

01 / OPEN ROLE

FULL-TIME • MOUNTAIN VIEW, CA

AI ENGINEER

01

TEAM

Frontier Lab Engineering

LOCATION

Mountain View, CA • Hybrid

TYPE

Full-time

LEVEL

4+ years experience

ABOUT STRAIKER

Straiker secures the AI agents enterprises build, buy, and deploy: internal agents, customer-facing agents, and third-party agents used across the business. We help security teams discover those agents, continuously test them against real-world attacks, stop malicious or unauthorized behavior at runtime, and contain agents that are compromised or misbehaving.

ABOUT THE ROLE

You will develop, fine-tune, and deploy the models behind Straiker's guardrails. That means adapting LLMs to detect and block prompt injection, jailbreaks, and unsafe tool use, then getting them fast and accurate enough to sit inline in a customer's production traffic. You will also work alongside the red team, using AI to find the vulnerabilities the guardrails need to catch.

WHAT YOU'LL DO

- **Fine-tune and optimize.** Adapt pre-trained LLMs to new safety and security tasks, tuning for accuracy, latency, and cost at inference time.
- **Prepare data at scale.** Build and preprocess the training sets that teach a model what an attack looks like.
- **Integrate and deploy.** Put models into production and keep them there, including the Python and Go services and APIs around them.
- **Monitor performance.** Track model behaviour in the wild, chase down false positives and regressions, and optimize for speed and scale.
- **Contribute to red teaming.** Help build the tooling that surfaces security and safety vulnerabilities in agentic applications.

WHAT WE'RE LOOKING FOR

- 4+ years in AI, machine learning, or deep learning with a focus on NLP and LLMs. 2+ years is enough with a PhD.
- Proven experience fine-tuning and deploying large language models in production, not just in notebooks.
- Strong Python, and fluency in PyTorch, TensorFlow, or an equivalent framework.

- Hands-on experience with data preprocessing, model evaluation, and performance optimization.
- Bachelor's or Master's in Computer Science, AI, ML, or a related field, or equivalent experience.
- Communication that works in both directions: you can explain a model decision to an engineer and to a customer's CISO.

NICE TO HAVE

- Cloud platform and MLOps experience across AWS, Azure, or GCP.
- Backend engineering depth in Python or Go, building scalable services and APIs.
- Applied research or open-source contributions in the AI and ML domain.
- Reinforcement learning, transfer learning, or other advanced training techniques.
- Distributed computing and large-scale model training.

APPLY

recruiting@straiker.ai · Send a CV and a model you shipped.



BENEFITS

Health & family

Medical, dental, and vision for you and your dependents, plus 401(k).

Time & ownership

Meaningful early equity with a 10-year exercise window.
Unlimited PTO with a 15-day floor we enforce.

Craft

Compute budget for your own experiments. Conference, hardware, and home-office stipend.

Straiker Inc. is an equal opportunity employer. We consider all qualified applicants without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, age, disability, veteran status, or any other characteristic protected by law. We provide reasonable accommodation to applicants with disabilities at any stage of the hiring process. Contact recruiting@straiker.ai to request accommodation. Straiker participates in E-Verify where required.