Kaspersky Industrial CyberSecurity: visão geral da solução

kaspersky BRING ON THE FUTURE

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity: visão geral da solução

Introdução

Historicamente, as empresas do setor industrial do mundo inteiro têm maneiras diferentes de abordar a cibersegurança em suas redes de TI e TO (tecnologia operacional). A maioria das empresas já tem medidas amadurecidas de detecção de violações e resposta a incidentes em sua infraestrutura corporativa, mas, no caso da TO, em geral elas utilizam o método clássico de folgas de ar. As indústrias estão se tornando cada vez mais 'digitais', investindo mais e mais em tecnologias inteligentes, novos sistemas de automação e a adoção da Indústria 4.0. Isso realmente acaba com a folga entre os ambientes de TI e TO que é usada para evitar que ameaças cibernéticas cheguem aos sistemas de controle industrial (ICSs, Industrial Control Systems). Segundo o ICS CERT da Kaspersky, na primeira metade de 2019, a porcentagem de computadores de ICSs em que foram detectados objetos maliciosos alcançou 41,2%[1].

O que são essas ameaças?

Primeiramente, elas incluem o risco de infecções acidentais por malware convencional. Você não precisa ser um alvo para se tornar uma vítima. Uma única unidade flash ou e-mail de phishing com um cavalo de Troia direcionado a bancos ou ransomware inserido involuntariamente no ambiente do ICS pode afetar gravemente os negócios centrais da empresa. Mesmo que a ocorrência de infecções acidentais não seja frequente, é claro que um hacker motivado também pode invadir redes de TO e provocar danos consideráveis a equipamentos caros ou à produção, ou ainda roubar informações valiosas.

Quais são as medidas de cibersegurança adequadas para o ICS?

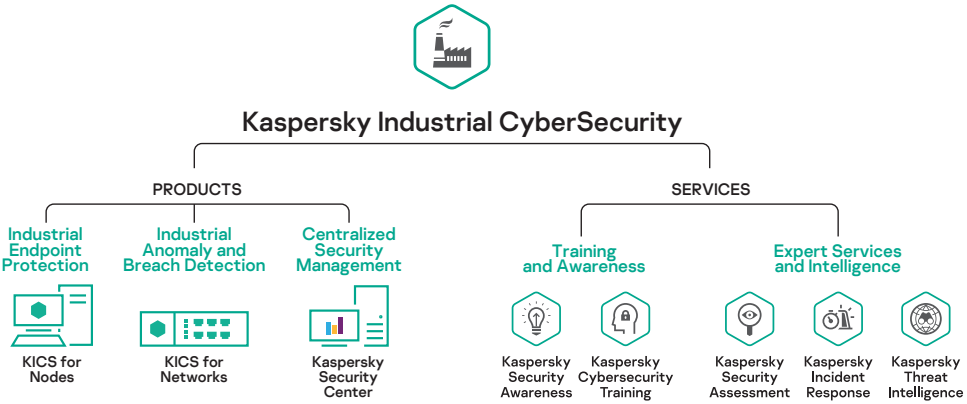
1. Proteção dos endpoints industriais para evitar infecções acidentais e dificultar as invasões deliberadas.
2. Monitoramento da rede de TO e detecção de anomalias para identificar ações maliciosas no nível dos controladores lógicos programáveis (PLCs, Programmable Logical Controllers).
3. Programas de treinamento para funcionários com o intuito de reduzir os acidentes e minimizar as falhas humanas.
4. Serviços de especialistas dedicados para investigar a infraestrutura, realizar análises de dados especializadas ou atenuar o impacto dos incidentes.

1 Cenário de ameaças para sistemas de automação industrial; primeiro semestre de 2019; Kaspersky ICS CERT

O que a Kaspersky oferece?

A **Kaspersky aborda todas as necessidades relacionadas à cibersegurança das indústrias em seu portfólio do Kaspersky Industrial CyberSecurity (KICS).** O KICS oferece uma abordagem holística para a cibersegurança industrial, agregando valor a todos os estágios do processo de segurança da TO do cliente – desde a avaliação da cibersegurança e treinamentos relacionados até tecnologias avançadas e resposta a incidentes.

Componentes do Kaspersky Industrial CyberSecurity



Em 2020, a Kaspersky foi mencionada no relatório da Gartner "Competitive Landscape: Operational Technology Security"[2] como fornecedor representante em quatro categorias de produtos, incluindo:

- Segurança de endpoints da TO;
- Monitoramento e visibilidade da rede da TO;
- Detecção de anomalias, resposta a incidentes e geração de relatórios;
- Serviços de segurança da TO[2].

O Arc Advisory Group enfatiza que a Kaspersky oferece uma combinação exclusiva de inteligência de ameaças, Machine Learning e conhecimento humano que dá suporte à proteção ágil contra qualquer tipo de ameaça[3].

Ao mesmo tempo, um estudo da Forrester[4] mostra um ROI de 368% para uma empresa que usa o Kaspersky Industrial CyberSecurity, além de outros benefícios, como suporte especializado e tranquilidade.

2 Gartner: Competitive Landscape: Operational Technology Security, março de 2020
https://ics.kaspersky.com/KICS-cited-in-Gartnercompetitive-landscape-OTsecurity

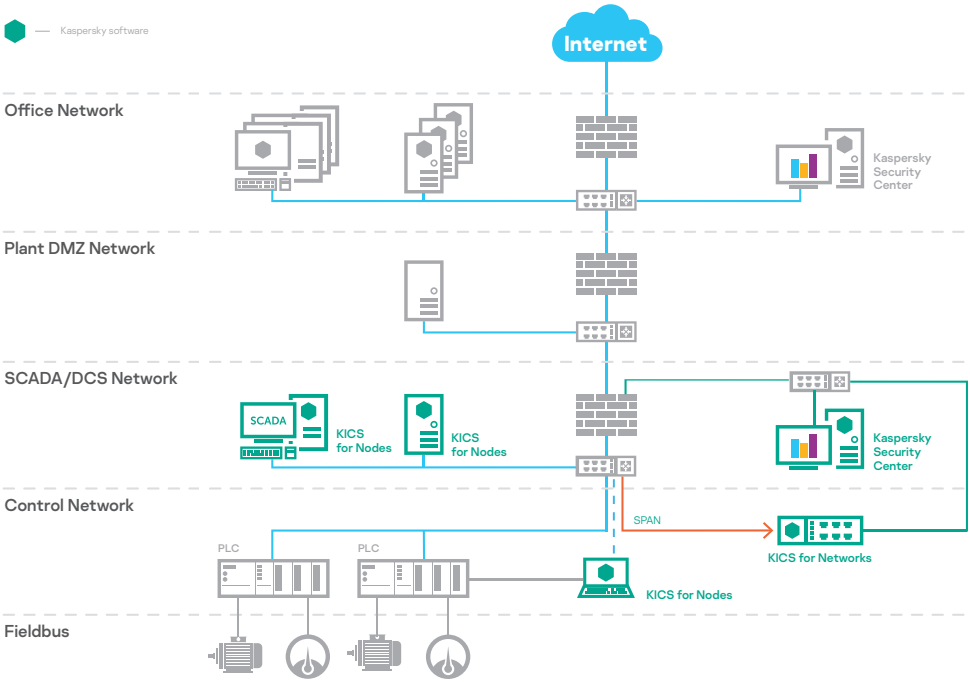
3 Arc Advisory: Kaspersky Moves Forward with Improved Cybersecurity Solutions, 2018

4 Forrester Research: The Total Economic Impact™ of Kaspersky Industrial CyberSecurity, abril de 2019.
https://www.kaspersky.com/ forrester-tei-for-kics

Produtos

Os produtos do **KICS foram projetados para proteger de forma abrangente os elementos industriais da sua organização: O KICS for Nodes está voltado para endpoints industriais, enquanto o KICS for Networks monitora a segurança da rede industrial.**

Implementação de produtos do Kaspersky Industrial CyberSecurity



KICS for Networks

O **KICS for Networks é uma solução de visibilidade e monitoramento de redes de TO, fornecido como dispositivo virtual ou de software e conectado passivamente à rede de ICS.**

Os benefícios:

- ✓ **Descoberta de ativos** identificação e inventário de ativos de TO passivos
- ✓ **Inspeção detalhada de pacotes** análises quase em tempo real de telemetria de processos técnicos
- ✓ **Controle da integridade da rede** detecção de hosts e fluxos de rede não autorizados
- ✓ **Sistema de detecção de invasões** envia alertas sobre atividades de rede maliciosas
- ✓ **Controle de comandos** inspeciona comandos em protocolos industriais
- ✓ **Sistemas externos** recursos de detecção externa por meio de integração via API
- ✓ **Machine Learning para detecção de anomalias (MLAD)** encontra anomalias físicas ou cibernéticas por meio de telemetria em tempo real e mineração de dados históricos (rede neural recorrente)

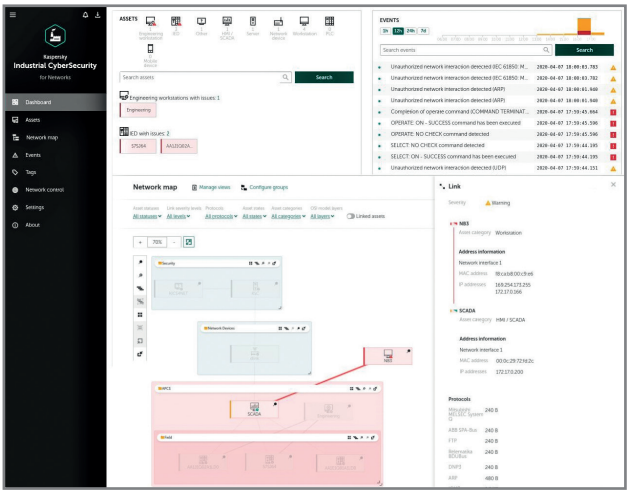
O KICS for Networks detecta anomalias e invasões nas redes de ICS em seus primeiros estágios e garante que sejam tomadas as medidas necessárias para evitar qualquer impacto negativo sobre os processos industriais.

O KICS for Networks é uma solução independente de dispositivo que permite ao cliente escolher o fornecedor de dispositivos de computação industrial que ele mais confia.

A interface do KICS for Networks exibe um painel ao vivo e um mapa da rede, o que possibilita o trabalho com ativos e eventos de segurança.

Exemplo de dispositivo do KICS for Networks

Interface do KICS for Networks



KICS for Nodes

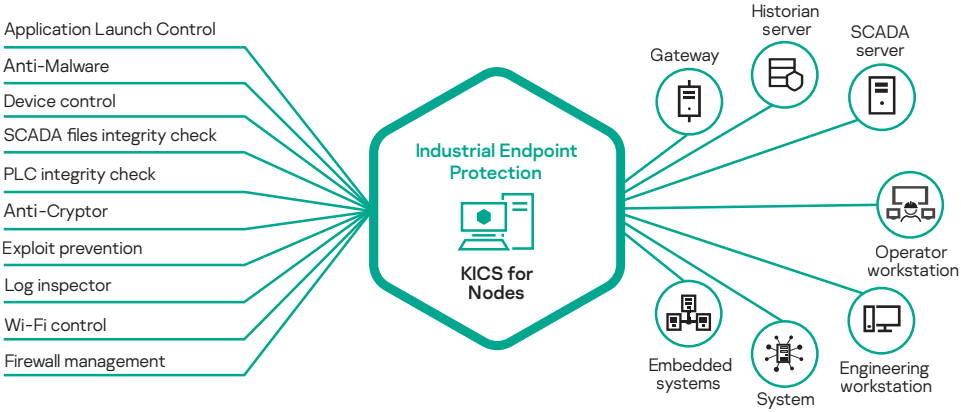
O KICS for Nodes é um produto de segurança de endpoints da TO, fornecido como um software para máquinas Windows e Linux.

Os benefícios:

- ✓ **Baixo impacto em dispositivos protegidos**
- ✓ **A mais alta compatibilidade**
- ✓ **Proteção avançada contra malware**
- ✓ **Controle do ambiente**

O KICS for Nodes foi projetado especialmente para consumir recursos mínimos. Baseado em sistemas de segurança e Embedded, sua arquitetura modular significa que você só precisa instalar os componentes de proteção de que necessita. Os componentes de proteção podem ser configurados para o modo de prevenção de ameaças ou para o modo somente detecção. Essa abordagem é ideal para máquinas herdadas de baixo desempenho que exigem o máximo de poder de computação disponível.

Funções do KICS for Nodes e endpoints compatíveis



"Nós decidimos firmar parceria com a Kaspersky porque era possível implementar o Kaspersky Industrial CyberSecurity sem precisar interromper nossas operações e também porque a solução é compatível com os sistemas de controle que usamos"

Jan Houben, gerente de fábrica da AGC Glass Germany GmbH

O KICS for Nodes protege os nós industriais de vários tipos de ameaças cibernéticas resultantes de fatores humanos, malware genérico, ataques direcionados ou sabotagem. Ele é compatível com componentes de software e hardware de sistemas de automação industrial, como SCADA, PLC e DCS.

Kaspersky Security Center

O **Kaspersky Security Center é uma solução de gerenciamento de segurança centralizado. Ele fornece controle e visibilidade das camadas industriais em vários locais, bem como das redes corporativas ao redor.**

Os benefícios:

- ✓ **Gerenciamento de sistemas**
  - Coleta centralizada de dados do sistema
  - Implementação de software centralizada
  - Detecção de vulnerabilidades e gerenciamento de patches
  - Recursos de gerenciamento de clientes estendido
- ✓ **Gerenciamento de políticas**
  - Gerenciamento centralizado de políticas de segurança
  - Programação e execução remotas de tarefas
- ✓ **Relatórios e notificação**
  - Log de eventos
  - Painéis e relatórios
  - Notificações por SMS/e-mail
- ✓ **Integração com SIEMS**
  - Arcsight, Splunk, Qradar
  - Servidor Syslog
- ✓ **Integração com HMI**
- ✓ **Integração com o painel do MES**
  - Status de segurança e fornecimento de informações para host compatível com IEC 104/OPC 2.0

Kaspersky Industrial CyberSecurity: serviços

Nosso pacote de serviços é uma parte importante do portfólio do KICS – nós fornecemos todo o ciclo de serviços de segurança, da avaliação de cibersegurança industrial até a resposta a incidentes.

Serviços especializados

"A experiência deles na área de cibersegurança de ICS, o profissionalismo e a complexidade da solução, em comparação com outros fornecedores, nos trouxeram grande valor agregado e garantiram um futuro brilhante para a estratégia de segurança de nossa empresa"

Ondřej Sýkora, gerente de C&A da Plzeňský Prazdroj

- **Avaliação da cibersegurança industrial:** A Kaspersky oferece uma avaliação da cibersegurança industrial minimamente invasiva, incluindo testes de penetração externo e interno, avaliação da segurança da TO e avaliação da segurança da solução de automação. Especialistas da Kaspersky fornecem insights importantes sobre a infraestrutura da empresa e fazem recomendações sobre como fortalecer a postura de cibersegurança do ICS.
- **Inteligência de ameaças:** Análises de dados atualizadas coletadas por especialistas da Kaspersky ajudam a melhorar a proteção do cliente contra ataques cibernéticos industriais direcionados. Fornecidas como feeds de inteligência de ameaças ou relatórios personalizados, essas análises atendem a necessidades específicas do cliente, de acordo com parâmetros regionais, de setor e de software de ICS.

"Ao realizar o exercício e aprender com o conhecimento da equipe da Kaspersky, nós reforçamos a proteção contra ameaças de cibersegurança"

Yu Tat Ming, CEO da PacificLight

- **Resposta a incidentes:** Caso ocorra um incidente de cibersegurança, nossos especialistas coletam e analisam os dados, reconstituem o desenrolar do incidente, determinam possíveis fontes e motivações, e elaboram um plano de recuperação. Além disso, a Kaspersky oferece um serviço de análise de malware, com o qual seus especialistas categorizam todas as amostras de malware fornecidas, analisam suas funções e comportamento e desenvolvem recomendações e um plano para sua remoção do sistema e para reverter qualquer ação maliciosa.

Treinamento e conscientização

"A Kaspersky era a melhor empresa para dar treinamento em habilidades de cibersegurança industrial profissional para nosso grupo de ICS"

Søren Egede Knudsen, diretor técnico da Ezenta

- **Treinamento em conscientização sobre cibersegurança industrial:** Módulos de treinamento interativo no local e on-line e jogos de cibersegurança para os funcionários que interagem com sistemas industriais computadorizados e seus gerentes. Os participantes obtêm uma nova perspectiva do atual cenário de ameaças e dos vetores de ataque direcionados especificamente ao ambiente industrial, exploram cenários práticos e adquirem habilidades de trabalho de cibersegurança. O curso no local pode ser personalizado e adaptado para durar um ou dois dias.

- **Programas de treinamento de especialistas:** Os módulos de treinamento em Testes de penetração de ICS e Perícias digitais de ICS foram desenvolvidos para profissionais de cibersegurança. Os participantes obtêm todas as habilidades avançadas necessárias para realizar testes de penetração abrangentes ou perícias digitais em ambientes industriais. Certificação incluída.

Saiba mais sobre o KICS em
https://ics.kaspersky.com

#Kaspersky
#BringontheFuture

www.kaspersky.com.br

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

* Prêmio World Leading Internet Scientific and Technological Achievement Award na 3rd World Internet Conference

** Prêmio especial da China International Industry Fair (CIIF) 2016