居浪

求职意向：AI Agent FDE（前线部署工程师）

男丨25岁丨硕士 17314833596 langju123456@gmail.com
github.com/langju123456



个人优势

1. 佛罗里达大学本科、圣路易斯华盛顿大学信息系统管理硕士（2025.12），中英双语；AI软件公司创始人兼技术负责人，专注AI Agent在客户现场的落地交付，覆盖场景识别、方案设计、研发集成、PoC→试点→生产上线的全过程。
2. 业务需求转化：主导真实店主需求访谈与试点、14场客户会议的企业数字化咨询、海外轨道交通投标的技术需求澄清；能深入客户业务识别适合Agent的关键流程，还原成业务流程、数据与权限边界和验收标准，并主动划清范围。
3. 现场落地：从原型走到客户现场，按客户实际设备与使用方式调整架构和部署（含本地私有化部署），完成备份切换、排障与复验，把"能跑"推进到"能用"。
4. Agent工程：独立实现工作流编排、Tool Calling、RAG、多模型接入（云端与本地）、持久化任务与审批回执分离；熟悉MCP、Agent评测、可观测与安全权限控制，对AI辅助生成的代码负责审阅与验收。
5. 评测与持续优化：自建Agent评测与失败归因体系，用独立验证器度量准确率并兼顾延迟与成本；把可复用组件、部署说明和排障记录沉淀为交付规范。

工作经历

Lang Horizon Technologies llc 创始人 · AI应用全栈工程师 2026.01-至今

自营AI软件项目研发与交付。创立并经营公司，主导美业服务Copilot、SoloScale AI OS、ForgeFlow、EvidenceLoop、BuildLog、X Post Lab六项自研产品从0到1的需求、研发与交付，面向AI应用研发与客户需求落地。

1. 客户需求与范围：与真实店主做需求访谈和原型测试，把一线记录、老板决策与客户回访拆成可验收的流程与数据边界；按证据成熟度决定范围和下一步，未完成项写进交付材料。
2. 部署与交付：按客户实际设备与使用条件选择部署方式，完成门店本地私有化轻量部署、macOS桌面打包与云端GPU实验环境配置，交付材料包含配置说明、排障记录与已知限制。
3. 研发与集成：用Codex、Claude Code推进AI辅助开发，本人负责架构取舍、关键路径和代码审阅；对接多家云端与本地模型、OAuth及第三方API，基于MCP约束工具边界，统一结构化输出、超时与错误处理。
4. 质量与验收：每个产品配自动化测试、类型检查与CI，关键版本另设独立产品复验；以真实HTTP、浏览器流程和真实模型运行验收，修复后重新复验再交付。

南京康尼机电股份有限公司 海外技术销售工程师 2023.12-2024.05

面向海外客户的轨道交通投标与技术方案支持：参与2-3个项目，连接海外客户与研发、生产、销售团队，围绕需求澄清、技术方案和交付约束推进协作。

1. 梳理客户业务与技术需求，将规格、交付要求和问题清单转化为技术方案、需求澄清材料及后续执行事项，支持英文客户沟通。
2. 结合CRM/ERP业务流程识别人工操作、信息断点和数据管理问题，输出流程分析及改进需求，为后续数字化方案提供业务依据。

项目经历

美业服务 Copilot｜从需求访谈到门店落地 2026.09-至今

面向真实店主的服务记录与跟进Agent，需求访谈、PoC、门店试点到本地部署运维全程负责。
1. 需求转化：将服务前查档、服务后即时语音/文字记录、员工核对、老板整理与回访转为可操作流程；区分服务原话、人工采用文字、老板决定及后续执行。
2. 数据与权限：FastAPI/Pydantic/SQLAlchemy/SQLite构建API，按员工/老板角色划分数据访问；原音频、首次转写与人工修订分离保存，回访建议须授权，写回前检查来源版本与租约，原话修改后旧建议失效。
3. 现场适配：按门店现有电脑的配置做轻量化改造，改为单机数据库与持久化顺序任务，加入版本化ASR/AI缓存、音频去重、本地快照与恢复检查，形成店内部署与运维方案。
4. 故障与验收：完成数据库/代码备份与服务切换，用隔离数据库与合成音频验证保存、授权回听与重启持久化，经独立产品复验。

Ardent Mills｜供应链数字化转型校企Capstone（项目负责人） 2025.09-2025.12

1. 面向北美面粉与谷物原料企业，带领6人团队，经14场客户、业务与技术相关方会议，澄清供应链B2B集成、主数据与数据治理问题，将业务、技术及信息安全要求转成需求清单和实施优先级。
2. 管理Sprint、Scope与Roadmap，比较EDI、API与混合集成方案，向客户管理层及技术团队汇报分阶段路线图；交付咨询方案与路线图。

ForgeFlow｜面向企业的Agent受控执行与审计平台 2026.10-至今

1. 面向企业对审计、安全与权限控制的要求：FastAPI/PostgreSQL持久化执行记录，lease/epoch与幂等，验证SIGKILL回滚、重启恢复与跨进程回放；基于MCP SDK设定sandbox工具边界，模型提议、服务端判定、审批与回执分离。
2. 本地Qwen3:8B驱动Supervisor/PM两个角色完成5个场景20次调用；系统性审阅修复审批绕过等问题后，932项隔离测试通过。

EvidenceLoop｜Agent评测与失败归因（开源） 2026.10-至今

1. 独立验证器从数值、单位、来源、状态、权限五维判定Agent结果并归因到具体错误路径；在3个尺寸模型上采集776条真实轨迹，定位嵌套工具参数为主要失败源，重构接口后关键通过率由17%–43%提升至65%–85%。源码：github.com/langju123456/evidenceloop

SoloScale AI OS｜LLM应用与工程证据工作台 2026.01-至今

1. RAG与Agent编排：使用SQLite FTS5/BM25与RRF融合排序做证据检索，保留来源与内容哈希；BoundedEvidenceAgent按查询规划→检索→覆盖检查→有依据草稿执行，核对引用ID/哈希并配人工确认。
2. 适配Ollama、OpenAI-compatible与DeepSeek，交付macOS桌面版，720项测试通过。源码：github.com/langju123456/soloscale-ai-os

教育经历

圣路易斯华盛顿大学 信息系统管理（MISM） 硕士 2024.08-2025.12

佛罗里达大学 信息系统（B.S.B.A.） 本科 2019.09-2023.05

专业技能

Agent交付： AI Agent设计、Workflow编排、Function Calling / Tool Calling、多Agent协作、LangChain / LangGraph / LlamaIndex / smolagents、MCP
RAG与知识库： 文档分块、Embedding、Chroma / FAISS、BM25+向量混合检索、RRF融合、引用核验
模型与部署： OpenAI / DeepSeek / Qwen / Llama、Ollama / vLLM、私有化部署与本地推理、LoRA微调
系统集成： Python / FastAPI / HTTP API、PostgreSQL / SQLite / SQL、第三方API对接、Docker / Linux / Git / CI/CD
评测与安全： Agent评测、可观测、审批与审计、权限控制、沙箱隔离
客户与方案： 需求分析、方案设计、PoC→生产、中英双语客户沟通、Claude Code / Codex

证书与语言

Hugging Face课程：Agents（卓越证书） | MCP | Deep RL | Robotics
DeepLearning.AI：ML Specialization | ML in Production | 语言：英语精通、西班牙语熟练