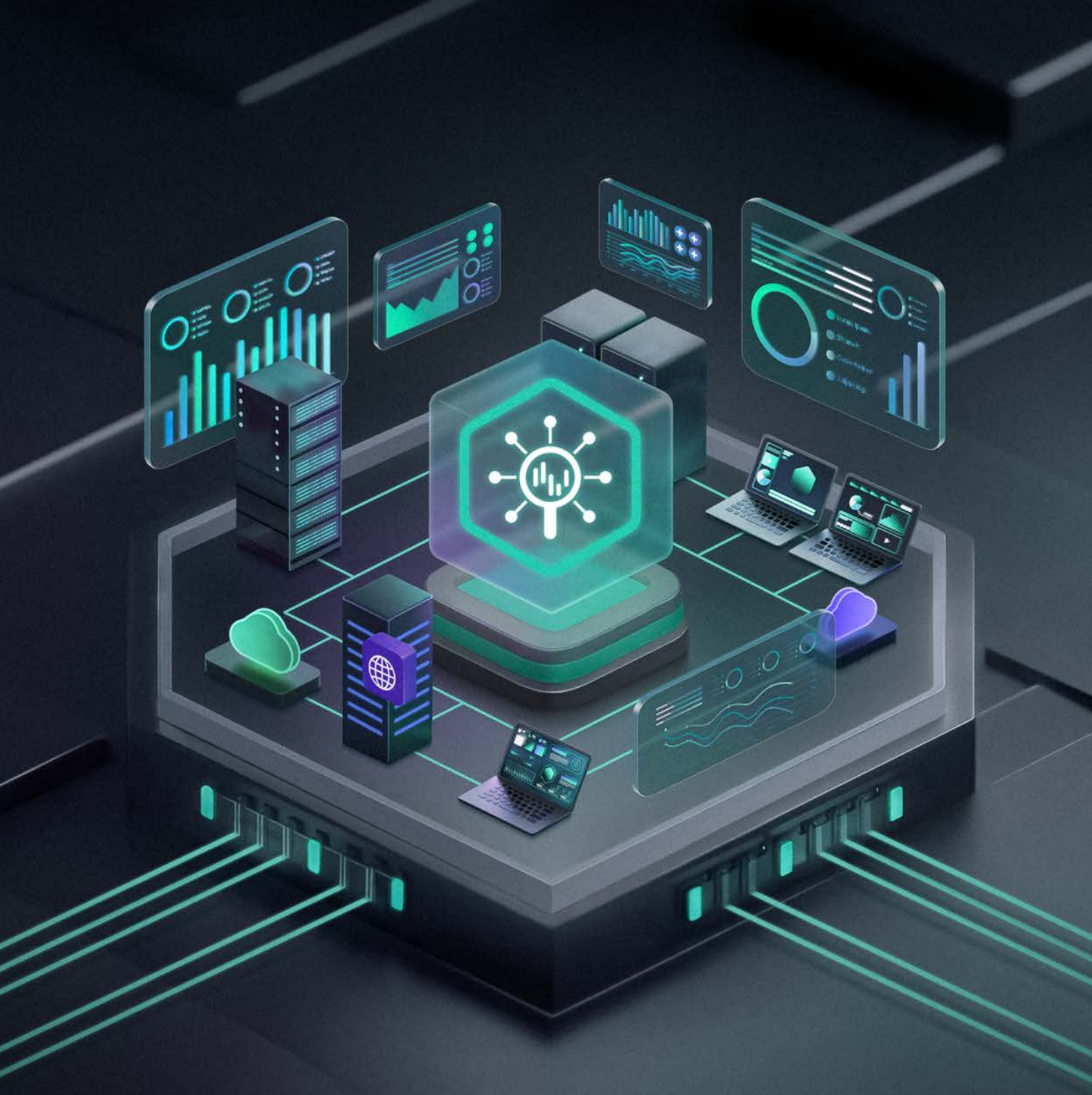


Ficha Técnica

Kaspersky SIEM

Transforme sus operaciones de seguridad con una solución de última generación, impulsada por IA y fortalecida con inteligencia de amenazas de primer nivel

kaspersky bring on the future

Kaspersky SIEM es una solución pensada para organizaciones con infraestructuras de TI complejas, grandes volúmenes de datos y requisitos normativos estrictos. El producto está preparado para MSSP con soporte multitenencia integrado.

Estas organizaciones reconocen que una seguridad eficaz no solo depende de la prevención, sino también de la capacidad de detectar, analizar y responder a las amenazas en tiempo real en diversos sistemas.

Maximice el impacto de sus operaciones de seguridad

Las grandes organizaciones se enfrentan a una cantidad cada vez mayor de amenazas persistentes avanzadas (APTs). En 2024, se detectaron APTs en una de cada cuatro empresas y representaron el 43 % de todos los incidentes de alta gravedad[1]. Las consecuencias fueron costosas y abarcaron desde la interrupción de la actividad empresarial hasta pérdidas financieras y daños a largo plazo a la reputación.

Además, los equipos de seguridad están sometidos a una presión sin precedentes. Los sistemas de protección generan enormes volúmenes de datos, lo que aumenta los costos de almacenamiento y eleva el precio de las implementaciones de SIEM. Los expertos calificados escasean, mientras que los equipos existentes están desbordados: el 70 % de los centros de operaciones de seguridad (SOC) tienen dificultades para seguir el ritmo de la avalancha de alertas[2]. Además, la complejidad de la administración de los sistemas SIEM supone una carga adicional para unos recursos ya de por sí limitados.

Incluso los centros de operaciones de seguridad más experimentados corren el riesgo de perder eficacia e impacto sin las herramientas actuales basadas en inteligencia artificial que los ayudan a eliminar el ruido y centrarse en lo más importante.

Prepare a su equipo con un SIEM basado en IA y respaldado por inteligencia de amenazas de primer nivel

Kaspersky SIEM es una solución de última generación diseñada para ayudar a su equipo de seguridad a administrar y analizar los datos de seguridad entrantes. Se destaca en lo siguiente:

- Recopila, procesa y almacena eventos procedentes de diversas fuentes, incluidos productos de Kaspersky, sistemas operativos, aplicaciones de terceros, herramientas de seguridad y bases de datos.
- Analiza y correlaciona los datos entrantes en tiempo real para enriquecerlos con inteligencia de amenazas líder en el sector y detectar actividades sospechosas.
- Emite alertas oportunas para permitir una rápida investigación y respuesta ante incidentes.
- Almacena datos durante un período prolongado sin exceder el presupuesto destinado a costosos equipos de almacenamiento, gracias a las opciones de almacenamiento en caliente y en frío con una función de búsqueda simultánea sin interrupciones.

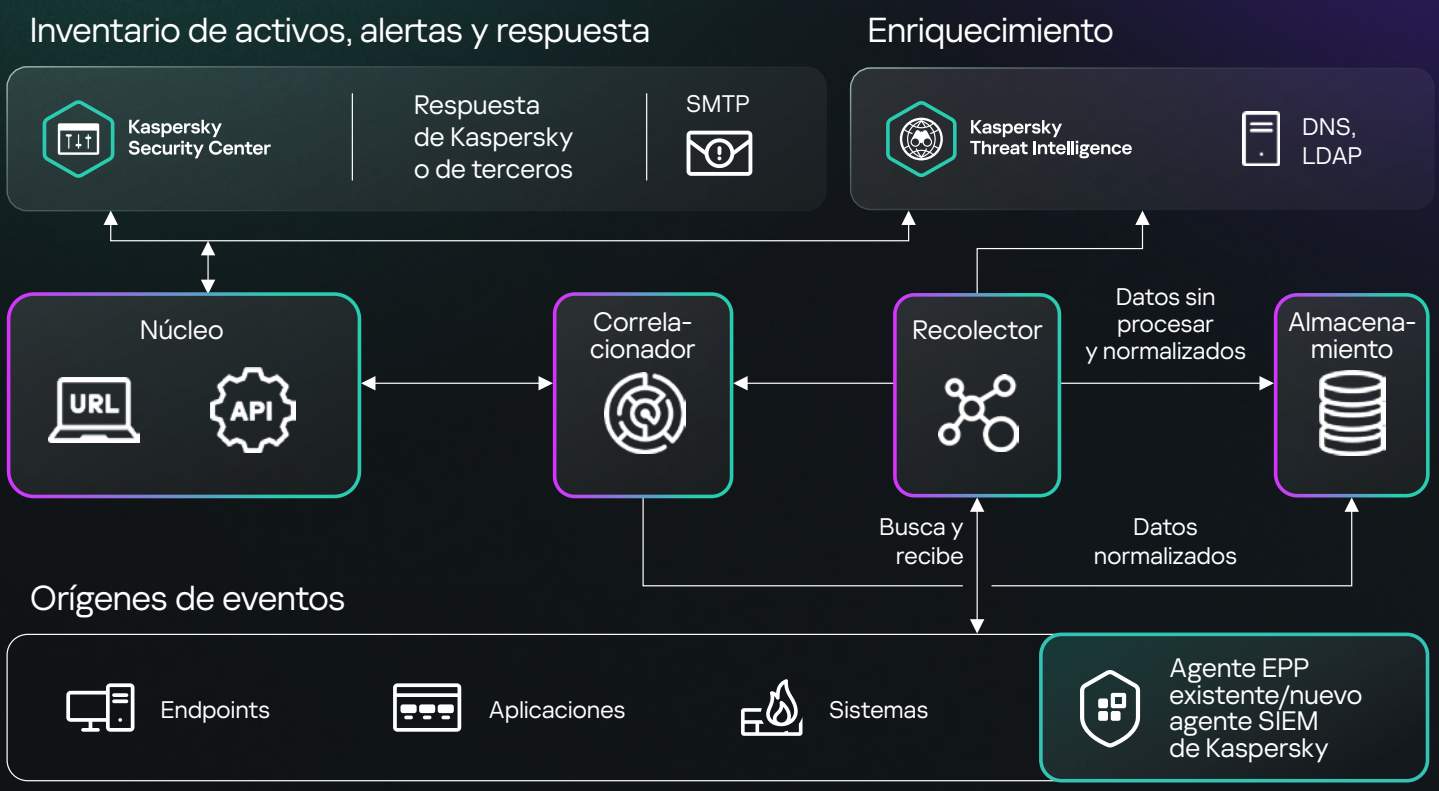
Al unificar los registros de las fuentes de seguridad y correlacionarlos en tiempo real, Kaspersky SIEM les proporciona a sus analistas la visibilidad y el contexto completos para responder de manera eficaz.

Ofrece capacidades avanzadas de búsqueda y análisis que les permiten a sus buscadores de amenazas descubrir amenazas previamente desconocidas. El análisis de datos históricos y el establecimiento de bases de referencia estadísticas con el conjunto de reglas de detección UEBA ayudan a su equipo a identificar anomalías y detener ataques sofisticados.

Con Kaspersky SIEM, su SOC obtiene la visibilidad, inteligencia y eficacia que necesita para convertir datos abrumadores en información de seguridad práctica. La solución puede funcionar sin conexión a Internet, lo que garantiza la plena soberanía de los datos.

1 Informe de los analistas de Kaspersky Managed Detection and Response para 2024
2 Kaspersky Report: The portrait of modern information security professional, 2024.

¿Cómo funciona?



Gracias a la arquitectura de microservicios de la solución, sus administradores pueden crear y configurar los microservicios que necesitan para usar Kaspersky SIEM como una herramienta de administración de registros o un sistema SIEM integral.

Kaspersky SIEM se basa en una Open Single Management Platform[3], que integra tanto los productos de Kaspersky como los de terceros en un sistema de seguridad centralizado. Constituye una parte esencial de una estrategia de defensa integral, que protege los entornos corporativos e industriales y detecta los ciberataques que se desplazan de los sistemas de TI a los de TO.

Lo que distingue a Kaspersky SIEM

Maximiza el rendimiento y minimiza los costos

Reduzca los costos de hardware y virtualización hasta en un 50 % y disminuya el costo total de propiedad con un SIEM modular de alto rendimiento que supera las soluciones heredadas y administra cientos de miles de EPS por instancia.

Un ecosistema Kaspersky integrado

Aproveche más de 200 integraciones preconfiguradas de Kaspersky y de terceros con opciones de respuesta integradas. Nuestro perfecto ecosistema ofrece una interfaz única para la inteligencia de amenazas, utiliza sensores de endpoints como agentes SIEM y proporciona capacidades de integración sin igual entre otros proveedores.

Experiencia integrada en SOC

Acceda a más de 700 reglas de detección preconfiguradas, actualizadas trimestralmente con mapeo MITRE y guías de respuesta, todas desarrolladas por el SOC de Kaspersky, uno de los equipos de búsqueda de amenazas con más experiencia del sector.

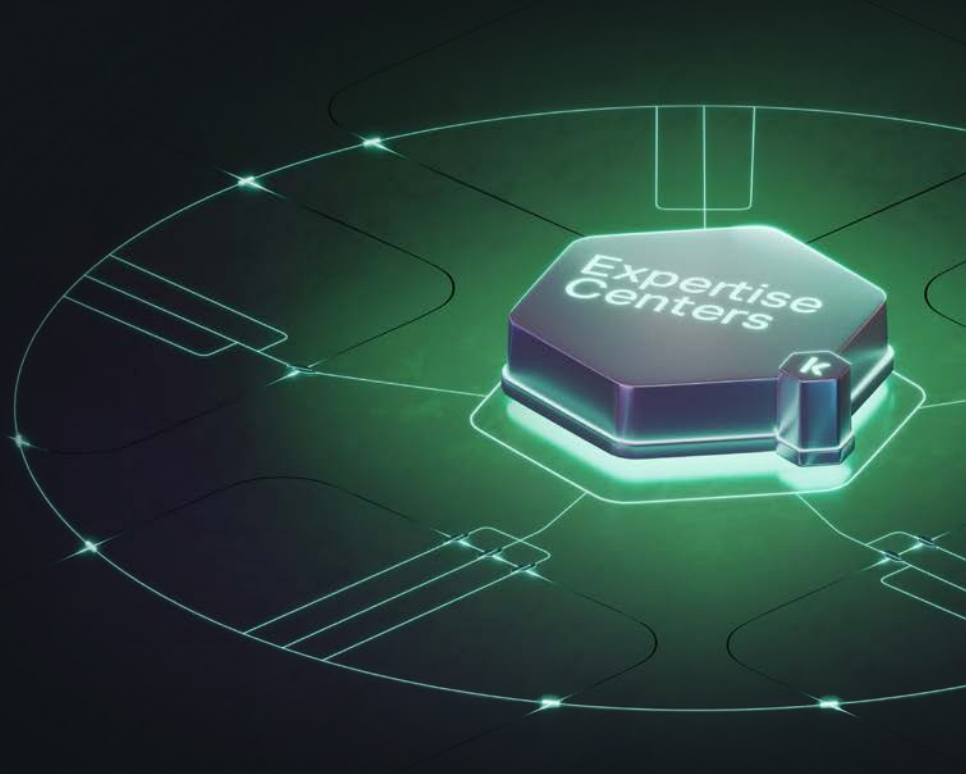
Detección de amenazas impulsada por IA

Los componentes mejorados con IA identifican rápidamente actividades sospechosas en toda su infraestructura, con detección de hijacking de DLL mediante IA, puntuación de riesgos de activos basada en IA y mucho más. Estas características mejoran la precisión de la detección, reducen los falsos positivos y minimizan el impacto de los ciberincidentes, lo que ayuda a mejorar su MTTD y MTTR.

3 Kaspersky Next XDR Expert, impulsado por esta plataforma, amplía sus capacidades con la búsqueda avanzada de amenazas, guías automatizadas y una administración optimizada de casos.

Kaspersky SIEM aprovecha los años de conocimiento acumulado y las habilidades perfeccionadas de los Centros de Experiencia de Kaspersky, cinco centros especializados y unificados dedicados a promover la ciberseguridad.

Más información



Kaspersky SIEM incluye Servicios de soporte prémium las 24 horas del día, los 7 días de la semana, entre los que se incluyen integraciones personalizadas proporcionadas por Kaspersky Professional Services o socios de confianza, lo que aprovecha las capacidades API de los productos conectados.

Brindamos una implementación rápida, asistencia para una migración fluida y experiencia continua para garantizar que obtenga el máximo valor de su implementación SIEM.

Kaspersky SIEM

latam.kaspersky.com

Más información

#kaspersky
#bringonthefuture