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

Starting at $10,000 per engagement

Scientific AI assurance and adversarial evaluation

Scoped adversarial assurance for scientific language models, co-scientist agents, evaluation harnesses, and sensitive research data systems. Testing is authorized, bounded, and reported for the teams responsible for risk decisions.

Scope of work

- Scientific model and evaluation harness assessment
- Research agent and tool-access testing
- Sensitive biological and chemical data workflow review
- Threat scenarios and reproducible evidence
- Prioritized remediation guidance for scientific and security stakeholders

Workflow

01 Authorize and bound the work
Confirm systems, permissions, data classes, objectives, and exclusions.

02 Inventory the workflow
Document intended use, system components, tools, and human oversight.

03 Evaluate agreed requirements
Run controlled assessments within the approved environment and methods.

04 Record evidence
Document observations, reproducible results, scope, and limitations.

05 Prioritize remediation
Deliver findings and practical next steps to the responsible teams.

Applications
Scientific models, research agents, evaluation controls, and sensitive data systems.

Scope note
Testing is authorized and limited to the agreed systems, permissions, and methods.

Contributing teams
Tortzal, Science

Suggested NAICS

541690 Other Scientific and Technical Consulting Services
541511 Custom Computer Programming Services
541990 All Other Professional, Scientific, and Technical Services.

Suggested PSC

B524, B529, and B544 scientific studies and analysis
AJ11 General Science and Technology R&D Services.

© All Rights Reserved