SECURØ CocoAI

Pioneros en el Hacking ético de IA en el entorno educativo

Tras su primer año en el mercado, CocoAI —la startup EdTech fundada en 2025 que está transformando la forma en que las familias gestionan su bienestar digital— decidió someter su plataforma a una rigurosa evaluación de seguridad avanzada. Con un Producto Mínimo Viable (MVP) consolidado y una base de usuarios en expansión, la compañía dio un paso decisivo: transicionar de un enfoque de seguridad puramente pasivo hacia una estrategia ofensiva proactiva, garantizando la privacidad absoluta de los estudiantes y blindando su rentabilidad financiera frente al abuso de recursos de IA.

EL RETO

Desde su concepción, CocoAI partía de una base de seguridad responsable y alineada con los estándares de calidad del sector. La plataforma ya contaba con mecanismos de mitigación tradicionales, tales como la autenticación de doble factor (2FA), políticas sistemáticas de respaldo (backups) y la selección rigurosa de proveedores de infraestructura que garantizaban la soberanía de los datos y el estricto cumplimiento normativo. Sin embargo, el verdadero desafío residía en la falsa sensación de seguridad generada por estas medidas de carácter pasivo. Pese a contar con una arquitectura aparentemente robusta, la plataforma presentaba desafíos críticos que pasaban desapercibidos debido a la ausencia de un análisis bajo la óptica de la seguridad ofensiva.

La falta de una simulación de intrusión activa dejaba expuestos puntos ciegos en la lógica interna de la API, un área donde el 2FA convencional resultaba insuficiente. En el sector educativo, donde las instituciones demandan un estándar de privacidad absoluto e inquebrantable, se hacía evidente que las buenas prácticas operativas de escritorio ya no bastaban. Se requería una validación técnica de alto nivel capaz de transformar la confianza intuitiva en una robustez estructural verificable y blindada ante accesos no autorizados en las comunicaciones.

SOLUCIÓN PLANTEADA

Para mitigar estos riesgos de forma definitiva, CocoAI adoptó una solución estratégica: el lanzamiento de un Programa de Divulgación de Vulnerabilidades (VDP). Este marco operativo permitió realizar una búsqueda activa, continua y abierta de fallos de seguridad,

sometiendo la lógica de negocio a un examen profundo que las herramientas de escaneo pasivo y perimetral son incapaces de cubrir. A través de esta colaboración proactiva con investigadores de seguridad, se identificaron vulnerabilidades críticas de diversa naturaleza que afectaban de forma directa tanto a la privacidad de los usuarios como a la estabilidad financiera de la plataforma.

IMPACTO

La intervención permitió a CocoAI realizar una transición crítica hacia una infraestructura técnicamente validada. Aunque la experiencia para el usuario final (profesores y alumnos) se mantuvo fluida e ininterrumpida, el impacto interno en la organización fue radical: la empresa pasó de operar bajo una presunción de seguridad a poseer un ecosistema blindado, donde cada vulnerabilidad detectada se tradujo de inmediato en una mejora arquitectónica definitiva.

Los beneficios se consolidan en dos dimensiones clave:

Tranquilidad estratégica y confianza operativa: la dirección de la startup destaca que el valor principal del programa no fue únicamente técnico, sino emocional y estratégico. Subrayaron haber experimentado un "aumento en la tranquilidad a medida que se detectaban y se arreglaban problemas", otorgándoles la claridad necesaria para centrar sus esfuerzos en la expansión del negocio con la certeza de operar sobre bases sólidas.

Defensa estructural mediante código: a diferencia de las soluciones superficiales o los parches temporales, los hallazgos impulsaron una reingeniería en la estructura de la plataforma. Esto mitigó el riesgo de explotación de tokens de IA y educó al equipo de desarrollo bajo la filosofía de "protección desde el diseño", garantizando que el software futuro nazca seguro antes de ser desplegado.

"Pasamos de asumir que todo estaba bien a saber con certeza que nuestra plataforma es segura. Ese cambio nos dio la tranquilidad que necesitábamos para enfocarnos en crecer."