kaspersky BRING ON THE FUTURE

Kaspersky CyberTrace

La cantidad de alertas de seguridad que procesan los analistas de seguridad de la información crece exponencialmente cada día. Con esta cantidad de datos analizados, se vuelve casi imposible priorizar, clasificar y validar las alertas. Se reciben demasiados avisos provenientes de numerosos productos de seguridad, lo que silencia las alertas importantes y provoca el agotamiento de los analistas. Los SIEM y las herramientas de gestión de registros y de análisis de seguridad que recopilan datos de seguridad y correlacionan las alarmas correspondientes ayudan a reducir la cantidad de alertas que requieren de un examen adicional, sin embargo, los especialistas de primer nivel siguen extremadamente sobrecargados.

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.

Facilitamos el eficaz análisis y evaluación de las alertas

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 y, al mismo tiempo, ofrecer a sus especialistas de primer nivel suficiente contexto para identificar de inmediato las alertas que se deben investigar o escalar a los equipos de Respuesta a Incidentes (IR) 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 herramienta de análisis y fusión de inteligencia frente a amenazas que facilita una integración perfecta de las fuentes de datos sobre amenazas con las 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 con cualquier fuente de inteligencia frente a amenazas que desee utilizar (fuentes de inteligencia de amenazas de Kaspersky, otros proveedores, inteligencia de código abierto [OSINT] o sus fuentes personalizadas) en formatos JSON, STIX, XML y CSV, y admite la integración inmediata con numerosos orígenes de registros y soluciones de SIEM.

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 la siguiente figura se muestra una arquitectura general de la integración de la solución:

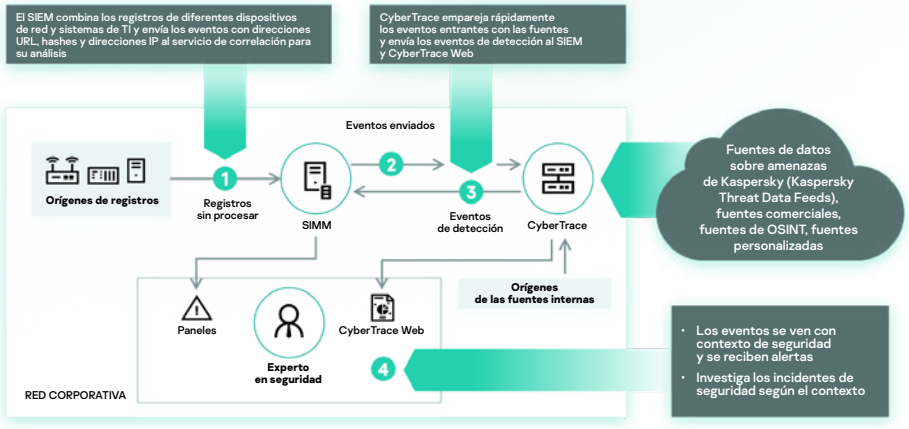


Figura 1. Esquema de integración de Kaspersky CyberTrace

Funciones 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:

- 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. Filtrar los resultados por proveedor de inteligencia simplifica el proceso de análisis de la inteligencia de amenazas.
- Las páginas con información detallada sobre cada indicador ofrecen un análisis aún más acabado. En cada página, se presenta toda 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. Si el indicador se detectó, la información sobre las fechas de detección y los vínculos a la lista de detecciones estarán disponibles.

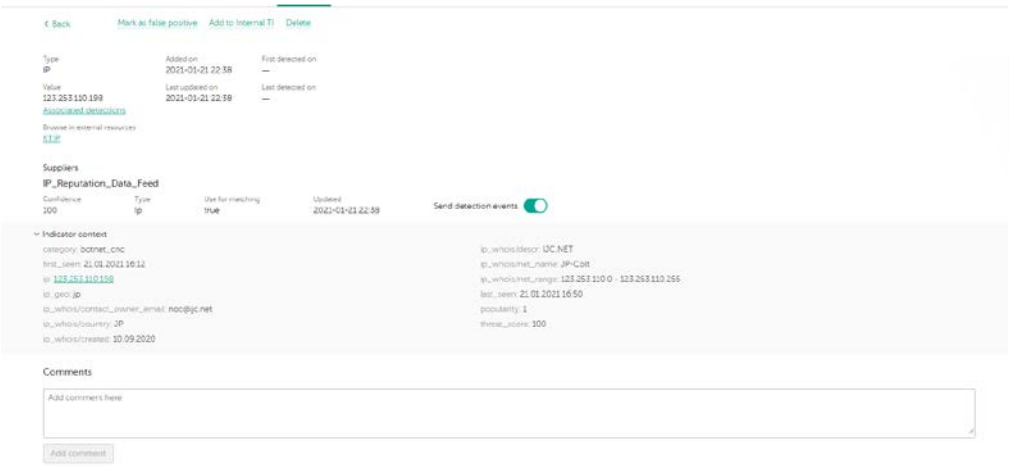


Figura 2. Información detallada sobre un indicador de todos los proveedores de inteligencia de amenazas

- 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. Permite visualizar gráficamente la relación entre direcciones URL, dominios, direcciones IP, archivos y otros contextos que se encuentran 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.

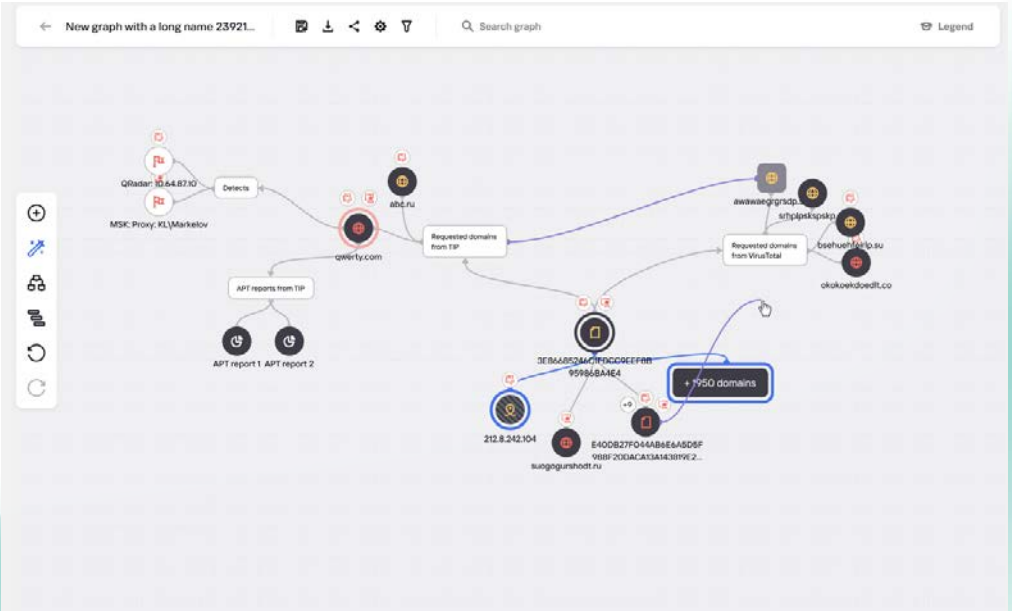


Figura 3. Gráfico de investigación

- 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 otras plataformas TI.

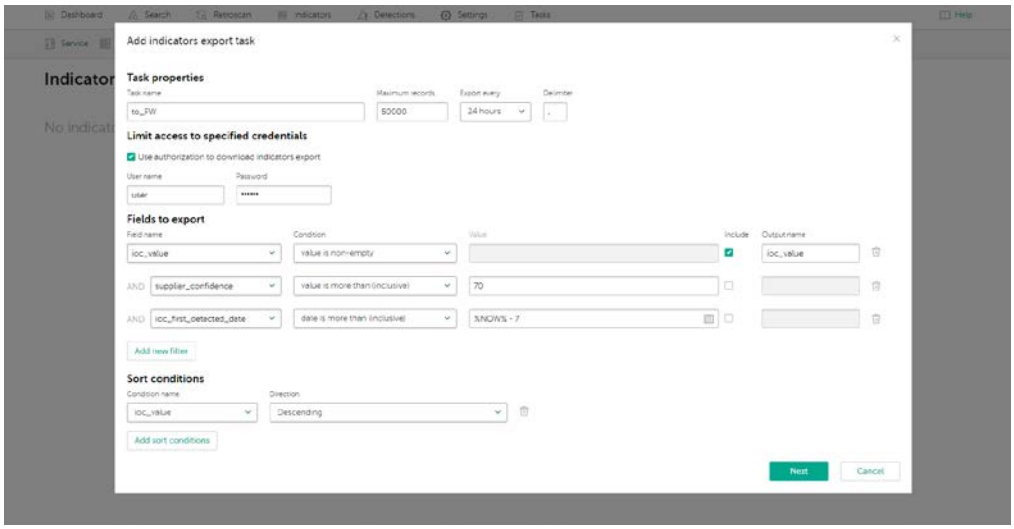


Figura 4. Tarea de exportación de indicadores

- 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 sus pesos.

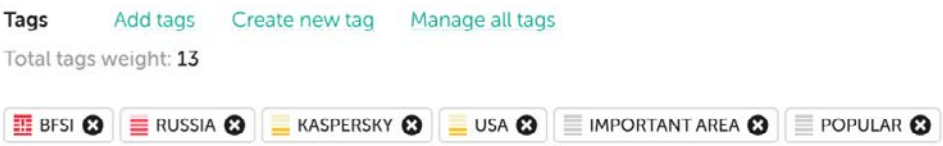


Figura 5. Etiquetas de IOC

- La función de correlación histórica (retroscan) le permite analizar objetos de eventos revisados anteriormente mediante las las entradas más recientes para encontrar amenazas no detectadas anteriormente. Todas las detecciones históricas se incluyen en el informe para futuras investigaciones.
- Un filtro para enviar eventos de detección a las soluciones SIEM permite reducir la carga sobre estas y sobre los analistas abrumados por la cantidad de alertas. Le permite enviar solamente las detecciones más peligrosas a SIEM, aquellas que deben tratarse como incidentes. Todas las demás detecciones se guardan en la base de datos interna y se pueden utilizar durante el análisis de causa raíz o en la búsqueda de amenazas.
- La tenencia múltiple admite los MSSP o los casos de uso de grandes empresas cuando un proveedor de servicios (oficina central) debe manejar eventos de diferentes sucursales (empresas) por separado. Esto permite que una sola instancia de Kaspersky CyberTrace se conecte a diferentes soluciones SIEM de distintas empresas; además, puede configurar qué fuentes se utilizarán para cada una.

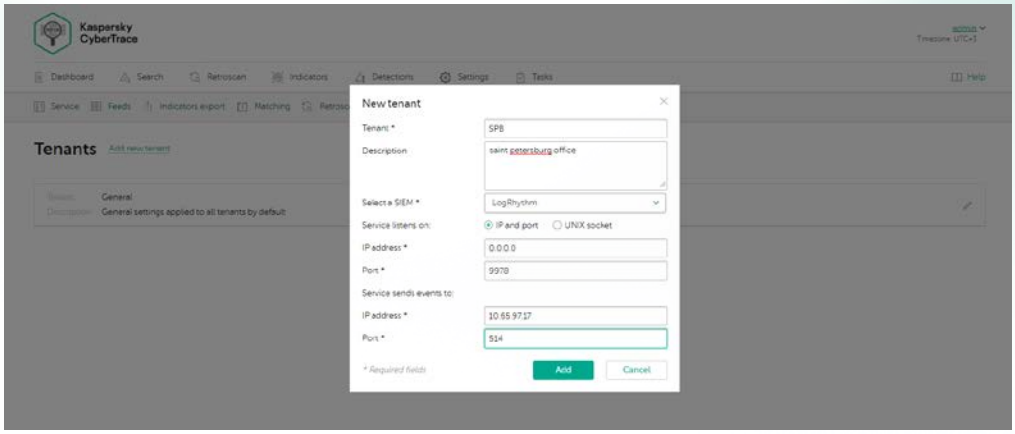
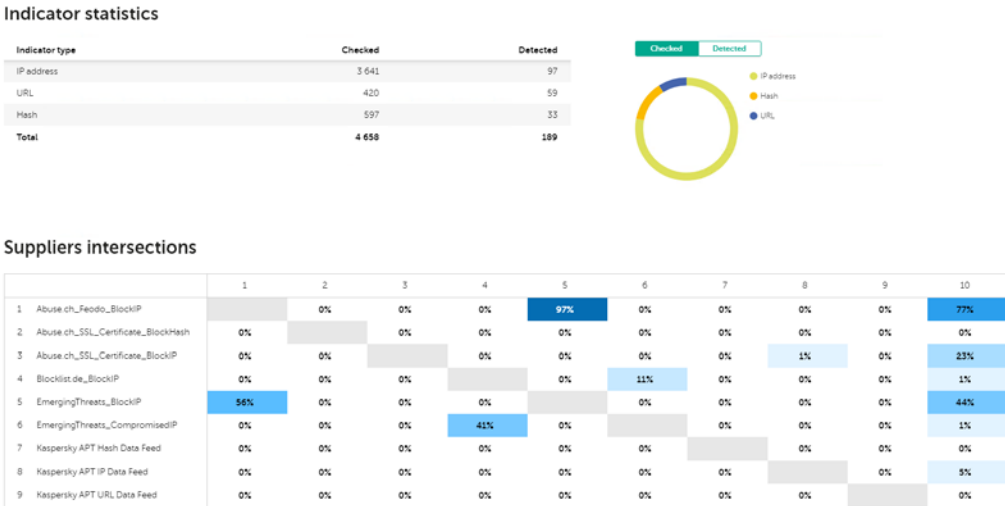


Figura 6. Creación de una nueva empresa

- 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 de amenazas más valiosos.



Indicator statistics

Indicator type	Checked	Detected
IP address	3 641	97
URL	420	59
Hash	597	33
Total	**4 658**	**189**

Suppliers intersections

	1	2	3	4	5	6	7	8	9	10
1 Abuse.ch_Feodo_BlockIP		0%	0%	0%	97%	0%	0%	0%	0%	77%
2 Abuse.ch_SSL_Certificate_BlockHash	0%		0%	0%	0%	0%	0%	0%	0%	0%
3 Abuse.ch_SSL_Certificate_BlockIP	0%	0%		0%	0%	0%	0%	1%	0%	23%
4 Blocklist.de_BlockIP	0%	0%	0%		0%	11%	0%	0%	0%	1%
5 EmergingThreats_BlockIP	56%	0%	0%	0%		0%	0%	0%	0%	44%
6 EmergingThreats_CompromisedIP	0%	0%	0%	41%	0%		0%	0%	0%	1%
7 Kaspersky APT Hash Data Feed	0%	0%	0%	0%	0%	0%		0%	0%	0%
8 Kaspersky APT IP Data Feed	0%	0%	0%	0%	0%	0%	0%		0%	5%
9 Kaspersky APT URL Data Feed	0%	0%	0%	0%	0%	0%	0%	0%		0%

Figura 7. Matriz de intersección de fuentes y estadísticas de indicadores

- HTTP Rest API le permite buscar y administrar la inteligencia de amenazas. Mediante el uso de Rest API, Kaspersky CyberTrace puede integrarse fácilmente en entornos complejos para automatizarlos y organizarlos.
- Se admite la integración en Kaspersky Unified Monitoring y Analysis Platform (KUMA), incluida la integración de interfaz de usuario web (UI única).

Si bien Kaspersky CyberTrace y Kaspersky Threat Data Feeds se pueden utilizar por separado, cuando se usan juntos, fortalecen en gran medida las 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 lograr lo siguiente:

- Sintetizar y priorizar eficazmente las alertas de seguridad
- Reducir la carga de trabajo de los analistas y evitar el agotamiento
- Identificar de inmediato las alertas críticas para la empresa y tomar decisiones más informadas sobre cuáles se deben escalar a los equipos de respuesta ante incidentes
- Formar una defensa proactiva e inteligente.

Entre otras características del producto, se incluyen las siguientes:

- Conectores de 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
- Filtros avanzados de 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 dispositivos de red
- Y mucho más

Noticias sobre ciberamenazas: www.securelist.com
Noticias sobre seguridad de TI: business.kaspersky.com
Seguridad de TI para pequeñas y medianas empresas: kaspersky.com/business
Seguridad de IT para grandes empresas: kaspersky.es/enterprise-security
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.es

Hemos pasado pruebas. Somos independientes. Somos transparentes. Nos comprometemos a construir un mundo más seguro en el que la tecnología nos mejore la vida. Por eso la protegemos, para que todas las personas del mundo puedan beneficiarse de las oportunidades que brinda la tecnología. Proteja su futuro gracias a la ciberseguridad.

Obtenga más información en kaspersky.com/transparency

Proven.
Transparent.
Independent.