

Zachary Lichtman

📍 Madison, Wisconsin | ✉️ zalichtman@wisc.edu | 🌐 zlichtman.com | 🗣️ zlichtman | 🔗 https://www.linkedin.com/in/zach-lichtman | 📞 (847) 226-5527

🎓 EDUCATION

University of Wisconsin Madison · B.S. in Computer Science Expected May 2028
Relevant Coursework: Artificial Intelligence, Neural Networks, Data Structures & Algorithms, Discrete Mathematics, Computer Engineering

💼 EXPERIENCE

- AI Engineering Intern, Infotainment DevOps & Production Software** — *Hyundai America Technical Center, Inc. (HATCI)* May - Aug 2026
- Architected **VERDICT**, an **evaluation harness** that decides whether a production LLM voice assistant is safe to ship to **millions of vehicles**.
 - Drives multi-turn spoken conversations with frontier in-vehicle models, including a head unit leased through Jumpstarter.
 - Grades every turn with **31 scorers across 98 dimensions**, from deterministic checks to Prometheus-2, G-Eval, and FLASK judges.
 - Decides via adaptive resampling, cluster-robust bootstrap, and equivalence tests against preregistered margins; refuses without evidence.
 - Earned **adoption and support from Red Hat** for use by multiple carmakers.
 - Contributed to HATCI's **OpenShift development platform**, standardizing development for **1,000+ engineers**.
 - Serves engineers across Hyundai, Kia, and Genesis's global R&D network.
 - Automated distributed testing via hardware-in-the-loop orchestration and Cuttlefish device emulation.
 - Built Tekton CI pipelines with GitOps delivery (Argo CD, Ansible) and embedded Linux (Yocto) build/debug tooling.
 - Partnered with **Amazon's voice team** on production integration and pre-release validation of in-vehicle voice features.
- AI Engineering Intern** — *Brainsprout* 2025 - 2026
- Built PyTorch/MONAI pipelines that render anatomically accurate 3D brain models used in neurosurgical education.
- Cybersecurity Researcher** — *OpenAI Daybreak Cybersecurity Member (2026)* 2022 - Present
- Identified and responsibly disclosed an IDOR (insecure direct object reference) vulnerability in **OpenAI's ChatGPT**.

🔗 OPEN SOURCE

- iOS Apps** — *Swift 6, SwiftUI, Supabase, Mapbox, MusicKit, Apple Foundation Models, MLX*
- PowderMeet** — Routes separated skiers to a meeting point by trail difficulty, lift lines, closures, and pace. **Live at 159 Epic and Ikon resorts**.
 - Heartable** — Unifies music split across Spotify and Apple Music: one library, shareable mixtapes, and playlist backups with diff and restore.
 - Tsukumo** — Uses Apple's local model as a privacy barrier: AI agents must ask it for anything personal, and it decides what leaves the iPhone.
- macOS Apps** — *SwiftUI + AppKit, Accessibility API, Vision, ScreenCaptureKit, CoreAudio* Notarized, on Homebrew
- MacSpaces** — Puts the dead space around the MacBook notch to work: hover for music, calls, timers, notes, files, and coding agents.
 - Tape** — Ends overlapping-window clutter by laying windows side by side on a scrolling strip, driven by keyboard or trackpad.
 - Folio** — Indexes image libraries on-device: Vision OCR and classification feed a SQLite FTS5 index, with feature-print similarity search.

👥 ACTIVITIES

- Technical Lead, Safety Scholars** — *Wisconsin AI Safety Initiative* 2026
- Leading the technical research projects behind our policy recommendations to state and federal lawmakers, and teaching the technical AI safety course.
- Publication: "Rational Machines; Irrational Standards"** — *Wisconsin Business Review (self-driving safety)* 2025
- Hackathon: Anthropic ClaudeHacks'26 — WhatIsTheMove** 2026
- Built to create community on campus: Claude ranks mood-matched spots and writes personality-specific icebreaker activities.
- Robotics** — *ML Engineer, AlohaMini (WiscoHumanoids) · Software Engineer, GNSS Navigation (Wisconsin Robotics)* 2024 - 2026
- Trained imitation-learning policies (Hugging Face LeRobot, ACT) on teleoperation data for the AlohaMini dexterous hand.
 - Validated GNSS navigation code for the autonomous rover, field-testing across varied terrain and signal conditions.

✂️ TECHNICAL SKILLS

Systems:	macOS, Linux (Debian), Yocto embedded Linux
Languages:	Swift, Python, C/C++, Rust, Java, TypeScript, HTML/CSS
AI / ML:	Claude & Codex SDKs, PyTorch, Hugging Face (LeRobot/ACT), MONAI, Kubeflow
AI Safety:	Alignment, Interpretability, Evals & Red-Teaming — Wisconsin AI Safety Initiative
Cybersecurity:	Kali Linux, Penetration Testing, Web Exploitation, Network Security, Auth0, Burp Suite — Northwestern CTD
Frontend & Design:	React, Next.js, PatternFly, Vercel, Mapbox, Figma, Adobe CC, Blender, Lucid
Backend & DevOps:	Spring Boot, Supabase, Tekton, Argo CD, GitLab, JFrog, Xcode, Git, Jira, Notion
Cloud & Infra:	AWS, Docker, OpenShift, Kubernetes, Knative, Ansible, Perses

🏠 PERSONAL

U.S. Figure Skating National Silver Award (2024) · UW Hoofers Mountaineering Club · Skiing · Piano · Study Abroad, San Sebastián, Spain