devoteam
Cyber Trust

"QUEREMOS TER ALGO QUE SEJA 360 GRAUS"

NA IT SECURITY CONFERENCE, HERMAN DUARTE, OFFENSIVE SECURITY SERVICES DIRECTOR DA DEVOTEAM CYBER TRUST, EXPLOROU A IMPORTÂNCIA DO RED TEAMING PARA A RESILIÊNCIA ORGANIZACIONAL FACE ÀS CIBERAMEAÇAS.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

A simulação de ciberataques, conhecida como Red Teaming, é uma prática essencial para a preparação e resiliência das organizações face às ameaças atuais. Com origem no contexto militar, envolve a criação de cenários realistas de ataque, onde uma equipa externa (Red Team) simula ações de adversários reais para desafiar e avaliar a defesa da organização, representada pela Blue Team.

Herman Duarte, especialista na área, explicou que o objetivo é um teste holístico de 360 graus, que envolve pessoas, processos e tecnologia, que permite que as organizações se preparem de forma eficaz para um ataque real, testando todas as suas capacidades de resposta.

"A forma mais simples que temos para fazer algo dentro das nossas organizações acaba por ser o Vulnerability Scanning", revelou o especialista. As organizações podem progredir para o Pen Testing e, finalmente, para o Red Teaming, que oferece um realismo maior nos testes, permitindo a identificação eficaz de vulnerabilidades. Essas etapas de maturidade são complementares, formando um "stack" integrado de práticas de segurança.

O Red Teaming simula ataques reais por uma equipa externa que identifica vulnerabilidades, enquanto a Blue Team, interna, defende a organização. As simulações concentram-se em áreas críticas, com táticas realistas baseadas em ameaças conhecidas. "É chave usar os cenários, os TTP, as táticas, as técnicas e os procedimentos que são usados por grupos conhecidos", referiu Duarte. Os resultados são partilhados em relatórios e workshops com a Blue Team, fortalecendo a preparação para ataques reais e ajudando as instituições a cumprir normas de segurança, como o DORA.