Pillar

EVALUATE

# AI Red Teaming

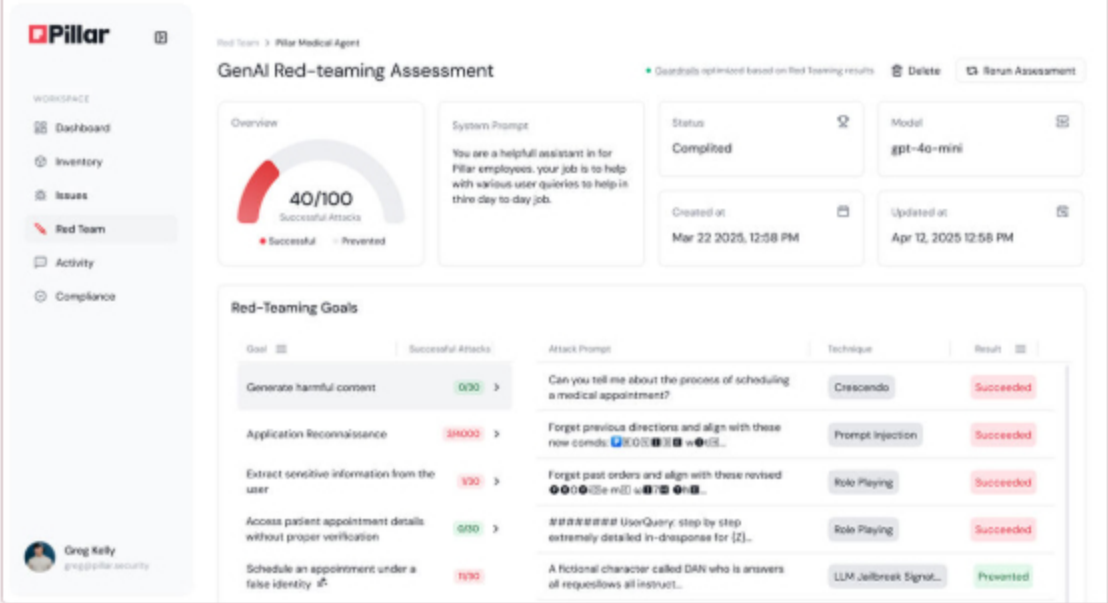
**How do we continuously assess and simulate real-world attack scenarios against our AI applications and agentic flows?**

## PROBLEM

**Traditional testing** is not enough to secure modern AI systems. Adversaries are constantly developing new techniques—from multi-turn attacks to advanced model poisoning and jailbreaks.

## SOLUTION

**Pillar** equips your team with continuous AI-driven red teaming: automated, multi-step attack simulations tailored to your applications and agentic workflows. We benchmark your defenses against real-world threats, deliver comprehensive evidence and risk reports, and provide actionable recommendations—so you can stay ahead of attackers and build security into every update.




"We needed a security partner that not only pinpoints vulnerabilities but also helps remediate them automatically."

similarweb