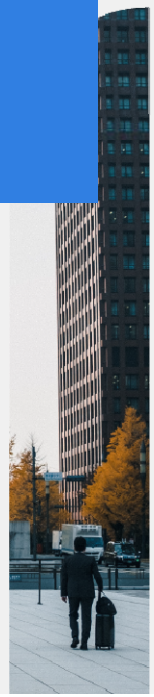
Cibersegurança:
Como Atender a Rotina Operacional do ONS

Fernando Lobo

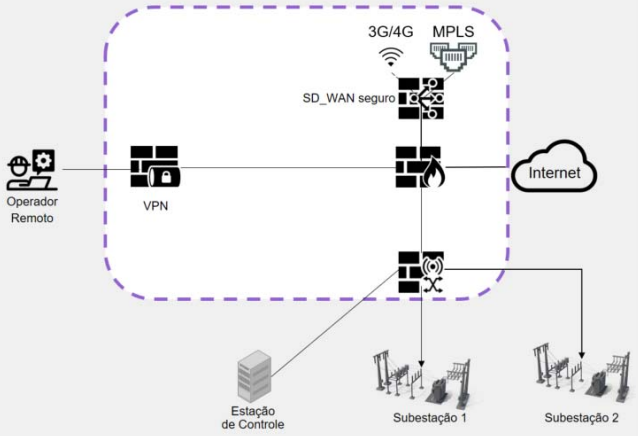
LATAM & Canada Operational Technologies Director



Agenda

ONS publica rotina de cyber para todo o setor elétrico

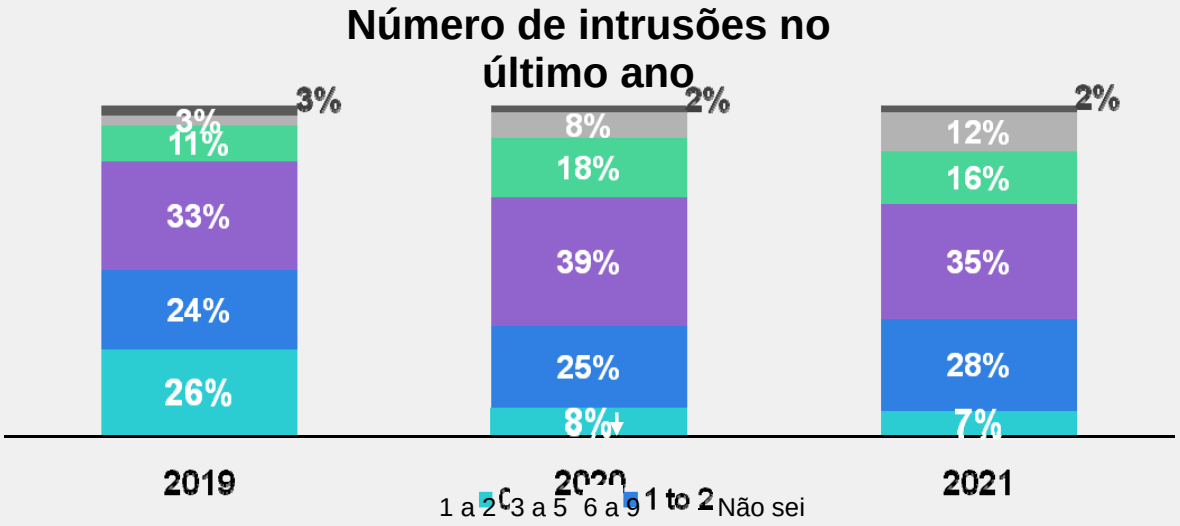
Arquitetura Segura para o Setor Elétrico



Intrusões - parte do novo normal

As interrupções afetam a produtividade, a receita e a segurança física

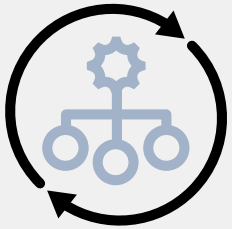
9 de 10 organizações em OT sofreram pelo menos uma intrusão no ano passado e 63% tiveram 3 ou mais intrusões, o que é semelhante aos resultados em 2020..



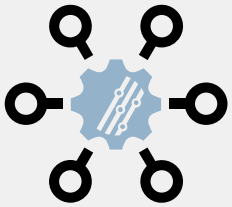
42% experienced insider breaches, which is up from **18%** last year.

Comparando as Organizações de Melhor e Pior Desempenho

Existe uma prática recomendada? Comparando aquelas sem intrusões e aquelas com 10 ou mais intrusões.



São mais propensos a usar **orquestração e automação** e ter **rastreamento e relatórios de segurança** em vigor.



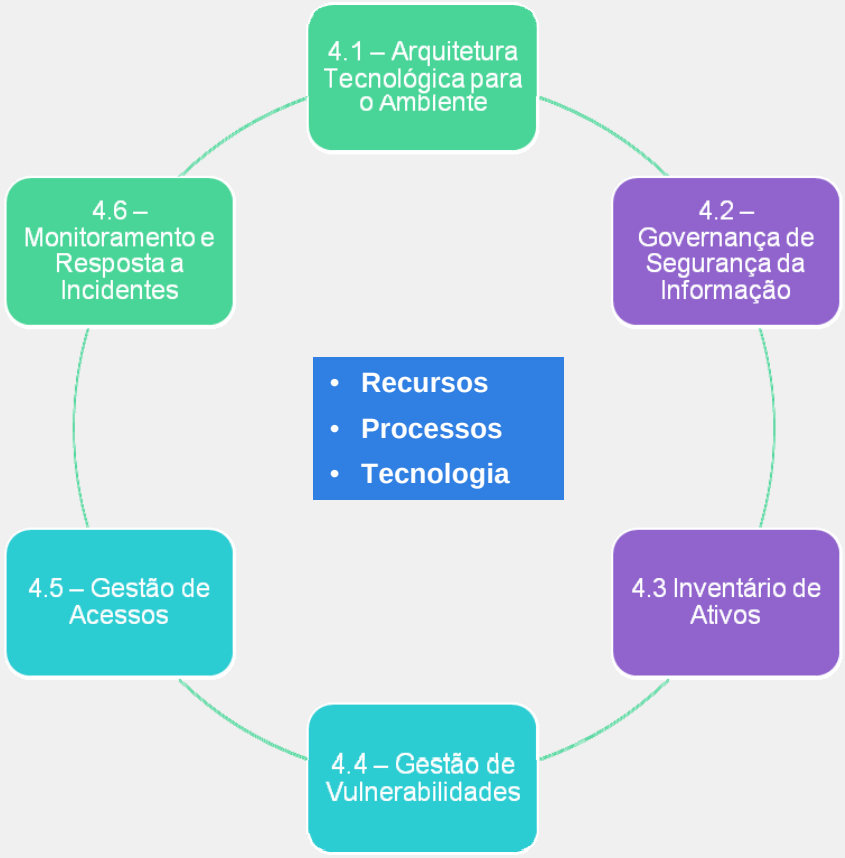
É mais provável que tenham **100% de visibilidade centralizada** em seu centro de operações de segurança.

Estavam mais preparados, e mais rápido, para **acomodar o trabalho remoto** impulsionado pela pandemia.

Análise da Rotina Operacional do ONS

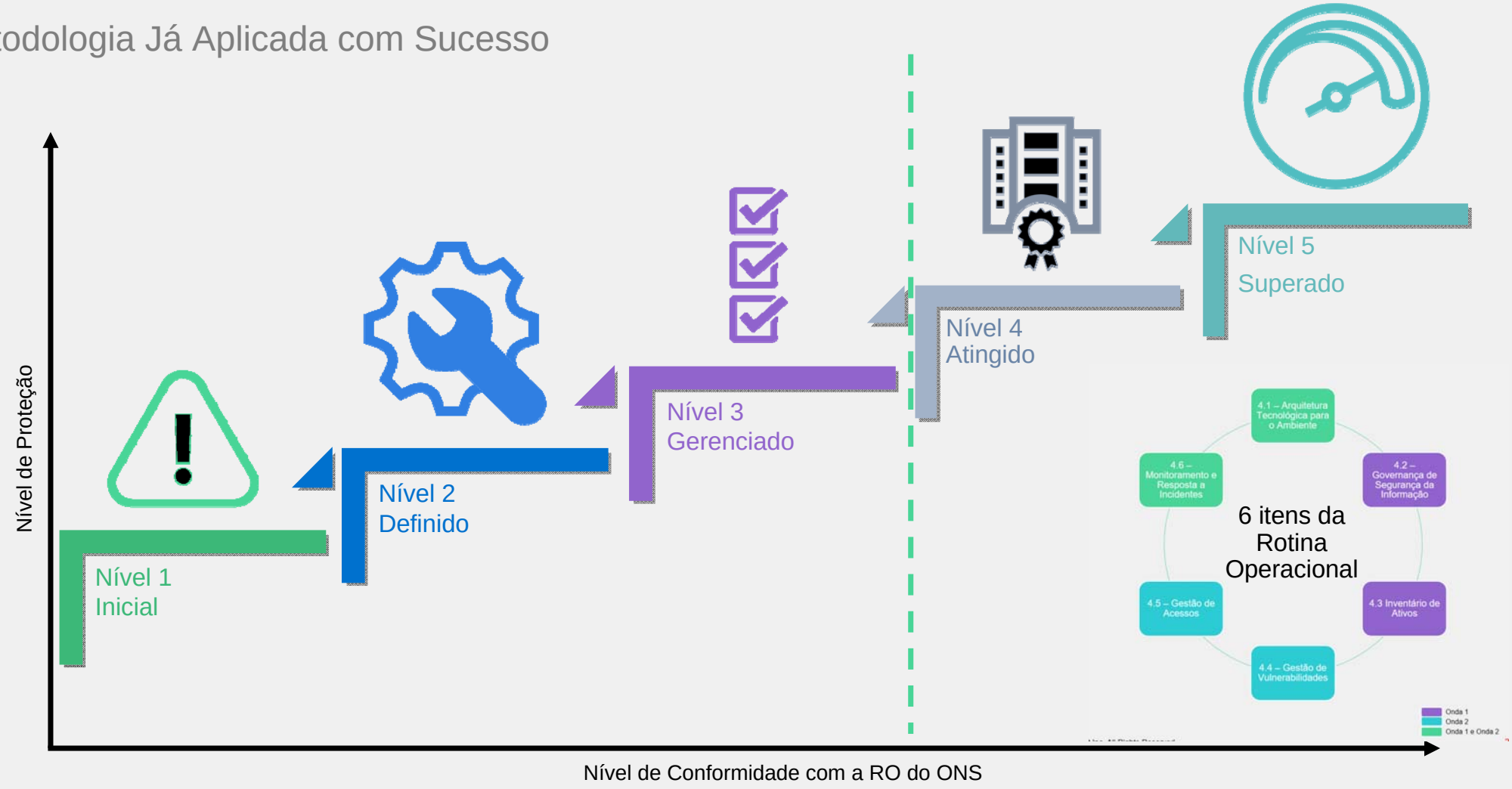
Informações sobre a RO-CB.BR.01

- ARCiber – **A**mbiente **R**egulado **Cibe**rnético
  - Centros de operação dos agentes;
  - Equipamentos que participam da infraestrutura de envio ou recebimento de dados e voz para ambientes operativos do ONS ou para centros de operação de outros agentes;
  - Ambiente operativo do ONS.
- Datas
  - Vigência: 09/07/2021
  - Onda 1: 09/01/2023
  - Onda 2: 09/10/2023



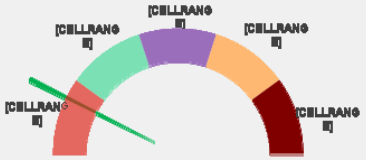
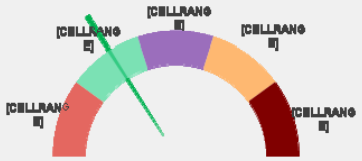
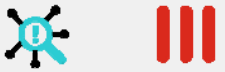
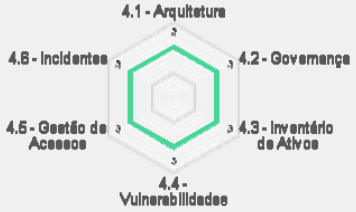
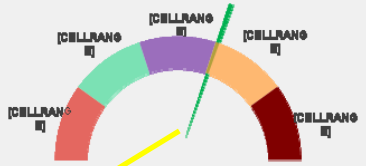
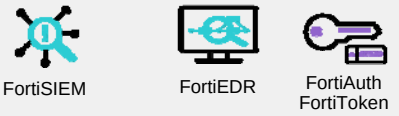
Score de Conformidade com a RO do ONS

Metodologia Já Aplicada com Sucesso



Resultado: Um Roadmap para Elevar o Nível de Segurança Cibernética

De forma gradual e dentro dos prazos estabelecidos

Fases de Projeto	Avaliação por Domínio	Nível de Conformidade Geral	Soluções Recomendadas
Situação Atual			
Fase 1 Inventário e Resposta a Incidentes			
Fase 2 Gestão de Acesso e Proteção de Endpoints			

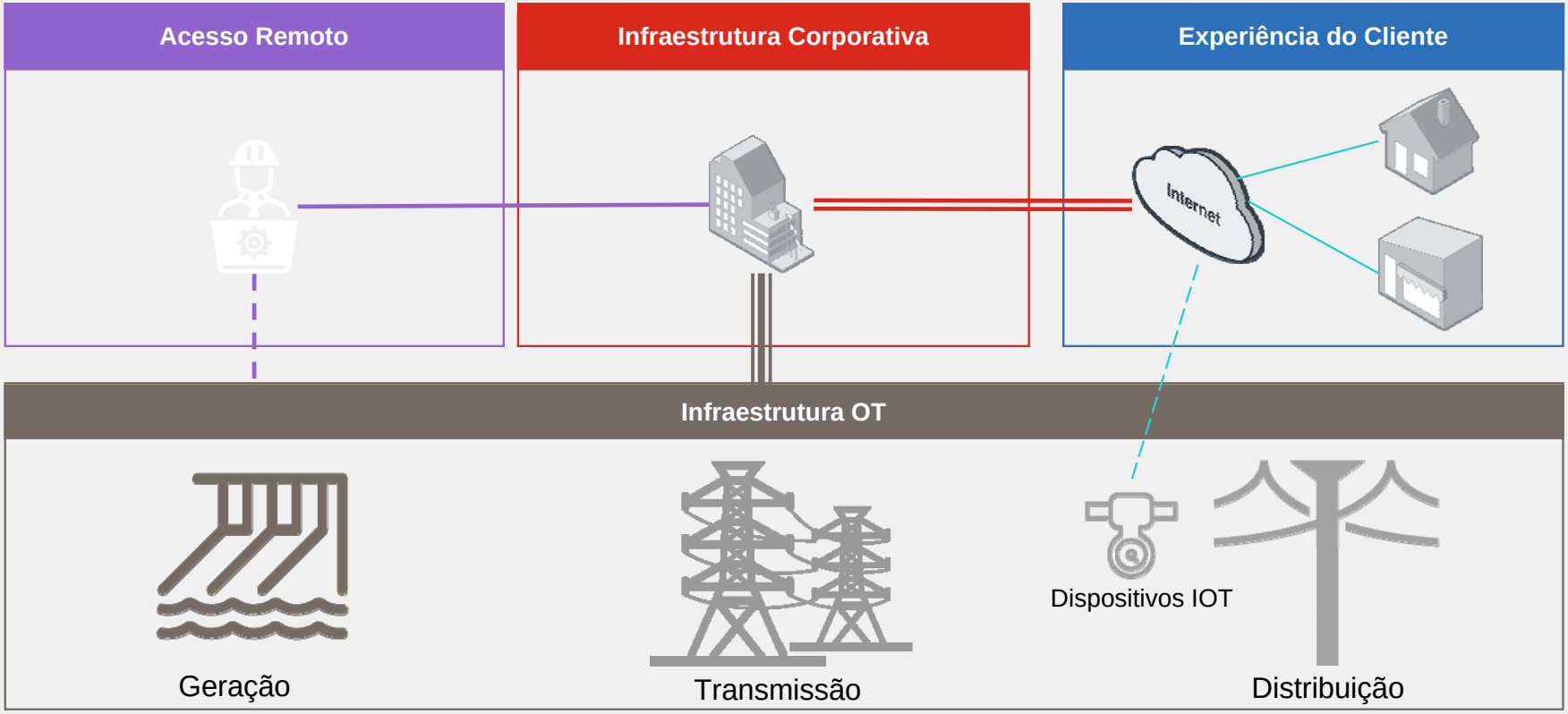
Conformidade atingida

Contudo...

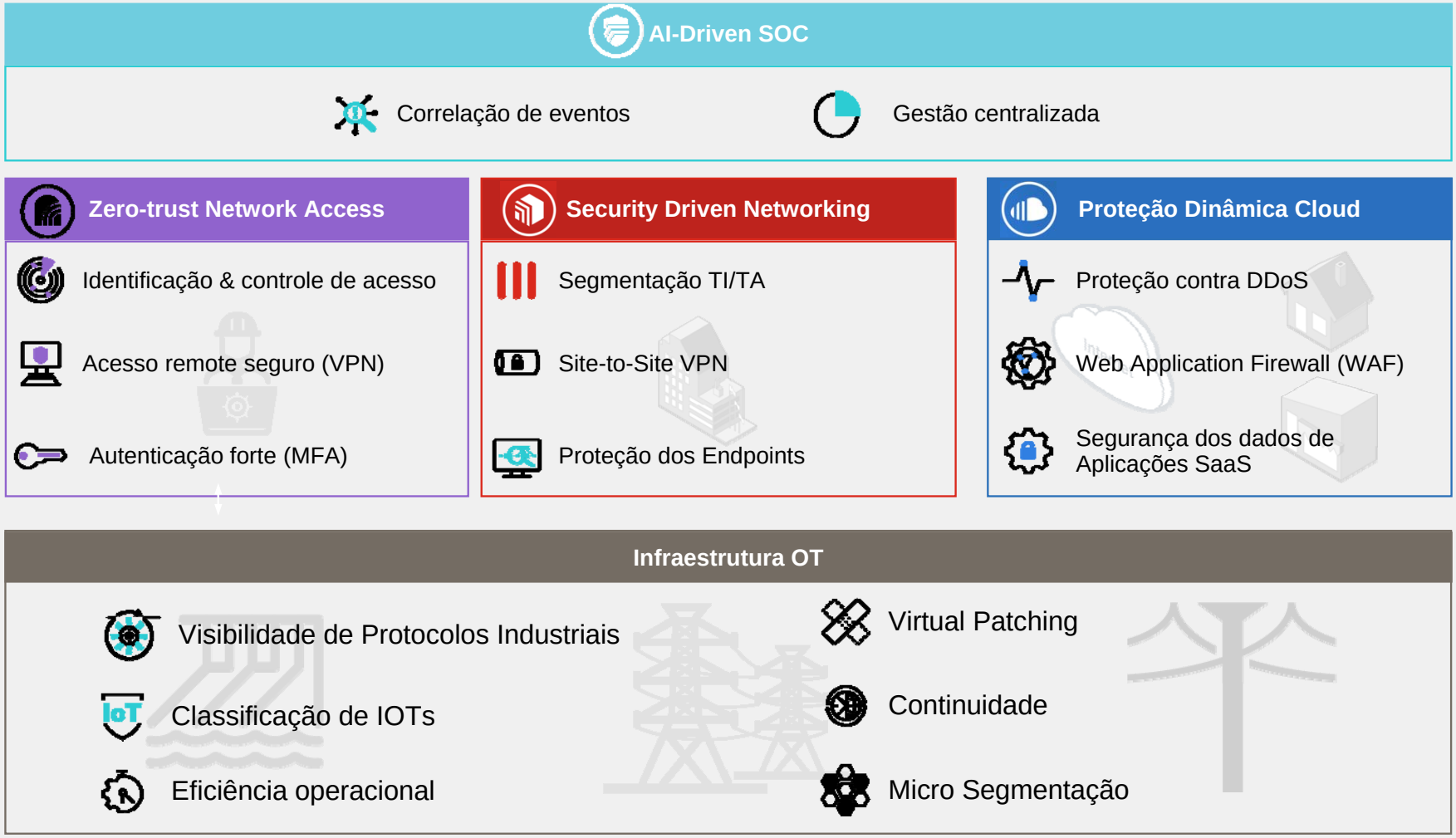
“Conformidade não é segurança” - Geraldo Fonseca (ONS)

Cibersegurança: Pilar para Transformação Digital

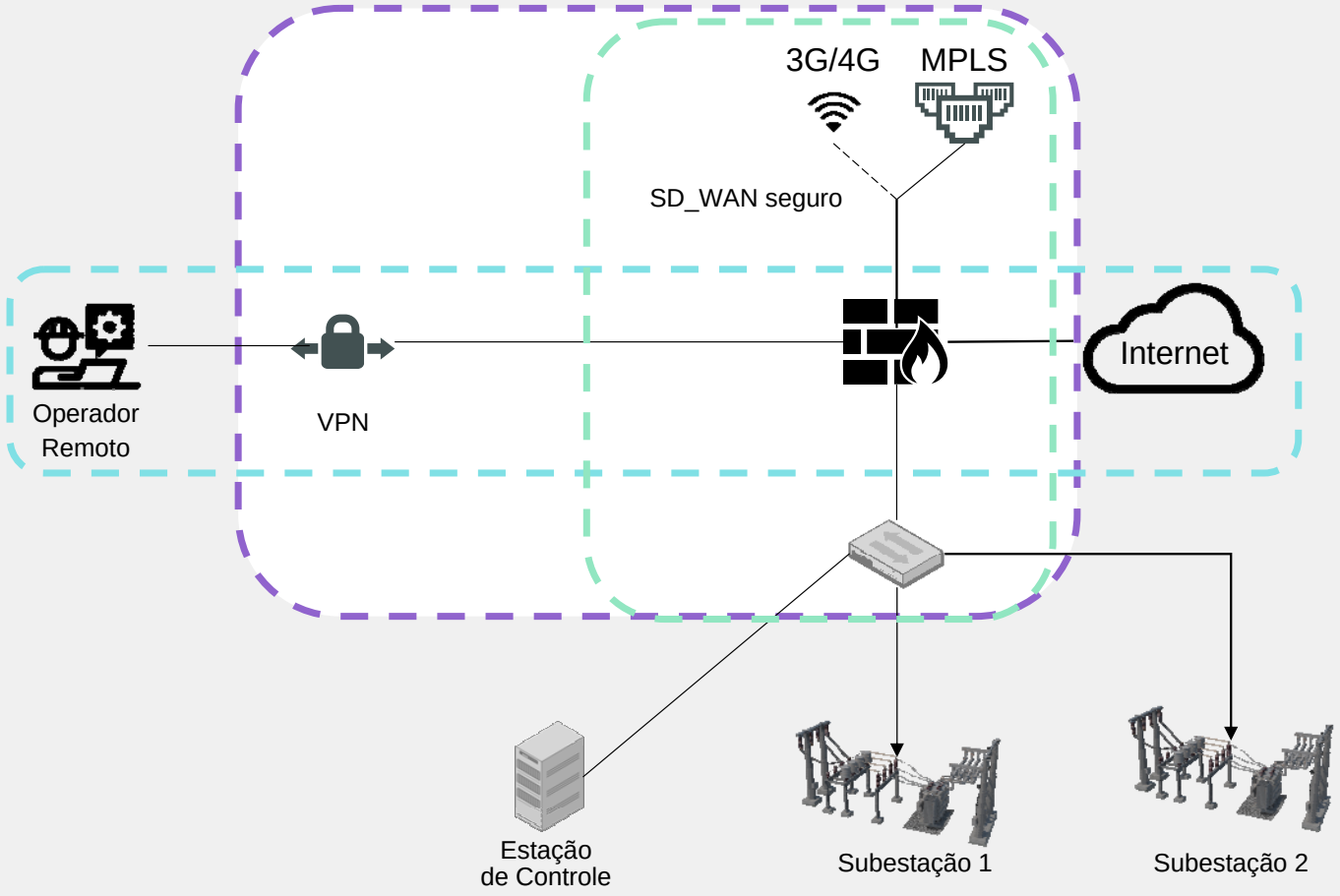
- Maior necessidade de acesso remoto
- Modernização usando dispositivos IoT
- Proliferação de Ransomwares



Proteção Integrada de Todo o Ambiente



Arquitetura Segura:
Segmentação de Rede e SD-WAN Integrados

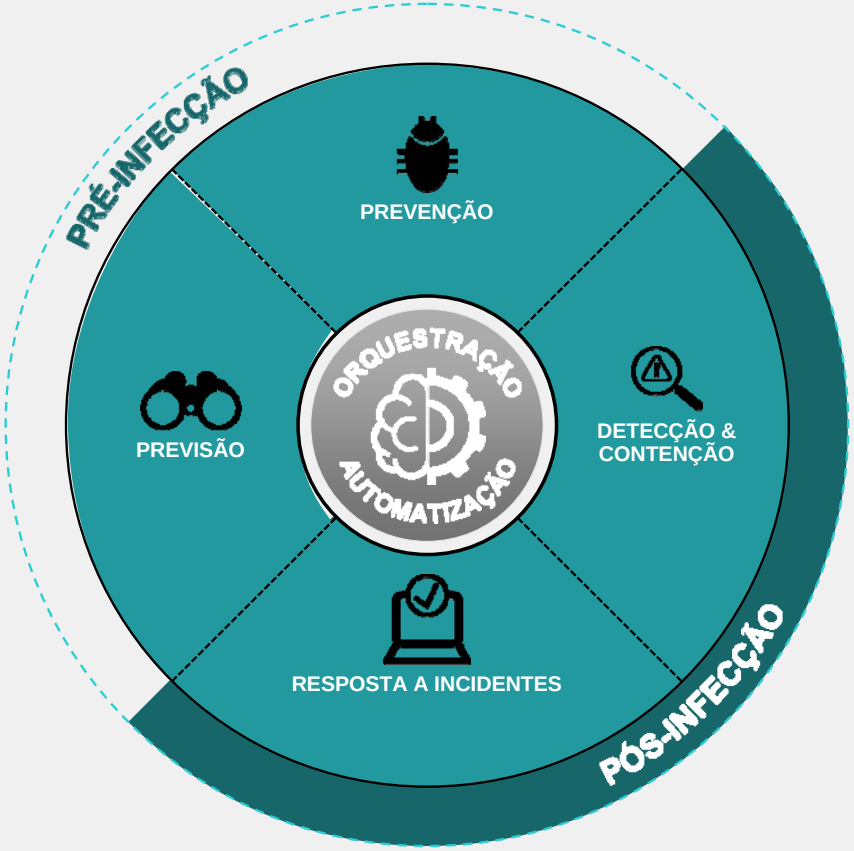


FortiGate
- Todas as funcionalidades em um único equipamento
- Opção Rugged para ambientes industriais

Requisitos ONS	
• Isolamento da Internet (4.1.2) • Terminação VPN (4.1.3)	**Atingido**
• SD-WAN Seguro • Segmentação TI/TA e micro-segmentação • Visibilidade de protocolos industriais	**Superado**

Arquitetura Segura: Proteção de Endpoints

Com políticas de Segurança específicas para o ambiente OT



FortiEDR

- Anti-vírus e EDR na mesma plataforma
- Possibilidade de infraestrutura on-premise
- Suporte a sistemas operacionais legados

Requisitos ONS	
• Solução antimalware (4.1.4)	**Atingido**
• EDR como ferramenta anti-ransomware • Controle de Dispositivos USB	**Superado**

*Pen drive icon by https://www.flaticon.com/

Arquitetura Segura: Gestão de Riscos

Indicadores de Performance e Disponibilidade

Detecção em tempo real de incidentes relacionados a OT

Descoberta de Infraestrutura

FortiSIEM
- Possibilidade de infraestrutura on-premise
- Customizável para atender os casos de uso específicos de OT

Requisitos ONS	
• Inventário de ativos (4.3.1) • Hardening (4.3.3) • Monitoramento e resposta a incidentes (4.6.1 e 4.6.2)	**Atingido**
• Aplicação de IOC para OT • Construção de um CMDB baseado no modelo Purdue	**Superado**

Fortinet: Liderança em Cibersegurança para TA

- Entre em contato conosco: latam_otci@fortinet.com


FORTINET