Kaspersky OT CyberSecurity

Solução unificada desenvolvida especificamente para a resiliência de sistemas ciberfísicos

kaspersky cybersecurity true to business

Kaspersky OT CyberSecurity

Onde a experiência proporciona resiliência

Tecnologias industriais
Soluções robustas de segurança industrial, testadas, em conformidade e aprovadas

Conhecimento acionável
Análise de ameaças confiável e treinamentos abrangentes em cibersegurança industrial

Experiência comprovada em campo
Um conjunto completo de serviços profissionais para uma cibersegurança robusta e abrangente

XDR de TI

Kaspersky Next XDR Expert

Convergência de TI - TO

Tecnologias

Soluções especializadas

- Kaspersky Antidrone
- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky SD-WAN

Kaspersky Industrial CyberSecurity

Native OT XDR

for Nodes
Proteção, detecção e resposta para endpoints

for Networks
Análise, detecção e resposta de tráfego de rede

Kaspersky OS Solutions

- Kaspersky Thin Client
- Kaspersky Automotive Secure Gateway

Conhecimento

Higiene cibernética	Inteligência de ameaças	Treinamento
Kaspersky Security Awareness	Kaspersky ICS Threat Intelligence	Kaspersky ICS CERT Training

Experiência

Descoberta	Resposta a incidentes	Proteção gerenciada
Kaspersky ICS Security Assessment	Kaspersky Incident Response	Kaspersky Managed Detection and Response

Kaspersky OT CyberSecurity

Cobertura completa para sistemas de missão crítica efetivamente fornecida

Kaspersky Industrial CyberSecurity

Native OT XDR

for Nodes

Proteção, detecção e resposta para endpoints

for Networks

Análise, detecção e resposta de tráfego de rede

Kaspersky Next XDR Expert

Convergência de TI - TO

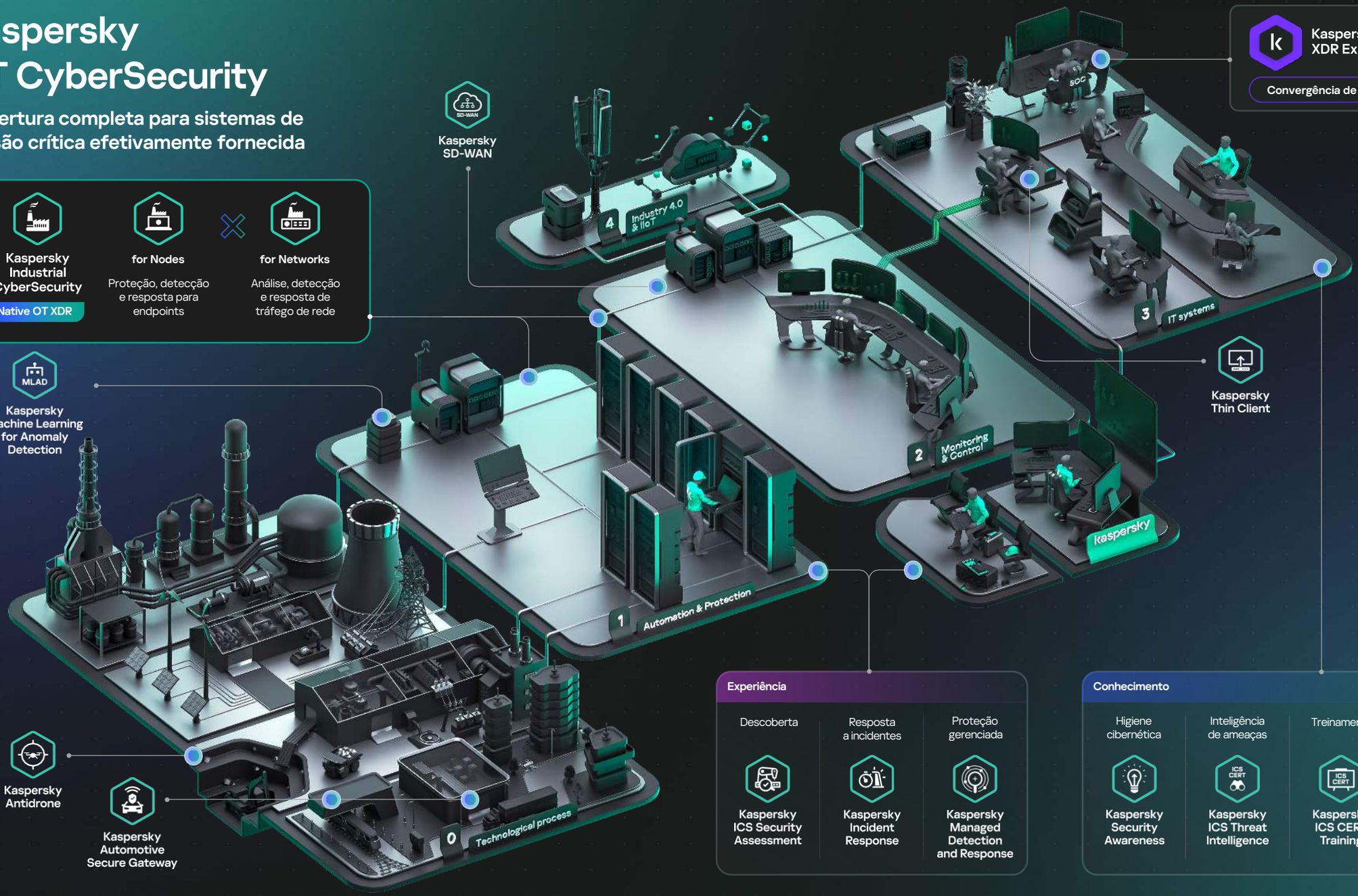
Kaspersky SD-WAN

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Thin Client

Kaspersky Antidrone

Kaspersky Automotive Secure Gateway



Experiência

Descoberta	Resposta a incidentes	Proteção gerenciada
Kaspersky ICS Security Assessment	Kaspersky Incident Response	Kaspersky Managed Detection and Response

Conhecimento

Higiene cibernética	Inteligência de ameaças	Treinamento
Kaspersky Security Awareness	Kaspersky ICS Threat Intelligence	Kaspersky ICS CERT Training

Kaspersky Industrial CyberSecurity

Consciência situacional de 360° e controle da exposição ao risco

- **Inventário de ativos e visibilidade da rede.**

  Rastreie todos os dispositivos conectados e suas configurações. Crie um gráfico da rede e analise os fluxos de dados.
- **Eliminação de ameaças.** Identifique e mitigue ameaças em hosts e redes, com insights sobre causas-raiz e medidas seguras de resposta.
- **Avaliação de riscos.** Avalie vulnerabilidades e monitore alterações nas configurações de segurança de hosts, dispositivos de rede e controladores.

Principais vantagens

- Compatibilidade testada e comprovada com mais de 200 sistemas e dispositivos de automação industrial
- Plataforma OT XDR integrada de forma transparente, que resolve múltiplos desafios e é desenvolvida especificamente para infraestruturas críticas
- Solução de baixo impacto operacional, que não afeta o desempenho do sistema nem a continuidade dos processos

O KICS e suas tecnologias principais são submetidos a auditorias líderes do setor

ISA/IEC 62443-4-1 | SOC 2 Tipo 2 | ISO/IEC 27001 | GB 42250-2022

Kaspersky Next XDR Expert

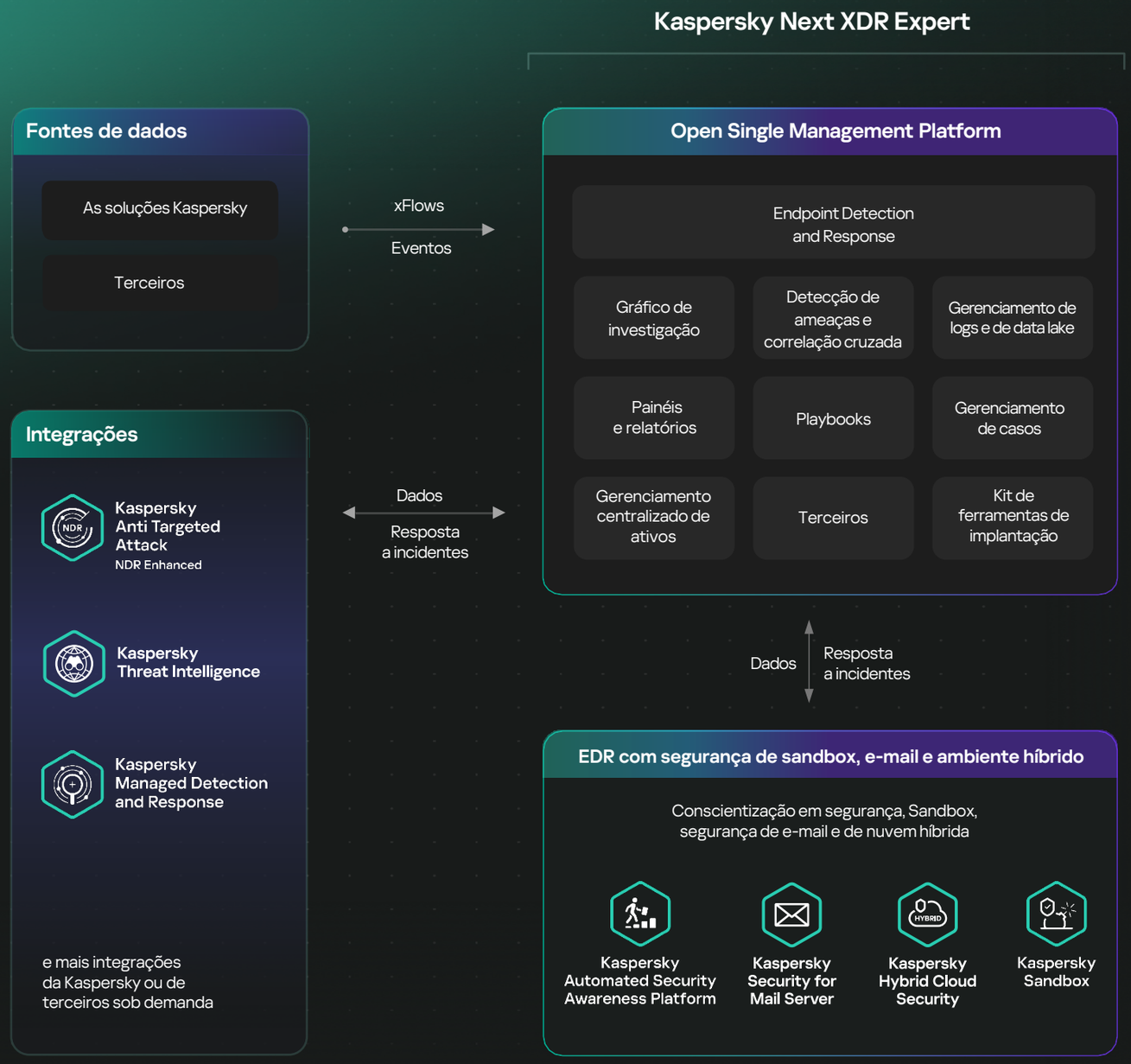
Proteção ponta a ponta nos segmentos industrial e corporativo da sua empresa

Por meio da integração estreita com o Kaspersky Next XDR Expert, a plataforma Kaspersky Industrial CyberSecurity possibilita novos cenários, incluindo interações com soluções de terceiros e recursos avançados de investigação e resposta. A integração ajuda a proteger o seu negócio onde os ambientes industriais e corporativos se interligam.

As equipes de segurança obtêm uma visão unificada da evolução de um incidente e identificam suas causas-raiz para evitar ocorrências semelhantes no futuro.

Principais vantagens

- Segurança e soberania de dados para infraestruturas convergentes de TI/TO/IoT com alta concentração de ativos
- A interoperabilidade nativa em todo o portfólio de produtos da Kaspersky proporciona uma integração fluida e incomparável



Kaspersky Machine Learning for Anomaly Detection

Detecção antecipada de anomalias e análises preditivas

- Detecta falhas de equipamentos e erros humanos muito antes de se tornarem críticos, ajudando a prevenir falhas e acidentes.
- Identifica ações atípicas de funcionários ou operações incomuns de equipamentos que possam indicar um ataque direcionado ou sabotagem.
- Identifica anomalias de difícil detecção na operação de sistemas ciberfísicos, causadas por pequenos desvios em múltiplos parâmetros do processo.

Integração com sistemas externos

O Kaspersky MLAD recebe telemetria de processos do KICS for Networks, de sistemas de automação industrial e de dispositivos IoT/IIoT

O processador de eventos do MLAD troca mensagens CEF com fontes externas: sistemas SIEM, dispositivos IIoT e dispositivos de rede

IACS – Sistemas de Automação e Controle Industrial

SIEM – Gerenciamento de Informações e Eventos de Segurança

IIoT – Internet Industrial das Coisas

IoT – Internet das Coisas

Kaspersky SD-WAN

Uma solução unificada que garante a confiabilidade de redes industriais distribuídas

O Kaspersky SD-WAN permite que empresas industriais criem redes resilientes e geograficamente distribuídas com gerenciamento centralizado, assegurando a continuidade dos processos industriais.

O Kaspersky Industrial CyberSecurity oferece suporte ao uso de infraestrutura SD-WAN para coletar tráfego industrial, fornecer monitoramento centralizado e proteger ativos e sistemas industriais distribuídos.

Principais vantagens

- Fácil escalabilidade
- Otimização de custos
- Gerenciamento conveniente
- Segurança centralizada

Kaspersky Antidrone

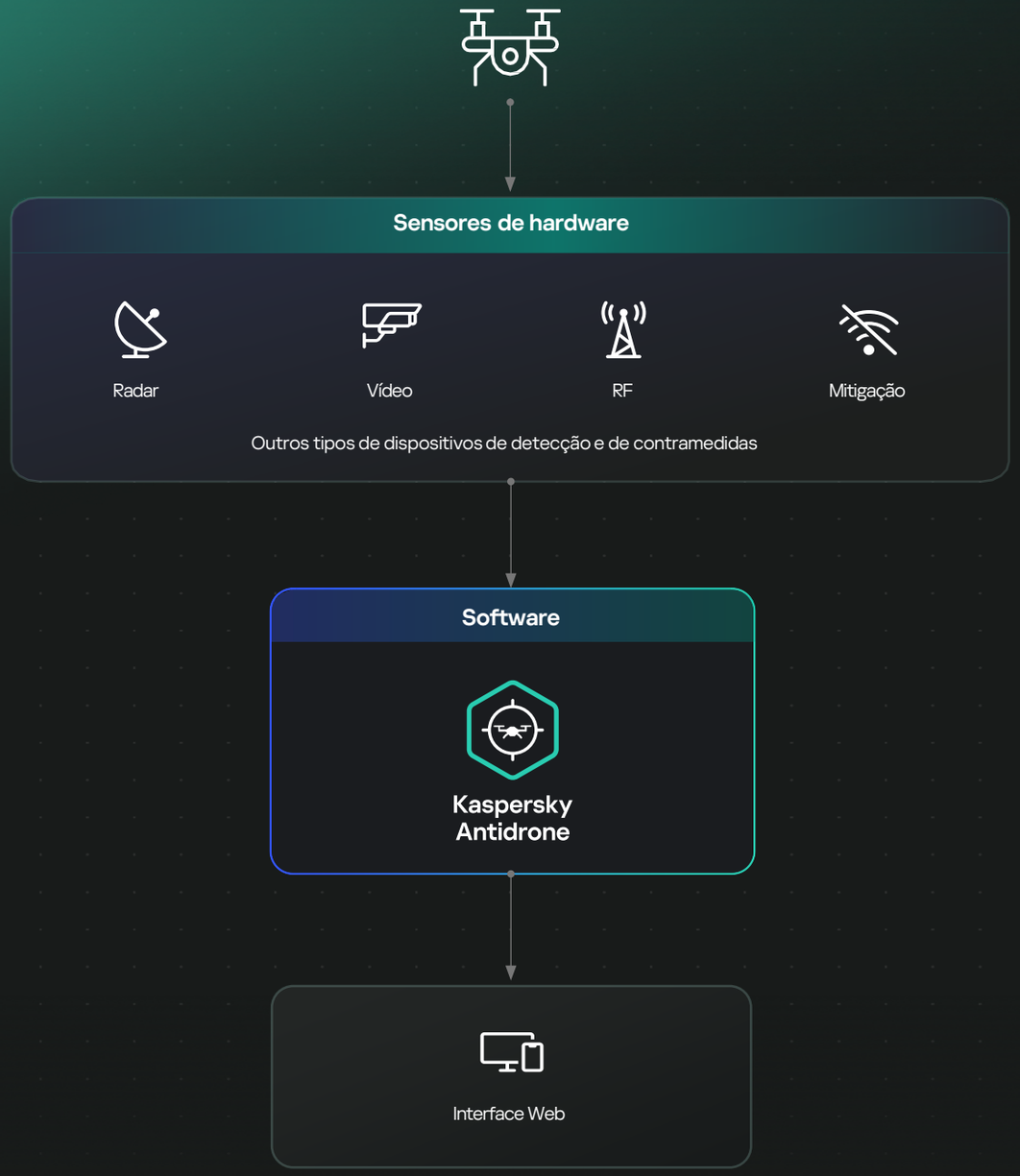
Solução de monitoramento e defesa contra drones

O Kaspersky Antidrone ajuda a reduzir o risco de paralisações de processos em empresas industriais ao impedir que drones não autorizados entrem em suas instalações. O sistema verifica automaticamente o espaço aéreo, detectando e classificando drones. As informações sobre o que está acontecendo são exibidas na interface web. Em caso de ameaça, e quando permitido, os operadores podem neutralizar o drone.

O Kaspersky Antidrone é uma solução modular que pode ser implementada em instalações industriais de qualquer porte. Também oferece suporte ao modo “amigo ou inimigo”, permitindo que as organizações operem seus próprios drones sem interferência, ao mesmo tempo em que impedem a entrada de veículos aéreos não tripulados não autorizados na área.

Principais vantagens

- O Kaspersky Antidrone permite que radares, scanners de RF, câmeras e bloqueadores de diferentes fornecedores sejam combinados e orquestrados em um único sistema unificado.
- A fusão de múltiplos sensores melhora significativamente a confiabilidade da detecção em condições com alta interferência, ruído ou baixa visibilidade.



Kaspersky Thin Client

Infraestrutura segura de acesso remoto e desktop virtualizado

Risco

As estações de trabalho de usuários estão entre os alvos mais comuns de ciberataques

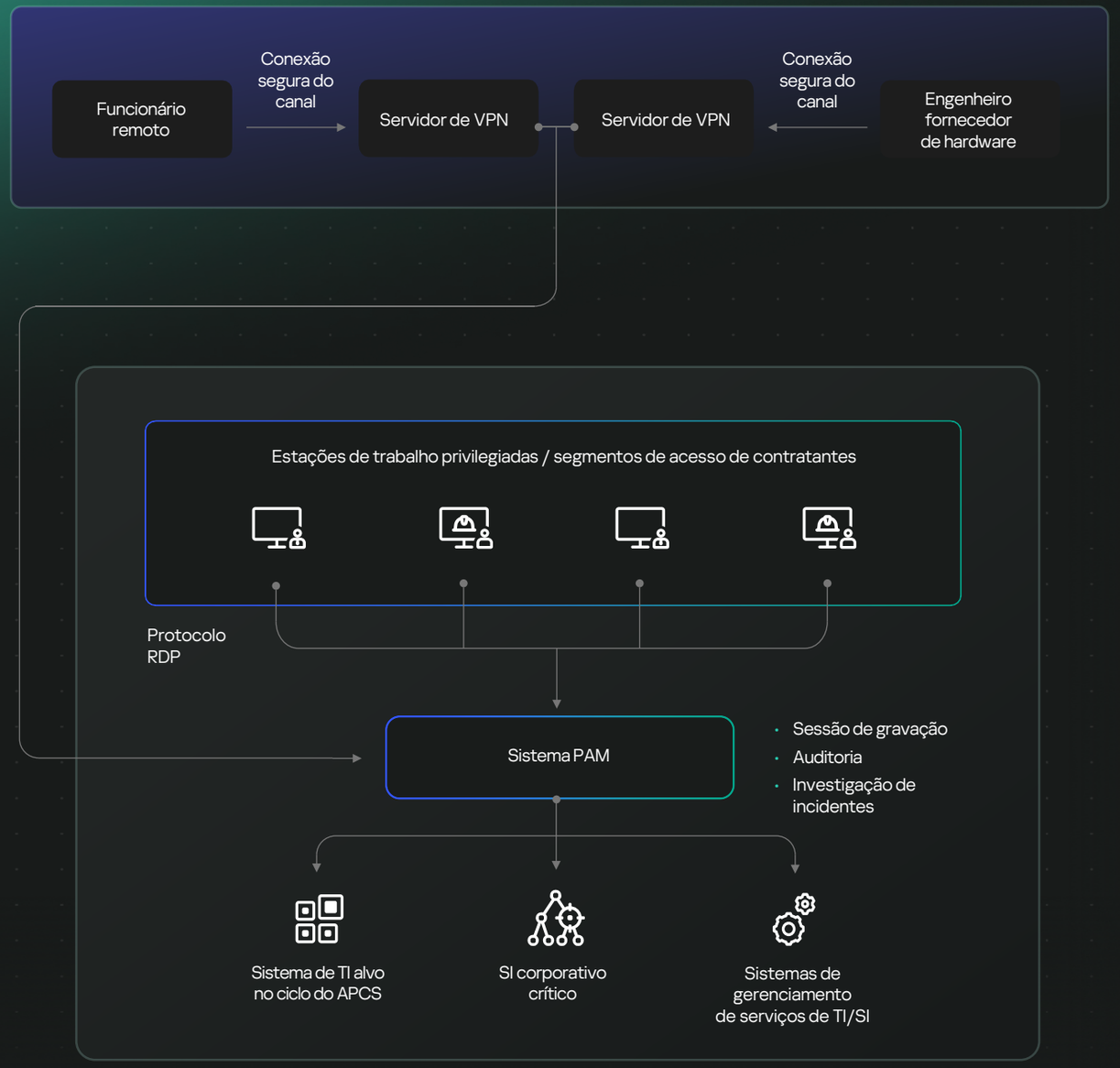
Solução

O Kaspersky Thin Client é uma solução para a construção de uma infraestrutura gerenciável e funcional de thin clients baseada no sistema operacional de microkernel KasperskyOS, desenvolvido pela própria Kaspersky.

Sem refrigeração ativa nem partes móveis, os thin clients oferecem desempenho altamente confiável em ambientes de produção.

Principais vantagens

- Segurança como parte do projeto
- Uma plataforma única de gerenciamento para SI e TI
- Integração de infraestrutura em apenas dois minutos



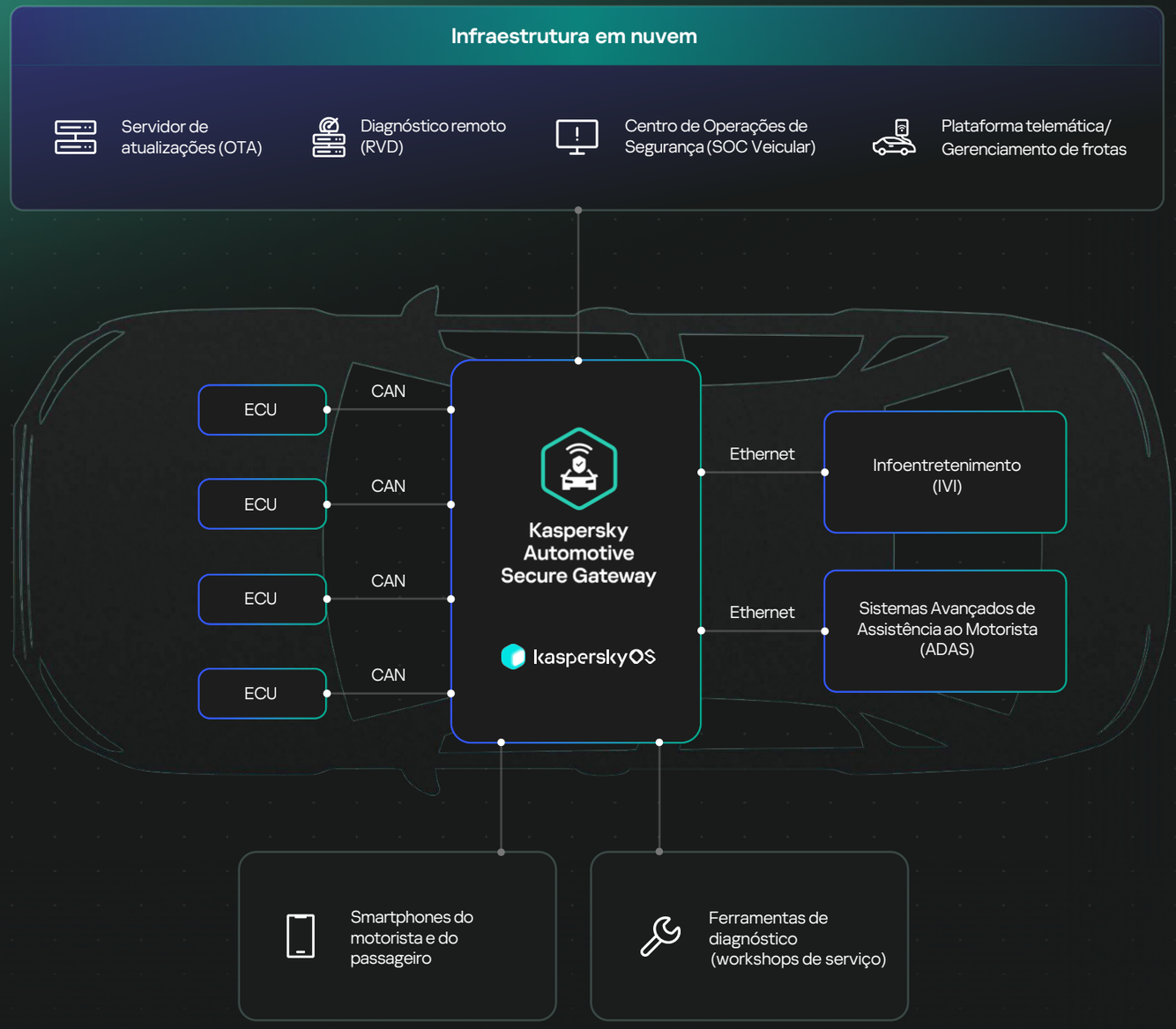
Kaspersky Automotive Secure Gateway

Desenvolvimento de sistemas de TI confiáveis para veículos conectados

- Gateway de software seguro para veículos conectados, que também oferece as funções de uma unidade de controle telemático (TCU)
- Segurança desde o nível do sistema operacional
- Conformidade com os requisitos mais recentes para garantir a cibersegurança e a segurança veicular (ISO 26262, ISO/SAE 21434, UN R155, UN R156, Uptane)
- Comunicação segura e confiável entre as unidades eletrônicas da arquitetura elétrica e eletrônica (E/E), bem como entre essas unidades e a nuvem veicular conectada e os dispositivos de diagnóstico
- Implementação de diagnósticos remotos, atualizações seguras over-the-air de ECUs e outros serviços telemáticos

Principais vantagens

- Segurança incomparável e imunidade cibernética para setores com altos requisitos de segurança da informação
- A integração de um gateway seguro e de uma unidade de controle telemático em uma única solução ajuda a reduzir custos
- Protocolos especializados ajudam a otimizar os custos do tráfego de dados móveis



Conhecimento

Kaspersky ICS Threat Intelligence

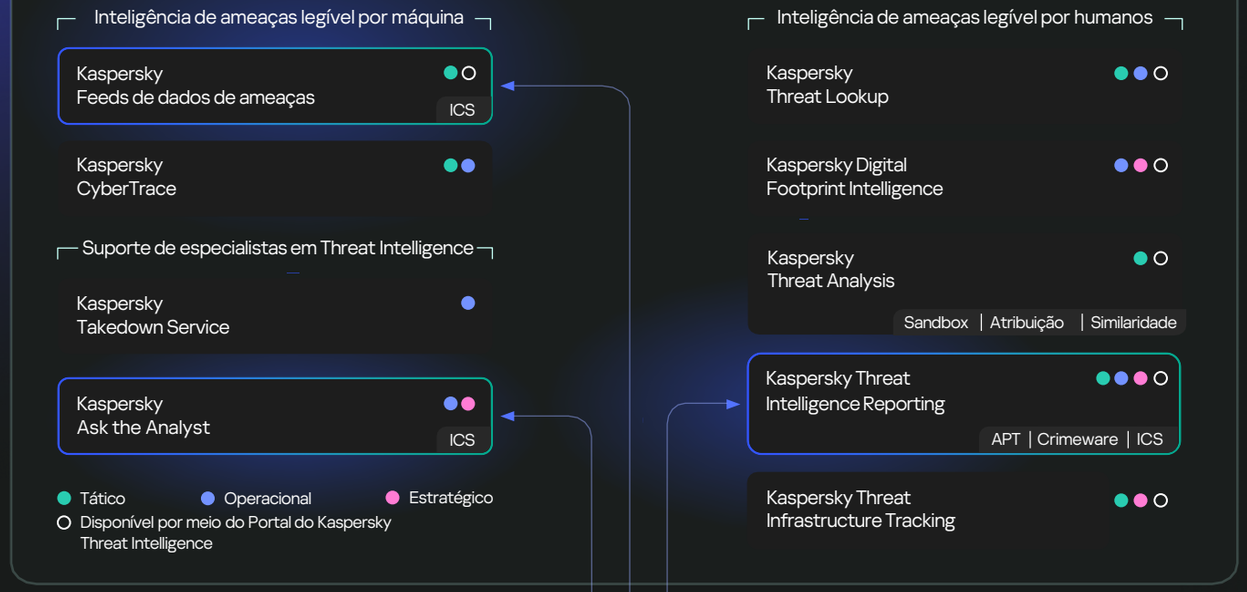
Visibilidade aprofundada sobre ameaças e vulnerabilidades de cibersegurança industrial para apoiar avaliações eficazes de risco, detecção de ataques, investigação de incidentes e resposta.

Respaldado pela expertise e experiência incomparáveis do Kaspersky ICS CERT, o primeiro CERT privado especializado em cibersegurança industrial.

Principais vantagens

- Detecção rápida de ameaças e recursos analíticos abrangentes
- Maior eficácia em investigações e na identificação proativa de ameaças
- Informações abrangentes sobre ameaças e vulnerabilidades para embasar a tomada de decisões

Produtos e serviços Kaspersky Threat Intelligence



Centros de especialização

Conhecimento

Kaspersky Threat Data Feeds

O serviço Kaspersky Threat Data Feed fornece inteligência de ameaças quase em tempo real para ajudar organizações industriais a proteger suas redes e sistemas contra ameaças cibernéticas. Os feeds de dados ICS incluem informações sobre arquivos maliciosos conhecidos e as vulnerabilidades mais recentes conhecidas, comprovadamente exploráveis em sistemas de controle industrial. Quando contextualizados, esses dados ajudam a revelar o panorama geral e a responder às perguntas “quem, o quê, onde e quando”, permitindo identificar adversários, tomar decisões mais rápidas e responder de forma eficaz.

Principais vantagens

- Resposta a incidentes aprimorada e acelerada, com recursos avançados de análise forense
- Soluções de segurança reforçadas
- Evita a exfiltração de dados sensíveis e de propriedade intelectual

O que você recebe:

Feed de dados de hash do Kaspersky ICS

Inteligência de ameaças para ICS atuais e outros sistemas usados em TO para simplificar e automatizar a detecção e a investigação imediata de ataques

prevenção # detecção # investigação

Kaspersky ICS Vulnerability Data Feed

Dados verificados e refinados sobre vulnerabilidades descobertas em software e hardware de sistemas ICS e outros sistemas utilizados em ambientes industriais, fornecidos em um formato legível por máquina

prevenção # detecção # investigação

ICS Vulnerability Data Feed em formato OVAL

Feed atualizado regularmente contendo definições OVAL para detecção automatizada de vulnerabilidades conhecidas em sistemas SCADA e outros softwares industriais

detecção

Kaspersky ICS Intelligence Reporting

O Kaspersky ICS Threat Intelligence Reporting fornece inteligência aprofundada e maior visibilidade sobre campanhas maliciosas direcionadas a organizações industriais, além de informações sobre vulnerabilidades encontradas nos sistemas de controle industrial mais amplamente utilizados e em suas tecnologias subjacentes. Informações detalhadas, adaptadas para organizações industriais, ajudam os clientes a proteger ativos críticos, incluindo componentes de software e hardware, e a garantir a segurança e a continuidade dos processos tecnológicos.

Os relatórios são disponibilizados por meio do Portal do **Kaspersky Threat Intelligence** e também estão disponíveis via API.

Principais vantagens

- Detecte e previna ameaças relatadas para proteger ativos críticos e garantir a segurança e a continuidade dos processos tecnológicos
- Correlacione atividades maliciosas ou suspeitas detectadas com pesquisas da Kaspersky para atribuir incidentes a campanhas específicas e identificar ameaças

O que você recebe:

Relatórios de APTs

Relatórios sobre novas APT e campanhas de ataque de alto volume visando organizações industriais e atualizações sobre ameaças ativas

Vulnerabilidades detectadas

Relatórios sobre vulnerabilidades identificadas pela Kaspersky nos produtos mais populares utilizados nos sistemas de controle industrial, a Internet das coisas industrial e infraestruturas em várias indústrias

O cenário de ameaças

Relatórios sobre as mudanças significativas no cenário de ameaças para sistemas de controle industriais, fatores críticos recém-descobertos que afetam os níveis de segurança de ICS e a exposição dos ICS a ameaças, incluindo informação específica da região, do país e do setor

Análise e mitigação de vulnerabilidades

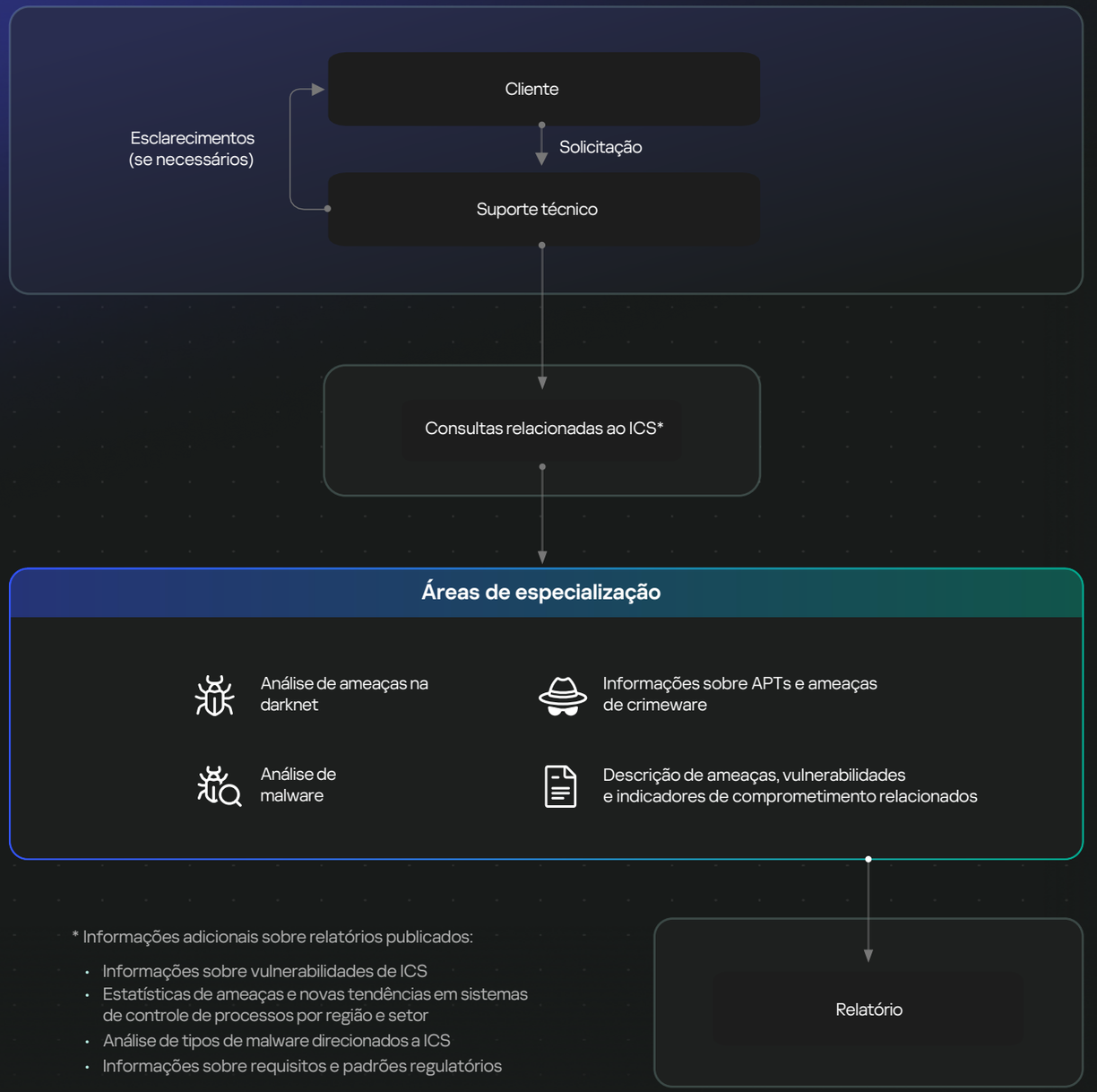
Nossos consultores fornecem recomendações acionáveis de especialistas da Kaspersky para ajudar a identificar e mitigar ameaças

Kaspersky Ask the Analyst

O Kaspersky Ask the Analyst complementa o portfólio do Kaspersky Threat Intelligence. Com esse serviço, você pode entrar em contato com especialistas para obter suporte e informações úteis sobre ameaças e vulnerabilidades específicas que enfrenta ou sobre as quais tenha interesse. Com esses dados, você pode aprimorar suas defesas contra ameaças que visam tanto à organização como um todo quanto sua infraestrutura industrial.

Principais vantagens

- Acesso a especialistas líderes em inteligência de ameaças, incluindo especialistas em segurança industrial do Kaspersky ICS CERT
- Informações contextuais personalizadas e detalhadas para investigações eficazes
- Instruções detalhadas de nossos especialistas sobre como responder a ameaças e vulnerabilidades de forma rápida e eficaz



* Informações adicionais sobre relatórios publicados:

- Informações sobre vulnerabilidades de ICS
- Estatísticas de ameaças e novas tendências em sistemas de controle de processos por região e setor
- Análise de tipos de malware direcionados a ICS
- Informações sobre requisitos e padrões regulatórios

Conhecimento

Fale conosco

Experimente agora

Saiba mais

Kaspersky Security Awareness

Transforme colaboradores em um firewall humano

O portfólio Kaspersky Security Awareness ajuda a construir uma forte cultura de cibersegurança em todos os níveis da sua organização:

- **Kaspersky Interactive Protection Simulation (KIPS)** – simulação gamificada adaptada a cenários industriais (geração de energia, petróleo e gás, petroquímica etc.). A solução demonstra como a cibersegurança afeta o desempenho dos negócios, permitindo que gestores vivenciem o impacto de decisões estratégicas.
- O **Kaspersky Automated Security Awareness Platform (ASAP)** desenvolve comportamentos seguros em toda a força de trabalho por meio de treinamentos interativos e simulações de ataques de phishing, capacitando funcionários com conhecimentos e habilidades essenciais em cibersegurança industrial.
- O **Kaspersky Executives Training** é um curso prático que proporciona a tomadores de decisão e líderes funcionais uma compreensão clara do cenário de cibersegurança.

Principais tópicos abordados

- E-mail
- Sites e Internet
- Senhas e contas
- Redes sociais e aplicativos de mensagens
- Cibersegurança para a indústria
- Segurança do PC
- Dispositivos móveis
- Dados confidenciais
- GDPR
- Segurança física dos dados
- Segurança de cartões bancários e PCI DSS
- Inteligência artificial e redes neurais
- Dados pessoais

Conhecimento

Fale conosco

Catálogo de treinamento

Kaspersky ICS CERT Training

Aprendizado aplicado

Nosso programa de treinamento em ICS foi desenvolvido para ajudar profissionais de TI, TO e segurança da informação, bem como gestores e outros colaboradores, a ampliar seus conhecimentos em cibersegurança industrial e desenvolver habilidades práticas especializadas.

Habilidades práticas de especialistas da Kaspersky

- Perícia digital e resposta a incidentes
- Exploração de vulnerabilidades em dispositivos TO/IoT e software industrial.
- Programas de treinamento interfuncionais para especialistas em TI, TO e SI

Kaspersky ICS Security Assessment

Garantia de resiliência cibernética em ambientes TO

Risco

Uma única vulnerabilidade é suficiente para que cibercriminosos assumam o controle de todo um sistema industrial

Solução

Uma abordagem abrangente para identificar vulnerabilidades e fragilidades de segurança em infraestruturas industriais

Principais vantagens

- Fortaleça os controles de segurança para proteger operadores, engenheiros e outros colaboradores
- Identifique vulnerabilidades que invasores poderiam explorar para interromper linhas de montagem, equipamentos de manufatura ou sistemas robóticos
- Proteja projetos, desenhos e programas de manufatura contra roubo
- Evite violações que possam comprometer a qualidade ou a segurança dos produtos

Abordagem da Kaspersky para Avaliação de Segurança Industrial

Teste de invasão externo
Caixa preta ou caixa cinza

Acesso à Internet

Infraestrutura industrial (TO)

- Arquitetura e equipamentos de rede
- Solução industrial, estações de trabalho e servidores
- Dispositivos e componentes

Dispositivos e componentes

Segurança de OT
- Teste de caixa branca
- Simulação de ataque
- Verificação de segurança

MES, LAN corporativo

Teste de penetração interna
Caixa preta ou caixa cinza

Ambiente de teste

Análise de segurança de componentes de hardware e software
- Teste de caixa branca
- Vulnerabilidades de Dia Zero
- Guias de endurecimento

Kaspersky Managed Detection and Response

Com tecnologia de IA. Aperfeiçoado por humanos.

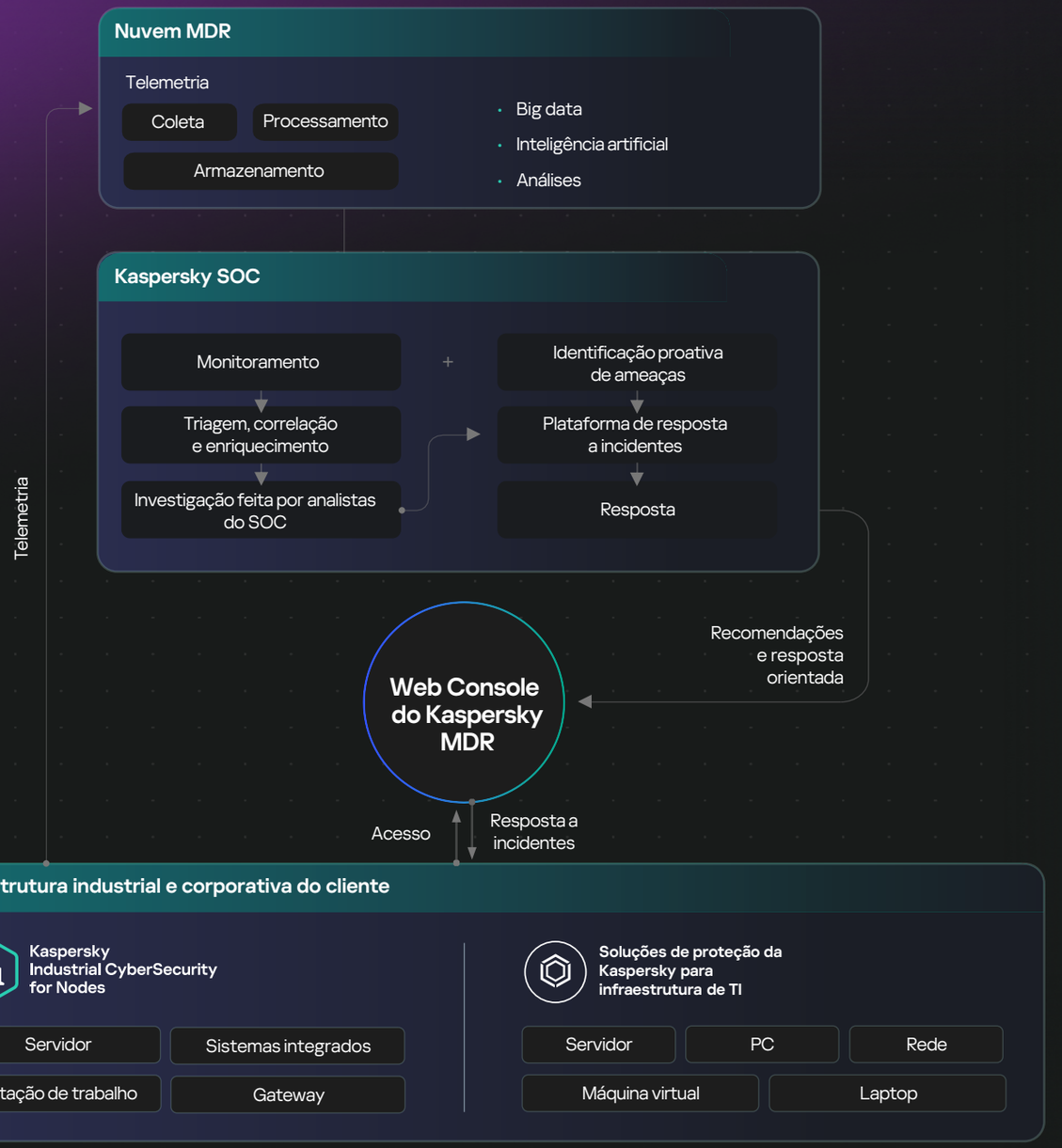
- Busca, detecção e eliminação contínuas de ameaças direcionadas à sua empresa industrial
- Redução de custos de segurança ao eliminar a necessidade de contratar novos especialistas em cibersegurança
- Obtenha todos os principais benefícios de um SOC sem precisar construir um internamente

22% dos nossos clientes são do setor industrial

Consulte o relatório de analista do MDR para saber mais

Principais vantagens

- Detecção proativa de ameaças: indicadores patenteados de ataque ajudam a identificar ameaças ocultas no sistema de controle
- Resposta orientada e automatizada (com investigação forense completa e análise de malware disponíveis sob demanda)
- Especialidade em cibersegurança de ICS respaldada por uma das equipes de detecção de ameaças proativas mais bem-sucedidas e experientes do setor



Kaspersky Incident Response

Gerenciamento das consequências de uma violação de segurança

Risco

Incidentes que afetam infraestruturas críticas exigem a expertise adequada para conduzir a resposta em instalações industriais. Ações incorretas e fora do tempo adequado podem aumentar significativamente os danos causados por um ataque.

Solução

- Eliminação rápida das consequências de um incidente pela Equipe Global de Resposta a Emergências da Kaspersky
- Suporte durante todo o ciclo de investigação e resposta a incidentes
- Inteligência, coleta e remediação com base em nossas próprias ferramentas inovadoras
- Especialização sob demanda e compartilhamento de conhecimento com suas equipes

Composição do serviço

Resposta a incidentes
Investigação e eliminação de ameaças

Digital forensics
Análise de evidências digitais

Análise de malware
Obtenha uma visão detalhada dos arquivos utilizados em um ataque

Explore a anatomia do mundo cibernético com o relatório global da Kaspersky Security Services

Um parceiro no qual você pode confiar

- Cerca de 30 anos de experiência de classe mundial e petabytes de dados de ameaças
- ICS CERT – nossa divisão internacional dedicada à pesquisa em segurança para TO/IoT
- Experiência comprovada na indústria de segurança de TI/TO com inúmeros prêmios e conquistas
- Mais de 200 certificações de interoperabilidade com soluções de fornecedores de automação
- Eficácia comprovada da tecnologia e conformidade com normas e requisitos do setor

Mais sobre as soluções de TO

Mais sobre as soluções de TI

Fale conosco