Uma plataforma de Detecção e Resposta Estendida (XDR) para segurança abrangente de empresas industriais.

Kaspersky Industrial CyberSecurity

kaspersky bring on the future

Atacado por malware

No primeiro trimestre de 2024, um total de 30 incidentes de segurança cibernética foram publicamente confirmados pelas organizações afetadas ou pelos responsáveis, sendo que o setor de fabricação representou 64,5% desses incidentes.

Kaspersky ICS CERT, junho de 2024

Saiba mais

Cenário de ameaças industriais

A nova realidade para proprietários e operadores de infraestruturas industriais é moldada por fatores como o crescente interesse dos hacktivistas em sistemas de automação, altos requisitos regulatórios, convergência de TI-TO e o aumento da variedade de ciberataques no setor industrial (no primeiro trimestre de 2024, as soluções da Kaspersky bloquearam malware de 10.865 famílias diferentes em sistemas de automação industrial).

A proliferação de tecnologias digitais, geralmente vista como algo positivo, exclui a lacuna entre os ambientes de TI e TO que costumavam proteger este último de cibercriminosos. Embora o simples pen drive inserido no ambiente ICS possa afetar seriamente o negócio principal de uma empresa, um grupo de hackers motivados pode penetrar nas redes TO, causar danos consideráveis e/ou roubar informações valiosas. Combinado com os padrões de automação que evoluem de recomendações comuns para requisitos legislativos e a crescente necessidade de compartilhar as melhores práticas, bem como gerenciar riscos, isso torna a cibersegurança das empresas industriais um desafio formidável.

A Kaspersky ICS CERT espera que organizações do seguindo setores enfrentem ataques cibernéticos com cada vez mais frequência:

Óleo, gás e produtos químicos

A digitalização da exploração, extração, transporte e refino — um fator competitivo chave para essas empresas — implica na integração de IIoT, drones e robôs, na implantação de soluções 5G, blockchain e realidade virtual, o que amplia o cenário para ações maliciosas.

Fabricação crítica

Buscando melhorar a relação custo-benefício, essas empresas implementam tecnologias de ponta, expandem a conectividade, exploram a nuvem e investigam cenários de convergência entre TI e TO, aumentando a exposição a ameaças completamente novas e em constante mudança.

Minerais, metais e mineração

Um alicerce para a fabricação crítica e nacionalmente importante, o setor precisa equilibrar despesas ao mesmo tempo em que introduz automação e tecnologias digitais. Sendo um petisco tanto para hacktivistas quanto para atacantes de alto potencial, ele não pode comprometer sua cibersegurança.

Energia, rede e serviços públicos

Tecnologia digital e emergente são vitais para impulsionar a transição energética, ao mesmo tempo em que mantêm a infraestrutura legada, que ainda é a espinha dorsal da maioria das instalações de energia. No entanto, representam o maior risco, exigindo esforços extras de cibersegurança.

Os principais alvos dos ataques APT incluirão:

Proprietários e operadores de infraestrutura crítica

Organizações estrategicamente importantes dos setores de petróleo e gás, químico, energia e serviços públicos enfrentam consequências potencialmente maiores de interferência operacional

Fabricação crítica

De uma única planta até uma escala nacional ou internacional, essas empresas, incluindo aquelas das indústrias de Metais e Mineração, Agricultura e manufatura global, se envolvem em operações de alto risco que envolvem custos significativos de incidentes

Os ataques aos sistemas industriais, especialmente os sistemas de controle industrial (ICS) e supervisão e aquisição de dados (SCADA), estão aumentando. Enquanto isso, as ameaças cibernéticas de hoje direcionadas a ambientes industriais parecem ser resistentes às soluções convencionais. Diante desse cenário, a Kaspersky oferece uma abordagem abrangente para essas indústrias. Explore nossos casos de sucesso de clientes, insights sobre o panorama de ameaças e ofertas dedicadas a cenários específicos em nosso site.

Escolher um parceiro em quem você possa confiar, com um profundo conhecimento das sobreposições entre a cibersegurança industrial e corporativa e a capacidade de fornecer uma ampla gama de tecnologias de segurança de ponta, nunca foi tão importante.

Saiba mais sobre APT e ataques financeiros a empresas industriais durante o início de 2024

Saiba mais

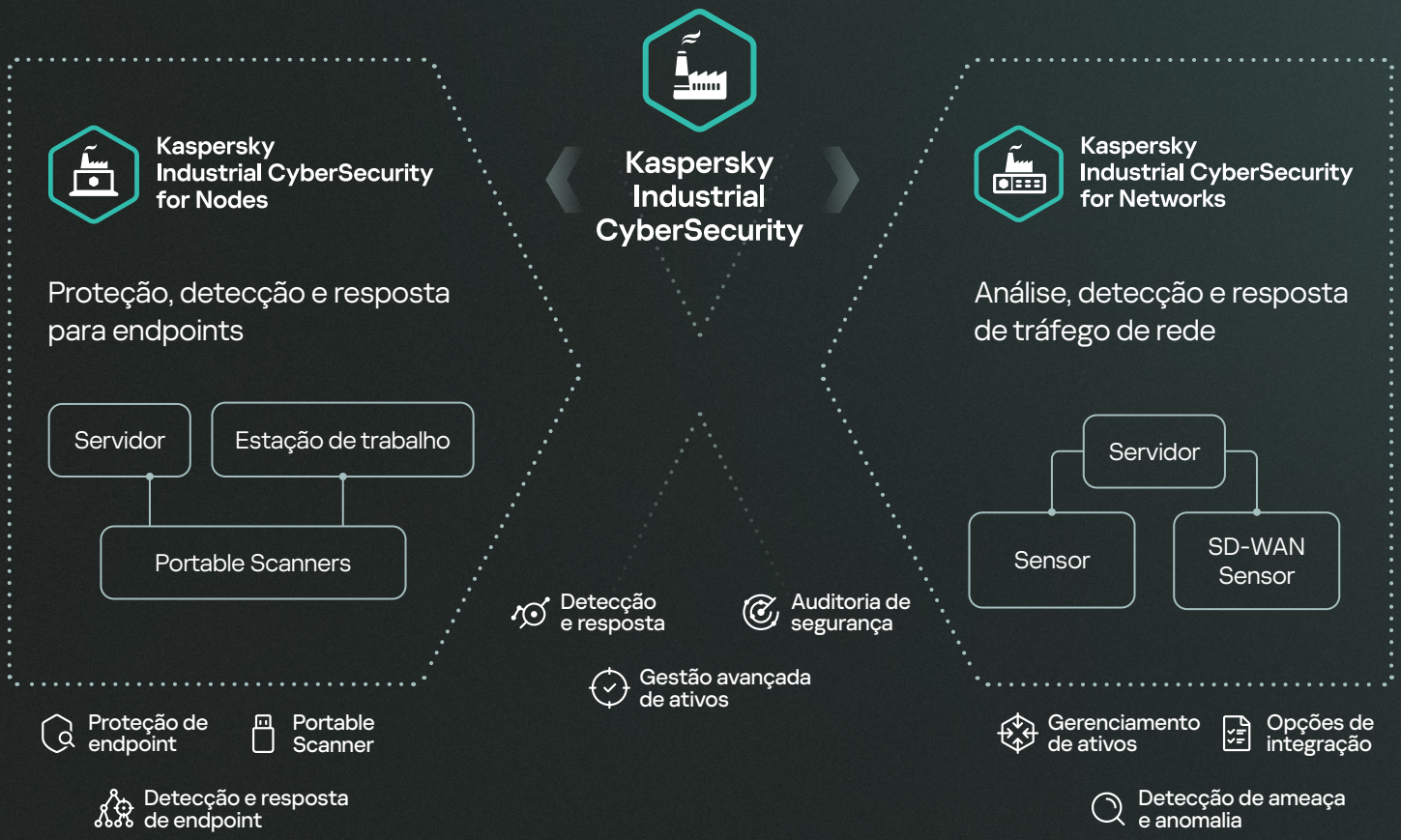
Tecnologias de segurança de ICS avançadas

A lacuna entre os ambientes de TI e TO que costumava proteger este último de cibercriminosos continua se estreitando, razão pela qual uma solução de segurança abrangente de nível empresarial de um único fornecedor para proteger a infraestrutura crítica é agora indispensável para proprietários e operadores de sistemas ciberfísicos. **O Kaspersky Industrial CyberSecurity (KICS),** uma plataforma XDR nativa composta pelos componentes KICS for Networks and KICS for Nodes, protege sistemas e redes de automação industrial.

KICS for Networks é um produto de análise, detecção e resposta de tráfego que oferece monitoramento, detecção de intrusão e gerenciamento de riscos de rede industrial, além de apresentar uma auditoria centralizada de nodos de rede industrial para vulnerabilidades e conformidade com padrões da indústria. **O KICS para Nodes** oferece proteção de endpoint de nível industrial, detecção e resposta com auditoria de conformidade baseada em OVAL*. Esta solução modular e de baixo impacto é compatível com Linux, Windows, sistemas legados, sistemas autônomos e CLPs. A versão do Portable Scanner protege máquinas autônomas e dispositivos de empreiteiros sem necessidade de instalação.

Em conjunto, esses componentes formam a plataforma KICS XDR que oferece inventário centralizado de ativos, gerenciamento de riscos e auditoria, possibilitando escalabilidade de segurança em infraestruturas diversas e distribuídas por meio de uma única plataforma com um gráfico abrangente de incidentes, análises e muito mais.

A plataforma KICS XDR permite aos usuários ver o quadro geral e o contexto mais amplo: a cadeia de incidentes nos níveis de rede e endpoint, parâmetros precisos de ativos, mapas de comunicação e topologia de rede, mesmo em segmentos nos quais o espelhamento de tráfego ainda não está disponível e muito mais.



* Linguagem aberta de avaliação e vulnerabilidade (OVAL)

Pontos de aplicação de plataforma

Convergência de ambientes de TO e de TI

Ambiente de TI

DMZ/GTW

Ambiente de TO

Kaspersky Industrial CyberSecurity for Nodes

- Estação de trabalho do operador
- Servidor SCADA
- Estação de trabalho do engenheiro
- ICS Gateway

Equipamento de rede

SPAN

Kaspersky Industrial CyberSecurity for Networks

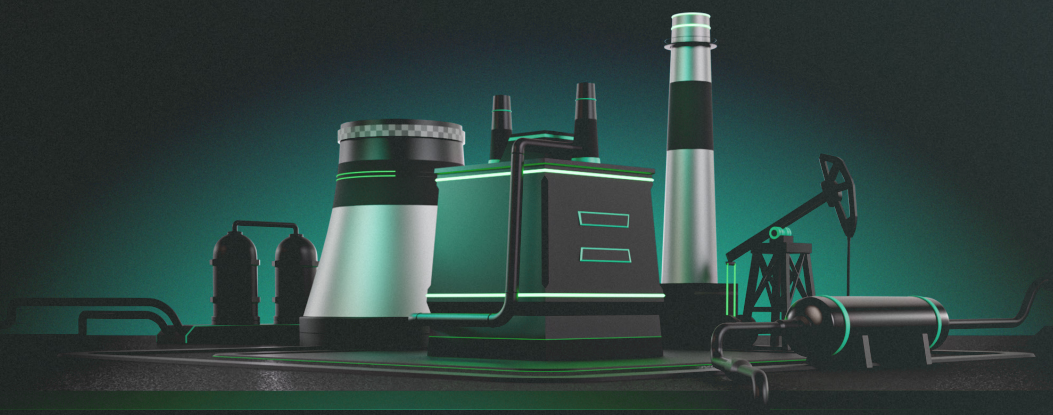
- Unidade de controle da baía (BCU)
- Dispositivo eletrônico inteligente (IED)
- Controladores lógicos programáveis (CLP)
- Sistema de proteção de relé e sistema instrumentado de segurança (SIS)
- Nodos isolados (verificação manual com KICS Portable Scanner)

Detecção precoce de anomalias e análise preditiva

Kaspersky Machine Learning for Anomaly Detection (Kaspersky MLAD) é um sistema inovador que usa uma rede neural para monitorar uma ampla gama de dados de telemetria simultaneamente. Ele detecta falhas de equipamentos e erros humanos, ajudando a prevenir falhas e acidentes, identifica ações atípicas de funcionários ou operações de equipamentos como sinais de um ataque especializado ou sabotagem, e combina detecção de anomalias com análise preditiva da condição e ciclo de vida do equipamento.

Saiba mais

Nível físico



Protegido por produtos Kaspersky

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

Solução de monitoramento de rede e análise de tráfego industrial. Permite uma Inspeção Profunda de Pacotes (DPI) dos protocolos industriais proprietários. Enviado como software ou appliance virtual.

O KICS for Networks identifica anomalias e intrusões no ICS em estágios iniciais, mostra como o ataque se desenvolve na rede e nos nodos (cadeia de ataque e telemetria de EDR) e garante que as ações necessárias sejam tomadas para prevenir qualquer impacto negativo nos processos industriais.

Gerenciamento de ativos

Descoberta de ativos
Obtenha insights sobre seus ativos com um banco de dados de vulnerabilidades, priorização de riscos e pesquisa ativa segura

Visibilidade de rede
Monitore o tráfego, forme mapas de topologia e acompanhe a postura da rede ao longo do tempo para máxima visibilidade

Conjunto de ferramentas de análise de tráfego
Acompanhe e analise sessões de rede, permitindo a exportação e armazenamento detalhados de dados de tráfego

Vantagens

- Especializado em aplicações e protocolos industriais. Suporte "direto da caixa" para uma ampla gama de protocolos de TO, dispositivos e ataques de rede + permite importação de projetos externos
- Regras predefinidas para configuração de auditoria de segurança
- Interface amigável e relatórios personalizáveis
- Conscientização completa de riscos em infraestrutura distribuída
- Ingesta amostras de tráfego de várias fontes: sensores de rede próprios, sensores SD-WAN, sensores de endpoint e sondas portáteis

Ecossistema e integrações

Ecossistema
Desbloqueie as extensas capacidades do ecossistema da Kaspersky por meio da integração com as seguintes soluções e nossa abordagem unificada de cibersegurança entre produtos:

- Kaspersky Next XDR Expert
Saiba mais

- Kaspersky IoT Secure Gateway (KISG)
Saiba mais

- Kaspersky Machine Learning for Anomaly Detection (MLAD)
Saiba mais

- Kaspersky Software-Defined Wide Area Network (SD-WAN)
Saiba mais

Gerencie todos os elementos do ecossistema por meio de um único console

Integrações de terceiros
Desfrute de compatibilidade perfeita com uma infinidade de ferramentas de segurança e plataformas externas

Detecção de ameaça e anomalia

Detecção de intrusão
Detecção baseada em assinatura e um mecanismo estatístico que detecta tentativas de força bruta ou de varredura

Controle de integridade de rede
O sistema aprende interações normais da rede e emite alarmes a cada desvio

Detecção de anomalias
Detecta anomalias básicas no nível de pacotes e protocolos
Poderia ser aprimorado com MLAD

DPI de protocolos industriais
Mantém o controle de processos e comandos e rastreia dados de telemetria de maneira eficiente

Correlação de eventos
Associa eventos de segurança com a classificação MITRE e uma única cadeia de ataque

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

Proteção, Detecção e Resposta de Endpoint de grau industrial, testada e certificada. Uma solução de baixo impacto, compatível e estável para sistemas Linux, Windows e autônomos.

KICS for Nodes protege todos os pontos de extremidade nos sistemas de automação digitais, gerenciados e distribuídos da atualidade. A solução coleta telemetria para criar uma representação visual clara e detalhada do progresso de um incidente em estações de trabalho, servidores, gateways e outros endpoints, tranquilizando os administradores do sistema de automação de que um incidente foi totalmente resolvido e não ocorrerá novamente.

Proteção de endpoint

Prevenção de ameaças em tempo real
Verificações personalizadas e sob demanda para unidades removíveis e áreas críticas para prevenir explorações e proteger arquivos

Atividade local de controle
Recursos de controle de dispositivo e Wi-Fi. Garantir a integridade do projeto do PLC para plena consciência da atividade local

Controle de atividade de rede
Gerenciar firewalls de host e bloquear sessões de rede, garantindo proteção contra ameaças de rede

Monitoramento de sistema
Verificar a integridade do arquivo, rastrear o acesso ao registro, detectar ameaças nos logs do sistema para garantir a segurança do SO

Detecção e resposta de endpoint

Detecção
Escaneia em busca de Indicadores de Comprometimento (IoCs), recursos abrangentes de monitoramento e relatórios

Resposta
Impedir a execução, quarentena/excluir arquivos, iniciar/encerrar processos, isolar redes e muito mais

- Nodos de Windows
- Portable Scanner
- Nodos de Linux
- Agente de auditoria

Portable scanner

Verificador de malware
As verificações antimalware de equipamentos autônomos e de todos os computadores trazidos para o local industrial

Verificação de OVAL Aplicar política de cibersegurança em máquinas autônomas com verificações manuais de vulnerabilidades e de conformidade

Captura de packets
Capturar e analisar o tráfego de rede para obter a máxima consciência, mesmo em infraestruturas isoladas

Inventário básico de ativos
Coletar dados abrangentes sobre hardware e software usando uma solução de zero pegadas

Vantagens

- Baixo impacto em dispositivos protegidos, consumo de recursos ajustável
- Compatibilidade com SOs antigos e fornecedores de automação industrial
- Configuração básica de segurança, bem como opções avançadas para proteger seus hosts de qualquer tipo de ameaça
- Implantação modular e configurações não intrusivas
- Suporte PLC: Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4; Schneider Electric Modicon M340, M580; dispositivos CODESYS V3; Fastwel CPM723-01
- Opções de licenciamento flexíveis, de 1 mês a 5 anos
- Configurações pré-definidas verificadas e eficientes para os ICS mais populares

- Gateway
- Servidor Historian
- Servidor SCADA
- Estação de trabalho do operador
- Sistemas integrados
- Estação de trabalho de gerenciamento de sistema
- Estação de trabalho de engenharia

KICS Platform e além

Cibersegurança unificada em todos os segmentos industriais e corporativos da sua empresa

Native OT XDR

Os componentes principais do Kaspersky Industrial Cybersecurity, KICS for Networks e KICS for Nodes são projetados para funcionar perfeitamente juntos dentro do nosso ecossistema, possibilitando uma experiência unificada e coesa. Quando adquiridos juntos, eles formam uma Plataforma XDR nativa que oferece funcionalidades adicionais valiosas entre os produtos.

Gestão avançada de ativos

Inventário de hardware de endpoint
Visibilidade abrangente de todos os dispositivos conectados em sua infraestrutura, garantindo um rastreamento preciso de ativos e aprimorando a gestão de segurança

Inventário de aplicativos, usuários e patches
Detalhes sobre implantações de software, acesso de usuários e status de patches dentro do seu ambiente. Dados enriquecidos para um gerenciamento adequado e redução de vulnerabilidades potenciais

Monitoramento de tráfego de endpoint
Monitoramento contínuo dos fluxos de dados em cada endpoint para detectar rapidamente padrões incomuns ou ameaças potenciais, garantindo uma resposta rápida a atividades suspeitas

Auditoria de segurança

Escaneamento de vulnerabilidades
Escaneie minuciosamente seus ativos para avaliar fraquezas de segurança, aumentar a conscientização de riscos, permitir uma resposta oportuna e fortalecer sua postura de segurança como um todo.

Auditoria de conformidade
Auditoria baseada em agente e sem agente para conformidade com os padrões do setor OVAL e XCCDF*. Um editor totalmente funcional, banco de dados de relatórios centralizado, cofre protegido para credenciais de nó e muito mais.

Controle de configuração
Garantir configurações seguras de ativos, rastrear alterações para riscos de segurança e manter a integridade da linha de base para ativos de hardware e software.

Detecção e resposta

Detecção
Identificação aprimorada e simplificada de ameaças por meio da correlação de eventos entre o host e a rede, com uma única visualização da cadeia de ataque. Enriquecimento de dados de alerta de rede para insights mais profundos sobre incidentes

Resposta
Mitigação robusta de ameaças por meio da prevenção de execução, isolamento de host e quarentena de arquivos. Integrações perfeitas de firewall aprimoram ainda mais sua capacidade de responder rapidamente e efetivamente a incidentes de segurança

XDR para TO aberto

Amplie a funcionalidade de suas soluções EDR com um mecanismo de correlação, respostas automatizadas e conectores de terceiros — aprimore sua plataforma KICS com a solução Kaspersky XDR Core para desbloquear:

- Monitoramento abrangente e correlação de eventos de segurança da informação (SIEM), integração com vários sistemas
- Gestão e enriquecimento de inteligência de ameaças

XDR para TI – TO simples

Ultrapasse e abrace a convergência final entre TI e TO. Combine sua plataforma KICS com nosso pacote especialista Kaspersky Next XDR — aproveite a funcionalidade de proteção de endpoint de classe mundial da Kaspersky e colha os benefícios das seguintes funcionalidades:

- Um único gráfico de investigação, manuais e gerenciamento de incidentes pela Kaspersky Single Management Platform
- Proteção complexa para infraestrutura de TI (IT XDR)

XDR Industrial

Kaspersky Industrial CyberSecurity

Saiba mais

Kaspersky Single Management Platform

XDR Corporate

Kaspersky Next XDR Expert

Saiba mais

* Extensible Configuration Checklist Description Format (XCCDF)

27 anos de experiência de classe mundial e petabytes de ameaças de dados

ICS CERT

ICS-CERT - Divisão própria de pesquisa de segurança de IoT / TO internacional

Experiência comprovada na indústria de segurança de TI/TO com inúmeros prêmios e conquistas

Mais de 200 certificados de compatibilidade com soluções de automação de fornecedores

Eficácia comprovada da tecnologia, conformidade com padrões e requisitos

Clientes ao redor do mundo

ROSATOM NORNICKEL EuroChem

NLMK TATNEFT ROSSETI Wintershine

alperia PacificLight КазМунайГаз AGC

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Saiba mais

www.kaspersky.com

#kaspersky
#bringonthefuture