MARSH

Advanced cybersecurity testing with Red Team

A superfície de ataque moderna se expande mais rápido do que a capacidade tradicional de controle. Esta sessão explica por que os testes pontuais já não são suficientes e como um exercício de Red Team simula adversários reais para avaliar prevenção, detecção, resposta e governança. O objetivo executivo não é acumular descobertas, mas obter evidências mensuráveis sobre rotas de ataque, lacunas de controle, tempos de detecção e capacidade de contenção para priorizar investimentos e resiliência.

1 De vulnerabilidades a objetivos críticos

O Red Team valida se um adversário pode alcançar um objetivo de negócio — a joia da coroa — sem ser detectado, combinando identidade, processos, confiança e tecnologia.

2 IA e cadeia de suprimentos ampliam a exposição

A IA acelera reconhecimento, phishing, exploração e evasão. Cadeia de Suprimentos, erros em CI/CD e ataques a modelos aumentam o risco operacional e reputacional.

3 Medir detecção e resposta

O valor está em métricas como MTTD, MTTR/MTTC, fidelidade dos alertas, ruído, escalonamento, execução do playbook e decisões críticas durante o ataque.

4 Evidências para decidir

O exercício entrega attack storyline, logs, indicadores, lacunas priorizadas e roadmap 30/60/90 para transformar o teste técnico em decisões de negócio.

5 Aprender antes do adversário

O Red Team não busca ‘vencer’ o SOC. Busca que a organização identifique rotas viáveis, melhore controles e aprenda antes de um ataque real.