Comment Cyber Crucible sert-il les environnements des forces de l'ordre et CJIS ?

Réponse courte : Cyber Crucible convient aux environnements Criminal Justice Information Services (CJIS) car il traite les données localement, ne collecte jamais d'informations de justice pénale (CJI), et peut fonctionner sur site ou en environnement isolé (air-gapped) à l'intérieur du périmètre de l'agence. Les données américaines sont traitées par du personnel basé aux États-Unis, ce qui répond aux exigences de la CJIS Security Policy en matière de personnel et de traitement des données.

Pourquoi l'architecture convient

- **Les CJI restent dans le périmètre.** Aucun contenu client n'est collecté ; l'analyse s'effectue sur le point de terminaison (endpoint), de sorte que les CJI ne sont pas transférées vers un cloud tiers.
- **Du personnel américain pour les données américaines.** Les sous-traitants offshore ne traitent pas les données américaines et ne développent pas les agents.
- **Chiffrement et contrôle d'accès.** Une authentification forte, un contrôle d'accès basé sur les rôles et le chiffrement répondent aux contrôles techniques de la politique.

La limite en toute transparence

La CJIS Security Policy est appliquée par l'agence et son CJIS Systems Agency d'État ; Cyber Crucible prend en charge plusieurs de ses domaines de contrôle mais ne constitue pas en soi une « certification » CJIS. Les détails relatifs à la vérification du personnel et aux contrôles sont disponibles sous accord de confidentialité (NDA).

Revision #1
Created 2026-07-24 07:15:23 UTC by Dennis Underwood
Updated 2026-07-24 07:15:23 UTC by Dennis Underwood