Erfüllt Cyber Crucible die CMMC- und DFARS-Anforderungen für die Defense Industrial Base?

Kurze Antwort: Cyber Crucible ist nicht CMMC-zertifiziert, und das wird auch klar so kommuniziert. Es unterstützt die Verpflichtungen eines Defense-Auftragnehmers gemäß DFARS 252.204-7012 und CMMC in erster Linie dadurch, dass keine Controlled Unclassified Information (CUI) erfasst werden und dass eine On-Premises- oder Air-Gapped-Bereitstellung innerhalb der eigenen Grenzen des Auftragnehmers unterstützt wird, wo CUI unter der Kontrolle des Auftragnehmers verbleibt.

Wie die Verpflichtungen des Auftragnehmers unterstützt werden

- **Keine Erfassung von CUI.** Der Endpoint-Agent analysiert Verhalten lokal, ohne die geschützten Dateien zu extrahieren, sodass CUI nicht an Cyber Crucible übertragen wird.
- **Grenzwahrende Bereitstellung.** On-Premises- und Air-Gapped-Modelle halten alle Daten innerhalb der geprüften Grenzen des Auftragnehmers.
- **Endpoint-Schutzkontrollen.** Malware-/Ransomware-Prävention und Überwachung entsprechen den relevanten CMMC-Praktiken und NIST-SP-800-171-Kontrollen, die der Auftragnehmer umsetzen muss.
- **US-Lieferkette.** US-Daten werden von in den USA ansässigen Ressourcen verarbeitet; Offshore-Auftragnehmer verarbeiten keine US-Daten und entwickeln auch nicht die Agenten. Die Software unterliegt der EAR-Kontrolle, nicht der ITAR.

Die ehrliche Grenze

Die CMMC-Zertifizierung wird von der Umgebung des Auftragnehmers gehalten, nicht von einem einzelnen Sicherheitstool; Cyber Crucible ist eine Kontrolle, die mehrere 800-171-Anforderungen unterstützt, kein Ersatz für die Bewertung des Auftragnehmers. Detaillierte Zuordnungen sind unter NDA verfügbar.

Revision #1
Created 2026-07-24 04:53:39 UTC by Dennis Underwood
Updated 2026-07-24 04:53:39 UTC by Dennis Underwood