¿Cómo le ayuda Cyber Crucible a proteger la privacidad de los datos del alumnado en centros escolares y universidades?

Respuesta breve: Cyber Crucible ayuda a las instituciones educativas de dos maneras: detiene el ransomware de forma autónoma sin necesidad de un centro de operaciones de seguridad (SOC) 24/7, y — a través de FortressAI — evalúa el acceso a datos de herramientas de IA en el dispositivo para que los registros estudiantiles y los datos familiares no lleguen accidentalmente a un sistema de IA público. Dado que el análisis es local y no se recopilan registros estudiantiles, los registros educativos protegidos permanecen dentro del perímetro de la institución.

Más información: protección contra ransomware para escuelas y universidades

Los dos problemas educativos que aborda

- **Ransomware sin un SOC.** La prevención a nivel de kernel detiene los ataques en menos de 200 milisegundos, sin necesidad de contratar analistas ni financiar un contrato de monitoreo ininterrumpido.
- **Gobernanza de IA para el aula.** FortressAI impide, conforme a la política que se aplica en el propio dispositivo, que los registros educativos protegidos y los datos personales de las familias lleguen a herramientas de IA y LLM, de modo que no se envíen a ningún sistema de IA público, ni siquiera como datos de entrenamiento.

Notas para la selección de proveedores

- Cyber Crucible trabaja bajo la dirección de la institución y no utiliza los datos del alumnado para ningún fin secundario.
- Las leyes estatales de privacidad estudiantil (por ejemplo, en California, Nueva York y Colorado) añaden obligaciones adicionales para los proveedores; el diseño de procesamiento local y de no recopilación respalda su cumplimiento. La documentación está disponible bajo acuerdo de confidencialidad (NDA).

Revision #3
Created 2026-07-24 02:04:15 UTC by Dennis Underwood
Updated 2026-11-24 15:46:44 UTC by Dennis Underwood