MARSH

Cyber Property Damage and Silent Cyber

A IA está acelerando a forma como os ataques são lançados, por que a segurança reativa já não é suficiente e como BAS e CTEM permitem validar controles reais, identificar exposições exploráveis e mobilizar remediação antes que o atacante avance.

1. A IA acelera o ataque. O tempo de comprometimento mais rápido observado com IA foi de 27 segundos, e os ataques com adversários habilitados por IA aumentaram 89% em 2025-2026.

2. CTEM conecta diagnóstico e ação. Escopo, descoberta, priorização, validação e mobilização permitem reduzir o tempo entre detecção e resolução com orientação contextual apoiada por IA.

3. O BAS valida controles reais. A simulação de violações e ataques testa EDR, firewall, SIEM, e-mail, nuvem e rede frente a TTPs reais para responder: este controle bloqueia este ataque?

4. Identidade é exposição crítica. 5 das 10 principais táticas MITRE são baseadas em identidade; a engenharia social e o vishing cresceram 442% entre o primeiro e o segundo semestre de 2024.

5. Métricas para o conselho. A validação contínua permite visualizar a postura, priorizar vulnerabilidades exploráveis, automatizar remediação e apresentar KPIs de redução de risco em nível executivo.

Mensagem para a Diretoria: não presuma que seus controles funcionam. Exija evidências contínuas de efetividade, redução da exposição e métricas acionáveis para investimento, resiliência e reporte ao conselho.