

Does Cyber Crucible have a patch management program?

Short answer: Yes. A risk-based patch and vulnerability-management program keeps software, kernel drivers, servers, and endpoints current, and findings are tracked to resolution.

How it works

Continuous automated security testing runs within the development pipeline, risk-based manual penetration testing is performed with an annual floor, and event-triggered testing runs on every significant change, covering both internal and external networks. Security patches and hot-fixes are applied per vendor recommendation, and owner groups are responsible for staying current on applicable patches. Removable and portable media are held to the same protection and scanning as fixed media.

Prioritization and deployment

Findings are prioritized by severity and exploitability, with actively exploited vulnerabilities handled through an expedited, out-of-band path. Patches follow the change-management process — validated before promotion to production — and kernel-driver updates are re-validated through Microsoft WHCP before release.

Framework alignment and the honest boundary

The program aligns to NIST SP 800-40, NIST SP 800-53 (SI-2, RA-5), CIS Control 7, and ISO/IEC 27001:2022 A.8.8. No certification is claimed. Specific target remediation windows and remediation evidence are provided to reviewers under NDA.

Revision #1

Created 2026-07-24 23:08:41 UTC by Dennis Underwood

Updated 2026-07-24 23:08:41 UTC by Dennis Underwood