MARSH

ICS/SCADA cyber threat landscape and best practices

Os ambientes OT/ICS operam plantas industriais, energia, petróleo e gás, mineração, manufatura e infraestrutura crítica. Diferentemente da TI, em OT um incidente pode se traduzir em interrupção física, paralisação produtiva, impacto na segurança e perdas financeiras. Para a Diretoria, o risco OT deve ser gerenciado como uma prioridade de continuidade e resiliência empresarial.

1 OT/ICS protege operações críticas

OT gerencia operações industriais. Um incidente pode interromper a produção, comprometer a segurança e afetar a infraestrutura crítica.

2 A América Latina enfrenta maior exposição

79% das organizações industriais e de infraestrutura crítica na LATAM enfrentam ransomware; apenas 7 dos 32 países possuem planos de proteção.

3 TI, terceiros e acessos remotos são vias de entrada

Mais de 200 initial access brokers tiveram como alvo 17 países da LATAM em 2025. VPNs, fornecedores e acessos remotos são pontos críticos.

4 A falta de visibilidade aumenta o risco

Propriedade fragmentada, ativos não inventariados, sistemas legados, patches irregulares e baixo monitoramento dificultam detectar e responder.

5 Os controles OT devem priorizar resiliência

A SANS recomenda cinco controles críticos: resposta a incidentes, arquitetura defensável, monitoramento, acesso remoto seguro e gestão de vulnerabilidades por risco.