KASPERSKY lab

Kaspersky Industrial CyberSecurity: overview 2018

www.kaspersky.com/ics
#truecybersecurity

Kaspersky Industrial CyberSecurity: visão geral das soluções em 2018

Ataques em sistemas industriais estão aumentando

Ataques cibernéticos em sistemas de controle industrial não estão apenas aumentando, mas passaram de especulativo para indiscutível [1]. Três em cada quatro empresas do setor industrial acreditam que tiveram um ataque cibernético em seus sistemas de controle [2]. Interrupção nos Negócios e na cadeia de suprimentos foram classificados como a preocupação de risco número um globalmente nos últimos seis anos; incidente cibernético ficou em segundo lugar em 2017 [3].
Para empresas que operam sistemas industriais ou infraestrutura crítica, os riscos nunca foram tão grandes. A segurança industrial tem consequências que vão muito além dos negócios e da reputação proteção. Quando se trata de proteger sistemas industriais de ameaças cibernéticas, existem considerações específicas e significantes em termos ecológicos, sociais e e macroeconômicos.

[1] PwC: Global State of Information Security 2015.
[2] SANS 2016 State of ICS Security Survey
[3] Allianz Risk Barometer 2017

Tecnologia operacional vs. Tecnologia da informação

Definido pelo padrão de automação IEC 62443, um sistema de controle industrial (ICS, na sigla em inglês) trata-se de um conjunto de pessoal, hardwares e softwares que podem afetar ou influenciar uma operação segura e confiável de um processo industrial (tecnológico).

Sistemas de controle industral incluem, mas não estão limitados a:

- Sistemas de Controle Distribuído (DCSs), Controladores Lógicos Programáveis (PLCs), Unidades Terminais Remotas (RTUs), Dispositivos Eletrônicos Inteligentes (IEDs), Controle de Supervisão e Aquisição de Dados (SCADA) e sistemas de diagnóstico.
- Associação de pessoas, redes de comunicação, interfaces de máquinas com o propósito de prover controle, segurança e funcionalidade operacional de manufatura para processos contínuos, discretos, de batelada, entre outros.

De forma mais sofisticada, infraestrutura de sistema industrial pode ser dividida em dois domínios:

- Tecnologia da Informação (TI) – sistemas para gerir dados no contexto de objetivos de negócio.
- Tecnologia Operacional (TO) – sistemas para gerenciar os processos de automação industrial.

As estratégias de segurança de TI tendem a ter por foco a proteção de dados, e a seguir os objetivos do modelo "C-I-A", em português: Confidencialidade de dados, Integridade e Disponibilidade. No entanto, para a maioria dos sistemas de TO, cibersegurança não se trata de dados, mas sim da garantia de continuidade dos processos tecnológicos. Portanto, em termos do modelo C-I-A, a 'disponibilidade' (availability, na expressão em inglês) é o termo principal das estratégias de segurança aplicadas à TO.
Isso distingue as necessidades de cibersegurança industrial, o que significa que mesmo a mais eficaz solução de cibersegurança de TI clássica é inapropriada para o uso em sistemas TO, o que deixa a disponibilidade (e em alguns casos a integridade) dos processos em risco.

Riscos e ameaças

Apesar da crescente preocupação com o crescimento dos ciberataques em sistemas de controle industrial, muitos modelos de segurança de TI continuam aderindo à crença de que isolar fisicamente sistemas (por meio de 'airgaps') e 'security by obscurity' é o suficiente. O que está longe de ser verdade – na era da indústria 4.0, a maioria das redes industriais não críticas são acessíveis via internet4, por escolha ou não. A pesquisa profunda feita pela Kaspersky Lab ICS CERT, com dados da Kaspersky Security Network, indica que os PCs industriais são regularmente atacados pelos mesmos malwares genéricos que afligem os sistemas de negócios (TI), que inclui (mas não se restringe) aos notórios trojans, vírus e worms. Durante a segunda metade de 2017, os produtos da Kaspersky Lab ao redor do mundo bloquearam tentativas de ataques em 37,8% de todos os computadores protegidos pela Kaspersky identificados como parte de uma infraestrutura industrial[5].

Outra ameaça em ascensão para ICS é o ransomware. O alcance e a diversidade desse tipo de vírus cresceram massivamente entre 2015 e o começo de 2017. Os usos desses são altamente significativos para o setor industrial – tais contaminações podem causar impacto de longo alcance em sistemas críticos, fazendo da ICS um alvo particularmente atrativo – como comprovado por vários incidentes provocados por ransomwares direcionados a sistemas SCADA durante 2017 (especialmente infecções do tipo WannaCry e exPetr). Eles são projetados para atacar sistemas industriais e podem ter seus objetivos específicos – no lugar de criptografar dados, o malware pode interromper operações ou bloquear o acesso a um recurso importante.

Assim como ameaças genéricas, a segurança industrial deve lidar com malwares específicos de ICS e ataques direcionados: Stuxnet, Havex, BlackEnergy, PLC Blaster, Ladder Logic Bomb, Pin Control Attack – a lista só aumenta. Como os ataques Stuxnet e BlackEnergy mostram, mídias USB infectadas ou um simples e-mail de phishing são suficientes para que cibercriminosos bem preparados invadam uma rede isolada.

Além dos malwares e ataques direcionados, as organizações industriais enfrentam outras ameaças e riscos, as quais, por sua vez, visam pessoas, processos e tecnologias –subestimar esses riscos podem tornar reais sérias consequências. A Kaspersky Lab desenvolve soluções e serviços que ajudam nossos clientes a lidar e gerenciar não somente malwares e ataques direcionados, mas também com outros ciberincidentes e fatores de risco, como:

[4] ICS e sua eficiência online 2016, Kaspersky Lab

[5] Cenário de ameaças para sistemas automotivos industriais para H2 2016, Kaspersky Lab ICS CERT.

- Erros de operadores do SCADA ou terceirizados;
- Ações fraudulentas;
- Cibersabotagem;
- Compliance;
- Falta de conhecimento e dados brutos para investigação forense.

A necessidade de cibersegurança industrial especializada

Somente fornecedores de cibersegurança que entendem as diferenças entre corporações industriais e orientadas para dados podem oferecer soluções que vão de encontro as necessidades únicas de segurança de sistemas e infraestruturas de controle industrial. A Forrester Research aconselha as organizações industriais a selecionar um fornecedor de segurança com o objetivo de "buscar conhecimentos especializados em indústria". A entidade identifica a Kaspersky Lab como um dos poucos desenvolvedores com conhecimentos especializados genuínos neste setor.

Kaspersky Lab: fornece segurança industrial confiável

Líder reconhecida em cibersegurança e proteção industrial[6], a Kaspersky Lab pesquisa e desenvolve continuamente soluções empenhadas na luta contra as ameaças em constante evolução às infraestruturas críticas e industriais. Desde a gestão de operações até o nível ICS e além, a Kaspersky Lab desempenha papel importante de auxílio à indústria, no âmbito da regulamentação e em parceria com as agências governamentais do mundo todo, tem como objetivo comum antecipar mudanças no cenário de ameaças e defender contra elas.

Como parceira confiável para organizações industriais líderes de mercado as quais contam há muitos anos com nossa proteção anti-malware, a Kaspersky Lab colabora com fornecedores e organizações reconhecidas de automação industrial, entre os quais Emerson, SAP, Siemens, Schneider Electric, Industrial Internet Consortium e outras, a fim de estabelecer compatibilidade, procedimentos especializados e estruturas de cooperação que protejam ambientes industriais de ameaças existentes e emergentes, bem como ataques altamente direcionados.
A Kaspersky Lab desenvolveu um portfólio de soluções especializadas com foco nas necessidades específicas do mercado de cibersegurança industrial - Kaspersky Industrial CyberSecurity (KICS). Essas soluções oferecem segurança efetiva contra ciberameaças em todos os níveis ICS – incluindo servidores SCADA, HMI, estações de trabalho e estações de

[6] Gartner Market Guide for Operational Technology Security, 2016

engenharia, PLCs e conexões de rede industrial – sem gerar impacto na continuidade e estabilidade operacional dos processos tecnológicos.

De acordo com a estratégia global de segurança multicamadas da Kaspersky Lab, a Kaspersky Industrial CyberSecurity oferece uma combinação de métodos de proteção. Com uma abordagem holística para a segurança cibernética industrial - desde a previsão de potenciais vetores de ataque, por meio de técnicas especializadas de detecção e prevenção, até a capacidade de responder proativamente a um incidente cibernético - o que se situa como garantia final do funcionamento ininterrupto e seguro de sua organização.

A arquitetura de segurança adaptativa

Kaspersky Industrial CyberSecurity: serviços

Nosso conjunto de serviços é parte importante do portfólio do KICS - fornecemos o ciclo completo de serviços de segurança, desde a avaliação industrial da cibersegurança até a resposta a incidentes.

Conhecimento (educação e inteligência)

- **Treinamento:** a Kaspersky Lab oferece cursos de treinamento desenhados para especialistas de TI/TO e operadores e engenheiros ICS. Durante o treinamento, os participantes adquirem informações sobre ameaças cibernéticas relevantes, suas tendências de desenvolvimento e métodos mais eficazes de proteção. Os cursos também permitem que profissionais de segurança desenvolvam suas habilidades em áreas específicas, entre essas: ICS Penetration Testing e Digital Forensics.

- **Programas de conscientização:** para aumentar a conscientização sobre questões relevantes de cibersegurança industrial, além de desenvolver as habilidades necessárias para abordá-las e resolvê-las, a Kaspersky Lab oferece "jogos" de

treinamento para gerentes de segurança e engenheiros. Por exemplo, o Kaspersky Industrial Protection Simulation (KIPS) replica ciberataques reais em sistemas de automação industrial, e demonstra os principais problemas associados ao fornecimento de cibersegurança da indústria.

- **Relatórios de Inteligência:** relatórios atualizados de inteligência de ameaças são preparados por nossa equipe de resposta a ataques cibernéticos a ICS.

Serviços especializados

- **Avaliação de cibersegurança:** para organizações preocupadas com o potencial impacto operacional da segurança de TI/TO, a Kaspersky Lab oferece uma avaliação industrial de segurança cibernética minimamente invasiva. Esse é um primeiro passo crucial no estabelecimento das exigências de segurança dentro do contexto de necessidades operacionais, essa avaliação pode fornecer uma visão significativa dos níveis de segurança cibernética, mesmo sem implantar mais tecnologias de proteção.

- **Integração de soluções:** se os sistemas de controle industrial de uma organização tiverem uma arquitetura única ou estiverem baseados em componentes de hardware e software personalizados não amplamente utilizados na indústria, a Kaspersky Lab, pode adaptar as ferramentas recomendadas de segurança cibernética para trabalhar com esses sistemas. Este serviço incorpora suporte para sistemas de software e hardware exclusivos, incluindo SCADA proprietário, PLCs e protocolos de comunicação industrial.

- **Investigação de incidentes:** no caso de um incidente de segurança cibernética, nossos especialistas coletarão e analisarão dados, reconstruirão o cronograma do incidente, determinarão possíveis fontes, motivação e desenvolverão um Plano de remediação. Além disso, a Kaspersky Lab oferece um serviço de análise de malware - dentro de sua estrutura, os especialistas da Kaspersky Lab categorizam qualquer amostra de malware fornecida, analisam suas funções e comportamento para desenvolver recomendações e um plano para a remoção do malware e para reverter quaisquer ações mal-intencionadas .

Kaspersky Industrial CyberSecurity: gestão centralizada de segurança

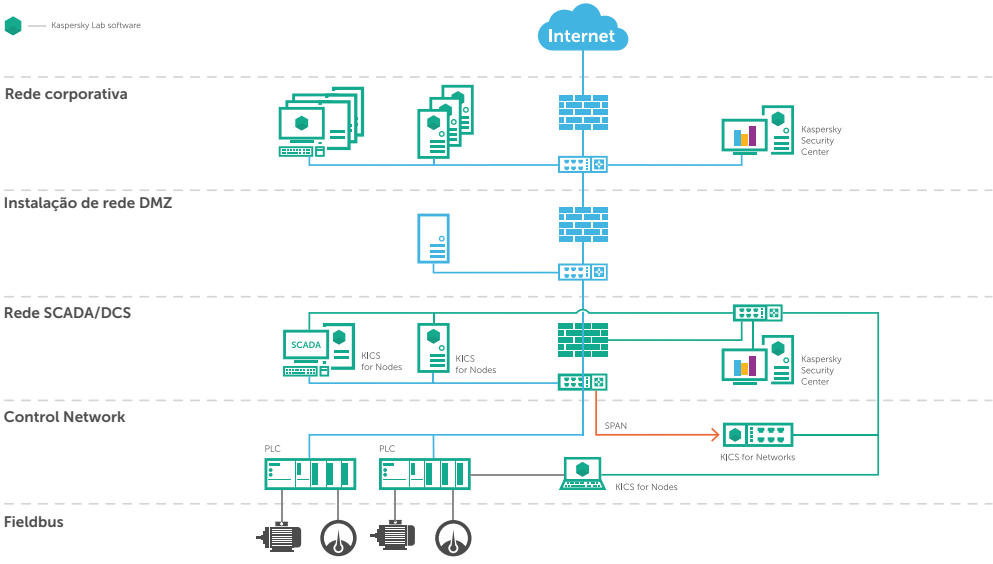
Kaspersky Security Center

Para garantir a melhor proteção contra todos os vetores de ataque, a segurança a nível industrial deve operar na rede e em seus nós. De forma a garantir um controle otimizado, facilidade de gerenciamento e visibilidade, o KICS - como todas as tecnologias de proteção da Kaspersky Lab - é controlado por meio de um

único console de gerenciamento, o Kaspersky Security Center que viabiliza:

- Gerenciamento centralizado de políticas de segurança – capacidade de ajustar diferentes configurações para diferentes nós e grupos.
- Testes facilitados de atualizações antes de implementá-las na rede, o que garante que o processo será finalizado de forma íntegra.
- Acesso baseado em atribuições, alinhado com as políticas de segurança e ações urgentes.

O Kaspersky Security Center garante a facilidade de controle e visibilidade não só para camadas industriais em vários locais, mas em todos os andares de negócios adjacentes, conforme ilustrado abaixo.



Kaspersky Security Gateway

O KICS também é capaz de enviar dados relacionados a eventos para outros sistemas, como SIEMs, MESs e soluções de Business Intelligence. Todos os eventos e anomalias detectados são relatados a sistemas terceiros - incluindo SIEM, mail, servidores syslog e sistemas de gerenciamento de rede - por meio de protocolos CEF 2.0, LEEF e Syslog. Além de ajudar a detectar, contornar e investigar ataques cibernéticos, o monitoramento detalhado da rede industrial suporta manutenção preventiva.

Integração com interfaces Human-Machine (HMIs)

A solução pode mandar notificações de segurança diretamente para HMIs e fornece às equipes informações que favoreçam reação imediata de modo a impedir que os ciberincidentes se agravem.

Kaspersky Industrial CyberSecurity for Nodes

O KICS for Nodes, ou nós de rede, foi projetado para abordar especificamente ameaças ao nível de operação em ambientes ICS. A solução protege os servidores ICS/SCADA, as HMIs e estações de trabalho e de engenharia contra os vários tipos de ataques cibernéticos passíveis de serem causados por fatores humanos, malware genérico, ataques direcionados ou sabotagem. O KICS for Nodes é compatível com os componentes de software e hardware de sistemas de automação industrial, como SCADA, PLC e DCS.

Ameaças e fatores de risco	Tecnologias Kaspersky Lab
Execução de software não-autorizada	Whitelisting; apenas modos de prevenção ou detecção (registro no lugar de bloqueio)
Malware	Mecanismos avançados de detecção anti-malware baseados em assinatura; Mecanismo de detecção baseado em nuvem, o qual usa a nuvem pública da Kaspersky Lab (KSN) ou a nuvem privada (KPSN)
Cryptors, incluindo ransomware	Anti-cryptor
Ataques de rede	Firewall baseado em Host
Conexão não autorizada de dispositivo	Controle de dispositivo
Conexão wireless não autorizada	Controle de rede Wi-Fi
Fraudes de programas PLC	Verificação de integridade do PLC
Específicos de ICS — airgaps; falsos positivos para software/processos ICS, etc.	Atualizações confiáveis, testadas com softwares de líderes no fornecimento industrial; certificação de produto por fornecedores de vanguarda em automação industrial.

Listas de aplicativos confiáveis

A natureza relativamente estática das configurações dos terminais ICS significa que as medidas de controle de integridade são significativamente mais eficazes do que nas redes corporativas dinâmicas. As tecnologias de controle de integridade apresentadas no KICS for Nodes incluem:

- Controle da instalação e inicialização do aplicativo de acordo com as listas de aplicações confiáveis (boas práticas para redes de controle industrial) ou políticas de objetos 'não confiáveis'.
- Controle do acesso de aplicativos aos recursos do sistema operacional: arquivos, pastas, registro , entre outros.
- Controle de todos os tipos de executáveis em ambientes Windows, incluindo .exe, .dll, .ocx, drivers, ActiveX, scripts, interpretes de linha de comando e drivers de kernel-mode.

- Atualização de dados de reputação de aplicativos.
- Categorias de aplicativos pré-definidas e determinadas pelo cliente com objetivo de gerenciar listas de aplicativos controlados.
- Ajustes refinados dos controles de aplicativos para diferentes usuários.
- Modos de prevenção ou de detecção: bloqueia qualquer aplicativo que não esteja na lista de confiáveis ou, executa no modo "visualização", o que permite que aplicativos não presentes na lista de permitidos sejam executados, sob monitoramento de atividade por parte do Kaspersky Security Center, que realizará avaliação acerca da natureza do programa.

Controle de dispositivo

Gerenciamento de acesso a dispositivos removíveis, periféricos e system busses, com base na categoria do dispositivo, família e identificação específica desse.

- Suporte para abordagens de lista de confiáveis ou não.
- Atribuição de política granular, por computador, por usuário, para um único usuário/computador ou grupo usuário/computador.
- Modo de prevenção ou somente de detecção.

Firewall baseado em Host

Configuração e aplicação de políticas de acesso à rede para nós protegidos, como servidores, HMIs ou estações de trabalho. As funcionalidades principais incluem:

- Controle de acesso em portas e redes restritas.
- Detecção e bloqueio de ataques de rede a partir de fontes internas, como laptops de terceiros, passíveis de introduzir um malware a fim de realizar infecção do Host durante conexão com a rede industrial.

Controle de rede Wi-Fi

Permite o monitoramento de qualquer tentativa não autorizada de conexão às redes Wi-Fi. A ferramenta Wi-Fi Control é baseada na tecnologia Default Deny, a qual implica bloquear automaticamente as conexões a qualquer rede do tipo "não permitida" nas configurações.

Verificação de integridade de PLC

Permite o controle adicional sobre as configurações do PLC por meio de verificações periódicas contra um servidor selecionado e seguro da Kaspersky Lab. Os resultados da verificação são comparados com os valores padronizados, de modo que todos os desvios são relatados.

Monitor de Integridade de Arquivos

Este recurso foi projetado para rastrear ações executadas em arquivos e pastas de arquivos especificados nas configurações de tarefa. Você pode usá-lo para detectar mudanças que possam indicar uma violação de segurança no servidor protegido - como alterações nos projetos do SCADA armazenados no servidor SCADA.

Proteção avançada anti-malware

As melhores tecnologias proativas de detecção e prevenção de malwares da Kaspersky Lab são adaptadas e desenvolvidas para atender o alto consumo de recursos e requerimentos de diponibilidade de sistema. Nossa avançada proteção anti-malware é projetada para funcionar efetivamente mesmo em ambientes estáticos ou raramente atualizados. O anti-malware da Kaspersky Lab cobre todo o espectro de tecnologias, incluindo:

- Detecção de malwares baseados em assinatura;
- Detecção no acesso e sob demanda;
- Detecção na memória (residente);
- Detecção Ransomware por meio de tecnologia especial Anti-Cryptor;
- Kaspersky Security Network (KSN) e a Kaspersky Private Security Network (KPSN) favorecem um melhor serviço de detecção de malwares.

Atualizações confiáveis

Para garantir que as atualizações de segurança da Kaspersky Lab não tenham impacto na continuidade do sistema protegido, verificações de compatibilidade são realizadas previamente tanto para lançamentos de base de dados / componentes como para processos de controle do sistema de software/configuração de atualizações. Os possíveis problemas de consumo de recursos podem ser detectados por meio de vários cenários diferentes:

- A Kaspersky Lab realiza verificações de compatibilidade de atualização de dados com o fornecedor de software SCADA em plataformas de teste da Kaspersky Lab.
- O seu fornecedor SCADA realiza verificações de compatibilidade.
- A Kaspersky Lab verifica as atualizações de segurança de base de dados para você: SCADA, estações de trabalho, servidor e imagens HMI são integradas nas plataformas experimentais da Kaspersky Lab.
- As atualizações de segurança da Kaspersky Lab são testadas em nossas instalações e automatizadas via Kaspersky Security Center.

Kaspersky Industrial CyberSecurity for Networks

A solução de segurança de nível de rede da Kaspersky Lab opera a nível de protocolo de comunicação industrial (Modbus, IEC stack, ISO, etc.), analisa tráfego industrial para anomalias por meio da tecnologia avançada de DPI (Deep Packet inspection). O controle de integridade da rede e os recursos IDS também são fornecidos.

Ameaças e fatores de risco	Tecnologias Kaspersky Lab
Surgimento de dispositivos de rede não autorizados em rede industrial	Network Integrity Control detecta dispositivos novos/desconhecidos
Surgimento de comunicações não autorizadas na rede industrial	Network Integrity Control monitora as comunicações entre dispositivos conhecidos/desconhecidos
Comandos maliciosos do PLC: • Comando enviado por um operador ou terceiro contratado • Insider (ações de fraude) • Ataque/Malware	A Tecnologia DPI analisa comunicações de/para PLCs e exerce controle sob os comandos e valores de parâmetros do processo tecnológico.
Ataques de rede	Um Sistema Avançado de Detecção de Intrusão identifica todos os padrões de ataque de rede conhecidos, incluindo exploração de vulnerabilidades em software e hardware industriais
Falta de dados para investigação e análise forense	Ferramentas forenses: monitoramento e registro seguro de eventos suspeitos na rede industrial e ataques detectados.

Inspeção de tráfego não-invasiva na rede industrial

O KICS for Networks oferece monitoramento passivo de tráfego de anomalias e segurança de rede, permanece invisível para potenciais ataques. A instalação é tão simples como habilitar/configurar o espelhamento de portas; a integração facilitada entre software e dispositivo virtual ou hardware em equipamentos de rede industrial existentes é obtida por meio da porta SPAN do Switch ou através de um TAP. O KICS for Networks possui uma arquitetura modular - os sensores podem ser implantados separadamente a partir de uma unidade de controle central.

Industrial DPI para detecção de anomalias

O KICS for Networks fornece aos usuários industriais uma plataforma confiável para monitorar o fluxo de comando do controle de processo e telemetria de dados, o que permite, entre outras coisas:

- Detecção de qualquer comando que reconfigure um PLC ou altere o seu estado.
- Parâmetro de controle de mudanças nas variáveis de processo.
- Proteção contra ameaças externas, ao mesmo tempo que elimina o risco de interferência "avançada" de engenheiros, operadores SCADA ou outros funcionários internos com acesso direto aos sistemas.

Aprendizado de Máquina

Nosso DPI (Deep Package Inspection) industrial não só pode ser configurado por uma abordagem baseada em regras padrão - também possui a possibilidade de detectar anomalias dentro de processos industriais por meio de um poderoso modelo de previsão baseado em LSTM. O aprendizado de máquina eleva a detecção de anomalia industrial a um novo nível, possibilita a descoberta de incidentes nas redes industriais mais complexas e freqüentemente reconfiguradas.

Controle de integridade da rede para inventário de segurança e de ativos

O KICS for Networks identifica todos os ativos conectados à rede Ethernet - incluindo servidores SCADA, HMIs, estações de trabalho e de engenharia, PLCs, IEDs e RTUs. Todos os dispositivos novos ou desconhecidos e suas comunicações são detectados automaticamente. Isso fornece às equipes de segurança a capacidade de desenvolver seu próprio, confiável e seguro inventário de ativos de rede, no lugar de usar ferramentas de gerenciamento de ativos TO/TI potencialmente vulneráveis altamente visadas por cibercriminosos.

Ferramentas forenses

A solução da Kaspersky Lab fornece aos usuários industriais um sistema seguro de registro, que disponibiliza ferramentas para análise de dados e perícia digital. O sistema também impede qualquer alteração nos registros do ICS.

Serviços adicionais da Kaspersky Industrial CyberSecurity

Kaspersky Security Network

A Kaspersky Security Network (KSN) é uma arquitetura distribuída complexa baseada em nuvem, dedicada a reunir e analisar inteligência de ameaças de segurança a partir de milhões de nós em todo o mundo. A KSN não só detecta e bloqueia as mais recentes ameaças e ataques de zero-day, como ajuda a localizar e inserir em listas de 'não confiáveis' fontes de ataques fornecendo dados de reputação para sites e aplicativos.

Todas as soluções corporativas da Kaspersky Lab, o que inclui as soluções industriais, podem ser conectadas à KSN, se necessário. Alguns dos principais benefícios são:

- Taxas de detecção superiores;
- Tempos de reação reduzidos -baseados em assinatura tradicional levam horas: KSN reage em cerca de 40 segundos;
- Taxas baixas de falsos positivos;
- Consumo reduzido de recursos para soluções de segurança no local.

Kaspersky Private Security Network (KPSN)

Para organizações com preocupações muito específicas com a privacidade de dados, a Kaspersky Lab desenvolveu a opção Kaspersky Private Security Network. Ela fornece quase todas as vantagens do KSN, mas sem enviar qualquer informação para fora da rede.

A KPSN pode ser implantada no centro de dados de qualquer organização, onde os especialistas de TI internos mantém o controle total sobre esse. As instalações locais do KPSN podem ajudar a atender aos requisitos de compliance específicos do país ou legislação inerente a atividade industrial.

Funções importantes KPSN:

- Serviços de reputação de arquivos e URL: hashes MD5 para arquivos, expressões regulares para URLs e padrões de comportamento de malware são armazenados; centralmente, categorizados e rapidamente implantados para o cliente;
- Software de Gerenciamento de Gravação (RMS): às vezes, os softwares de segurança cometem erros e incorretamente categorizam arquivos ou URLs como confiáveis/não confiáveis. O RMS atua impedindo "falsos positivos", retificando erros e analisando continuamente para melhorar a qualidade;
- Informação e inteligência baseadas na nuvem.

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity é um portfólio de tecnologias e serviços projetados para proteger as camadas de tecnologia operacional e elementos da sua organização - incluindo servidores SCADA, HMIs, estações de engenharia, estações de trabalho, PLCs, conexões de rede e até engenheiros - sem impacto na continuidade operacional e na consistência do processo industrial.

Saiba mais em
www.kaspersky.com/ics

Tudo sobre cibersegurança ICS:
https://ics.kaspersky.com
Notícias de ciberameaças: **www.securelist.com**

#truecybersecurity

www.kaspersky.com.br

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

* Prêmio Líder Mundial de Conquistas Científicas e Tecnológicas na 3ª Conferência Mundial da Internet.

** Prêmio especial na China Internacional Industry Fair (CIIF) em 2016