Redes Industriais Resilientes:

Conectividade e Segurança como Vantagem Competitiva

AVISO IMPORTANTE

O conteúdo técnico da palestra é de responsabilidade da empresa palestrante.

Fique à vontade para baixar o arquivo em PDF e se atualizar com as novas tecnologias apresentadas nesta edição.

Qualquer dúvida em relação ao conteúdo apresentado, você pode entrar em contato direto com o palestrante.

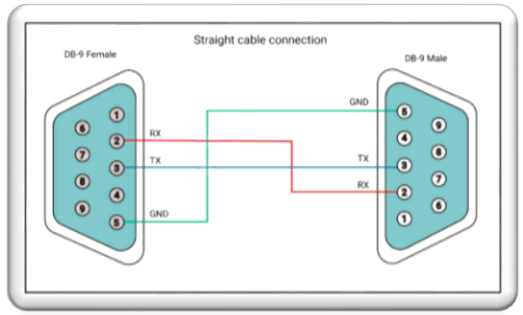
Agenda

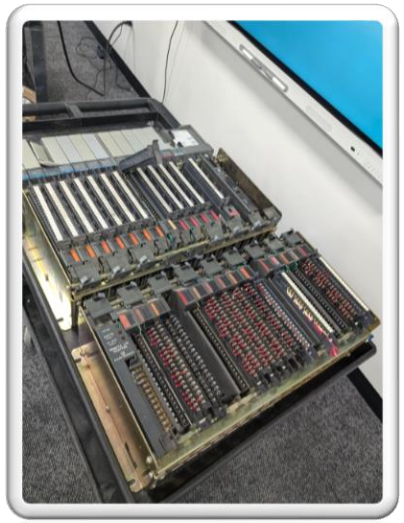
- O Cenário Atual das Redes Industriais
- **O que é resiliência em Redes Industriais**
- Os 3 Pilares da Resiliência
- **Do Técnico ao Negócio**
- Caminhos para implantação

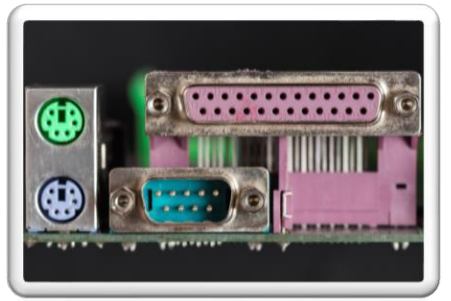
ECO AUTOMAÇÃO INDUSTRIAL

O Cenário Atual das Redes Industriais

ANTES: Redes Industriais **eram isoladas**





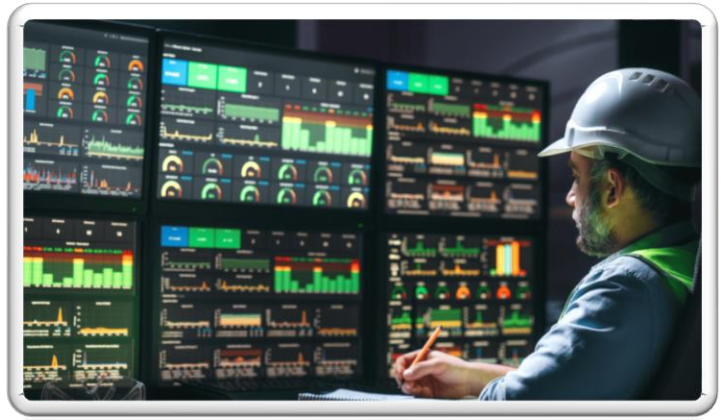


PROFIBUS®

ECO AUTOMAÇÃO INDUSTRIAL

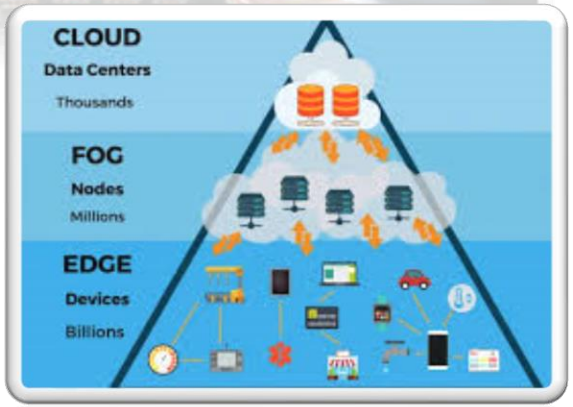
O Cenário Atual das Redes Industriais

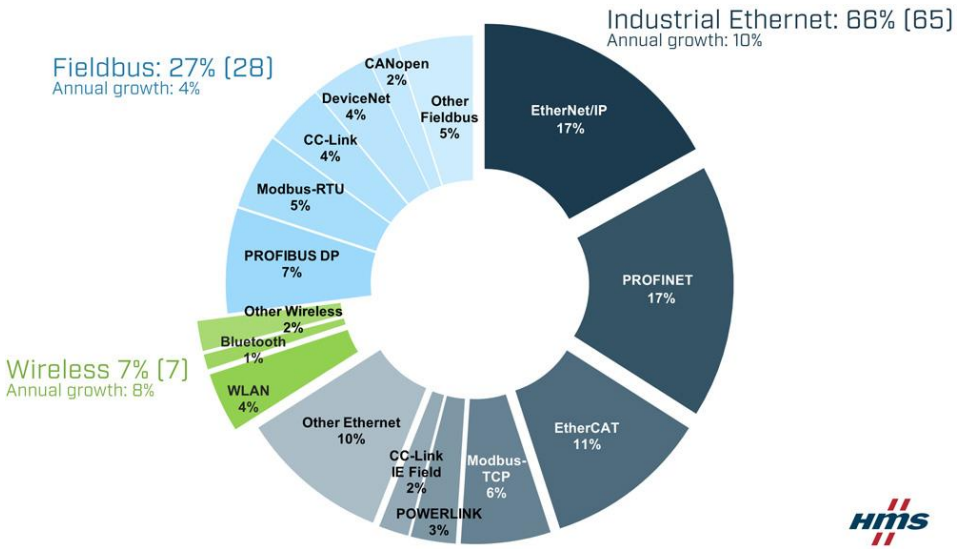
AGORA: Convergência **TI + OT**



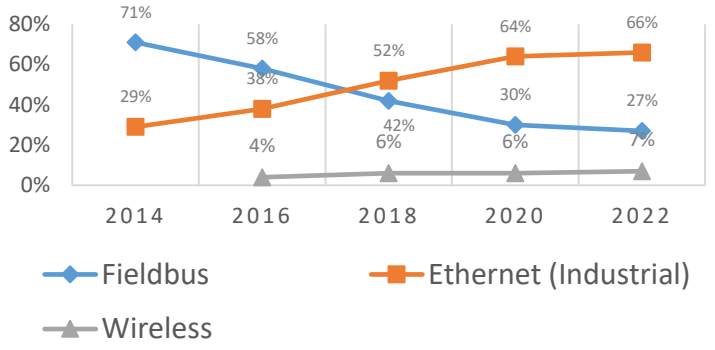
MQTT

Node-RED





Market shares **2022** according to HMS Networks – fieldbus, industrial Ethernet and wireless.

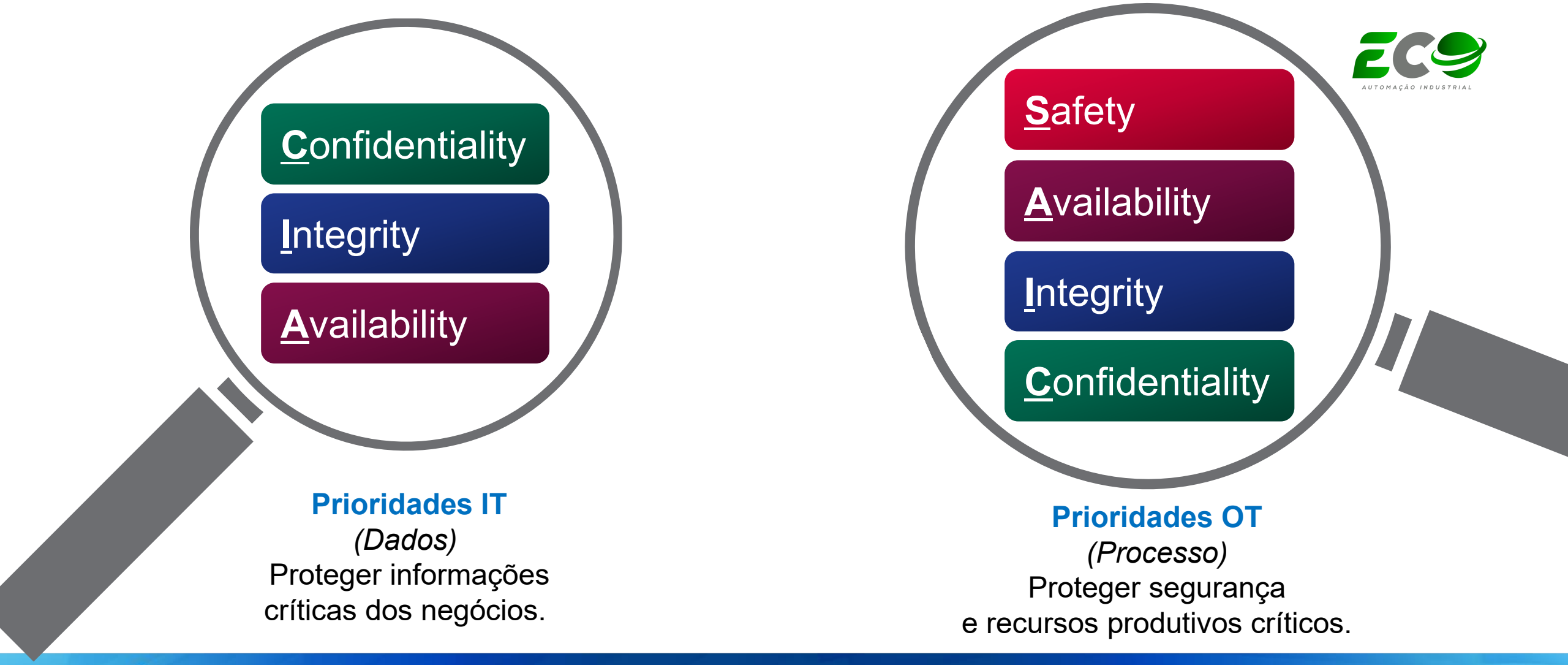


O novo ecossistema industrial

Convergência IT/OT:

Integração de redes industriais e corporativas

O novo ecossistema industrial



Prioridades IT
(Dados)
Proteger informações
críticas dos negócios.

Prioridades OT
(Processo)
Proteger segurança
e recursos produtivos críticos.

O novo ecossistema industrial

Chão de Fábrica

Sensores, máquinas e sistemas OT (SCADA, CLP). Dados brutos e operações críticas em tempo real.

Edge Computing

Processamento local de dados, decisões rápidas e redução da latência antes de enviar para a nuvem.

Integração TI

Conectividade com sistemas corporativos (ERP, MES), permitindo a visualização e análise de dados operacionais.

IA

Otimização de processos e manutenção preditiva com inteligência artificial.

AUTOMAÇÃO INDUSTRIAL

O novo ecossistema industrial

A complexidade aumenta com protocolos heterogêneos (Ethernet industrial, Profinet, Modbus TCP, MQTT, OPC UA) e a necessidade de comunicação fluida entre as camadas.

Tendências Globais

1. ***Aderência crescente a estruturas de conformidade regulatória como NIS2, IEC 62443, Lei de Ciber-resiliência da UE, Diretrizes da TSA, entre outras.***

2. *O Diretor de Segurança da Informação (CISO) tem um papel fundamental na condução da cibersegurança em OT, mas enfrenta desafios para promover mudanças no nível das plantas.*

3. ***As organizações têm contado com soluções de visibilidade para começar, mas muitas ainda não implementaram nenhuma camada de proteção.***

4. *As organizações continuam a priorizar a cibersegurança industrial e buscam maneiras de identificar falhas e reduzir riscos nas operações.*

ECO AUTOMAÇÃO INDUSTRIAL

Cenários de riscos

1. ***Sistemas Legados;***
2. *Redes anteriormente isoladas (Air Gapped);*
3. ***Ransomware;***
4. *Número crescente de vulnerabilidades;*
5. ***Proliferação de dispositivos x IoT;***
6. *Ameaças Internas;*
7. ***Riscos de Supply Chain.***

ECO AUTOMAÇÃO INDUSTRIAL

Redes OT precisam de Cibersecurança aprimorada

1. ***As redes OT não foram projetadas para serem seguras contra ameaças externas;***
2. *Convergência desafiadora entre os sistemas de TI e OT;*
3. ***Complexidade e diversidade das redes OT e da cadeia de suprimentos;***
4. *Riscos diretos à segurança (danos físicos, perigos ambientais, perda de vidas);*
5. ***Escassez de habilidades versus conformidade regulatória;***
6. *O cenário de ameaças está se profissionalizando.*

ECO AUTOMAÇÃO INDUSTRIAL

CURIOSIDADES

Em 2023, estimava-se que existiam mais de **29 bilhões de dispositivos** conectados globalmente!

VOCÊS SABIAM?

Aproximadamente, **70% dos ataques cibernéticos na indústria**, visam redes OT, mostrando a importância da segurança industrial.

ECO AUTOMAÇÃO INDUSTRIAL

O problema da conectividade sem segurança

Redes industriais, historicamente confiáveis, não foram projetadas para o cenário de ameaças atual.

Casos Reais de Ataques

- **Stuxnet (2010):** Sabotagem de centrífugas nucleares iranianas, demonstrando o poder de um ataque direcionado a sistemas OT.
- **Norsk Hydro (2019):** Ataque de ransomware que custou à empresa mais de US$ 50 milhões e afetou suas operações globais.
- **Colonial Pipeline (2021):** Ransomware que paralisou a maior distribuidora de combustível dos EUA, causando pânico e desabastecimento.

ECO AUTOMAÇÃO INDUSTRIAL

O problema da conectividade sem segurança

Os riscos vão além dos ciberataques, **incluindo falhas de comunicação e erro humano.** A falta de segmentação e dispositivos legados são pontos de entrada críticos.

CURIOSIDADES

Ransoware as a Service , compra de pacotes de ataque na deep web.

VOCÊS SABIAM?

Infras críticas no mundo (agua, energia) **sofre 13 ataques por Segundo.**

O que é resiliência em Redes Industriais

Resiliência é a **capacidade de uma rede industrial manter a operação estável, mesmo diante de falhas, ataques ou picos de demanda.** É garantir que a produção não pare — a qualquer custo.

Alta Disponibilidade

Segurança Integrada

Monitoramento Proativo

ECO AUTOMAÇÃO INDUSTRIAL

O que é resiliência em Redes Industriais

Resiliência em redes industriais é como um hospital: **não pode parar de funcionar, mesmo se houver queda de energia ou ataque.**

Por isso existem geradores como backup, protocolos de segurança e monitoramento 24/7.

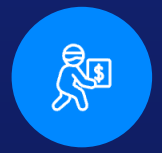
ECO AUTOMAÇÃO INDUSTRIAL

Os 3 Pilares da Resiliência

Para construir redes industriais verdadeiramente resilientes, é fundamental atuar em três frentes complementares.

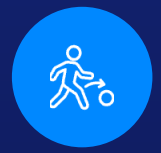
Desenho da Rede Inteligente

- Segmentação OT e TI (VLANs, DMZ).
- Switches industriais robustos.
- Topologias redundantes (PRP/HSR, MRP, RSTP).



Segurança Integrada

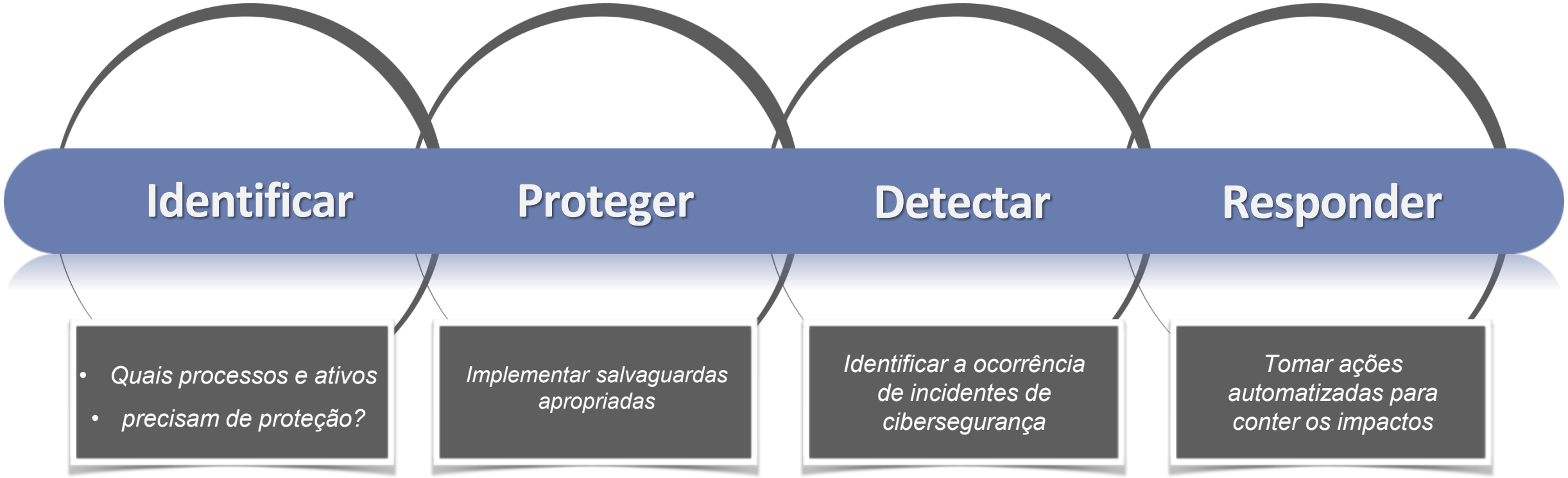
- VPNs industriais dedicadas para acesso remoto seguro.
- Firewalls e ACLs/DPI para controle de tráfego.
- Autenticação multifator e políticas de atualização.



Monitoramento Contínuo

- Ferramentas de monitoramento.
- Alarmes para tráfego anômalo e quedas.
- Dashboards em tempo real para gestão proativa.

Cybersecurity Framework



ECO
AUTOMAÇÃO INDUSTRIAL

Cybersecurity Framework

Identificar

- *Avaliação de Riscos*
- *Avaliação de Vulnerabilidades*
- *Arquitetura de Rede*
- *Fluxos de Dados*
- *Inventário de Hardware e Software*

Proteger

- *Autenticação*
- *Segmentação de Rede*
- *Controles de Acesso Lógico*
- *Acesso Remoto*
- *Fluxos de Informação*
- *Controle de Mudanças*

Detectar

- *Varredura de Vulnerabilidades*
- *Eventos Operacionais*
- *Monitoramento de Rede*
- *Detecção de Código Malicioso*

Responder

- *Resposta Automatizada*

ECO AUTOMAÇÃO INDUSTRIAL

Do Técnico ao Negócio

Investimento em Cybersecurity tem que vir de cima, da alta Gestão

Precisa de Patrocínio e Patrocinador

Precisa de Conscientização

"Resiliência em rede não é só proteção — **é estratégia ao Negócio**."

Do Técnico ao Negócio

Benefícios Técnicos

- **Menos Downtime:** Redução drástica de paradas inesperadas.
- **Melhor Desempenho:** Tráfego segmentado evita gargalos e colisões, otimizando a comunicação.
- **Facilidade de Manutenção:** Acesso remoto seguro e monitoramento preciso agilizam a atuação da equipe.

Do Técnico ao Negócio

Impacto no Negócio

- **ROI Direto:** Evitar uma única parada pode compensar todo o investimento em resiliência.
- **Conformidade:** Atendimento a normas como ISO 27001 e IEC 62443, essenciais para auditorias e certificações.
- **Confiança de Clientes:** Indústrias resilientes atraem e retêm clientes em setores críticos, fortalecendo contratos e reputação.

Do Técnico ao Negócio

Antes

- Empresa com rede única para administrativo e produção.
- Infecção via e-mail corporativo.
- Linha parada **3 dias**, prejuízo milionário.

Depois

- Segmentação de rede (OT x TI), VPN segura, monitoramento 24/7.
- Tentativa de intrusão bloqueada sem afetar a produção.

"Com pequenas mudanças estruturais, você transforma uma vulnerabilidade em resiliência."

ECO AUTOMAÇÃO INDUSTRIAL

Caminhos para Implantação

“A resiliência não é um projeto único,
mas um ciclo contínuo de aprimoramento”

Caminhos para Implantação

Transformar a teoria em prática exige um **ciclo contínuo de ações estratégicas.**

ECO AUTOMAÇÃO INDUSTRIAL

Caminhos para Implantação

Para dar certo essa integração:

- **Formar um time multidisciplinar é o primeiro passo**
- Definir a estratégia de negócios
- **Definir os parceiros e tecnologia e implementar de forma gradual em pilotos ou MVPs**

Se amanhã sua **rede** fosse **comprometida,** quanto tempo sua **produção sobreviveria?**

Se alguma informação **vazasse,** daria **uma grande,** vantagem competitiva **para o concorrente?**

ECO AUTOMAÇÃO INDUSTRIAL

Se alguém

Acessar o sistema

Se alguém

Acessar o sistema

Alterar os dados

Se alguém

Acessar o sistema

Alterar os dados

Copiar informações

Se alguém

Acessar o sistema

Alterar os dados

Copiar informações

Deletar processos críticos

AUTOMAÇÃO INDUSTRIAL

Se alguém

Acessar o sistema

Alterar os dados

Copiar informações

Deletar processos críticos

Roubar os dados

Essas ações

Essas ações resultariam em um

Essas ações
resultariam em um
GRANDE

Essas ações
resultariam em um
GRANDE
PROBLEMA?

OBRIGADO!

Clayton Becker

Business Manager

+20 anos atuando em projetos de TI e OT
Apoio técnico e estratégico na implementação da Indústria 4.0 e transformação digital em Fabricantes de máquinas e Indústrias.