Wie unterstützt Cyber Crucible Schulen und Universitäten beim Datenschutz für Schülerdaten?

Kurzantwort: Cyber Crucible unterstützt Bildungseinrichtungen auf zwei Arten: Es stoppt Ransomware autonom, ohne ein rund um die Uhr besetztes Security Operations Center zu benötigen, und – über FortressAI – bewertet es den Datenzugriff von KI-Tools direkt auf dem Gerät, sodass Schülerdaten und Familiendaten nicht versehentlich an ein öffentliches KI-System gelangen. Da die Analyse lokal erfolgt und keine Schülerdaten gesammelt werden, verbleiben geschützte Bildungsunterlagen innerhalb der Grenzen der Einrichtung.

Mehr erfahren: Ransomware-Schutz für Schulen und Hochschulen

Die zwei Bildungsprobleme, die adressiert werden

- **Ransomware ohne SOC.** Die Prävention auf Kernel-Ebene stoppt Angriffe in unter 200 Millisekunden – ohne dass Analysten eingestellt oder ein Vertrag für die permanente Überwachung finanziert werden müssen.
- **KI-Governance für den Unterricht.** FortressAI setzt direkt auf dem Gerät Richtlinien durch, die verhindern, dass geschützte Bildungsunterlagen und persönliche Familiendaten KI-Tools und LLMs erreichen. So werden diese Daten nicht an ein öffentliches KI-System gesendet – auch nicht als Trainingsdaten.

Hinweise zur Anbieterauswahl

- Cyber Crucible arbeitet nach Weisung der Einrichtung und verwendet Schülerdaten zu keinen weiteren Zwecken.
- Bundesstaatliche Datenschutzgesetze für Schülerdaten (zum Beispiel in Kalifornien, New York und Colorado) sehen zusätzliche Anbieterpflichten vor; das Design mit lokaler Verarbeitung und ohne Datensammlung unterstützt deren Einhaltung. Dokumentation ist unter NDA verfügbar.

Revision #3
Created 2026-07-24 04:53:19 UTC by Dennis Underwood
Updated 2026-11-24 15:43:42 UTC by Dennis Underwood