

A Cyber Crucible utiliza IA e é um modelo de linguagem de grande porte?

Resposta curta: A Cyber Crucible utiliza IA proprietária — mas apenas durante o desenvolvimento, não no seu endpoint, e não se trata de um modelo de linguagem de grande porte. Sua Genetic AI é uma ferramenta de descoberta em tempo de design que identifica o conjunto determinístico de variáveis comportamentais que indicam um ataque. Essas descobertas se tornam heurísticas fixas e determinísticas em nível de kernel. Em tempo de execução, nenhuma IA, nenhum LLM e nenhum modelo adaptativo é executado no dispositivo.

Por que isso representa uma posição mais forte, não mais fraca

- **Nenhum modelo em tempo de execução significa nenhum desvio (drift).** O comportamento do endpoint é determinístico, repetível e testável — não probabilístico.
- **Nenhuma superfície de inferência ativa.** Não há modelo no dispositivo que um invasor possa manipular ou envenenar.
- **Nenhum dado de cliente em qualquer modelo.** Conteúdo, credenciais e chaves do cliente nunca são usados para treinar, alimentar ou ajustar um modelo, e nenhum dado do cliente sai do endpoint para processamento de IA.

Para um avaliador de instituição financeira ou de setor regulado, essa costuma ser a resposta sobre IA que esperam ouvir: capacidade sem um modelo ativo e opaco tomando decisões no endpoint.

Relacionado

Veja *Como a IA é governada no ciclo de vida de desenvolvimento da Cyber Crucible?* para saber como o trabalho em tempo de design é controlado.