

How is AI governed in Cyber Crucible's development lifecycle?

Short answer: Because Cyber Crucible's Genetic AI is used only at design time, it is governed under the secure development lifecycle (SDLC) rather than as a live production system. The discovery work happens in a controlled internal environment, its output is validated and translated into deterministic kernel heuristics, and the resulting drivers are independently signed under Microsoft WHCP before release.

The governed lifecycle

Phase	Governance
Design	Security requirements set; AI discovery is part of the design phase, under the SDLC
Discovery	Genetic AI identifies deterministic attack-indicating variables using internal research datasets only
Derivation	Findings become fixed, deterministic kernel heuristics — no live model is deployed
Validation	Deterministic outcomes are repeatable and testable; models and drivers validated through QA
Release	Windows drivers WHCP-signed; changes follow formal change management

Data and integrity

No customer content, credentials, or keys are used to train, feed, or tune a model. Models are proprietary and built in-house, with no third-party model dependency. Model integrity is maintained through version control, SDLC/QA validation, and WHCP signing; confidentiality through a controlled development environment.