Plataforma de inteligencia
frente a amenazas

Kaspersky CyberTrace

kaspersky preparados para el futuro

Kaspersky CyberTrace

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 sus flujos de trabajo de operaciones de seguridad existentes.

Facilitación del análisis y de la evaluación eficaz de las alertas

El número de alertas que procesan los analistas de ciberseguridad está aumentando de forma exponencial. Con esta cantidad de datos analizados, la priorización eficaz de las alertas, la clasificación y la validación es casi imposible.

Se reciben demasiados avisos provenientes de numerosos productos de seguridad, lo que silencia las alertas importantes y provoca el agotamiento de los analistas. Los sistemas SIEM y otras herramientas de análisis de seguridad comparan eventos y permiten reducir el número de alertas, aunque el trabajo de los analistas de seguridad sigue estando sobrecargado.

Sistemas SIEM

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 profesionales de la seguridad pueden automatizar el proceso inicial de evaluación y reciben 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.

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 incluye 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.

Integraciones

Kaspersky CyberTrace puede integrarse con cualquier fuente de datos sobre inteligencia de amenazas en formatos JSON, STIX, XML y CSV:

1. Fuentes de datos sobre inteligencia de amenazas de Kaspersky
2. Fuentes de datos de otros proveedores
3. OSINT o fuentes personalizadas

Para comodidad de los clientes, CyberTrace permite la integración inmediata con numerosas soluciones SIEM y orígenes de registros.

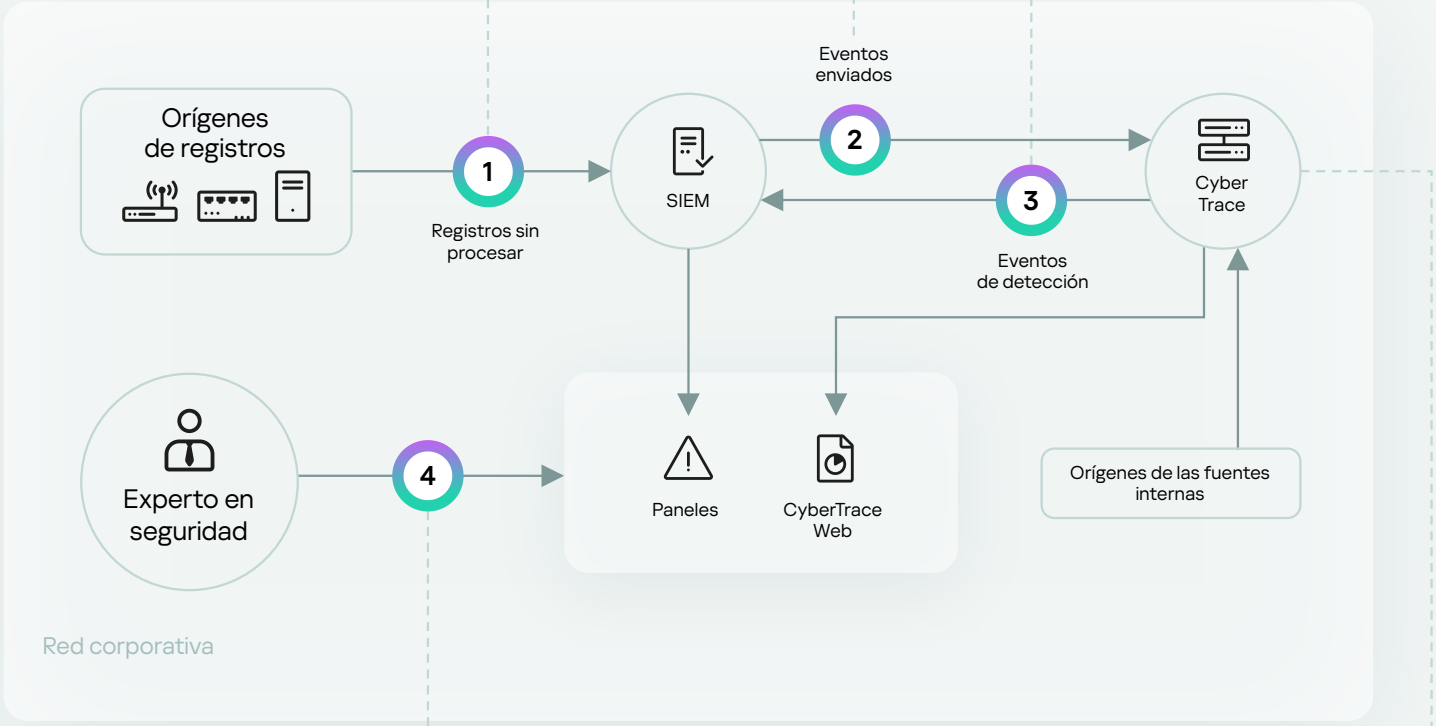
Esquema de integración de Kaspersky CyberTrace

Kaspersky CyberTrace es capaz de aumentar las funcionalidades de SIEM con una capa adicional de análisis y correlación de datos entrantes, lo que reduce en gran medida la carga de trabajo sobre SIEM. Comparar eventos con fuentes de datos permite identificar amenazas y proporcionar un contexto valioso sobre los incidentes detectados. En la siguiente figura, se muestra una arquitectura general de la integración de la solución.

SIEM añade registros de eventos provenientes de diferentes sistemas informáticos y dispositivos de red

Registros con direcciones URL, hashes y direcciones IP se envían a CyberTrace para más análisis

CyberTrace empareja rápidamente los eventos entrantes con las fuentes y envía los eventos detectados al SIEM y CyberTrace Web



- Los eventos se ven con contexto de seguridad y se reciben alertas
- Investiga los incidentes de seguridad según el contexto

Fuentes de datos sobre amenazas de Kaspersky, fuentes comerciales, fuentes de OSINT, fuentes personalizadas

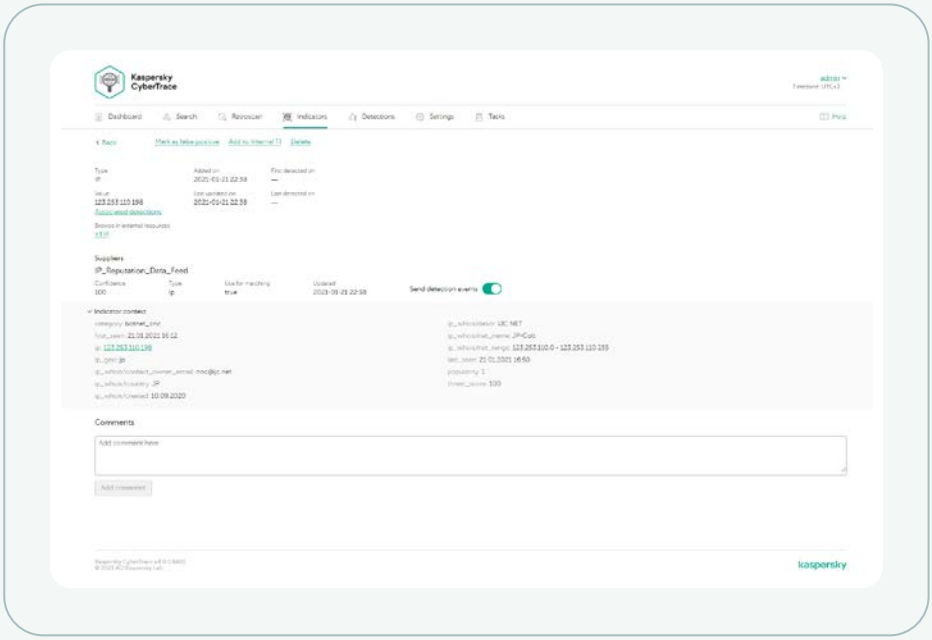
Características del producto

Kaspersky CyberTrace ofrece un conjunto de instrumentos para utilizar la inteligencia frente a amenazas con el fin de realizar una evaluación de alertas eficaz y brindar una correcta respuesta inicial:

Información detallada sobre un indicador de todos los proveedores de inteligencia frente a amenazas

Una base de datos de indicadores con búsqueda de texto completo y la capacidad de buscar mediante consultas avanzadas permite búsquedas complejas en todos los campos de indicadores, como los campos de contexto. Filtrar los resultados por proveedor de inteligencia simplifica el proceso de análisis de inteligencia frente a amenazas.

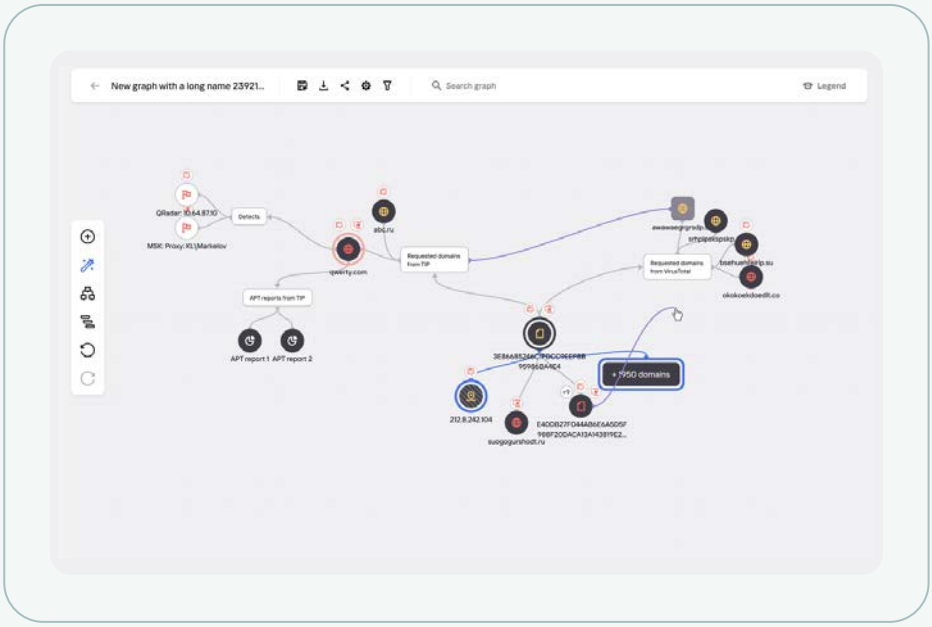
Las suscripciones por correo electrónico y los documentos PDF de los Equipos de Respuesta de Emergencias Informáticas (CERT) nacional/gubernamental/financiero, los proveedores de TI y las comunidades se pueden utilizar como fuente de IoC para CyberTrace. La extracción de IOC es posible tanto desde el cuerpo como de los documentos adjuntos del correo electrónico (XML, CSV, JSON, PDF). Los servidores IMAP/POP3 y las carpetas locales/compartidas con un conjunto de archivos PDF se pueden usar como orígenes de fuentes.



Las páginas con información detallada sobre cada indicador proporcionan un análisis aún más acabado. Cada página presenta toda la información sobre un indicador de todos los proveedores de inteligencia frente a amenazas (desduplicación) para que los analistas puedan evaluar las amenazas en los comentarios y añadir inteligencia interna sobre el indicador. Si este fue detectado, la información sobre las fechas de detección y los enlaces a la lista de detecciones estará disponible.

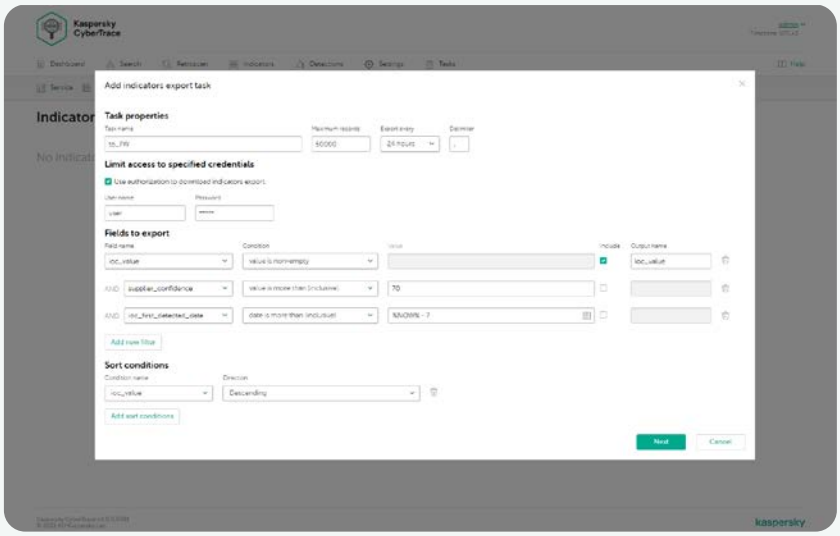
Gráfico de investigación

Un gráfico de investigación permite explorar visualmente datos y detecciones almacenados en CyberTrace y descubrir características de las amenazas. Permite la visualización gráfica de la relación entre URL, dominios, IP, archivos y otros contextos encontrados durante las investigaciones. El gráfico incluye las siguientes características: transformaciones, minigráficos, nodos de agrupamiento, adición manual de enlaces, adición de indicadores y búsqueda de nodos en el gráfico. Es compatible con un enriquecimiento de IoC en un gráfico de investigación de VirusTotal.



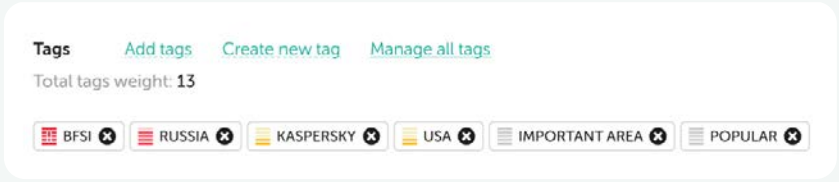
Tarea de exportación de indicadores

La función de exportación de indicadores admite la integración nativa de IoC exportados con controles de seguridad de terceros, como las listas de política (listas de bloqueo) así como el uso compartido de datos de amenazas entre instancias de Kaspersky CyberTrace o con otras plataformas de TI.



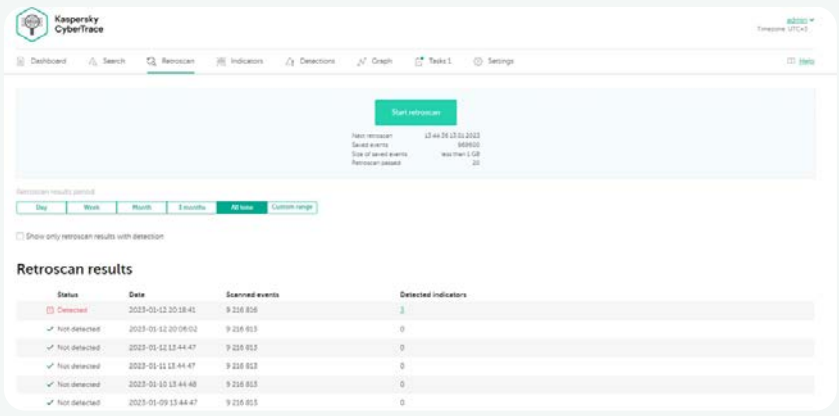
Etiquetas de IoC

El etiquetado de IoC simplifica su administración. Puedes crear cualquier etiqueta y especificar tu peso (importancia) y usarla para etiquetar IoC manualmente. También puede ordenar y filtrar IoC de acuerdo con estas etiquetas y sus pesos.



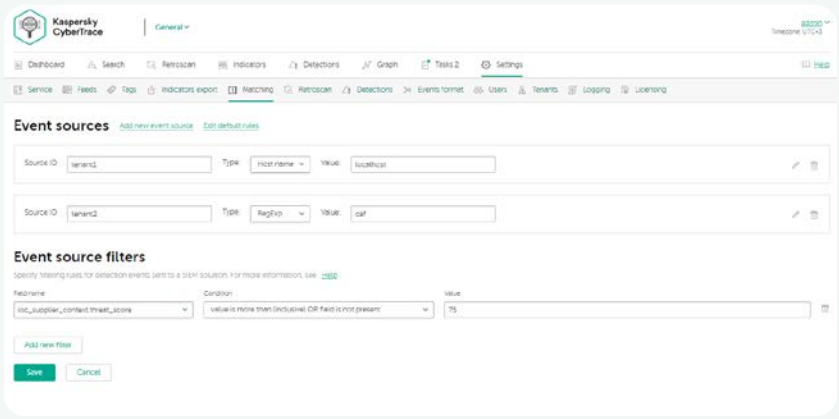
Función retroscan

La función de correlación histórica (retroscan) le permite analizar los elementos observables de eventos previamente comprobados utilizando las fuentes más recientes para encontrar amenazas no detectadas anteriormente. Todas las detecciones históricas están incluidas en el informe para investigaciones futuras.



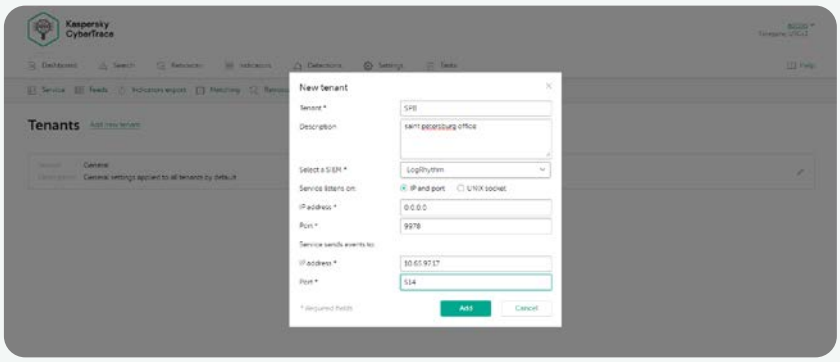
Filtros para orígenes de datos

Un filtro para enviar los eventos de detección al SIEM reduce su sobrecarga y la del analista que se enfrenta a la fatiga de alertas. Le permite enviar al SIEM solo las detecciones más peligrosas, es decir, las que se deben tratar como incidentes. El resto de las detecciones se guardan en la base de datos interna y se pueden utilizar durante los análisis de causas raíz o en la búsqueda de amenazas.



Capacidad multiempresa

Capacidad multiempresa admite MSSP o casos de uso de grandes empresas cuando un proveedor de servicios (oficina central) necesita gestionar eventos de distintas sucursales (usuarios) por separado. Esto permite a una única instancia de Kaspersky CyberTrace conectarse con diferentes soluciones SIEM de distintos usuarios, y puede configurar qué fuentes utilizará cada uno.



Estadísticas de indicadores y matriz de intersección de fuentes

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

HTTP RestAPI te permite buscar y gestionar la inteligencia frente a amenazas

Al usar Rest API, Kaspersky CyberTrace puede integrarse fácilmente con entornos complejos para realizar tareas de automatización y orquestación. Además, también se admite la integración con la plataforma de supervisión, análisis y respuesta de Kaspersky.

Otras características del producto

- Conectores del SIEM para una amplia gama de soluciones de SIEM a fin de visualizar y administrar datos sobre detecciones de amenazas
- Búsqueda de indicadores a pedido (hashes, direcciones IP, dominios y direcciones URL) para una investigación a fondo de las amenazas
- Filtrado avanzado de las fuentes
- Análisis masivo de registros y archivos
- Interfaz de línea de comandos para plataformas Windows y Linux
- Modo independiente, en el que Kaspersky CyberTrace recibe y analiza los registros de diversos orígenes, como los dispositivos de red
- Y mucho más

Si bien Kaspersky CyberTrace y Kaspersky Threat Data Feeds se pueden utilizar por separado, cuando se usan juntos, fortalecen significativamente sus capacidades de detección de amenazas, brindando a sus operaciones de seguridad una visibilidad global de las ciberamenazas.

Con Kaspersky CyberTrace y Kaspersky Threat Data Feeds, las organizaciones pueden:

Sintetizar y priorizar eficazmente las alertas de seguridad.

Reducir la carga de trabajo de los analistas y evitar sobrecargas.

Identificar de inmediato las alertas críticas y tomar decisiones más fundamentadas sobre cuáles se deben escalar a los equipos de respuesta ante incidentes.

Formar una defensa proactiva e inteligente

Kaspersky CyberTrace

Más información

www.kaspersky.es

#kaspersky
#bringonthefuture