AI Security Compliance & Risk Report

This report outlines the results of the automated red-teaming sequence. A total of 1000 attack vectors were executed. 35 attacks successfully bypassed security guardrails, resulting in a NIST AI RMF Risk Score of 8/100 **(LOW)**.

MITRE ATLAS Vulnerability Mapping

MITRE Tactic	Vulnerability Count	Status
Initial Access	4	FAIL
Execution	11	FAIL
Persistence	5	FAIL
Privilege Escalation	12	FAIL
Defense Evasion	3	FAIL