What independent security validation does Cyber Crucible have?

Short answer: Cyber Crucible's Windows kernel drivers are objectively tested and cryptographically signed under Microsoft's Windows Hardware Compatibility Program (WHCP). That is an external, independent attestation of the quality and tamper-resistance of the product's most privileged component — the code where correctness matters most.

Why WHCP is meaningful

Most of the endpoint market avoided kernel-level development because it is genuinely difficult and expensive. Cyber Crucible operates at the kernel deliberately, and submits its drivers to Microsoft's program so that an outside party — not just Cyber Crucible — validates that the most sensitive code is correct and resistant to tampering.

- The validation is **scoped precisely to the driver**, not represented as a whole-product certification.
- It is an objective, repeatable test rather than a subjective administrative audit.

How it fits the bigger picture

For a reviewer used to looking for a SOC 2 report, WHCP is a concrete, independent data point that a SOC 2 does not provide: direct validation of the kernel component. It complements — rather than replaces — the control evidence in Cyber Crucible's prepared vendor package.

Revision #2
Created 2026-07-23 15:18:06 UTC by Dennis Underwood
Updated 2026-07-23 18:19:37 UTC by Dennis Underwood