

¿Cyber Crucible utiliza IA, y es un modelo de lenguaje grande?

Respuesta breve: Cyber Crucible utiliza IA propietaria — pero únicamente durante el desarrollo, no en su endpoint, y no es un modelo de lenguaje grande. Su Genetic AI es una herramienta de descubrimiento en tiempo de diseño que identifica el conjunto determinista de variables de comportamiento que indican un ataque. Esos hallazgos se convierten en heurísticas fijas y deterministas a nivel de kernel. En tiempo de ejecución, no se ejecuta ninguna IA, ningún LLM ni ningún modelo adaptativo en el dispositivo.

Por qué esto es una posición más sólida, no más débil

- **La ausencia de un modelo en tiempo de ejecución significa que no hay deriva (drift).** El comportamiento del endpoint es determinista, repetible y comprobable, no probabilístico.
- **No existe una superficie de inferencia en vivo.** No hay ningún modelo en el dispositivo que un atacante pueda manipular o envenenar.
- **Ningún dato de cliente forma parte de ningún modelo.** El contenido, las credenciales y las claves del cliente nunca se utilizan para entrenar, alimentar o ajustar un modelo, y ningún dato del cliente sale del endpoint para su procesamiento por IA.

Para un revisor de una institución financiera o de un organismo regulador, esta suele ser la respuesta sobre IA que esperan escuchar: capacidad sin un modelo opaco y en vivo tomando decisiones en el endpoint.

Relacionado

Consulte *¿Cómo se gobierna la IA en el ciclo de vida de desarrollo de Cyber Crucible?* para conocer cómo se controla el trabajo en tiempo de diseño.

Revision #1

Created 2026-07-24 02:02:43 UTC by Dennis Underwood

Updated 2026-07-24 02:02:43 UTC by Dennis Underwood