



# Kaspersky Threat Data Feeds



# Kaspersky Threat Data Feeds

## Kaspersky Threat Data Feeds

Los ciberataques ocurren a diario. La frecuencia, la complejidad y la ofuscación de las ciberamenazas crecen de forma sostenida a medida que intentan comprometer sus defensas. Los adversarios emplean esquemas de intrusión complejos, campañas y tácticas, técnicas y procedimientos (TTP) personalizados para interrumpir las operaciones de su negocio o perjudicar a sus clientes. Es evidente que se necesitan nuevos métodos de protección basados en la inteligencia de amenazas.

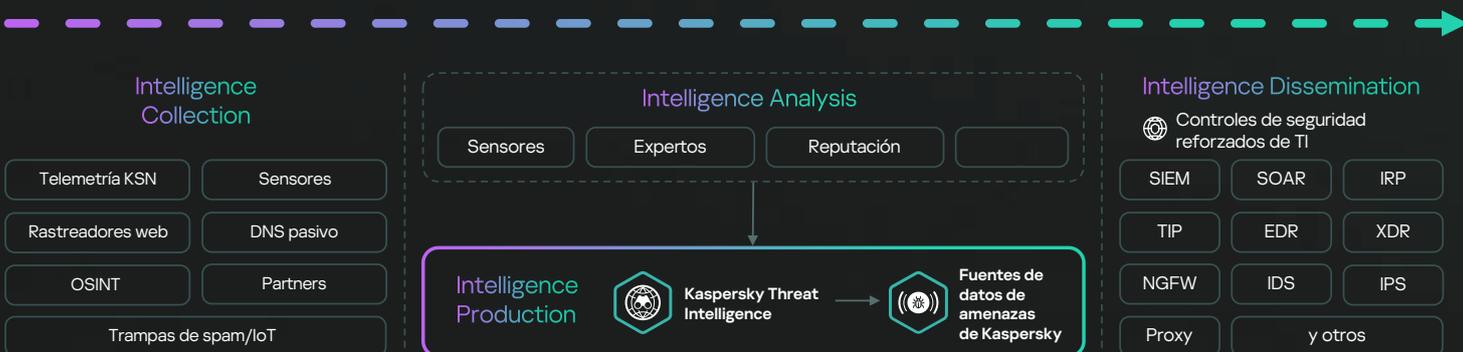
Mediante la integración en los sistemas de seguridad existentes, como las plataformas SIEM, SOAR y las fuentes de inteligencia de amenazas actualizadas, que contienen información sobre direcciones IP, URL y hashes de archivos sospechosos o peligrosos, los equipos de seguridad pueden automatizar el proceso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

### Datos contextuales

Las entradas de las fuentes proporcionadas por Kaspersky contienen los siguientes datos contextuales que le permiten confirmar y priorizar con rapidez las amenazas:

- 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 ataques según la clasificación de MITRE ATT&CK
- Marcas de fecha y hora
- Geolocalización
- Popularidad y demás

### ¿Cómo funciona?



# Kaspersky Threat Data Feeds se genera a partir de fuentes fusionadas, heterogéneas y altamente confiables de Kaspersky:



## Kaspersky SecurityNetwork

Una sofisticada infraestructura en la nube que recopila y analiza datos anónimos sobre ciberamenazas de más de 400 millones de participantes voluntarios en todo el mundo, brindando la respuesta más rápida a nuevas amenazas gracias al análisis de macrodatos, el aprendizaje automático y el conocimiento humano.



## Rastreadores web

Recopilar nuevas muestras legítimas y de malware de diversas fuentes: OSINT, investigación de los analistas de Kaspersky y nuestros propios sistemas automáticos de procesamiento y análisis que extraen las direcciones URL del malware.



## BotFarm

Un equipo especializado en la investigación de botnets extrae configuraciones de bots, aplica ingeniería inversa a sus protocolos de comunicación y supervisa los comandos de los centros de comando para obtener información valiosa sobre las amenazas.



## Trampas de spam

Cada año, nuestros sistemas antiphishing evitan más de 500 millones de clics en vínculos de phishing y más de 160 millones de archivos adjuntos de correo electrónico maliciosos, de los que extraemos datos adicionales para mejorar nuestros flujos de datos.



## Partners

Participamos en asociaciones con otros proveedores y organizaciones de ciberseguridad para compartir muestras maliciosas.



## Sensores

Honeypots, sinkholes y otros métodos de interceptación de ataques ITW. Por ejemplo, dispositivos de IoT, sistemas vulnerables, software, etc. Los analistas de Kaspersky investigan los intentos de ataque y los métodos de los atacantes, extraen indicadores de compromiso y los vinculan a otras fuentes de datos.



## DNS pasivo

Los datos se recopilan globalmente de terceros de confianza, como organizaciones de hosts y proveedores de servicios de Internet (ISP).



## OSINT

Los datos de los adversarios se recopilan automáticamente de fuentes de acceso público, como medios de comunicación, redes sociales, informes públicos, la red oscura, etc. Utilizamos estos datos para buscar nuevas muestras maliciosas y explorar la infraestructura del adversario, con el fin de ampliar continuamente nuestra base de conocimientos.

Cada indicador detectado se somete a un proceso de detección en varias etapas dentro de un sistema de procesamiento automatizado que utiliza tecnologías de confianza y reputación, junto con modelos de aprendizaje automático entrenados en cientos de millones de muestras de archivos reales, tanto de confianza como maliciosos, para eliminar los falsos positivos. Cada indicador se analiza también en múltiples entornos de prueba, de los que se extraen numerosos atributos adicionales, como TTP, comportamiento de la red, comportamiento del sistema operativo y otras muchas relaciones.

Todo esto convierte a **Kaspersky Threat Intelligence** en una poderosa fuente de inteligencia a nivel táctico que puede fortalecer sus centros de supervisión de amenazas y detectar adversarios en las primeras líneas de su organización.

## Aspectos destacados



Las fuentes de datos se generan de manera automática en tiempo real según hallazgos en todo el mundo, lo que proporciona tasas de **detección** y **precisión altas**.



La **facilidad de implementación** se garantiza mediante documentación complementaria, muestras, un gerente técnico de cuentas específico y servicio de soporte técnico de Kaspersky, todo combinado para permitir la integración simple.



Los formatos simples de divulgación ligeros (JSON, CSV, OpenIOC, STIX) a través de HTTPS, TAXII o mecanismos de entrega específicos permiten una **integración fácil** de las fuentes en las soluciones de seguridad. Las principales plataformas de SIEM y TI son totalmente compatibles.



Las fuentes de datos repletas de falsos positivos carecen de valor, por lo que se realizan pruebas y se le aplican filtros muy exhaustivos antes de publicarlas para garantizar la entrega de **datos completamente revisados**.



Cientos de expertos, entre ellos analistas de seguridad de todo el mundo, y expertos en seguridad reconocidos mundialmente de equipos GReAT y de I+D, contribuyen de forma conjunta para generar estas fuentes. Los responsables de la seguridad reciben información crucial y alertas generadas a partir de los **datos de la más alta calidad**, sin riesgo de que se vean desbordados por indicadores y advertencias innecesarios.



Todas las fuentes se generan y se controlan mediante una infraestructura muy tolerante a fallas, lo que garantiza una **disponibilidad continua**.

## Beneficios

1

Refuerce sus soluciones de defensa de la red, como SIEM, firewalls, NGFW, IPS/IDS, proxy de seguridad, soluciones DNS, protección contra APT con indicadores de compromiso (IOC) continuamente actualizados 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.

2

Mejore y acelere sus capacidades forenses y de respuesta 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 obtener una mayor investigación y respuesta.

3

Evite la exfiltración de activos y propiedad intelectual confidenciales de las máquinas infectadas al exterior de la organización. Detecte rápidamente los activos infectados para proteger la reputación de su marca, mantener la ventaja competitiva y asegurar las oportunidades de negocio.

4

Como MSSP, impulse el crecimiento de su empresa ofreciendo inteligencia de amenazas de primer nivel como un servicio premium para sus clientes.

5

Como CERT, mejore y amplíe sus capacidades de identificación y detección de ciberamenazas.

## Kaspersky Threat Intelligence

**Kaspersky Threat Intelligence** proporciona acceso a una gran variedad de información recopilada por nuestros analistas e investigadores de primer nivel. Estos datos ayudarán a su organización a contrarrestar con eficacia las ciberamenazas actuales.

Nuestra empresa cuenta con un profundo conocimiento, amplia experiencia en la investigación de ciberamenazas y una perspectiva única sobre todos los aspectos de la ciberseguridad, lo que nos permite ofrecer información de inteligencia actualizada sobre amenazas tácticas, operativas y estratégicas. Esto nos convirtió en un socio de confianza de organizaciones gubernamentales y de fuerzas de seguridad de todo el mundo, como Interpol y varias unidades CERT. Y todo esto está disponible para usted con datos relevantes y prácticos a través del **Portal de Kaspersky Threat Intelligence**.



# Kaspersky Threat Intelligence

Conozca más

<https://latam.kaspersky.com>

© 2024 AO Kaspersky Lab.  
Las marcas comerciales registradas y las marcas de  
servicio pertenecen a sus respectivos propietarios.

#kaspersky  
#bringonthefuture