Resiliência cibernética industrial – oito etapas para proteger sua empresa

A segurança cibernética industrial pode ser abrangente.
Ganhe visibilidade dividindo sua estratégia nessas oito etapas.

kaspersky bring on the future

Primeira edição: Fevereiro de 2025

Conteúdo

Introdução

Se a complexidade e a automação são proeminentes em sua organização, sua superfície de ataque provavelmente é ampla, com um excesso de esconderijos para agentes mal-intencionados. Nossos especialistas em segurança cibernética industrial monitoram sistemas de controle industrial (ICS) globalmente e uma parte significativa deles é direcionada todos os meses. Os criminosos aproveitam tudo, desde scripts maliciosos e páginas de phishing até worms, vírus e ransomware – todos os quais podemos repelir.

A maioria dos ataques cibernéticos industriais começa na infraestrutura de tecnologia da informação (TI) do alvo, na cadeia de suprimentos ou no pool de contratados antes de sangrar para a tecnologia operacional (OT) e causar interrupções. Isso é problemático porque as vítimas geralmente têm uma baixa tolerância ao tempo de inatividade, com interrupções na produção convidando a pressão de terceiros afetados. Na infraestrutura crítica, é pior ainda porque as consequências não se limitam aos clientes – há impactos no mundo real sobre o público, como luzes se apagando ou torneiras secando.

Um ataque bem-sucedido pode afetar não apenas a estratégia e a reputação de uma organização, mas também levar a interrupções de processos, interrupções na cadeia de suprimentos, perdas financeiras e problemas regulatórios. As empresas de alto perfil devem, portanto, respeitar a segurança cibernética industrial, que é a pedra angular de qualquer estratégia de transformação digital sensata.

Ao adotar práticas abrangentes de segurança de IT-OT, essas organizações podem evitar a interrupção de operações críticas e mitigar a maioria dos riscos financeiros, de reputação e tecnológicos representados por ataques cibernéticos.

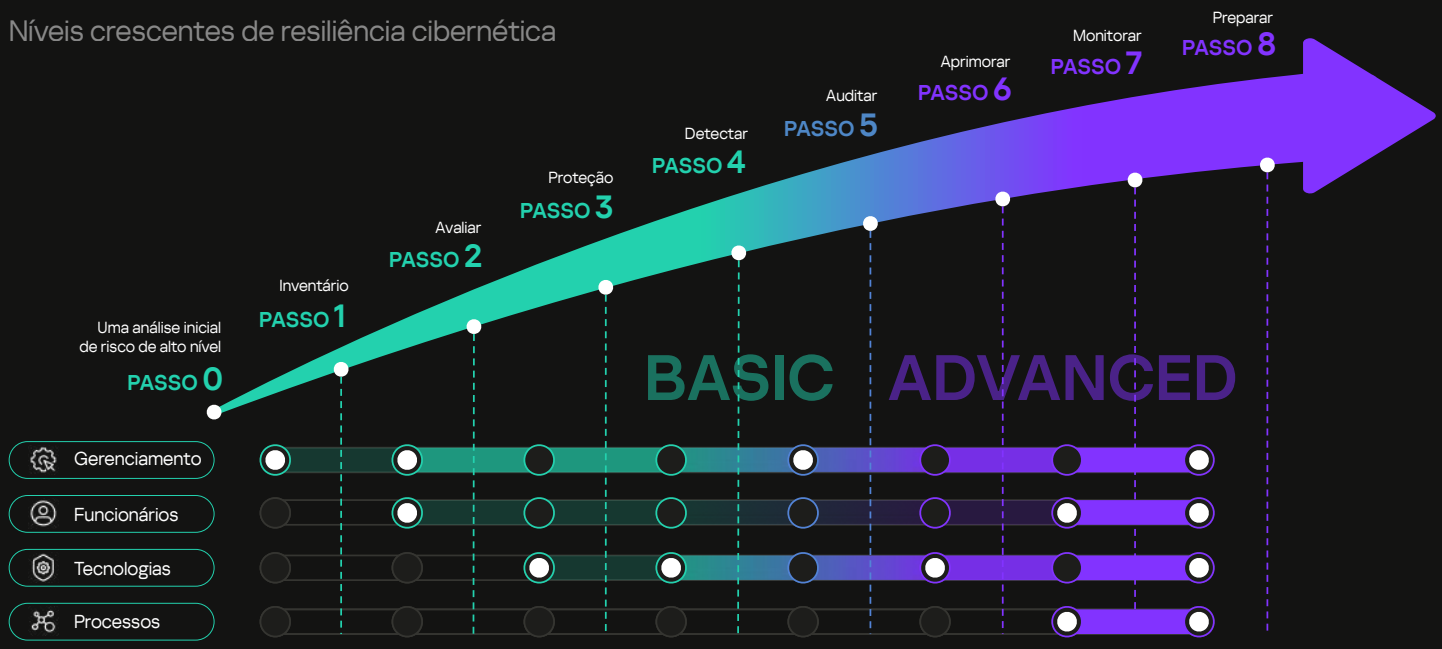
O ponto de partida lógico

Uma estratégia lógica deve começar com uma análise de risco inicial de alto nível antes de abordar as etapas tangíveis e acionáveis neste documento – quase uma etapa zero. Isso faz parte do grupo de padrões ISA/IEC 62443 e é o estágio em que você determina quais riscos inaceitáveis existem atualmente em sua organização. A evidência resultante é crucial para obter a aprovação e o orçamento da alta administração. De acordo com a ISA Global Cybersecurity Alliance, ele "permite um método relativamente rápido para determinar as áreas de maior risco dentro de um sistema de automação".[1]

A primeira tarefa que cobrimos juntos, no entanto, é o inventário de ativos. Isso garantirá que você tenha visibilidade total de sua OT, permitindo que você execute uma avaliação de risco detalhada e defina as ameaças enfrentadas por seus negócios. Você poderá implementar vários níveis de segurança – pense em proteção de endpoint, segmentação de rede, etc. – para impedir ameaças cibernéticas direcionadas ao ICS. A partir deste ponto, trata-se de fortalecer contínua e simultaneamente sua tecnologia de segurança, pessoas, processos e tecnologia de gerenciamento de segurança.

No total, abordaremos oito etapas que podem ajudar qualquer empresa industrial a desenvolver resiliência cibernética (ou pelo menos torná-la mais acessível). Essas etapas se alinham com as melhores práticas descritas em vários guias, estruturas e padrões do setor, como ISA/IEC 62443, e são especialmente úteis para empresas industriais de alto perfil (aquelas impulsionadas por suas extensas infraestruturas). Isso ocorre porque eles se envolvem em operações de alto risco que envolvem custos significativos de incidentes e sua ênfase está na adoção das melhores práticas globais de gerenciamento de segurança cibernética.

Níveis crescentes de resiliência cibernética



Organizações governamentais, privadas e públicas também podem se beneficiar deste plano. Sua demanda e operações de segurança cibernética são regulamentadas por agências governamentais, legislação nacional e padrões internacionais específicos do setor. Essas organizações enfrentam consequências potenciais consideravelmente maiores da inferência operacional do que a maioria, particularmente aquelas em:

- Petróleo, gás, petroquímica e química (offshore, transporte por dutos, refinarias, processamento petroquímico, etc.)
- Geração de energia térmica, nuclear ou renovável; redes elétricas (subestações de transmissão e distribuição de energia, operadores de sistemas de energia, etc.) e concessionárias
- Metais e mineração (mineração de metais ferrosos e não ferrosos, processamento e fabricação básica, mineração de carvão, produção de cimento, etc.)
- Minerais e produtos químicos (processamento de potássio, fosfato, nitrogênio, ureia, amônia, etc.)
- Logística e transporte (aeroportos, portos marítimos, ferrovias, etc.)
- Manufatura (eletrônicos, alimentos e bebidas, saúde e produtos farmacêuticos, papel e celulose, etc.)

A maioria das etapas iniciais deste guia é essencial para alcançar **a resiliência** cibernética industrial básica. Esta área é pesada em conformidade e diz respeito a proteções fundamentais, muitas vezes reativas. As últimas etapas facilitam **amplamente a resiliência**cibernética industrial avançada, que é proativa, contínua e eficaz contra ameaças cibernéticas sofisticadas, minimizando o risco para as operações.

[1] O'Brien, P. Avaliação de risco de segurança cibernética de acordo com ISA/IEC 62443-3-2. Aliança de Segurança Global ISA

1 Inventário: gerenciamento de ativos

Comece sua jornada de resiliência de segurança cibernética criando (ou atualizando) o inventário de ativos da sua organização. É aqui que você contabilizará todos os seus sistemas, software, hardware, segmentos de rede, conduítes, caminhos de comunicação e dispositivos para entender o que deve – e pode – ser protegido. Em seguida, você pode começar a planejar sua estratégia de segurança usando segurança essencial (antimalware, por exemplo, é considerado a proteção básica para organizações de baixa maturidade) e outras estratégias avançadas de mitigação, como segmentação.

O inventário de ativos faz parte de sua tecnologia de gerenciamento de segurança e deve amadurecer simultaneamente com sua tecnologia de segurança. Em última análise, ajudará em sua tentativa de alcançar **a resiliência** cibernética industrial básica. Catalogar componentes de hardware, software e rede significa que você poderá identificar ativos críticos e possíveis vulnerabilidades, permitindo uma proteção direcionada que protege ativos valiosos de forma adequada. Um inventário detalhado de ativos também permite monitorar e gerenciar o ciclo de vida de cada ativo, simplificando o processo de atualização e aplicação de patches.

Fluxo de trabalho recomendado

1. **Descreva seus objetivos** – defina o escopo do ambiente industrial a ser avaliado e confirme as metas de seu inventário de ativos, como detalhar todos os dispositivos, sistemas e suas interconexões.

2. **Prepare-se para a descoberta** – reúna as ferramentas e os recursos necessários para a descoberta.

3. **Use sondagem** ativa – embora o monitoramento ativo seja frequentemente evitado em ambientes industriais, é útil obter dados confiáveis de forma eficiente; você pode fazer isso com segurança se entender e respeitar as limitações e especificidades de seus equipamentos industriais.

4. **Mapeie sua rede** – use ferramentas de mapeamento de rede para identificar os dispositivos conectados à sua rede industrial automaticamente, garantindo a precisão dos dados. Procure usar ferramentas de varredura especializadas projetadas para redes industriais. Os de uso geral, como Nmap e PowerShell, exigem habilidades que muitos (se não a maioria) dos engenheiros e operadores do site não possuem, e seu uso indevido em um ambiente de controle de supervisão e aquisição de dados (SCADA) pode prejudicar as operações.

5. **Inventário** – liste seus ativos descobertos em um inventário centralizado. Inclua todos os detalhes de ativos disponíveis; por exemplo, fabricante do dispositivo, modelo, especificações de hardware, versão de firmware e software, serviços em execução/portas abertas e localização. Os ativos que não possuem parâmetros de dados importantes podem afetar a segurança.

6. **Monitore continuamente** – crie processos de monitoramento contínuo, mantendo o inventário de ativos atualizado e gerenciando vulnerabilidades.

Lembre-se: se você não consegue ver parte de sua infraestrutura ou não sabe que ela existe, não pode protegê-la.

Tecnologias

Kaspersky Industrial CyberSecurity

A Kaspersky pode te ajudar

Para obter visibilidade total do seu ambiente de OT, considere testar a plataforma**de Detecção e Resposta Estendida (XDR) do** Kaspersky Industrial CyberSecurity (KICS), que inclui KICS para Nós e KICS para Redes. O KICS for Networks pode recuperar dados importantes passivamente de uma cópia espelhada do tráfego de rede OT fornecido pelo equipamento de rede ativo. Ele pode enriquecer esses dados com informações adicionais de telemetria recebidas de endpoints industriais protegidos pelo KICS para nós, ajudando a revelar áreas da infraestrutura de rede não cobertas pelo monitoramento passivo do tráfego copiado (áreas cegas). Existem outros recursos úteis também, como marcação, status de ativos e um diagrama de topologia de rede que mostra conexões de rede física e é construído automaticamente com base na pesquisa de equipamentos de rede ativos, destacando o status de segurança dos dispositivos.

O KICS Portable Scanner também pode economizar uma enorme quantidade de recursos para sua empresa: é uma unidade flash plug-in que coleta todos os dados de hardware e software automaticamente sem a necessidade de nenhuma competência de administrador de sistema, trazendo dados e exportando-os para um único registro com segurança. Enquanto isso, a descoberta automatizada de ativos permanentes e a detecção de hosts/anomalias invasoras garantem a descoberta imediata de desvios.

Entre o KICS para nós, o KICS para redes e o agente de endpoint, os dados são coletados em todos os aspectos cruciais da infraestrutura industrial:

- Dispositivos
- Aplicativos
- Patches
- Usuários
- Arquivos executáveis

Se esses dados não forem coletados e analisados, uma organização não pode se considerar segura.

Em última análise, a plataforma KICS XDR garante uma alta cobertura de infraestruturas de automação heterogêneas – e suas soluções funcionam imediatamente.

Recursos aplicáveis da plataforma KICS

KICS for Nodes	**Scanner portátil:** scanner de malware, varredura Open Vulnerability and Assessment Language (OVAL) (vulnerabilidade, conformidade), captura de pacotes, inventário básico de ativos
KICS for Networks	**Gerenciamento de ativos:** descoberta de ativos, visibilidade da rede, cronograma da postura da rede
KICS - Plataforma de XDR de TO nativa	**Gerenciamento avançado de ativos:** inventário de hardware de endpoint; inventário de aplicativos, usuários e patches; monitoramento de tráfego de endpoint **Auditoria de segurança:** verificação de vulnerabilidade, auditoria de conformidade, controle de configuração

Experiência

Kaspersky Professional Services

Se você não tiver recursos internos ou estiver buscando total tranquilidade, pode confiar o processo de descoberta de ativos aos nossos especialistas da **Kaspersky Professional Services (KPS).**

Exemplos de estrutura

Estrutura	O Kaspersky OT CyberSecurity ajuda a cumprir			
ISA/IEC 62443-3-3[2]	SR 1.1	SR 1.2	SR 1.3	SR 7.8 ^
ISA/IEC 62443-3-2	ZCR 1.1	ZCR 2.2		
NIS2[3]	Artigo 21: Medidas de gestão de riscos de segurança cibernética (parágrafo 2. [d, g, i] e parágrafo 3.)			
NIST SP 800-82r3[4]	6.1.1: Gerenciamento de ativos			
GB/T 44462.1[5]	7.3.5.5.2: Gerenciamento de ativos			

*A Kaspersky pode ajudar a verificar o cumprimento dos requisitos.
^ Tem maior efeito e valor.

Quer assistência de mapeamento detalhado?
Compartilhe os detalhes do seu projeto e obtenha ajuda de nossos especialistas: ICSExperts@kaspersky.com

2 Sociedade Internacional de Automação. (2024). Série de padrões ISA/IEC 62443.
3 Diretiva (UE) 2022/2555 (Diretiva SRI 2)
4 NIST. (2023, setembro). NIST SP 800-82r3 – Guia para Segurança de Tecnologia Operacional (OT). Sociedade Internacional de Automação NIST.
5 Associação de Padrões de Comunicações da China (CCSA). Segurança cibernética corporativa da Internet industrial. GB/T 44462.1 —2024.

2 Avaliar: análise de risco detalhada

O próximo passo a considerar – supondo que você tenha executado sua avaliação de risco de alto nível "passo zero" – é uma avaliação de risco detalhada. Isso ajudará você a obter uma compreensão concreta do nível de risco atual em sua organização, considerando possíveis vetores de ameaças e contramedidas existentes/planejadas. É um aspecto crucial para alcançar **a resiliência** cibernética industrial básica e está relacionado à sua tecnologiade gerenciamento de segurança.

A avaliação de risco detalhada ajudará você a atender aos critérios de risco corporativo e permitirá a criação de requisitos detalhados de segurança cibernética para cada zona. As avaliações de risco cibernético são cruciais em ambientes industriais, pois iluminam as ameaças ocultas, ajudando você a priorizar investimentos e evitar interrupções com consequências potencialmente catastróficas.

Fluxo de trabalho recomendado

1. **Identifique vulnerabilidades** – identifique vulnerabilidades em seus componentes críticos de infraestrutura, como controladores lógicos programáveis (PLCs) e sistemas SCADA. Avalie possíveis pontos fracos em hardware, software, configurações de rede e processos operacionais.

2. **Avaliar ameaças** – examinar possíveis ameaças (potenciais agentes mal-intencionados; seus objetivos, foco de atividade e capacidades; suas táticas, técnicas e procedimentos [TTPs]).

3. **Impactos de uma análise** – analise os possíveis impactos de um ataque cibernético, como riscos à saúde e interrupção operacional. Em seguida, defina as implicações financeiras, regulatórias e de segurança de cada impacto potencial.

4. **Priorize os riscos** – ordene os riscos identificados de acordo com o perigo que eles representam e a probabilidade de ocorrerem.

5. **Considere a conformidade e as melhores práticas** – realize avaliações de risco na profundidade e frequência descritas nos requisitos regulatórios e/ou melhores práticas aplicáveis ao seu setor e região.

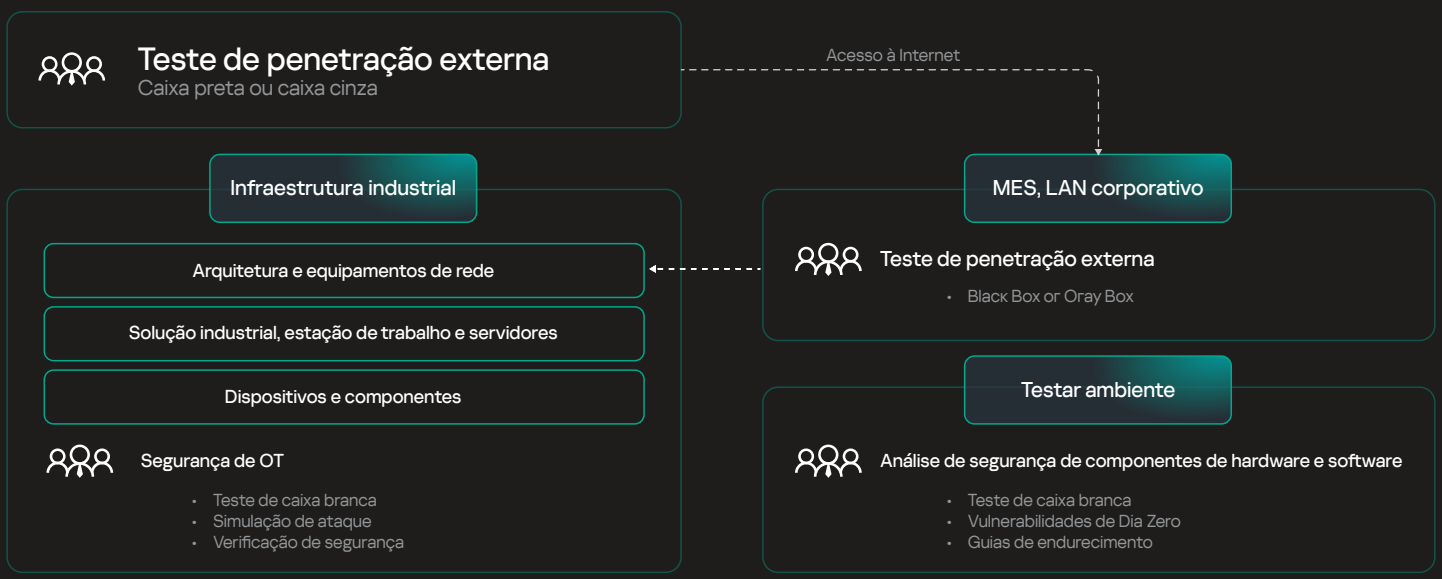
A Kaspersky pode te ajudar

Experiência

Kaspersky ICS Security Assessment

O serviço KasperskyICS Security Assessmentidentifica falhas em todas as camadas do seu ICS, desde a segurança física e de rede até vulnerabilidades específicas do fornecedor em componentes do ICS, como sistemas SCADA e PLCs. Ele determina a eficácia de suas medidas de segurança existentes e fornece as ações exclusivas necessárias para fortalecê-las.

Nossa abordagem de avaliação de segurança industrial



Conhecimento

Kaspersky ICS Threat Intelligence

Nosso **serviço ICS Intelligence Reporting** fornece informações importantes sobre ameaças e vulnerabilidades relacionadas à OT, incluindo análises de gravidade e mitigações que ajudarão muito durante o curso da modelagem de ameaças, análise de impacto e priorização de riscos.

Exemplos de estrutura

Estrutura	O Kaspersky OT CyberSecurity ajuda a cumprir
ISA/IEC 62443-3-2	ZCR 3 (TODOS) SR 5.1^ SR 5.2^ ZCR 5.3 ZCR 5.4 ZCR 5.5 ZCR 5.8 ZCR 5.10 SR 5.12^ SR 5.13^
NIS2	Artigo 21: Medidas de gestão de riscos de segurança cibernética (parágrafo 2. [a, f]) Artigo 22: Avaliações coordenadas dos riscos de segurança das cadeias de abastecimento críticas a nível da União (n.º 1).
NIST SP 800-82R3	3.3.6: Implementar uma estrutura de gerenciamento de risco para OT 6.1.3: Avaliação de riscos
GB/T 44462.1	7.3.5.2: Gerenciamento de segurança

^ Tem maior efeito e valor.

Quer assistência de mapeamento detalhado?
Compartilhe os detalhes do seu projeto e obtenha ajuda de nossos especialistas: ICSExperts@kaspersky.com

3 Proteção: segurança essencial

No mundo industrial, a segurança essencial é proteger a força vital das operações, garantindo que todos os processos sejam executados sem problemas, com segurança e sem interrupções. Sua implementação ajuda a criar linhas de base de segurança destinadas a manter e proteger a integridade da execução e configuração do sistema OT (bem como detectar, bloquear e remediar ameaças cibernéticas). Ele faz parte de sua tecnologia de segurança e é a peça central de sua **resiliência** cibernética industrial básica. Se, no entanto, seu objetivo é alcançar **resiliência cibernética** industrial avançada, essa tecnologia deve evoluir com o tempo.

Talvez o componente de segurança essencial mais reconhecível seja a proteção de endpoint, que protege os dispositivos (endpoints) em seus ambientes ICS e OT. Esses endpoints incluem uma ampla variedade de ICS, como servidores SCADA, interfaces homem-máquina, historiadores de dados, estações de trabalho de engenharia e painéis locais.

Fluxo de trabalho recomendado

1. **Fortaleça e configure seus endpoints** – implemente configurações seguras para seus endpoints que se alinhem aos padrões relevantes do setor. Reduza sua superfície de ataque desinstalando software desnecessário, desligando/excluindo serviços desnecessários e bloqueando portas desnecessárias e instalando regularmente atualizações de segurança para o restante do software e firmware. Entre em contato com o provedor de ICS relevante (fornecedor ou organização de serviços) para obter aprovação para essas alterações e implementá-las corretamente.

2. **Configure linhas de base de integridade** do sistema – defina como são as operações padrão e seguras para cada sistema e crie configurações de linha de base, capturando o estado do software, firmware, configurações e padrões de comunicação de rede. Este será um ponto de referência para detectar e responder a desvios.

3. **Implante a segurança** de endpoint – devido à complexidade dos ambientes industriais que incorporam IT e OT, a maioria das soluções prontas para uso não são adequadas. Escolha um software projetado para ambientes industriais como o seu.

4. **Implemente mecanismos** de controle de acesso – limite o pessoal que pode acessar e interferir nas configurações do endpoint. Siga o princípio de privilégios mínimos ao criar funções e atribuir privilégios. Use modos de autenticação confiáveis recomendados pelo fornecedor do sistema de automação, como autenticação multifator, e monitore as tentativas de acesso ao endpoint para registrar tentativas não autorizadas.

Muitos sistemas de controle e automação usados em empresas industriais são conservadores e/ou desatualizados. Eles podem estar operando há anos sem atualizações substanciais e devem permanecer os mesmos, o que dificulta a proteção. Esses sistemas são vulneráveis por padrão e a implementação da proteção de integridade (proteção de linha de base) pode ser uma medida de segurança aplicável quando não há possibilidade de aplicação de patches.

A Kaspersky pode te ajudar

Tecnologias

Kaspersky Industrial CyberSecurity for Nodes

O KICS for Nodes é um software de proteção de endpoint OT ideal e recomendado com consumo mínimo de recursos. Ele combina funções de proteção, detecção e resposta, bem como integração da plataforma KICS e provisão de telemetria para inventário e análise de risco em sistemas OT legados e modernos.

Recursos aplicáveis da plataforma KICS

KICS for Nodes	**Proteção de endpoint:** prevenção de ameaças em tempo real, controle de atividade local, controle de atividade de rede, monitoramento de sistema, ecossistema e integrações

Experiência

Kaspersky Professional Services

Se você quiser saber se seus esforços de proteção foram bem-sucedidos antes de se comprometer com qualquer ação, a verificação **de integridade cibernética da** KPS é um ótimo ponto de partida. Ele pode ser entregue remotamente ou no local e avaliará a eficácia de sua abordagem e infraestrutura de segurança atuais de acordo com as práticas recomendadas. Você receberá um relatório detalhando a investigação, destacando quaisquer problemas de segurança descobertos, juntamente com nossas recomendações com base nos padrões de segurança da indústria.

Exemplos de estrutura

Estrutura	O Kaspersky OT CyberSecurity ajuda a cumprir				
ISA/IEC 62443-3-3	SR 1.6	SR 2.1	SR 2.3	SR 2.4	SR 2.5
	SR 2.8	SR 3.2	SR 4.1	SR 7.2^	SR 7.7
NIS2	Artigo 21: Medidas de gestão de riscos de segurança cibernética (parágrafo 2. [d, e, j]) Artigo 25: Padronização (parágrafo 1.)				
GB/T 44462.1	7.3.1.1 Segurança do host ICS				

*A Kaspersky pode ajudar a verificar o cumprimento dos requisitos.
^ Tem maior efeito e valor.

Quer assistência de mapeamento detalhado?
Compartilhe os detalhes do seu projeto e obtenha ajuda de nossos especialistas: ICSExperts@kaspersky.com

4 Detectar: detecção de anomalias e

A detecção de ameaças e anomalias são componentes cruciais de qualquer boa estratégia de segurança cibernética. No entanto, em nenhum lugar isso é mais verdadeiro do que nas organizações industriais, devido aos seus sistemas complexos, processos sensíveis e criticidade. A implementação dessas medidas de tecnologia de segurança não apenas ajudará você a identificar ameaças antecipadamente, mas também a entender como os ataques se desenvolvem. Isso permitirá que você responda rapidamente, evite interrupções operacionais e fortaleça sua postura de segurança – atividades que evidenciam **resiliência** cibernética industrial avançada.

Muitas tecnologias normalmente implantadas em soluções de segurança cibernética também são benéficas para o pessoal de engenharia. Por exemplo, os seguintes recursos melhorariam muito a experiência digital de um engenheiro de sistema de automação responsável:

- Visibilidade da rede e detecção de anomalias da rede
- Inspeção profunda de pacotes (DPI) de comunicações industriais com recursos de aprendizado de máquina (ML)
- Sistema de controle de configuração
- Auditoria detalhada do sistema

Esses recursos são outra maneira de aumentar a segurança das operações de manutenção interna e a visibilidade da atividade de terceiros contratados, atuando como ferramentas de diagnóstico de sistema poderosas e independentes.

Fluxo de trabalho recomendado

1. **Implemente seu conjunto de** ferramentas – escolha ferramentas e tecnologias apropriadas para detecção de ameaças e anomalias; por exemplo, sistemas de detecção de intrusão de rede (IDS/NIDS) ajudarão você a monitorar o tráfego e a atividade da rede. A análise de tráfego de rede auxilia na diferenciação de comportamentos normais e anormais em processos industriais.

2. **Reúna dados** – otimize sua coleta de dados em várias fontes (pense no tráfego de rede de todos os segmentos e hosts disponíveis; telemetria de sistemas Linux e Windows; logs de SCADA, PLC/dispositivo final inteligente e outros controladores e equipamentos de rede; visualização da topologia real da rede e fluxo de dados, etc.) compilando dados em uma plataforma centralizada para correlação e análise.

3. **Estabeleça o comportamento** da linha de base – defina o comportamento "normal" para operações em sistemas industriais e defina parâmetros para detectar desvios.

4. **Buscar anomalias** – identifique comportamentos anômalos por meio de análise estatística e modelos de ML.

5. **Detecte ameaças** – use mecanismos de detecção para identificar perigos conhecidos e atividades maliciosas, mas esteja ciente de que a experiência em OT por si só não é suficiente. Há um cruzamento crescente entre ativos de OT, dispositivos de Internet das Coisas (IoT) e sistemas de TI e cada um deve ser protegido igualmente para minimizar o risco de interrupção. Portanto, é crucial buscar fornecedores de segurança OT que prosperem em ambientes digitalmente convergentes.

6. **Remediar** – limitar o impacto de qualquer violação potencial, identificar a causa e implementar uma estratégia de remediação abrangente.

7. **Esteja à frente de** futuro – seja qual for a maturidade atual do seu sistema, certifique-se de que haja próximas etapas para ser ainda mais abrangente. O objetivo deve ser adotar a convergência IT - OT em um centro de operações de segurança unificado (SOC), fechando as lacunas de visibilidade e tratando a segurança IT - OT como uma entidade. Os benefícios de expandir seu SOC para cobrir OT (criando uma instalação de nível empresarial) incluem melhor compartilhamento de informações, maior visibilidade para os líderes de segurança e tempo reduzido para detectar e mitigar ameaças.

A Kaspersky pode te ajudar

Tecnologias

Kaspersky Industrial CyberSecurity for Networks

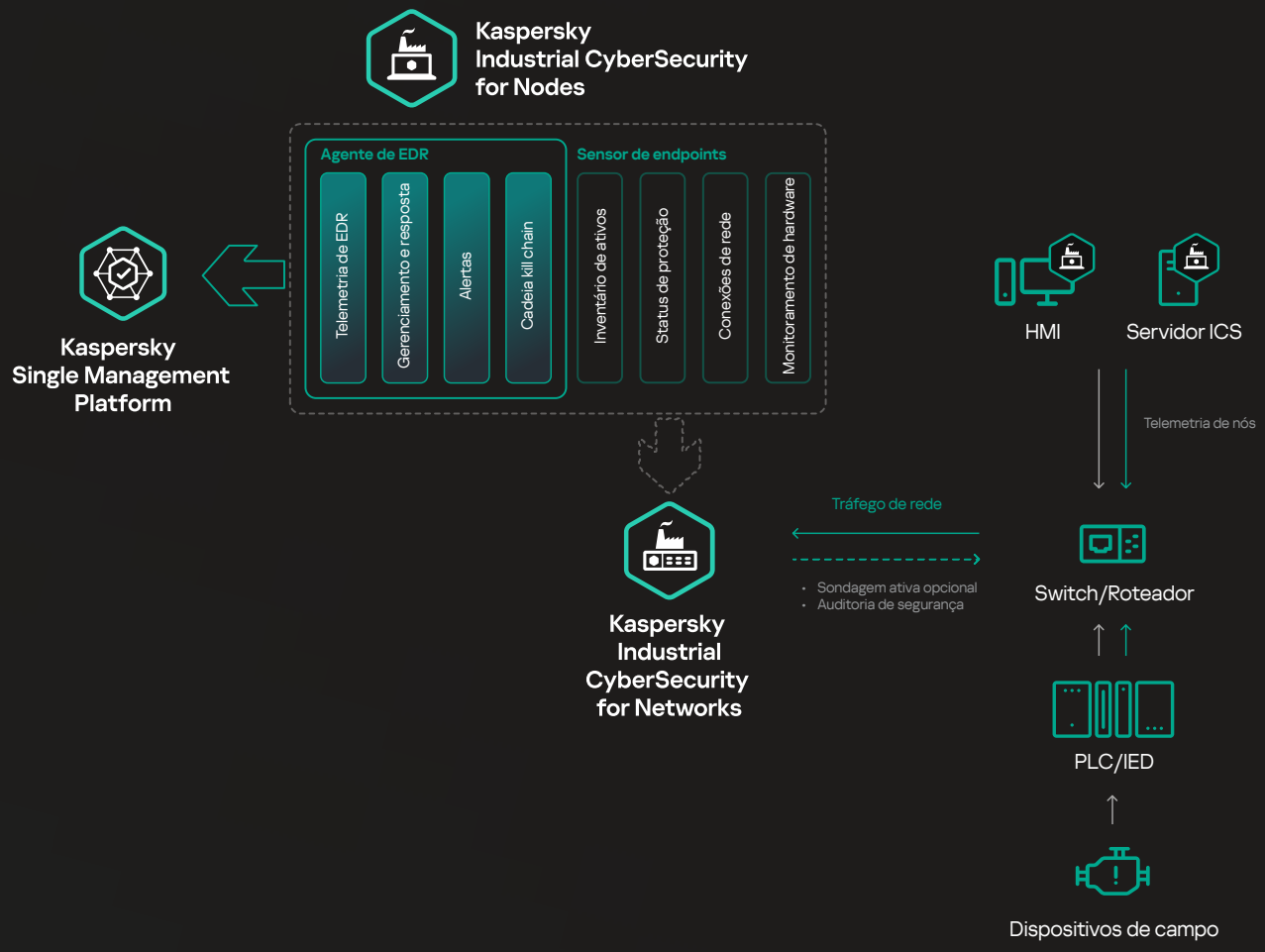
Seu fornecedor deve ser capaz de funcionar efetivamente no local, em ambientes robustos e em áreas de baixa conectividade de rede (se necessário). Portanto, é importante procurar um fornecedor de segurança OT que possa resolver desafios complexos de segurança cibernética com recursos avançados que se fundem com seu portfólio existente e evoluem com o tempo.

Se você acabou de começar a convergir seus processos e tecnologias de segurança cibernética ou está procurando caça a ameaças, visualização integrada da cadeia de eliminação de IT - OT e análise de causa raiz, prosperamos em ambientes convergentes e somos capazes de gerenciar a ameaça tripla de IT - OT- IoT.

O KICS for Networks analisa o tráfego da rede industrial para identificar desvios nos valores dos parâmetros do processo, detectar sinais de ataques à rede e monitorar a operação e os estados atuais do dispositivo na rede. Uma combinação de inspeção profunda de pacotes (DPI) de protocolos industriais e recursos do sistema de detecção de intrusões (IDS) permite a identificação e mitigação de potenciais ciberameaças em tempo real. Isso ajuda a proteger o ambiente de ICS contra acesso não autorizado, malware e outras atividades maliciosas.

Quando o KICS for Networks é combinado com **o KICS for Nodes**, você desbloqueia os recursos da plataforma OT XDR – ou seja, detecção e resposta. Isso inclui uma única visualização da cadeia de eliminação, enriquecimento de alertas, etc. e facilita o monitoramento de amostras de tráfego de rede de sistemas isolados por meio do KICS Portable Scanner (com veredictos padrão do KICS para redes).

Troca de dados de componentes da plataforma KICS XDR



Recursos aplicáveis da plataforma KICS

KICS for Networks	**Detecção de ameaças e anomalias de rede:** detecção de intrusão, detecção de anomalias, controle de integridade de rede, DPI de protocolos industriais e correlação de eventos
KICS for Nodes	**Detecção e resposta de endpoint:** varreduras de detecção, relatórios, medidas de resposta, ecossistema e integrações
KICS - Plataforma de XDR de TO nativa	**Detecção e resposta estendidas:** visualização de cadeia de eliminação única, enriquecimento de alertas, prevenção de execução, isolamento de host e arquivo e integração de firewall

Tecnologias

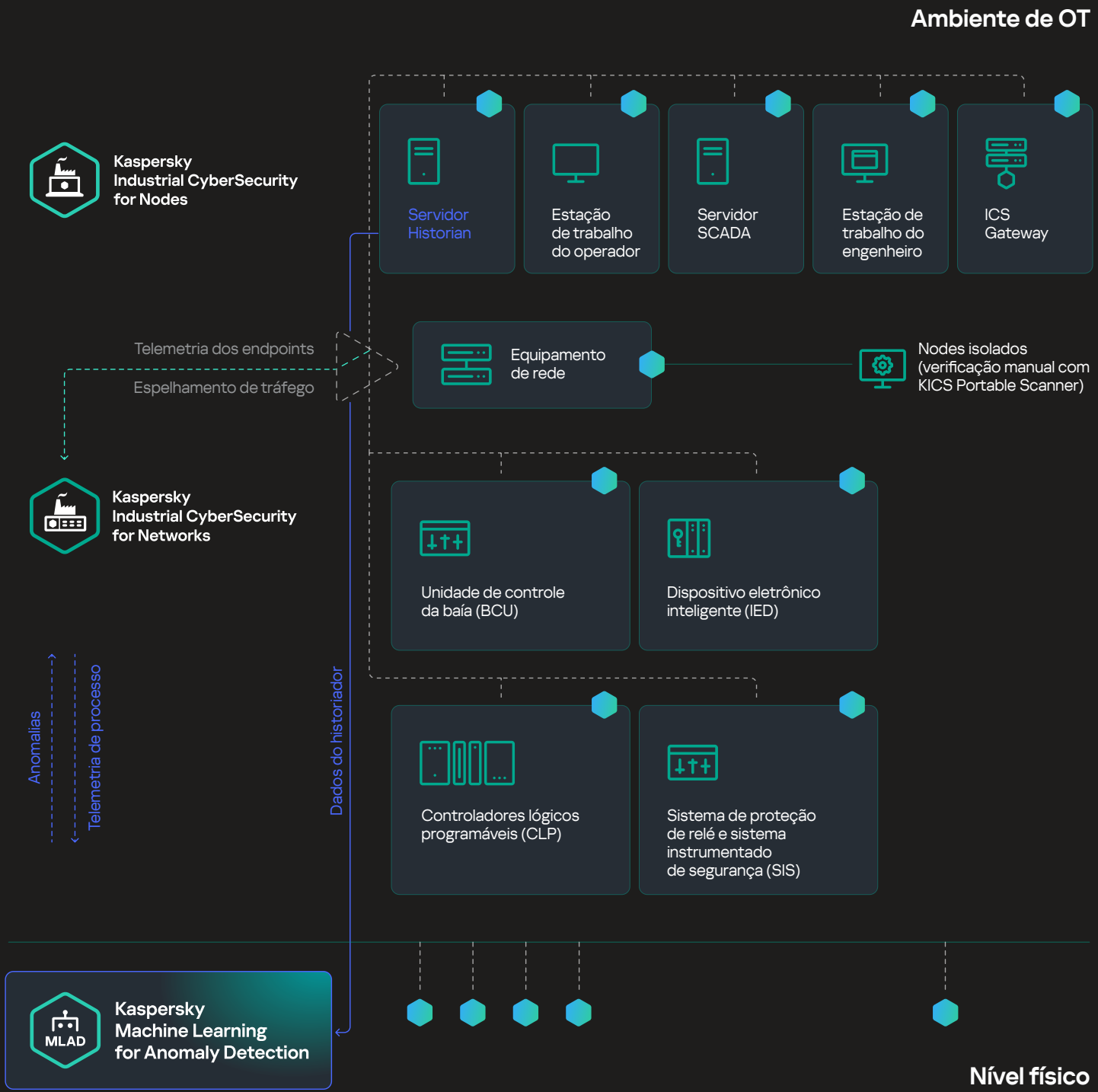
MLAD

Kaspersky Machine Learning for Anomaly Detection

Apesar da abrangência do KICS, sempre existe o risco de sua organização enfrentar ameaças desconhecidas avançadas ou ataques de dia zero. Eles nunca podem ser totalmente contabilizados, e é por isso que projetamos **o Machine Learning for Anomaly Detection (MLAD)** – uma extensão do KICS e gêmeo digital de ativos industriais com recursos de ML. Mas, embora o MLAD possa se destacar como sua última linha de defesa, prevendo anomalias, ele funciona como uma ferramenta digital para monitorar e otimizar os principais indicadores de desempenho dos processos tecnológicos.

Quando combinados, o MLAD e o KICS for Networks detectam ameaças e anomalias conhecidas. Enquanto o KICS for Networks detecta e bloqueia rapidamente perigos com base em vulnerabilidades ou assinaturas conhecidas, o MLAD rastreia continuamente padrões sutis e/ou complexos que podem indicar uma ameaça desconhecida grave, como um grupo de ameaças persistentes avançadas.

Detecção de anomalias de processos tecnológicos alimentados por ML



Tecnologias

Kaspersky Next XDR Expert

O Kaspersky XDR Expert é ideal para clientes que já possuem soluções de Endpoint e EDR implementados e não querem substituí-las, preferindo ampliar a funcionalidade com um mecanismo de correlação, respostas automatizadas e conectores de terceiros.

Ele é construído na Open Single Management Platform, uma plataforma de tecnologia aberta que permite a integração com a Kaspersky e aplicativos de terceiros em um único sistema de segurança para fornecer cenários entre aplicativos. Os recursos de correlação cruzada (SIEM) de nosso XDR permitem que o KICS centralize o gerenciamento em vários locais industriais, correlacionando e coletando dados de fontes externas dentro de objetos industriais.

Exemplos de estrutura

Estrutura	O Kaspersky OT CyberSecurity ajuda a cumprir			
ISA/IEC 62443-3-3	SR 1.11 SR 3.1^	SR 2.2 SR 3.5^	SR 2.10 SR 3.8	SR 2.12 SR 5.3
NIS2	Artigo 21: Medidas de gestão de riscos de segurança cibernética (parágrafo 2. [b, c, d, e]) Artigo 23: Obrigações de relatório (parágrafo 4. [all])			
NIST SP 800-82R3	4,1 Gerenciando o risco de segurança de OT			
GB/T 44462.1	7.3.3.2. Segurança nas fronteiras			

*A Kaspersky pode ajudar a verificar o cumprimento dos requisitos.
^ Tem maior efeito e valor.

Quer assistência de mapeamento detalhado?
Compartilhe os detalhes do seu projeto e obtenha ajuda de nossos especialistas: ICSExperts@kaspersky.com

5 Auditar: auditorias de segurança e conformidade

Para construir uma imagem realista da segurança cibernética de sua organização, você deve se concentrar na conformidade e realizar auditorias de segurança regulares. Essas avaliações sistemáticas estão relacionadas à sua tecnologiade gerenciamento de segurança e são uma parte essencial da **resiliência** cibernética industrial básica que pode determinar se você está se alinhando com os critérios e atingindo os benchmarks. Eles são os vigilantes do seu ambiente industrial, garantindo que as operações não apenas sejam executadas com eficiência, mas também com segurança e dentro dos limites regulatórios. O resultado deve ser uma melhor adesão às melhores práticas e, em última análise, sistemas mais robustos.

Fluxo de trabalho recomendado

1. **Identifique estruturas** – confirme os padrões e regulamentos mais relevantes do setor (por exemplo, NIST SP 800-82, ISA/IEC 62443, GDPR, etc.).

2. **Implemente controles** técnicos – eles ajudarão você a comprovar a conformidade com os padrões regulatórios e identificar áreas a serem melhoradas.

3. **Realize workshops** de avaliação de risco – realizar workshops regulares focados na análise de risco dentro do contexto industrial. Inclua as principais partes interessadas cujo papel é identificar e avaliar os riscos associados a processos, sistemas e ativos. Desenvolver e implementar procedimentos de proteção e reconfiguração para reduzir os riscos.

4. **Execute auditorias** de segurança – realize auditorias de segurança regulares para avaliar a eficácia de seus controles técnicos, identificando lacunas. Idealmente, você deve usar auditores internos e externos.

Tecnologias

Kaspersky Industrial CyberSecurity

A Kaspersky pode te ajudar

A **plataforma** OT XDR nativa da KICS oferece suporte a auditorias de segurança ativas e passivas de endpoints e redes, permitindo que você obtenha mais com menos recursos. Nossa auditoria de conformidade centralizada de nós de rede industrial é baseada no padrão OVAL, identificando e monitorando riscos e vulnerabilidades específicos de OT.

KICS for Networks. Avaliação de vulnerabilidade, risco e configuração de segurança de OT

Recurso	Auditoria de segurança		
Sub-recurso	Auditoria de vulnerabilidade e conformidade (OVAL +XCCDF)	Controle de configuração	
Dados	• Vulnerabilidades de SO e software • Vulnerabilidades de software ICS • Conformidade com as configurações de segurança recomendadas • Conformidade com as normas regulatórias	• Usuários e grupos • Aplicações e patches • Serviços • Objetos de inicialização • Drivers • Tarefas agendadas	
Métodos de coleta de dados	Sem agentes • SSH	Industrial • Protocolo nativo ICS**	Agente • do KICS for Nodes
Fontes de dados	Estações de trabalho, servidores e dispositivos de rede baseados em Linux		Estações de trabalho e servidores Windows e Linux

* - Linguagem aberta de avaliação e vulnerabilidade (OVAL)
- Extensible Configuration Checklist Description Format (XCCDF)

** s7comm; Modbus; Ethernet/IP, Emerson DeltaV

Recursos aplicáveis da plataforma KICS

KICS - Plataforma de XDR de TO nativa	**Auditoria de segurança:** verificação de vulnerabilidade, auditoria de conformidade, controle de configuração
KICS for Nodes	**Scanner portátil:** Varredura OVAL (vulnerabilidades, conformidade)

Exemplos de estrutura

Estrutura	O Kaspersky OT CyberSecurity ajuda a cumprir
ISA/IEC 62443-3-3	SR 1.5 SR 1.7 SR 2.9 SR 2.11 SR 3.4 SR 3.7 SR 3.9 SR 6.1 SR 7.6^
NIS2	Artigo 20: Governança (parágrafo 1.) Artigo 21: Medidas de gestão de riscos de segurança cibernética (parágrafo 2. [d, e, f, i])
NIST SP 800-82R3	3.3.1: Estabeleça a governança de segurança cibernética de OT
GB/T 44462.1	7.3.2.3 Segurança de configuração 7.3.4.2. Segurança de aplicativos ICS

^ Tem maior efeito e valor.

Quer assistência de mapeamento detalhado?
Compartilhe os detalhes do seu projeto e obtenha ajuda de nossos especialistas: ICSExperts@kaspersky.com

6 Aprimorar: zonas e conduítes

As zonas são conjuntos de redes, dispositivos e serviços agrupados de acordo com seus requisitos de função, criticidade, segurança e proteção. Eles são a base para segmentação e monitoramento e controle de acesso e podem ser essenciais para a conformidade. Os conduítes, por outro lado, representam os caminhos de comunicação que unem zonas ou as conectam a redes externas. Seu papel é no controle de tráfego, criptografia, filtragem de segurança e redundância e resiliência. Juntos, eles fazem parte de sua tecnologia de segurança e são cruciais para alcançar **resiliência cibernética** industrial avançada.

A modelagem inicial de zona e conduíte desempenha um papel fundamental na organização e proteção da arquitetura de rede de ambientes de OT e deve ser feita antes de sua avaliação de risco detalhada. Esta etapa, no entanto, é referente ao aprimoramento de suas zonas e conduítes, pois sua organização agora deve estar em posição de identificar incidentes e violações de política em zonas e usar o fluxo de dados real para melhorar a arquitetura.

Você pode mitigar os riscos cibernéticos e manter a integridade operacional revisitando suas zonas e conduítes e executando as seguintes medidas.

Fluxo de trabalho recomendado

1. **Melhorar continuamente a segmentação de rede e determinar as restrições** de fluxo de informações necessárias – o projeto da infraestrutura de rede não é um processo estático; redefinir limites lógicos e agrupar componentes com base na evolução dos requisitos de função, criticidade, segurança e proteção (por exemplo, 1. controle de processo, 2. operações).

2. **Mapear zonas** – projetar um mapa físico e lógico das interconexões de zona.

3. **Conduítes** de modelo – liste aqueles que conectam zonas e redes externas e determine os controles de segurança (firewalls, etc.) que você implementará em cada ponto; confirme os requisitos de acesso seguro, como mecanismos de autenticação.

4. **Implemente e configure** – segmente a rede de acordo com suas zonas e conduítes, implemente controles de segurança e acesso e monitore anomalias.

5. **Teste sua configuração** – use avaliações de vulnerabilidade e testes de penetração para confirmar a eficácia de suas zonas e conduítes. As regras de configuração do firewall (regra padrão, limpeza não utilizada, etc.) devem ser testadas antes da implantação.

A Kaspersky pode te ajudar

Tecnologias

Kaspersky Thin Client

O acesso remoto seguro à infraestrutura de TO permite que engenheiros e operadores monitorem e controlem os sistemas remotamente, o que pode ajudar a otimizar a produção, reduzir o tempo de inatividade e melhorar a programação de manutenção. Mas a arquitetura industrial de IoT-nuvem é complexa e, se essas conexões forem expostas a vulnerabilidades, as vantagens potenciais podem ser superadas em breve pelos riscos de um ataque cibernético. **O Kaspersky Thin Client** simplifica a migração de uma infraestrutura de desktop local para uma infraestrutura de thin client confiável, fácil de gerenciar e imune a cibernéticas para conexão segura a desktops virtuais, incluindo uma zona confiável para conectar usuários à infraestrutura industrial.

Tecnologias

Kaspersky SD-WAN

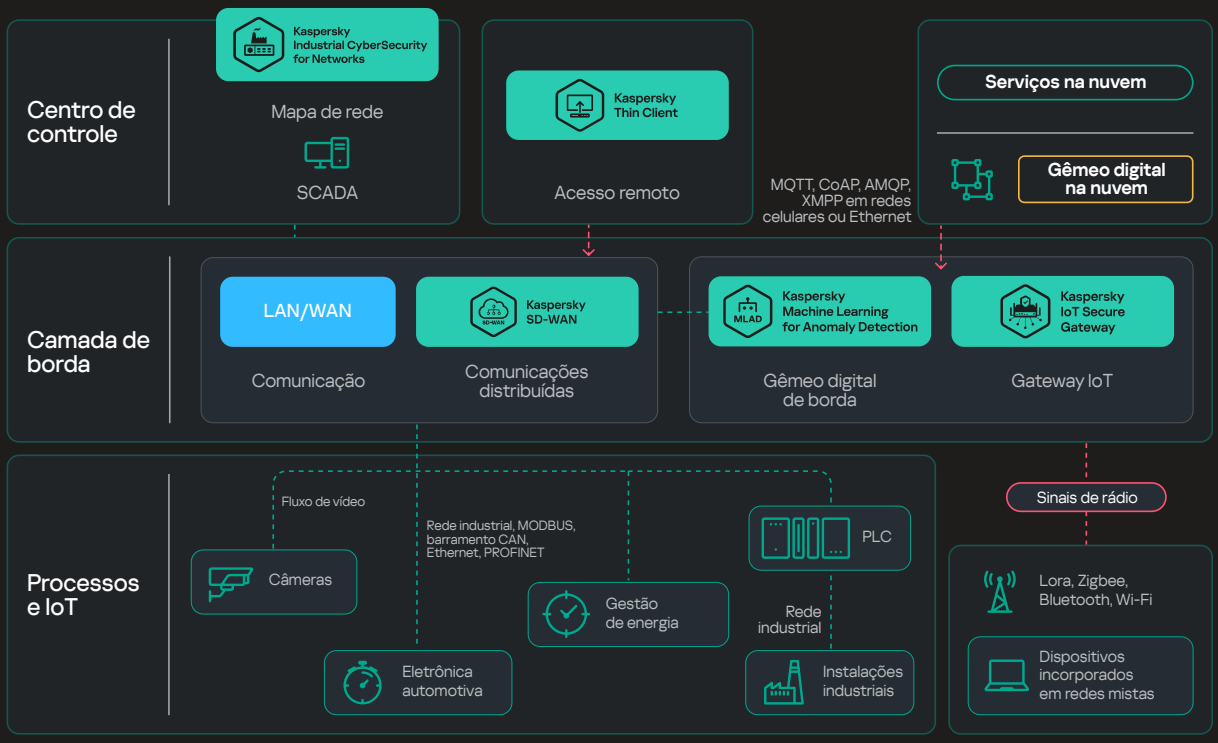
O Kaspersky SD-WAN foi projetado para construir redes seguras e tolerantes a falhas com gerenciamento unificado, essencial para organizações industriais que abrangem várias filiais, equipes distribuídas, recursos de nuvem e funcionários remotos. Ele permite que você implante automaticamente ferramentas de controle de tráfego e segurança (próprias e de terceiros) imediatamente. Isso não apenas garantirá que sua transmissão de dados seja mais segura do que nunca, mas também é escalável, fácil de gerenciar e econômica.

Tecnologias

Kaspersky IoT Secure Gateway

O KISG, parte do Kaspersky IoT Infrastructure Security, pode ser instalado entre a infraestrutura de OT e redes de dados externas, bloqueando ataques a ICS, equipamentos e canais de compartilhamento de informações. Ele é criado de acordo com os princípios de segurança por design, não requer proteção adicional e oferece suporte a aplicativos de terceiros para computação de borda. (Este cenário é aplicável a dispositivos inteligentes conectados/expostos a redes públicas.)

O KICS for Networks fornece controle de violação de política de zona e conduíte



Recursos aplicáveis da plataforma KICS

KICS for Networks	**Ecossistema e integrações:** Uma série de integrações de terceiros ou sinergia dentro do ecossistema Kaspersky OT Cybersecurity: - Kaspersky Next XDR Expert - Kaspersky IoT Secure Gateway (KISG) - Kaspersky Machine Learning for Anomaly Detection (MLAD) - Kaspersky Software-Defined Wide Area Network (SD-WAN)

Exemplos de estrutura

Estrutura	O Kaspersky OT CyberSecurity ajuda a cumprir				
ISA/IEC 62443-3-3	SR 1.11	SR 1.13	SR 3.6	SR 5.1^	SR 5.2^
NIS2	Artigo 21: Medidas de gestão de riscos de segurança cibernética (parágrafo 2. [h, i, j])				
NIST SP 800-82R3	4,1 Gerenciando o risco de segurança de OT				
GB/T 44462.1	7.3.3.1. Segurança arquitetônica				

^ Tem maior efeito e valor.

Quer assistência de mapeamento detalhado?
Compartilhe os detalhes do seu projeto e obtenha ajuda de nossos especialistas: ICSExperts@kaspersky.com

7 Monitorar: operações de segurança especializadas

Seu SOC é o coração de sua capacidade defensiva proativa, mas simplesmente estabelecer um ou contratar um terceiro desinteressado não é suficiente. Confiar em medidas básicas e sistemas SIEM não será suficiente no cenário de ameaças em evolução, onde as ameaças cibernéticas são altamente sofisticadas. Tais medidas são necessárias, sim, mas sozinhas carecem da análise proativa e contextual necessária para gerenciar ataques complexos.

Depois de implementar um SIEM, sua organização deve se esforçar para obter um SOC maduro e habilitado para XDR. Quando processos eficazes , como proteção de sistemas (avaliação, implementação e sustentabilidade) e gerenciamento de incidentes (detecção, resposta e recuperação) são apoiados por pessoas especializadas , você sabe que está desenvolvendo resiliência**cibernética industrial**avançada.

Sua organização deve estar continuamente evoluindo sua capacidade defensiva com inteligência de ameaças e recursos de resposta a incidentes que a tornem mais forte "direito de boom". Um SOC reforçado pode investigar, conter e mitigar ameaças rapidamente, minimizando danos e reduzindo o tempo de recuperação – marcas registradas de **resiliência** cibernética industrial avançada.

Fluxo de trabalho recomendado

1. **Defina metas** de SOC – descreva seus objetivos e decida se ele fará parte de sua organização, terceirizado ou uma mistura de ambos, dependendo da disponibilidade de recursos.

2. **Desenvolva o SOC** – preencha-o com pessoal, monitoramento de segurança e ferramentas de caça a ameaças, ferramentas e infraestrutura de coleta e análise de artefatos, sistemas de triagem de incidentes e plataformas de colaboração.

3. **Aumente a capacidade** humana – capacite os analistas de SOC em segurança cibernética industrial e garanta que eles entendam os ambientes e protocolos de OT (ou terceirizem para especialistas).

4. **Forme uma equipe** de resposta a incidentes – reúna especialistas em TI, segurança cibernética e OT em uma equipe e defina funções e responsabilidades para detecção, análise, priorização, contenção e recuperação. Nomeie as principais partes interessadas do jurídico, finanças, marketing, etc., que ajudarão em elementos de resposta não técnicos, como relatórios regulatórios e gerenciamento de mídia.

5. **Refine o plano** de resposta a incidentes – você deve ter esboçado seu plano de resposta a incidentes como parte de suas políticas; adicione cor com:

- Categorização de incidentes e níveis de gravidade
- Partes interessadas nomeadas
- Ações específicas de investigação e resposta
- Protocolos de comunicação e relatórios
- Etapas de recuperação
- etc.

A Kaspersky pode te ajudar

Se você tem seu próprio SOC ou está procurando uma solução SOC de terceiros completa, nós o cobrimos com tecnologia, conhecimento e experiência.

Tecnologias

Kaspersky Next XDR Expert

Embora seja possível criar seu SOC usando uma solução XDR de sua escolha antes de adicionar nossos recursos de resposta a incidentes, inteligência de ameaças e até mesmo detecção e resposta gerenciada (MDR), **o Kaspersky Next XDR Expert** é a escolha de elite. Ele oferece segurança cibernética unificada nos segmentos industrial e corporativo de sua empresa, facilitando a verdadeira convergência de TI e OT (em operações de segurança) quando combinado com o KICS. Sua detecção aprimorada de ameaças, resposta automatizada e visibilidade em tempo real fornecem a melhor defesa proativa, enquanto o suporte premium 24 horas por dia, 7 dias por semana, oferece tranquilidade em relação à continuidade dos negócios.

Experiência

Kaspersky Incident Response

O **serviço Kaspersky ICS Incident Response Handbook** tem como objetivo criar um conjunto de cenários e instruções detalhados para todas as fases de resposta a incidentes relevantes para sua organização. Contabilizamos todos os aspectos importantes, incluindo a estrutura organizacional e os recursos humanos disponíveis, os sistemas de segurança cibernética em uso e os produtos ICS em operação.

Recursos maduros da plataforma Kaspersky Next XDR

Conhecimento

Kaspersky ICS Threat Intelligence

Se você deseja simplesmente obter informações, nosso **serviço de inteligência** de ameaças ICS concede acesso a feeds quase em tempo real de indicadores de comprometimento para ameaças relacionadas à OT, além de análises profundas de ataques direcionados a empresas industriais.

Experiência

Kaspersky Managed Detection and Response

Também podemos oferecer serviços SOC dedicados e completos por meio do **Kaspersky MDR**. Está disponível tanto para o segmento corporativo quanto para o industrial de sua empresa, fornecendo a experiência e os recursos necessários para rastrear ameaças cibernéticas industriais e responder de maneira adequada.

Exemplos de estrutura

Estrutura	O Kaspersky OT CyberSecurity ajuda a cumprir	
ISO/IEC 27001	SR 3.3	SR 6.2^
NIS2	Artigo 21: Medidas de gestão de riscos de segurança cibernética (parágrafo 2. [b, c]) Artigo 23: Obrigações de Relatórios ((parágrafo 4. [all])	
NIST SP 800-82R3	3.3.8: Desenvolva um recurso de resposta a incidentes	
GB/T 44462.1	7.3.5.5. Gestão de operações	

^ Tem maior efeito e valor.

Quer assistência de mapeamento detalhado?
Compartilhe os detalhes do seu projeto e obtenha ajuda de nossos especialistas: ICSExperts@kaspersky.com

8 Preparar: tolerância a falhas e prontidão

O elemento humano é frequentemente negligenciado na segurança cibernética. A tecnologia é tão boa quanto aqueles que a configuram e usam, o que significa que cada funcionário ou contratado é um ponto de acesso potencial à sua organização. E quando se trata de prevenir um ataque ou responder efetivamente a um incidente, as pessoas são seu maior patrimônio.

A tolerância a falhas, por outro lado, está relacionada à sua tecnologia de gerenciamento de segurança e garantirá que você possa resistir e se recuperar de um incidente cibernético sem comprometer a continuidade operacional. Seu ICS deve continuar a funcionar durante um ataque, e é nesta etapa que você testará essa teoria. Lembre-se de que esses sistemas podem se degradar com o tempo, portanto, você deve garantir sua disponibilidade contra degradação e negação de serviços (DoS).

A resiliência cibernética industrial avançada só pode ser alcançada quando seus vários ICS são resilientes a diferentes tipos de eventos DoS, incluindo a indisponibilidade parcial ou total da funcionalidade do sistema em diferentes níveis. Mais importante, os incidentes de segurança do ICS não devem afetar a segurança (como sistemas instrumentados de segurança).

Ao realizar exercícios de "tempestade cibernética" que simulam ataques cibernéticos em larga escala, você pode testar a infraestrutura que construiu nas etapas anteriores, garantindo que tudo funcione durante a degradação do sistema ou ataques DoS. O ICS também deve se orgulhar da capacidade de retornar a um estado seguro conhecido após interrupção ou falha.

Fluxo de trabalho recomendado

1. **Treine sua equipe** – écrucial que seu pessoal tenha as habilidades técnicas e o know-how para proteger seu ambiente industrial exclusivo. Você deve exigir treinamento regular focado em segurança cibernética ICS, SCADA e OT e considerar:

- Capacitar funcionários em toda a organização para melhorar a resiliência a phishing, engenharia social, etc.
- Realização de exercícios práticos e simulações para melhorar a capacidade de resposta.

2. **Incentive a colaboração entre** equipes – as unidades de TI, OT e segurança cibernética precisam trabalhar em conjunto para aumentar a tolerância a falhas e a eficiência da resposta. Para conseguir isso:

- realizar exercícios e exercícios conjuntos para melhorar a comunicação e a coordenação durante os incidentes
- desenvolver uma compreensão compartilhada de dependências operacionais e sistemas críticos
- Realize exercícios regulares de mesa e simulações de crise para testar seu plano de resposta a incidentes com as partes interessadas relevantes.

3. **Pratique a resiliência** – construa tolerância a falhas nos sistemas centrais para manter a operacionalidade sob pressão. Para conseguir isso:

- Instalar mecanismos de backup para componentes críticos de infraestrutura
- auditar periodicamente a resiliência do sistema
- Crie planos de contingência e backups para os piores cenários.

4. **Realize retrospectivas de resposta a** incidentes – não se trata apenas de ter um plano de resposta a incidentes e procedimentos definidos; você deve fazer um balanço completo após cada incidente cibernético para aprender lições e reconstruir mais forte, atualizando seu plano de acordo.

A Kaspersky pode te ajudar

Conhecimento

Kaspersky Security Awareness

Os cibercriminosos terão como alvo sua equipe como pontos de entrada para seus sistemas. Para resiliência humana, equipe as pessoas com as habilidades de segurança cibernética necessárias usando **o Kaspersky Security Awareness Training**.

Conhecimento

Kaspersky ICS CERT Training

Para aprimorar os recursos de seus profissionais de segurança de TI e OT, envolva-os com nosso vasto **programade treinamento ICS CERT** . Isso inclui o Kaspersky Digital Forensics e o Incident Response in ICS, que permitem realizar investigações forenses em ambientes industriais e fornecer análises e recomendações especializadas.

Exemplos de estrutura

Estrutura	O Kaspersky OT CyberSecurity ajuda a cumprir		
ISA/IEC 62443-3-3	SR 7.1	SR 7.4	SR 7.5
NIS2	Artigo 21: Medidas de gestão de riscos de cibersegurança (n.° 2 [b, c, g])		
NIST SP 800-82R3	3.3.2: Construa e treine uma equipe multifuncional para implementar o programa de segurança cibernética de OT 3.3.5: Estabelecer um programa de treinamento de conscientização sobre segurança cibernética para o ambiente OT 4.3.5: Avalie		
GB/T 44462.1	7.3.5. Gerenciamento de segurança		

^ Tem maior efeito e valor.

Quer assistência de mapeamento detalhado?
Compartilhe os detalhes do seu projeto e obtenha ajuda de nossos especialistas: ICSExperts@kaspersky.com

Conclusão

As organizações estão cada vez mais conectando o ICS à Internet à medida que buscam uma vantagem competitiva, mas isso as deixa vulneráveis a ameaças cibernéticas. Portanto, são necessários esforços multidirecionais para desenvolver ambientes de OT seguros, e isso inclui profissionais de segurança cibernética de OT com conhecimento além da segurança de TI. É essa experiência que torna nossa divisão de pesquisa de segurança ICS tão valiosa.

Felizmente, sua organização pode proteger suas partes interessadas da perda de ativos críticos (e as implicações econômicas e de segurança nacional associadas) aplicando os princípios básicos de design de resiliência cibernética industrial.

Alcançar **resiliência** cibernética industrial avançada permitirá que sua organização resista a ataques maliciosos direcionados a operações industriais e até mesmo impeça que adversários que violam seu perímetro controlem, examinem ou roubem sistemas de missão crítica.

Já protegemos mais de 1.000 clientes industriais e temos uma vasta experiência na adoção de padrões internacionais e melhores práticas. Com base nessa experiência, definimos oito etapas estratégicas que se aplicam universalmente aos sistemas de automação durante as fases de projeto e operação:

1. Manter um inventário de ativos de software, hardware e redes industriais. Isso é crucial para a segurança baseada em risco.

2. Executar uma avaliação de risco detalhada para que você tenha uma compreensão concreta dos riscos de segurança específicos da sua organização. Isso ajudará você a planejar contramedidas eficientes.

3. Implementando segurança essencial, como proteção de endpoint, para proteger os dispositivos em seus ambientes ICS e OT.

4. Realizar a detecçãode ameaças e anomalias, o que permitirá identificar ameaças antecipadamente e entender como os ataques se desenvolvem.

5. Realização de auditorias regulares de segurança e conformidade para garantir que as operações funcionem sem problemas e dentro dos limites regulatórios.

6. Aprimorando sua modelagem de zona e conduíte para otimizar sua arquitetura de ambiente OT. Isso permitirá que você reduza os riscos e mantenha a integridade operacional.

7. Esforçando-se para operações de segurança maduras por meio de um SOC habilitado para XDR. Isso permitirá que você investigue, contenha e mitigue ameaças rapidamente.

8. Aumentando sua tolerância a falhas e prontidão, para que sua empresa possa resistir e se recuperar de um incidente cibernético sem comprometer a continuidade operacional.

Como prosperamos na interseção de segurança corporativa-industrial, estamos perfeitamente posicionados para ajudá-lo a obter proteção corporativa e de infraestrutura crítica sustentável e podemos ajudar em cada uma dessas etapas.

Saiba mais em nosso site dedicado:
https://lp.kaspersky.com/global/industrialcyberresilience

Primeira edição: Fevereiro de 2025