MARSH

Cyber Property Damage and Silent Cyber

La IA está acelerando la forma en que se lanzan los ataques, por qué la seguridad reactiva ya no es suficiente, y cómo BAS y CTEM permiten validar controles reales, identificar exposiciones explotables y movilizar remediación antes de que el atacante avance.

1. La IA acelera el ataque. El tiempo de ruptura más rápido observado mediante IA fue de 27 segundos, y los ataques con adversarios habilitados por IA aumentaron 89% en 2025-2026.

2. CTEM conecta diagnóstico y acción. Alcance, descubrimiento, priorización, validación y movilización permiten reducir el tiempo entre detección y resolución con orientación contextual apoyada en IA.

3. BAS valida controles reales. La simulación de brechas y ataques prueba EDR, firewall, SIEM, email, nube y red frente a TTPs reales para responder: ¿este control bloquea este ataque?

4. Identidad es exposición crítica. 5 de las 10 principales tácticas MITRE están basadas en identidad, la ingeniería social y el vishing crecieron 442% entre el primer y segundo semestre de 2024.

5. Métricas para el consejo. La validación continua permite visualizar postura, priorizar vulnerabilidades explotables, automatizar remediación y presentar KPIs de reducción de riesgo a nivel ejecutivo.

Mensaje para la Dirección: no asuma que sus controles funcionan. Exija evidencia continua de efectividad, reducción de exposición y métricas accionables para inversión, resiliencia y reporte al consejo.