

¿Cómo presta servicio Cyber Crucible a entornos de fuerzas del orden y CJIS?

Respuesta breve: Cyber Crucible se adapta a los entornos de Criminal Justice Information Services (CJIS) porque procesa los datos de forma local, nunca recopila información de justicia penal (CJI, por sus siglas en inglés) y puede ejecutarse en las instalaciones o de forma aislada (air-gapped) dentro del perímetro de la agencia. Los datos de EE. UU. son gestionados por personal ubicado en EE. UU., lo cual respalda las expectativas de la CJIS Security Policy en materia de personal y manejo de datos.

Por qué la arquitectura se adapta

- **La CJI permanece dentro del perímetro.** No se recopila contenido del cliente; el análisis se realiza en el endpoint, por lo que la CJI no se transfiere a una nube de terceros.
- **Personal de EE. UU. para datos de EE. UU.** Los contratistas externos ubicados fuera del país no manejan datos de EE. UU. ni desarrollan los agentes.
- **Cifrado y control de acceso.** La autenticación robusta, el control de acceso basado en roles y el cifrado respaldan los controles técnicos de la política.

El límite honesto

La CJIS Security Policy es aplicada por la agencia y su CJIS Systems Agency estatal correspondiente; Cyber Crucible respalda varias de sus áreas de control, pero en sí misma no constituye una "certificación" CJIS. Los detalles sobre la verificación de antecedentes del personal y los controles están disponibles bajo acuerdo de confidencialidad (NDA).

Revision #1

Created 2026-07-24 02:05:05 UTC by Dennis Underwood

Updated 2026-07-24 02:05:05 UTC by Dennis Underwood