??? ???? Cyber Crucible ??????? CMMC ?DFARS ?????? ???????? ???????? ?????????

الإجابة المختصرة: إن Cyber Crucible غير حاصلة على شهادة CMMC، وهي تعلن ذلك بوضوح. وهي تدعم التزامات المقاول الدفاعي بموجب DFARS 252.204-7012 وCMMC بشكل أساسي من خلال عدم جمع المعلومات غير المصنّفة الخاضعة للرقابة (CUI)، ومن خلال دعم النشر داخل المنشأة أو في بيئة معزولة (air-gapped) ضمن حدود المقاول نفسه، حيث تبقى CUI تحت سيطرة المقاول.

لمعرفة المزيد: [حماية المتعاقدين في قطاع الدفاع من برامج الفدية في البيئات المعزولة عن الشبكة]

??? ???? ???????? ???????

- **عدم جمع CUI.** يقوم عميل نقطة النهاية بتحليل السلوك محلياً دون استخراج الملفات التي يحميها، وبالتالي لا يتم نقل CUI إلى Cyber Crucible.
- **نشر يحافظ على الحدود.** تحافظ نماذج النشر داخل المنشأة والمعزولة (air-gapped) على بقاء جميع البيانات ضمن الحدود التي تم تقييمها للمقاول.
- **ضوابط حماية نقاط النهاية.** تتوافق آليات منع البرمجيات الخبيثة/برمجيات الفدية والمرافقة مع ممارسات CMMC ذات الصلة وضوابط NIST SP 800-171 التي يجب على المقاول تطبيقها.
- **سلسلة توريد أمريكية.** تتم معالجة البيانات الأمريكية بواسطة موارد مقرها الولايات المتحدة؛ والا يتعامل المقاولون من الخارج مع البيانات الأمريكية والا يطورون العملاء (agents). البرنامج خاضع لضوابط EAR، وليس ITAR.

?????? ???????

إن شهادة CMMC تُمنح لبيئة المقاول، وليس لأداة أمنية فردية؛ Cyber Crucible هي ضابط يدعم عدة متطلبات من NIST SP 800-171، وليست بديلاً عن تقييم المقاول. تتوفر تفاصيل المطابقة بموجب اتفاقية عدم إفصاح (NDA).

Revision #3
Created 2026-07-24 03:32:17 UTC by Dennis Underwood
Updated 2026-11-24 15:41:52 UTC by Dennis Underwood