Documento Técnico
do Produto

Kaspersky SIEM

kaspersky bring on the future

Conteúdo

Mercado de Gerenciamento de Informações e Eventos de Segurança

Líderes de cibersegurança em organizações enfrentam inúmeros desafios, incluindo um número crescente de tentativas de penetrar em sua infraestrutura, escassez de pessoal de cibersegurança e ataques cada vez mais complexos.

Além disso, as organizações devem cumprir os requisitos regulatórios relacionados à retenção de dados, auditoria e investigação de incidentes, o que impacta o mercado global de SIEM.

As organizações também estão sob pressão para separar os alertas de ciberataques por prioridade e triá-los de forma mais eficiente devido ao seu crescimento e aumento de complexidade.

Além disso, as condições de trabalho remoto levaram as empresas a adotar aplicativos SaaS e permitir que os funcionários tragam seus próprios dispositivos (BYOD), destacando a necessidade de estender a visibilidade da rede além do perímetro tradicional.

Finalmente, encontrar especialistas qualificados em segurança da informação é um desafio no mercado atual. As empresas estão procurando maneiras de otimizar seus recursos e melhorar a eficiência da cibersegurança. Consequentemente, as organizações desejam dados de inteligência facilmente acessíveis e acionáveis para suas equipes de SOC.

De acordo com o Relatório Kaspersky Human Factor 360.

77%

das empresas sofreram pelo menos uma violação de segurança cibernética, sendo que muitas enfrentaram até seis nesse período.

41%

das empresas percebem que têm falhas nas suas infraestruturas de segurança e planejam fazer mais investimentos nesta área no futuro.

Saiba mais

Sobre o Kaspersky SIEM e sua arquitetura

A Kaspersky Unified Monitoring and Analysis Platform é uma solução SIEM integrada de última geração para gerenciamento de dados e eventos de segurança. Ele se destaca em receber, processar e armazenar eventos de informações de segurança, e analisar e correlacionar os dados recebidos. A plataforma também possui um recurso de busca, gera alertas quando ameaças potenciais são detectadas e suporta respostas automatizadas aos alertas gerados e à caça de ameaças.

Alta performance arquiteturamodular permite processar centenas de milhares de eventos por segundo (EPS) em cada instância e reduzir o custo total de propriedade (TCO) otimizando os requisitos do sistema.

Ao incorporar produtos de terceiros e da Kaspersky em um sistema centralizado de segurança da informação, o Kaspersky SIEM é uma parte essencial de uma estratégia de defesa abrangente capaz de proteger ambientes corporativos e industriais, além de detectar ciberataques que começam em sistemas de TI e passam para sistemas de OT.

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

A solução recebe eventos de segurança de várias fontes, incluindo produtos da Kaspersky, sistemas operacionais, aplicativos de terceiros, ferramentas de segurança e vários bancos de dados, correlaciona os eventos entre si e os enriquece com dados de feeds de inteligência de ameaças para identificar atividades suspeitas nas infraestruturas de rede corporativa e fornecer notificação oportuna de incidentes de segurança.

Ao coletar registros de todos os controles de segurança e fazer a correlação dos dados em tempo real, o **Kaspersky SIEM reúne e proporciona toda a informação necessária para examinar e responder ao incidente.**

Além disso, o Kaspersky SIEM permite que os caçadores de ameaças descubram ameaças previamente desconhecidas, permitindo que os operadores analisem e correlacionem dados históricos, além de estabelecer bases estatísticas para identificar anomalias.

A plataforma unificada de monitoramento e análise da Kaspersky inclui os seguintes componentes:

Um **Core** com uma interface gráfica centralizada para controlar e monitorar as configurações dos componentes do sistema. A plataforma pode ser acessada por meio de soluções de terceiros usando a API.

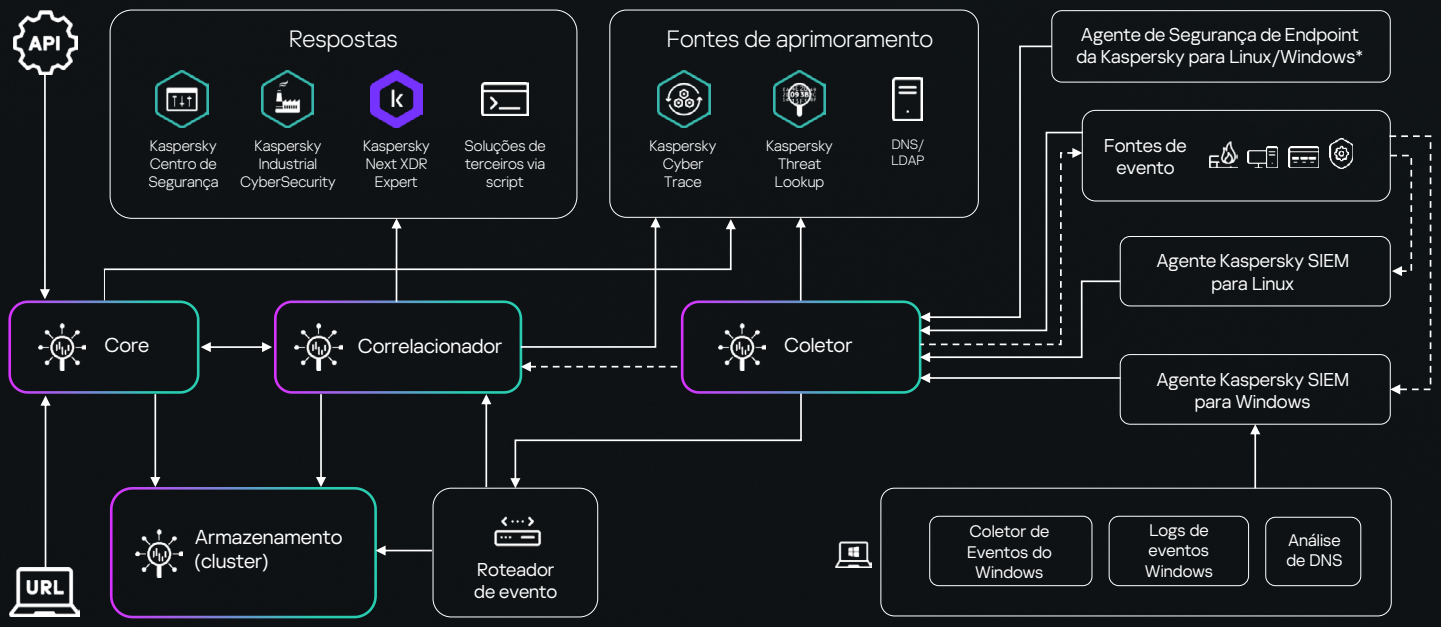
As regras de correlação são usadas para detectar sequências específicas de eventos processados e tomar certas ações após o reconhecimento, como criar eventos/alertas de correlação ou interagir com uma lista ativa. O **Correlator** utiliza listas ativas para realizar ações necessárias após analisar eventos normalizados recebidos dos coletores e gera alertas com base em critérios de correlação.

Um ou mais **Coletores** recebem eventos de fontes externas e os pré-processam: normalizam (alteram para um único formato), filtram, agregam e enriquecem com dados de fontes externas usando dicionários, chamadas para o serviço de DNS e outras ferramentas.

O armazenamento é usado para armazenar eventos normalizados para que possam ser rapidamente e continuamente acessados a partir do SIEM para extrair dados analíticos.

Agentes encaminham eventos brutos de estações de trabalho e servidores para coletores SIEM. O envio de eventos de log do Windows diretamente para o coletor agora é possível no Kaspersky Endpoint Security for Windows 12.6 ou Linux 12.2. Isso reduz significativamente a quantidade de trabalho necessária para integrar fontes de eventos com o sistema SIEM da Kaspersky.

Roteadores de eventos reduzem a carga nos links e o número de portas abertas nos firewalls ao receberem eventos de forma constante e sem atrasos quando os coletores são instalados em escritórios remotos com baixa largura de banda ou links de dados que já estão ocupados.



Funcionalidade do Kaspersky SIEM

Conectores integrados e personalizados para centenas de fontes da Kaspersky e de fornecedores terceirizados, com atualizações e melhorias regulares.

Integração de fontes de eventos externos com criação livre de conectores adicionais pela equipe de Serviços Profissionais da Kaspersky.

Consultas de pesquisa rápidas e relatórios prontos sobre eventos de segurança.

Armazenamento seguro local de logs para conformidade regulatória e investigação de incidentes.

O Kaspersky SIEM suporta pesquisas de eventos em vários armazenamentos para ajudar os operadores a encontrar eventos relevantes em clusters de armazenamento distribuídos de forma mais rápida e fácil.

Monitorar, processar e armazenar informações sobre eventos de segurança

A plataforma unificada de monitoramento e análise da Kaspersky recebe eventos de logs e normaliza dados de diferentes fontes de eventos para torná-los consistentes. Esses eventos de segurança da informação podem incluir tentativas de login, interações com bancos de dados ou transmissões de informações de sensores e são coletados de toda a infraestrutura de TI protegida da empresa. Embora um evento individual possa não parecer significativo, considerados em conjunto, múltiplos eventos isolados pintam um quadro maiorde atividade maliciosa que pode ser usada para identificar problemas de segurança.

O data lake, nosso repositório local centralizado, fornece uma plataforma para coletar, indexar e analisar logs de várias fontes, incluindo soluções de segurança (EPP, FW, IAM, etc.), sistemas operacionais, aplicativos de negócios (sistemas de RH, ferramentas de escritório), sistemas de segurança física (sistemas automatizados de controle de acesso) e outros dispositivos.

Os eventos são transmitidos para o correlacionador para análise e armazenamento para retenção, uma vez que foram filtrados e agregados. Para identificar alertas, o coletor recebe eventos de fontes, os processa e os encaminha para armazenamento, correlacionador e/ou serviços de terceiros. Eventos brutos são encaminhados de estações de trabalho e servidores para coletores de SIEM (em certos casos por agentes) e podem ser enviados para outros sistemas para análise adicional.

Eventos de correlação são produzidos pela solução após o reconhecimento de um evento específico ou de uma série de eventos relacionados, e também são analisados e retidos. Se um evento ou sequência de eventos indicar uma ameaça potencial à segurança, o Kaspersky SIEM gera um alerta com informações sobre a ameaça e quaisquer outras informações relevantes que os especialistas em segurança precisam considerar.

Protocolos de transporte confiáveis, com criptografia opcional, são usados para transferir eventos entre componentes. Um data diode pode ser usado pelo sistema para coletar dados de segmentos isolados.

O Kaspersky SIEM permite a gestão centralizada de ativos ao fornecer um amplo inventário de servidores, estações de trabalho e dispositivos de rede. A plataforma pode coletar dados sobre vulnerabilidades de ativos de fontes como scanners de vulnerabilidades e correlacioná-los com dados de categoria de ativos para identificar ameaças. Isso fornece às equipes de segurança visibilidade completa do cenário de ativos.

Para apoiar os analistas, a cobertura da matriz MITRE ATT&CK por regras é exibida para avaliar melhor o nível de segurança.

Mais de 650 regras de correlação pré-configuradas para detectar cenários de ataque regularmente atualizadas pelos servidores da Kaspersky com mapeamento MITRE e recomendações de resposta.

Melhoria da relevância dos dados por meio do enriquecimento com dados analíticos coletados do Portal do Kaspersky Threat Intelligence (usando Kaspersky Threat Lookup e Kaspersky CyberTrace).

Os dados sobre ativos e infraestrutura são coletados do Kaspersky Security Center e de fontes de terceiros.

Os usuários podem comparar um evento com valores agrupados, agregados, médios, máximos e mínimos para um período de tempo específico usando a funcionalidade de mineração de dados do ClickHouse. Isso expande significativamente as capacidades da lógica de detecção sem exigir a criação de inúmeras regras de serviço.

Para facilitar a criação e edição de conteúdo, permitimos que os usuários descubram antecipadamente a quais regras de correlação a alteração pretendida se aplicará antes de fazer quaisquer alterações nos critérios de filtro.

Correlação em tempo real e histórica de eventos de segurança

O Kaspersky SIEM realiza a correlação cruzada quase em tempo real usando regras personalizadas para identificar ataques e ameaças, além de centenas de regras predefinidas desenvolvidas pelo Kaspersky SOC, uma das equipes de caça a ameaças mais bem-sucedidas e experientes do setor. Os especialistas do SOC da Kaspersky possuem inúmeros certificados que confirmam seu alto nível de expertise e conhecimento.

Os eventos estão **correlacionados em tempo real**. O correlacionador analisa eventos normalizados, cria alertas de acordo com as regras de correlação e gerencia todas as operações de listas ativas.

O princípio de funcionamento do correlacionador é baseado na análise da assinatura do evento, o que significa que cada evento é tratado de acordo com as regras de correlação especificadas pelo usuário. O software gera um evento de correlação e o envia para armazenamento quando encontra uma série de eventos que atendem aos requisitos da regra de correlação. O usuário pode personalizar as regras de correlação para serem acionadas pelos resultados de uma análise anterior, enviando o evento de correlação para o correlacionador para análise adicional. As saídas da regra de correlação podem ser utilizadas por outras regras de correlação. Por exemplo, vários alertas menores podem gerar um alerta maior (várias tentativas de força bruta podem ser analisadas para descobrir um incidente de força bruta em massa).

A plataforma utiliza dados históricos para identificar tendências, encontrar ameaças que antes não eram identificadas e apontar ataques que foram ignorados por certos elementos de segurança, tudo isso melhora a detecção geral de ameaças.

Soluções de terceiros ou produtos integrados como **Kaspersky EndpointDetection and Response** realizam a detecção no lado do sensor. Ao ajustar as configurações do produto, os usuários podem controlar esse processo e obter eventos e telemetria que esses produtos já processaram por meio de sua própria lógica de detecção.

O mecanismo de correlação da solução incorpora detecção no lado da plataforma. Graças ao poderoso mecanismo de correlação da plataforma, os usuários podem criar regras de correlação adaptáveis. Regras prontas e pacotes normalizadores também estão disponíveis para dar suporte a produtos de terceiros comercialmente acessíveis que estão em constante expansão e atualização.

O princípio de funcionamento do correlacionador é baseado na análise da assinatura do evento, o que significa que cada evento é tratado de acordo com as regras de correlação especificadas pelo usuário. O software gera um evento de correlação e o envia para armazenamento quando encontra uma série de eventos que atendem aos requisitos da regra de correlação.

Caça a ameaças para descobrir ameaças previamente desconhecidas, permitindo que os operadores analisem e correlacionem dados históricos usando um poderoso banco de dados orientado a colunas.

Os usuários podem facilmente localizar filtros, dicionários e regras que estão todos unificados por uma única tag usando a função de busca baseada em tags. Armazenar o histórico de consultas de pesquisa permite que o usuário acesse consultas anteriores com facilidade.

A plataforma pode armazenar dados por um longo período sem exceder o orçamento para hardware de armazenamento caro, graças às opções de armazenamento quente e frio usando ClickHouse e o Sistema de Arquivos Distribuído Hadoop (HDFS) ou discos locais.

Os administradores podem evitar problemas de espaço no subsistema de disco usando configurações flexíveis: a profundidade do armazenamento de eventos pode ser definida em gigabytes como uma porcentagem do espaço em disco, além de dias.

Kaspersky Next XDR Expert

Uma ampla gama de capacidades de resposta por meio de playbooks está disponível com o Kaspersky Next XDR Expert.

Saiba mais

Armazenamento de dados de eventos de segurança

O componente de armazenamento do Kaspersky SIEM é usado para armazenar eventos normalizados, a fim de acessar rapidamente e continuamente dados analíticos da **Plataforma Unificada de Monitoramento e Análise da Kaspersky**.

ClickHouse garante continuidade e velocidade de acesso. O armazenamento está conectado a um serviço de armazenamento Kaspersky SIEM via um cluster ClickHouse. Discos de armazenamento a frio também podem ser adicionados a clusters do ClickHouse.

Os usuários podem adicionar espaço em repositórios para agrupar eventos armazenados com base em um atributo específico. Isso permite que os administradores definam diferentes tempos de armazenamento para eventos com base em suas características específicas.

A plataforma de Monitoramento e Análise Unificada da Kaspersky também lida com a compressão de dados para reduzir drasticamente o uso do espaço em disco sem comprometer a recuperação de dados. A solução da Kaspersky suporta duas áreas: uma para recuperação rápida de dados e outra para armazenar uma grande quantidade de dados.

A plataforma tem duas seções distintas: uma para armazenamento a frio que pode ser realizado no Hadoop Distributed File System ou em discos locais, e a outra para armazenamento operacional usando o ClickHouse. Essa separação é transparente para os usuários.

Sem precisar alternar entre arquivos, os operadores podem criar consultas de pesquisa em uma única interface e concentrar todos os esforços na investigação. Isso **reduz o custo total de propriedade do sistema** mantendo uma excelente experiência do usuário. A plataforma suporta buscas de eventos em vários armazenamentos para ajudar os operadores a encontrar eventos relevantes em clusters de armazenamento distribuído de forma mais rápida e fácil.

As organizações podem permanecer em conformidade com os requisitos regulatórios para retenção de dados, auditoria e investigação de incidentes, coletando e armazenando de forma segura logs de uma variedade de fontes. Além disso, o armazenamento centralizado e estruturado facilita para as empresas recuperar e analisar logs conforme necessário.

Capacidades de resposta adequadas

A funcionalidade de resposta integrada usando produtos Kaspersky aumenta a eficiência da segurança. Por exemplo, para ampliar as capacidades de resposta do endpoint, o Kaspersky SIEM pode ser combinado com o Kaspersky Endpoint Detection and Response para gerenciar o isolamento de ativos na rede e regras de prevenção ou executar aplicativos e scripts. Essas ações de resposta podem ser realizadas manualmente ou automaticamente em ativos com o agente Kaspersky Endpoint Security.

A coleta automatizada de informações de inventário (software instalado, vulnerabilidades, equipamentos, proprietários de ativos, etc.) pode ajudar a contextualizar eventos de segurança da informação e auxiliar nas investigações de incidentes.

O Kaspersky SIEM utiliza o Kaspersky CyberTrace, uma plataforma de inteligência de ameaças completa que suporta dezenas de feeds de dados de ameaças prontos para uso (comerciais e públicos) para transmitir automaticamente o enriquecimento de eventos em tempo real com informações contextuais sobre indicadores de comprometimento.

Os componentes de inteligência artificial do Kaspersky SIEM permitem a detecção rápida de atividades suspeitas na infraestrutura

Ferramentas de inteligência artificial e aprendizado de máquina

A Kaspersky utiliza algoritmos preditivos, técnicas de agrupamento, redes neurais, técnicas de modelagem estatística e algoritmos especializados para aumentar a eficácia de nossos produtos na detecção mais rápida de ameaças e na priorização precisa das detecções.

As equipes de monitoramento e resposta podem priorizar alertas e focar na prevenção de danos potenciais, verificados por sistemas de big data e inteligência artificial. O módulo de IA ajuda na triagem, analisando dados históricos, priorizando alertas recebidos e fornecendo pontuações de risco baseadas em IA para ativos. Esta abordagem ajuda a gerar hipóteses valiosas que podem ser usadas para buscas proativas.

A plataforma utiliza regras de correlação definidas pelo usuário para vincular eventos em tempo real. Seu módulo de correlação aplica algoritmos de inteligência artificial para detectar atividades anômalas, como picos repentinos de tráfego ou múltiplos acessos ao serviço, sinalizando um incidente potencial e permitindo a detecção precoce antes que ocorram danos.

O Kaspersky SIEM também incorpora dados da Kaspersky Threat Intelligence, gerados usando tecnologias de IA e big data. O banco de dados é continuamente enriquecido com os resultados da análise manual de APT, dados operacionais da Darknet, informações do Kaspersky Security Network e insights da análise regular de novos malwares.

Todas essas tecnologias ajudam os usuários a minimizar danos potenciais causados por incidentes cibernéticos e aumentar o MTTR e MTTD.

Excelente visualização com painéis e relatórios apresenta dados nos formatos mais utilizáveis para identificar tendências, padrões e eventos anômalos.

Com widgets personalizáveis para a fácil visualização e exibição de indicadores, os analistas podem priorizar incidentes, determinar causas raiz e responder a ameaças de forma mais eficiente, enquanto as organizações podem acompanhar a eficácia de suas operações de segurança, identificar tendências e avaliar a saúde geral de seu sistema de segurança.

Os usuários podem enriquecer os dados do campo do evento com conteúdos de dicionários, tabelas, ativos e atributos da conta e usar esses dados para pesquisa e visualização. Isso ajuda a criar painéis e relatórios com mais dados contextuais.

Esta solução ajuda os usuários a criar seus próprios widgets com configurações ajustáveis, bem como layouts com **vários grupos de widgets:**

Principais métricas de alerta

(gravidade, prioridade e status)

- Ativos afetados.
- Notificações recentes
- Principais fontes de dados com o maior número de alertas
- Alertas atribuídos a operadores específicos
- Usuários e/ou dispositivos afetados
- Alertas por política

Indicadores-chave de incidentes

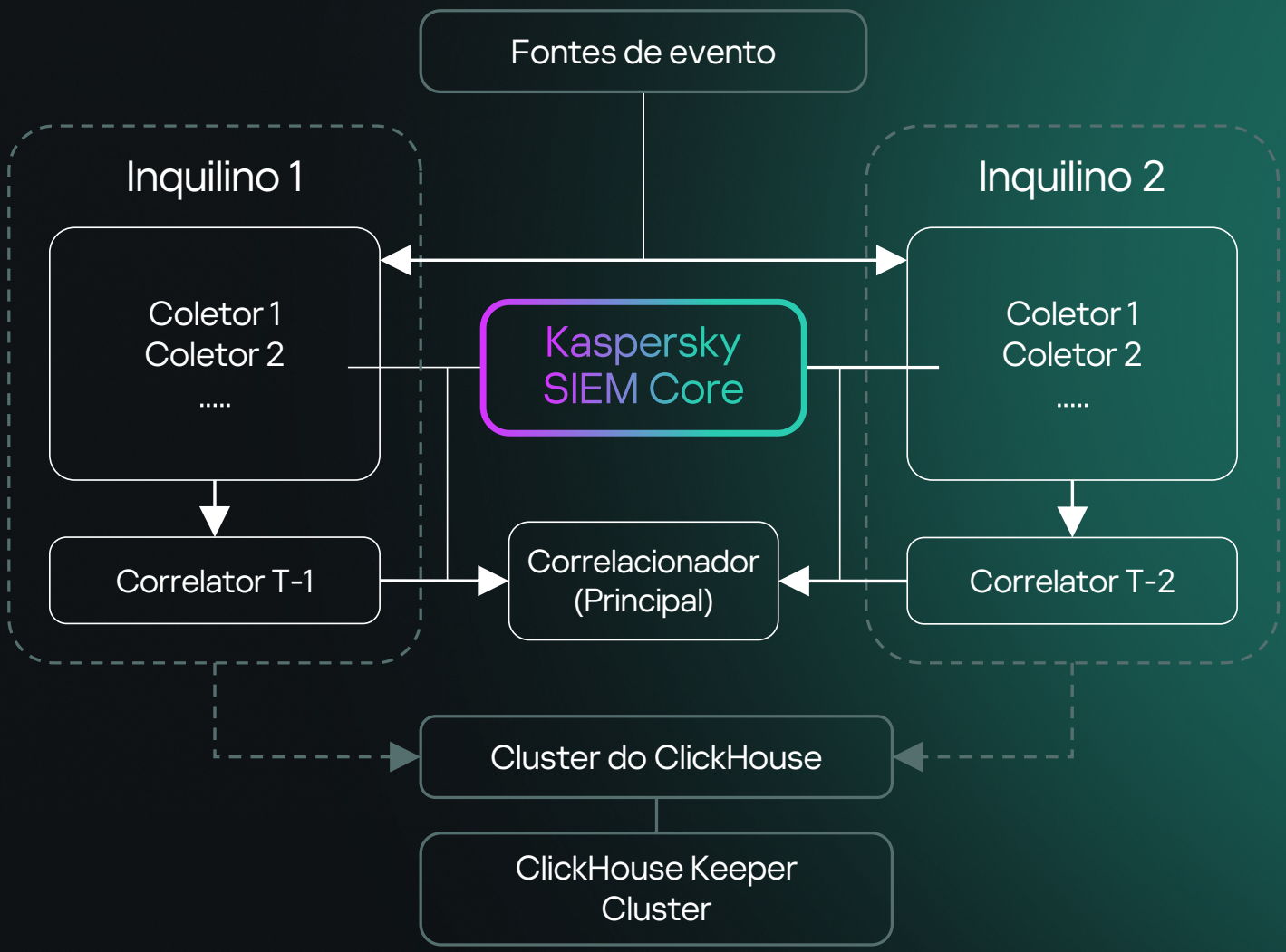
(gravidade e atribuição)

- Dispositivos afetados
- Principal IP interno e externo pelo Netflow Traffic Volume (BytesIn).
- Principais nós para gerenciamento remoto (portas 3389, 22)
- Total de bytes do NetFlow para portas internas
- Principais fontes com base no número de eventos, categorias, ativos e usuários

Arquitetura de multi-locação

O Kaspersky SIEM oferece suporte completo a multi-inquilinos, o que significa que os usuários de um inquilino não podem ver os dados (eventos, alertas, incidentes etc.) de outro inquilino. No modo de multilocação, uma única instância da aplicação Kaspersky SIEM implantada na organização principal permite isolar as filiais para que recebam e processem seus próprios eventos.

O sistema é administrado de forma centralizada por meio da interface principal, e os inquilinos operam de forma independente, tendo acesso apenas aos seus próprios recursos, serviços e configurações. Eventos relacionados ao inquilino são armazenados separadamente. Os usuários podem acessar vários inquilinos simultaneamente. O administrador geral também pode especificar quais dados do inquilino serão exibidos em diferentes partes da interface da web.



A plataforma oferece um sistema baseado em filtros para distribuir eventos para espaços. O acesso do usuário aos eventos agora é definido no nível do espaço. Isso permite o controle granular de acesso a eventos dentro de um único locatário.

O sistema é gerenciado centralmente por meio da interface principal, enquanto os inquilinos operam independentemente uns dos outros e têm acesso apenas aos seus próprios recursos, serviços e configurações. Os eventos dos inquilinos são armazenados separadamente.

Ampla gama de integrações prontas para uso

A plataforma unificada de monitoramento e análise da Kaspersky está totalmente integrada às soluções e tecnologias da Kaspersky para o uso coordenado de produtos com eficiência aprimorada. Fornecedores terceirizados não conseguem igualar nosso nível de integração perfeita com nossos próprios produtos, que inclui uma única interface para integração de Inteligência de Ameaças, a capacidade de usar nossos sensores de endpoint como agentes SIEM e muito mais.

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

e outros

A integração com o rico portfólio de serviços do **Kaspersky Threat Intelligence** ajuda a identificar e priorizar ameaças e obter acesso rápido a informações contextuais sobre novos ataques, indicadores de comprometimento e táticas e técnicas de atacantes.

* Inclui possíveis integrações com Kaspersky Endpoint Detection and Response Expert, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Next EDR Foundations, Kaspersky Next EDR Optimum, Kaspersky Next EDR Expert

O Kaspersky SIEM se destaca na recepção de dados (logs) de outros sistemas e dispositivos. Para facilitar a implementação rápida sem o custo adicional de configurar regras de análise de origem, a plataforma vem com uma ampla gama de integrações prontas para uso para produtos da Kaspersky e produtos de terceiros.

Por domínio de segurança

- Proteção de Endpoint (soluções EPP e EDR)
- Proteção de tráfego de e-mail e web (proteção de e-mail, NDR, FW/NGFW, UTM, IDS)
- Conscientização sobre segurança
- Carga de trabalho na nuvem (CASB, CWPP)
- Inteligência contra Ciberameaças (CTI)
- Segurança de Identidade (IAM, PAM)
- Segurança de TO/IoT
- Prevenção contra perda de dados (DLP)

Por tipo de dados

- XML
- Syslog
- CSV
- JSON
- SQL
- CEF
- Utilidades principais
- Expressão Regular
- 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)
- Arquivo
- Diode
- FTP
- NFS
- WMI
- WEC
- ETW (análise de DNS)
- SNMP
- SNMP Traps
- VmWare API
- MS Office 365

Integrações adicionais podem ser desenvolvidas pela equipe da Kaspersky Professional Services ou por parceiros, incluindo o uso das APIs de produtos conectáveis. Veja a lista completa de fontes de eventos suportadas.

Lista completa

Por fornecedor

- 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
- Nexo
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto Networks
- Penta Security
- Proofpoint
- Radware
- Futuro Gravado
- ReversingLabs
- SailPoint
- SentinelOne
- SonicWall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro Trustwave
- VMware
- Vormetric
- WatchGuard
- Windchill FRACAS
- Zettaset
- Zscaler
- etc.

Kaspersky Premium Support

Suporte Premium para Kaspersky SIEM

O Suporte Premium do Kaspersky para o Kaspersky SIEM vem com licenças Premium e Premium Plus, garantindo uma resposta rápida e assistência de alta qualidade para quaisquer problemas para manter o seu Kaspersky SIEM funcionando sem problemas.

Comunicação	Suporte padrão	Licença premium	Licença Premium Plus
Conta da Empresa (portal web)	●	●	●
Telefone		●	●
E-mail		●	●

Serviço			
Identificadores personalizados para o Kaspersky SIEM		5	10
Assistência remota para diagnosticar problemas		●	●
Aumento da prioridade para solicitação de suporte		Alto	Mais alta
Patching privado			●
Gerente Dedicado de Contas Técnicas (TAM)			●
Relatórios de status da TAM			Relatório trimestral

Tempos de resposta			
Questões críticas	Sem SLA	2 horas (24/7)	30 minutos (24 horas por dia, 7 dias por semana)
Questões de alto nível	Sem SLA	6 horas (8/5)	4 horas - 24 horas por dia, 7 dias por semana
Questões de nível médio	Sem SLA	8 horas (8/5)	6 horas (8/5)
Questões de baixo nível	Sem SLA	10 horas (8/5)	8 horas (8/5)

Resposta rápida

As solicitações são priorizadas com SLAs rigorosos para uma resolução mais rápida e confiável de problemas.

Analisadores personalizados

Os analisadores personalizados permitem que o SIEM processe formatos de log exclusivos de suas fontes de dados específicas.

Gerente de Conta Técnica (TAM) exclusivo

Com a licença Premium Plus, um TAM gerencia todos os problemas com responsabilidade elevada

Patches privados

Obtenha correções e patches personalizados, projetados para problemas específicos, com a licença Premium Plus.

Por que nos escolher

Economize até 50% nos requisitos de instalação de hardware ou virtualização e diminua o TCO com uma solução modular de alto desempenho que constantemente supera os fornecedores de SIEM legados em termos de eficiência e custo, além de tratar de milhares de EPS em cada instância.

Tenha flexibilidade com nossas opções de licenciamento. Além disso, também rastreamos o fluxo médio de EPS por dia após a agregação e a filtragem para limitar os excessos e não restringir o acesso ao Kaspersky SIEM caso eles ocorram.

Aproveite uma ampla variedade de integrações da Kaspersky e de terceiros com opções de resposta integradas. Nenhum outro fornecedor supera o nosso nível de integração simplificada com nossos próprios produtos, incluindo uma única interface para a integração com o Threat Intelligence, a capacidade de usar sensores de endpoint como agentes SIEM e muito mais.

Armazene dados localmente de forma econômica e sem comprometer a qualidade, sem ultrapassar o orçamento por um período prolongado, com opções de armazenamento quente e frio usando o ClickHouse e o Hadoop Distributed File System (HDFS) ou discos locais, sendo capaz de pesquisar rapidamente em ambas as áreas simultaneamente.

Aumente a relevância dos dados, acelere a detecção e a triagem graças ao enriquecimento com a inteligência de ameaças tática, operacional e estratégica fornecida pelo Kaspersky Threat Intelligence Portal por nossa equipe de pesquisadores e analistas líderes mundiais.

Pronto para MSSP com suporte multilocação nativo, em que uma única instalação de SIEM na infraestrutura principal das organizações permite a criação de SIEM isolado para locatários que recebem e processam seus próprios eventos.

Empresas em todo o mundo contam com a Plataforma Unificada de Monitoramento e Análise da Kaspersky para desenvolver processos abrangentes de segurança da informação que aprimoram a eficiência da cibersegurança.

Saiba mais

A Kaspersky usou seu próprio SIEM para descobrir malware previamente desconhecido direcionado a dispositivos iOS.

Ao monitorar o tráfego de rede de nossa própria rede Wi-Fi corporativa dedicada a dispositivos móveis usando a Plataforma Unificada de Monitoramento e Análise da Kaspersky, detectamos atividade suspeita originada de vários telefones baseados em iOS.

Porque é impossível examinar os dispositivos iOS modernos por dentro, criamos backups offline dos dispositivos em questão, examinamos eles usando a ferramenta de verificação móvel (Mobile Verification Toolkit) mvt-ios e descobrimos vestígios de comprometimento.

A Apple respondeu lançando atualizações de segurança para corrigir quatro vulnerabilidades de dia zero identificadas por pesquisadores da Kaspersky.

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

Essas vulnerabilidades afetam uma ampla gama de produtos da Apple, incluindo iPhones, iPods, iPads, dispositivos macOS, Apple TVs e Apple Watches. A Kaspersky também informou a Apple sobre a exploração de um recurso de hardware, o qual a empresa posteriormente mitigou.

Por que a Kaspersky?

O Kaspersky SIEM aproveita anos de conhecimento acumulado e habilidades refinadas dos 5 Centros de Excelência.

Saiba mais

27

Por **mais de 27 anos**, temos construído ferramentas e fornecido serviços para mantê-lo seguro com nossas tecnologias mais testadas e premiadas.

Saiba mais

Somos uma **empresa global de cibersegurança privada** com milhares de clientes e parceiros ao redor do mundo e comprometidos com transparência e independência.

Saiba mais

Kaspersky Unified Monitoring and Analysis Platform

Saiba mais

www.kaspersky.com.br

#kaspersky
#bringonthefuture