BO SHANG

商博

Founder, ErosolarAI · Security & AI Engineer

bo@ero.solar · LinkedIn · github.com/Aroxora · erosolarai.com

Open to relocating to China (Shenzhen / Greater Bay Area), on-site.

SUMMARY

Security & AI engineer with over a decade across offensive and defensive security — vulnerability assessment, penetration testing, incident response, and the engineering of production security tooling. Builds and operates the controls that protect networks, systems, and digital assets: continuous threat monitoring, security-log and threat-intelligence analysis, vulnerability management, and automated detection-and-response pipelines. Founder of ErosolarAI ( ); creator of Vigil, an AI-driven security agent spanning network, endpoint, cloud, and API defense. Also ships production full-stack AI products — the Anvilwing coding CLI, the Helia browser, and the Erosolar chatbot — and independent technical research (see GitHub).

EXPERIENCE

ErosolarAI ( )

2023 – Present
Remote

Founder & Lead Security / AI Engineer

- Founded an applied-AI studio shipping Anvilwing (terminal coding CLI), Helia (agentic browser), the Erosolar chatbot, and Provenika — most on DeepSeek models.
- Built Vigil, an AI-powered security agent pairing an LLM command-line agent with an offensive/defensive toolkit spanning network, endpoint, cloud, and API defense plus threat intelligence.
- Engineered continuous monitoring & detection pipelines — security-log analysis, Nmap/CVE correlation, CISA KEV threat-intel, secret scanning, SBOM generation.
- Implemented Model Context Protocol (MCP) tool servers exposing security capabilities to the LLM for automated investigation and response; designed a three-tier authorization model with scope/target verification and refusal detection.
- Architected platforms across ~200 TypeScript modules (React 19 SPA, AWS Lambda, Firebase, multi-stage Docker), with security documentation throughout.

Trenchwork

2021 – Present
Remote

Founder & Principal Security Engineer

- Independent security consultancy: penetration testing, vulnerability assessments, red-team exercises, code audits, and incident response under contract.
- Built a CVE Discovery Engine for zero-day research — grammar-aware coverage fuzzer, static pattern analyzer, differential binary analyzer, and an LLM novelty engine.
- Led incident response end to end — containment, forensics, root-cause analysis, remediation — supporting disaster-recovery and business-continuity goals.
- Built an Exploit-Chaining Engine (A*/beam-search attack graphs) to validate real risk and prioritize remediation; delivered clear technical reports and fixes.

Independent Security Researcher & Consultant

2014 – 2021
Remote

Vulnerability Research / Red Team

- Delivered offensive and defensive engagements — penetration testing, vulnerability research, and custom tooling — for a range of clients.
- Reverse-engineered binaries with Ghidra and IDA Pro; developed proof-of-concept exploits and actionable remediation guidance.

Kensho Technologies
2013 – 2014
Software Engineer
Cambridge, MA

- Early engineer at an AI/analytics startup applying machine learning to financial and economic data; built data-ingestion services and internal tooling.

Independent / Contract
2010 – 2013
Software Engineer
Remote

- Delivered full-stack web applications across front-end, back-end, and database layers.

TECHNICAL SKILLS

Security Operations & Monitoring: SIEM & security-log analysis, Wazuh, threat-intel feeds (CISA KEV), Nmap/CVE correlation, ClamAV, secret scanning, SBOM generation

Offensive Security: Penetration testing, vulnerability assessment, Metasploit, Burp Suite, Ghidra, IDA Pro, Hashcat, John the Ripper, BloodHound, Kali Linux (70+ tools)

Incident Response & Governance: Containment & forensics, root-cause analysis, remediation, security audits, compliance support, risk mitigation

Cloud & Infrastructure: AWS (Lambda, API Gateway, EventBridge, S3, IAM, Secrets Manager), Firebase (Auth, Firestore, Functions, Hosting), Docker

Languages: TypeScript, JavaScript, Python, C/C++, x86/ARM Assembly

AI / LLM: LLM agent orchestration, Model Context Protocol (MCP), streaming tool-calling, prompt design

SELECTED PROJECTS

Anvilwing — terminal coding CLI
anvilwing.com · npm

- Claude-Code-class coding agent on DeepSeek v4 Pro with /loop, scheduled cloud runs, background agents, and web/iOS control of a live local session.

Helia — agentic AI browser
Electron + Chromium

- ChatGPT-Atlas-style browser with a side-panel AI that has full page context and drives the page via the Chrome DevTools Protocol; signed & notarized macOS builds.

Vigil — AI-powered security agent
TypeScript / AWS

- LLM command-line agent + 70-tool offensive/defensive toolkit (Kali + Ghidra); CVE-discovery and exploit-chaining engines and MCP defense servers, for authorized testing.

defense-cad — EW simulation & OSINT threat modeling
Python / NumPy / SciPy

- Datalink sidelobe-detection and emitter-geolocation simulation (TDOA/FDOA/DF) with aspect-dependent RCS models — built entirely from OSINT and first-principles physics; unclassified, public, ITAR/EAR-compliant methodology.

EDUCATION

Tufts University — School of Engineering
2006 – 2010
Bachelor of Science in Computer Engineering
Medford, MA

LANGUAGES

English: Fluent — speaking and reading.

Mandarin Chinese: Understands spoken Mandarin and reads Pinyin; does not read Hanzi.