MARSH

Advanced cybersecurity testing with Red Team

La superficie de ataque moderna se expande más rápido que la capacidad tradicional de control. Esta sesión explica por qué las pruebas puntuales ya no son suficientes y cómo un ejercicio de Red Team simula adversarios reales para evaluar prevención, detección, respuesta y gobierno. El objetivo ejecutivo no es acumular hallazgos, sino obtener evidencia medible sobre rutas de ataque, brechas de control, tiempos de detección y capacidad de contención para priorizar inversión y resiliencia.

1 De vulnerabilidades a objetivos críticos

El Red Team valida si un adversario puede alcanzar un objetivo de negocio —la joya de la corona— sin ser detectado, combinando identidad, procesos, confianza y tecnología.

2 IA y cadena de suministro amplían exposición

La IA acelera reconocimiento, phishing, explotación y evasión. Cadena de Suministro, errores en CI/CD y ataques a modelos aumentan el riesgo operativo y reputacional.

3 Medir detección y respuesta

El valor está en métricas como MTTD, MTTR/MTTC, fidelidad de alertas, ruido, escalamiento, ejecución del manual y decisiones críticas durante el ataque.

4 Evidencia para decidir

El ejercicio entrega attack storyline, logs, indicadores, brechas priorizadas y roadmap 30/60/90 para convertir la prueba técnica en decisiones de negocio.

5 Aprender antes que el adversario

Red Team no busca ‘ganarle’ al SOC. Busca que la organización identifique rutas viables, mejore controles y aprenda antes de un ataque real.