limitado a las personas seleccionadas. Nuestros analistas aprovechan este acceso para detectar e investigar de forma proactiva las amenazas más perjudiciales y notorias, así como las amenazas dirigidas a organizaciones específicas.

Kaspersky Ask the Analyst amplía nuestra cartera de inteligencia de amenazas, lo que te permite solicitar asesoramiento e información sobre amenazas específicas a las que te enfrentas o que te interesan. El servicio adapta las potentes capacidades de inteligencia e investigación de amenazas de Kaspersky a tus necesidades específicas, lo que le permite construir unas defensas resistentes contra las amenazas dirigidas a tu organización.

Productos de Kaspersky Ask the Analyst (suscripción unificada basada en solicitudes)

APT y crimeware

Información adicional sobre informes publicados e investigaciones en curso (además del servicio APT/Crimeware Intelligence Reporting)

Descripciones de amenazas, vulnerabilidades e IoC relacionados

- Descripción general de una familia específica de malware
- Contexto adicional para las amenazas (hashes relacionados, URLs, CnCs, etc.)
- Información sobre una vulnerabilidad específica (su nivel de estado crítico y los mecanismos de protección correspondientes en los productos de Kaspersky)

Solicitudes de ICS

- Información adicional sobre informes publicados
- Información de vulnerabilidad de ICS
- Estadísticas y tendencias de amenazas de ICS de una región/sector
- Información de análisis de malware de ICS sobre las normas o estándares

Inteligencia de la Dark Web

- Investigación de la dark web en determinados artefactos, direcciones IP, nombres de dominio, nombres de archivos, correos electrónicos, enlaces o imágenes
- Análisis y búsqueda de información

Análisis de malware

- Análisis de muestras de malware
- Recomendaciones sobre otras medidas de corrección

Funcionamiento

Kaspersky Ask the Analyst se puede adquirir por separado o como complemento de cualquiera de nuestros servicios de inteligencia de amenazas. Puedes enviar tus solicitudes a través de Kaspersky Company Account, nuestro portal corporativo de servicio al cliente. Te responderemos por correo electrónico, pero si lo deseas, podemos organizar una videoconferencia o una sesión de pantalla compartida. Una vez aceptada tu solicitud, se te informará del plazo estimado para procesarla.

Casos de uso

1

Especifique cualquier detalle en los informes de inteligencia de amenazas publicados anteriormente.

2

Obtenga inteligencia adicional para los IoC ya proporcionados.

3

Obtén detalles sobre las vulnerabilidades y recomendaciones sobre cómo protegerse contra la explotación.

4

Obtén detalles adicionales sobre las actividades específicas de la Dark Web que sean de tu interés

5

Obtén un informe general de la familia de malware que incluya su comportamiento, su impacto potencial y detalles sobre cualquier actividad relacionada que Kaspersky haya observado

6

Prioriza las alertas o incidentes de forma eficaz con información contextual detallada y la categorización de los IoC relacionados proporcionados mediante informes cortos.

7

Solicita ayuda para identificar si la actividad inusual detectada está relacionada con una APT o un crimeware

8

Envía archivos de malware para un análisis integral que permita comprender el comportamiento y la funcionalidad de las muestras proporcionadas.

Kaspersky Ask the Analyst beneficios

Amplía tu experiencia

Obtén acceso a la carta a los expertos del sector sin tener que buscar ni invertir en especialistas de tiempo completo que son difíciles de encontrar.

Acelera las investigaciones

Analice y priorice los incidentes con eficacia según información contextual adaptada y detallada.

Responde con rapidez

Responde rápidamente a las amenazas y vulnerabilidades gracias a nuestra asistencia para bloquear los ataques a través de vectores conocidos.

Amplía tus conocimientos y recursos

Kaspersky Ask the Analyst te ofrece acceso a un grupo de investigadores de Kaspersky para cada caso en particular. El servicio proporciona una comunicación integral entre expertos para aumentar sus capacidades actuales con nuestros conocimientos y recursos únicos.

Conclusión

Contrarrestar las ciberamenazas de hoy requiere una visión global de las tácticas y herramientas que utilizan los actores de amenazas. La generación de esta inteligencia y la identificación de las contramedidas más eficaces requieren una dedicación constante y altos niveles de experiencia. Con los petabytes de datos de amenazas que se pueden extraer, las tecnologías avanzadas de aprendizaje automático y un grupo exclusivo de expertos a nivel mundial, trabajamos para asistir a nuestros clientes con la inteligencia frente a amenazas más reciente del mundo y los ayudamos a mantener su inmunidad incluso ante ciberataques desconocidos.

Ventajas clave

Permite la visibilidad de amenazas global, la detección de ciberamenazas a tiempo, la priorización de alertas de seguridad y una respuesta efectiva frente a incidentes de seguridad.

El conocimiento único de las tácticas, las técnicas y los procedimientos que utilizan los actores en diferentes sectores y regiones permite la protección proactiva frente a amenazas específicas y complejas.

Una descripción general integral de su estado de seguridad con recomendaciones útiles sobre las estrategias de mitigación le permiten enfocarse en su estrategia defensiva en áreas identificadas como objetivos principales de ciberataque.

Previene el agotamiento de los analistas y ayuda a que tu personal se concentre en las amenazas genuinas.

La respuesta acelerada y mejorada frente a incidentes y las capacidades de búsqueda le ayudan a reducir el tiempo de espera contra ataques y a minimizar en gran medida los posibles daños.

Kaspersky Threat Intelligence

Más información

www.kaspersky.es

#kaspersky
#bringonthefuture