Informe técnico
sobre el producto

Kaspersky SIEM

kaspersky bring on the future

Contenido

Mercado de la información de seguridad y la administración de eventos

Los líderes de ciberseguridad de las organizaciones enfrentan diversos desafíos, entre los que se incluyen un creciente número de intentos de penetración en su infraestructura, la escasez de personal especializado y ataques cada vez más complejos.

Además, deben cumplir con los requisitos normativos relacionados con la retención de datos, la auditoría y la investigación de incidentes, lo cual impacta directamente en el mercado global de SIEM.

Por otro lado, las organizaciones también se ven presionadas a clasificar las alertas de ciberataques por prioridad y gestionarlas de manera más eficiente debido a su crecimiento y complejidad creciente.

Adicionalmente, la expansión del trabajo remoto ha impulsado la adopción de aplicaciones SaaS y el uso de dispositivos personales (BYOD) por parte de los empleados, lo que subraya la necesidad de extender la visibilidad de la red más allá del perímetro tradicional.

Finalmente, encontrar expertos calificados en seguridad de la información sigue siendo uno de los mayores retos en el mercado actual. Las empresas están buscando formas de optimizar sus recursos y mejorar la eficiencia de la ciberseguridad. Como consecuencia, desean obtener datos prácticos y de fácil acceso para sus equipos del SOC.

Según Kaspersky Human Factor 360 Report

77 % de las empresas sufrió al menos una intrusión en la ciberseguridad y muchas reportaron hasta seis incidentes durante ese período

41 % de las empresas sienten que tienen brechas en sus infraestructuras de ciberseguridad y planean aumentar las inversiones en esta área en el futuro

Conozca más

Acerca de Kaspersky SIEM y su arquitectura

Kaspersky United Monitoring and Analysis Platform es una solución SIEM de última generación para la gestión de datos y eventos de seguridad. Se distingue en la recepción, el procesamiento y el almacenamiento de eventos de información sobre la seguridad, en el análisis y la correlación de datos entrantes. La plataforma también ofrece una función de búsqueda, genera alertas ante amenazas potenciales y admite respuestas automatizadas tanto para las alertas como para la búsqueda de amenazas.

La arquitectura modular de alto rendimiento permite procesar cientos de miles de eventos por segundo (EPS) en cada instancia y reduce el costo total de propiedad (TCO) mediante la optimización de los requisitos del sistema.

Mediante la integración de productos de terceros y de Kaspersky en un sistema centralizado de seguridad de la información, Kaspersky SIEM se posiciona como un componente esencial en una estrategia de defensa integral. Es capaz de proteger entornos corporativos e industriales, detectando ciberataques que se originan en sistemas IT y se propagan a sistemas OT.

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

La solución recopila eventos de seguridad de diversas fuentes, incluidos productos de Kaspersky, sistemas operativos, aplicaciones de terceros, herramientas de seguridad y bases de datos. Estos eventos se correlacionan y se enriquecen con datos provenientes de fuentes de inteligencia sobre amenazas, con el objetivo de identificar actividades sospechosas en las infraestructuras de la red corporativa y proporcionar notificaciones oportunas sobre incidentes de seguridad.

Al agregar registros de todos los controles de seguridad y correlacionar los datos en tiempo real, **Kaspersky SIEM proporciona la información necesaria para investigar y responder incidentes.**

Además, la solución facilita la detección de amenazas previamente desconocidas por parte de los buscadores de amenazas al permitirles analizar y asociar datos históricos, así como establecer referencias estadísticas para identificar anomalías.

Kaspersky Unified Monitoring and Analysis Platform incluye los siguientes componentes

Un **núcleo** con una interfaz de usuario gráfica centralizada para controlar y supervisar la configuración de los componentes del sistema. Se puede acceder a la plataforma desde soluciones de terceros a través de la API.

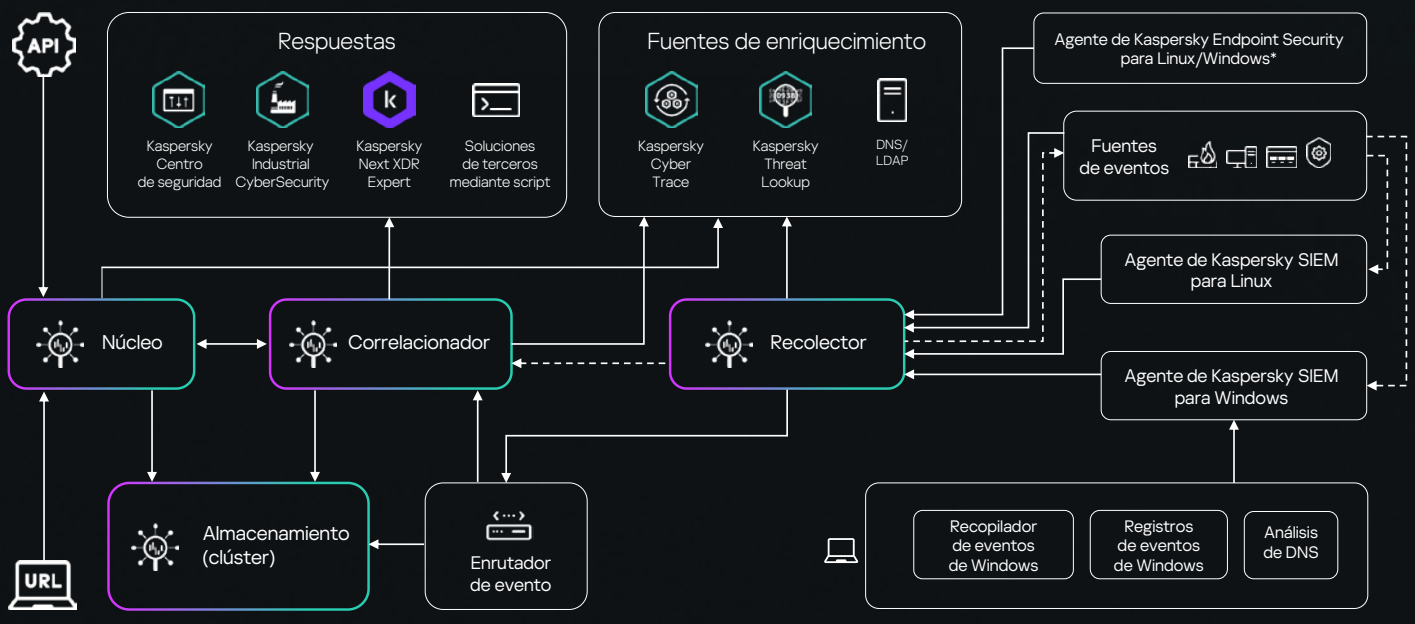
Las reglas de correlación se usan para detectar secuencias específicas de eventos procesados y tomar determinadas acciones tras el reconocimiento, como crear eventos de correlación/alertas o interactuar con una lista activa. El **correlacionador** utiliza listas activas para ejecutar acciones requeridas tras analizar los eventos normalizados recibidos de los colectores y genera alertas basadas en los criterios de correlación.

Uno o más **colectores** reciben eventos de fuentes externas y llevan a cabo un preprocesamiento: los normalizan (convirtiéndolos a un formato único), los filtran, agregan y enriquecen con datos adicionales mediante el uso de diccionarios, consultas al servicio DNS y otras herramientas.

El almacenamiento se usa con el propósito de guardar eventos normalizados para que se pueda acceder a ellos de forma rápida y constante desde el sistema SIEM con el objetivo de extraer datos analíticos.

Los agentes envían eventos sin procesar de estaciones de trabajo y servidores a los colectores SIEM. El envío de eventos del registro de Windows directamente al colector ahora está disponible en Kaspersky Endpoint Security para Windows 12.6 o Linux 12.2. Esto reduce considerablemente la cantidad de trabajo que se necesita para integrar las fuentes de eventos con el sistema de Kaspersky SIEM.

Los enrutadores de eventos reducen la carga en las conexiones y la cantidad de puertos abiertos en los firewalls mediante la recepción constante de eventos sin demoras cuando los colectores se instalan en oficinas remotas con bajo ancho de banda o en conexiones de datos de mucha actividad.



Funcionalidad de Kaspersky SIEM

Conectores integrados y personalizados a cientos de fuentes de Kaspersky y proveedores externos con actualizaciones y mejoras regulares.

Integración de fuentes de eventos externas con creación gratuita de conectores adicionales del equipo de Kaspersky Professional Services.

Búsqueda rápida de consultas e informes preparados sobre eventos de seguridad.

Almacenamiento local seguro de registros para el cumplimiento normativo y la investigación de incidentes.

Kaspersky SIEM admite las búsquedas de eventos en múltiples almacenamientos para ayudar a los operadores a buscar eventos relevantes en clústeres de almacenamiento distribuidos de forma más rápida y simple.

Supervise, procese y almacene información sobre los eventos de seguridad

Kaspersky Unified Monitoring and Analysis Platform recibe eventos de registros y normaliza datos de diferentes fuentes de eventos para que sean coherentes. Estos eventos de seguridad de la información pueden incluir intentos de inicio de sesión, interacciones con bases de datos o transmisiones de datos desde sensores, y se recopilan en toda la infraestructura IT protegida de la empresa. Si bien un evento individual puede parecer insignificante, en su conjunto, varios eventos individuales ofrecen un panorama más amplio de actividades maliciosas que se puede usar para detectar problemas de seguridad.

El lago de datos, nuestro repositorio local centralizado, proporciona una plataforma para recopilar, indexar y analizar registros de varias fuentes, incluidas soluciones de seguridad (EPP, FW, IAM, etc.), sistemas operativos, aplicaciones empresariales (sistemas de RR. HH., herramientas de la oficina), sistemas físicos de seguridad (sistemas de control automatizado de acceso) y otros dispositivos.

Los eventos se transmiten al correlacionador para su análisis y almacenamiento una vez que se hayan completado el filtrado y la agregación. Para identificar alertas, el colector recibe eventos de fuentes, los procesa y los envía al almacenamiento, correlacionador o servicios de terceros. Los eventos sin procesar se reenvían de estaciones de trabajo y servidores a colectores SIEM (en algunos casos, a través de agentes) y se pueden enviar a otros sistemas para llevar a cabo análisis adicionales.

La solución produce eventos de correlación tras el reconocimiento de un evento particular o una serie de eventos relacionados, y también los analiza y retiene. Si un evento o una secuencia de eventos indican una amenaza de seguridad potencial, Kaspersky SIEM genera una alerta con información sobre la amenaza y cualquier otro dato relevante que los especialistas de seguridad necesitan analizar.

Se utilizan protocolos de transporte confiables, con cifrado opcional, para transferir eventos entre componentes. El sistema puede usar un diodo de datos para recopilar datos de segmentos aislados.

Además, facilita la administración centralizada de activos mediante el suministro de un inventario grande de servidores, estaciones de trabajo y dispositivos de red. La plataforma puede recopilar información sobre posibles riesgos en los activos desde analizadores de vulnerabilidades y correlacionarla con categorías de activos para identificar amenazas. Esto permite que los equipos de seguridad puedan ver todo el entorno de activos.

Para respaldar a los analistas, se muestra la cobertura que tienen las reglas de la matriz MITRE ATT&CK para evaluar mejor el nivel de seguridad.

Más de 650 reglas de correlación preconfiguradas para detectar escenarios de ataque actualizados con regularidad por los servidores de Kaspersky con asignación de MITRE y recomendaciones de respuesta.

Relevancia mejorada de datos a través del enriquecimiento con datos analíticos recopilados de Kaspersky Threat Intelligence Portal (mediante Kaspersky Threat Lookup y Kaspersky CyberTrace).

Los datos sobre activos e infraestructuras se recopilan de Kaspersky Security Center y fuentes de terceros.

Los usuarios pueden comparar un evento con valores agrupados, agregados, promedio, máximos y mínimos para un período específico usando la funcionalidad de minería de datos de ClickHouse. Esto amplía considerablemente las capacidades de la lógica de detección sin que se requiera la creación de numerosas reglas de servicio.

Para facilitar la creación y edición de contenido, permitimos a los usuarios descubrir de antemano las reglas de correlación que el cambio previsto aplicará antes de realizar cambios en el criterio de filtrado.

Correlación histórica y en tiempo real de eventos de seguridad

Kaspersky SIEM realiza una correlación cruzada casi en tiempo real mediante reglas personalizadas para identificar ataques y amenazas, junto con cientos de reglas predefinidas desarrolladas por el SOC de Kaspersky, uno de los equipos más experimentados y exitosos en la detección de amenazas activas del sector. Quienes integran el SOC de Kaspersky poseen numerosos certificados que confirman su alto nivel de experiencia y conocimientos.

Los eventos se **correlacionan en tiempo real**. El correlacionador analiza eventos normalizados, crea alertas de conformidad con las reglas de correlación y gestiona todas las operaciones de la lista activa.

El principio operativo del correlacionador se basa en el análisis de identificación de eventos, lo que significa que cada evento se gestiona de conformidad con las reglas de correlación especificadas por el usuario. El software genera un evento de correlación y lo envía al almacenamiento cuando encuentra una serie de eventos que cumple los requisitos de la regla de correlación. El usuario puede personalizar las reglas de correlación que los resultados de un análisis anterior activarán mediante el envío del evento de correlación al correlacionador para un mayor análisis. Los resultados generados por una regla de correlación pueden ser utilizados por otras reglas similares. Por ejemplo, varias alertas pequeñas pueden combinarse para generar una alerta mayor, como al analizar varios intentos de fuerza bruta para identificar un incidente masivo de este tipo.

La plataforma usa datos históricos para detectar tendencias, buscar amenazas previamente no identificadas e identificar ataques pasados por alto por algunos elementos de seguridad. Todo esto mejora la detección general de amenazas.

Soluciones de terceros o productos integrados como **Kaspersky Endpoint Detection and Response** llevan a cabo detecciones del lado del sensor. Mediante el ajuste de la configuración del producto, los usuarios pueden controlar este proceso y obtener eventos y telemetría que estos productos ya procesaron a través de su propia lógica de detección.

El motor de correlación de la solución incorpora detección del lado de la plataforma. Gracias al poderoso motor de correlación de la plataforma, los usuarios pueden crear reglas de correlación adaptables. También se ofrecen reglas listas para usar y paquetes del normalizador para respaldar productos de terceros disponibles comercialmente que se expanden y actualizan con regularidad.

El principio operativo del correlacionador se basa en el análisis de identificación de eventos, lo que significa que cada evento se gestiona de conformidad con las reglas de correlación especificadas por el usuario. El software genera un evento de correlación y lo envía al almacenamiento cuando encuentra una serie de eventos que cumple los requisitos de la regla de correlación.

Detección de amenazas para detectar amenazas previamente desconocidas al permitir a los operadores analizar y correlacionar datos históricos usando una potente base de datos columnar.

Gracias a la función de búsqueda basada en etiquetas, los usuarios pueden buscar con facilidad filtros, diccionarios y reglas que están unificados por una única etiqueta. El almacenamiento del historial de consultas de búsqueda permite al usuario acceder a consultas anteriores con facilidad.

La plataforma puede almacenar datos durante un período extendido sin excederse del presupuesto, ya que no necesita hardware de almacenamiento costoso gracias a la opciones de almacenamiento en frío y caliente mediante ClickHouse y el Sistema de archivos distribuido de Hadoop (HDFS) o los discos locales.

Los administradores pueden prevenir problemas de espacio en el subsistema del disco mediante configuraciones flexibles: el alcance del almacenamiento de eventos se puede configurar en gigabytes como un porcentaje del espacio en disco, además de poder configurarlo en días.

Almacenamiento de datos sobre eventos de seguridad

El componente de almacenamiento de Kaspersky SIEM se utiliza para almacenar eventos normalizados con el objetivo de acceder de forma rápida y continua a datos analíticos de **Kaspersky Unified Monitoring and Analysis Platform**.

ClickHouse garantiza la continuidad y la velocidad de acceso. El almacenamiento se conecta al servicio de almacenamiento de Kaspersky SIEM a través de un clúster de ClickHouse. También se pueden agregar discos de almacenamiento en frío a los clústeres de ClickHouse.

Los usuarios pueden agregar espacio de los repositorios en eventos almacenados por grupos en función de un atributo específico. Esto permite a los administradores establecer diferentes tiempos de almacenamiento para los eventos en función de sus características específicas.

Kaspersky Unified Monitoring and Analysis Platform también gestiona la compresión de datos para reducir considerablemente el uso del espacio en disco sin afectar la recuperación de datos. La solución de Kaspersky admite dos áreas: una para la recuperación rápida de datos y la otra para el almacenamiento de una gran cantidad de datos.

La plataforma tiene dos secciones diferentes: una para el almacenamiento en frío que se puede ejecutar en el Sistema de archivos distribuido de Hadoop o en los discos locales, y la otra para el almacenamiento operativo a través de ClickHouse. Esta separación es clara.

Sin tener que alternar entre archivos, los operadores pueden crear consultas de búsqueda en una única interfaz y concentrar todo su esfuerzo en la investigación. Esto **reduce el costo de propiedad del sistema** al mismo tiempo que mantiene una excelente experiencia del usuario. La plataforma admite las búsquedas de eventos en múltiples almacenamientos para ayudar a los operadores a buscar eventos relevantes en clústeres de almacenamiento distribuidos de forma más rápida y simple.

Las organizaciones pueden mantener el cumplimiento con los requisitos normativos para la retención de datos, la auditoría y la investigación de incidentes mediante la recopilación y el almacenamiento seguros de registros de diferentes fuentes. Además, el almacenamiento centralizado y estructurado permite que las empresas recuperen y analicen registros fácilmente según lo necesiten.

Capacidades de respuesta integradas

La funcionalidad de respuesta integrada usando productos de Kaspersky aumenta la eficiencia de la seguridad. Por ejemplo, para extender las capacidades de respuesta en endpoints, Kaspersky SIEM puede asociarse con Kaspersky Endpoint Detection and Response para administrar el aislamiento de la red de activos y reglas de prevención o ejecutar aplicaciones y scripts. Estas medidas de respuesta pueden llevarse a cabo de forma manual o automática en los activos con el agente de Kaspersky Endpoint Security.

La recopilación automatizada de información de inventario (software instalado, vulnerabilidades, equipos, propietarios de activos, etc.) puede ayudar a poner en contexto los eventos de seguridad de la información y asistir en las investigaciones de incidentes.

Kaspersky SIEM utiliza Kaspersky CyberTrace, una plataforma de inteligencia de amenazas con funcionalidades completas que admite decenas de fuentes de datos de amenazas predeterminadas (comerciales y públicas) para transmitir el enriquecimiento de eventos automáticamente en tiempo real con información contextual acerca de indicadores de compromiso.

Los componentes de inteligencia artificial de Kaspersky SIEM facilitan la detección rápida de actividades sospechosas en la infraestructura.

Herramientas de inteligencia artificial y aprendizaje automático

Kaspersky usa algoritmos predictivos, técnicas de agrupamiento, redes neuronales, técnicas de modelado estadístico y algoritmos expertos para aumentar la efectividad de nuestros productos a la hora de detectar amenazas más rápido y priorizar las detecciones de forma precisa.

Los equipos de supervisión y respuesta pueden priorizar las alertas y concentrarse en la prevención de daños potenciales con el respaldo de los sistemas de IA y macrodatos. El módulo de IA simplifica la clasificación al analizar datos históricos, priorizar las alertas entrantes y asignar clasificaciones de riesgo basadas en inteligencia artificial para los activos. Este enfoque ayuda a generar hipótesis valiosas que se pueden utilizar para búsquedas proactivas.

La plataforma usa reglas de correlación definidas por el usuario para vincular eventos en tiempo real. Su módulo de correlación aplica algoritmos de inteligencia artificial para detectar actividades anómalas, como picos bruscos de tráfico o múltiples accesos al servicio, que indican un posible incidente, lo que facilita la detección temprana antes de que se produzcan daños.

Kaspersky SIEM también incorpora datos de Kaspersky Threat Intelligence, generados con tecnologías de IA y macrodatos. La base de datos se enriquece constantemente con los resultados de análisis de APT manuales, datos operativos de la red oscura, información de Kaspersky Security Network y datos de nuevos análisis de malware regulares.

Todas estas tecnologías ayudan a los usuarios a minimizar daños potenciales causados por ciberincidentes y a aumentar el MTTR y MTTD.

La visualización destacada con paneles e informes presenta datos en los formatos más utilizados para identificar tendencias, patrones y eventos anómalos.

Gracias a los widgets personalizables que facilitan la visualización de indicadores, los analistas pueden priorizar incidentes, identificar las causas raíz y responder a amenazas con mayor eficiencia. Al mismo tiempo, las organizaciones pueden monitorear la efectividad de sus operaciones de seguridad, detectar tendencias y evaluar el estado general de su sistema de protección.

Además, los usuarios pueden enriquecer los datos de eventos con contenido de diccionarios, tablas, activos y atributos de la cuenta, y utilizar esos datos para la búsqueda y la visualización. Esto ayuda a crear paneles e informes con datos más contextuales.

Esta solución ayuda a los usuarios a hacer sus propios widgets con configuraciones ajustables, así como diseños con **diferentes grupos de widgets:**

Métricas de alerta clave

(gravedad, prioridad y estado)

- Activos afectados
- Notificaciones recientes
- Principales fuentes de datos con la mayor cantidad de alertas
- Alertas asignadas a operadores específicos
- Usuarios o dispositivos afectados
- Alertas por política

Indicadores de incidentes clave

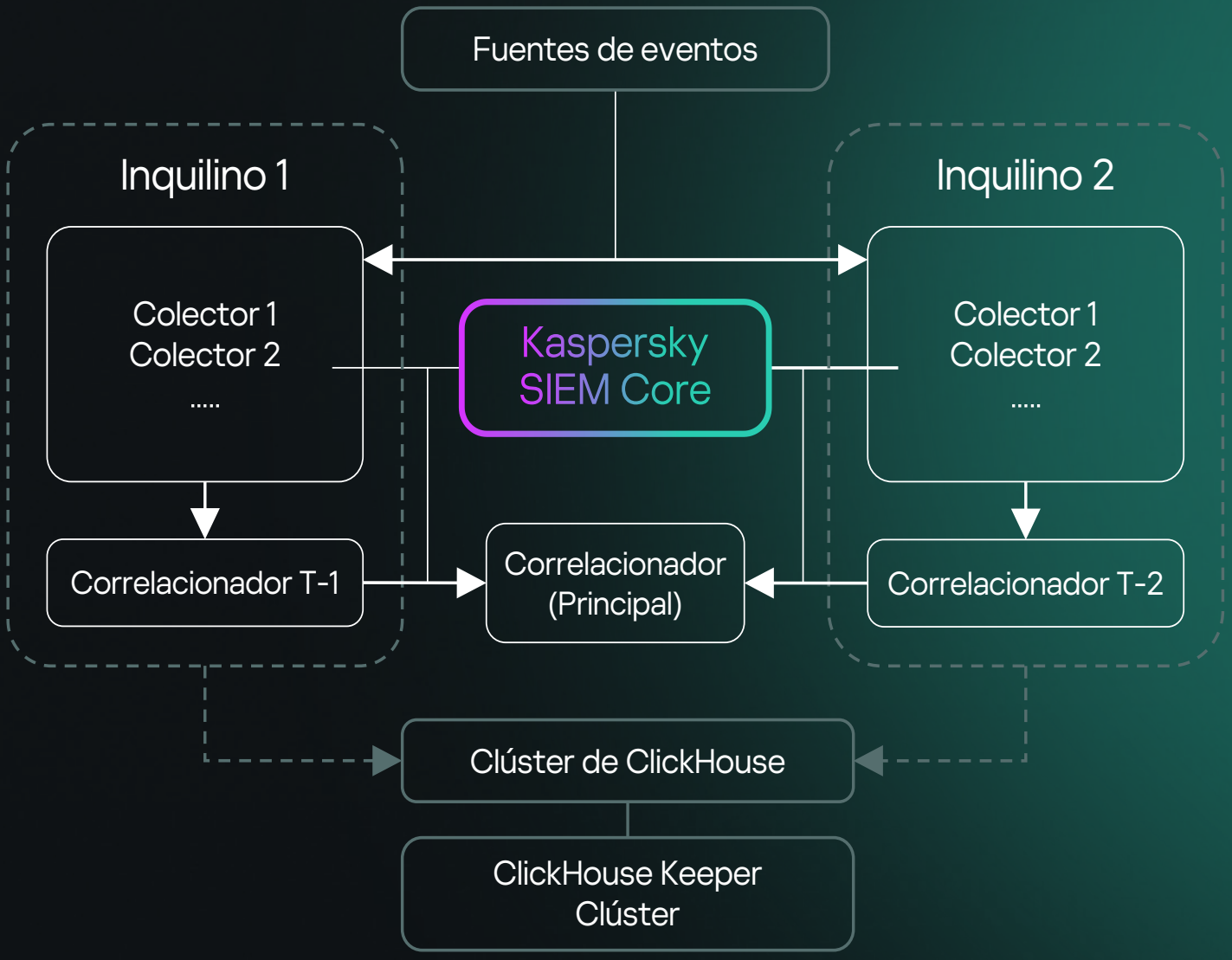
(gravedad y asignación)

- Dispositivos afectados
- Principales IP internas y externas basadas en volumen de tráfico de Netflow (BytesIn)
- Principales nodos para la administración remota (puertos 3389, 22)
- Bytes de NetFlow totales para puertos internos
- Principales fuentes basadas en la cantidad de eventos, categorías, activos y usuarios

Arquitectura de múltiples inquilinos

Kaspersky SIEM admite múltiples inquilinos, lo que significa que los usuarios de un inquilino no pueden ver los datos (eventos, alertas, incidentes, etc.) de otro inquilino. En el modo de múltiples inquilinos, una sola instancia de la aplicación Kaspersky SIEM implementada en la organización principal facilita el aislamiento de las ramificaciones para que puedan recibir y procesar sus propios eventos.

El sistema se administra centralmente a través de la interfaz principal y los inquilinos funcionan de forma independiente con acceso solo a sus propios recursos, servicios y configuraciones. Los eventos relacionados con el inquilino se almacenan por separado. Los usuarios pueden acceder a diferentes inquilinos al mismo tiempo. El administrador general también puede especificar los datos del inquilino que se mostrarán en diferentes partes de la interfaz web.



La plataforma ofrece un sistema basado en filtros para distribuir eventos en espacios. El acceso del usuario a eventos ahora se configura en el nivel del espacio. Esto permite realizar un control detallado del acceso a los eventos dentro de un único inquilino.

El sistema se administra centralmente a través de la interfaz principal mientras que los inquilinos funcionan de forma independiente y tienen acceso solo a sus propios recursos, servicios y configuraciones. Los eventos de los inquilinos se almacenan por separado.

Amplia gama de integraciones listas para usar

Kaspersky Unified Monitoring and Analysis Platform está integrada con las soluciones y tecnologías de Kaspersky para el uso coordinado de productos con eficiencia mejorada. Los proveedores externos no pueden igualar nuestro nivel de integración fluida con nuestros propios productos, lo que incluye una sola interfaz para la integración de Threat Intelligence, la capacidad de usar nuestros sensores de endpoint como agentes SIEM y mucho más.

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response *

Kaspersky Security Center

Kaspersky Secure Mail Gateway

Kaspersky Web Traffic Security

Kaspersky Threat Lookup

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Automated Security Awareness Platform

y más

La integración con la amplia cartera de servicios de **Kaspersky Threat Intelligence** permite identificar y priorizar amenazas, además de ofrecer acceso rápido a información contextual sobre nuevos ataques, indicadores de compromiso, así como tácticas y técnicas empleadas por los atacantes.

* Incluye posibles integraciones con Kaspersky Endpoint Detection and Response Expert, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Next EDR Foundations, Kaspersky Next EDR Optimum, Kaspersky Next EDR Expert

Kaspersky SIEM es experto en la recepción de datos (registros) de otros sistemas y dispositivos. Para facilitar la implementación rápida sin los gastos adicionales de configurar reglas de análisis de fuentes, la plataforma ofrece una amplia variedad de integraciones predefinidas para los productos de Kaspersky y productos de terceros:

Por dominio de seguridad

- Protección de endpoints (soluciones de EPP y EDR)
- Protección de correos electrónicos y tráfico web (protección de correos electrónicos, NDR, FW/NGFW, UTM, IDS)
- Security Awareness
- Carga de trabajo en la nube (CASB, CWPP)
- Inteligencia sobre amenazas (CTI)
- Seguridad de identidades (IAM, PAM)
- Seguridad OT/Internet de las cosas
- Prevención de pérdida de datos (DLP)

Por tipo de dato

- XML
- Syslog
- CSV
- JSON
- SQL
- CEF
- Clave-valor
- Expresiones regulares
- NetFlow v5
- NetFlow v9
- IPFIX

Por tipo de transporte

- TCP
- UDP
- NetFlow
- sFlow
- NATS JetStream
- Kafka
- HTTP
- SQL (SQLite, MSSQL, MySQL, PostgreSQL, Cockroach, Oracle, Firebird, ClickHouse, Elasticsearch)
- Archivo
- Diodo
- FTP
- NFS
- WMI
- WEC
- ETW (análisis de DNS)
- SNMP
- Capturas de SNMP
- API de VMware
- MS Office 365

El equipo de Kaspersky Professional Services o los socios pueden crear integraciones adicionales, incluido el uso de API de productos conectables. Consulte la lista completa de fuentes de eventos admitidas.

Lista completa

Por proveedor

- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilon
- Ayehu
- Barracuda Networks
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- Check Point
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- Deep Instinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- ESET
- F5 BIG-IP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion soft
- Intralinks
- Juniper Networks
- Kemp Technologies
- Kerio
- Lieberman Software
- MariaDB
- Microsoft
- MikroTik
- Minerva Labs
- NetIQ
- NETSCOUT
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto Networks
- Penta Security
- Proofpoint
- Radware
- Recorded Future
- ReversingLabs
- SailPoint
- SentinelOne
- SonicWall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro Trustwave
- VMware
- Vormetric
- WatchGuard
- Windchill FRACAS
- Zettaset
- Zscaler
- Etc.

Kaspersky Premium Support

Soporte técnico premium para Kaspersky SIEM

El soporte técnico premium de Kaspersky para Kaspersky SIEM incluye licencias Premium y Premium Plus, lo que garantiza una respuesta rápida y asistencia de alta calidad ante cualquier problema para que Kaspersky SIEM funcione a la perfección

Comunicación	Soporte estándar	Licencia Premium	Licencia Premium Plus
Cuenta de la empresa (portal web)	●	●	●
Teléfono		●	●
Correo		●	●

Servicio			
Analizadores personalizados para Kaspersky SIEM		5	10
Asistencia remota para diagnosticar problemas		●	●
Alta priorización de solicitudes de soporte		Alta	Máxima
Aplicación de parches privados			●
Administrador técnico de cuentas asignado (TAM)			●
Informes de estado de TAM			Informe trimestral

Tiempos de respuesta			
Problemas críticos	Sin SLA	2 horas (24/7)	30 minutos (24/7)
Problemas de nivel alto	Sin SLA	6 horas (8/5)	4 horas (24/7)
Problemas de nivel intermedio	Sin SLA	8 horas (8/5)	6 horas (8/5)
Problemas de nivel bajo	Sin SLA	10 horas (8/5)	8 horas (8/5)

Respuesta rápida

Las solicitudes se priorizan con SLA estrictos para lograr una resolución de problemas más rápida y confiable

Analizadores personalizados

Los analizadores personalizados permiten que SIEM procese formatos de registro únicos de sus fuentes de datos específicas

TAM dedicado

Con la licencia Premium Plus, un TAM administra todos los problemas con rendición de cuentas superior

Parches privados

Obtenga correcciones y parches personalizados, diseñados para problemas específicos, con la licencia Premium Plus

¿Por qué elegirnos?

Ahorre hasta 50 % en requisitos de instalación de virtualización o hardware y reduzca el TCO con una solución modular de alto rendimiento que supera constantemente a los proveedores SIEM tradicionales en cuanto a la rentabilidad y que puede gestionar cientos de miles de EPS en cada instancia.

Manténgase flexible con nuestras opciones de licencia. Realizamos un seguimiento del flujo promedio de EPS por día después de agregarlos y filtrarlos para limitar las saturaciones y no restringir el acceso a Kaspersky SIEM en caso de que se produzcan.

Benefíciese de la amplia variedad de integraciones de Kaspersky y de terceros, con opciones de respuesta integradas. Otros proveedores no pueden igualar nuestro nivel de integración fluida con nuestros propios productos, lo que incluye una sola interfaz para la integración de Threat Intelligence, la capacidad de usar nuestros sensores de endpoint como agentes SIEM y mucho más.

Almacene datos localmente sin compromisos, de forma rentable y sin superar el presupuesto durante un período extendido con las opciones de almacenamiento en frío y calor usando ClickHouse y el Sistema de archivos distribuido de Hadoop (HDFS) o los discos locales, mientras puede realizar búsquedas rápidas en ambas áreas al mismo tiempo.

Mejore la relevancia de los datos y acelere la detección y evaluación mediante el enriquecimiento con inteligencia sobre amenazas en los niveles táctico, operativo y estratégico, proporcionada por nuestro equipo global de investigadores y analistas a través de Kaspersky Threat Intelligence Portal.

Aproveche la arquitectura de múltiples inquilinos integrada en un MSSP y la solución para grandes empresas, que permite una compatibilidad nativa con esta arquitectura. Una única instalación de SIEM en la infraestructura principal de la organización puede crear instancias de SIEM aisladas para cada inquilino, donde estos reciben y procesan sus propios eventos.

Las empresas de todo el mundo utilizan Kaspersky Unified Monitoring and Analysis Platform para desarrollar procesos integrales de seguridad de la información que mejoran la eficiencia de la ciberseguridad.

Conozca más

Kaspersky utilizó su propio sistema SIEM para detectar malware previamente desconocido dirigido a dispositivos iOS

Mientras supervisábamos el tráfico de red de nuestra propia red Wi-Fi corporativa dedicada a los dispositivos móviles con Kaspersky Unified Monitoring and Analysis Platform, detectamos actividades sospechosas que se originaban en múltiples teléfonos con iOS.

Dado que es imposible examinar los dispositivos iOS modernos desde dentro, creamos copias de seguridad sin conexión de los dispositivos en cuestión, los examinamos usando mvt-ios del Kit de herramientas de verificación móvil y detectamos rastros de vulneración.

Apple respondió con el lanzamiento de actualizaciones de seguridad para abordar cuatro vulnerabilidades de día cero identificadas por los investigadores de Kaspersky:

CVE-2023-32434, CVE-2023-32435, CVE-2023-38606, CVE-2023-41990

Estas vulnerabilidades afectan una amplia variedad de productos Apple, incluidos iPhone, iPod, iPad, dispositivos macOS, Apple TV y Apple Watch. Kaspersky también informó a Apple sobre el aprovechamiento de una función de hardware, que la empresa mitigó posteriormente.

¿Por qué Kaspersky?

Kaspersky SIEM saca provecho de años de conocimientos acumulados y habilidades refinadas de los 5 Centros de Experiencia.

Conozca más

27

Desarrollamos herramientas y brindamos servicios desde hace **más de 27 años** para mantener su seguridad con nuestras tecnologías más probadas y más premiadas.

Conozca más

Somos una **empresa de ciberseguridad privada internacional** con miles de clientes y socios en todo el mundo y nos comprometemos a ser transparentes e independientes.

Conozca más

Kaspersky Unified Monitoring and Analysis Platform

Conozca más

latam.kaspersky.com

#kaspersky
#bringonthefuture