Verfügt Cyber Crucible über einen Change-Management-Prozess?

Kurze Antwort: Ja. Produktionsänderungen folgen einem dokumentierten Change-Management-Prozess mit Überprüfung, Tests und Freigabe. Da das Produkt auf Kernel-Ebene arbeitet, wird Änderungsdisziplin als Sicherheitskontrolle behandelt und nicht lediglich als technische Praxis.

Was der Prozess abdeckt

Änderungen an Anwendungscode, Kernel-Treibern, Serverkonfigurationen und unterstützender Infrastruktur durchlaufen definierte Lebenszyklusphasen: Sicherheitsanforderungen werden bereits im Design festgelegt; der Quellcode wird versionskontrolliert verwaltet, und Geheimnisse werden niemals im Klartext eingebettet; automatisierte Tests validieren Änderungen vor der Freigabe; und Produktionsänderungen erhalten eine formelle Überprüfung und Genehmigung. Die Aufgabentrennung wird eingehalten, sodass der Urheber einer Änderung nicht deren alleiniger Genehmiger ist. Server-Baselines folgen genehmigten Konfigurationsrichtlinien, und nicht benötigte Dienste werden nach Möglichkeit deaktiviert.

Notfalländerungen und Treiberänderungen

Notfalländerungen nutzen einen beschleunigten Pfad, der dennoch eine Autorisierung, gezielte Tests und eine Überprüfung nach der Umsetzung erfordert. Windows-Kernel-Treiber durchlaufen eine interne Qualitätssicherung und werden vor der Veröffentlichung zur Zertifizierung im Rahmen des Windows Hardware Compatibility Program (WHCP) von Microsoft eingereicht – eine unabhängige, externe Prüfung der am höchsten privilegierten Komponente.

Abgleich mit Rahmenwerken und die ehrliche Grenze

Der Prozess orientiert sich an NIST SP 800-53 (CM-Familie) und ISO/IEC 27001:2022 A.8.32. Cyber Crucible beansprucht keine Zertifizierung. Das detaillierte Change-Management-Verfahren sowie

unterstützende Nachweise werden Prüfern unter NDA zur Verfügung gestellt.

Revision #1
Created 2026-07-24 23:30:05 UTC by Dennis Underwood
Updated 2026-07-24 23:30:05 UTC by Dennis Underwood