M3 · 职业版 Agent · 课程设计

Agent 工程实战 · 职业版

8 讲、3 周、可评测可上线

面向开发者与产品经理

产出：工作流 + 评测集 + 权限清单

复用通识版 3 讲

本节目录

一、课程定位

二、8 讲结构

三、每讲固定结构

四、验收标准

五、排期

六、复用与新增

七、售卖方式

八、风险

九、当前状态与试学

一、课程定位

项目	设定
课程名	Agent 工程实战（职业版）
规模	8 讲，3 周
人群	开发者、产品经理、自动化负责人
前置	会基础 Python 或 API 调用；看过通识版第 7–9 讲更佳
产出	1 个可运行工作流 + 1 套评测集 + 1 份权限清单

状态：8 讲已全部完成（2026-11-20），待试学。

与通识版的区别：通识版讲“Agent 是什么、怎么搭一个”，职业版讲“怎么让它稳定、可评测、可上线”。

二、8 讲结构

讲	主题	当讲产出	来源
1	Agent 架构与边界	一张架构图	升级第 7 讲
2	工具调用与记忆	三个工具 + 记忆策略	新增
3	评测与验证	20 条评测集	新增（样课已出）
4	常驻 Agent 与成本	成本表 + 限流规则	新增
5	企业级 Agent OS	权限与队列设计	新增
6	多智能体编排	一张协作流程图	新增
7	权限、安全与日志	风险清单 + 审计字段	新增
8	项目：可运行工作流	工作流 + 演示 + 复盘	新增

三、每讲固定结构

1. 一个真实故障（不是成功案例）；

2. 三个工程判断；

3. 一次可复现的演示；

4. 30–45 分钟练习；

5. 验收清单；

6. 上线与成本提示。

四、验收标准

维度	标准
正确性	评测集通过率 ⩾ 80%
稳定性	连续 20 次运行无崩溃
可观测	每步有日志，失败可定位
安全	最小权限、敏感动作需确认
成本	单任务成本可计算、有上限

五项全过才算“可上线”。

五、排期

周	内容	里程碑
W1	第 1–3 讲	架构图 + 工具 + 评测集
W2	第 4–6 讲	成本表 + 权限 + 编排图
W3	第 7–8 讲	审计 + 可运行工作流

六、复用与新增

- 复用：通识版第 7 讲（Agent 边界）、第 8 讲（搭第一个）、第 9 讲（知识库问答）。
- 新增：评测、常驻与成本、企业级架构、多智能体、权限审计、项目课。
- 与视频课共享：验收表方法、报价与交付结构。

七、售卖方式

版本	内容	适合
自学版	8 讲讲义 + 模板	个人开发者
团队版	8 讲 + 内训 + 案例改造	企业团队
陪跑版	8 讲 + 2 次评审	正在落地的团队

先卖团队版：Agent 的付费方通常是公司，不是个人。

八、风险

风险	对策
平台差异大	讲架构与评测，不绑定单一平台
成本不可控	每讲都算一次单任务成本
安全事件	权限清单与人工确认作为硬性交付
案例涉密	全部用合成数据演示

九、当前状态与试学

1. 8 讲已全部完成（第 1–8 讲，第 3 讲为首发样课）；
2. 与视频课共用一套试学流程：3 人、7 天、评分表 + 问卷；
3. 试学后决定先卖哪一门：视频课面向创作者，Agent 课面向团队。