How does Cyber Crucible support government and high-security environments?

Short answer: Through complete data sovereignty — fully on-premises installation in physically secured racks, air-gapped operation, and multi-tenant architecture — with no public cloud, no third-party SOC, and no data sharing.

Sovereignty by architecture

For organizations requiring absolute control, nothing needs to leave the environment. There are no third-party platforms in the path, no external access, and no vendor-hosted analysis of your data.

This matters because many vendors upload sensitive identity data — private keys, session tokens — to their hosted SOC teams. That centralized storage is a single point of failure and a high-value target for state-sponsored attackers, and it can be reached through legal compulsion without your knowledge.

Quiet by default

Threats are neutralized silently at the kernel level. Only you know an attack was attempted, and if no data was touched there are typically no external alerts or required disclosures.

Multi-tenant

The architecture supports multi-tenant deployments, which suits managing multiple departments or agencies from a single secure on-premises instance.

Revision #3
Created 2026-07-20 19:24:12 UTC by Dennis Underwood
Updated 2026-07-21 19:32:27 UTC by Dennis Underwood