

Does Cyber Crucible embed third-party libraries or foreign code?

Short answer: No. Kernel sensors, drivers, and Genetic AI behavioral models are engineered in-house. No foreign state-sponsored SDKs, unverified third-party libraries, or hidden telemetry hooks are embedded in the software. Windows kernel drivers are submitted for certification under Microsoft's Windows Hardware Compatibility Program (WHCP).

The engineering moat

Building kernel sensors and behavioral models in-house is expensive and slow. Most vendors assemble components instead. That assembly is precisely where supply chain risk enters a security product — the tool with the deepest system privileges is also the one where an unverified dependency does the most damage.

Cyber Crucible's components are proprietary and maintained internally, which removes that class of exposure rather than managing it.

External validation

All Windows kernel drivers undergo internal quality assurance testing and are submitted for certification under Microsoft's Windows Hardware Compatibility Program (WHCP) — independent validation of quality and tamper resistance for code running at the kernel level.

No hidden telemetry

There are no hidden telemetry hooks. What the software collects is documented, and the categories it never collects are explicitly enumerated.

Revision #2

Created 2026-07-21 18:59:41 UTC by Dennis Underwood

Updated 2026-07-21 19:32:51 UTC by Dennis Underwood