Anticípese a sus adversarios

Kaspersky Threat Intelligence

kaspersky preparados para el futuro

Kaspersky
Threat Intelligence

Kaspersky Threat Intelligence

Threat Intelligence de Kaspersky le brinda acceso a la inteligencia necesaria para mitigar ciberamenazas, recopilada por nuestro equipo líder de investigadores y analistas.

Gracias a nuestro conocimiento, experiencia e inteligencia avanzada en todos los aspectos de la ciberseguridad, en Kaspersky nos hemos convertido en el socio de confianza de las principales fuerzas del orden y agencias gubernamentales del mundo, incluyendo a Interpol y destacados equipos CERT. Kaspersky Threat Intelligence le ofrece acceso inmediato a inteligencia táctica, operativa y estratégica sobre amenazas.

Además, ofrece una visión integral del panorama global de amenazas, combinando fuentes de inteligencia, datos de amenazas e investigación interna, todo ello analizado por nuestro equipo de expertos para proporcionar información práctica que ayude a las organizaciones a protegerse de las ciberamenazas.

Tácticos

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
- Monitoreo

Operativos

Este nivel suele incluir datos sobre campañas y TTP de orden superior. Puede 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:
- Respuesta a incidentes
- Búsqueda de amenazas

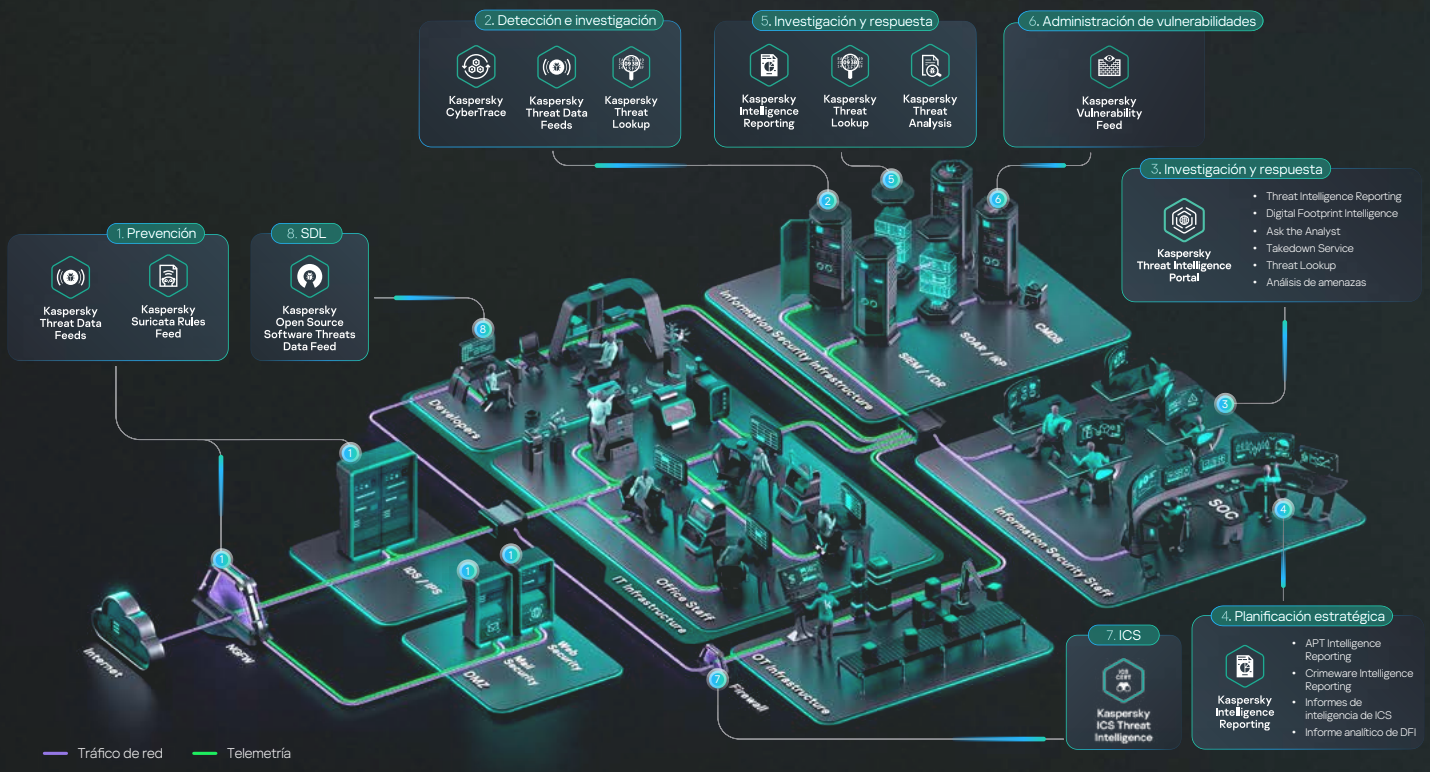
Estratégico

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
- Director de tecnología
- Director de información
- CEO

Procesos:
- Creación de una estrategia de IS
- Mayor conciencia

Esquema de uso de Kaspersky Threat Intelligence



Kaspersky Threat Intelligence le permite lo siguiente:

Identificar y prevenir amenazas de forma proactiva

Le mantiene informado sobre le mantiene informado sobre las amenazas y vulnerabilidades más recientes, permitiéndole tomar medidas proactivas para proteger sus sistemas antes de que ocurra un ataque.

Obtener visibilidad de los rastros digitales

Proporciona una proporciona una visión integral de sus rastros digitales, incluidos aquellos activos que puedan ser vulnerables a un ataque o estar en riesgo.

Mejorar sus capacidades de detección de amenazas

Le ayuda a le ayuda a mejorar sus soluciones de seguridad existentes con la inteligencia de amenazas más reciente, incrementando su capacidad para detectar y bloquear amenazas avanzadas.

Mejorar la respuesta ante incidentes

Ofrece información ofrece información en tiempo real sobre amenazas emergentes e indicadores de riesgo, permitiéndole responder de manera rápida y eficaz a los incidentes.

Cumplir con las regulaciones y normas

Todas las empresas están sujetas a diversas regulaciones y normas dentro de su industria. Kaspersky Threat Intelligence apoya el cumplimiento de normativas al ayudarlo a cumplir con estos requisitos.

Ampliar sus conocimientos internos

El equipo de expertos de Kaspersky se encuentra entre los investigadores más experimentados y respetados de la industria, y aporta 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 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. Una protección eficaz necesita nuevos métodos basados en la inteligencia de amenazas.

Al integrar fuentes de inteligencia de amenazas actualizadas en los sistemas de seguridad existentes, como las plataformas SIEM, SOAR y de inteligencia de amenazas, 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, ofrecen a los especialistas suficiente contexto para identificar de inmediato qué alertas deben investigarse o escalarse a los equipos de Respuesta a Incidentes para una investigación y respuesta más profunda.

Kaspersky Threat Data Feed ofrece inteligencia de amenazas en tiempo real para proteger sus redes y sistemas de ciberamenazas. Las fuentes de datos incluyen información sobre malware conocido, sitios web de phishing, las últimas vulnerabilidades y exploits, además de otros tipos de ciberamenazas. Esta información le ayudará a bloquear el tráfico malicioso, actualizar su 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 confiables, como Kaspersky Security Network, nuestros propios rastreadores web, el servicio de monitoreo de botnets (rastreo 24/7 de las botnets y sus objetivos), trampas de spam, datos de grupos de investigación, socios 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 ayudan a recopilar información de amenazas sobre una alerta o un evento y permiten profundizar en los detalles. También ayuda a responder a las preguntas "¿Quién? ¿Qué? ¿Dónde? ¿Por qué?" e identificar el origen de un ataque, lo que permite tomar decisiones rápidas para proteger su 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 le permiten confirmar y priorizar con rapidez las amenazas:

1. Nombres de amenazas
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 ataques según la clasificación de MITRE ATT&CK
6. Marcas de fecha y hora
7. Geolocalización
8. Popularidad y demás

Beneficios de Kaspersky Threat Data Feed

Mejore y acelere su respuesta ante incidentes y sus capacidades de análisis forense

automatizando el proceso de evaluación inicial. Proporcione a sus analistas de seguridad el contexto necesario para identificar de inmediato las alertas que deben investigarse o escalarse a los equipos de respuesta a incidentes para una investigación y respuesta más profundas.

Refuerce sus soluciones de seguridad,

como SIEM, firewalls, IPS/IDS, proxies de seguridad, soluciones DNS y protección contra APT, con indicadores de compromiso (IOC) continuamente actualizados y contexto útil. Esto le proporcionará información sobre ciberataques y una mayor comprensión de la intención, capacidades y objetivos de sus adversarios. Los principales SIEM (incluidos ArcSight, IBM QRadar, MS Sentinel, Splunk, entre otros) y las plataformas de TI son totalmente compatibles.

Evite la exfiltración de activos y de propiedad intelectual sensible

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.

Haga crecer su empresa de MSSP

ofreciendo inteligencia de amenazas de primer nivel como un servicio premium para sus clientes. Como CERT, mejore y amplíe sus capacidades de identificación y detección de ciberamenazas.

Kaspersky CyberTrace

Kaspersky CyberTrace

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

Al integrar inteligencia de amenazas actualizada al minuto y en un formato 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. A su vez, pueden proporcionar a sus especialistas de primer nivel el contexto suficiente para identificar de inmediato las alertas que deben investigarse o escalarse a los equipos de Respuesta a Incidentes para una investigación y respuesta más profundas.

Kaspersky CyberTrace es una plataforma de inteligencia de amenazas que facilita la integración fluida de fuentes de datos sobre amenazas con soluciones SIEM. De esta manera, los analistas pueden aprovechar de forma más eficaz la inteligencia de amenazas en su flujo de trabajo de operaciones de seguridad existente. Se integra con cualquier fuente de inteligencia de amenazas (Kaspersky, otros proveedores, OSINT o fuentes de clientes) en formatos JSON, STIX, XML y CSV, y permite la integración inmediata con varias fuentes de registro y soluciones SIEM.

Aspectos destacados

La información detallada sobre cada indicador brinda un análisis aún más completo. En cada página se presenta toda la información sobre un indicador, consolidada de todos los proveedores de inteligencia de amenazas (deduplicada), para que los analistas puedan estudiar las amenazas en los comentarios y agregar inteligencia interna sobre cada indicador.

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

El etiquetado de IoC simplifica su administración. Puede crear cualquier etiqueta, especificar su peso (importancia) y usarla para etiquetar los IOC manualmente. También puede ordenar y filtrar los IOC según estas etiquetas y su importancia.

El gráfico de investigación le permite explorar visualmente los datos y detecciones almacenados en CyberTrace, y descubrir los puntos en común 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 facilitar el intercambio de datos de amenazas entre instancias de Kaspersky CyberTrace y otras plataformas de TI.

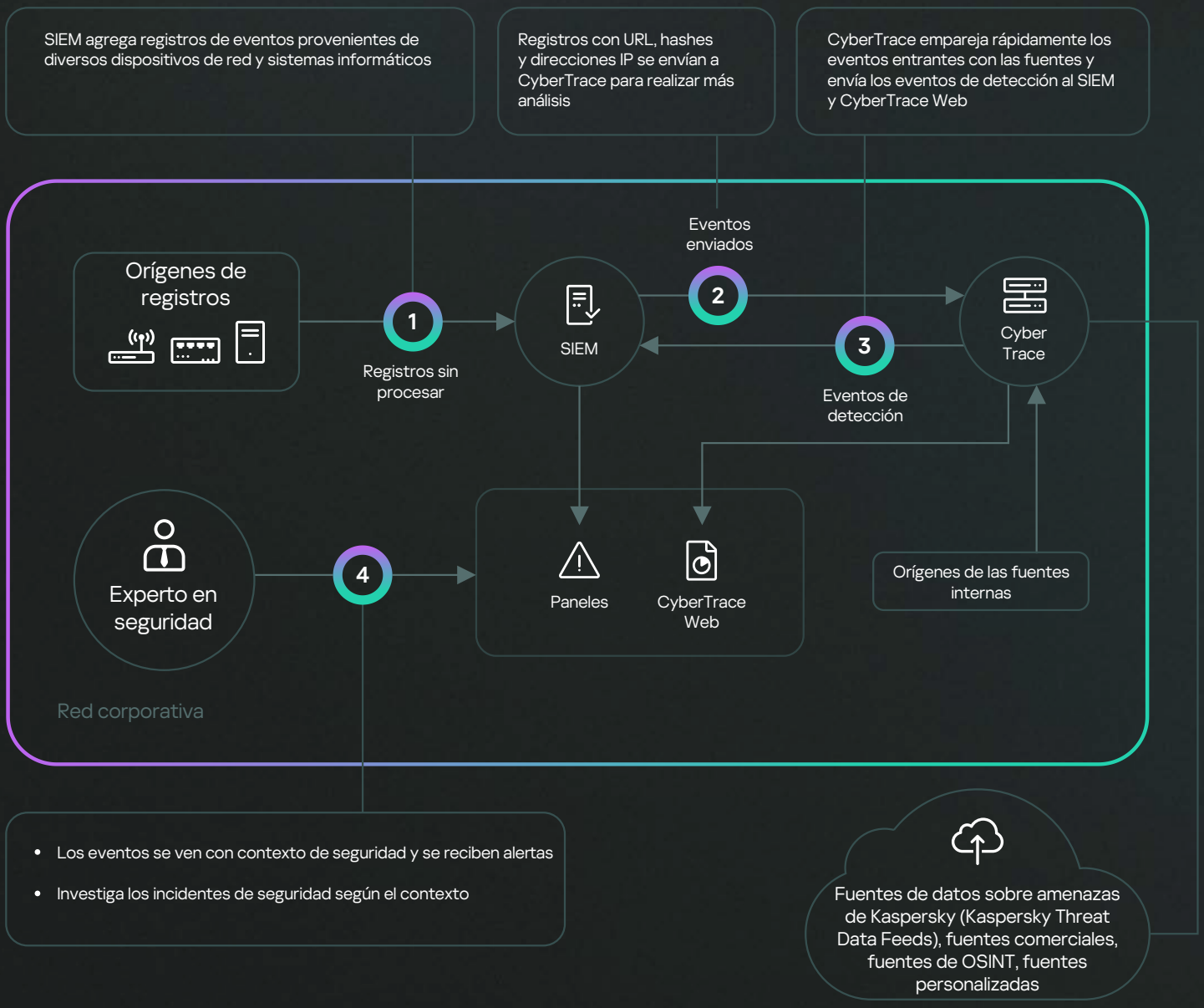
La función de correlación histórica (análisis retrospectivo) le permite analizar las observaciones de los eventos revisados anteriormente mediante las últimas entradas para encontrar amenazas descubiertas con anterioridad.

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 la carga en SIEM y la de los analistas.

HTTP RestAPI le permite buscar y administrar la inteligencia de amenazas.

¿Cómo funciona?



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 considerablemente la carga del SIEM.

Beneficios del uso de CyberTrace con Kaspersky Threat Data Feeds

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

Identificar inmediatamente las alertas críticas para su empresa y comunicárselas 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, con 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 sus 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 que adquirió Kaspersky sobre las ciberamenazas y sus relaciones, reunidos en un único y poderoso 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 su 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 le ayuda a proteger su organización y mejorar sus índices de respuesta ante incidentes.

¿Cómo funciona?

Objetos para analizar

Aspectos destacados

Inteligencia de confianza

Un atributo clave de Kaspersky Threat Lookup es la confiabilidad de sus datos de inteligencia, enriquecidos con información contextual práctica. 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

Sea proactivo en la prevención, la detección y la respuesta a ataques para minimizar su impacto y frecuencia. Rastree y neutralice ataques de manera proactiva lo antes posible. Cuanto antes se detecte una amenaza, menos daños causará, más rápidas serán las correcciones y con mayor prontitud podrán volver a la normalidad las operaciones de la red.

Fácil de usar

Interfaz web o API RESTful. Use el servicio en modo manual con una interfaz web (a través de un navegador) o acceda a él mediante una simple API RESTful, según lo prefiera.

Amplia gama de formatos de exportación

Los IOC (indicadores de compromiso) y la información contextual pueden exportarse en formatos muy usados, como STIX, OpenIOC, JSON, Yara, Snort o incluso CSV, para obtener el máximo beneficio de la inteligencia sobre amenazas, automatizar el flujo de trabajo operativo o integrarse con controles de seguridad como los SIEM.

Beneficios de Kaspersky Threat Lookup

1. Realiza búsquedas exhaustivas de indicadores de amenaza con un contexto altamente validado, lo que le permitirá priorizar los ataques y enfocarse en mitigar las amenazas que representen el mayor riesgo para su negocio.
2. Diagnostica y analiza, de forma, de forma más eficiente, los incidentes de seguridad de los hosts y la red, y priorice las señales de los sistemas internos frente a amenazas desconocidas.
3. Potencia sus capacidades de respuesta ante incidentes y de búsqueda de amenazas para alterar el esquema del ataque antes de que los sistemas y datos importantes estén en riesgo.
4. Busca indicadores de amenaza desde una interfaz web o la API RESTful.
5. Examina datos avanzados, incluidos certificados, certificados, nombres usados habitualmente, rutas de archivos o URL relacionadas con el fin de detectar nuevos objetos sospechosos.
6. Verifica si el objeto descubierto se extendió o es único y comprenda por qué un objeto debe tratarse como malicioso.

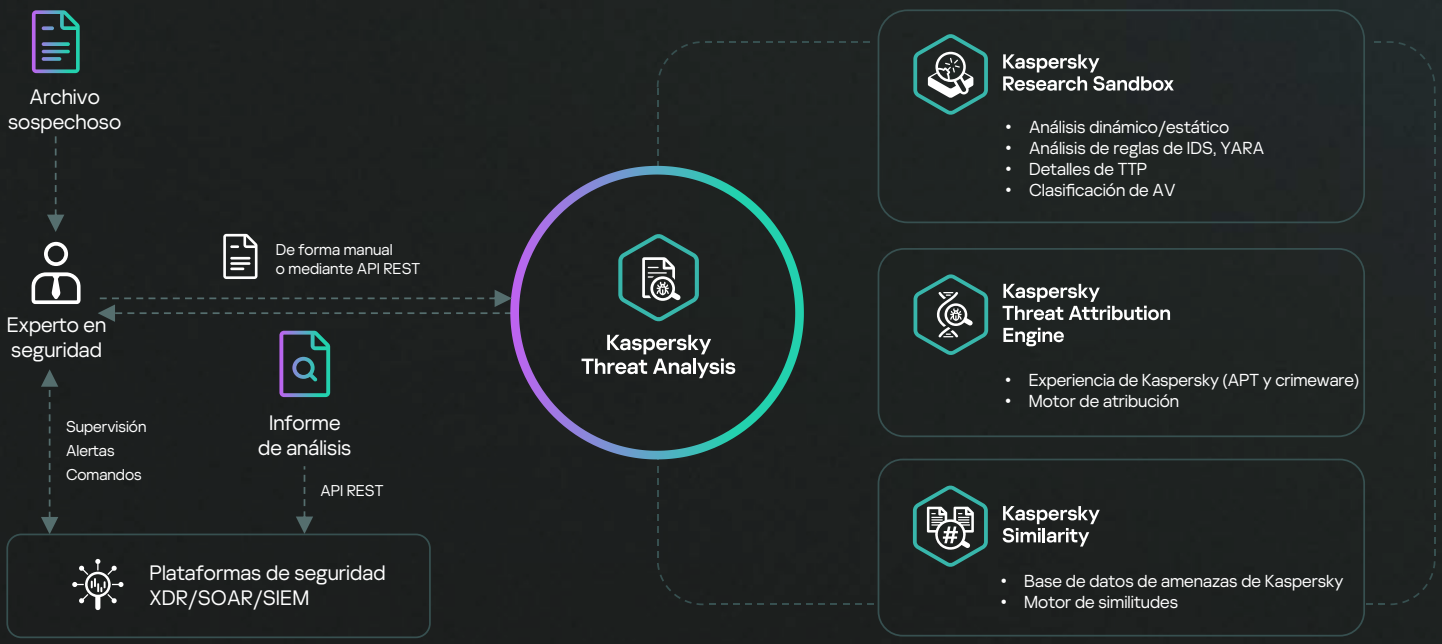
Kaspersky
Threat Analysis

Kaspersky Threat Analysis

Al enfrentarse a una ciberamenaza potencial, las decisiones que toma y su eficiencia resultan aspectos críticos. En la actualidad, es imposible evitar los ataques selectivos solo con herramientas antivirus tradicionales. Los motores antivirus son capaces de detener solo amenazas conocidas y sus variaciones, mientras que los atacantes más sofisticados usan todos los medios a su disposición para evadir la detección automática. La cantidad de alertas de seguridad que procesan los centros de operaciones de seguridad (SOC) crece exponencialmente día a día. Con la cantidad de muestras de malware generadas cada día, se vuelve casi inviable priorizar, evaluar y validar con eficiencia las alertas.

Para ayudar a los investigadores de seguridad a mantenerse al tanto de las amenazas emergentes y existentes, Kaspersky proporciona un marco único y resiliente para automatizar el análisis rutinario de archivos sospechosos. Además de contar con herramientas de análisis de amenazas tradicionales, como los sandbox, Kaspersky Threat Analysis ofrece tecnologías de atribución de última generación y soluciones avanzadas de análisis de similitud. Este enfoque híbrido brinda un análisis eficiente de amenazas, permitiendo tomar decisiones informadas y mantener las infraestructuras protegidas. Kaspersky Threat Analysis se proporciona a través de interfaces web unidas y RESTful.

Componentes de Kaspersky Threat Analysis



Kaspersky
Research Sandbox

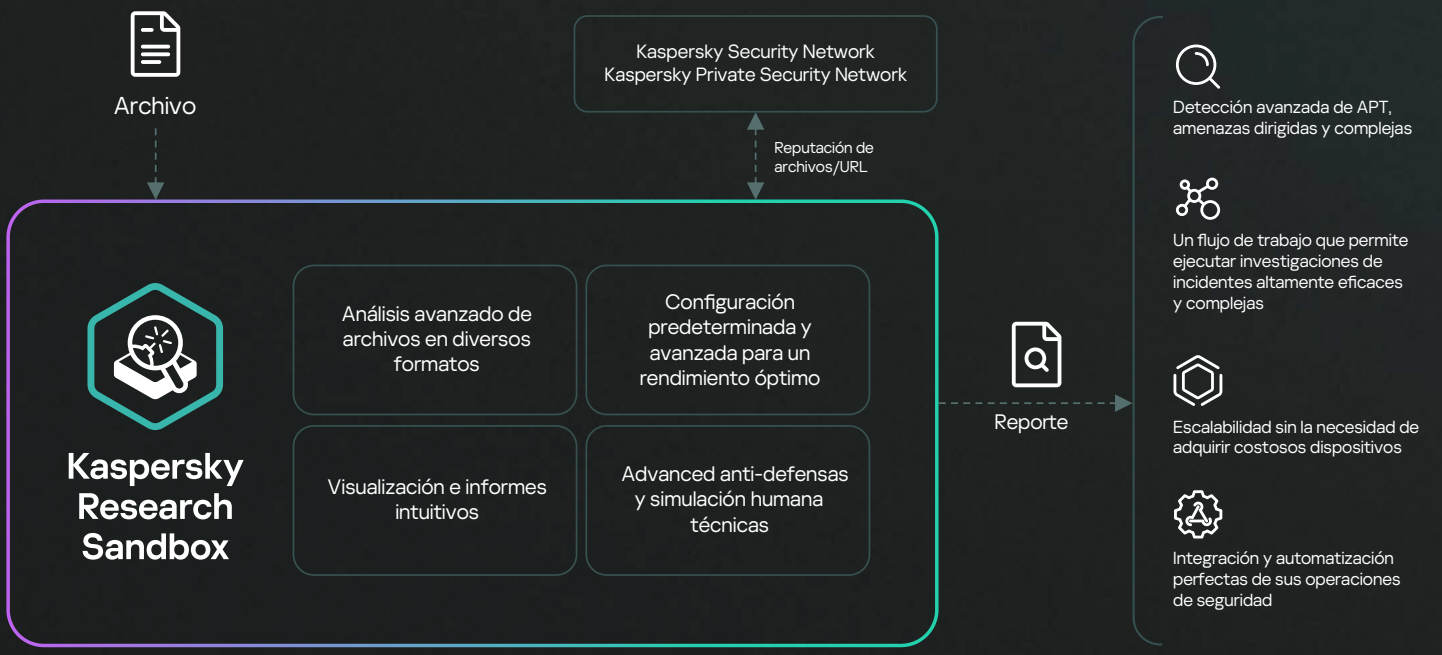
Kaspersky Research Sandbox

Kaspersky Research Sandbox se desarrolló 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 del malware que hemos adquirido durante nuestra investigación ininterrumpida de amenazas, lo que nos permite detectar más de 420.000 nuevos objetos maliciosos cada día.

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

Esta tecnología, que se implementa en las instalaciones, evita la divulgación de datos fuera de la organización. Además, permite crear entornos de ejecución personalizados para el análisis y adaptarlos a escenarios reales. De este modo, se incrementa la precisión en la detección de amenazas y la velocidad de la investigación.

¿Cómo funciona?



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
- Más de 1.000 búsquedas únicas para la extracción de tácticas, técnicas y procedimientos (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
- Carga manual de muestras y una API REST mejorada para su integración en flujos de trabajo automatizados

Kaspersky
Threat Attribution
Engine

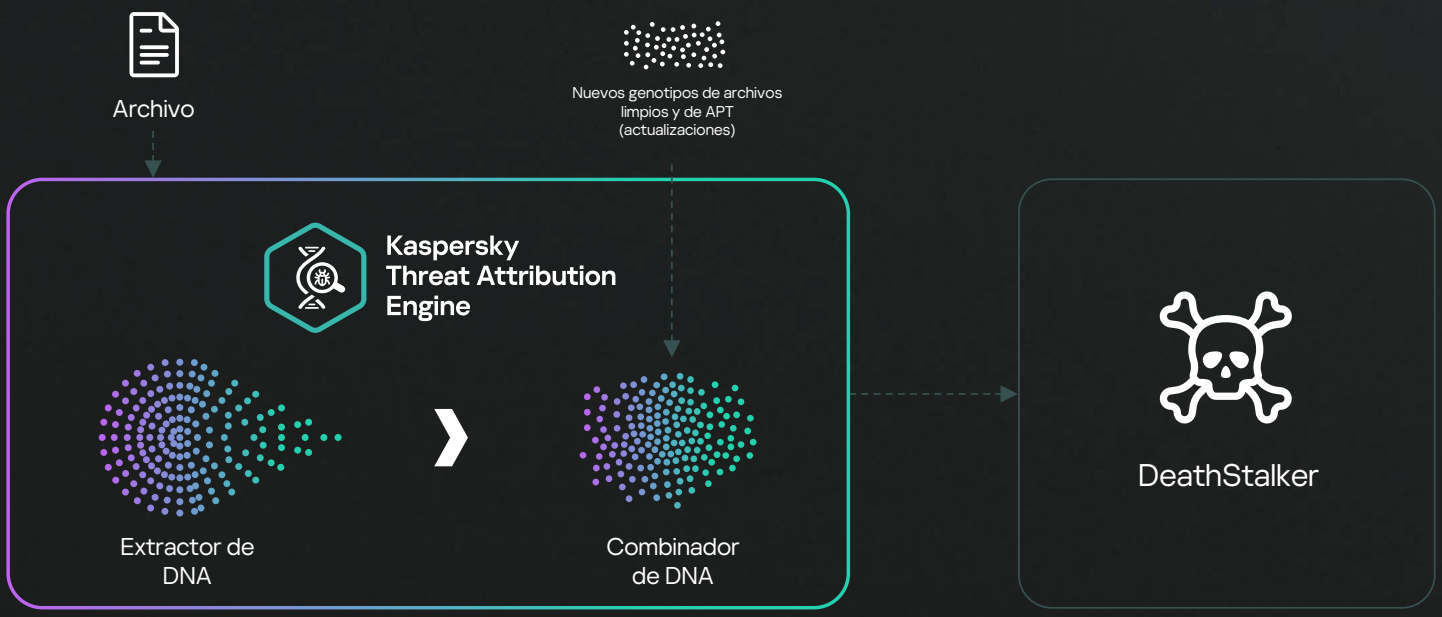
Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine es una herramienta de análisis única que proporciona conocimientos e información acerca del origen del malware de alto perfil y sus posibles autores. Vincula un archivo sospechoso a amenazas avanzadas persistentes (APT), atacantes y campañas conocidas de manera rápida, mediante un algoritmo único y una base de datos especial que contiene muestras de malware de APT y el mayor conjunto de archivos limpios de la industria, recopilados por expertos de Kaspersky a lo largo de más de 25 años.

Hacemos seguimiento a más de 1.100 atacantes y campañas, y publicamos más de 200 informes de inteligencia de amenazas al año. Nuestra investigación continua respalda una colección de APT que contiene más de 100.000 archivos, los cuales, junto con el uso de herramientas automatizadas, ofrecen niveles de atribución con una precisión 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 pueda tomar medidas proactivas a tiempo y así evitar que un atacante logre infiltrarse en su sistema. Kaspersky Threat Attribution Engine se puede implementar en entornos seguros y aislados, lo que restringe el acceso de cualquier agente externo a la información procesada y los objetos enviados. La implementación local ofrece funciones adicionales para agregar agentes y muestras propias, lo que permite detectar archivos similares a los de su colección privada, así como exportar reglas YARA para realizar búsquedas automatizadas de archivos similares en su infraestructura e integrarse con soluciones de terceros.

¿Cómo funciona?



Método de búsqueda patentado

Para vincular el malware con las entidades de atribución, Kaspersky Threat Attribution Engine utiliza un método patentado y exclusivo de búsqueda de genotipos y cadenas similares entre 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 archivos en busca de genotipos y cadenas que se asemejen a los de muestras de APT previamente analizadas o ya vinculadas con entidades de atribución.

3

Basado en los genotipos y cadenas similares encontrados en las muestras de APT, se genera un informe sobre el origen de la muestra analizada, las entidades de atribución relacionadas y cualquier semejanza entre esta muestra y las muestras conocidas de APT.

Aspectos destacados del producto

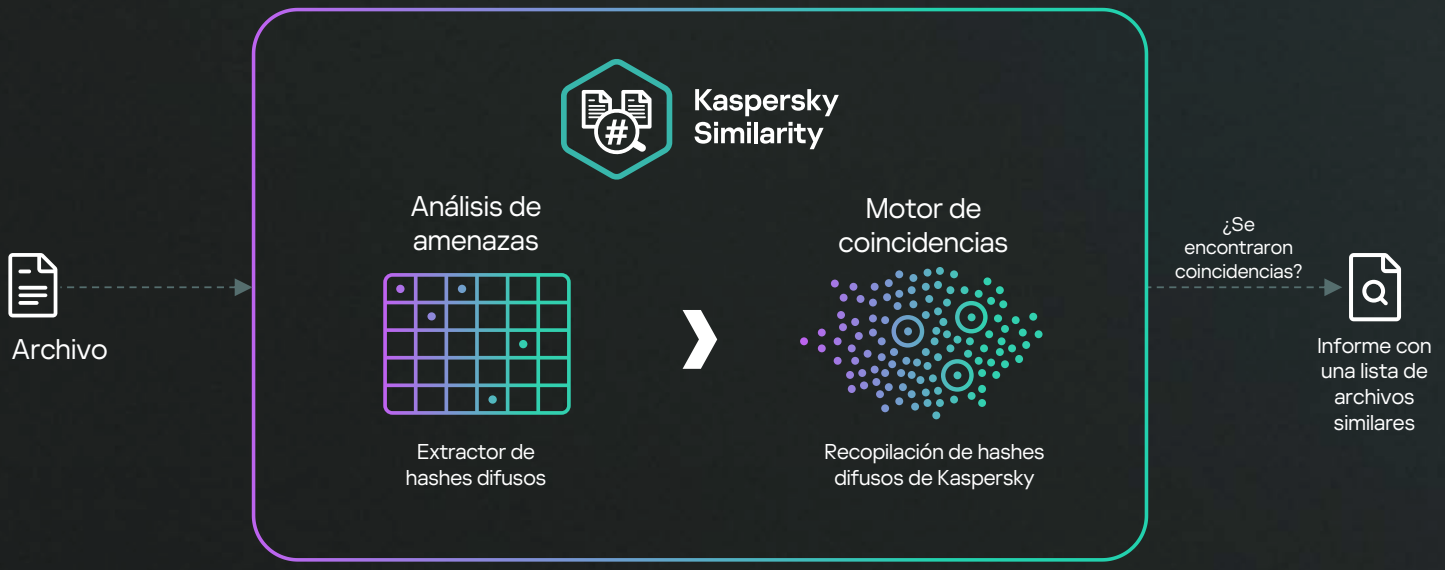
- Tecnología patentada
- Acceso instantáneo a un repositorio de datos seleccionados sobre miles de agentes, muestras y campañas de APT.
- Carga manual de muestras y una API REST mejorada para su integración en flujos de trabajo automatizados
- Operatividad para descomprimir archivos protegidos con contraseña 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 que permite una configuración rápida del producto y un ahorro de costos, ya que no es necesario invertir en hardware por adelantado.

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 le permite buscar malware similar (por ej., evasivo) y buscarlo en la infraestructura para que esté 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 crearon un conjunto de hashes para determinar la similitud entre diferentes archivos, basándose en estos atributos.

Kaspersky Similarity les permite a los usuarios enviar un archivo sospechoso, extraer sus hashes y compararlos con hashes de archivos 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 según la puntuación de similitud. El informe contiene el contexto adicional, con metadatos para cada archivo similar:

- Confiabilidad 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 de archivo

Aspectos destacados

- Tecnología patentada
- Utiliza una de las bases de datos de archivos maliciosos y limpios más extensas de la industria, recopilada durante más de 25 años, lo que permite una cobertura máxima y mayor precisión en las comparaciones
- Carga manual de muestras y una 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:

Conozca más

Beneficios de Kaspersky Threat Lookup

1

Potencie su respuesta ante incidentes y sus actividades forenses con Kaspersky Research Sandbox, que le proporciona el análisis dinámico más avanzado de archivos sospechosos con capacidad para encontrar amenazas de día cero y obtener resultados asignados a las TTP de MITTRE ATT&ACK.

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 integral del vector de ataque con pasos claros de mitigación que permiten reducir los tiempos de respuesta ante incidentes de meses a minutos.

3

Detecte amenazas evasivas con Kaspersky Similarity, que permite encontrar muestras maliciosas diseñadas específicamente para eludir las tecnologías antimalware tradicionales y detectar los ataques APT más sofisticados, que pueden permanecer sin ser detectados durante años.

Kaspersky Intelligence Reporting

Informes de Kaspersky Threat Intelligence

Para contrarrestar las ciberamenazas modernas, se requiere una visión completa de las tácticas, las técnicas y los procedimientos que usan los cibercriminales. Aunque los C&C y las herramientas que se utilizan en los ataques cambian con frecuencia, es difícil que los atacantes cambien su comportamiento y métodos durante la ejecución de un ataque. Identificar y exponer estos patrones de inmediato ayuda a implementar mecanismos de defensa eficientes de antemano, lo cual desarma a los cibercriminales e interrumpe la cadena de ataques.

La suscripción a los Informes de Kaspersky Threat Intelligence proporciona un acceso continuo y exclusivo a nuestra investigación, lo que proporciona información actualizada sobre las amenazas más peligrosas, permitiéndole a usted y a su equipo de seguridad implementar proactivamente 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 le 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.

Más de 200
informes privados al año

Más de 300
Ciberdelincuentes

Más de 500
ciberespionaje

Más de 2.500
Reglas YARA

Más de 170.000
IOC

Los informes analíticos incluyen lo siguiente:

Perfiles de ciberdelincuentes

Asignación a MITRE ATT&CK

Resumen ejecutivo (información orientada al nivel ejecutivo)

El análisis técnico exhaustivo incluye lo siguiente:

- Métodos de ataque
- Exploits utilizados
- Descripción del malware
- Descripción de los protocolos y la infraestructura de C&C
- Análisis de víctimas
- Análisis de exfiltración de datos
- Atribuciones

Indicadores de compromiso (IOC) y reglas YARA / SIGMA / de Suricata

Recomendaciones de los expertos de Kaspersky

Ofrecemos varias opciones de informes comerciales en función de sus necesidades y de las características específicas de su 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, 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 su 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, como la venta de datos robados en la web oscura, el fraude financiero, el ransomware y el malware para cajeros automáticos y puntos de venta (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 su empresa realiza una gran cantidad de negocios en línea o si tiene en su poder datos confidenciales de clientes, por ejemplo, si es una entidad financiera o una plataforma de comercio electrónico.

Kaspersky ICS Threat Intelligence

Proporciona inteligencia detallada y un mayor conocimiento de las campañas maliciosas dirigidas a las organizaciones industriales, así como información sobre las vulnerabilidades presentes 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 la investigación de amenazas y vulnerabilidades de ICS, respuesta ante incidentes y análisis de seguridad, establecido en 2016, es el encargado de ofrecer este informe. Estos reportes 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 desee 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 de amenazas de sistemas de control industrial (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

Consulte con los expertos de Kaspersky ICS CERT, quiénes le proporcionarán asesoramiento individual sobre las amenazas y vulnerabilidades de ciberseguridad industrial, estadísticas y panorama de amenazas, normas industriales, etc. más importantes para usted.

Kaspersky Threat Intelligence Reporting le 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 / de Suricata.

Perfiles de ciberdelincuentes

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

MITRE ATT&CK

Todas las TTP descritas en los informes se le 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 las TTP relevantes.

Análisis retrospectivo

Se ofrece acceso a todos los informes privados publicados con anterioridad durante el período de su suscripción.

Compatibilidad con API RESTful

Integración y automatización perfectas de sus flujos de trabajo de seguridad.

Kaspersky
Digital Footprint
Intelligence

Kaspersky Digital Footprint Intelligence

A medida que su negocio crece, la complejidad y distribución de sus entornos de TI también aumentan, lo que dificulta la protección de una presencia digital ampliamente distribuida sin control ni propiedad directos. Los ambientes 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 tener una imagen precisa de la presencia en línea de su organización, sino también poder hacer un seguimiento de sus cambios y reaccionar ante las amenazas externas dirigidas a los activos digitales expuestos.

Si bien las organizaciones utilizan una amplia gama de herramientas en sus operaciones de seguridad, sigue habiendo amenazas digitales al acecho que requieren capacidades muy específicas: detectar y mitigar filtraciones de datos, supervisar planes y esquemas de ataque de ciberdelincuentes ubicados en foros de la web oscura, etc. Para ayudar a los analistas de seguridad a explorar la visión que tiene el adversario de los recursos de su empresa, detectar rápidamente los posibles vectores de ataque disponibles para ellos y ajustar sus defensas en consecuencia, Kaspersky creó 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

La 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 vulnerabilidades existentes, con una evaluación integral de riesgos y una puntuación mejorada, basada en la puntuación base del CVSS, la disponibilidad de exploits públicos, la experiencia en pruebas de penetración y la ubicación del recurso de red (alojamiento/infraestructura).

Supervisión de la web oscura

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

Descubrimiento de filtraciones de datos

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

Soporte de tenencia múltiple

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

Fuentes de inteligencia

Es esencial que tenga una comprensión integral de la postura de seguridad externa de su empresa. Para brindar esta información, los analistas de seguridad de Kaspersky recopilan y agregan información de las siguientes fuentes de inteligencia:

Sus datos no estructurados

- Direcciones IP
- Dominios de la empresa
- Marcas comerciales
- 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 a través de las fuentes de Kaspersky, así como en la web oscura y superficial.

Informes analíticos*

¿Cómo funciona?

Configurar	Recopilar	Filtro	Notificación
Descubrimiento de la información sobre los activos digitales de la empresa	Recopilación automatizada de datos desde la web 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 oportunas en el Portal de Kaspersky Threat Intelligence o a través de la API

*Servicio complementario

Valores comerciales de Digital Footprint Intelligence

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

Detección de amenazas

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

Reduzca los ciberriesgos

Brinde a las partes interesadas (director de experiencia de cliente y Junta Directiva) información sobre dónde enfocar el gasto en ciberseguridad, revelando las brechas en la configuración actual y los riesgos que conllevan.

Reaccione más rápido

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

Reduzca la superficie de ataque

Gestione la presencia digital de su empresa y controle los recursos de red externos para minimizar los vectores de ataque y las vulnerabilidades que pueden usarse en un ataque.

Comprenda a sus adversarios

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

Conozca lo desconocido

Mejore su capacidad de resistencia ante ciberataques e identifique las amenazas externas a la jurisdicción de sus 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 administrados (MSSP) y sus clientes, además de a las organizaciones grandes de múltiples filiales.

Kaspersky Takedown Service

Kaspersky Takedown Service

Los ciberdelincuentes crean dominios maliciosos y de phishing que se utilizan para atacar su empresa y sus marcas. La incapacidad de mitigar rápidamente estas amenazas, luego de que se identifican, puede conducir a una pérdida de ingresos, daños a la marca, pérdida de confianza del cliente, filtración de datos y demás. Sin embargo, la administración de la eliminación de estos dominios es un proceso complejo que requiere de experiencia y tiempo.

Kaspersky Takedown Service mitiga rápidamente las amenazas planteadas por los dominios maliciosos y de phishing antes que causen algún daño a su marca y empresa. La administración de extremo a extremo del proceso completo ahorra tiempo y recursos valiosos. El servicio se presta en todo el mundo.

Kaspersky bloquea más de 15.000 URLs de phishing y estafa, y evita más de un millón de intentos de acceso a estas 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 administrar su eliminación y 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 la colaboración con organizaciones internacionales, organismos de seguridad nacionales y regionales (como INTERPOL, Europol, la Unidad de Crimen Digital de Microsoft, la Unidad Nacional de Delitos de Alta Tecnología (NHTCU) de la policía de los Países Bajos y la Policía de Londres), así como con los Equipos de Respuesta a Emergencias Informáticas (CERT) de todo el mundo.

Visibilidad completa

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

Administración de extremo a extremo

Administraremos todo el proceso de eliminación y reduciremos su participación.

Cobertura global

No importa dónde se registre un dominio malicioso o de phishing, Kaspersky solicitará su eliminación a la organización regional correspondiente y a las autoridades legales pertinentes.

Funcionamiento

Puede enviar sus 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 o regional respectiva (CERT, registro, etc.) que posee los derechos legales necesarios para desactivar los dominios. Recibirá notificaciones en cada etapa del proceso hasta que se elimine el recurso deseado.

Protección simple

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

Kaspersky
Ask the Analyst

Kaspersky Ask the Analyst

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

En una época de ciberataques capaces de aniquilar 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 luchen solos contra las amenazas sofisticadas: es importante que puedan obtener ayuda de expertos externos. Los especialistas externos pueden explicar la posible trayectoria de los ataques complejos y APT, brindando consejos útiles sobre la forma más decisiva de eliminarlos.

La investigación continua de amenazas permite a Kaspersky descubrir, infiltrarse y supervisar las comunidades cerradas y los foros clandestinos de todo el mundo, que los atacantes y ciberdelincuentes suelen frecuentar. 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.

El servicio Kaspersky Ask the Analyst amplía nuestro portafolio de inteligencia de amenazas, permitiéndole solicitar asesoramiento e información sobre amenazas específicas a las que se enfrenta o en las que está interesado. El servicio adapta las potentes capacidades de inteligencia e investigación de amenazas de Kaspersky a sus necesidades específicas, permitiéndole construir defensas resistentes contra las amenazas que afectan a su organización.

Productos 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 y IoC relacionados

- Descripción general de una familia específica de malware
- Contexto adicional de las amenazas (hashes relacionados, URL, CnCs, etc.)
- Información sobre una vulnerabilidad específica (su nivel de gravedad 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 para una región/industria
- Información de análisis de malware de ICS sobre las normas o estándares

Inteligencia de la web oscura

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

Análisis de malware

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

¿Cómo funciona?

Kaspersky Ask the Analyst se puede adquirir por separado o como complemento de cualquiera de nuestros servicios de inteligencia de amenazas. Puede enviar sus solicitudes a través de Kaspersky Company Account, nuestro portal corporativo de servicio al cliente. Le responderemos por correo electrónico, pero si lo desea, podemos organizar una videoconferencia o una sesión de pantalla compartida. Una vez aceptada su solicitud, le informaremos del plazo estimado para el procesamiento.

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

Obtenga detalles sobre las vulnerabilidades y recomendaciones sobre cómo protegerse si hay intentos de aprovecharlas.

4

Obtenga detalles adicionales sobre las actividades específicas de la web oscura que sean de su interés.

5

Consiga una descripción general de la familia del malware, que incluya su comportamiento, su impacto potencial y detalles sobre cualquier otra actividad relacionada que Kaspersky haya observado.

6

Priorizar las alertas o incidentes de forma eficaz, gracias a la detallada información contextual y la categorización de los IoC relacionados, proporcionadas en informes cortos.

7

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

8

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

Beneficios de Kaspersky Ask the Analyst

Amplíe su experiencia

Obtenga acceso a pedido a los expertos del sector, sin tener que buscar ni invertir en especialistas de tiempo completo, que son difíciles de encontrar.

Acelere las investigaciones

Use información contextual adaptada y detallada para analizar y priorizar incidentes con eficacia.

Responda rápido

Responda rápidamente a las amenazas y vulnerabilidades con nuestra guía para bloquear ataques a través de vectores conocidos.

Amplíe sus conocimientos y recursos

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

Conclusión

Para contrarrestar las ciberamenazas de hoy, se requiere una visión completa de las tácticas y las herramientas que usan los cibercriminales. Generar esta inteligencia e identificar las contramedidas más eficaces requiere dedicación constante y altos niveles de experiencia. Con una gran cantidad de petabytes de datos de amenazas para aprovechar, tecnologías avanzadas de aprendizaje automático y un grupo exclusivo de expertos a nivel mundial, trabajamos para asistir a nuestros clientes con la inteligencia de amenazas más reciente del mundo y los ayudamos a mantener inmunidad incluso ante ciberataques desconocidos.

Ventajas clave

Permite la visibilidad de amenazas globales, 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, técnicas y procedimientos que utilizan los actores en diferentes industrias 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 su fuerza de trabajo se concentre en amenazas genuinas.

La respuesta acelerada y mejorada frente a incidentes y las capacidades de búsqueda permiten reducir el tiempo de espera contra ataques y minimizar de gran manera el posible daño.

Kaspersky Threat Intelligence

Conozca más

https://latam.kaspersky.com

#kaspersky
#bringonthefuture