OZCORP SCIENTIFIC LLC
7 Calle Tabonuco Ste 105
Guaynabo, PR 00968

Desde $10,000 por proyecto

Aseguramiento de IA científica y evaluación adversarial

Evaluación adversarial de alcance definido para modelos de lenguaje científicos, agentes co-científicos, sistemas de evaluación y sistemas de datos de investigación sensibles. Las pruebas son autorizadas, delimitadas y documentadas para apoyar decisiones de riesgo.

Alcance del trabajo

- Evaluación de modelos científicos y sistemas de prueba
- Pruebas de agentes de investigación y acceso a herramientas
- Revisión de flujos de datos biológicos y químicos sensibles
- Escenarios de amenazas y evidencia reproducible
- Recomendaciones priorizadas para equipos científicos y de seguridad

Proceso de trabajo

01 **Autorizar y delimitar el trabajo**
Confirmar sistemas, permisos, clases de datos, objetivos y exclusiones.

02 **Inventariar el flujo**
Documentar uso previsto, componentes, herramientas y supervisión humana.

03 **Evaluar los requisitos acordados**
Realizar evaluaciones controladas dentro del entorno y los métodos autorizados.

04 **Registrar evidencia**
Documentar observaciones, resultados reproducibles, alcance y limitaciones.

05 **Priorizar medidas correctivas**
Entregar hallazgos y próximos pasos prácticos a los equipos responsables.

Aplicaciones
Modelos científicos, agentes de investigación, controles de evaluación y sistemas de datos sensibles.

Nota de alcance
Las pruebas son autorizadas y se limitan a los sistemas, permisos y métodos acordados.

Equipos participantes
Tortzal, Science

NAICS sugerido

541690 Otros servicios de consultoría científica y técnica
541511 Programación informática personalizada
541990 Otros servicios profesionales, científicos y técnicos.

PSC sugerido

B524, B529 y B544 estudios y análisis científicos
AJ11 servicios de I+D en ciencia y tecnología.

© All Rights Reserved