Kaspersky Threat Intelligence

kaspersky PREPARADOS PARA EL FUTURO

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.

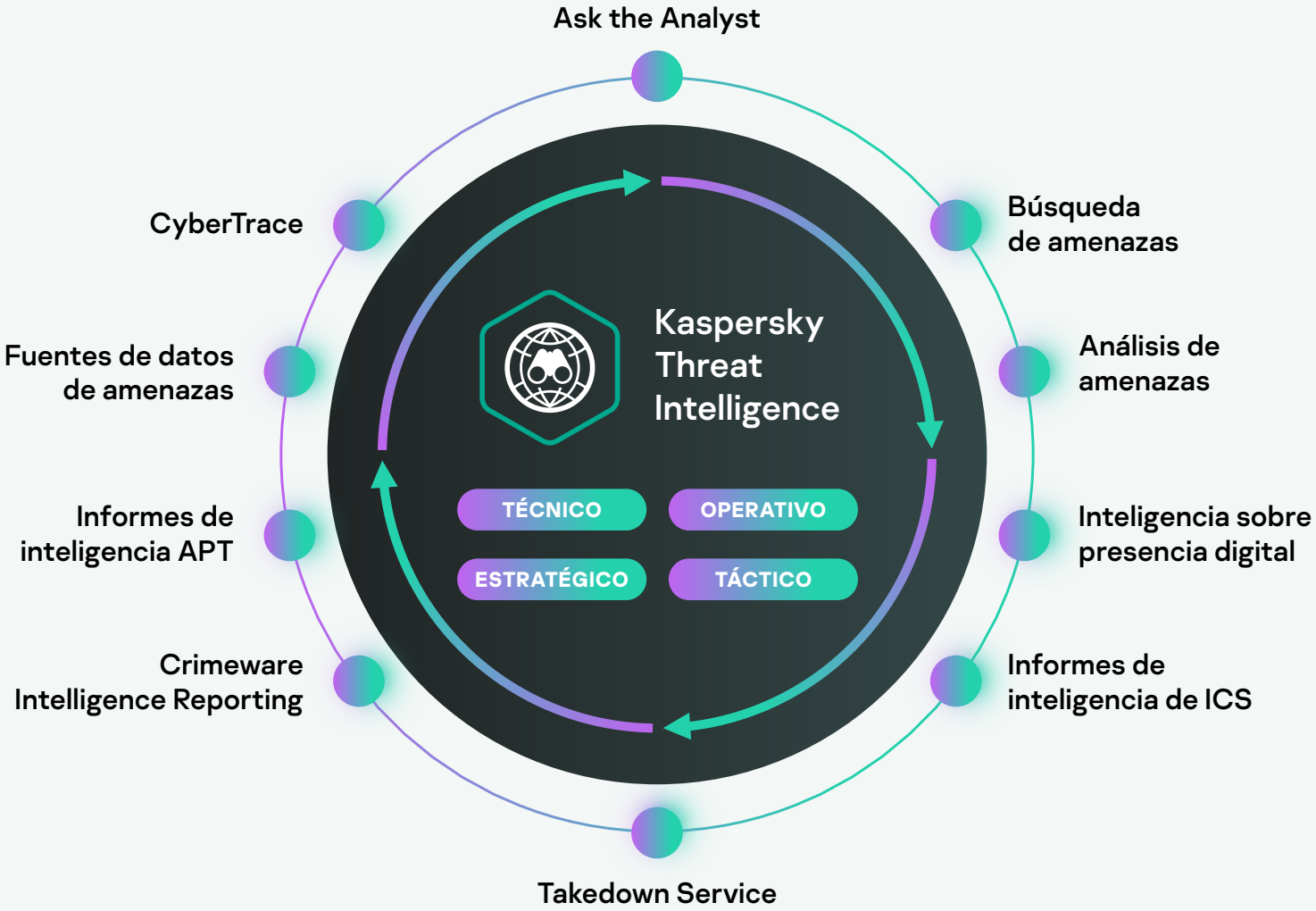
Kaspersky Threat Intelligence

Threat Intelligence de Kaspersky le proporciona acceso a la inteligencia que necesita para mitigar ciberamenazas de la mano de 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 productos de folio de Kaspersky Threat Intelligence incluye

Threat Data Feeds, CyberTrace (una plataforma de inteligencia frente a amenazas), 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 bajo demanda.



Kaspersky Threat Data Feeds

Los ciberataques ocurren diariamente. La frecuencia, la complejidad y la ofuscación de las ciberamenazas crecen de forma constante a medida que intentan comprometer 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 empresa o dañar a sus clientes. Es evidente que se necesitan nuevos métodos de protección basados en la inteligencia de amenazas.

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

Datos contextuales

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

Recopilación y procesamiento

Las fuentes de datos proceden de una fusión de fuentes heterogéneas de gran fiabilidad 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.

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 el soporte técnico de Kaspersky para permitir una integración sencilla.

Los formatos de divulgación ligeros sencillos (JSON, CSV, OpenIoC, STIX) a través de HTTPS, TAXII o mecanismos de entrega específicos permiten una integración fácil de las fuentes en las soluciones de seguridad.

Las fuentes de datos repletas de falsos positivos carecen de valor, por lo que se realizan pruebas y se les aplican filtros muy exhaustivos antes de publicarlas para garantizar una distribución de datos totalmente revisados.

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

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

Ventajas

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) en constante actualización y contexto útil, con el fin de proporcionar información sobre ciberataques y una mayor comprensión de la intención, las capacidades y los objetivos de sus adversarios. Los principales SIEM (como 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 una mayor investigación y respuesta.

Evite la exfiltración de activos y propiedad intelectual confidenciales de los equipos infectados fuera de la organización. Detecte rápidamente los activos infectados para proteger la reputación de su marca, mantener su 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

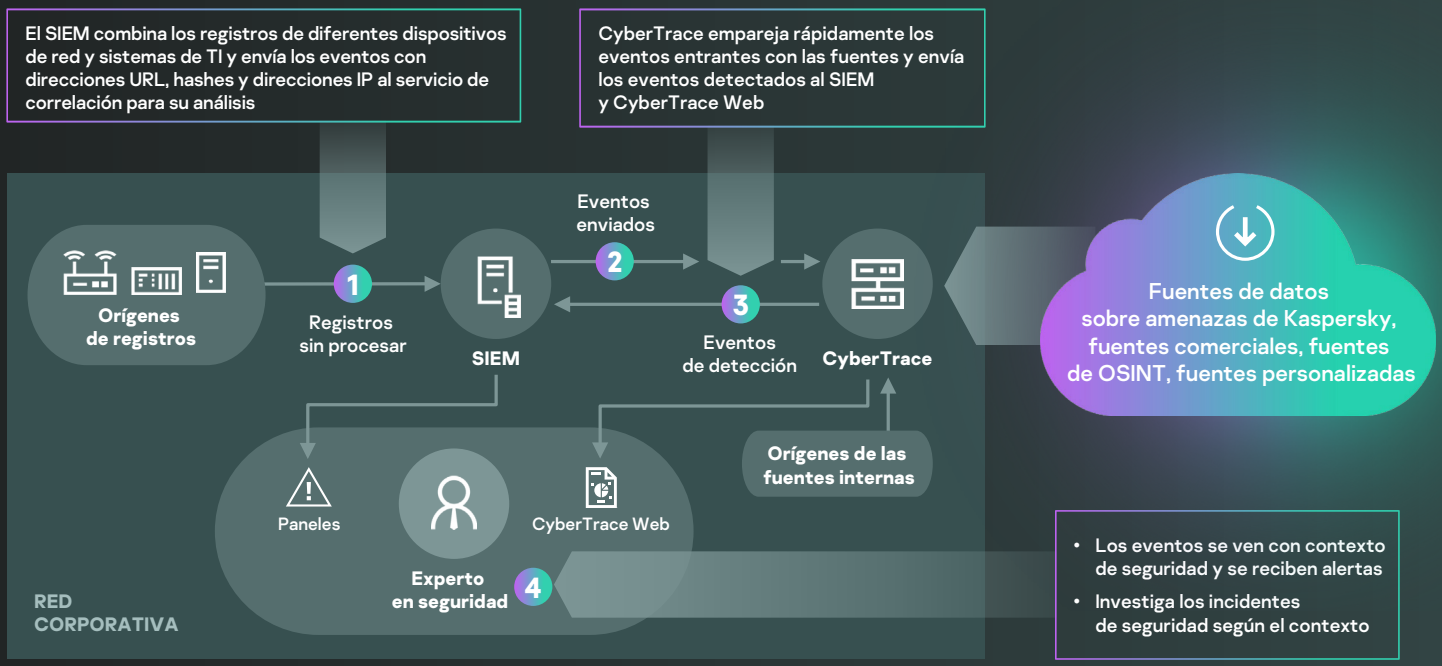
Mediante la integración de la inteligencia frente a amenazas actualizada al minuto y legible por máquinas en los controles de seguridad existentes, como los SIEM, los centros de operaciones de seguridad pueden automatizar el proceso inicial de evaluación al tiempo que ofrecen a sus especialistas de primer nivel el contexto suficiente para identificar de inmediato las alertas que se deben investigar o escalar a los equipos de respuesta ante incidentes para 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 una integración perfecta de las fuentes de datos sobre amenazas con soluciones de SIEM para ayudar a los analistas a aprovechar de manera más eficaz 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 ofrece un conjunto de instrumentos para hacer efectiva la inteligencia frente a amenazas:

- Una base de datos de indicadores con búsqueda de texto completo y la capacidad de realizar búsquedas mediante consultas de búsqueda avanzada permite realizar búsquedas complejas en todos los campos indicadores, incluidos los campos de contexto.
- Las páginas con información detallada sobre cada indicador ofrecen un análisis aún más profundo. En cada página, se presenta toda la información sobre un indicador de todos los proveedores de inteligencia frente a amenazas (desduplicación) para que los analistas puedan estudiar las amenazas en los comentarios y aportar inteligencia frente a amenazas interna acerca del indicador.
- Un gráfico de investigación permite explorar visualmente los datos y las detecciones que se almacenan en CyberTrace, así como 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 manualmente. 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 los proveedores de inteligencia frente a amenazas más valiosos.
- HTTP RestAPI le permite buscar y gestionar la inteligencia frente a 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 de la solución:



Gracias a Kaspersky CyberTrace y Kaspersky Threat Data Feeds, los analistas de seguridad podrán:

- 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, por 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 de Kaspersky sobre las ciberamenazas y sus relaciones reunidos en un único y potente 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 fiabilidad 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 proactivo 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 antes 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 frente a amenazas y fuentes externas (incluidos 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 acceso a través de una sencilla API RESTful, según las 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 ampliamente utilizados y más 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.

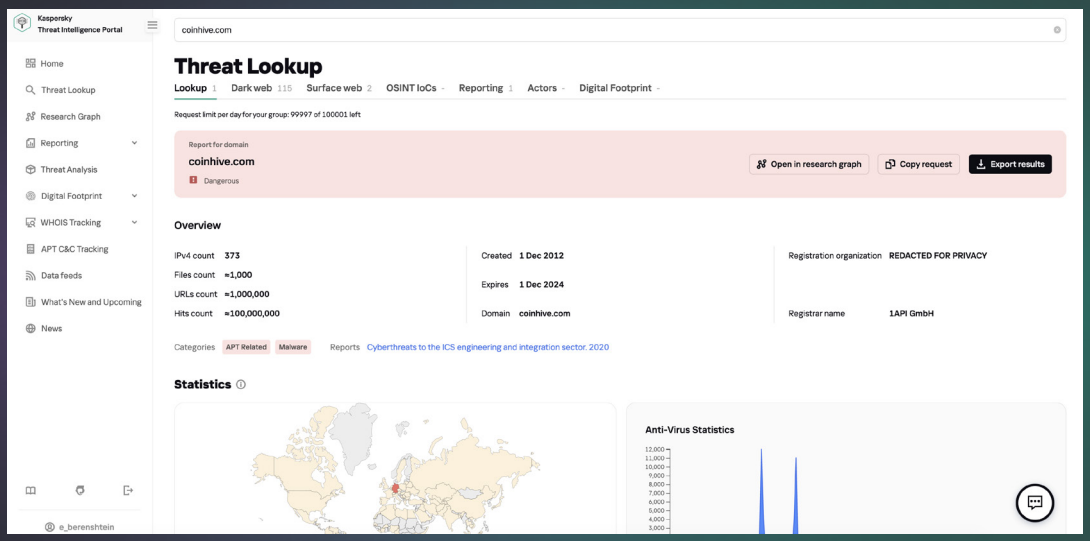
Ventajas

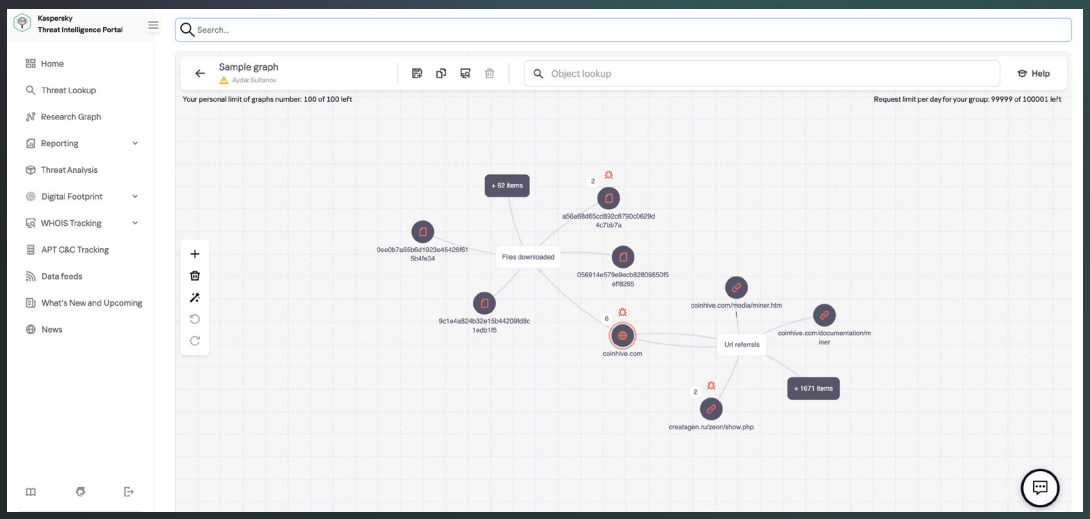
Realice búsquedas exhaustivas sobre indicadores de amenaza con un contexto de amenazas altamente validado que le permite priorizar los ataques y enfocarse en mitigar las amenazas que impliquen el mayor riesgo para su negocio.

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





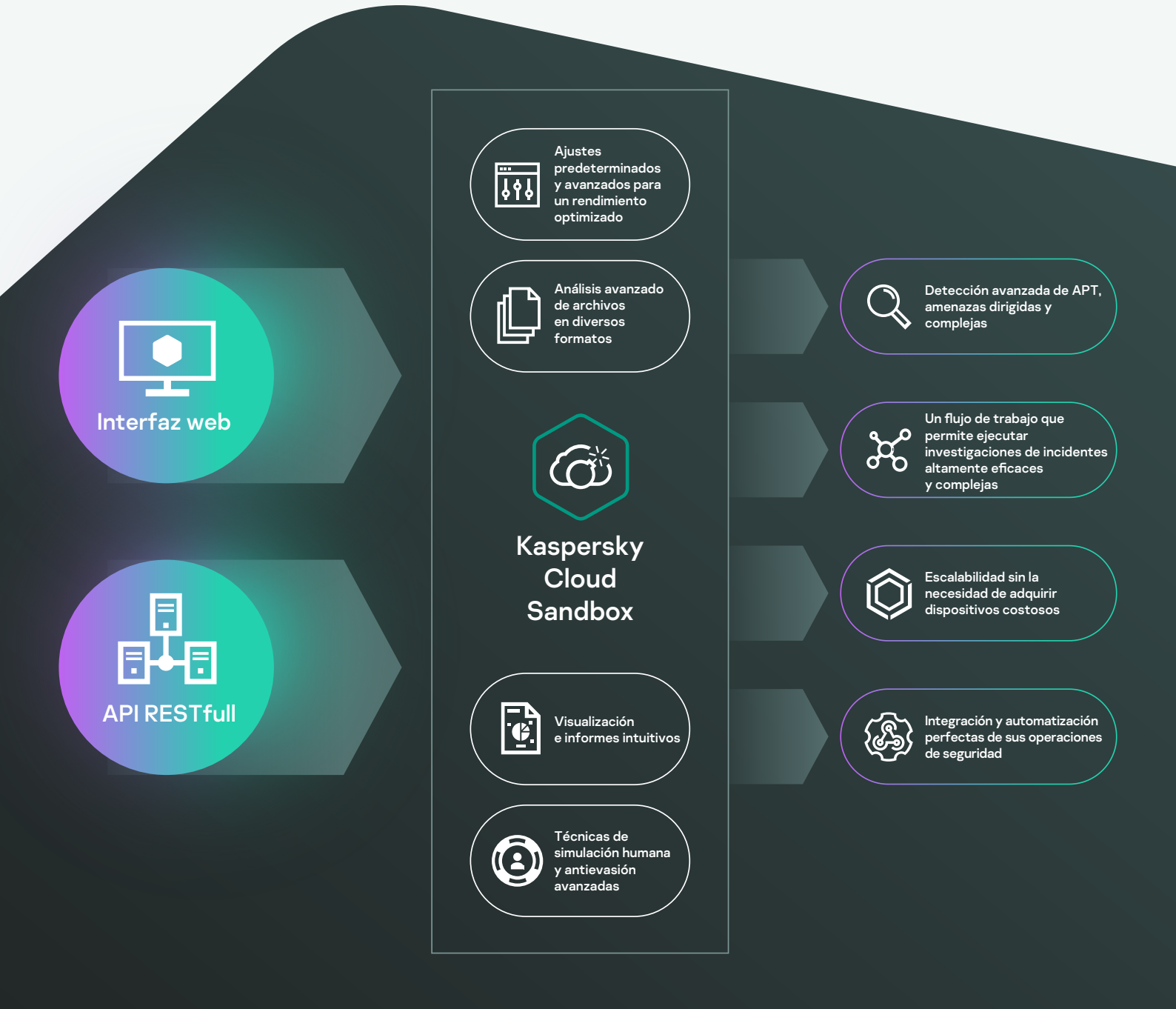
Ahora puede

- Buscar indicadores de amenaza desde una interfaz web o la API RESTful.
- Examinar datos avanzados, como certificados, nombres usados habitualmente, rutas de archivos o URL relacionadas, para 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 actuales 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 cada vez mayor 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 al tiempo 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 exhaustivos

- 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**

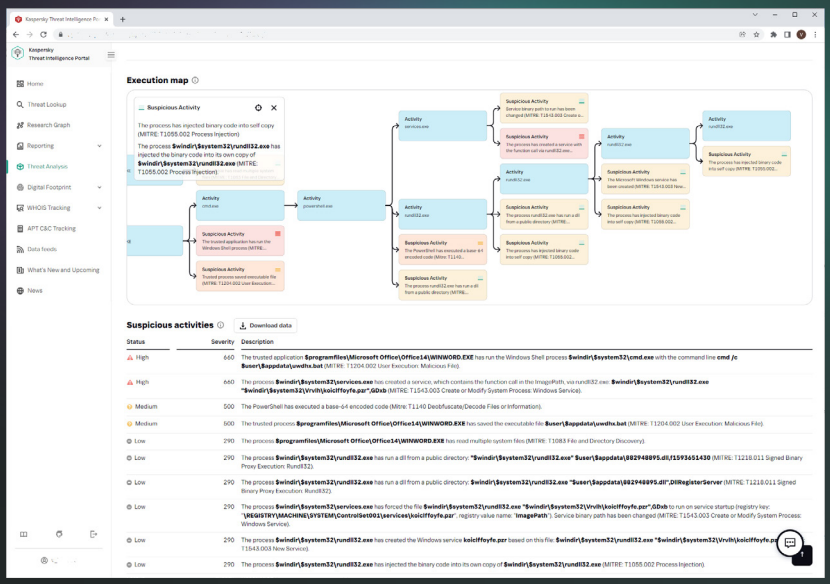
Detección y mitigación proactiva de amenazas

El malware utiliza una variedad de métodos para ocultar su ejecución y pasar desapercibido. Si el sistema no cumple con los parámetros requeridos, lo más probable es que el programa malicioso se autodestruya sin dejar rastro. 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 ha desarrollado en nuestro laboratorio interno de sandbox y ha evolucionado durante más de una década. La tecnología posee todo el conocimiento sobre el comportamiento de malware durante más de 20 años de investigación de amenazas continua. Esto nos permite detectar más de 360 000 nuevos objetos maliciosos cada día para proporcionar al cliente soluciones de seguridad líderes en el sector.

Como parte de nuestro portal de inteligencia frente a amenazas, Cloud Sandbox es el componente esencial en su flujo de trabajo de inteligencia frente a ellas. Threat Lookup recupera la inteligencia detallada de amenazas más reciente 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, por 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 por los recursos del sistema.

Informes de inteligencia de APT de Kaspersky

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 contienen un resumen ejecutivo que ofrece información orientada al nivel C y fácil de entender, y que describe la APT relacionada, junto con una descripción técnica detallada de la APT con los IOC y las reglas YARA relacionadas para entregar a los investigadores de seguridad, analistas de malware, ingenieros de seguridad, analistas de seguridad de redes e investigadores de APT datos procesables que permitan una respuesta rápida y precisa ante la amenaza.

Nuestros expertos también le notificarán inmediatamente sobre cualquier cambio que detecten en las tácticas de los grupos cibercriminales. Además, tendrá acceso a la base de datos completa de informes de ATP, otro componente de investigación y análisis importante en sus defensas de seguridad.

Ventajas

MITRE ATT&CK
Todos los TPP descritos en los informes se 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 sí que 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 todo el periodo 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 actores de amenazas
Incluye el posible país de origen y la actividad principal, las familias de malware utilizadas, los sectores y las geografías objetivo, así como 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, los IOC, los comandos y las infraestructuras, etc.

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

Kaspersky Digital Footprint Intelligence

A medida que su empresa 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 entornos 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.

Las organizaciones utilizan una amplia gama de herramientas en sus operaciones de seguridad, pero sigue habiendo amenazas digitales al acecho: capacidades para detectar y mitigar actividades internas, planes y esquemas de ataque de cibercriminales 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 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 atacarle? ¿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 exhaustiva 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:

- 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 las 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 atacarle.
- Supervisión discreta de sitios de pastebin, foros públicos, blogs, canales de mensajería instantánea, foros y comunidades online clandestinos y restringidos para detectar cuentas vulneradas, filtraciones de información o ataques contra su organización que estén en proceso de planificación y discusión.

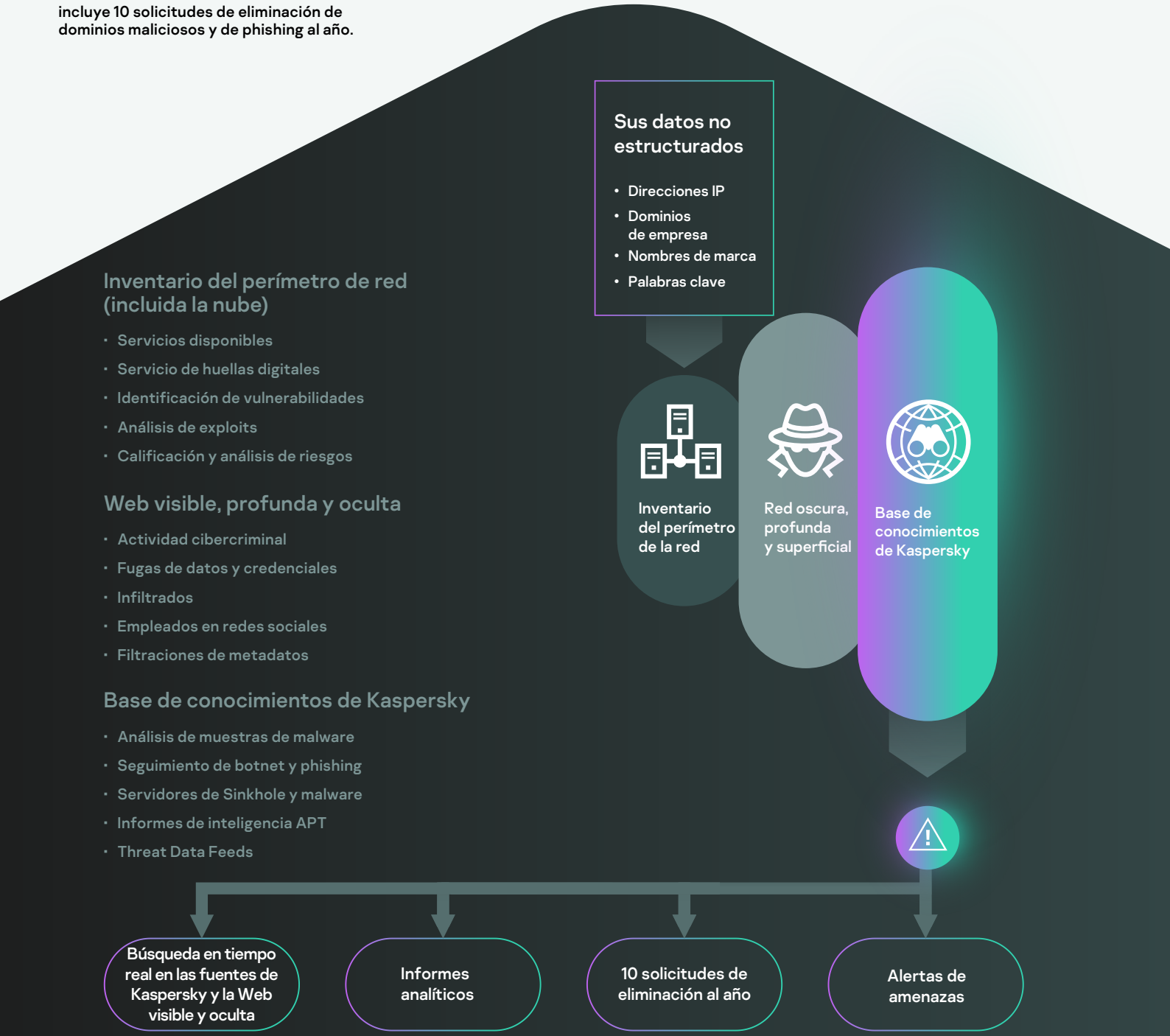
Aspectos destacados

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

El producto está disponible en el portal Kapersky 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.

Busque en la Web visible y oculta información casi en tiempo real sobre eventos de seguridad globales que amenazan a sus activos, así como datos expuestos sensibles 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. **El 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.

Lo que los datos de inteligencia de amenazas le permitirán

Detectar y evitar

amenazas informadas para proteger los activos importantes, como 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 las vulnerabilidades de sus activos y entornos industriales basada en análisis precisos de su alcance y gravedad para tomar decisiones fundamentadas sobre la gestión de parches e implementar otras medidas preventivas que recomiende Kaspersky.

Aprovechar

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

- 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 investigación continua de amenazas

permite que Kaspersky descubra, se infiltre y supervise las comunidades cerradas y los foros de la web oscura de todo el mundo que frecuentan los adversarios y ciberdelincuentes. 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. Actualmente, la situación volátil de las amenazas está en rápido crecimiento y presenta técnicas de ciberdelincuencia cada vez más ágiles. Las organizaciones se enfrentan a incidentes complejos provocados por ataques no relacionados con el malware, ataques sin archivos, ataques living-off-the-land, vulnerabilidades de día cero y combinaciones de todos estos ataques integrados en amenazas complejas, similares a APT y ataques dirigidos.

En una época donde los ciberataques perjudican a las 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 combatan solos la guerra contra las amenazas sofisticadas: **es importante que puedan obtener ayuda de expertos externos.** La experiencia externa puede aclarar la posible trayectoria de los ataques complejos y APT, y dar consejos útiles sobre la forma más decisiva de eliminarlos.

Productos de Ask the Analyst

(Suscripción unificada basada en solicitudes)

El servicio **Kaspersky Ask the Analyst** amplía nuestra cartera de inteligencia de amenazas, lo que le permite solicitar asesoramiento e información sobre amenazas específicas a las que se enfrenta o que le interesan. El servicio adapta las potentes capacidades de inteligencia e investigación de amenazas de Kaspersky a sus necesidades específicas, lo que le permite construir unas defensas resistentes contra las amenazas dirigidas 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 corrección

Descripciones de amenazas, vulnerabilidades e IoC relacionados

- Descripción general de una familia específica de malware
- Contexto adicional para las amenazas (hashes relacionados, URLs, CnCs, etc.)
- Información sobre una vulnerabilidad específica (su nivel de estado crítico y los mecanismos de protección correspondientes en los productos de Kaspersky)

Inteligencia de la web oscura[2]

- Investigación de la web oscura en 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 de una región/sector
- 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

Aumente su experiencia

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

Acelere las investigaciones

Analice y priorice los incidentes con eficacia sobre la base de información contextual personalizada y detallada.

Responda con rapidez

Responda rápidamente a las amenazas y vulnerabilidades gracias a nuestra asistencia para bloquear los 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 de asistencia a los clientes corporativos. Le responderemos por correo electrónico, pero si lo desea, podemos organizar una videoconferencia o una sesión de pantalla compartida. Una vez aceptada su solicitud, se le informará del plazo estimado para procesarla.

Casos de uso del servicio:

- Aclare cualquier detalle de los informes de inteligencia de amenazas publicados anteriormente.
- Obtenga inteligencia adicional para los IoC ya proporcionados.
- Obtenga detalles sobre las vulnerabilidades y recomendaciones sobre cómo protegerse contra la explotación.
- Obtenga información adicional sobre actividades específicas de la web oscura que sean de su interés.
- Obtenga un informe general de la familia de malware que incluya su comportamiento, su impacto potencial y detalles sobre cualquier actividad relacionada que Kaspersky haya observado.
- Priorice las alertas o incidentes de forma eficaz con información contextual detallada y la categorización de los IoC relacionados proporcionados mediante 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.

Amplíe sus conocimientos y recursos

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

Kaspersky Takedown Service

Reto

Los cibercriminales crean dominios maliciosos y de phishing que se utilizan para atacar su empresa y sus marcas. La incapacidad de mitigar rápidamente estas amenazas una vez identificadas puede conducir a una pérdida de ingresos, daños a la marca, pérdida de la confianza del cliente, filtración de datos y mucho más. Pero la gestión 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 acceso a las 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 la gestión de eliminación y permitiremos 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 ante emergencias informáticas (CERT) de 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/regional respectiva (CERT, registro, etc.) que posea los derechos legales necesarios para desactivar los dominios. Recibirá notificaciones en cada etapa del proceso hasta que se elimine el recurso deseado.

Protección sencilla

Kaspersky Takedown Service mitiga rápidamente las amenazas planteadas por los dominios maliciosos y de phishing antes de que causen algún daño a su marca y empresa. La gestión integral del proceso completo le 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.

Gestión integral

Gestionaremos todo el proceso de eliminación para minimizar su participación.

Visibilidad completa

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

Integración con Digital Footprint Intelligence

El servicio se integra con 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. Una solución única es un componente importante de una estrategia de ciberseguridad integral.

Principales ventajas

- 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 personal se concentre en las amenazas genuinas.
- El conocimiento único de las tácticas, las técnicas y los procedimientos que utilizan los actores en diferentes sectores 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 le ayudan a reducir el tiempo de espera contra ataques y a minimizar en gran medida los posibles daños.

Conclusión

Contrarrestar las ciberamenazas de hoy requiere una visión global de las tácticas y herramientas que utilizan los actores de amenazas. La generación de esta inteligencia y la identificación de las contramedidas más eficaces requieren una dedicación constante y altos niveles de experiencia. Con los petabytes de datos de amenazas que se pueden extraer, las 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 frente a amenazas más reciente del mundo y los ayudamos a mantener su inmunidad incluso ante ciberataques desconocidos.

FORRESTER®

Kaspersky se posiciona como un líder en Forrester Wave: Servicios externos de inteligencia contra amenazas, 2021

www.kaspersky.es

© 2022 AO Kaspersky Lab.
Las marcas comerciales y de servicios registradas pertenecen a sus respectivos propietarios.