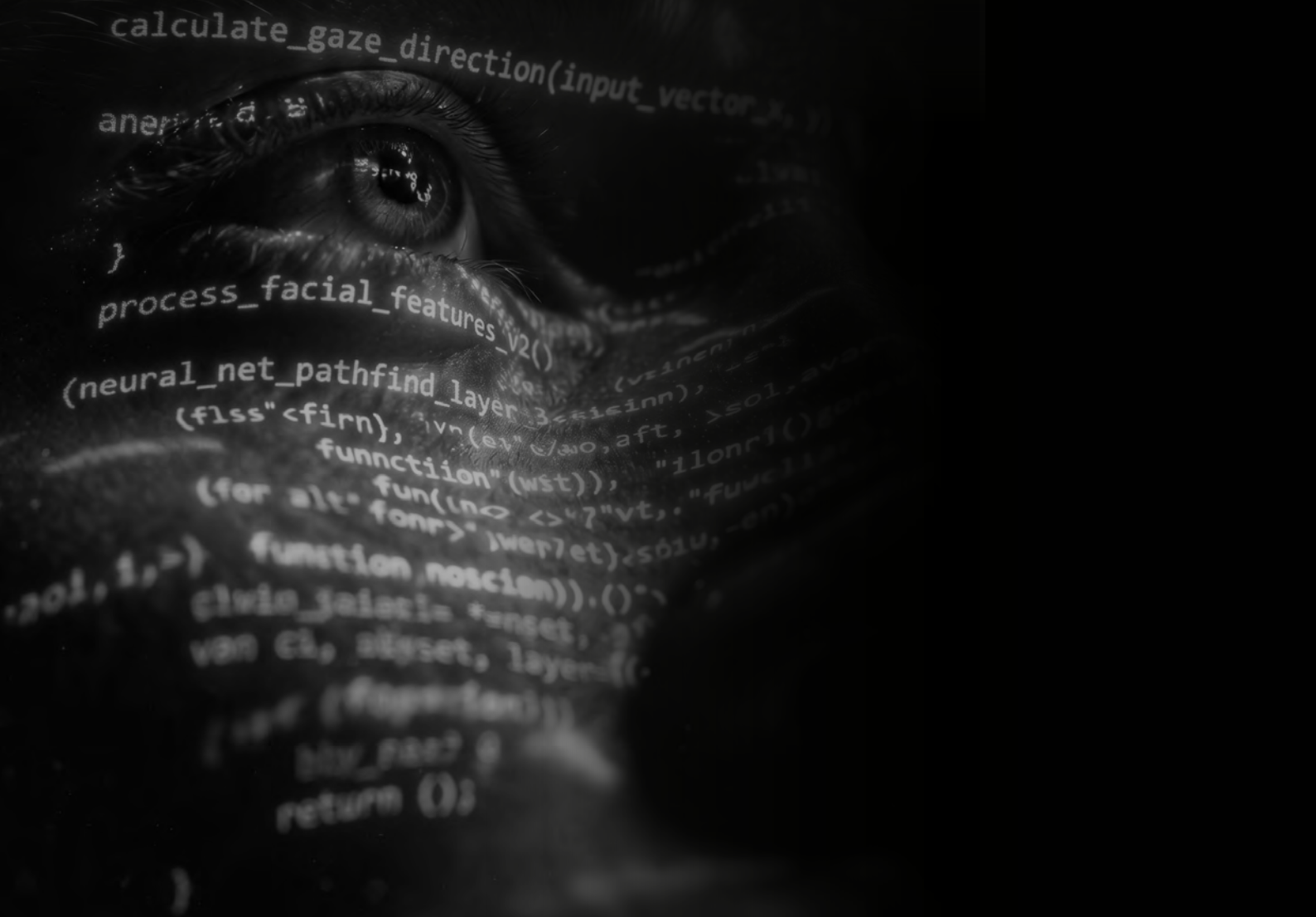
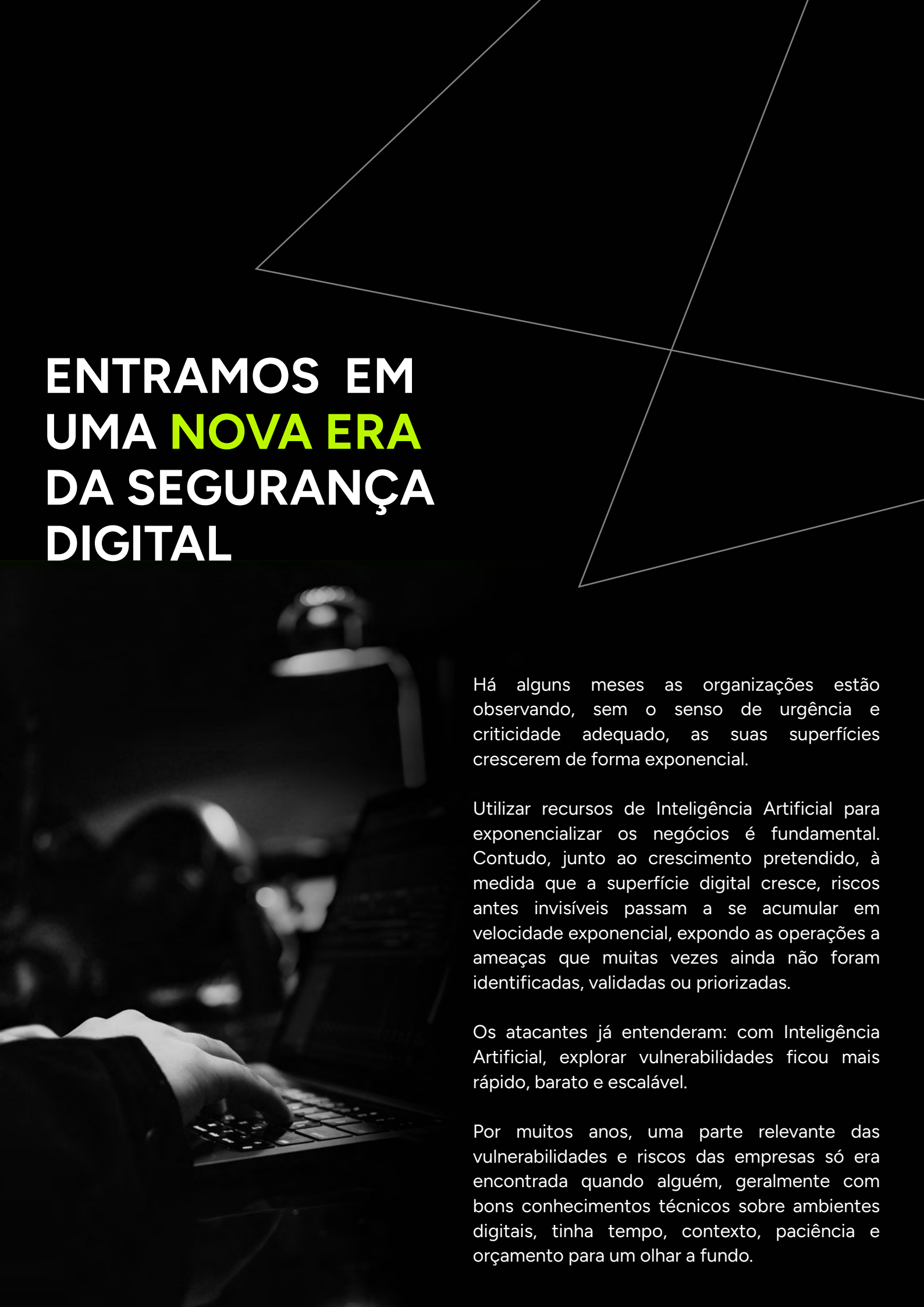


MANIFESTO SOBRE A ERA DOS ATAQUES AUTÔNOMOS





ENTRAMOS EM UMA **NOVA ERA** DA SEGURANÇA DIGITAL

Há alguns meses as organizações estão observando, sem o senso de urgência e criticidade adequado, as suas superfícies crescerem de forma exponencial.

Utilizar recursos de Inteligência Artificial para exponencializar os negócios é fundamental. Contudo, junto ao crescimento pretendido, à medida que a superfície digital cresce, riscos antes invisíveis passam a se acumular em velocidade exponencial, expondo as operações a ameaças que muitas vezes ainda não foram identificadas, validadas ou priorizadas.

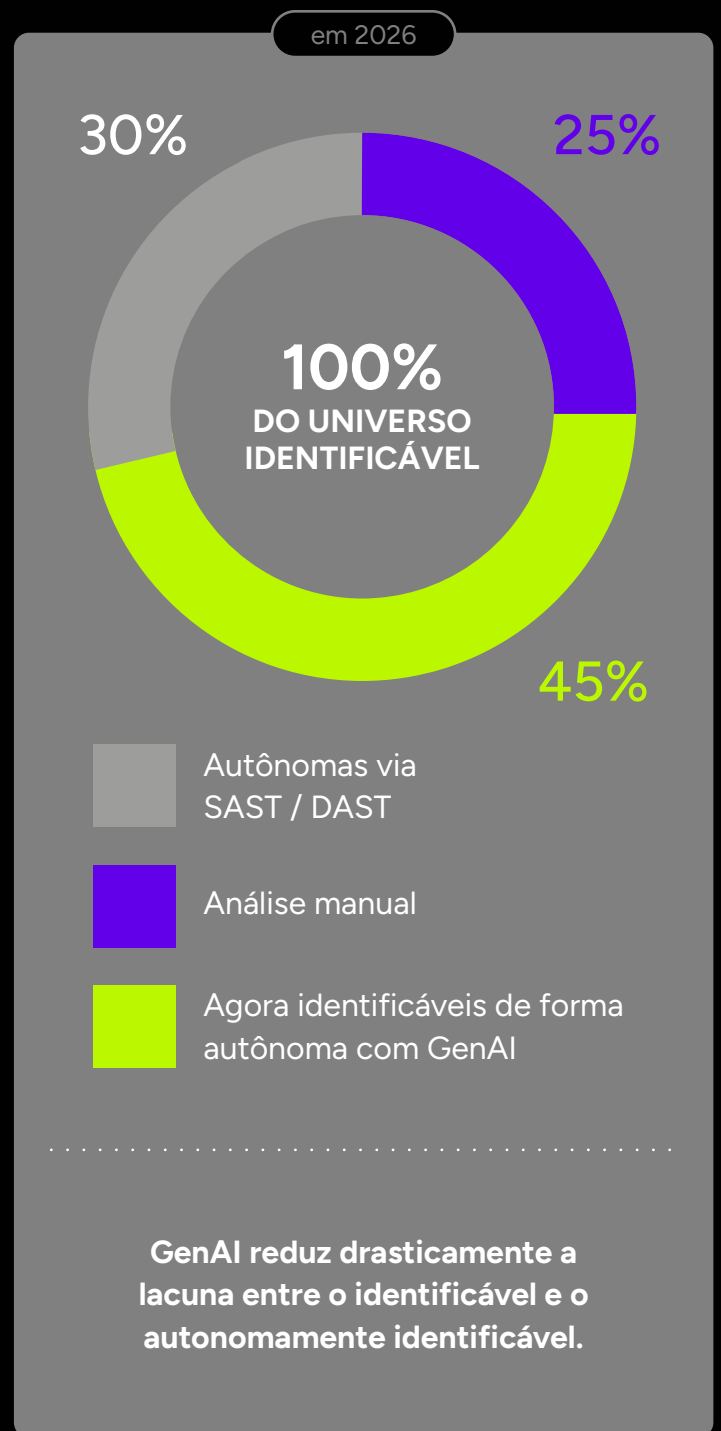
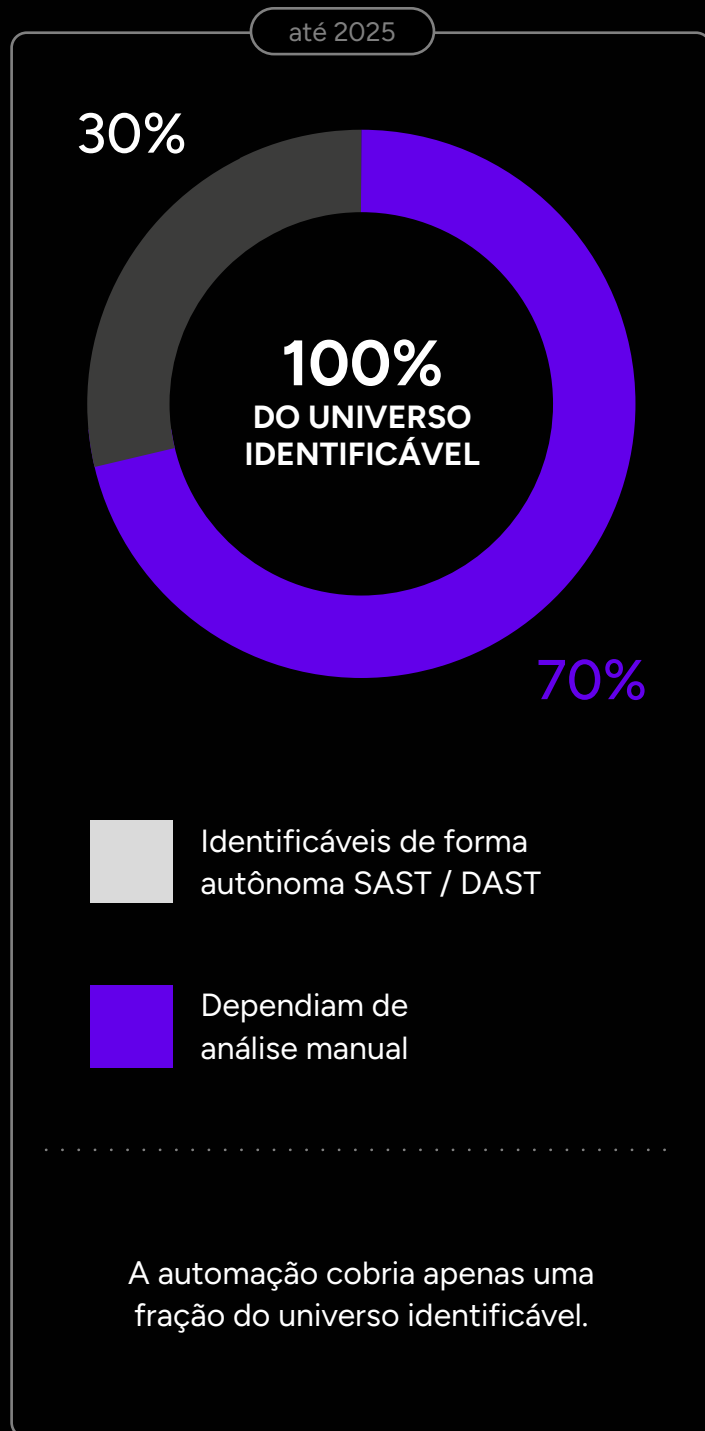
Os atacantes já entenderam: com Inteligência Artificial, explorar vulnerabilidades ficou mais rápido, barato e escalável.

Por muitos anos, uma parte relevante das vulnerabilidades e riscos das empresas só era encontrada quando alguém, geralmente com bons conhecimentos técnicos sobre ambientes digitais, tinha tempo, contexto, paciência e orçamento para um olhar a fundo.

A NOVA ERA DA IDENTIFICAÇÃO AUTÔNOMA DE VULNERABILIDADES

Do universo total de vulnerabilidades identificáveis.

← 2026 AMPLIA A COBERTURA AUTÔNOMA →



Em 2026, a identificação autônoma deixa de se limitar ao SAST/DAST e passa a capturar uma parcela muito maior do universo de vulnerabilidades identificáveis. O espaço que resta para análise 100% manual torna-se significativamente menor.

A IA generativa tornou autônoma uma parte cada vez maior da descoberta ofensiva. O que antes exigia pentest exaustivo, escopo livre e investigação manual agora começa a ser revelado por sistemas capazes de ler aplicações, comparar respostas, testar hipóteses, insistir em fluxos e montar caminhos de ataque exatamente como um adversário avançado.

Isso impacta na maneira como as estratégias de defesa cibernética serão construídas de agora em diante.

A superfície das empresas não ficou necessariamente pior de um dia para o outro. Mas ficou mais visível e exposta do que em toda a história.

Existe uma janela, de curta de adequação, onde a perenidade digital só será alcançada em estratégias onde haja a adoção de três princípios fundamentais:

- Testes autônomos contínuos em substituição de avaliações pontuais e calendários anuais. Premissas: alta capacidade técnica de execução dos testes autônomos e processos robustos visando abrangência dos testes e sucesso nas tratativas.
- Governança contínua da adoção de AI, sobretudo em deployments de software e nas implicações diretas ao aumento de superfície internet-facing.
- Simulação adversarial híbrida, visando descoberta de caminhos reais de ataque mais do que listas isoladas de vulnerabilidades: "Se o adversário é humano usando AI generativa, a simulação é igualmente híbrida". Premissa: adoção de calendários de Red Team Assessments periódicos.

PRINCÍPIOS DO TESTE AUTÔNOMO

Nossa maior prioridade é descobrir, antes do adversário, os caminhos de ataque que já existem na superfície digital da organização. Reconhecemos que 2026 marca uma mudança geracional: vulnerabilidades antes difíceis, caras e demoradas de encontrar agora podem ser reveladas de forma autônoma, repetível e em escala.

O risco não aumenta apenas quando uma nova falha é criada. O risco também aumenta quando uma falha antiga se torna fácil de encontrar.

A segurança não pode mais depender da baixa probabilidade de alguém olhar com profundidade. A GenAI reduziu o custo da atenção ofensiva.

O adversário não precisa mais se apaixonar pelo alvo. Máquinas podem explorar superfícies sem cansaço, sem tédio e sem a limitação econômica do pentest manual tradicional.

Aplicações devem ser testadas como sistemas vivos: com usuários, permissões, fluxos, regras de negócio, APIs, estados, erros, integrações e exceções.

O foco não deve ser encontrar mais tickets, e sim revelar caminhos: da exposição à exploração, da exploração ao impacto, do impacto à correção.

Pensando no novo "pareto do risco cibernético", a nova dinâmica dos testes deve ser #AIFirst + #InternetFacingFirst.

Scanners tradicionais continuam úteis, mas não são suficientes. Num nível mais fundamental da barreira da identificação autônoma, existe a barreira do IoC ou dos plugins, onde padrões estáticos revelados de forma dinâmica pelos ambientes ainda revelam vulnerabilidades importantes a custos ínfimos.

Pentesters e red teamers continuam essenciais, mas seu papel muda. Humanos devem orientar, validar impacto, impor limites e transformar

achados em decisão. Máquinas devem ampliar profundidade, escala e persistência.

A pergunta passou a ser: "O que um adversário utilizando recursos de agentes autônomos encontrará no meu ambiente? Como chegamos até aqui em termos tecnológicos e como devemos adaptar nossos ambientes a esta nova realidade?".

Conselhos, executivos e CISOs devem acompanhar o processo de adequação e acompanhamento de forma simples. Qual a estratégia de testes autônomos? O que está exposto? Como pode ser abusado? Qual seria o impacto? O que precisa ser corrigido primeiro?

A falsa paz do que não aparecia acabou. O que estava escondido por falta de tempo, custo ou paciência tende a aparecer.

Toda organização deve assumir que sua superfície será lida. A única escolha estratégica é se ela será lida primeiro pela defesa ou pelo adversário.

A era em que vulnerabilidades sobreviviam escondidas pelo custo de encontrá-las acabou. A GenAI baixou o preço da descoberta ofensiva.

Toda superfície será atacada.

**A DIFERENÇA
ESTÁ EM
QUEM CHEGA
PRIMEIRO:
VOCÊ OU O
CRIMINOSO.**

VULTUS

SEGURANÇA DE ELITE
COM VISÃO DE NEGÓCIO

