

Comment Cyber Crucible prend-elle en charge la loi FERPA et la confidentialité des données des élèves pour les écoles et les universités ?

Réponse courte : Cyber Crucible aide les établissements d'enseignement de deux façons : elle arrête les ransomwares de manière autonome sans centre opérationnel de sécurité (SOC) fonctionnant 24 h/24 et 7 j/7, et — grâce à FortressAI — elle évalue l'accès aux données par les outils d'IA directement sur l'appareil, afin que les dossiers des élèves et les données familiales ne parviennent pas accidentellement à un système d'IA public. Comme l'analyse est locale et qu'aucun dossier d'élève n'est collecté, les données scolaires protégées restent au sein du périmètre de l'établissement.

Les deux problématiques éducatives traitées

- **Les ransomwares sans SOC.** La prévention au niveau du noyau arrête les attaques en moins de 200 millisecondes, sans qu'il soit nécessaire d'embaucher des analystes ni de financer un contrat de surveillance continue.
- **La gouvernance de l'IA en classe.** FortressAI vérifie chaque invite (prompt) directement sur l'appareil, afin que les dossiers scolaires protégés et les données personnelles familiales ne soient pas envoyés à un système d'IA public — y compris à titre de données d'entraînement.

Points à retenir pour la sélection des fournisseurs

- Cyber Crucible agit en tant que fonctionnaire scolaire / prestataire de services sous la direction de l'établissement et n'utilise les données des élèves à aucune autre fin secondaire.

- Les lois étatiques sur la confidentialité des données des élèves (par exemple en Californie, à New York et au Colorado) imposent des obligations supplémentaires aux fournisseurs ; la conception fondée sur le traitement local et l'absence de collecte de données permet de s'y conformer. La documentation est disponible sous accord de confidentialité (NDA).
-

Revision #1

Created 2026-07-24 07:14:30 UTC by Dennis Underwood

Updated 2026-07-24 07:14:31 UTC by Dennis Underwood