Uma plataforma XDR
para segurança abrangente
de empresas industriais

Kaspersky Industrial CyberSecurity

kaspersky BRING ON THE FUTURE

Atacado por malware

Desde o início de 2023, cerca de 35% dos computadores relacionados ao ICS foram atacados por malware – quase 5% a menos que no ano anterior.

Kaspersky ICS CERT, outubro de 2023

Saiba mais

Ciberameaças enfrentadas por ICS e empresas industriais

A nova realidade para proprietários e operadores de infraestruturas industriais é moldada pelo 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 (um aumento de quase 50% no primeiro semestre de 2023 em comparação com o segundo semestre de 2022, de acordo com as estatísticas do Kaspersky ICS CERT).

A penetração das tecnologias digitais, geralmente vista como algo positivo, apaga a lacuna entre os ambientes de TI e de TO que costumava proteger este último dos cibercriminosos. Enquanto um único pen drive introduzido no ambiente de ICS pode afetar seriamente o negócio principal de uma empresa, um grupo de invasores motivados pode penetrar nas redes TO e causar danos consideráveis e/ou roubar informações valiosas. Combinado com os padrões de automação que evoluem de recomendações comuns para requisitos legislativos e com a crescente necessidade de compartilhar as práticas recomendadas, bem como gerenciar riscos, isso torna a cibersegurança das empresas industriais um enorme desafio.

O Kaspersky ICS CERT espera que organizações dos seguintes setores enfrentem ataques cibernéticos com cada vez mais frequência:

Petróleo, gás e produtos químicos

O alto valor dos dados e sistemas que essas empresas controlam torna-as num alvo atraente para ransomware e atores maliciosos que buscam interromper operações ou manipular preços.

Produção industrial de alto nível

Essas empresas desempenham papéis críticos na sociedade e possuem dados valiosos que podem ser explorados para ganho financeiro, resultando em imensos danos econômicos e de reputação.

Minerais, metais e mineração

A indústria de minerais, metais e mineração é visada por seus recursos valiosos, impacto financeiro e cadeias de suprimento interconectadas.

Energia, rede e serviços

O papel fundamental da energia, da rede e dos serviços públicos em nossas vidas diárias é a principal razão para os ataques que visam criar caos ou influenciar outras ações.

Os principais alvos dos ataques APT incluirão:

Proprietários e operadores de infraestrutura crítica

Organizações governamentais ou públicas estratégicas enfrentam consequências possivelmente maiores de interferência operacional.

Agentes industriais notórios

De uma única planta até uma escala nacional ou internacional, essas empresas se envolvem em operações de alto risco, envolvendo custos significativos de incidentes.

A estabilidade dos processos de produção e negócios, assim como a proteção de ativos valiosos, estão diretamente relacionadas ao desenvolvimento sustentável das empresas industriais e das instalações de infraestrutura crítica. Os ataques aos sistemas industriais, especialmente os sistemas de controle industrial (ICS) e supervisão e aquisição de dados (SCADA), estão aumentando. Enquanto isso, as ciberameaças modernas direcionadas a ambientes industriais parecem ser imunes às soluções convencionais.

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

Saiba mais sobre os TTPs comuns de ataques contra organizações industriais.

Saiba mais

A plataforma KICS XDR permite aos usuários ver o quadro geral e o contexto mais amplo: a cadeia de incidentes no nível da rede e do endpoint, parâmetros precisos do ativo, mapas de comunicação e topologia da rede, mesmo em segmentos onde a espelhamento de tráfego ainda não está disponível, e muito mais.

Sensor de endpoint

- Status de proteção
- Auditoria de segurança
- Comunicações em rede
- Transmissão de telemetria do host
- Monitoramento de equipamentos
- Incident Response

Tecnologias de segurança de ICS avançadas

Kaspersky Industrial CyberSecurity (KICS) é uma plataforma nativa de detecção e resposta estendida (XDR) para empresas industriais, especialmente projetada e certificada para proteger equipamentos, ativos e redes de TO críticos contra ciberameaças. A plataforma compreende tecnologias integradas que garantem a segurança dos componentes principais do sistema de automação e controle industrial em todos os níveis. O KICS for Nodes é um software de proteção, detecção e resposta de endpoint com auditoria de conformidade e funcionalidade de sensor de endpoint. O KICS for Networks foi desenvolvido para análise, detecção e resposta de tráfego de rede de TO. A função de gerenciamento centralizado em nível de site, essencial para dimensionar as operações de segurança TO para um grande volume de infraestruturas industriais diversificadas e geograficamente distribuídas, está integrada à plataforma.

A integração perfeita entre os componentes da plataforma fornece visibilidade total de várias redes de TO geograficamente distribuídas e dos sistemas de automação, proporcionando experiência avançada ao cliente, reconhecimento de situação e flexibilidade de implantação. Com a Detecção e Resposta Estendida, a plataforma KICS permite a convergência de TI e TO e oferece inúmeros benefícios de um único fornecedor.

Pontos de aplicação de plataforma

Convergência de ambientes de TO e de TI

DMZ/GTW

Ambiente de TI

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

Uma solução proprietária de nível de protocolo para monitoramento de rede industrial e análise de tráfego, disponibilizada como software ou como um dispositivo 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 morte do EDR e telemetria) e garante que as ações necessárias sejam tomadas para prevenir qualquer impacto negativo nos processos industriais.

A solução ajuda a detectar e classificar os riscos com base em dados de vulnerabilidades e conexões de rede, bem como o papel de vários ativos, para prevenir incidentes.

Benefícios

Inventário de ativos

Inventário automático de ativos e coleta de dados usando métodos passivos e ativos de coleta de dados

Inventário e visualização de rede

- Mapa de comunicações de rede
- Diagrama de topologia de rede

Avaliação de vulnerabilidade e de risco

- Vulnerabilidade e gestão de riscos específicos de TO
- Pontuação automática e priorização
- Recomendações de remediação de riscos

Detecção de anomalias na rede

Controle de integridade de rede com monitoramento de desvio de linha de base e detecção de atividade de rede maliciosa e suspeita

Controle de processo TO e inspeção profunda de pacotes (DPI)

- Extração de dados de carga útil industrial
- Controle de processo em tempo real
- Controle de comando industrial
- Monitoramento avançado do processo TO por Kaspersky MLAD

Troca de dados e integração

- Informações descentralizadas
- Integração com Kaspersky e sistemas de terceiros ou do cliente (IEC 104, OPC, CEF, Syslog, conectores baseados em API)

Conformidade centralizada auditoria de por nós de rede industrial

KICS for Networks oferece auditoria centralizada de nós de rede industrial, incluindo auditoria baseada em agente (via KICS for Nodes) e auditoria sem agente de hardware de rede e endpoints em busca de vulnerabilidades e conformidade com os padrões da indústria OVAL* e XCCDF**.

- Auditoria de segurança automatizada centralizada para nós do Windows, Linux e dispositivos de rede
- Auditoria de conformidade Editor completo para verificações de conformidade e parâmetros
- Todos os relatórios e dados de ativos estão disponíveis em um só lugar — a base de ativos KICS for Networks
- Cofre protegido para credenciais de nós
- Apoiar quaisquer bases de dados OVAL de terceiros ou personalizadas
- Banco de dados de vulnerabilidades integrado do SCADA por ICS CERT

* Linguagem aberta de avaliação e vulnerabilidade (OVAL)
** O formato de descrição de lista de verificação de configuração extensível (XCCDF)

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

Proteção, detecção e resposta de endpoint de nível industrial, testada e certificada. Uma solução de baixo impacto, compatível e estável para Linux, Windows e sistemas autônomos.

Protege todos os endpoints de um sistema de automação moderno, digital, gerenciado e distribuído. A solução coleta a telemetria para criar uma representação visual clara e detalhada do progresso de um incidente em estações de trabalho, servidores, gateways e outros endpoints, garantindo aos administradores do sistema de automação que um incidente foi totalmente resolvido e não acontecerá novamente.

KICS for Nodes Portable Scanner aplica uma política de cibersegurança em máquinas autônomas, sistemas de automação ou equipamentos nos quais o software de segurança não pode ser instalado. Com uma pequena pegada digital, não interfere nas soluções de segurança existentes.

- Solução sem instalação que oferece consciência situacional máxima e visibilidade de TO, mesmo para uma infraestrutura independente.
- Permite que você faça verificações sob demanda em várias máquinas durante janelas de manutenção simultaneamente e fornece relatórios convenientes.
- Realiza verificações de conformidade antimalware de equipamentos que acessam um site de TO, incluindo computadores de contratantes terceiros.

- Controle de dispositivos
- Controle de integridade de arquivo
- Controle de integridade de PLC
- Anti-Cryptor
- Prevenção contra exploits
- Proteção contra ameaças à rede
- Inspetor de registros do Windows
- Controle de Wi-Fi
- Gerenciamento de firewall
- Monitor de registros
- Auditoria de segurança
- Agente de EDR
- Sensor de endpoint (integração com KICS for Networks)

- Estações de Windows
- Estações de Linux
- Scanner portátil
- Agente de auditoria

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

Benefícios

Baixo impacto

- Baixo impacto nos dispositivos protegidos para o melhor desempenho do sistema
- Não requer reinicialização para instalação, atualização ou melhoria
- Modo somente de detecção disponível
- Consumo ajustável de recursos do sistema

Compatibilidade

- Suporte a sistemas operacionais legados a partir do Windows XP SP2 e Windows Server 2003 SP1
- Compatibilidade com fornecedores de automação industrial
- Scanner portátil como uma opção sem necessidade de instalação

Proteção estendida

- Proteção contra malware, ransomware e explorações
- Análise de registros
- Controle de firewall
- Tecnologia integrada ICS EDR
- Atualizações de banco de dados off-line

Implantação modular

- Opções flexíveis e configurações não intrusivas seguras feitas para TO
- A arquitetura modular permite a seleção apenas dos componentes protetivos necessários

Suporte a PLC

- Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4
- Schneider Electric Modicon M340, M580
- Dispositivos baseados em CODESYS V3
- Fastwel CPM723-01

Auditar

- Padrão aberto OVAL para auditoria abrangente de segurança e conformidade

Fatores de eficácia do Kaspersky XDR

Compreensão contextual de características únicas, requisitos, sistemas especializados, protocolos e considerações operacionais

A integração com ICS permite uma visibilidade e análise abrangentes do tráfego da rede industrial e do comportamento do sistema

Inteligência de ameaças específicas a TO para aproveitar a experiência da Kaspersky na área de proteção contra ameaças ao ambiente industrial

Customização e configuração para adaptar a solução à tolerância específica ao risco, arquitetura de rede e necessidades de conformidade regulatória

Um **único fornecedor** para obter o máximo de suporte e colaboração do fornecedor, incluindo a disponibilização de atualizações e correções pontuais.

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

Os ataques aos sistemas industriais, especialmente ICS e SCADA, estão aumentando. Nunca foi tão importante como agora 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 ponta em cibersegurança industrial e corporativa.

Kaspersky XDR é a ferramenta perfeita para criar um ambiente de trabalho seguro e livre de ameaças. Sua compatibilidade com uma variedade de produtos de segurança facilita o estabelecimento de um ciberespaço seguro, oferecendo opções específicas para a indústria de seu negócio e protegendo você de qualquer ameaça, por menor que seja. As opções de integração do Kaspersky XDR permitem que ele forneça uma visão unificada e abrangente das ameaças, equipando sua equipe de segurança com todas as ferramentas e dados necessários para proteger sua empresa de ameaças atuais e possíveis.

Saiba mais

Convergência TI/TO com Kaspersky Hybrid XDR

Cibersegurança em TI

Saiba mais

Kaspersky Extended Detection and Response

Cibersegurança em TO

Saiba mais

Limites ambientais

Vinte e seis anos de experiência de classe mundial e petabytes de dados de ameaça processados

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 100 certificados de interoperabilidade com soluções de fornecedores de automação

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.br

As marcas registradas e marcas de serviço © 2023 AO Kaspersky Lab são propriedade de seus legítimos proprietários.

#kaspersky
#bringonthefuture