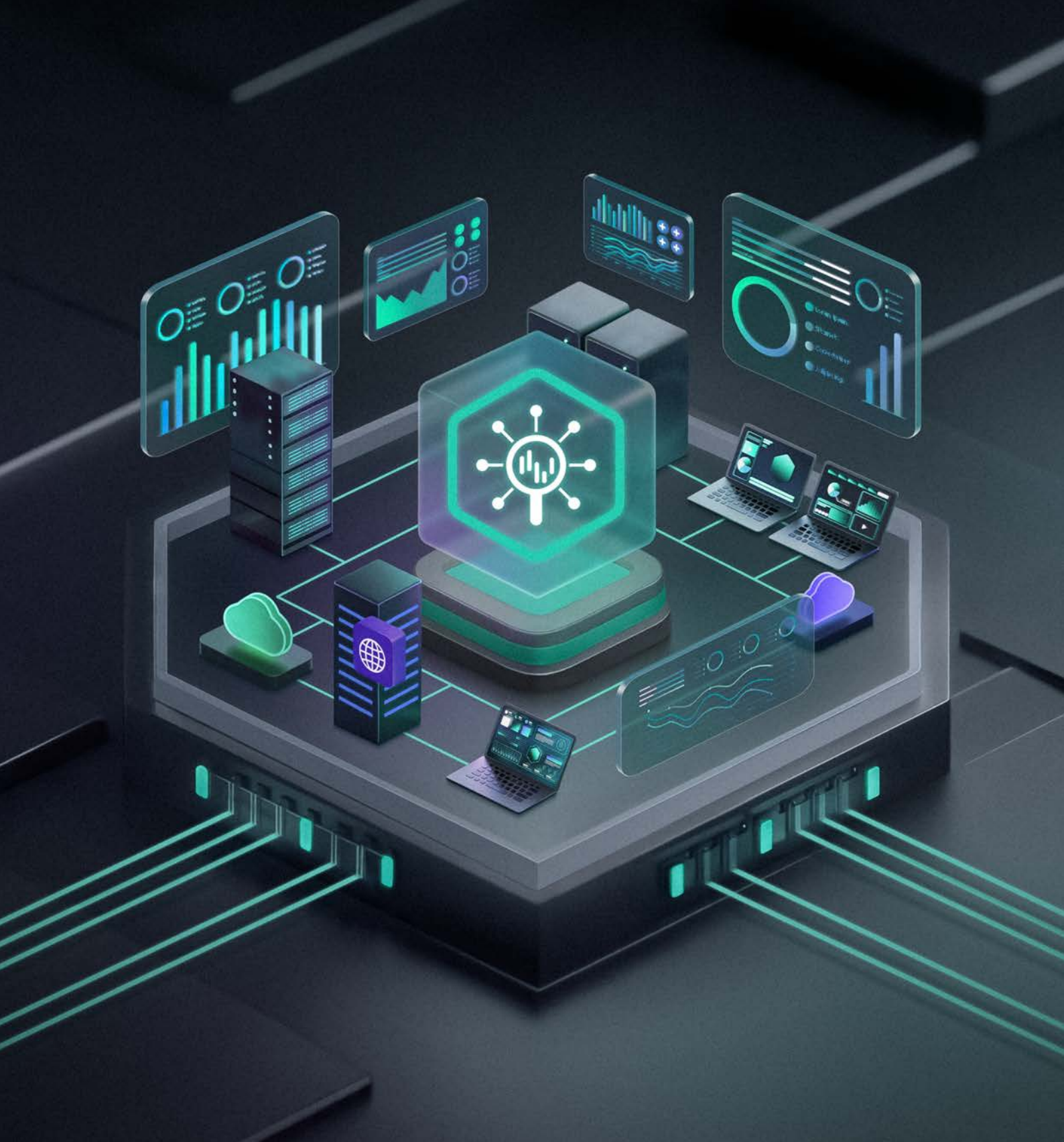


Datasheet

Kaspersky SIEM

Revolucione suas operações de segurança com nossa solução de última geração, orientada por IA e aprimorada com inteligência de ameaças de primeiro mundo

kaspersky bring on the future

O Kaspersky SIEM foi projetado para organizações com infraestruturas de TI complexas, alto volume de transação de dados e exigências regulatórias rigorosas. O produto é ideal para MSSP com suporte multitenancy integrado.

Essas organizações entendem que segurança eficaz vai muito além da prevenção: depende da capacidade de detectar, analisar e responder a ameaças em tempo real nos mais diversos sistemas.

Maximize o impacto das suas operações de segurança

Organizações de grande porte enfrentam um volume crescente de Ameaças Persistente Avançadas (APT). Em 2024, foram detectadas APTs em uma de nossas quatro empresas e esses ataques corresponderam a 43% de todos os incidentes de máxima gravidade[1]. As consequências foram onerosas, desde interrupção dos negócios a prejuízos financeiros e comprometimento da reputação em longo prazo.

As equipes de segurança operam sobre uma pressão sem precedentes. Sistemas de proteção geram volumes gigantescos de dados, elevando os custos de armazenamento e encarecendo a implementação de SIEM. Especialistas altamente capacitados são raros, enquanto as equipes atuantes encontram-se sobrecarregadas: 70% dos Centros de Operação de Segurança (SOC) lutam para manter os ambientes tranquilos diante da enxurrada de alertas[2]. Além disso, a complexidade da administração dos sistemas de SIEM complica ainda mais a situação dos recursos limitados.

Até mesmo os Centros de Operação de Segurança mais experientes correm o risco de perder eficiência e impacto sem as ferramentas orientadas por IA atuais, que os ajudam a reduzir a saturação e focar no que realmente interessa.

Equipe seu pessoal com um SIEM orientado por IA, desenvolvido com inteligência de ameaças de primeiro mundo.

O Kaspersky SIEM é uma solução de última geração, projetado para ajudar sua equipe de segurança a gerenciar e analisar o influxo de dados de segurança. O produto é eficaz para:

- Coleta, processamento e armazenamento de eventos de diversas fontes, incluindo de produtos Kaspersky, sistemas operacionais, aplicativos de terceiros, ferramentas de segurança e bancos de dados.
- Analisar e correlacionar o influxo de dados em tempo real, enriquecendo as informações com inteligência de ameaças líder de mercado para detectar atividades suspeitas.
- Fornecimento de alertas em tempo hábil que possibilitam a investigação e reposta rápidas a incidentes.
- Armazenar dados para um período prolongado sem ultrapassar o orçamento com hardware oneroso. Graças a opções de armazenamento frio e quente e funcionalidade de pesquisa simultânea.

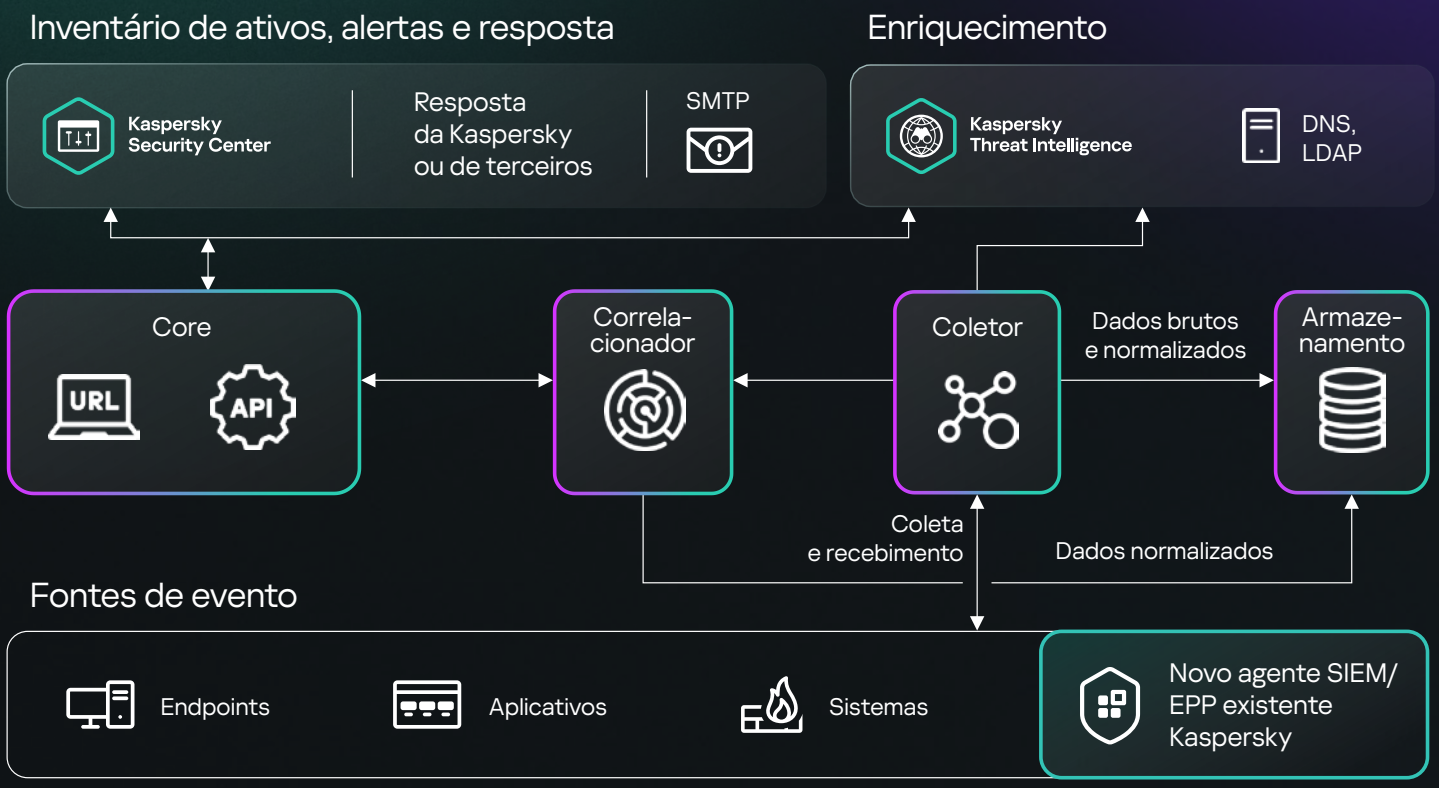
Ao unificar logs de fontes de segurança e correlacioná-los em tempo real, o Kaspersky SIEM capacita seus analistas com a visibilidade completa e contexto necessário para responder a ameaças com eficiência.

A solução oferece pesquisa avançada e recursos analíticos que permitem a você caçar ameaças para revelar perigos previamente desconhecidos. A análise de dados históricos e a parametrização estatística com conjunto de regras de detecção UEBA ajudam sua equipe a identificar anomalias e deter ataques sofisticados.

Com Kaspersky SIEM, seu SOC obtém a visibilidade, inteligência e eficiência necessárias para transformar uma quantidade maciça de dados em informações de segurança utilizáveis. A solução pode operar sem conectividade com a internet, garantindo a soberania completa de dados.

1 Relatório de Análise de Detecção e resposta gerenciada para 2024
2 Relatório Kaspersky: O retrato do profissional moderno de segurança da informação, 2024

Como funciona



Graças à arquitetura de microsserviços da solução, os administradores podem criar e configurar os microsserviços de que precisam para usar o Kaspersky SIEM como uma ferramenta SIEM completa ou um sistema de gerenciamento de logs.

O Kaspersky SIEM é projetado em uma única plataforma de gerenciamento open source[3], integrando ambos os produtos Kasperky e de terceiros em um sistema de segurança centralizado. A solução é parte essencial de uma estratégia de defesa abrangente, protegendo ambientes corporativos e industriais e detectando ciberataques que migram de sistemas de TI para sistemas OT.

O diferencial do Kaspersky SIEM

Máximo de desempenho, mínimo de custos

Diminua os custos de hardware e de virtualização em até 50% e reduza o TCO com um SIEM modular de alto desempenho que é superior a soluções ultrapassadas e trata de centenas de milhares de EPS por instância

Um ecossistema Kaspersky integrado

Tire proveito de mais de 200 integrações Kaspersky e de terceiros pré-configuradas com opções de resposta integradas. Nosso ecossistema oferece uma interface única para inteligência de ameaças, usa sensores de endpoints como agentes SIEM e fornece recursos de integração imbatíveis no mercado.

Experiência em SOC integrado

Obtenha acesso a mais de 700 regras de detecção pré-configuradas, atualizadas trimestralmente com mapeamento MITRE e orientação a resposta, tudo desenvolvido pelo Kaspersky SOC, uma das equipes de busca por ameaças mais experientes do setor.

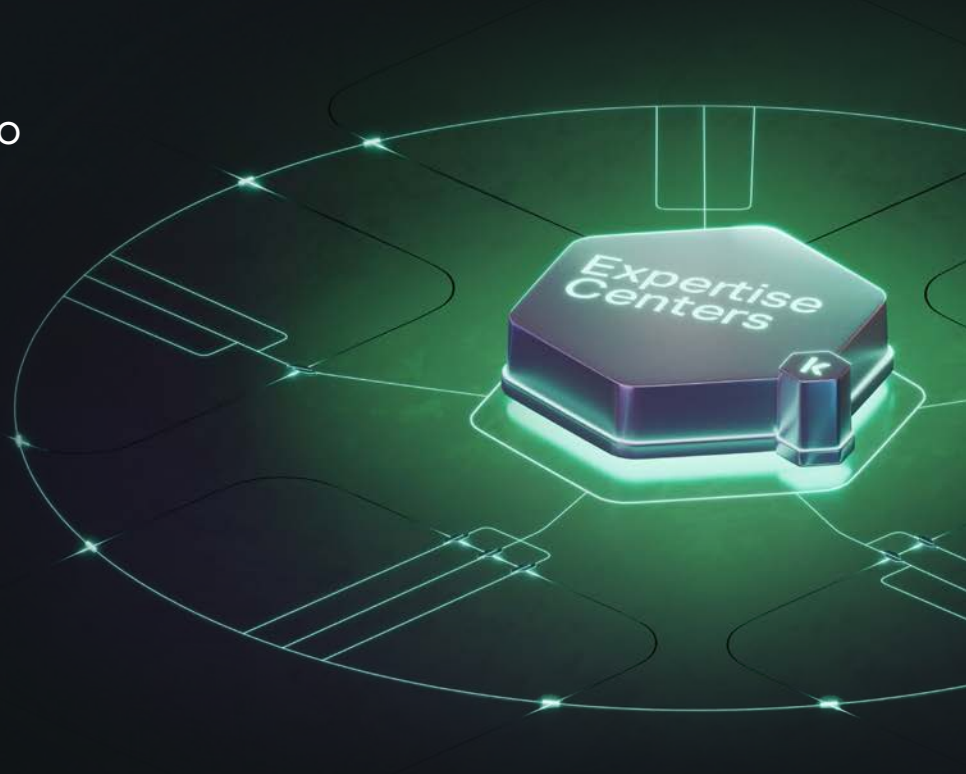
Detecção/soluções de ameaças com IA

Componentes aprimorados por IA identificam rapidamente atividades suspeitas em toda a sua infraestrutura, com detecção de IA para sequestro de DLL, pontuação de risco baseada em IA para ativos e muito mais. Esses recursos melhoram a precisão de detecção, reduzem falsos positivos e minimizam o impacto de incidentes cibernéticos, ajudando a aprimorar seus tempos de resposta MTTD e MTTR.

3 O Kaspersky Next XDR Expert, desenvolvido nessa plataforma, recursos estendidos com caça a ameaças avançadas, roteiros de ação automatizados e gerenciamento de casos otimizado.

O Kaspersky SIEM tira proveito de anos de conhecimento acumulado e habilidades sofisticadas do Kaspersky Expertise Centers, com cinco hubs especializados unificados para uma cibersegurança avançada.

Saiba mais



O Kaspersky SIEM conta com um suporte 24 horas e serviços premium, incluindo integrações personalizadas fornecidas pelo Kaspersky Professional Services ou parceiros de confiança, tirando proveito de recursos API de producos conectados.

Fornecemos implementação turnkey, suporte para migração impecável e expertise contínua para garantir que você obtenha o máximo valor da sua implementação SIEM.

Kaspersky SIEM

www.kaspersky.com.br

Saiba mais

#kaspersky
#bringonthefuture