

Wie wird KI im Entwicklungslebenszyklus von Cyber Crucible gesteuert?

Kurze Antwort: Da die Genetic AI von Cyber Crucible ausschließlich zur Entwurfszeit eingesetzt wird, unterliegt sie der Governance des sicheren Entwicklungslebenszyklus (SDLC) und nicht der eines produktiv laufenden Systems. Die Discovery-Arbeit erfolgt in einer kontrollierten internen Umgebung, ihre Ergebnisse werden validiert und in deterministische Kernel-Heuristiken übersetzt, und die resultierenden Treiber werden vor der Veröffentlichung unabhängig unter Microsoft WHCP signiert.

Der gesteuerte Lebenszyklus

Phase	Governance
Design	Sicherheitsanforderungen werden festgelegt; die KI-Discovery ist Teil der Design-Phase, im Rahmen des SDLC
Discovery	Genetic AI identifiziert deterministische, angriffsanzeigende Variablen ausschließlich anhand interner Forschungsdatensätze
Ableitung	Erkenntnisse werden zu festen, deterministischen Kernel-Heuristiken — es wird kein live laufendes Modell bereitgestellt
Validierung	Deterministische Ergebnisse sind reproduzierbar und testbar; Modelle und Treiber werden durch QA validiert
Freigabe	Windows-Treiber werden WHCP-signiert; Änderungen folgen einem formalen Change-Management

Daten und Integrität

Es werden keine Kundeninhalte, Zugangsdaten oder Schlüssel verwendet, um ein Modell zu trainieren, zu speisen oder abzustimmen. Die Modelle sind proprietär und werden intern entwickelt, ohne Abhängigkeit von Drittanbieter-Modellen. Die Modellintegrität wird durch Versionskontrolle, SDLC-/QA-Validierung und WHCP-Signierung sichergestellt; die Vertraulichkeit durch eine kontrollierte Entwicklungsumgebung.

Revision #1

Created 2026-07-24 04:51:39 UTC by Dennis Underwood

Updated 2026-07-24 04:51:39 UTC by Dennis Underwood