

Does Cyber Crucible use AI, and is it a large language model?

Short answer: Cyber Crucible uses proprietary AI — but only during development, not on your endpoint, and it is not a large language model. Its Genetic AI is a design-time discovery tool that identifies the deterministic set of behavioral variables indicating an attack. Those findings become fixed, deterministic kernel-level heuristics. At runtime, no AI, no LLM, and no adaptive model runs on the device.

Why this is a stronger position, not a weaker one

- **No runtime model means no drift.** Endpoint behavior is deterministic, repeatable, and testable — not probabilistic.
- **No live inference surface.** There is no on-device model for an attacker to manipulate or poison.
- **No customer data in any model.** Customer content, credentials, and keys are never used to train, feed, or tune a model, and no customer data leaves the endpoint for AI processing.

For a financial-institution or regulated reviewer, this is usually the AI answer they are hoping to hear: capability without a live, opaque model making decisions on the endpoint.

Related

See *How is AI governed in Cyber Crucible's development lifecycle?* for how the design-time work is controlled.

Revision #2

Created 2026-07-23 15:18:09 UTC by Dennis Underwood

Updated 2026-07-23 18:19:41 UTC by Dennis Underwood