Como apoia a Cyber Crucible o cumprimento dos requisitos do CMMC e do DFARS para a base industrial de defesa?

Resposta curta: A Cyber Crucible não possui certificação CMMC, e afirma isso claramente. Ela apoia as obrigações de um contratante de defesa nos termos do DFARS 252.204-7012 e do CMMC principalmente por não coletar Informações Não Classificadas Controladas (CUI) e por oferecer suporte à implantação local (on-premises) ou em ambiente isolado (air-gapped) dentro do próprio perímetro do contratante, onde as CUI permanecem sob o controle do contratante.

Saiba mais: proteção contra ransomware em ambiente isolado (air-gapped) para fornecedores da defesa

Como isso apoia as obrigações do contratante

- **Nenhuma CUI coletada.** O agente de endpoint analisa o comportamento localmente sem extrair os arquivos que protege, de modo que as CUI não são transferidas para a Cyber Crucible.
- **Implantação que preserva o perímetro.** Os modelos on-premises e air-gapped mantêm todos os dados dentro do perímetro avaliado do contratante.
- **Controles de proteção de endpoint.** A prevenção e o monitoramento de malware/ransomware correspondem às práticas relevantes do CMMC e aos controles do NIST SP 800-171 que o contratante deve implementar.
- **Cadeia de suprimentos dos EUA.** Os dados dos EUA são tratados por recursos baseados nos EUA; contratados offshore não lidam com dados dos EUA nem desenvolvem os agentes. O software é controlado pelo EAR, não pelo ITAR.

O limite honesto

A certificação CMMC é detida pelo ambiente do contratante, não por uma ferramenta de segurança individual; a Cyber Crucible é um controle que apoia diversos requisitos do 800-171, não um

substituto para a avaliação do contratante. Detalhes de mapeamento estão disponíveis sob NDA.

Revision #3
Created 2026-07-24 06:03:17 UTC by Dennis Underwood
Updated 2026-11-24 15:49:39 UTC by Dennis Underwood