¿Cumple Cyber Crucible con los requisitos de CMMC y DFARS para la base industrial de defensa?

Respuesta breve: Cyber Crucible no cuenta con certificación CMMC, y lo indica claramente. Respalda las obligaciones de un contratista de defensa bajo DFARS 252.204-7012 y CMMC principalmente al no recopilar Información No Clasificada Controlada (CUI) y al admitir implementaciones locales (on-premises) o aisladas de la red (air-gapped) dentro del perímetro propio del contratista, donde la CUI permanece bajo el control del contratista.

Cómo respalda las obligaciones del contratista

- **No se recopila CUI.** El agente de endpoint analiza el comportamiento de forma local sin extraer los archivos que protege, por lo que la CUI no se transfiere a Cyber Crucible.
- **Implementación que preserva el perímetro.** Los modelos on-premises y air-gapped mantienen todos los datos dentro del perímetro evaluado del contratista.
- **Controles de protección de endpoints.** La prevención y el monitoreo de malware/ransomware se corresponden con las prácticas CMMC pertinentes y los controles de NIST SP 800-171 que el contratista debe implementar.
- **Cadena de suministro estadounidense.** Los datos estadounidenses son gestionados por recursos con sede en EE. UU.; los contratistas externos (offshore) no manejan datos de EE. UU. ni desarrollan los agentes. El software está controlado por EAR, no por ITAR.

El límite honesto

La certificación CMMC la posee el entorno del contratista, no una herramienta de seguridad individual; Cyber Crucible es un control que respalda varios requisitos de 800-171, no un sustituto de la evaluación del contratista. El detalle de la correspondencia (mapping) está disponible bajo NDA.

Revision #1
Created 2026-07-24 02:04:34 UTC by Dennis Underwood

Updated 2026-07-24 02:04:34 UTC by Dennis Underwood