Panorama de **ameaças cibernéticas**

O cenário mudou. Ataques hoje são mais **rápidos, automatizados e orientados** por IA

Segundo a CrowdStrike, a aceleração não acontece por acaso.
O uso de IA por atacantes cresceu 89% em 2025.

Modelo atual de ataque mudou:

- Automação em escala
- Uso de IA para ataques mais rápidos
- Adaptação em tempo real
- Exploração de múltiplas superfícies

Principais vetores de ataque agora são:

- APIs
- Aplicações Web
- Identidade e credenciais de acesso

Os ataques não acontecem mais só **"na infraestrutura"**:
Eles exploram **superfícies expostas** e **identidades válidas.**

1. Aplicações WEB

Principais Ameaças

- Exploração de falhas conhecidas antes da correção de patches
- Manipulação de fluxos da aplicação (burlar login, alterar etapas de checkout, acessar funções indevidas)
- Automação de ataques em formulários e inputs (injeções, testes em massas e exploração contínua de pontos de entrada)

Estratégias de Proteção

- Proteção da aplicação em tempo real (WAAP/WAF)
- Controle de automação e bots
- Análise comportamental e proteção de fluxos

2. APIs

Principais Ameaças

- Abuso de APIs expostas (endpoints acessíveis e exploráveis diretamente)
- Falta de controle de acesso e autenticação (uso indevido de permissões e dados)
- Exploração automatizada de APIs (enumeração, scraping e ausência de rate limiting)

Estratégias de Proteção

- Descoberta e governança de APIs
- Autenticação e controle granular de acesso
- Proteção contra abuso e automação (rate limiting + bots)

3. Identidade e credenciais de acesso

Principais Ameaças

- Comprometimento de credenciais legítimas
- Sessões sequestradas ou reutilizadas (tokens e sessões válidas sendo explorados sem detecção)
- Tentativas automatizadas de acesso (credential stuffing / brute force) (testes em massa com credenciais vazadas)

Estratégias de Proteção

- Autenticação forte e controle de acesso (MFA, menor privilégio)
- Análise comportamental de identidade e uso
- Mitigação de tentativas automatizadas de login

Problema central

O **tempo de resposta humano** não acompanha o ritmo de ataques.

Novo modelo de defesa:

- Proteção contínua de aplicações e APIs
- Detecção baseada em comportamento
- Resposta automatizada
- Gestão contínua de exposição
- Monitoramento Contínuo

Tecnologia isolada não resolve.
Fluxo de defesa integrado e contínuo, sim!

Vamos avaliar juntos o nível de exposição da sua empresa?

Agende uma conversa e veja **onde estão seus principais riscos.**

3STRUCTURE