

¿Cómo se gobierna la IA en el ciclo de vida de desarrollo de Cyber Crucible?

Respuesta breve: Dado que la Genetic AI de Cyber Crucible se utiliza únicamente en el momento del diseño, se rige bajo el ciclo de vida de desarrollo seguro (SDLC) en lugar de como un sistema de producción en vivo. El trabajo de descubrimiento se realiza en un entorno interno controlado, su resultado se valida y se traduce en heurísticas de kernel deterministas, y los controladores resultantes se firman de forma independiente bajo Microsoft WHCP antes de su publicación.

El ciclo de vida gobernado

Fase	Gobernanza
Diseño	Se establecen los requisitos de seguridad; el descubrimiento con IA forma parte de la fase de diseño, bajo el SDLC
Descubrimiento	Genetic AI identifica variables deterministas indicadoras de ataques utilizando únicamente conjuntos de datos de investigación internos
Derivación	Los hallazgos se convierten en heurísticas de kernel fijas y deterministas: no se implementa ningún modelo en vivo
Validación	Los resultados deterministas son repetibles y comprobables; los modelos y controladores se validan mediante control de calidad (QA)
Publicación	Los controladores de Windows se firman bajo WHCP; los cambios siguen una gestión formal del cambio

Datos e integridad

No se utiliza ningún contenido de clientes, credenciales ni claves para entrenar, alimentar o ajustar un modelo. Los modelos son propietarios y se desarrollan internamente, sin dependencia de modelos de terceros. La integridad del modelo se mantiene mediante control de versiones, validación SDLC/QA y firma WHCP; la confidencialidad se mantiene mediante un entorno de desarrollo controlado.

Revision #1

Created 2026-07-24 02:02:51 UTC by Dennis Underwood

Updated 2026-07-24 02:02:51 UTC by Dennis Underwood