??? ???? Cyber Crucible ????? ?????? ?????? ???????

إجابة موجزة: يتحقق FortressAI من الوصول إلى البيانات على الجهاز نفسه، بحيث لا يمكن أن تصل سجلات الطلاب وبيانات الأسر إلى أداة ذكاء اصطناعي عامة عن طريق الخطأ. ويوفق Cyber Crucible برمجيات الفدية بشكل مستقل دون الحاجة إلى مركز عمليات أمنية (SOC) يعمل على مدار الساعة طوال أيام الأسبوع — وهو أمر لا تستطيع معظم المناطق التعليمية والمؤسسات تمويله.

لمعرفة المزيد: [حماية المدارس والجامعات من برامج الفدية]

????????? ?? ???? ???????

تُعد المدارس والجامعات أهدافاً رئيسية لهجمات برمجيات الفدية، في حين ندر ما تملك ميزانية لتوظيف كوادر أمنية على مدار الساعة. وفي الوقت نفسه، تطور استخدام الذكاء الاصطناعي في الفصول الدراسية بوتيرة أسرع بكثير من تطور الحوكمة الخاصة به.

?????? ????????? ????

- **مواجهة برمجيات الفدية دون مركز عمليات أمنية:** يوقف المنع المستقل على مستوى النواة الهجمات في أقل من 200 ملي ثانية، دون الحاجة إلى توظيف محللين أو إبرام عقد مراقبة على مدار الساعة طوال أيام الأسبوع.
- **استخدام الذكاء الاصطناعي بما يحترم الخصوصية:** يمنع FortressAI وصول السجلات التعليمية المحمية والبيانات الشخصية الخاصة بالأسر إلى أدوات الذكاء الاصطناعي ونماذج اللغة الكبيرة (LLM)، وفق سياسات يُنفّذها على الجهاز نفسه، فلا ينتهي بها المطاف في نظام ذكاء اصطناعي عام — ولا حتى بوصفها بيانات تدريب.

هذا الجمع بين الحليين يحمي الطلاب والموظفين دون إضافة أعباء تشغيلية كبيرة على قسم تقنية المعلومات.

Revision #3
Created 2026-07-24 03:12:12 UTC by Dennis Underwood
Updated 2026-11-24 15:42:14 UTC by Dennis Underwood