刘世鑫 Agent Harness 产品经理

AI 产品负责人 / Agent 产品架构实践者

目标岗位：DeepSeek Agent Harness 产品经理｜桌面端 Agent / Coding Agent / 企业级 Agent 工作流

邮箱： shanpowu05@163.com
微信： I-season
GitHub： @gloweaseco-leo
视频号/作品集： @高管大壮（微信认证）

个人定位

业务视角看 AI： AI 的价值不在于单次生成答案，而在于进入企业真实流程，把合同、审批、经营分析、项目开发、运维和服务质检等高摩擦场景，改造成可执行、可确认、可追踪、可评估的任务系统。

AI 视角看过往行业： 我经历的地产、工程运营、新能源、服务运营，本质上都是流程、规则、数据、权限、责任和风险组成的复杂系统。Agent 要进入这些系统，必须由 Harness 管理上下文、工具、状态、人工确认、失败恢复、审计留痕和反馈评估。

职业定位： 15 年复杂组织管理经验 + 近两年 AI 产品 / Agent 实战，适合承担 Agent Harness、企业 AI 应用、AI 工作台、AI FinOps / 可观测性等方向的产品定义、原型验证和用户反馈闭环。

职业时间线

2023.01 - 至今 **独立 AI 产品实验室**	AI 产品负责人 / Agent 产品孵化实践：以 AI 产品能力迁移、原型验证和行业场景抽象为主；围绕 Agent、RAG、OCR/ASR、AI Coding、工作流和本地部署形成产品方法论。把业务流拆解为任务入口、数据结构、工具调用、权限复核、审计留痕、质量评估和迭代反馈，输出合同解析、企业知识库、Agent 工作流、TokenRadar、FDE Workbench 等产品原型。
2023.01 - 至今 **光伏投资开发（并行）**	股东 / 项目开发与运营参与者：参与项目获取、屋顶资源判断、客户沟通、收益测算、合同协同和日常管理；沉淀线索获取、资源评估、用电负荷、收益模型、并网审批、EPC 建设、运维监控等流程规则，为 AI 投资测算、风险识别、运维预警类产品提供真实业务理解。
2021.04 - 2022.12 **实地集团**	助理总裁：分管运营管理、工程管理、客户服务和产业公司，统筹 159 个在建项目；推动数字化大运营体系、分供方支付统筹、工抵房决策、存量资产分类处置等机制，本质是把复杂组织中的资金流、合同流、审批流和风险流结构化。
2019.11 - 2021.03 **佳兆业集团**	广州公司常务副总 / 控股总部轮岗：分管大运营、投资、融资等线条，负责投资拓展、旧改孵化、12 个在建项目运营统筹、年度预算和快速开盘体系；参与经营分析会和大运营体系落地，强化“经营数据 - 流程规则 - 决策反馈”的产品化意识。
2009.07 - 2019.11 **龙湖集团**	区域副总经理 / 事业部总经理 / 集团工程区域负责人 / 项目总监：经历工程、运营、项目经营、区域管理和组织建设全周期；管辖 13 城、81 个项目、约 1300 万㎡在建面积、约 400 人工程管理团队，输出启动会、运营停止点、新公司组织建设等制度，把项目经验沉淀为规则、流程、标准和组织产品。

重点产品与作品

AI FDE Workbench / 现场部署工程师工作台 ｜ 产品定义 / 原型验证

• 面向企业 AI 现场部署工程师，设计自然语言驱动工作台：需求理解、Connector 接入、Transform 清洗、Ontology 建模、Agent Assembly、Eval / Release 和交付报告生成。

• 本质是把企业 AI 落地流程做成 Agent Harness：模型负责推理，Harness 管理工具、上下文、任务状态、人工确认、调试轨迹和验收标准。

关键词： FDE · AI Workbench · 企业 Agent · Ontology · 交付闭环

TokenRadar 桌面端 AI API 成本雷达 ｜ Local LLM API Gateway + Token Observability

• 定位为本地 AI API 成本治理工具，统计不同 Agent、项目、模型、API Key 的 Token 消耗、调用成本、延迟、失败率、重试和异常使用。

• MVP 设想：OpenAI-compatible / DeepSeek / Qwen-DashScope 请求代理、本地 SQLite、价格表、项目归因、预算提醒；企业版演进为 AI FinOps & API Key Governance Platform。

• 与 Harness 的关系：Agent 越自动化，越需要调用链可观测、成本可归因、Key 可治理、异常可追踪。

关键词： Token Observability · API Gateway · AI FinOps · Key Governance

OpenClaw / Hermes 移动端 Agent 部署实践 | 开源 Agent 用户反馈样本

• 将 OpenClaw、Hermes 等开源 Agent 框架部署到安卓 / Termux / Ubuntu 环境，验证本地 Agent 运行、权限、后台常驻、易用性和稳定性问题。

• 公开视频教程累计播放破百万，沉淀普通用户在 Agent 部署门槛、配置理解、工具调用、失败提示和交互方式上的真实反馈。

关键词： OpenClaw · Hermes · Termux · 用户反馈 · 本地 Agent

合同智能解析与风险审查系统 | OCR + LLM + Human-in-the-loop

• 设计合同上传、OCR 解析、关键字段提取、风险条款高亮、AI 修改建议、人工确认、版本追溯和审计留痕流程。

• 产品边界：AI 提供证据和建议，人类负责确认与最终决策；适合说明高风险业务场景下 Agent 的权限、复核和责任边界。

关键词： OCR + LLM · 风险识别 · 人工复核 · 审计留痕

企业知识库与 AI Agent 工作流 | RAG + 多步骤任务执行

• 设计文档上传、解析、分段、索引、权限、引用、反馈修正和复核机制，从知识问答到资料生成、流程推进、人工审批和归档。

关键词： RAG · 工作流 · 权限控制 · Trace / Replay

善用模型、工具与 AI 使用强度

模型	DeepSeek、Claude、ChatGPT、Qwen / DashScope；关注国产模型私有化、API 调用、长上下文、工具和成本
工具	Cursor、v0、Bolt、Codex、OpenClaw、Hermes、Dify、GitHub、Notion；用于 PRD、原型、代码、调试、部署和知识库。
使用方式	AI 已成为主要工作界面：每天用于产品拆解、架构推演、提示词工程、代码阅读、原型生成、Demo 修正和面试材料准备，学习的主要工具。
量化口径	AI 使用强度：近 30 天累计 Token 消耗约 200M–400M；日均 AI Coding / AI 产品设计时间 6–10 小时；累计完成 10–15 个 AI 产品原型 / 蓝图 / Demo；月度 API 调用约 8,000–20,000 次，覆盖主流工具链。

商业化 / 真实经营验证

跨境电商创业	从 0 到 1 操盘美区 TikTok 与独立站，跑通选品、内容种草、流量转化和用户反馈闭环。
工商业分布式光伏投资开发	股东身份参与项目获取、收益测算、合同协同和日常管理，具备真实产业项目开发和经营参与经验。
开源 Agent 内容产品化	OpenClaw / Hermes 部署教程形成百万级传播和真实用户反馈，可作为教程包、服务包和社群产品的商业化基础。
企业 AI 原型 / 解决方案	合同解析、知识库、质检、FDE Workbench、TokenRadar 等处于原型验证与试商业化阶段

核心能力

复杂业务抽象能力 基于 15 年地产、工程、投资、运营与新能源项目经验，熟悉业务流、审批流、合同流、资金流和风控流，能够从复杂组织中识别 AI 可介入的任务链、风险节点、确认节点和数据节点。	**Agent Harness 产品化** Agent Loop、Tool Use、MCP、Memory、Planning、Context Engineering、Human-in-the-loop、Trace/Replay、Evaluation。
AI 原生原型 使用 Cursor / v0 / Bolt / Codex 快速完成 PRD、交互、Demo、技术方案与交付说明，能和工程师讨论数据结构、状态机、权限等	**用户反馈与评估** 关注任务成功率、失败分类、用户接管率、成本可观测、反馈进入评估集和模型与 Harness 协同迭代。
通用素能：具备系统拆解、高速学习迁移、一线用户问题感、跨角色翻译和早期产品 Owner 意识。长期处理多角色、多流程、多约束的复杂组织问题，能够将模糊目标拆解为任务链、状态节点、风险边界和验收标准；2023 年后主动完成从产业管理到 AI 产品与 Agent 方向的能力迁移，习惯用原型、真实反馈和评估指标验证产品判断。	

教育背景与关键词

教育	西安理工大学 | 工程管理 | 硕士研究生 | 2009.09 - 2012.06；西安理工大学 | 土木工程 | 本科 | 2005.10 - 2009.06；混沌创商院 | 2023.03。
关键词	Agent Harness | 桌面端 Agent | Coding Agent | OpenClaw | Hermes | Cursor | v0 | Codex | DeepSeek | Qwen | RAG | OCR / ASR | Tool Use | MCP | Context Engineering | Human-in-the-loop | Trace / Replay | Token Observability | AI FinOps | 企业 AI 应用落地 | 复杂组织流程 | 合同风控 | 新能源数字化