

Cyber OT

Lições dos ataques reais à indústria

Da ameaça cibernética ao risco operacional

David Alves

Solutions Sales Manager, Kaspersky



1. O cyber virou **risco operacional**

O que realmente estamos tentando proteger?

Em OT, servidores, redes, HMIs e PLCs são **meios** — o objetivo final é **proteger a operação**.

Impactos possíveis: produção, disponibilidade, qualidade, segurança das pessoas, meio ambiente e reputação.

A pergunta-chave não é apenas “o sistema foi comprometido?”, mas

“o que acontece com o processo físico?”



2. O ataque não precisa chegar ao PLC

Muitos incidentes OT começam — e às vezes terminam — fora do controlador.

- ✓ Active Directory, VPN, virtualização, servidores, estações de engenharia e credenciais podem ser suficientes para interromper a operação.
- ✓ Uma empresa pode parar a produção por segurança mesmo sem evidência de manipulação direta do processo.
- ✓ Convergência IT/OT também significa convergência de risco.

Pergunta:

quais sistemas digitais são indispensáveis para manter a operação?



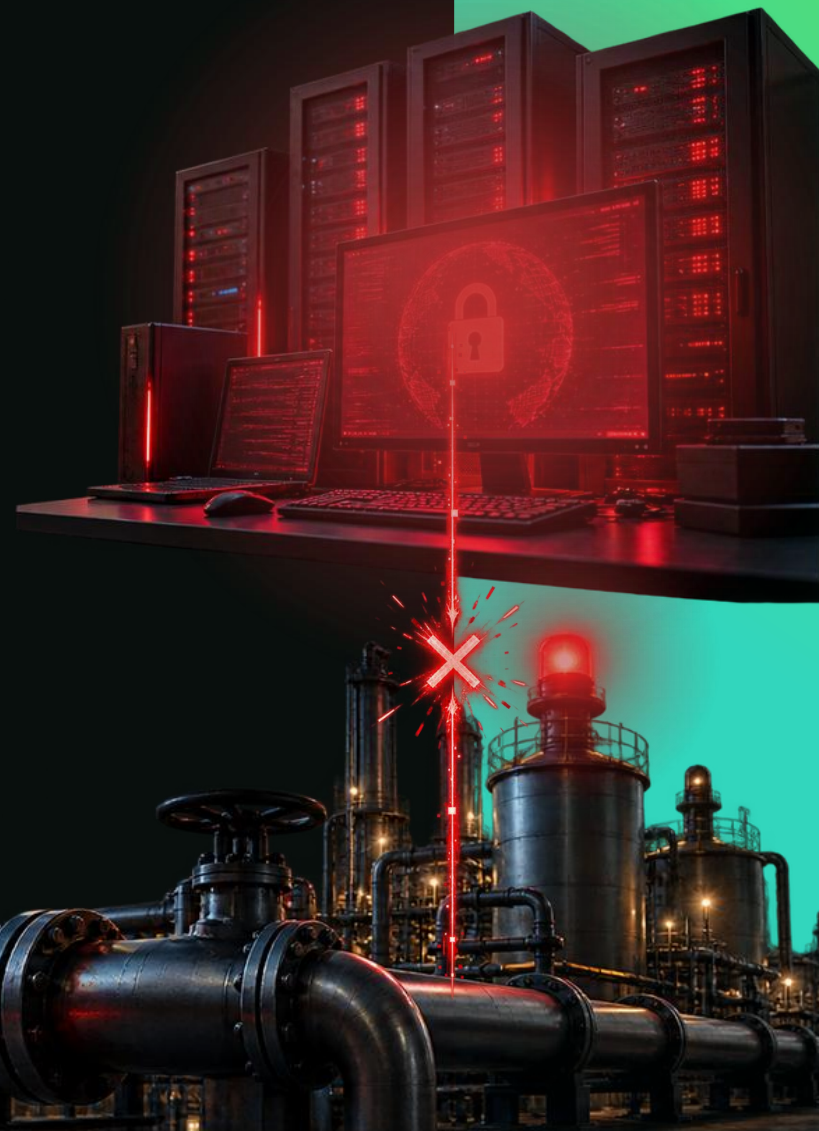
3. Colonial Pipeline (2021)

Ransomware em IT → interrupção de uma operação física crítica

- O ransomware DarkSide **comprometeu** a rede corporativa; a companhia interrompeu proativamente o sistema de dutos.
- O caso mostrou que impacto operacional não exige, necessariamente, **comprometimento direto da rede OT**.

Lição: segmentação, controle de acessos, visibilidade IT/OT e planos de continuidade precisam ser tratados como **um único problema operacional**.

IT comprometido **≠** impacto apenas em IT



4. Norsk Hydro (2019)

LockerGoga: ransomware, operação manual e resiliência industrial

- O ataque atingiu a **organização global** e causou desafios operacionais relevantes, especialmente em **Extruded Solutions**.
- Diversas unidades recorreram a procedimentos e **operação manual** para manter a produção.
- A Hydro estimou o custo total do incidente em aproximadamente **NOK 800 milhões**.

Lição: resiliência não começa no recovery — ela precisa ser **desenhada antes** do incidente.



5. TRITON / TRISIS

Quando cybersecurity encontra process safety

- TRITON demonstrou uma classe de ameaça capaz de interagir com Safety Instrumented Systems (SIS).
- A discussão deixa de ser apenas confidencialidade e disponibilidade: passa a envolver potencial impacto sobre segurança física e processo.

Lição: equipes de cybersecurity, engenharia, automação e safety precisam compartilhar contexto, responsabilidades e resposta.



Cyber Risk + Process Safety



6. Volt Typhoon

Persistência silenciosa e técnicas “Living off the Land”

- Agências dos EUA alertaram para atividade contra infraestrutura crítica usando contas válidas e ferramentas legítimas do próprio ambiente.
- A estratégia favorece persistência prolongada e dificulta a distinção entre atividade administrativa e comportamento malicioso.

Lição: inventário, baseline de comportamento, logs, contexto de rede e capacidade de hunting tornam-se fundamentais.

“ Não podemos proteger aquilo que não conhecemos.



7. O padrão por trás dos incidentes



8. Como desenhar uma **defesa OT**

Cinco capacidades que reduzem risco sem comprometer a operação.



1. Conhecer

Inventário, ativos, versões, vulnerabilidades e dependências

2. Segmentar

Zonas, conduítes, DMZ e controle de fluxos

3. Proteger

Endpoints OT respeitando disponibilidade e legado

4. Monitorar

Tráfego industrial, protocolos, anomalias e contexto

5. Responder

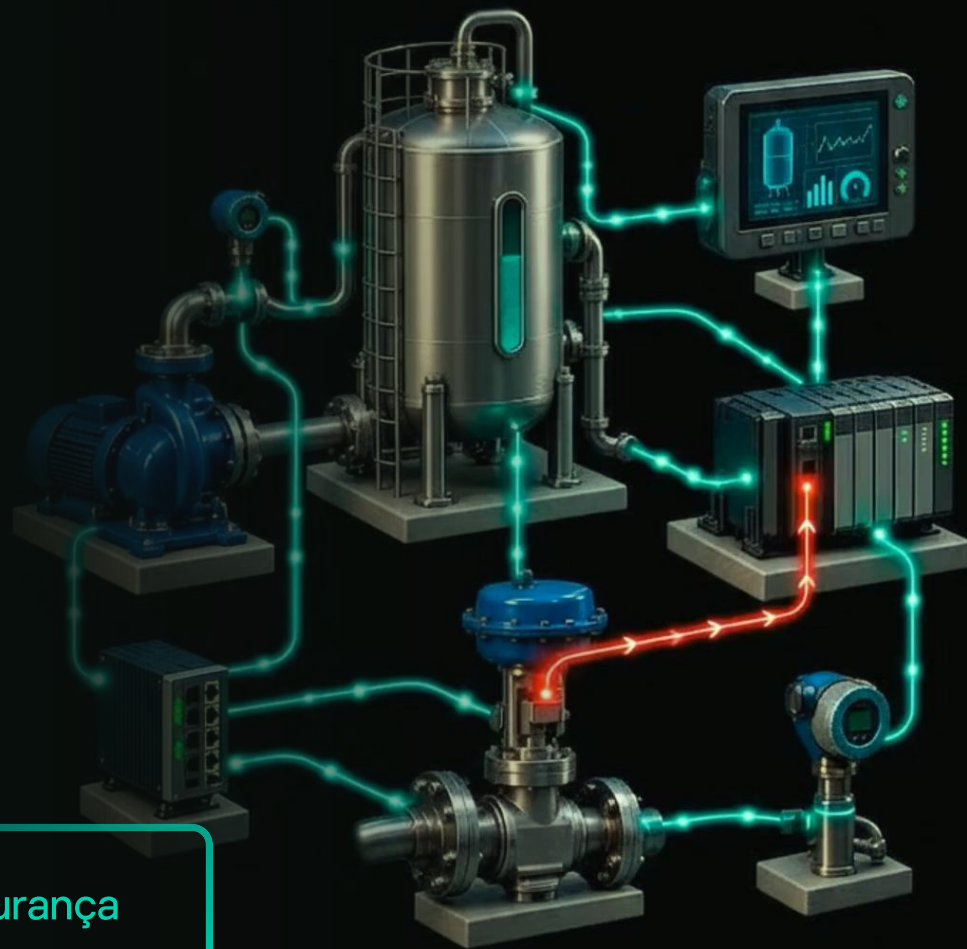
Playbooks conjuntos entre SOC, OT, engenharia e produção

9. Em OT, contexto é o diferencial

- Uma **conexão** pode ser legítima — ou representar uma mudança perigosa no processo.
- **Perguntas úteis:**
Este ativo deveria falar com aquele?
Este protocolo é esperado?
Este comando faz parte da manutenção programada?
- **Monitoramento** de rede OT permite observar protocolos industriais sem instalar agentes em todos os dispositivos.

Exemplos: Modbus, S7, EtherNet/IP, OPC, IEC 104 e DNP3.

Dados + contexto operacional = informação de segurança



Ecosistema de proteção OT: tecnologia + inteligência + serviço

Capacidades complementares para proteger ativos, detectar anomalias, investigar e responder.

MLAD

Processo industrial

Machine Learning sobre telemetria de processo para identificar desvios e anomalias tecnológicas.

KICS for Nodes

Endpoints OT

Proteção, detecção e resposta em HMIs, estações de engenharia, servidores e hosts Windows/Linux.

KICS for Networks

Rede industrial

Visibilidade de ativos, DPI de protocolos OT, NDR, detecção de intrusões e anomalias.

MDR

Operação 24x7

Especialistas analisam telemetria, investigam incidentes e apoiam recomendações de resposta.



KIXDR OT

Correlação e resposta

Correlaciona eventos de rede + endpoint, enriquece incidentes e amplia o contexto de investigação.

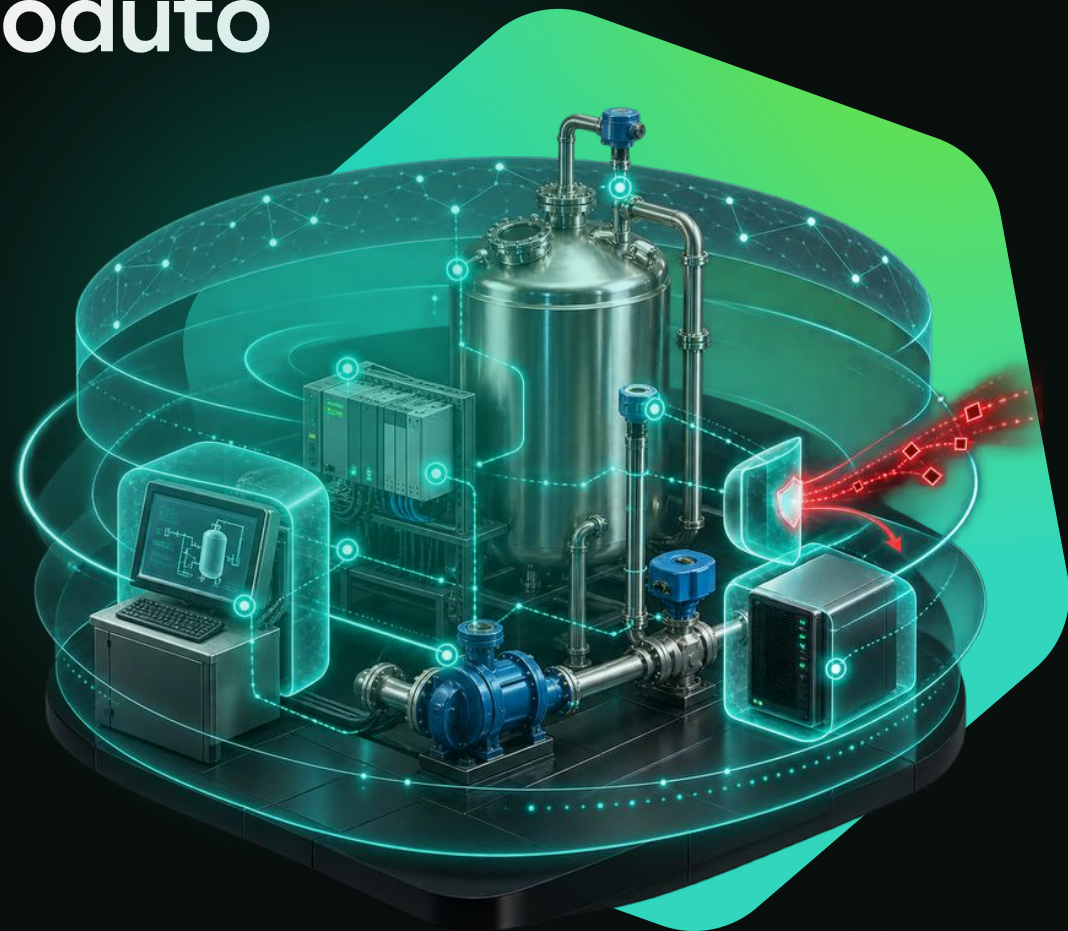
Mensagem: não existe uma única tecnologia que resolva OT — a cobertura vem da combinação de endpoint, rede, XDR, processo e expertise.

10. Onde a tecnologia entra – sem começar pelo produto

Primeiro a necessidade; depois a **capacidade tecnológica**.

- **Visibilidade e inventário** → conhecer ativos e comunicação.
- **Monitoramento e detecção** → identificar anomalias, intrusões e mudanças relevantes.
- **Proteção de endpoints OT** → proteger estações e servidores respeitando requisitos industriais.
- **Gestão e resposta** → correlacionar eventos e apoiar investigação e contenção.

Na Kaspersky, essas capacidades são cobertas pelo portfólio **Kaspersky Industrial CyberSecurity (KICS)**, incluindo KICS for Networks e KICS for Nodes.



11. Dos incidentes às capacidades



Colonial Pipeline

Dependência IT/OT →

Segmentação +
visibilidade +
continuidade

TRITON/TRISIS

Cyber + safety →

Monitoramento OT
+ controle de
mudanças



Norsk Hydro

Ransomware e
recuperação →

Endpoint + resposta +
recovery

Volt Typhoon

Persistência e LOTL →

Baseline + hunting +
telemetria + contexto



+



+



Pessoas Tecnologia Processo

12. Como levar a conversa para a gestão

Cybersecurity OT não é uma discussão sobre ferramenta — é uma discussão sobre risco.

- Qual é o **custo** de uma hora ou um dia de parada?
- Quais **processos** não podem parar?
- Quanto **tempo** conseguimos operar manualmente?
- Qual é o nosso tempo aceitável para **detectar**, **conter** e **recuperar**?
- Quais **cenários cyber** podem gerar impacto em produção, safety ou meio ambiente?

Trocar “quanto custa cybersecurity?” por
“quanto custa perder a operação?”



13. Três perguntas para levar para casa

**Cyber risk é
operational risk.**

1 Você sabe exatamente o que tem?

2 Você consegue ver o que está acontecendo?

3 Você está preparado para responder sem colocar a operação em risco?

Fontes e leituras recomendadas

Links clicáveis para os incidentes e para a abordagem de segurança OT.

[Colonial Pipeline – U.S. Department of Energy](#)



[Volt Typhoon – Joint Cybersecurity Advisory](#)



[Colonial Pipeline – FBI / DarkSide](#)



[CISA – Industrial Control Systems](#)



[Norsk Hydro – página oficial do incidente](#)



[Kaspersky Industrial CyberSecurity – visão geral PT-BR](#)



kaspersky



OBRIGADO!
OBRIGADO!
OBRIGADO!



David Alves

Solutions Sales Manager Enterprise, Kaspersky