# Aditi Narasimhan

408-707-4063 | aditi.narasimhan@gmail.com | linkedin.com/in/aditinarasimhan | aditinara.com

## Experience

**Research Lead** Aug. 2026 – Present

**Founding AI Research Engineer** Nov. 2025 – Aug. 2026

*Corridor – $30M funding / $200M valuation, acquired by Cognition* *San Francisco, CA*

- Developed the evaluation harness for Argos, a security context selection model, and co-trained Qwen3.5-9B with LoRA on Baseten Loops. Argos ranked first at security context selection among 14 tested models.
- Created the SECCRET benchmark to evaluate security-context relevance for coding-agent plans, with graded labels, human validation, and reproducible evaluations; gave a talk on SECCRET and Argos at DEF CON 34.
- Developed evaluations and prepared training data for a security model targeting pre-commit code scans.
- Built agent steering and guardrail generation pipelines to guide coding agents toward secure code by default. Migrated core AI workflows to Python/FastAPI and LangGraph on ECS Fargate with LangSmith tracing; cut main-path latency by approximately 89% and longer-job runtime by over 83%.
- Designed an automated PR approver and built a 197-PR evaluation; reduced false approvals by 80% versus the historical reviewer and saved approximately $16K/month.
- Built Corridor's research function from the ground up: scoped projects, mentored researchers, and established evaluation and publication processes. Co-authored the majority of Corridor's research articles and blog posts.

**Software and Policy Engineer** May 2025 – Nov. 2025

*nbhd.ai*

- Built Python and Rust APIs for AI evaluation, powering DEF CON 33's Generative Red Teaming challenge.
- Authored blogposts on AI governance and evaluations, presented a proposal at Hackers on the Hill's Cyber Policy Shark Tank, and earned 3rd place at Critical Effect 2025 Conference.

**Software Engineer, IRIS Rover** Aug. 2023 – June 2024

*Astrobotic* *Pittsburgh, PA*

- Built OpenCV terrain visualization using planar homography; integrated a CNN to flag lunar obstacles.

**Software Engineering Intern** Summers 2022, 2023, 2024

*Wells Fargo* *Fremont, CA*

- Built an NLP chatbot to help developers and agents select the appropriate APIs during code generation.
- Implemented card PIN authentication with React and Spring Boot; achieved 100% BDD coverage of new features.

## Selected Projects

**Maternity Digital Twins** | *99P Labs*

- Led a multidisciplinary team spanning hardware, software, electrical engineering, HCI, and AI/ML to deliver a postpartum-care prototype.
- Co-developed an aggregate anomaly detection model and a fine-tuned LLM assistant, integrated with sensors and patient- and provider-facing iOS applications.

**picoCTF Development & Security Research** | *CyLab, Carnegie Mellon University*

- Developed cryptography problems for picoCTF; represented picoCTF and ran a competition at RSAC 2025.
- Conducted white-hat security research with Dr. David Brumley; earned CVEs including CVE-2024-56157.

## Education

**Carnegie Mellon University** Aug. 2020 – May 2025

*M.S. Electrical and Computer Engineering, Software Engineering concentration* *GPA: 4.0/4.0*

*B.S. Electrical and Computer Engineering; double major in Philosophy* *GPA: 3.8/4.0*

## Technical Skills

**Languages**: Python, Rust, TypeScript, C/C++, Java, JavaScript
**ML & Evaluation**: Supervised fine-tuning (SFT), LoRA, benchmark design, evaluation harnesses, anomaly detection
**Frameworks & Libraries**: LangChain, LangGraph, FastAPI, Keras, OpenCV, React
**Infrastructure & Tools**: Baseten Loops, LangSmith, Docker, AWS ECS Fargate, Git

## Leadership & Teaching

**Co-founder, HOPEful Engineering Collective, CMU.** Built a tech ethics organization, led outreach, and moderated panels for 100+ attendees.

**Head Teaching Assistant & Guest Instructor, CMU.** Co-developed the Ethics and Policy Issues in Computing curriculum and taught weekly lectures; redesigned and co-taught ECE Senior Capstone ethics lectures; held weekly discussions for the AI, Society, and Humanity course.