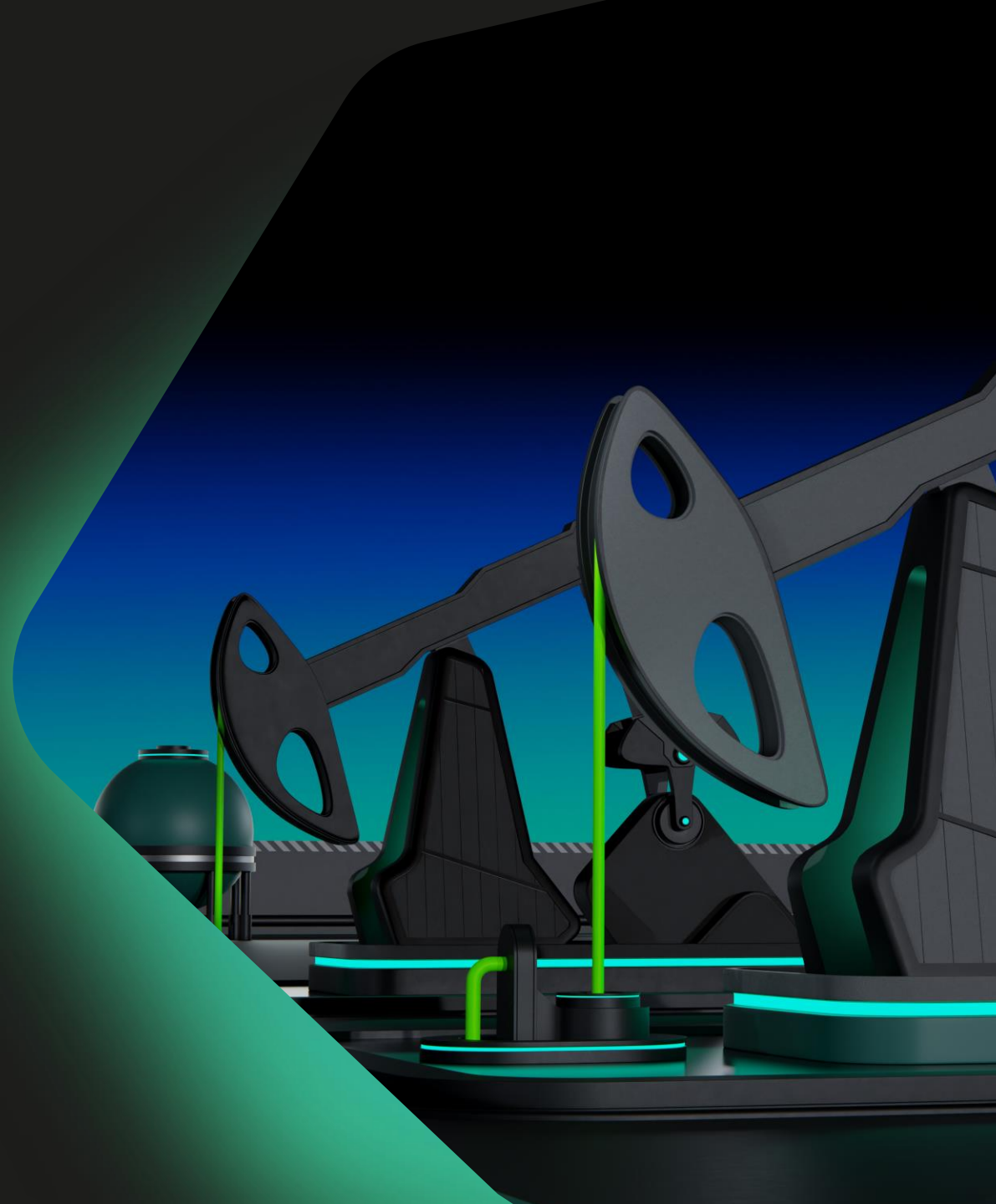


Kaspersky OT Cybersecurity

Oferta para empresas
do setor de petróleo e gás



Resumo do mercado

O setor de petróleo e gás domina o mercado de fornecimento de energia e tem enorme influência sobre a economia global. A alta demanda por força de trabalho e o consumo crescente de recursos de eletricidade e climatização destacam a importância do setor energético. Além da energia, petróleo, gás natural e liquefeito (LNG) são recursos essenciais para:



Construção civil e materiais de alta tecnologia



Indústria química e fertilizantes



Ciências biológicas e farmacêutica



Muitas outras esferas cruciais

Nos últimos anos, as empresas de petróleo e gás também tiveram um papel importante na transição para a sustentabilidade, tirando proveito de recursos abrangentes, expertise e infraestrutura para facilitar a mudança.

As estratégias focam em:



Transformação ESG



Os 17 Objetivos de Desenvolvimento Sustentável (SDG) da ONU¹

Ações e tecnologias de capacitação para apoiar a estratégia de sustentabilidade

Tendências em digitalização

- Soluções de aprendizagem de máquina e inteligência artificial usadas na manutenção preditiva e para uma confiabilidade aumentada
- Réplicas digitais para simulação e otimização de processos
- Tecnologias AR e VR para treinamento de pessoal
- Convergência dos sistemas de TI e OT
- Robotização e automação para lidar com tarefas de alto risco
- IIoT e sensores para monitoramento

Ações adicionais

- Conformidade com iniciativas e diretivas
- Eletrificação, solarização e eficiência energética
- Aumento da cibersegurança
- Renovação de equipamentos

Adoção de uma estratégia de sustentabilidade ao implementar instrumentos de digitalização é uma tarefa impossível sem uma cibersegurança estável, de maneira que o risco de paralisação na produção seja minimizado.

O investimento crescente em cibersegurança resultou em uma redução recente na quantidade de ataques.

Iniciativas sustentáveis de empresas de P&G

- Energia de baixo carbono
- Garantia da segurança das pessoas (zero índice de acidentes fatais e redução de TRIR²)
- Emissões Net-Zero
- Respeito aos direitos humanos
- Preservação de recursos hídricos (prevenção de contaminação)
- Combate à corrupção
- Redução de resíduos (circularidade de produtos)
- Engajamento de públicos envolvidos
- Proteção da biodiversidade



Diminuição da quantidade de computadores ICS atacados no setor de petróleo e gás no segundo semestre de 2023 (comparado com o mesmo período em 2021)³

(1) - Objetivos de Desenvolvimento Sustentável foram adotados pelas Nações Unidas como estratégia de ação para garantir a paz e a prosperidade global até 2030.
(2) - Taxa global de acidentes registrados. (3) - De acordo com o cenário de ameaça analisado pela Kaspersky para estatísticas de sistemas de automação industrial para o segundo semestre de 2023.

Digitalização no setor de petróleo e gás

Aplicação de tendências de transformação digital

IIoT e nuvem

- 1 Aquisição e processamento de dados sísmicos
- 2 Otimização de perfuração
- 3 Detecção de vazamento em tubulação
- 4 Monitoramento de refinarias
- 5 Otimização de roteamento e monitoramento de armazenamento

Robotização e 5G

- 1 Robôs e drones submarinos e aéreos não operados para inspeção e operação de perfuração
- 2 Monitoramento de condições de tubulação em locais de difícil acesso e aquisição de dados
- 3 Inspeção de usinas e de capacidade para rápido fechamento em caso de problemas

Hiper-automação, IA, ML e RPA

- 1 Localização e definição de pontos de perfuração
- 2 Previsões de falhas de bombeamento
- 3 Análise de dados de tubulações e transporte
- 4 Previsão de falha em refinarias
- 5 Previsão de demanda do cliente

Metaverso industrial: AR, VR

- 1 Treinamento, colaboração de pessoal e manutenção em ambientes virtuais

Réplicas digitais (Digital Twins)

- 1 Modelagem de cenários de perfuração
- 2 Réplicas de sistema de tubulação para monitoramento
- 3 Modelagem de processos de refinaria de petróleo para detecção de gargalos

Convergência TI/TO

- 1 Análise de dados em tempo real de sensores e equipamentos

Operação

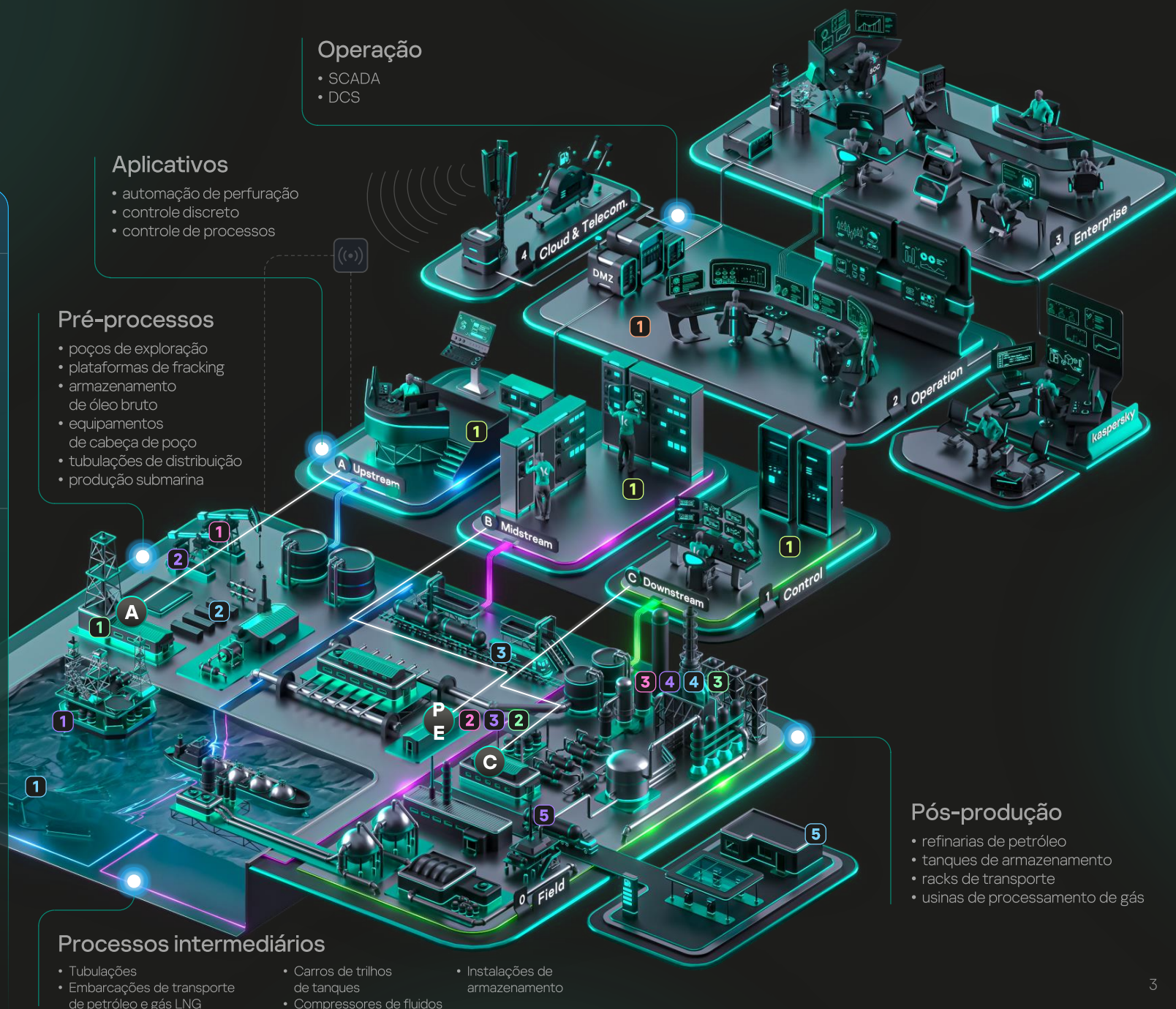
- SCADA
- DCS

Aplicativos

- automação de perfuração
- controle discreto
- controle de processos

Pré-processos

- poços de exploração
- plataformas de fracking
- armazenamento de óleo bruto
- equipamentos de cabeça de poço
- tubulações de distribuição
- produção submarina



Cibersegurança como tecnologia capacitadora

Legenda de cores de tendências de digitalização

- IoT e nuvem
- Réplicas digitais (Digital Twins)
- Robotização e 5G
- Metaverso industrial: AR, VR
- Hiper-automação, IA, ML e RPA
- Convergência TI/TO

1



Ao mesmo tempo, a transformação digital no setor de petróleo e gás avança no mesmo ritmo dos problemas e desafios da segurança...

- 1 Expansão da superfície de ataque
- 2 Infraestrutura legada e convergência de IT/OT fora de controle
- 3 Acesso externo à infraestrutura de TO
- 4 Escassez de pessoal
- 5 Regulamentações de proteção da infraestrutura crítica

Clique no item para continuar

1. Expansão da superfície de ataque

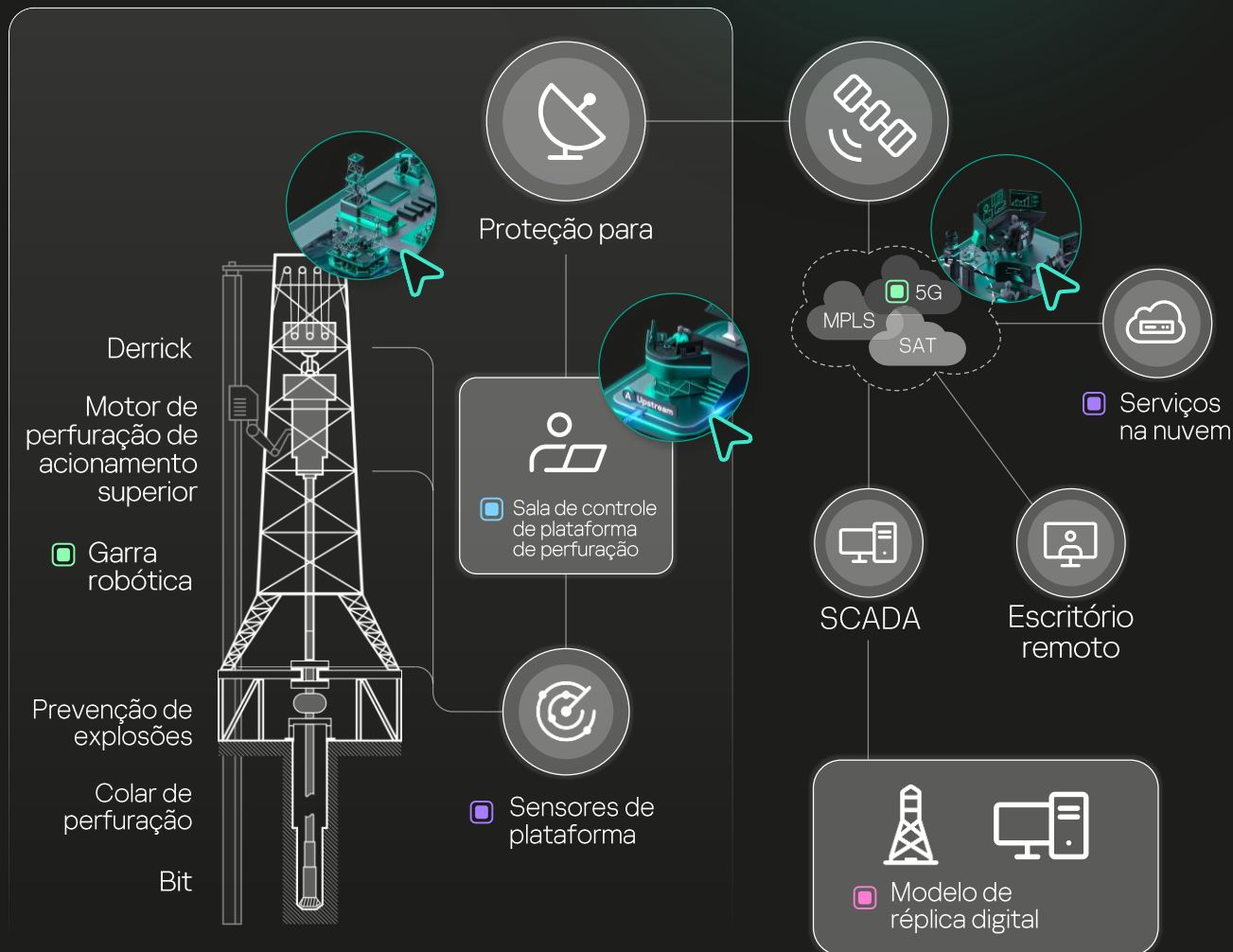
IIoT e nuvem

Réplicas digitais (Digital Twins)

Hiper-automação

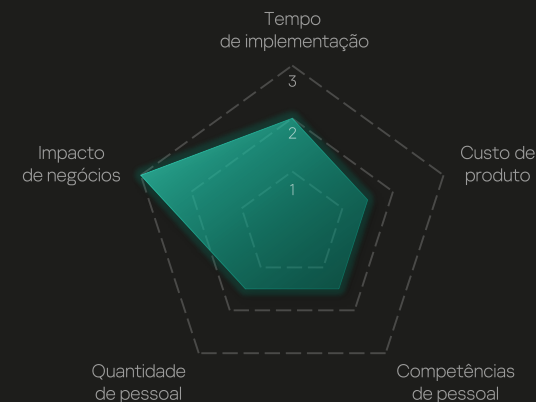
Robotização e 5G

Exemplo de processo de pré-produção



O ICS administra e monitora unidades de perfuração, oleodutos e refinarias, criando um ambiente de processo complexo. Um sistema tão interconectado se torna vulnerável a ciberataques quando uma conexão a um computador ou terminal permite acesso a uma superfície mais ampla.

Características da solução



A Kaspersky pode te ajudar



- Cobertura da infraestrutura de TO/IIoT de ponta a ponta
- Visibilidade de sistemas e de redes
- Auditorias de segurança periódicas minuciosas

Ecosistema de serviços de suporte



- Identificação de falhas de segurança em infraestruturas de ICS
- Verificação de componentes críticos



- Detecção proativa de ameaças
- Resposta orientada e automatizada
- Expertise em cibersegurança para ICS

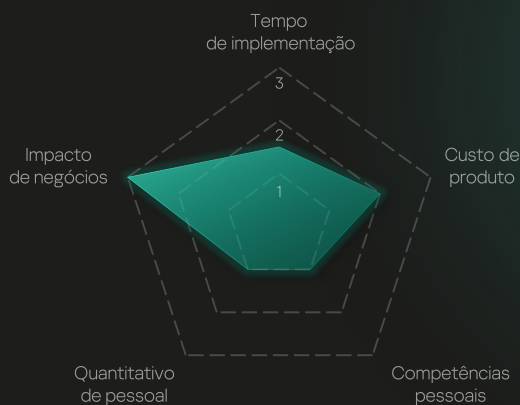
2. Infraestrutura legada e convergência de IT/OT fora de controle



A integração de IT e OT se tornou um fator vital na arquitetura de processos de P&G, mas sua implementação pode enfrentar riscos de segurança

- Infraestrutura legada desprotegida com tecnologia obsoleta
- Disparidade de prioridades entre a cibersegurança de sistemas que pode resultar em mecanismos de proteção conflitantes
 - Foco da TI na confidencialidade e integridade de dados
 - Foco da OT está nas operações e disponibilidade em tempo real

Características da solução



A Kaspersky pode te ajudar



- Detecção de ameaças e anomalias, medidas de resposta seguras sobre hosts e redes
- Gestão centralizada de riscos, política de segurança e gerenciamento de ativos em todos os níveis do IACS



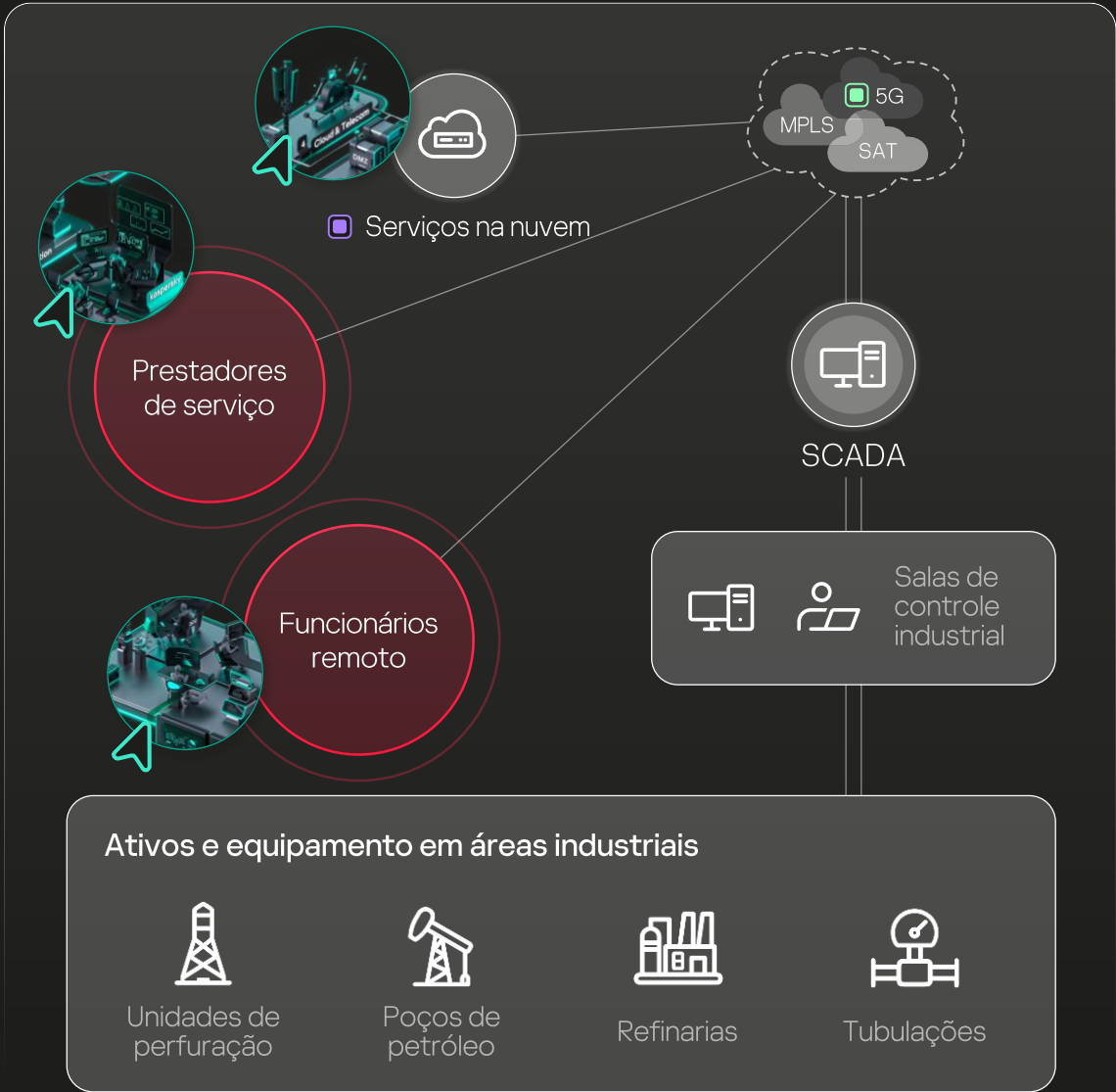
- Proteção de endpoints robusta contra ransomware, malware, ataques sem-arquivo e APTs
- Visibilidade completa e defesas robustas para todos os endpoints da organização.

Ecossistema de serviços de suporte



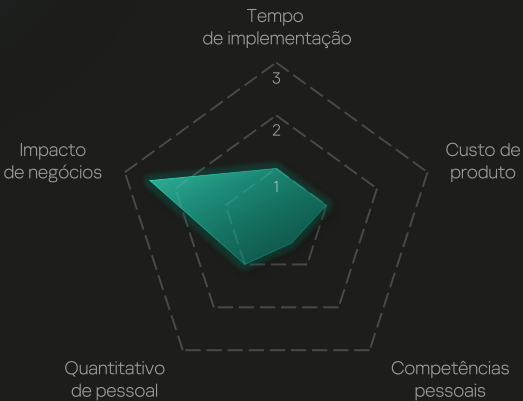
- Detecção de ameaças
- Investigações e caça ativa de ameaças
- Informações completas sobre vulnerabilidade e ameaça

3. Acesso externo à infraestrutura de OT



Capacidade de acesso remoto a tubulações, refinarias e outros sistemas de P&G permitem monitorar, orientar e analisar dados de processos industriais para funcionários e fornecedores remotos, graças à convergência de TI/OT. Esta otimização exige a proteção da conexão externa, conforme usuários com mais acesso à infraestrutura de OT pode expor a empresa a altos riscos de ciberataques.

Características da solução



A Kaspersky pode te ajudar

Kaspersky SD-WAN

Kaspersky Thin Client

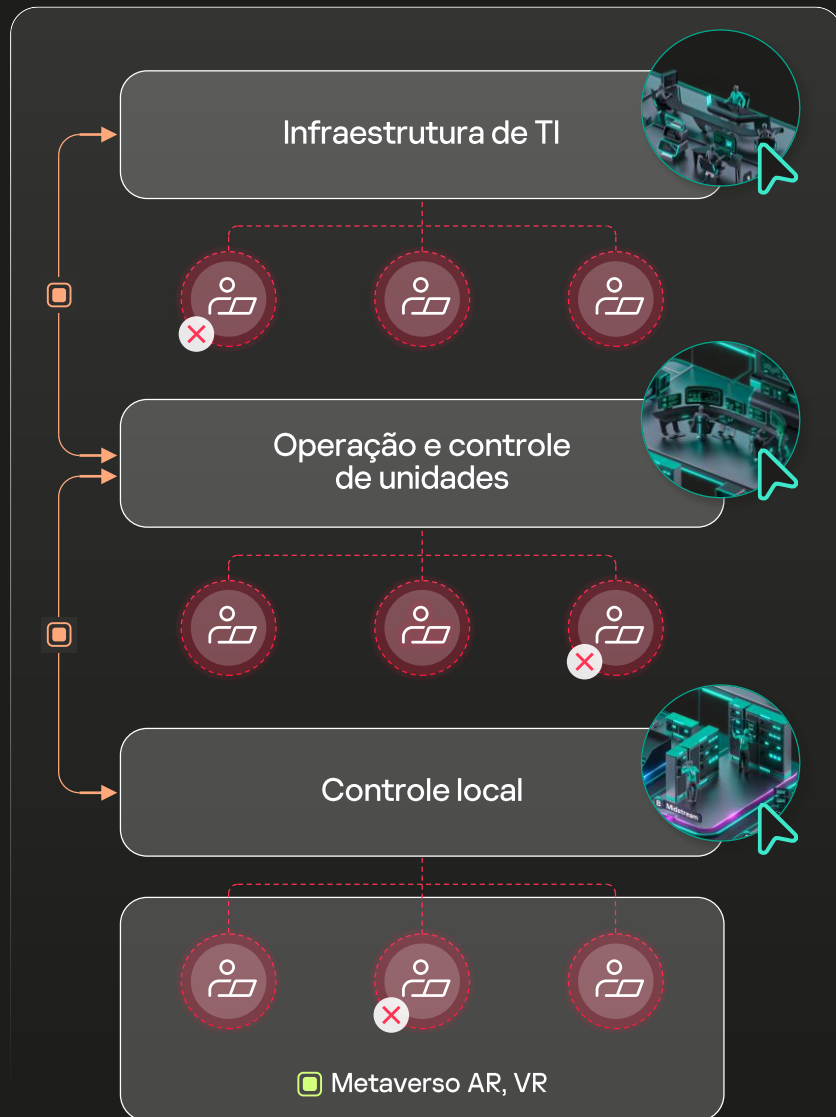
Implementação rápida da rede distribuída

- Fácil escalabilidade
- Gerenciamento conveniente
- Segurança centralizada

- Dispositivos com imunidade cibernética para acesso remoto seguro
- Ferramenta de gerenciamento centralizado para simplificar a administração da infraestrutura de dispositivos

4. Escassez de pessoas

Metaverso industrial Convergência TI – TO



Por mais de uma década, o setor de P&G enfrentou o desafio de recrutar e reter profissionais qualificados. Esse problema aumentou drasticamente com a transformação digital e a alta demanda de profissionais com expertise híbrida digital e técnica.

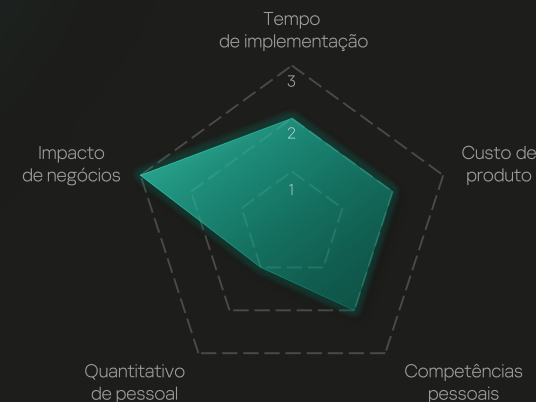
43%

dos funcionários

pesquisados globalmente em 2020 manifestavam vontade de deixar o setor energético nos próximos cinco anos ¹

(1) — Cenário no segundo semestre de 2022

Características da solução



A Kaspersky pode te ajudar



Kaspersky Industrial CyberSecurity

- Carga de trabalho reduzida para o pessoal responsável pela cibersegurança
- Resposta mais rápida a ameaças



Kaspersky Extended Detection and Response

- Open Single Management Platform
- Cibersegurança unificada em todos os segmentos industriais e corporativos

Ecosistema de serviços de suporte



Kaspersky Security Awareness

- Materiais de treinamento
- Treinamento gamificado com simulações de situações de negócios
- Módulos de aprendizado interativos e ataques simulados de phishing



Kaspersky ICS CERT

Habilidades práticas de especialistas

- Perícia digital e resposta a incidentes
- Exploração de vulnerabilidades
- Programas de treinamento trans-funcional

Clique no produto para saber mais

5. Regulamentações CIP

As regulamentações de cibersegurança para o setor energético, especialmente o setor de petróleo e gás, lidam com as ameaças e vulnerabilidades emergentes, e definem o padrão da indústria para a proteção de sistemas OT. Países em todo o mundo implementam normas e diretivas específicas que geralmente incluem:

- Gestão e avaliação de riscos
- Políticas e procedimentos
- Segurança de sistema
- Resposta e relatórios de incidentes
- Treinamento de pessoal



- ISA / IEC 62433
- ISO / IEC 27001
- ISA99



- Diretiva NIS2
- Diretrizes ENISA sobre cibersegurança para OT e ICS
- Estratégia de cibersegurança da UE
- Ato de cibersegurança da UE
- Ato de resiliência cibernética da UE



- NIST CSF
- NIST SP 800-82
- Diretiva de Segurança de Oleodutos TSA
- Norma API 1164
- Modelo de Maturidade de Capacidade de Cibersegurança DOE



- Estratégia de cibersegurança governamental
- Estrutura de avaliação cibernética da NCSC



- Ato de Segurança de TI 2.0 (Alemanha)
- BSI KritisV
- Compêndio de segurança BSI ICS (Alemanha)
- DVGW
- VDMA 66418



- Estratégia de Cibersegurança Nacional
- Estrutura de Cibersegurança ANSSI para ICS
- Lei de Proteção de Infraestrutura de Informação Crítica



- Estratégia de Cibersegurança da Holanda (NLCS)
- Ato de Segurança de Sistemas e Redes de Informação (WBNI)
- Guia NSCS para Medidas de Cibersegurança



- Estrutura de segurança nacional
- Decreto Real CNPI 704/2011
- Guias de Segurança CCN-STIC



- Ato de Cibersegurança da Suécia
- Ato de Segurança Protetiva da Suécia
- Orientação MSB



- Estratégia de Cibersegurança Nacional
- Lei de Cibersegurança No. 362/2018
- Regulamentações de Autoridade Regulatória de Energia Nacional



- Plano de Ação e Estratégia de Cibersegurança Nacional
- BTK CIPR
- Regulamentação de Cibersegurança EPDK



- Estratégia Nacional de Cibersegurança
- Estrutura PNSI
- Regulamentações ANP



- Diretrizes NCIIPC
- Ato de Tecnologia da Informação (IT) 2000



- GB/T 44462-2024
- GB/T 22239-2019
- GB/T 32919-2016
- GB/T 25070-2019



- Estratégia de Cibersegurança Nacional
- Regulamentação BSSN No. 4/2021
- Regulamento Presidencial No. 82/2022



- Normas de Garantia de Informação UEA
- Estrutura do Conselho de Cibersegurança UEA
- Norma de Segurança IoT UEA
- Política CIIP UEA



- NCA OTCC-1:2022
- NCA ECC-2-2024
- NCA CGLIoT-1:2024

Contate-nos para saber mais sobre normas e regulamentações regionais

A Kaspersky pode te ajudar

A Kaspersky fornece serviços e soluções baseadas no princípio de "defesa profunda", conforme recomendado por provedores de solução de segurança industrial, bem como organismos regulatórios em diversos países



Kaspersky
Industrial
CyberSecurity

Os produtos são projetados para garantir a conformidade das empresas de petróleo e gás com as normas **IEC 62443**, **NIS2**, **NERC CIP**, **SOC 2 Tipo 2**, **ISO/IEC 27001**



Compatibilidade testada com:



Mais de 130

sistemas de mais de 50 fornecedores

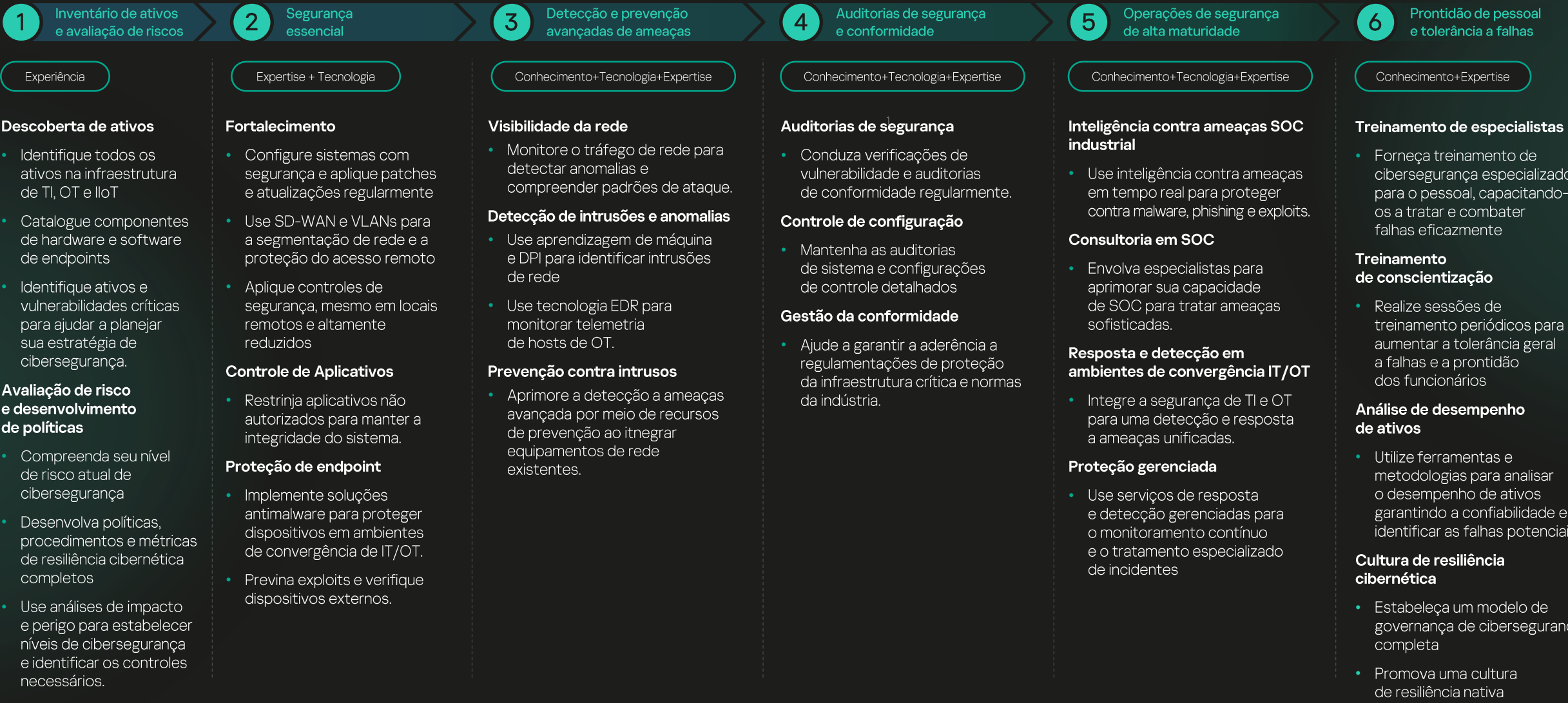


Conscientização de Segurança e Treinamento de Especialistas Kaspersky

Solução projetada para capacitar funcionários com habilidades de cibersegurança essenciais, promovendo a conformidade com os requisitos da Diretiva NIS 2

Leia mais sobre a Diretiva NIS 2 e a conformidade dos nossos produtos

Resiliência cibernética com o ecossistema OT Kaspersky



Saiba mais sobre a abordagem completa da Kaspersky para a cibersegurança em todos os níveis



Experiência Kaspersky no setor de petróleo e gás

+10 anos

de experiência no setor
de petróleo e gás

138 projetos

concluídos

12%
Proteção de empresas
de P&G com **12%**
do total da produção
mundial

60 empresas

já contando com a proteção

O Ecossistema de Cibersegurança OT Kaspersky fornece uma proteção completa para infraestruturas industriais no setor de petróleo e gás. A plataforma é capaz de detectar e responder a ataques complexos de maneira centralizada em toda a rede industrial.

Estudos de caso de clientes típicos

- Ajudar a integrar setores industriais e corporativos em uma infraestrutura protegida e unificada com uma segurança de ponta a ponta
- Centralização de todas as funções de segurança da informação em redes geográficas dispersas para aprimorar a visibilidade das atividades de infraestrutura e para um uso mais eficaz dos recursos humanos
- Auxílio na proteção de sistemas projetados sobre sistemas operacionais defasados e sem compatibilidade com equipamento de sistemas de segurança e sensíveis à verificação
- Garantia da operação estável do sistema de segurança da informação sob requisitos de alta disponibilidade e restrições de consumo de recursos

Por que as empresas do setor de petróleo e gás preferem a Kaspersky

- Expertise aprofundada em ciberameaças com o monitoramento consistente do cenário de ameaças
- Sistemas de segurança da informação criados levando em consideração para acompanhar as últimas tendências no cenário digital
- **Auxílio no cumprimento dos requisitos regulatórios**
- Nenhum impacto sobre o fluxo de trabalho e operação de dispositivos industriais
- Ofertas de produtos que participam regularmente em testes realizados por institutos de pesquisa internacionais, com um número recorde de primeiros lugares conquistados
- **Soluções testadas para garantir a compatibilidade com os produtos de fornecedores líderes de mercado**



>80%

de todos os requisitos
de segurança
da norma IEC 62443-3
com cobertura
da Kaspersky



242

sistemas de 57
fornecedores ICS
foram certificados

Estudos de caso de sucesso no setor de petróleo e gás

Nos últimos 10 anos, a experiência da Kaspersky atuou em:



Protegeu uma multinacional integrada com **80 campos de exploração** localizados com milhares de quilômetros de distância



Garantiu a segurança de um terminal específico regional com uma capacidade de produção de **205.000** toneladas de produtos petroquímicos, fornecendo controle de transporte marítimo e ferroviário



Implementou um sistema de cibersegurança para uma grande empresa de transporte de gás, parte de uma infraestrutura crítica e fornecimento de gás para mais de **20 milhões** de pessoas



5 maiores empresas de P&G da Rússia

- Proteção APCS usando a solução Kaspersky Industrial CyberSecurity
- Treinamento especial de "Conscientização de Cibersegurança Industrial" com base na experiência real na investigação de incidentes cibernéticos industriais

22 anos trabalhando com a Kaspersky

[Saiba mais](#)



Grande centro de P&D de pré-produção RN-BashNIPIneft

O sistema de segurança da informação centralizada é projetado com base em todo um ecossistema de produtos Kaspersky, garantindo uma proteção robusta contra ciberameaças e uma carga de trabalho otimizada para o pessoal de cibersegurança.

[Saiba mais](#)



Uma das maiores refinarias de petróleo do mundo

Optar pelo Kaspersky Industrial CyberSecurity (KICS) XDR resultou em:

- Segurança da informação mais robusta para refinarias
- Melhor cibersegurança e monitoramento e análise de processos de produção
- Detecção e resposta rápida de ameaças em potencial

[Saiba mais](#)

SIA VARS

O único terminal petroquímico na região do Báltico

Uso da solução Kaspersky Industrial CyberSecurity para garantir a proteção confiável de sistemas de controle de linha de produção automatizados para o transporte e armazenamento de produtos químicos.

[Saiba mais](#)

www.kaspersky.com.br

© 2024 AO Kaspersky Lab.
As marcas registradas e de serviço pertencem aos seus respectivos proprietários.

Gerencie sua segurança com a Kaspersky e torne-se um parceiro

Fale conosco e participe da nossa conferência global para clientes

Saiba mais



#kaspersky
#bringonthefuture