

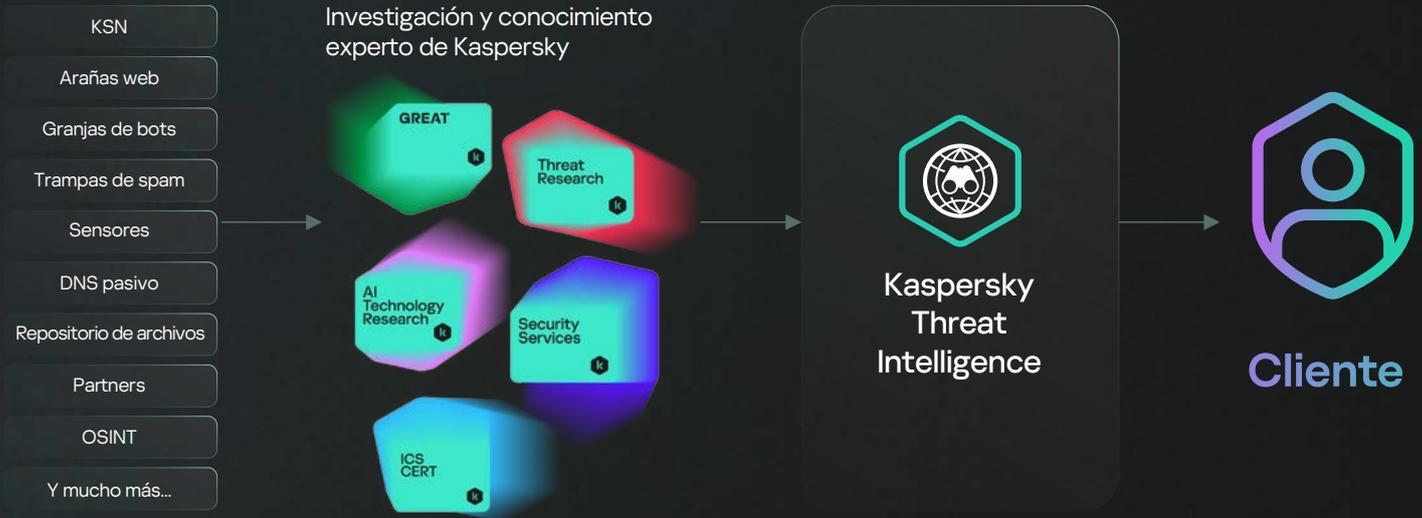
Kaspersky Threat Intelligence

Anticípese a sus adversarios



kaspersky

Fuentes de Kaspersky Threat Intelligence



Kaspersky Threat Intelligence proporciona acceso a una gran variedad de información recopilada por nuestros **analistas e investigadores de primer nivel** para ayudar a tu organización a contrarrestar de manera eficaz las ciberamenazas actuales.

Inteligencia sobre amenazas potenciada por una experiencia y unos conocimientos mundiales únicos



Cada centro contribuye a las soluciones y servicios de Kaspersky

- Investigación de amenazas
- Investigación de incidentes



Equipo de análisis e investigación global de Kaspersky

- Investigación de las amenazas más complejas: APT, campañas de ciberespionaje, ciberepidemias globales, etc.
- Seguridad de las tecnologías del futuro
- Investigación de la ciberdelincuencia financiera sofisticada



Kaspersky Investigación de amenazas

- Investigación antimalware
- Metodologías SSDLC y seguras por diseño
- Investigación de filtrado de contenidos



Kaspersky Investigación en Tecnología por IA

- Ciberseguridad de IA
- Soluciones de detección de amenazas basadas en IA
- Investigación en IA generativa



Kaspersky Servicios de seguridad

- MDR
- Evaluación de la seguridad
- Inteligencia sobre presencia digital
- Incident Response
- Asesoría para SOC



Kaspersky ICS CERT

- Análisis de las amenazas a las infraestructuras críticas
- Asociaciones tecnológicas, análisis y normas
- Investigación y evaluación de la vulnerabilidad de ICS

Aspectos destacados de Kaspersky Threat Intelligence

Nuestros **profundos conocimientos**, **nuestra amplia experiencia** en la investigación de ciberamenazas y nuestra **visión única** de todos los aspectos de la ciberseguridad nos han convertido en un socio de confianza para empresas de todo el mundo y en un valioso aliado de las fuerzas del orden y las organizaciones gubernamentales, incluidas la Interpol y numerosas unidades CERT.



Coverage of global threats, with longstanding experience researching threats in regions where most attacks originate



Continuous contribution by Kaspersky experts



Threat Intelligence for IT and OT segments



Aspectos destacados de Kaspersky Threat Intelligence

Nosotros rastreamos:

+ 300

 actores de amenazas

+ 500

 spear phishing.

+ 200

informes privados
al año

+1700000

IoC relacionados con
informes

+2500

Regla YARA relacionadas
con informes

Niveles de datos de inteligencia frente a amenazas



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

Systems:

SIEM

NGFW

SOAR

IPS

IDS

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

Systems:

SIEM

NTA

TIP

EDR / XDR

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 incluye tendencias, motivaciones de los ciberdelincuentes y sus clasificaciones.

Funciones:

CISO

CTO

Director de IT

Director ejecutivo

Procesos:

Creación de una estrategia de IS

Concienciación

Formatos para la entrega de inteligencia de amenazas

7



Inteligencia frente a amenazas legible por máquina



Kaspersky
Threat Data
Feeds

Más de 30 fuentes de datos de amenazas sobre diferentes necesidades con cobertura TI y TO y una plataforma de TI



Inteligencia frente a amenazas legible por humanos



Kaspersky
Threat Intelligence
Portal

La cartera principal de Kaspersky Threat Intelligence para entornos de TI y TO con un único punto de acceso desde Kaspersky Threat Intelligence Portal



Inteligencia experta frente a ciberamenazas



Kaspersky
Takedown
Service



Kaspersky
Ask the Analyst

Guía experta de profesionales con experiencia

Kaspersky Threat Intelligence



Inteligencia frente a amenazas legible por máquina



Inteligencia frente a amenazas legible por humanos



Kaspersky Threat Data Feeds



Más de 30 fuentes de datos de amenazas listos para usar para diferentes tareas

Fuentes de datos de amenazas creados a medida según las necesidades de tu organización.

- TI táctica
- TI operativa

Fuentes de datos de amenazas generales

- URL maliciosas
- URL de ransomware
- URL de phishing
- URL de C&C de botnets
- Botnet móvil C&C URL
- Hashes maliciosos
- Hashes maliciosos móviles
- Reputación de IP
- URL de IoT
- Haches de ICS
- Hashes de APT
- IP de APT
- URL de APT
- Hashes de crimeware
- URL de crimeware



Plataforma de TI

Pon en funcionamiento rápidamente tus diversas fuentes de información sobre amenazas y reduce la carga de trabajo de los SIEM

Kaspersky CyberTrace

Fuentes de datos de amenazas específicas



Kaspersky Threat Intelligence Portal



Un **único punto de acceso** a Kaspersky Threat Intelligence desde una IU o API única en la que los servicios funcionan en conjunto y se fortalecen entre sí. Al tener **todo el conocimiento experto y la experiencia en ciberamenazas de Kaspersky** en un único sitio, pueden supervisarse las amenazas relevantes para una organización específica mediante las tecnologías de normalización y procesamiento de datos privados y pueden analizarse muestras de malware y sus respectivas atribuciones.

- TI táctica
- TI operativa
- TI estratégica



Versión gratuita de Kaspersky Threat Intelligence Portal



El panorama de amenazas en Kaspersky Threat Intelligence Portal

Inteligencia de amenazas específica según la región y la industria para comprender cuáles son las amenazas que enfrenta tu organización

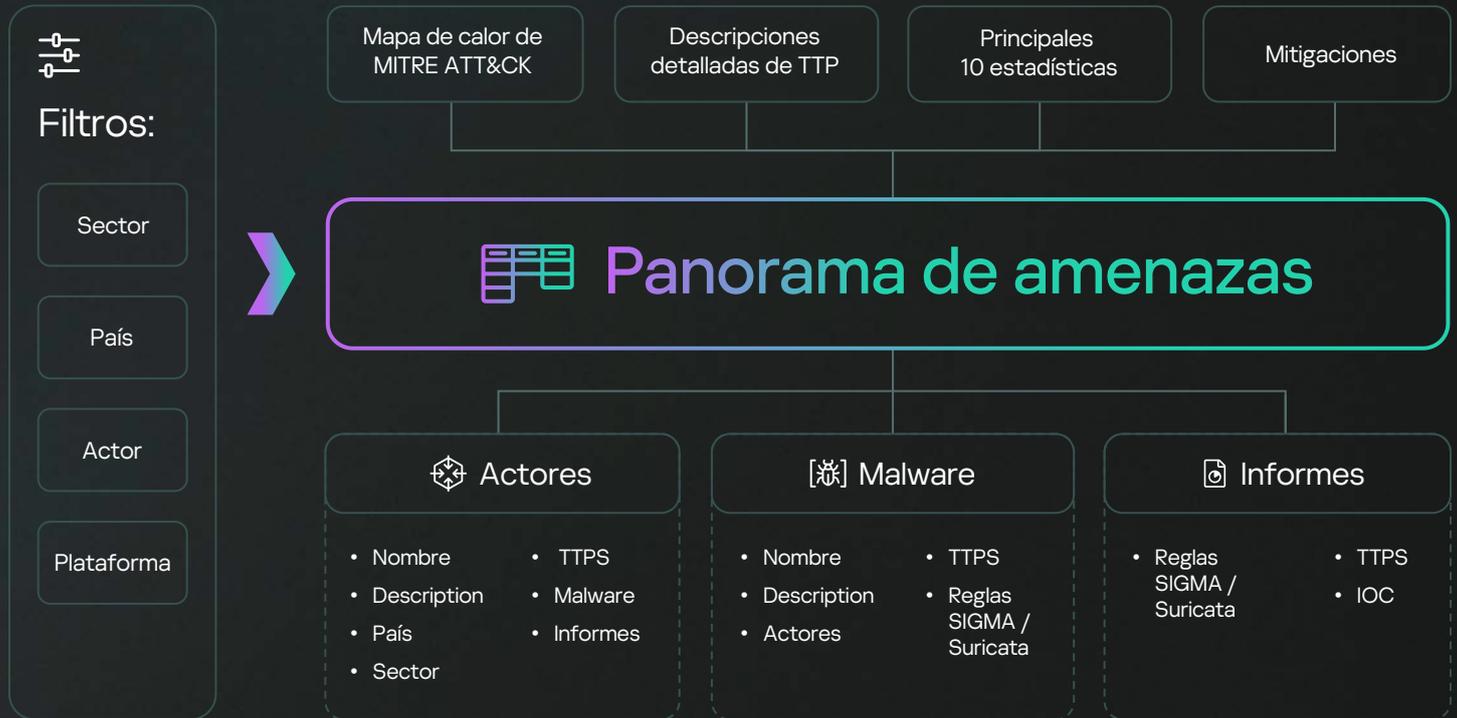
- Alineación con MITRE ATT&CK
- Actualizaciones en tiempo real basadas en las investigaciones en curso de Kaspersky
- Autollenado de perfiles de adversarios y software
- Repositorio de reglas de detección



400 000+

Archivos maliciosos que detectamos a diario

Cómo funciona el panorama de amenazas



Asistencia experta de Kaspersky Threat Intelligence

13



Kaspersky Ask the Analyst

- TI operativa
- TI estratégica

El servicio 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.

Te ofrecemos 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.



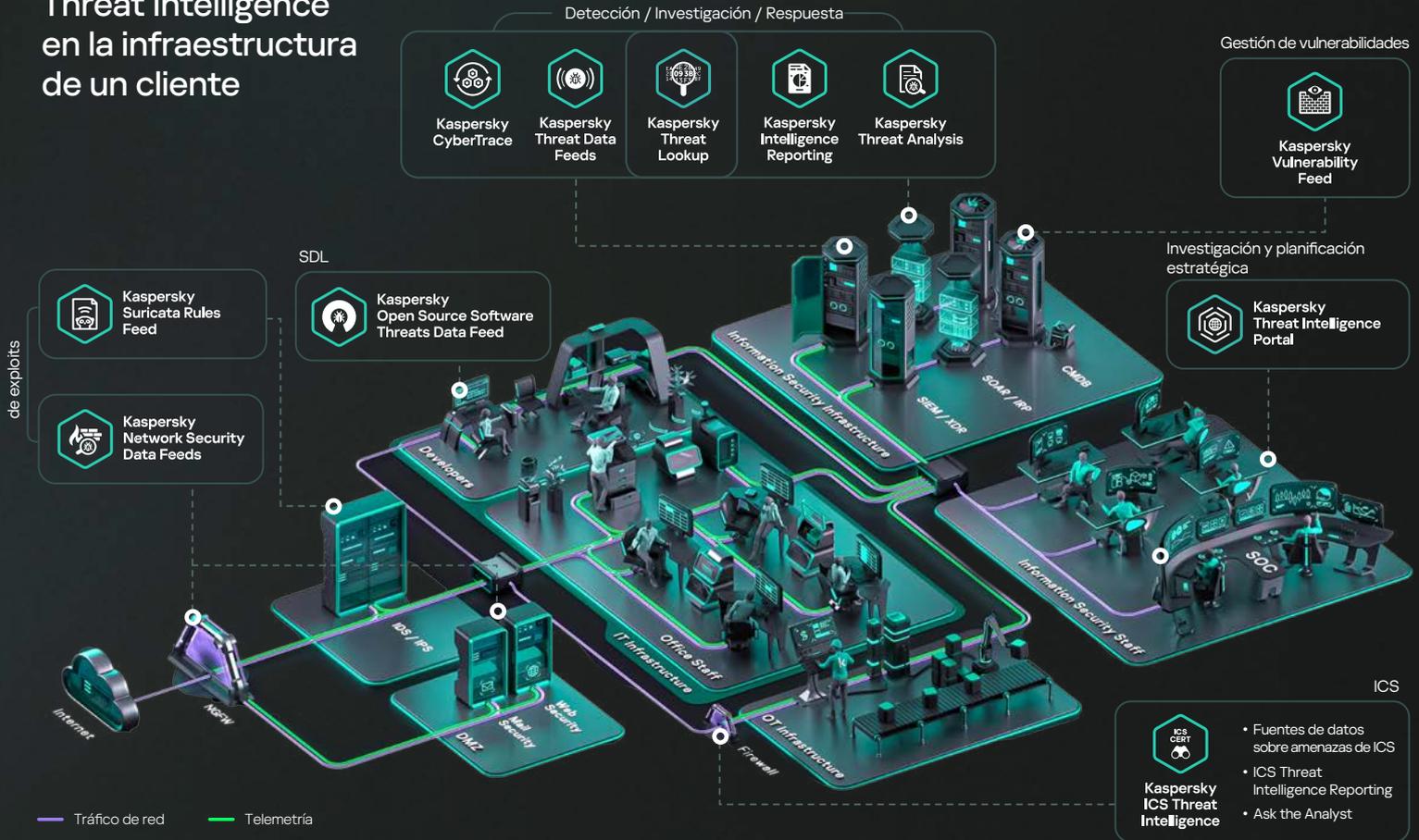
Kaspersky Takedown Service

- TI operativa

Kaspersky Takedown Service **mitiga rápidamente las amenazas que representan los dominios maliciosos y de phishing** antes de que causen algún daño a tu marca y empresa. Nuestra extensa experiencia en el análisis de dominios nos proporcionan el conocimiento sobre cómo recopilar toda la evidencia necesaria para comprobar que son maliciosos. Nos encargaremos de gestionar tu eliminación.

El servicio se presta a escala mundial en cooperación con organizaciones internacionales y organismos policiales nacionales y regionales.

Ejemplo de Kaspersky Threat Intelligence en la infraestructura de un cliente



ICS CERT

- Fuentes de datos sobre amenazas de ICS
- ICS Threat Intelligence Reporting
- Ask the Analyst

Kaspersky ICS Threat Intelligence

Oferta de Kaspersky Industrial Threat Intelligence

15

Inteligencia frente
a amenazas legible
por máquina



Kaspersky
Threat Data
Feeds

Datos legibles por
máquinas sobre
las amenazas y
vulnerabilidades de la
ciberseguridad industrial:

Fuentes de datos de hashes de ICS
de Kaspersky Fuentes de datos de
vulnerabilidades de ICS de Kaspersky
Fuentes de datos de vulnerabilidades
de ICS de Kaspersky en formato
OVAL

Inteligencia frente
a amenazas legible
por humanos



Kaspersky
ICS Intelligence
Reporting

Accede a publicaciones
periódicas sobre amenazas
y vulnerabilidades de
ciberseguridad industrial
en el Kaspersky Threat
Intelligence Portal

Asistencia de expertos en
inteligencia frente
a amenazas



Kaspersky
Ask the Analyst

Consulta directamente con los
expertos de Kaspersky ICS CERT
para obtener asesoramiento
personalizado sobre amenazas
y vulnerabilidades de
ciberseguridad industrial,
estadísticas de amenazas,
el panorama de amenazas,
estándares de la industria y más.

● Táctico

● TI operativa

● TI estratégica

Por qué elegir Kaspersky Threat Intelligence



Una oferta de TI líder reconocida por analistas de la industria

Verificada por analistas de diversas empresas internacionales de investigación, como Frost & Sullivan, Quadrant Knowledge Solutions, Forrester, IDC, entre otras.



Diversas fuentes únicas y creíbles para generar inteligencia de amenazas confiable

La infraestructura de Kaspersky Security Network cubre más de 100 millones de sensores en 200 países: son los repositorios más grandes de archivos maliciosos y legítimos, la web oscura, actividades continuas de búsqueda de amenazas y respuesta ante incidentes, rastreadores web, trampas para correo no deseado, entre otras.



Experiencia de personas de renombre en TI y TO

Más de 200 expertos certificados de 5 centros de especialización, incluido el equipo GREAT e ICS-CERT, distribuidos por todo el mundo y que hablan más de 20 idiomas. Los expertos de Kaspersky siempre están entre los primeros en descubrir las amenazas más notorias, desde Stuxnet y WannaCry hasta Operation Triangulation.



Presencia global

Una fuerte presencia en las regiones donde se originan la mayoría de los ataques (Rusia, CEI, China, etc.) nos da la capacidad única de recopilar, analizar y distribuir inteligencia sobre amenazas 100 % verificada para organizaciones de cualquier país.



Experiencia única en tecnologías de detección de malware

Como el mayor proveedor de antivirus (con los productos más galardonados), procesamos millones de nuevas muestras de malware cada día, utilizando nuestras propias tecnologías de detección de amenazas.



Experiencia única en investigación APT

Rastreamos cientos de actores y campañas APT, publicamos anualmente más de 200 informes estratégicos de TI en profundidad y poseemos la mayor colección de archivos APT del sector, que incluye más de 70 000 muestras.



TI con tecnología de IA para mejorar la detección, la respuesta y la generación de informes ante amenazas

IA / ML nos permite extraer información procesable, generar informes personalizados y automatizar el análisis, lo que nos ahorra / tiempo y recursos significativos.



Proveedor robusto y seguro

Infraestructura transparente y tolerante a fallos con elevadas capacidades de SLA y supervisión, creada mediante metodologías SDLC, con evaluaciones periódicas independientes de terceros (SOC 2 Tipo 2 o ISO 27001).

Éxitos empresariales públicos



Esto nos aporta una gran visibilidad de las amenazas a las que se enfrentan nuestros clientes. Cuando se produce una alerta, tener esa información legítima y fiable, junto con todos los datos colaterales que se obtienen, es vital para crear una imagen completa de la situación y de lo que podemos aprender de ella.

Paul Colwell
CyberGuard Technologies



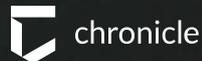
Leer la historia



Kaspersky suele ser la primera en identificar el surgimiento de una nueva amenaza, incluso antes de que los fabricantes de software lo sepan.

Kaspersky cuenta con la experiencia necesaria para informar sobre nuevas amenazas, que acechan en sombra y son desconocidas, en lugar de limitarse a bombardear datos reciclados que no añaden nada nuevo a nuestros conocimientos.

Juan Andres Guerrero Saade,
investigador, Chronicle Security



Leer la historia



Kaspersky superó mis expectativas con sus funciones y su capacidad para escuchar lo que necesitábamos. Nos dieron confianza en el producto y en la gente que había detrás y nos permitieron tener una red más segura.

Rashid AlNahlawi
Asesor de seguridad informática,
Comité Olímpico de Qatar



Leer la historia

Tareas que permite Kaspersky Threat Intelligence



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.



Mejora tu 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.



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.



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 tus equipos de seguridad de la información.



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.

Gracias.

Kaspersky Threat Intelligence Portal,
donde vive el conocimiento
de la ciberseguridad



Kaspersky
Threat Intelligence
Portal



Más información



Solicitar una demo

