VANTICO

Pentest IA/LLM

LLM é o modelo de aprendizado utilizado por grande parte das ferramentas de Inteligência Artificial Generativa, capaz de analisar e gerar textos complexos em linguagem humana.

Por seu crescente uso e importância para os negócios, essas aplicações têm sido alvo de ataques cibernéticos.

- Injeção de prompt
- Exposição de dados não autorizados
- Roubo de modelo
- Envenenamento de dados no treinamento
- Vulnerabilidades de Supply Chain
- Modelo de negação de serviço

são alguns dos exemplos de vulnerabilidades ligadas ao LLM.

O Pentest é uma das melhores formas de testar essas aplicações, localizando as ameaças existentes que podem ser exploradas por criminosos.

Por meio do **Pentest LLM da Vantico** é possível **identificar:**

- Identificação de vetores de ataques;
- Análise de entradas maliciosas que podem tentar enganar o sistema;
- Testes de injeção de código;
- Análise de falhas na arquitetura;
- E muito mais.

Confira nossas metodologias:

OWASP Top 10 Riscos para LLM	Framework NIST para Gestão de Riscos em Inteligência Artificial

Por que testar com a Vantico?

- Rapidez até 50% maior no início do Pentest
- Transparência em cada etapa, com atualizações em tempo real
- Autonomia para solicitar e gerenciar testes, e visualizar e gerar relatórios
- Escopo flexível, adequado às suas necessidades

Pronto(a) para começar?

Agende uma demo em: www.vantico.com.br

Vantico