BO SHANG

商博

ErosolarAI 创始人 · 安全与 AI 工程师

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

可搬迁至中国（深圳 / 粤港澳大湾区），现场办公。

个人摘要

拥有十余年攻防安全经验的安全与 AI 工程师，涵盖漏洞评估、渗透测试、事件响应，以及生产级安全工具的工程化开发。擅长构建并运营保护网络、系统与数字资产的安全控制：持续威胁监控、安全日志与威胁情报分析、漏洞管理，以及自动化检测与响应流水线。ErosolarAI（朝阳智能）创始人；AI 驱动安全代理 Vigil 的创建者，覆盖网络、终端、云与 API 防御。亦交付生产级全栈 AI 产品——Anvilwing 编码命令行、Helia 浏览器与 Erosolar 对话引擎——以及独立技术研究（详见 GitHub）。

工作经历

ErosolarAI（朝阳智能） 2023

创始人兼首席安全 / AI 工程师

- 创立应用型 AI 工作室，发布 Anvilwing（终端编码命令行）、Helia（智能体浏览器）、Erosolar 对话引擎与 Provenika，多基于 DeepSeek 模型。
- 构建 Vigil：AI 驱动的安全代理，将 LLM 命令行代理与覆盖网络、终端、云、API 防御及威胁情报的攻防工具集结合。
- 设计并实现持续监控与检测流水线——安全日志分析、Nmap/CVE 关联、CISA KEV 威胁情报、密钥扫描、SBOM 生成。
- 实现 Model Context Protocol (MCP) 工具服务器，将安全能力开放给 LLM；设计三级授权模型，含范围/目标校验与拒绝检测。
- 在约 200 个 TypeScript 模块上完成平台架构（React 19 单页应用、AWS Lambda、Firebase、多阶段 Docker），全程维护安全文档。

Trenchwork 2021

创始人兼首席安全工程师

- 运营独立安全咨询机构，按合同提供渗透测试、漏洞评估、红队演练、代码审计与事件响应。
- 构建用于零日发现的 CVE 发现引擎——语法感知覆盖率模糊测试器、静态模式分析器、差分二进制分析器与 LLM 新颖性引擎。
- 端到端主导事件响应——遏制、取证、根因分析与修复——支撑灾难恢复与业务连续性目标。
- 构建漏洞利用链引擎（A*/集束搜索攻击图）以验证真实风险并对修复进行优先级排序；交付清晰技术报告与修复建议。

独立安全研究员与顾问 2014 – 2021

漏洞研究 / 红队

- 为多家客户交付攻防安全项目——渗透测试、漏洞研究与定制工具。
- 使用 Ghidra 与 IDA Pro 进行二进制逆向；开发 PoC 漏洞利用与可执行的修复建议。

Kensho Technologies 2013 – 2014

软件工程师

- AI / 分析创业公司早期工程师，将机器学习应用于金融与经济数据；构建数据摄取服务与内部工具。

独立 / 合同 2010 – 2013

软件工程师

- 为客户交付涵盖前端、后端与数据库层的全栈 Web 应用。

技术技能

安全运营与监控： SIEM 与安全日志分析、Wazuh、威胁情报源（CISA KEV）、Nmap/CVE 关联、ClamAV、密钥扫描、SBOM 生成

攻击性安全： 渗透测试、漏洞评估、Metasploit、Burp Suite、Ghidra、IDA Pro、Hashcat、John the Ripper、BloodHound、Kali Linux（70+ 工具）

事件响应与治理： 遏制与取证、根因分析、修复、安全审计、合规支持、风险缓解

云与基础设施： AWS（Lambda、API Gateway、EventBridge、S3、IAM、Secrets Manager）、Firebase、Docker

编程语言： TypeScript、JavaScript、Python、C/C++、x86/ARM 汇编

AI / LLM： LLM 代理编排、Model Context Protocol (MCP)、流式工具调用、提示词设计

精选项目

Anvilwing — 终端编码命令行 anvilwing.com · npm

- 基于 DeepSeek v4 Pro 的 Claude-Code 级编码代理，支持 /loop、云端定时运行、后台代理，并可经网页/iOS 操控本机实时会话。

Helia — 智能体 AI 浏览器 Electron + Chromium

- 仿 ChatGPT Atlas 的浏览器，侧栏 AI 通晓整页上下文并经 Chrome DevTools Protocol 操控页面；macOS 版本已签名并经 Apple 公证。

Vigil — AI 驱动的安全代理 TypeScript / AWS

- LLM 命令行代理 + 70 种攻防工具集（Kali + Ghidra）；含 CVE 发现与漏洞利用链引擎及 MCP 防御服务器，用于合规授权测试。

defense-cad — 电子战仿真与 OSINT 威胁建模 Python / NumPy / SciPy

- 数据链旁瓣探测与辐射源定位仿真（TDOA/FDOA/测向）及随视角变化的 RCS 模型——完全基于公开情报与第一性原理物理；非密、公开、符合 ITAR/EAR 方法论。

教育背景

塔夫茨大学 · 工程学院 2006 – 2010

计算机工程学士

语言能力

英语： 流利（口语与阅读）。

普通话： 能听懂口语、能阅读拼音；不能阅读中文汉字。