What does it mean that Cyber Crucible is independent of Windows libraries?

Short answer: Cyber Crucible does not rely on the Windows system libraries it is protecting. It was deliberately decoupled from them, so that when attackers compromise, crash, or hijack those libraries, Cyber Crucible keeps running, keeps enforcing, and keeps reporting.

Why this was built

In the second half of 2025, attackers shifted to infecting core Windows libraries in memory. Because nearly every security vendor depends on those same libraries to function, that single move rendered a large portion of the market blind.

Cyber Crucible spent roughly nine months inventing novel sensors and a further five-month engineering effort to remove Windows library dependencies entirely — including eliminating volatile MiniFilter dependencies.

What it looks like architecturally

The architecture runs seven fully independent subsystems inside the kernel, including its own isolated encryption, networking, metadata analysis, and event tracking. A further phase of this work replaces the standard Windows networking library (`ws32_2.dll`) with a custom kernel-level network stack.

Proven in the field

With two customers, attackers blocked by the kernel-only decision engine then tried to prevent the customer from being notified by attacking the OS networking layer. Because Cyber Crucible's network communications are independent of the operating system, protection held and the intelligence still reached the customer.

Revision #3
Created 2026-07-20 19:23:53 UTC by Dennis Underwood
Updated 2026-07-21 19:32:09 UTC by Dennis Underwood