kaspersky PREPARADOS PARA EL FUTURO

Kaspersky CyberTrace

La cantidad de alertas de seguridad procesadas por los analistas de seguridad de información crece exponencialmente cada día. 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 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 analistas de seguridad siguen extremadamente sobrecargados.

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.

Facilitación del análisis y de la evaluación eficaz 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 analistas de seguridad 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. 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 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.

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 sus flujos de trabajo de operaciones de seguridad existentes. 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.

Kaspersky CyberTrace utiliza un proceso interno de análisis y correlación de datos entrantes, lo que reduce significativamente la carga de trabajo de SIEM. 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:

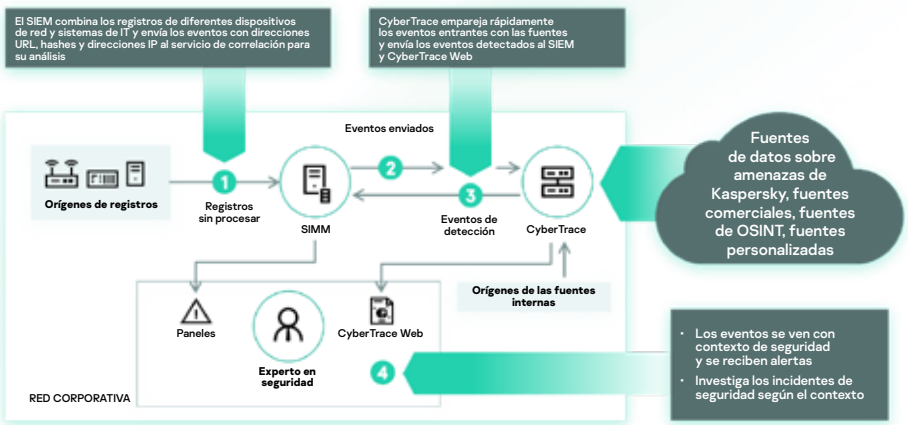

Figura 1. Esquema de integración de Kaspersky CyberTrace

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:

- 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 páginas con información detallada sobre cada indicador ofrecen un análisis aún más profundo. 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.

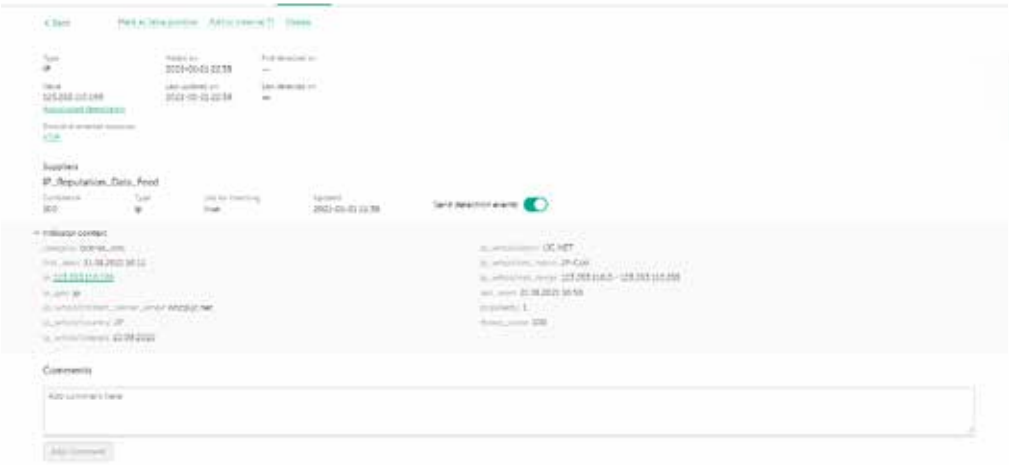

Figura 2. Información detallada sobre un indicador de todos los proveedores de inteligencia frente a amenazas

- 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.

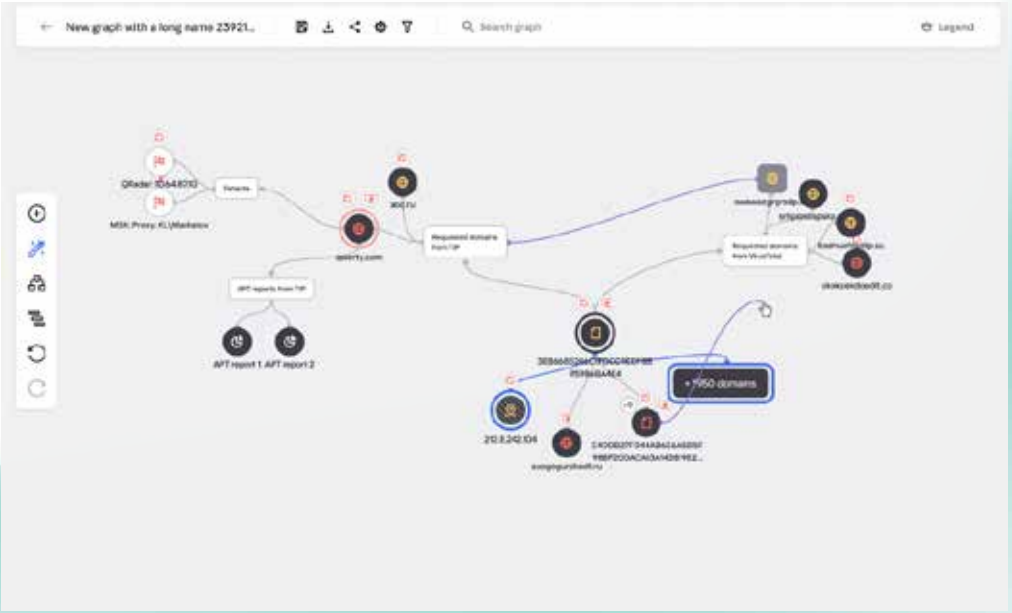

Figura 3. Gráfico de investigación

- La función de exportación de indicadores admite la exportación de conjuntos de indicadores a los controles de seguridad, 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.

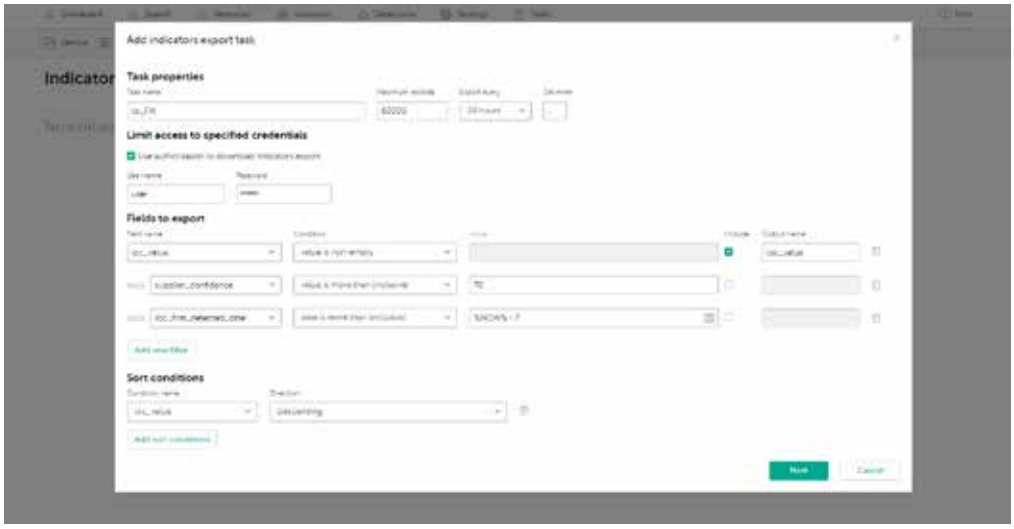

Figura 4. Tarea de exportación de indicadores

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

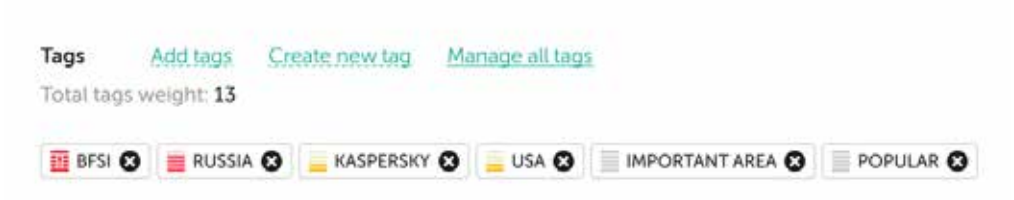

Figura 5. Etiquetas de IoC

- La función de correlación histórica (retroscan) le permite analizar 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.
- Un filtro para enviar los eventos de detección al SIEM reduce la carga de estos y 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 detecciones se guardan en la base de datos interna y se pueden utilizar durante los análisis de causa raíz o en la caza de amenazas.
- 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.

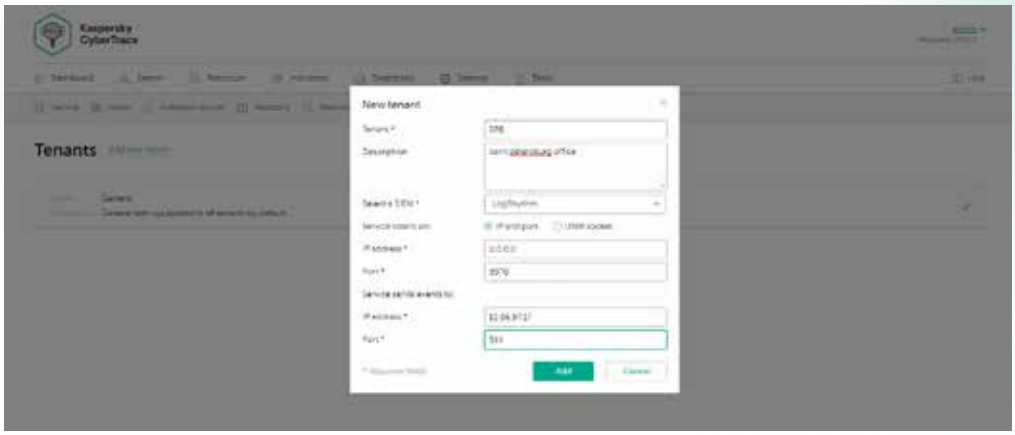

Figura 6. Creación de nuevo usuario

- 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.

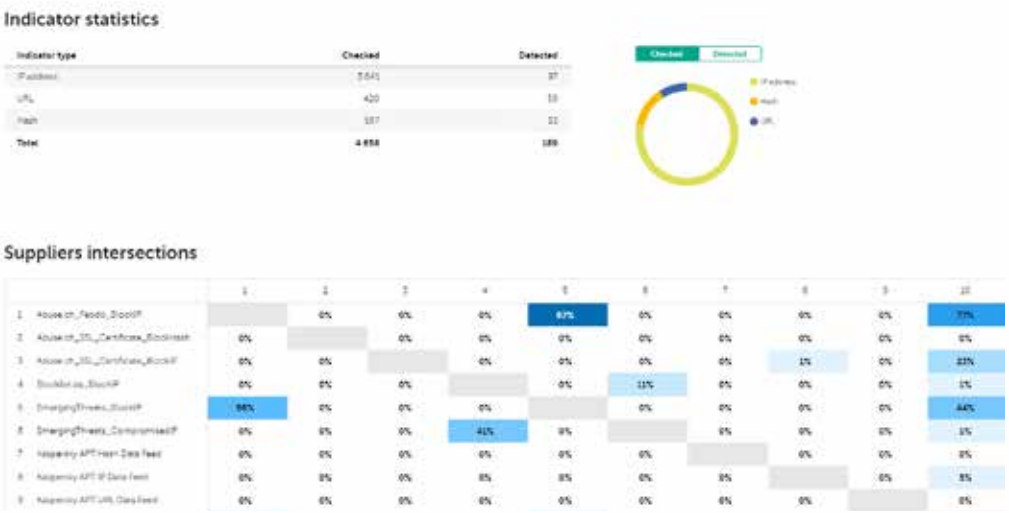

Figura 7. Estadísticas de indicadores y matriz de intersección de fuentes

- La API REST de HTTP le permite buscar y gestionar la inteligencia frente a amenazas. Al utilizar la API REST, Kaspersky CyberTrace se puede integrar fácilmente en entornos complejos de automatización y organización.
- Se admite la integración con la plataforma Kaspersky Unified Monitoring and Analysis (KUMA), incluida la integración de interfaz de usuario web (IU única).

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

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

Noticias sobre ciberamenazas: www.securelist.com
Noticias sobre seguridad de IT: business.kaspersky.com
Seguridad de TI para pymes: https://www.kaspersky.es/small-to-medium-business-security
Seguridad de TI para grandes empresas: kaspersky.es/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.es

Seguridad probada. 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.

Más información en kaspersky.es/transparency

Proven.
Transparent.
Independent.