Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

El desafío

El seguimiento, el análisis, la interpretación y la mitigación de las amenazas para la seguridad de la IT es una tarea colosal, puesto que no dejan de evolucionar. Empresas de todos los segmentos se enfrentan a la falta de información relevante y actualizada que necesitan para poder gestionar los riesgos derivados de las amenazas a la seguridad de IT.

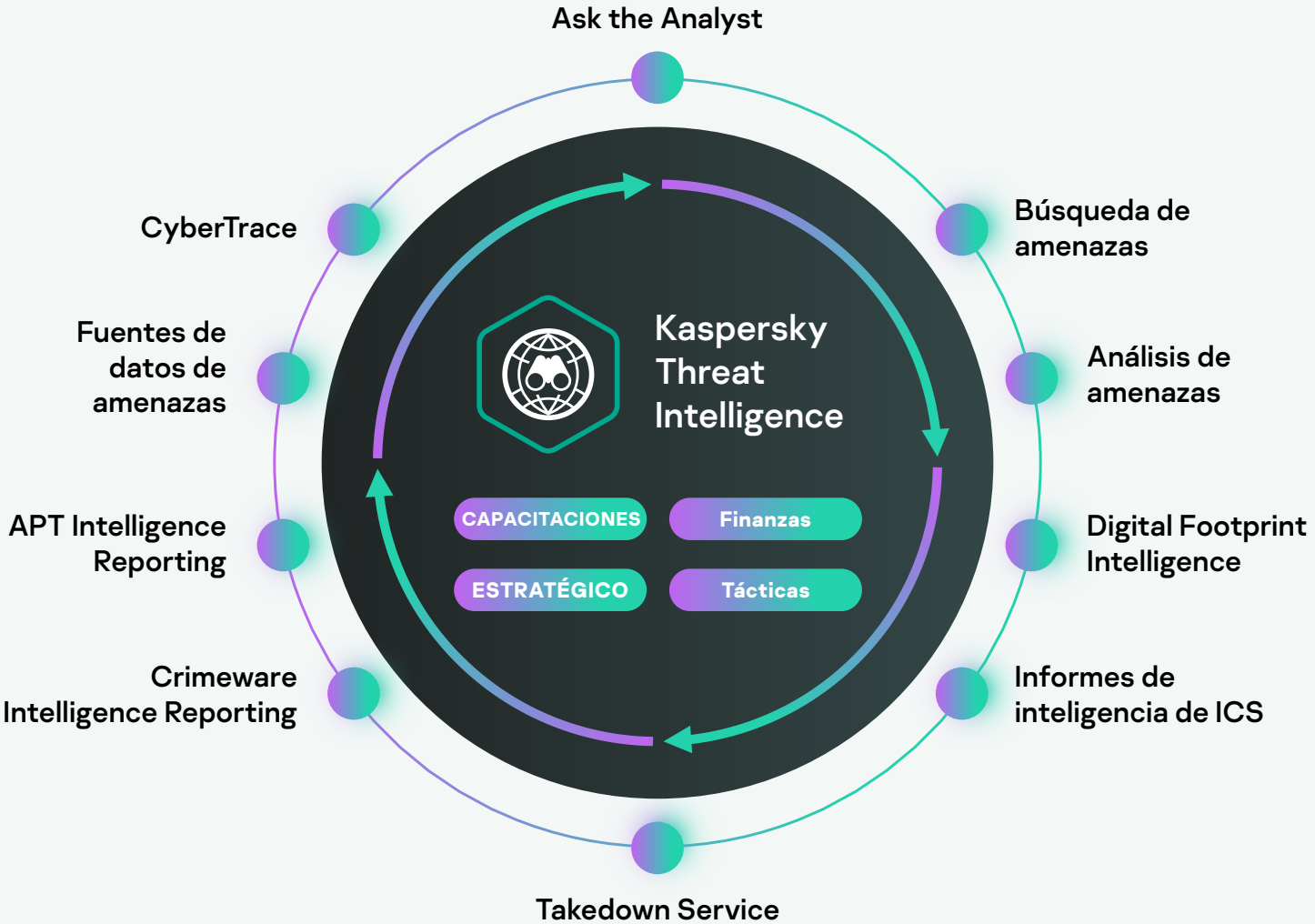
Kaspersky Threat Intelligence

Threat Intelligence de Kaspersky le da acceso a la inteligencia que necesita para mitigar ciberamenazas, proporcionada por nuestro equipo líder de investigadores y analistas.

Gracias a sus conocimientos, experiencia e inteligencia avanzada sobre todos los aspectos de la ciberseguridad, Kaspersky se ha convertido en el partner de confianza de las fuerzas del orden y las agencias gubernamentales más importantes del mundo, entre las que se incluyen la Interpol e importantes equipos CERT. Kaspersky Threat Intelligence le ofrece acceso inmediato a inteligencia de amenazas técnica, táctica, operativa y estratégica.

La cartera de Kaspersky Threat Intelligence incluye lo siguiente:

Threat Data Feeds, CyberTrace (una plataforma de Threat Intelligence), Threat Lookup, Threat Analysis (Cloud Sandbox y Cloud Threat Attribution Engine), una variedad de opciones de Threat Intelligence Reporting y servicios que proporcionan experiencia en inteligencia frente a amenazas a petición del cliente.



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 utilizan complicados esquemas de ataque de intrusión, campañas, así como tácticas, técnicas y procedimientos (TTP) personalizados para interrumpir las actividades de su negocio o dañar a sus clientes. Es evidente que se necesitan nuevos métodos de protección basados en la inteligencia de amenazas.

Mediante la integración de fuente de inteligencia de amenazas actualizadas que contienen información sobre IPs sospecchosas y peligrosas, URLs y archivos en los sistemas de seguridad existentes como SIEM, SOAR y plataformas de inteligencia de amenazas, 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 obtener una mayor investigación y respuesta.

- FUENTE DE DATOS DE REPUTACIÓN DE DIRECCIONES IP
- FUENTE DE DATOS DE HASHES (WIN/*nix/MacOS/AndroidOS/iOS)
- FUENTES DE DATOS DE DIRECCIONES URL (maliciosas, phishing y C&C)
- FUENTE DE URL DE RANSOMWARE
- FUENTES DE IOC DE APT
- FUENTE DE VULNERABILIDAD
- FUENTE DE DNS PASIVO (pDNS)
- FUENTE DE URL DE IoT
- FUENTE DE LISTAS DE PERMISO
- FUENTE DE DATOS DE HASHES DE SCI

Y MÁS

Kaspersky Threat Data Feeds

Datos contextuales

Todos los registros de cada fuente de datos se mejoran con contexto útil (nombres de amenazas, marcas de tiempo, geolocalización, direcciones IP resueltas de recursos web infectados, hashes, popularidad, etc.). Los datos contextuales ayudan a revelar una "visión de conjunto", lo que mejora la validación y complementación de un uso variado de los datos. Cuando están en contexto, los datos se pueden utilizar de forma más inmediata para responder a quién, qué, dónde y cuándo, lo que permite identificar a los adversarios y ayuda a tomar decisiones rápidas y a actuar.

Aspectos destacados

Las fuentes de datos se generan automáticamente en tiempo real, en función de las conclusiones recopiladas a nivel mundial (Kaspersky Security Network ofrece visibilidad de un gran porcentaje de todo el tráfico de Internet, con decenas de millones de usuarios finales en más de 213 países), lo que ofrece unos altos índices de detección y precisión.

Facilidad de implementación. Se combina toda la documentación complementaria, muestras, un responsable técnico de cuenta específico y soporte técnico de Kaspersky para permitir la integración simple.

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.

Recopilación y procesamiento

Las fuentes de datos proceden de una fusión de fuentes heterogéneas de gran confiabilidad como, por ejemplo, Kaspersky Security Network y nuestros propios rastreadores web, nuestro servicio de supervisión de botnets (supervisión ininterrumpida de botnets y de sus objetivos y actividades), trampas de spam, equipos de investigación y partners.

A continuación, todos los datos agregados se inspeccionan cuidadosamente en tiempo real mediante varias técnicas de procesamiento previo, como criterios estadísticos, sandboxes, motores heurísticos, herramientas de similitud, creación de perfiles de análisis, validación de analistas y verificación de listas de permisos.

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 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.

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

Ventajas

Refuerce sus soluciones de defensa de la red, como SIEM, firewalls, 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. Los principales SIEM (incluidos HP ArcSight, IBM QRadar, Splunk, etc.) y las plataformas de TI son totalmente compatibles.

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.

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.

Como MSSP, haga crecer su empresa proporcionando inteligencia de amenazas líder del sector como servicio premium a sus clientes. Como CERT, mejore y amplíe sus capacidades de identificación y detección de ciberamenazas.

Kaspersky CyberTrace

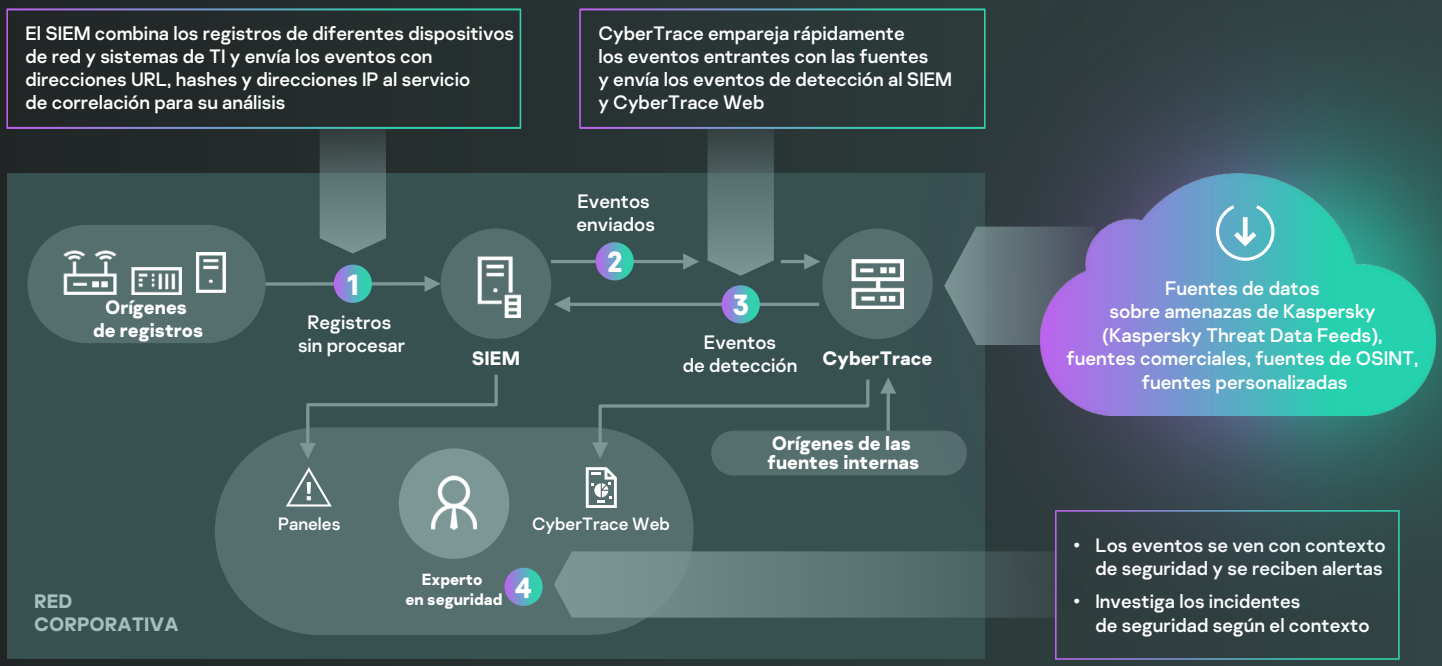
Mediante la integración de la inteligencia frente a amenazas actualizada al minuto y legible por máquinas en los controles de seguridad existentes, como los SIEM, los centros de operaciones de seguridad pueden automatizar el proceso inicial de evaluación. Al mismo tiempo, pueden ofrecer suficiente contexto a sus especialistas de primer nivel como para identificar de inmediato las alertas que se deben investigar o escalar a los equipos de Respuesta a Incidentes para obtener una mayor investigación y respuesta. Sin embargo, el crecimiento continuo de la cantidad de fuentes de datos sobre amenazas y de inteligencia frente a amenazas disponibles dificulta que las organizaciones determinen qué información es relevante para ellas. La inteligencia frente a amenazas se proporciona 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.

Kaspersky CyberTrace es una plataforma de inteligencia frente a amenazas que facilita la integración perfecta de fuentes de datos sobre amenazas con soluciones de SIEM. De esta manera, los analistas pueden aprovechar con mayor eficacia 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.

Kaspersky CyberTrace entrega un conjunto de instrumentos para hacer efectiva la inteligencia de amenazas:

- Una base de datos de indicadores con búsqueda de texto completo y la habilidad para buscar utilizando consultas avanzadas de búsqueda permite realizar complejas investigaciones a través de todos los cambios de indicadores, incluyendo campos de contexto.
- Las páginas con información detallada sobre cada indicador proporcionan un análisis aún más profundo. En cada página, se presenta la información sobre un indicador de todos los proveedores de inteligencia de amenazas (deduplicación) para que los analistas puedan estudiar las amenazas en los comentarios y agregar una inteligencia de amenazas interna acerca del indicador.
- Un gráfico de investigación permite explorar visualmente los datos y las detecciones que se almacenan en CyberTrace, y descubrir los puntos comunes 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), así como el intercambio de datos de amenazas entre las instancias de Kaspersky CyberTrace y con otras plataformas TI.
- El etiquetado de IOC simplifica su administración. Puede crear cualquier etiqueta y especificar su peso (importancia), y usarla para etiquetar IOC de forma manual. También puede ordenar y filtrar IOC de acuerdo con estas etiquetas y su importancia.
- La función de correlación histórica (retroscan) le permite analizar las observaciones de los eventos revisados anteriormente mediante las últimas entradas para encontrar amenazas descubiertas con anterioridad.
- Un filtro envía eventos de detección a las soluciones de SIEM, lo que reduce su carga y la de los analistas.
- La multitenencia es compatible con los MSSP y los casos de uso de grandes empresas.
- 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 a los proveedores de inteligencia de amenazas más valiosos.
- HTTP RestAPI le permite buscar y administrar la inteligencia de amenazas.

La herramienta utiliza un proceso interno de análisis y correlación de datos entrantes, lo que reduce significativamente la carga de trabajo de SIEM. 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. En el siguiente diagrama, se muestra una arquitectura general de la integración que ofrece la solución:



Gracias a Kaspersky CyberTrace y Kaspersky Threat Data Feeds, los analistas de seguridad serán capaces de lo siguiente:

- Sintetizar y priorizar eficazmente grandes cantidades de alertas de seguridad.
- Mejorar y acelerar los procesos de evaluación y respuesta inicial.
- Identificar de inmediato las alertas críticas para la empresa y tomar decisiones más informadas sobre cuáles se deben escalar a los equipos de IR.
- Formar una defensa proactiva e inteligente.

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.

Aspectos destacados

Inteligencia de confianza: un atributo clave de Kaspersky Threat Lookup es la confiabilidad de nuestros datos de inteligencia de amenazas, que se mejoran con contexto útil. Kaspersky está a la vanguardia de las pruebas antimalware[1], 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 una persona proactiva en la prevención, detección y respuesta frente 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, más rápido se harán las correcciones y con mayor prontitud podrán volver a la normalidad las operaciones de red.

Investigaciones de incidentes: un gráfico de investigación potencia las investigaciones de incidentes al permitirle explorar visualmente los datos y las detecciones almacenados en Threat Lookup. Ofrece una visualización gráfica de la relación entre las URL, los dominios, las IP, los archivos y otros contextos para que pueda comprender el alcance completo de un incidente e identificar su causa raíz.

Búsqueda maestra: busque información en todos los productos de inteligencia de amenazas y fuentes externas (incluyendo los IoC de OSINT, la Web oculta y la Web visible) en una única y potente interfaz.

Interfaz web o API RESTful fáciles de usar: use el servicio en modo manual mediante una interfaz web (a través de un navegador web) o acceda a través de una simple API RESTful, según sus preferencias.

Amplia gama de formatos de exportación: exporte IOC (Indicadores de compromiso) o contexto útil sobre los formatos de uso compartido legibles por máquina más utilizados y organizados, como STIX, OpenIOC, JSON, Yara, Snort o incluso CSV, para disfrutar de todas las ventajas de la inteligencia de amenazas, automatizar el flujo de trabajo de operaciones o integrarlos en los controles de seguridad como SIEM.

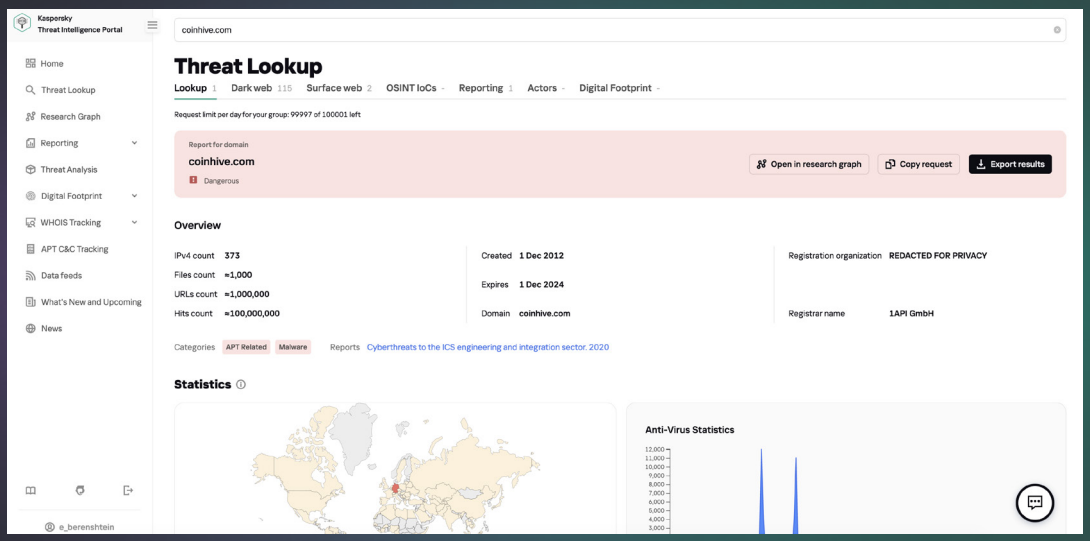
Ventajas

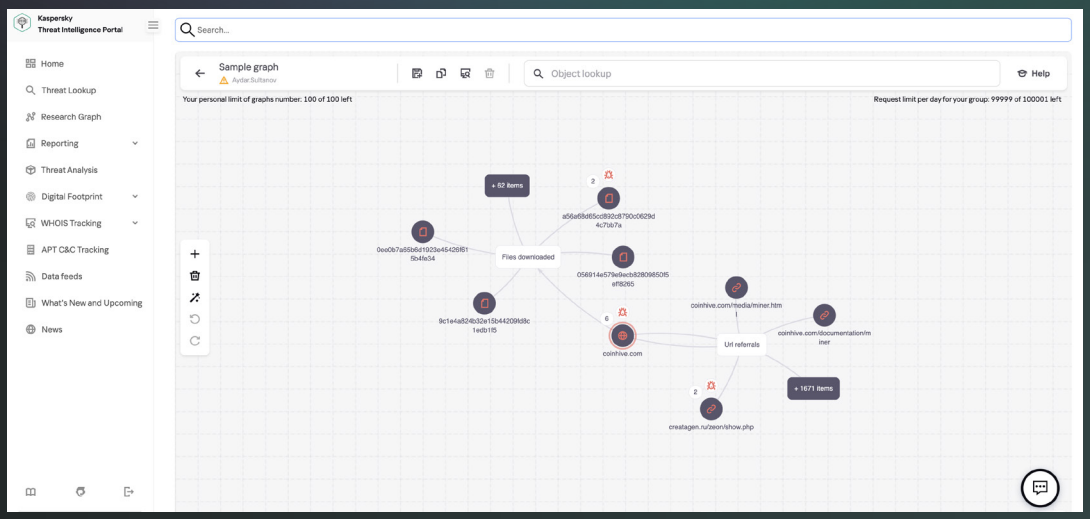
Realice búsquedas exhaustivas sobre indicadores de amenaza con un contexto de amenazas altamente validado que le permite priorizar los ataques y enfocarse en mitigar las amenazas que impliquen el mayor riesgo para su negocio.

Diagnostique y analice, de forma más eficiente y efectiva, los incidentes de seguridad de los hosts y la red, y priorice las señales de los sistemas internos frente a amenazas desconocidas.

Potencie 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 se vean comprometidos.

[1] kaspersky.com/top3





Ahora es posible

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

Examinar datos avanzados, que incluyen certificados, nombres usados habitualmente, rutas de archivos o URL relacionadas con el fin de detectar nuevos objetos sospechosos.

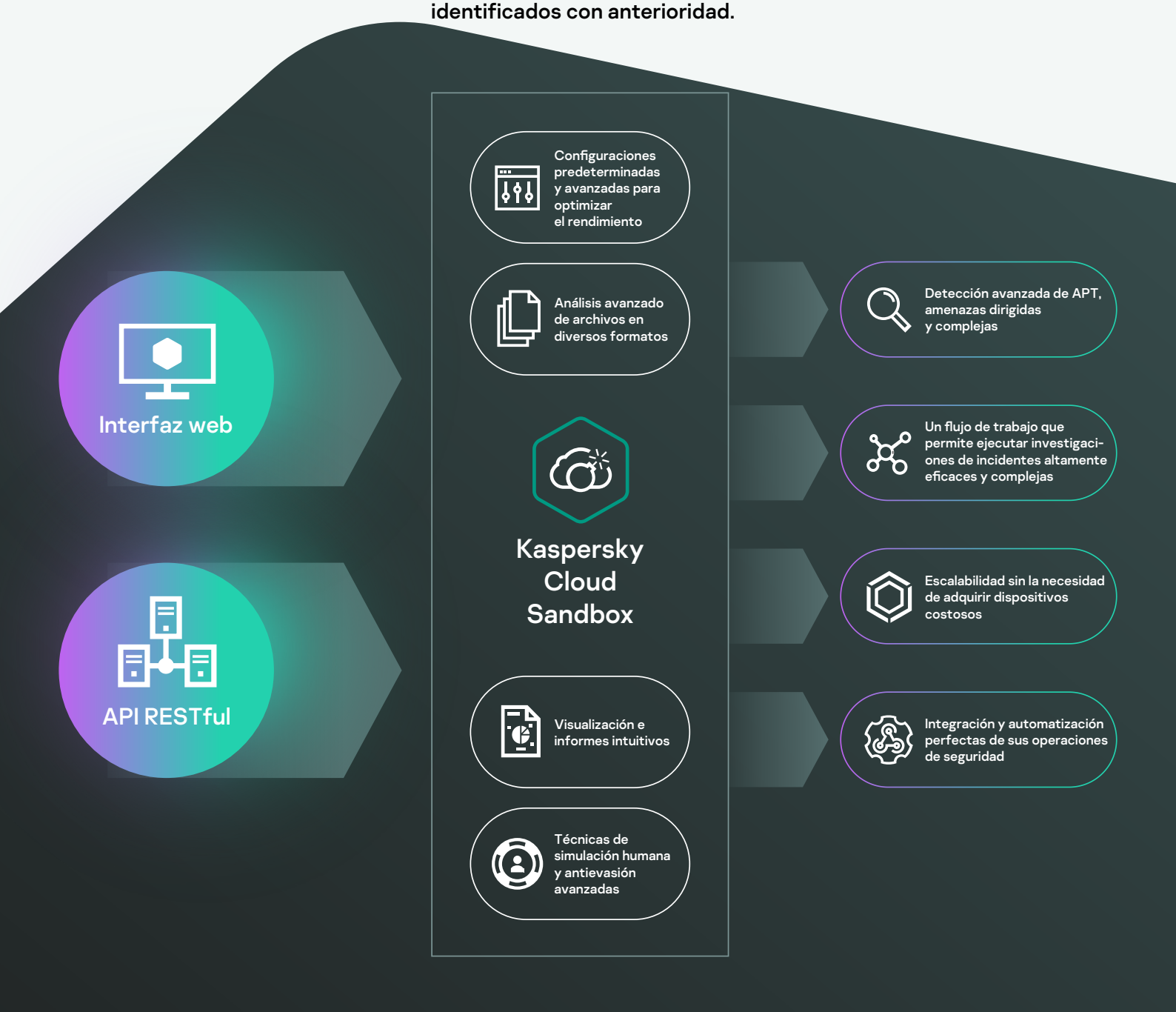
Comprobar si el objeto detectado es común o único.

Comprender por qué un objeto se debe tratar como malicioso.

Kaspersky Cloud Sandbox

Es imposible evitar los ataques dirigidos de la actualidad solo 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. Las pérdidas derivadas de incidentes de seguridad de la información siguen creciendo de forma exponencial, lo que evidencia la importancia creciente de las capacidades de detección inmediata de amenazas para garantizar una respuesta rápida y contrarrestar las amenazas antes de que se produzca un daño significativo.

Tomar una decisión inteligente basada en el comportamiento de un archivo, a la vez que se analiza la memoria del proceso, la actividad de la red, etc. es la estrategia óptima para entender las sofisticadas amenazas dirigidas y personalizadas recientes. Aunque los datos estadísticos pueden carecer de información sobre malware modificado recientemente, las tecnologías sandbox son herramientas poderosas que permiten la investigación de los orígenes de las muestras de archivos, los IOC de recopilación basados en análisis de comportamiento y la detección de objetos maliciosos no identificados con anterioridad.



Generación de informes integrales

- DLL cargados y ejecutados
- Conexiones externas con nombres de dominio y direcciones IP
- Archivos creados, modificados y eliminados
- Inteligencia detallada frente a amenazas con contexto práctico para cada indicador de compromiso (IOC) descubierto
- Volcados de memoria de procesos y volcados de tráfico de red (PCAP)
- Solicitudes y respuestas HTTP y DNS
- Extensiones mutuas creadas (mutexes)
- API RESTful
- Claves del registro creadas y modificadas
- Procesos creados por el archivo ejecutado
- Capturas de pantalla
- **y mucho más**

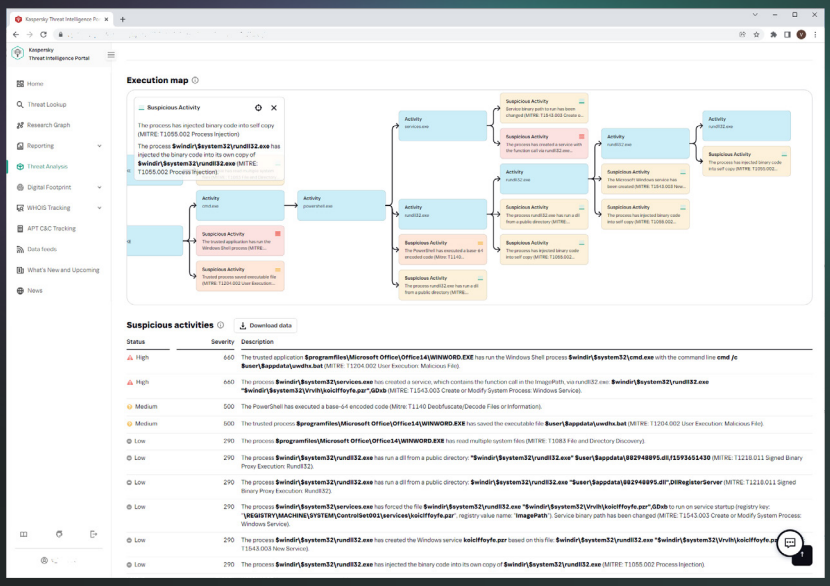
Detección y mitigación proactiva de amenazas

El malware utiliza una variedad de métodos para ocultar su ejecución a fin de que no lo detecten. Si el sistema no cumple con los parámetros requeridos, el programa malicioso se autodestruirá con toda seguridad, sin dejar rastros. Para que se ejecute el código malicioso, el entorno de sandbox debe ser capaz de imitar con precisión el comportamiento normal del usuario final.

Kaspersky Cloud Sandbox ofrece un enfoque híbrido que combina la inteligencia frente a amenazas proveniente de petabytes de datos estadísticos (gracias a Kaspersky Security Network y otros sistemas patentados), el análisis de comportamiento y una sólida antievasión con tecnologías de simulación del comportamiento humano, tales como auto clicker, desplazamiento de documentos y procesos ficticios.

Este producto se desarrolló en nuestro laboratorio interno de sandbox y evolucionó durante más de una década. La tecnología posee todo el conocimiento sobre el comportamiento de malware que adquirimos durante más de 20 años de investigación de amenazas continua. Esto nos permite detectar más de 360 000 nuevos objetos maliciosos cada día para proporcionarle al cliente soluciones de seguridad líderes en el rubro.

Como parte de nuestro Portal de inteligencia de amenazas, Cloud Sandbox es un componente importante en su flujo de trabajo de inteligencia de amenazas. Threat Lookup recupera la última inteligencia detallada de amenazas relacionada con direcciones URL, dominios, direcciones IP, hashes de archivos, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS/DNS, etc., mientras que Cloud Sandbox vincula ese conocimiento con los IOC generados por la muestra analizada.



Ahora, puede llevar a cabo investigaciones de incidentes complejas y eficaces, con lo que obtendrá una comprensión inmediata de la naturaleza de la amenaza y hará deducciones lógicas mientras realiza un análisis en profundidad con el fin de revelar los indicadores de amenazas interrelacionados.

La inspección puede consumir muchos recursos, especialmente cuando se trata de ataques de múltiples etapas. Kaspersky Cloud Research Sandbox potencia sus actividades forenses y de respuesta ante incidentes, proporcionando una escalabilidad para el procesamiento de archivos automático sin tener que adquirir dispositivos costosos ni preocuparse de los recursos del sistema.

Kaspersky APT Intelligence Reporting

Los clientes de Kaspersky APT Intelligence Reporting reciben un acceso único y continuo a nuestras investigaciones y descubrimientos, incluidos datos técnicos completos (en una variedad de formatos) sobre cada APT a medida que se descubren, así como sobre las amenazas que nunca se harán públicas. Los informes incluyen un resumen ejecutivo que ofrece información orientada al nivel C y fácil de entender, que describe la APT relacionada, y una descripción técnica detallada de la APT con los IOC y las reglas YARA relacionadas. De esta manera, se entrega a los investigadores de seguridad, analistas de malware, ingenieros de seguridad, analistas de seguridad de redes e investigadores de APT datos procesables que permiten una respuesta rápida y precisa ante la amenaza.

También, nuestros expertos lo alertarán inmediatamente sobre cualquier cambio que detecten en las tácticas de los grupos ciberdelincuentes. Además, tendrá acceso a la base de datos completa de informes de ATP, otro componente importante de investigación y análisis en sus defensas de seguridad.

Ventajas

Asignación de MITRE ATT&CK
Todos los TPP descritos 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 los TPP relevantes.

Información acerca de APT no públicas
Por diversas razones, no todas las amenazas de alto perfil se hacen públicas. Pero se comparten con todos nuestros clientes.

Acceso privilegiado
Obtención de descripciones técnicas sobre las amenazas más recientes durante investigaciones en curso, antes de que se hagan públicas.

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

Acceso a datos técnicos
Incluye una lista ampliada de IOC, disponible en formatos estándar, como openIOC o STIX y acceso a nuestras reglas YARA.

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.

Supervisión continua de campañas de APT
Acceso a inteligencia procesable durante la investigación con información sobre la distribución de ATP, IOC, comandos e infraestructuras, etc.

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

Inteligencia sobre presencia digital (Kaspersky Digital Footprint Intelligence)

A medida que su negocio 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 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 disponer de una imagen precisa de la presencia online de su organización, sino también llevar un seguimiento de sus cambios y reaccionar ante información actualizada sobre 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: capacidades para detectar y mitigar actividades internas, 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, descubrir rápidamente los posibles vectores de ataque disponibles para ellos y ajustar sus defensas en consecuencia, Kaspersky ha creado Kaspersky Digital Footprint Intelligence.

¿Cuál es la mejor manera de iniciar un ataque contra su empresa? ¿Cuál es la forma más rentable de atacarlo? ¿Qué información está disponible para los atacantes que eligieron su empresa como objetivo? ¿Su infraestructura ya está comprometida y no lo sabe?

Kaspersky Digital Footprint Intelligence responde a estas y otras preguntas, ya que nuestros expertos componen una imagen integral de su estado de ataque e identifican puntos débiles ideales para su explotación y revelan pruebas de ataques pasados, presentes e, incluso, planeados.

El producto ofrece lo siguiente:

- Inventario del perímetro de la red mediante métodos no invasivos para identificar los recursos de la red del cliente y los servicios expuestos que son un posible punto de entrada para un ataque, como interfaces de gestión que quedan accidentalmente en el perímetro o servicios mal configurados, interfaces de dispositivos, etc.
- Análisis personalizado de 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).
- Identificación, supervisión y análisis de cualquier ataque dirigido activo o que se esté planificando, campañas de APT dirigidas a su empresa, sector y región de operaciones.
- Identificación de amenazas específicamente dirigidas a sus clientes, partners y suscriptores, cuyos sistemas infectados podrían utilizarse para atacarlo.
- Supervisión discreta de sitios de pastebin, foros públicos, blogs, canales de mensajería instantánea, foros y comunidades online clandestinos y restringidos para detectar cuentas vulneradas, fugas de información o ataques contra su organización que estén en proceso de planificación y discusión.

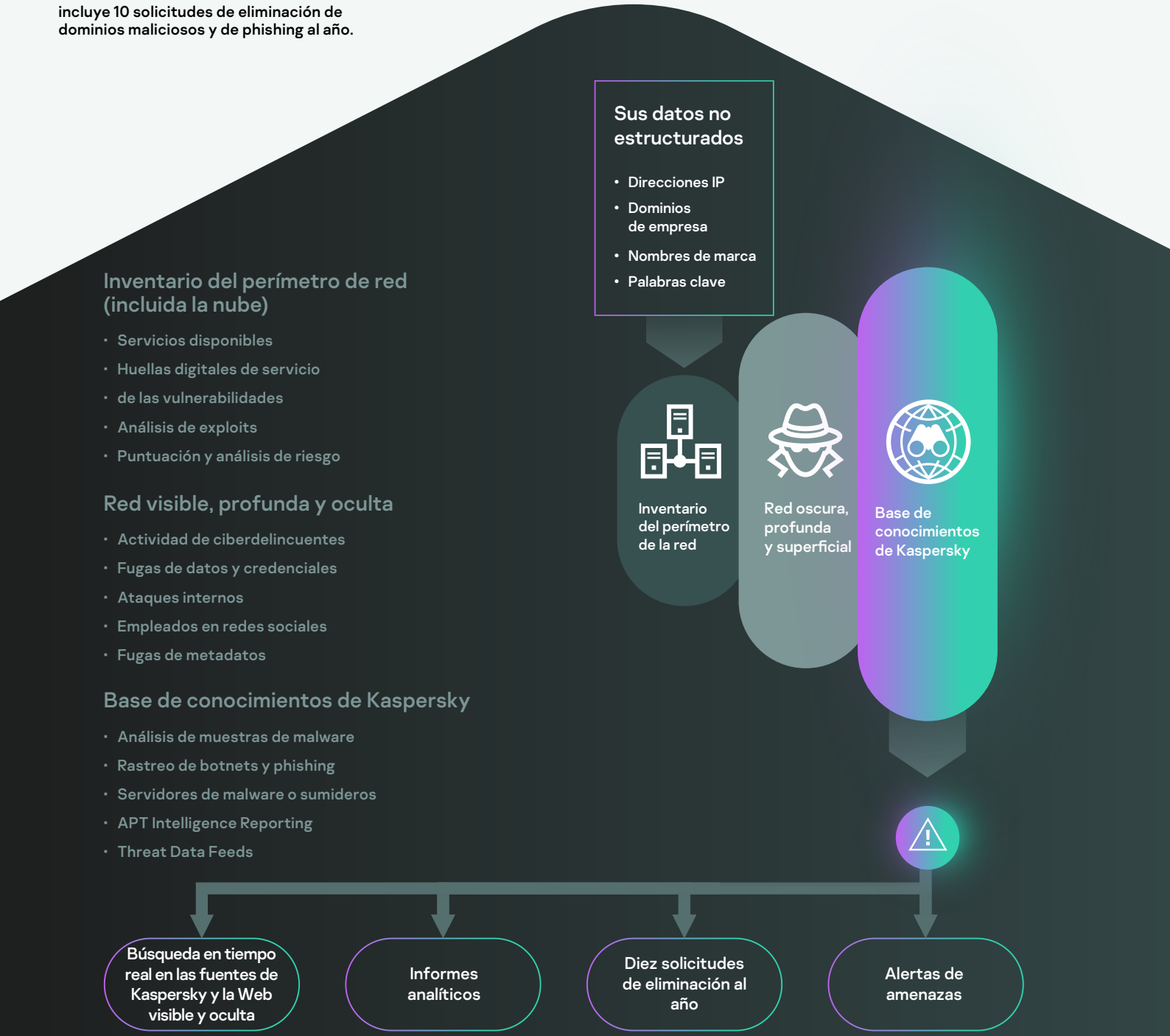
Aspectos destacados

Kaspersky Digital Footprint Intelligence utiliza técnicas de OSINT combinadas con un análisis automatizado y manual de la Web visible, profunda y oculta. También utiliza la base de conocimientos interna de Kaspersky para proporcionar información y recomendaciones útiles.

El producto está disponible en el portal Kaspersky Threat Intelligence. Puede adquirir cuatro informes trimestrales con alertas de amenaza de tiempo real anuales o adquirir un solo informe con alertas activas durante seis meses.

Búsqueda en la Web visible y oculta información casi en tiempo real sobre eventos de seguridad globales que amenazan sus activos, así como datos expuestos confidenciales en comunidades y foros clandestinos restringidos. La licencia anual incluye 50 búsquedas por día en fuentes externas y la base de conocimientos de Kaspersky.

Kaspersky Digital Footprint Intelligence crea una solución única con Kaspersky Takedown Service. La licencia anual incluye 10 solicitudes de eliminación de dominios maliciosos y de phishing al año.



Informes de inteligencia frente a amenazas de ICS de Kaspersky

Kaspersky ICS Threat Intelligence Reporting 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. Los informes se entregan a través de un portal basado en la web, lo que significa que puede comenzar a utilizar el servicio inmediatamente.

Informes que se incluyen en su suscripción

1. **Informes de APT.** Informes sobre nuevas APT y campañas de ataque de volumen elevado dirigidas a organizaciones industriales, así como actualizaciones de amenazas activas.
2. **Panorama de amenazas.** Informes sobre cambios significativos en el panorama de amenazas para los sistemas de control industrial, factores críticos recién detectados que afecten a los niveles de seguridad de ICS y exposición de ICS a amenazas, con información regional, nacional y sectorial.
3. **Vulnerabilidades encontradas.** Informes sobre vulnerabilidades identificadas por Kaspersky en los productos más populares utilizados en sistemas de control industrial, Internet industrial de las cosas e infraestructuras en diversos sectores.
4. **Análisis y mitigación de vulnerabilidades.** Nuestros asesoramientos proporcionan recomendaciones prácticas de los expertos de Kaspersky para ayudar a identificar y mitigar las vulnerabilidades en su infraestructura.

Los datos de inteligencia de amenazas le permitirán lo siguiente:

Detectar y evitar

amenazas reportadas para proteger los activos importantes, lo que incluye los componentes de software y hardware, y garantizar la seguridad y la continuidad del proceso tecnológico.

Correlacionar

cualquier actividad sospechosa y maliciosa que detecte en entornos industriales con los resultados de la investigación de Kaspersky para atribuir su detección a la campaña maliciosa en cuestión, identificar amenazas y responder rápidamente a los incidentes.

Realizar

una evaluación de la vulnerabilidad de sus activos y entornos industriales basada en análisis precisos del alcance y la gravedad de la vulnerabilidad a fin de tomar decisiones fundamentadas sobre la gestión de parches e implementar otras medidas preventivas que recomienda Kaspersky.

Aprovechar

la información sobre tecnologías, tácticas y procedimientos de ataques, vulnerabilidades recientemente descubiertas y otros cambios importantes en el panorama de amenazas para hacer lo siguiente:

- Identificar y evaluar los riesgos planteados por las amenazas notificadas y otras amenazas similares.
- Planificar y diseñar cambios en la infraestructura industrial para garantizar la seguridad de la producción y la continuidad de los procesos tecnológicos.
- Realizar actividades de concienciación sobre seguridad basadas en el análisis de casos reales para crear situaciones de formación del personal y planificar los ejercicios de "equipo rojo contra equipo azul".
- Tomar decisiones estratégicas fundamentadas para invertir en ciberseguridad y garantizar la resiliencia de sus operaciones.

Kaspersky Ask the Analyst

La constante investigación de amenazas

realizada por Kaspersky le permite descubrir, infiltrarse y hacer un seguimiento de 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.

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, y brindar consejos útiles sobre la forma más decisiva de eliminarlos.

Productos de Ask the Analyst

(Suscripción unificada por solicitud)

El servicio **Kaspersky Ask the Analyst** amplía nuestra cartera de inteligencia de amenazas, para que pueda 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, lo que le permite construir defensas resistentes contra las amenazas que atacan a su organización.

APT y crimeware

Información adicional sobre informes publicados e investigaciones en curso (además del servicio APT/Crimeware Intelligence Reporting)[1]

Análisis de malware

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

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)

Dark Web Intelligence[2]

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

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

[1] Disponible solo para clientes con APT/Crimeware Intelligence Reporting activo

[2] Ya está incluido en la suscripción de Kaspersky Digital Footprint Intelligence

Beneficios del servicio

Incremente sus conocimientos especializados

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.

Funcionamiento

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.

Use el servicio para:

- Recibir explicaciones sobre cualquiera de los detalles de los informes de inteligencia de amenazas publicados anteriormente.
- Obtener inteligencia adicional para los IoC ya proporcionados.
- Obtener detalles sobre las vulnerabilidades y recomendaciones sobre cómo protegerse si hay intentos de explotarlas
- Obtenga detalles adicionales sobre las actividades específicas de la Dark Web que sean de su interés.
- Obtener una descripción general de la familia de malware, que incluya su comportamiento, su impacto potencial y detalles sobre cualquier actividad relacionada que Kaspersky haya observado.
- 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.
- Solicite ayuda para identificar si la actividad inusual detectada está relacionada con una APT o un crimeware.
- Envíe archivos de malware para un análisis integral que permita comprender el comportamiento y la funcionalidad de las muestras proporcionadas.

Ampliar 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 aumentar sus capacidades actuales con nuestros conocimientos y recursos únicos.

Kaspersky Takedown Service

Reto

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 más. Sin embargo, la administración de la eliminación de estos dominios es un proceso complejo que requiere de experiencia y tiempo.

Solución

Kaspersky bloquea más de 15 000 URL de phishing y estafa, y evita más de un millón de intentos de ingreso a las URL a diario. 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 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 a Emergencias Informáticas (CERT) en todo el mundo.

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.

Beneficios del servicio

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.

Administración de extremo a extremo

Administraremos todo el proceso de eliminación y reduciremos su participación.

Visibilidad completa

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

Integración en Digital Footprint Intelligence

El servicio se integra en Kaspersky Digital Footprint Intelligence que entrega notificaciones en tiempo real sobre los dominios de phishing y malware, diseñados para dañar, abusar o suplantar su marca u organización. Tener una solución única es un componente importante dentro de una estrategia de ciberseguridad integral.

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.

Previene el agotamiento de los analistas y ayuda a que su fuerza de trabajo se concentre en amenazas genuinas.

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.

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.

Conclusión

Contrarrestar las ciberamenazas de hoy requiere una visión global de las tácticas y herramientas que utilizan los actores de amenazas. 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, en Kaspersky 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.

FORRESTER®

Kaspersky está posicionado como un líder en Forrester New Wave: Servicios de inteligencia de amenazas externas de 2021.

latam.kaspersky.com