Kaspersky® CyberTrace

El número de alertas de seguridad procesadas por los analistas de primer nivel del Centro de operaciones de seguridad crece cada día de manera exponencial y esto dificulta la eficiencia de la alerta, el triaje y la validación. Se reciben tantas alertas por parte de los productos de seguridad, que algunas importantes se pierden por el camino, para descontento del analista. Las herramientas de analítica de seguridad, la gestión del registro y el sistema SIEM que añaden datos de seguridad y correlacionan alarmas ayudan a reducir el número de alertas y garantizan el análisis adicional, pero los especialistas de primer nivel siguen desbordados.

Cómo habilitar un triaje y análisis eficaz

Al integrar la inteligencia de amenazas de lectura automática actualizada en los controles de seguridad ya existentes, como los sistemas SIEM, los Centros de operaciones de seguridad pueden automatizar el proceso de triaje inicial, ya que ofrecen a sus especialistas de primer nivel el contexto adecuado para identificar de inmediato alertas que no necesitan investigarse o escalarse a equipos de respuesta a incidentes para una investigación y respuesta más profunda. No obstante, el continuo crecimiento del número de fuentes de datos y de inteligencia de amenazas disponibles dificulta que las organizaciones determinen el tipo de información que es relevante para ellas. La inteligencia de amenazas se proporciona en diferentes formatos e incluye un gran número de indicadores de compromiso, lo que complica que los controles de seguridad de red o SIEM los asimilen.

Kaspersky CyberTrace es una fusión entre la inteligencia de amenazas y una herramienta de análisis que permite una integración continua de fuentes de datos de amenazas con soluciones que, a su vez, ayudan a los analistas a hacer uso de la inteligencia de amenazas para que sus operaciones de seguridad sean más eficaces. Se integra con cualquier fuente de inteligencia de amenazas (en formatos JSON, STIX, XML y CSV) que quiera utilizar (las fuentes de inteligencia de amenazas de Kaspersky, otros proveedores, OSINT o sus propias fuentes personalizadas) y admite la integración innovadora con numerosas soluciones y fuentes de registro. Al combinar automáticamente los registros contra las fuentes de inteligencia de amenazas, Kaspersky CyberTrace proporciona una visión de la situación que permite a los analistas de primer nivel tomar mejores decisiones en el momento

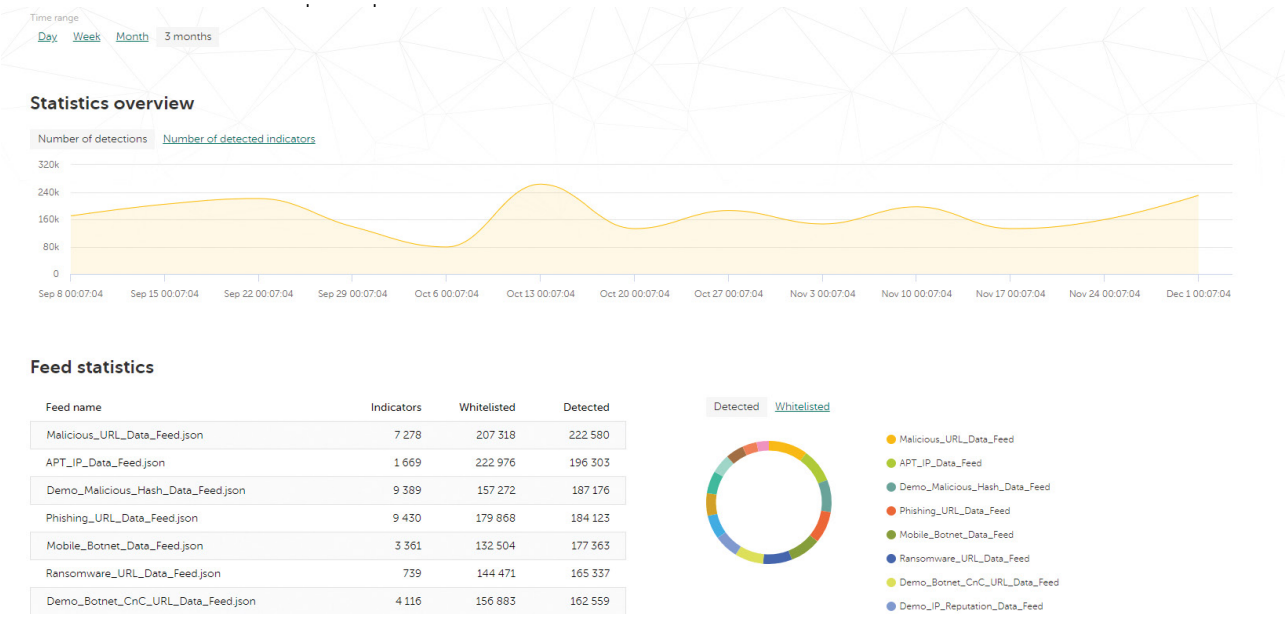


Imagen 1. Estadísticas de Kaspersky CyberTrace

Kaspersky CyberTrace ofrece una serie de instrumentos para poner en práctica la inteligencia de amenazas y llevar a cabo un triaje y una respuesta inicial eficaz:

- Fuentes de datos de amenazas de prueba de Kaspersky Lab y de OSINT a su disposición.
- Conectores SIEM de una amplia variedad de soluciones SIEM para visualizar y gestionar datos sobre detecciones de amenazas.
- Estadísticas de uso de fuentes de datos para medir la eficacia de las fuentes integradas.
- Búsqueda bajo demanda de indicadores (hash, direcciones IP, dominios, URL) para una investigación exhaustiva de amenazas.
- Una interfaz de usuario web que ofrece visualización de datos, acceso a la configuración, gestión de fuentes, normas de registro de análisis, listas negras y blancas.
- Filtración avanzada para fuentes (basado en el contexto que ofrece cada indicador, como el tipo de amenaza, geolocalización, popularidad, horarios y demás) y eventos de registro (basándose en sus condiciones personalizadas).
- Exporta los resultados de la búsqueda combinando fuentes de datos con formato CSV para la integración con otros sistemas (cortafuegos, red e IDS alojados, herramientas personalizadas).
- Análisis a gran escala de registros y archivos.
- Interfaz de línea de comandos para plataformas Windows y Linux.
- Modo stand-alone, donde Kaspersky CyberTrace no se integra con un sistema SIEM pero recibe y analiza los registros de fuentes como dispositivos para redes.
- Instalación en escenarios compatibles con DMZ en los que se debe aislar de Internet.

La herramienta utiliza un proceso interiorizado de análisis y combinación de los datos entrantes que reduce significativamente la carga de trabajo del sistema SIEM. Kaspersky CyberTrace evalúa los registros y eventos recibidos, combina los datos obtenidos con las fuentes y genera sus propias alertas sobre detección de amenazas. En la siguiente imagen se muestra la arquitectura de gran nivel que tiene lugar durante la integración de la solución:

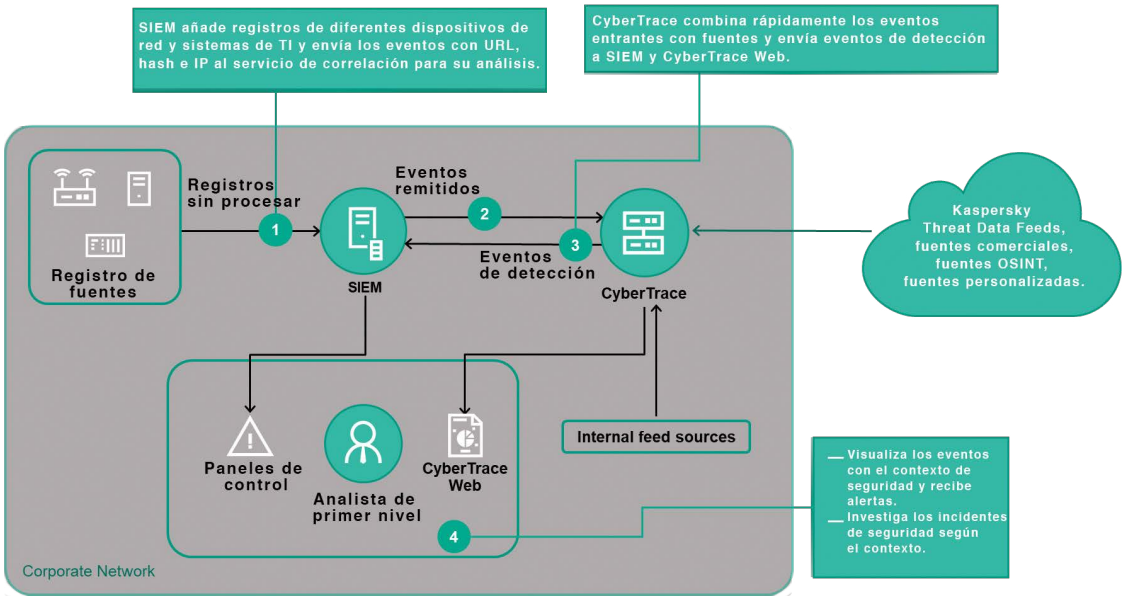


Imagen 2. Esquema de integración de Kaspersky CyberTrace

Kaspersky Lab también ofrece una serie de fuentes de datos de amenazas continuamente actualizadas compatibles con Kaspersky CyberTrace, lo que permitiría una visibilidad de amenazas global, la detección a tiempo de ciberamenazas, la priorización de alertas de seguridad y la respuesta eficiente de los incidentes de seguridad de la información:

- Reputación de IP: direcciones IP en contexto que comprenden hosts sospechosos y maliciosos.
- URL phishing y maliciosas: sitios web y enlaces phishing maliciosos.
- URL de botnet C&C: servidores C&C de botnet y objetos maliciosos relacionados en computadora.
- URL de botnet C&C móvil: servidores C&C de botnets en móviles.

- URL con ransomware: enlaces que hospedan objetos de ransomware o que pueden acceder a ellos.
- IoC de APT: dominios maliciosos, hosts, direcciones IP maliciosas, archivos maliciosos empleados para llevar a cabo ataques APT.
- DNS pasiva (pDNS): una serie de registros que contienen los resultados de la resolución DNS para dominios en las direcciones IP correspondientes[1].
- URL de IdC: páginas web empleadas para descargar malware que infecte dispositivos IdC[2].
- Hashes maliciosos: el malware más peligroso, frecuente y nuevo.
- Hash malicioso en móvil: compatible con la detección de objetos maliciosos que infectan las plataformas móviles Android y iOS.
- Troyano P-SMS: compatible con la detección de troyanos por SMS que permiten a los atacantes robar, eliminar y responder a mensajes de texto, además de llamar a los números de tarificación adicional.
- Listas blancas: se proporciona un conocimiento sistemático de software legítimo a soluciones y servicios de terceros.

Toda esta recopilación de datos se compone mediante una combinación de fuentes combinadas, heterogéneas y de confianza, como Kaspersky Security Network y sus más de 100 millones de usuarios de todo el mundo que comparten voluntariamente sus datos sobre ciberamenazas con nosotros, nuestras propias arañas web, el sistema de monitorización de botnets (en activo las 24 horas del día y los 365 días del año analizando todos los botnets conocidos para determinar sus objetivos y actividades, trampas spam, equipos de investigación de amenazas y socios de confianza.

Entonces, en tiempo real, se inspeccionan todos estos datos minuciosamente y se perfecciona el uso de varias técnicas de procesamiento, como criterios estadísticos, sistemas expertos de Kaspersky Lab (entornos aislados, motores heurísticos, analizadores múltiples, herramientas de similitud, creación de perfiles de comportamiento, etc.), la validación de nuestros analistas y la verificación de las listas blancas.

Cada registro de cada fuente de datos va acompañado de información contextual práctica (calificación de la amenaza, geolocalización, nombre de las amenazas, fecha, direcciones IP determinadas de recursos web infectados, hash, popularidad, etc.).

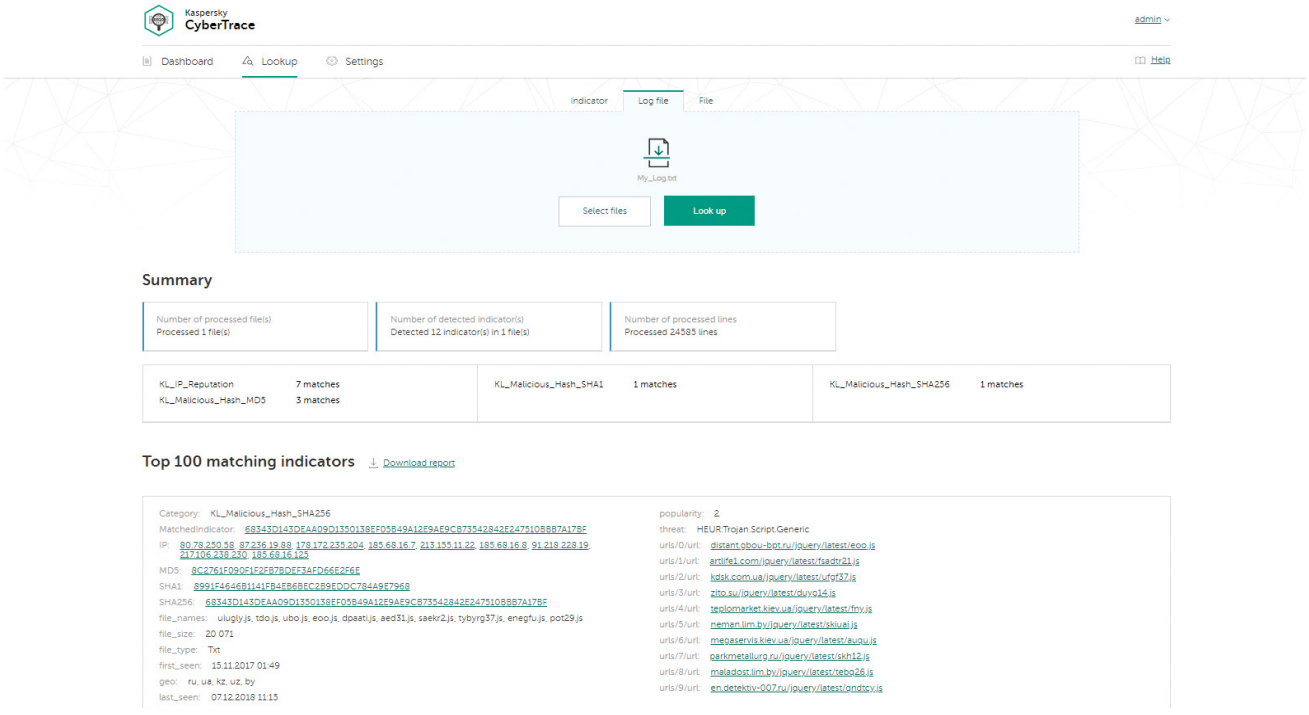


Imagen 3. Contexto Kaspersky Threat Data Feeds

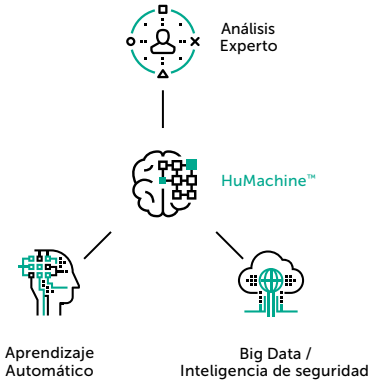
1 El servicio de integración se ofrecerá en el 2019

2 El servicio de integración se ofrecerá en el 2019

Esta información sobre el contexto ayuda a formarse una imagen más nítida, además de validar y admitir el amplio uso de los datos. Puestos en contexto, los datos se pueden utilizar más fácilmente para responder las preguntas "quién, qué, dónde y cuándo" con las que conseguirá identificar a sus adversarios y le ayudará a tomar buenas decisiones.

Aunque Kaspersky CyberTrace y Kaspersky Threat Data Feeds se pueden utilizar por separado, utilizados de forma conjunta refuerzan significativamente sus capacidades de detección de amenazas, fortaleciendo sus operaciones de seguridad con visibilidad global sobre las ciberamenazas. Con Kaspersky CyberTrace y Kaspersky Threat Data Feed, los analistas de los centros de operaciones de seguridad son capaces de:

- Sintetizar y dar prioridad de manera efectiva a la gran cantidad de alertas de seguridad.
- Mejorar y acelerar el triaje y los procesos de repuesta inicial.
- Identificar de inmediato las alertas críticas que sufra la empresa y tomar decisiones mucho más fundamentadas sobre cuál debería escalarse a los equipos de TI.
- Elaborar una defensa inteligente y proactiva.



Kaspersky Lab
Ciberseguridad para empresas: **www.kaspersky.com/enterprise**
Noticias sobre ciberamenazas: **www.securelist.com**
Noticias sobre seguridad informática: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

latam.kaspersky.com