Calean Tech

Use IA para se defender da IA

Medidas simples no Entra ID que cortam a maior parte dos ataques de identidade, e como acompanhar tudo todo dia.

A IA deixou o ataque mais barato. Um e-mail de phishing escrito por IA teve 54% de cliques, contra 12% de um e-mail comum, segundo a Microsoft. A boa notícia: as medidas que mais protegem a sua identidade são pequenas.

Por onde o ataque entra

Mais de 97% dos ataques de identidade são tentativas de senha em massa (password spray ou força bruta), segundo o Microsoft Digital Defense Report 2025. No relatório de violações de dados da Verizon de 2025, o uso de credenciais foi a principal porta de entrada, com 22% dos casos.

O alvo é a senha. Então a defesa começa na identidade.

Cinco medidas pequenas

- [ ] **Ligue o MFA para todo mundo.** A autenticação multifator reduz o risco de invasão de conta em 99,22%, segundo um estudo da Microsoft Research.
- [ ] **Bloqueie a autenticação legada.** Mais de 97% dos ataques de credential stuffing e mais de 99% dos ataques de password spray usam protocolos legados, segundo a Microsoft. Com eles bloqueados, esses ataques param.
- [ ] **Tenha poucos administradores.** Conta com privilégio é o alvo preferido. Menos administradores, menos portas.
- [ ] **Use acesso condicional.** Peça mais verificação quando o acesso vem de um lugar estranho ou de um aparelho sem controle.
- [ ] **Acompanhe as mudanças no diretório.** Um administrador novo ou uma regra nova fora de hora merece uma pergunta: isso era esperado?

Fight fire with fire

Combater fogo com fogo: usar a IA a seu favor. Medidas que ninguém acompanha se desfazem com o tempo, e é aí que entra o **onGuard for Entra ID**, da IPC Global.

- Coleta todo dia 37 extratos de identidade, segurança e uso do Entra ID e do Microsoft 365, com permissões só de leitura.
- Avisa sobre mudanças de risco no diretório, com a pergunta “isso era esperado?”.
- Gera relatórios ligados aos controles do CIS Microsoft 365 Foundations Benchmark e do NIST SP 800-53. São avaliações, não certificação nem auditoria.
- Roda na sua conta da AWS. Os dados ficam com você.

Fontes

- Microsoft Digital Defense Report 2025, Microsoft, outubro de 2025.
- How effective is multifactor authentication at deterring cyberattacks?, Microsoft Research, maio de 2023.
- Block legacy authentication with Conditional Access, Microsoft Learn, 2026.
- 2025 Data Breach Investigations Report, Verizon, 2025.