

Cyber Crucible utilise-t-il l'IA, et s'agit-il d'un grand modèle de langage ?

Réponse courte : Cyber Crucible utilise une IA propriétaire — mais uniquement pendant la phase de développement, pas sur votre terminal, et il ne s'agit pas d'un grand modèle de langage. Son IA génétique est un outil de découverte en phase de conception qui identifie l'ensemble déterministe de variables comportementales indiquant une attaque. Ces résultats deviennent des heuristiques fixes et déterministes au niveau du noyau. En exécution, aucune IA, aucun LLM et aucun modèle adaptatif ne s'exécute sur l'appareil.

Pourquoi c'est une position plus forte, et non plus faible

- **Aucun modèle en exécution signifie aucune dérive.** Le comportement du terminal est déterministe, reproductible et testable — et non probabiliste.
- **Aucune surface d'inférence en direct.** Il n'existe aucun modèle sur l'appareil qu'un attaquant pourrait manipuler ou empoisonner.
- **Aucune donnée client dans un quelconque modèle.** Le contenu client, les identifiants et les clés ne sont jamais utilisés pour entraîner, alimenter ou ajuster un modèle, et aucune donnée client ne quitte le terminal pour un traitement par IA.

Pour un évaluateur d'institution financière ou soumis à réglementation, c'est généralement la réponse en matière d'IA qu'il espère entendre : une capacité sans modèle en direct et opaque prenant des décisions sur le terminal.

Sujets connexes

Consultez *Comment la gouvernance de l'IA est-elle assurée dans le cycle de développement de Cyber Crucible ?* pour savoir comment le travail en phase de conception est contrôlé.