¿Cómo le ayuda Cyber Crucible a proteger la privacidad de los datos del alumnado?

Respuesta breve: FortressAI verifica el acceso a los datos en el dispositivo, de modo que los registros estudiantiles y los datos familiares no puedan llegar accidentalmente a una herramienta de IA pública. Cyber Crucible detiene el ransomware de forma autónoma sin requerir un centro de operaciones de seguridad (SOC) las 24 horas del día, los 7 días de la semana, algo que la mayoría de los distritos e instituciones no pueden financiar.

Más información: protección contra ransomware para escuelas y universidades

Los dos problemas de la educación

Las escuelas y universidades son objetivos preferidos del ransomware, y rara vez cuentan con presupuesto para una dotación de personal de SOC permanente. Al mismo tiempo, la adopción de IA en el aula ha avanzado mucho más rápido que la gobernanza correspondiente.

Cómo se abordan ambos problemas

- **Ransomware sin un SOC:** la prevención autónoma a nivel de kernel detiene los ataques en menos de 200 milisegundos, sin necesidad de contratar analistas ni financiar un contrato de monitoreo 24/7.
- **Uso de la IA alineado con la privacidad:** 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 acaben en ningún sistema de IA público, ni siquiera como datos de entrenamiento.

Esa combinación protege a los estudiantes y al personal sin agregar una carga significativa de trabajo de TI.

Revision #3
Created 2026-07-24 01:51:32 UTC by Dennis Underwood
Updated 2026-11-24 15:46:17 UTC by Dennis Underwood