Kaspersky Threat Data Feeds

kaspersky preparados para el fu

Kaspersky Threat Data Feeds

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. Es evidente que se necesitan nuevos métodos de protección basados en la inteligencia de amenazas.

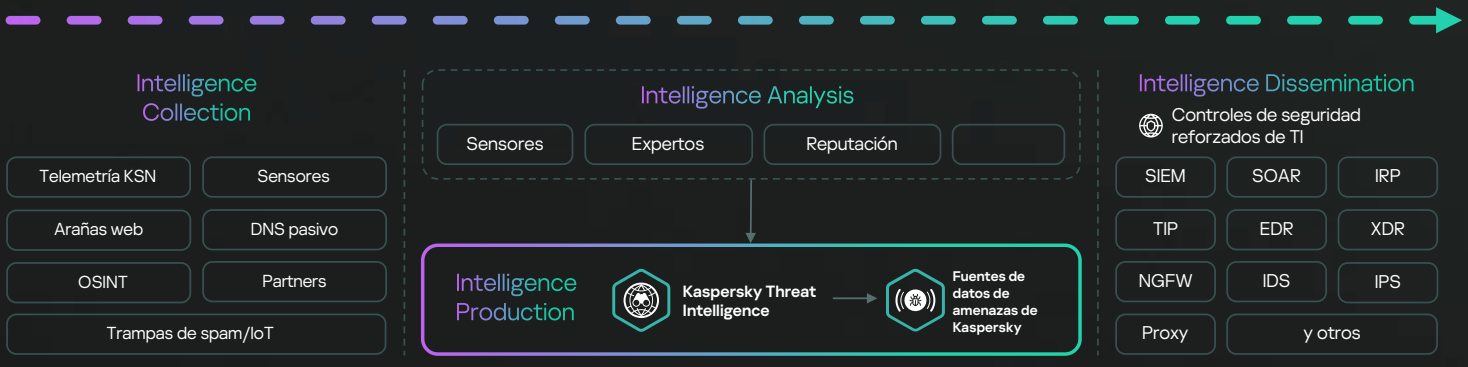
Mediante la integración en los sistemas de seguridad existentes, como las plataformas SIEM, SOAR y de inteligencia de amenazas de las fuentes de inteligencia de amenazas actualizadas que contienen información sobre direcciones IP, URL y hashes de archivos sospechosos y peligrosos, los equipos de seguridad 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.

Datos contextuales

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

- Nombres de amenaza
- 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.

Funcionamiento



Las fuentes de datos de amenazas de Kaspersky se agregan a partir de fuentes fusionadas, heterogéneas y muy fiables de Kaspersky:

Kaspersky SecurityNetwork

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

Arañas 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.

Grupos de bots

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 enlaces 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 para compartir muestras maliciosas con otros proveedores y organizaciones de ciberseguridad.

Sensores

Honeypots, sinkholes y otros métodos de interceptación de ataques ITW. Por ejemplo (incluidos 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 que exploren la infraestructura del adversario, a fin de ampliar continuamente nuestra base de conocimientos.

Cada indicador detectado se somete a un proceso de detección de varias etapas en un sistema de procesamiento automatizado que usa tecnologías de confianza y reputación y modelos de aprendizaje automático entrenados en muestras de cientos de millones de archivos reales de confianza y 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 tus centros de supervisión de amenazas y detectar adversarios en las primeras líneas de tu 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 exactitud y detección altas.

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

Los formatos de divulgación ligeros sencillos (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 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 les aplican filtros muy exhaustivos antes de publicarlas para garantizar una distribución de datos totalmente 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 innecesarias.

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

Ventajas

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) 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.

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 una mayor investigación y respuesta.

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

4. Como MSSP, haga crecer su empresa proporcionando inteligencia de amenazas líder del sector como servicio premium a sus clientes.

5. Como CERT, mejora y amplía tus 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 Tu organización a contrarrestar con eficacia las ciberamenazas actuales.

Nuestra empresa cuenta con un profundo conocimiento, una amplia experiencia en la investigación de ciberamenazas y una visión única de todos los aspectos de la ciberseguridad, lo que permite ofrecer información de inteligencia actualizada sobre amenazas tácticas, operativas y estratégicas.
Esto nos convierte 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 ti como datos relevantes y aplicables a través de Kaspersky Threat Intelligence Portal.

Kaspersky Threat Intelligence

Más información

www.kaspersky.es

#kaspersky
#bringonthefuture