ALIYA ALSAFA

Palo Alto, CA · 312-956-9200 · aalsafa@stanford.edu
aliyaalsafa.github.io · linkedin.com/in/aliya-alsafa · github.com/AliyaAlsafa

EDUCATION

Stanford University *Palo Alto, CA*
M.S. Computer Science, Artificial Intelligence track (coterminal) *Expected Jun 2027*
B.S. Computer Science, Systems track; Minor in Music, Piano Performance · GPA 3.70 *Jun 2026*

EXPERIENCE

Chainguard | Security Engineering Intern, Product Security · Remote *Summer 2026*

- Designed a test corpus of pull requests seeded with known vulnerability classes, giving the benchmark a ground truth to measure against, and wrote the test suite and harness that run detectors over it.
- Researched, implemented, and benchmarked 6 single-agent and multi-agent architectures, with variations on each, across Claude, GPT, and Gemini models on Google Vertex AI, scoring each on vulnerabilities found, false positive rate, and cost per run.
- Exposed Semgrep and CodeQL to the agents as MCP tools while also running them as standalone baselines, separating what the models add from what static analysis already catches.
- Raised the security lens evaluator's vulnerability-detection recall from 44% to 84% by combining the top-performing architecture with static analysis, prompt refinement, and an adjudication agent that verifies each finding is labeled correctly.

Redis | Security Engineering Intern · Remote *Summer 2024*

- Reproduced HackerOne bug bounty findings with penetration testing techniques and wrote an internal offensive-testing guide for developers.
- Built a Python tool to find and report abandoned corporate DNS records, reducing cloud attack surface; containerized and deployed it to AWS ECS.
- Wrote custom Wiz frameworks to scan the cloud environment against CIS Ubuntu Benchmarks; integrated DoControl into corporate SaaS apps.

RESEARCH

Stanford University | Research Assistant, Biomechanical Modeling of Piano Performance *2025 – Present*

- Training reinforcement learning policies in PyTorch to drive a physics-based model of piano-playing motion in NVIDIA Isaac Gym, over motion data retargeted from Blender, to study how simulated muscle activation informs piano performance technique.

Stanford Empirical Security Research Group | Undergraduate Researcher, advised by Zakir Durumeric *Apr 2025 – Jun 2026*

- Built Rust modules in the Retina network analysis framework to offload flow-rule installation onto commodity NICs (DPDK, Mellanox).
- Contributed Retina's functional test harness (Python runner over pcap fixtures and expected output, plus a Rust test crate), merged upstream after code review.
- Designed experiments measuring NIC performance (rule latency, drop counters, RSS distribution) under high-throughput loads.
- Joined through CURIS; presented the poster "Reducing Host Load Via Commodity NIC Offloading" at the ESRG summer session and completed it as a CS 191W senior project, now a CoNEXT 2026 submission.

SKILLS

Languages: Python, Rust, Go, C/C++, Java, SQL, Terraform

AI & Agents: Claude, OpenAI, and Gemini APIs via Vertex AI; MCP; agent orchestration; PyTorch; Isaac Gym; pytest eval harnesses

Security & Cloud: Semgrep, CodeQL, Wiz, DoControl, BlinkOps, Wireshark, HackerOne, AWS, GCP, Docker, Linux/Unix

Tools: Git, DPDK, Jira, Sumo Logic

AWARDS & ACTIVITIES

TryHackMe Campus Ambassador, Stanford — organize cybersecurity events for students on campus.

Juilliard Pre-College, diploma in classical piano (2015–2022), performing internationally; Lang Lang International Music Foundation Young Scholar (2018–present).

Stanford Applied Cyber; Women in Computer Science; Executive Board, Stanford Piano Society and Stanford XTRM Dance.