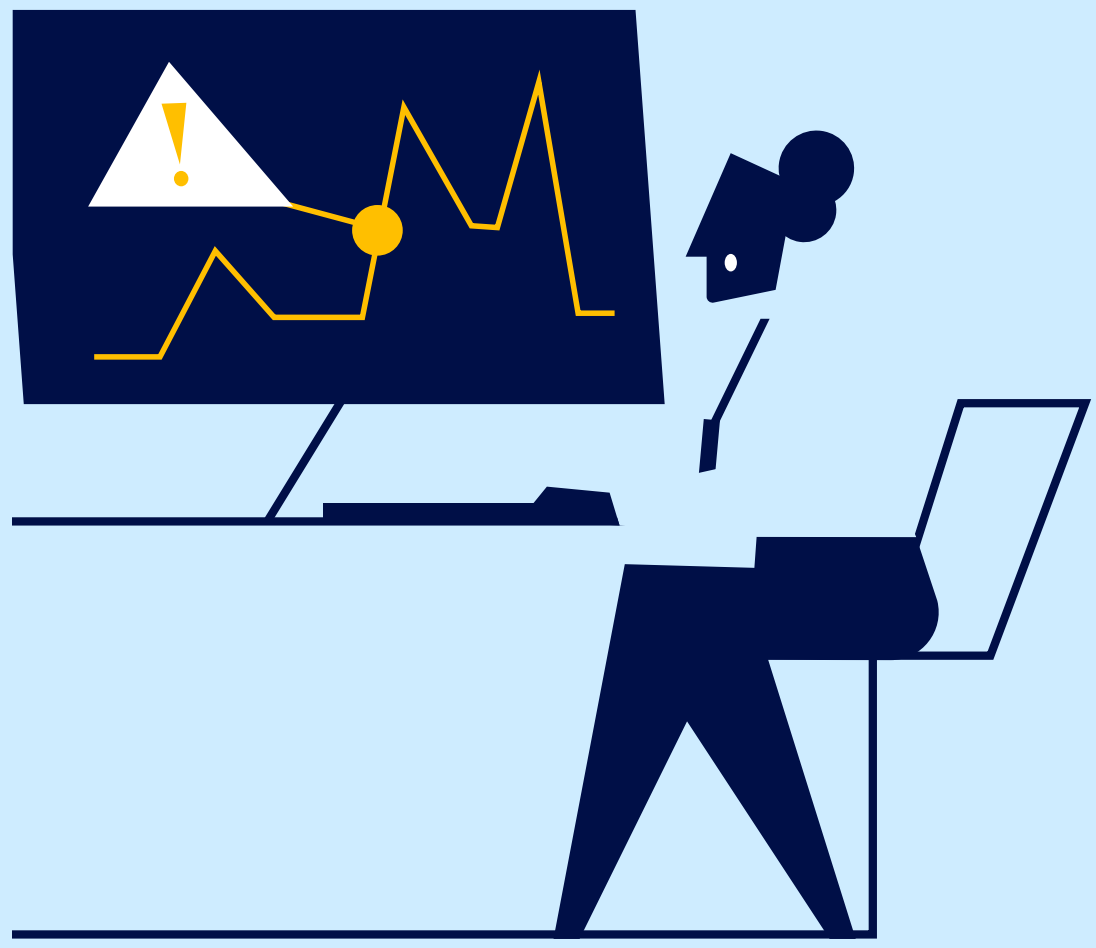
MARSH

# Cyber Securitity Strategy powered by AI

A IA está mudando o equilíbrio entre ataque e defesa. Sua capacidade de acelerar testes, detectar falhas e automatizar ações exige a integração de controles desde o design.



1

A IA amplia a superfície de ataque. Modelos avançados já podem identificar vulnerabilidades reais, automatizar testes e encadear exploits; a inovação deve avançar com controles integrados.

2

A adoção da IA não deve ser medida apenas por eficiência ou velocidade. Para gerar confiança, a alta direção precisa assegurar governança de modelos, proteção de dados, monitoramento de usos não autorizados e uma estratégia de cibersegurança baseada em risco.

3

A IA introduz riscos que nem sempre são gerenciados com controles tradicionais. Proteger dados, modelos, acessos, saídas e níveis de autonomia deve fazer parte da estratégia desde o design.

4

A maturidade deve evoluir. Passar de uma segurança improvisada para uma cibersegurança baseada em risco e dados permite reduzir os tempos de detecção, resposta e recuperação.

5

A IA só gera valor sustentável se for gerenciada com uma estratégia integrada de cibersegurança. Para a alta direção, isso implica visibilidade sobre usos não autorizados, monitoramento de ameaças, controles específicos, testes contínuos e métricas claras de exposição.