这是一个为你准备的详细 PPT 大纲。你可以直接将这些内容复制到 PowerPoint 中，或者使用 Markdown 转 PPT 的工具（如 Gamma, MindShow 等）快速生成。

这份 PPT 的逻辑流向是：背景挑战 -> 整体架构 -> 核心技术细节（**Embedding & 存储**） -> **Agent** 运作机制 -> 前端可视化方案 -> 落地计划。

PPT 主题：基于 Agent 与知识图谱的下一代资金风控系统设计

Slide 1: 封面

标题：下一代资金风控系统架构设计
副标题：结合 LLM Agent、RAG 与 知识图谱的可视化研判平台
汇报人：[你的名字/角色]
日期：2026年1月

Slide 2: 当前痛点与系统目标

核心痛点：

- 黑话难以识别：传统模型无法理解“跑分”、“凯子”、“U盾”等黑产专用术语。
- 关联隐蔽性强：资金链路层层拆分，难以通过单一规则发现团伙特征。
- 专家经验难以复用：资深专家的研判逻辑（SOP）停留在人脑或文档中，新人无法快速传承。

建设目标：

- 知识结构化：将非结构化专家文档转化为可检索向量与图谱。
- 研判自动化：利用 Agent 模拟专家思维链（CoT）进行辅助定性。
- 交互可视化：提供“图谱+列表”双视图，提升人工复核效率。

Slide 3: 整体技术架构 (High-Level Architecture)

(建议在此处插入一张架构图)

架构分层：

1. 数据层 **(Data Layer)**：

    - 结构化数据：交易流水、账户信息（存入 Graph DB）。
    - 非结构化数据：专家SOP、黑产情报、处置工单（存入 Vector DB）。
2. 模型层 **(Model Layer)**：
    - Embedding：BGE-M3 (针对风控领域微调)。
    - LLM：通用大模型 + ReAct 框架。
3. 应用层 **(Application Layer)**：
    - Agent Core：意图识别、工具调用、思维链推理。
    - Frontend：AntV G6 图可视 + 知识库表格可视。

Slide 4: 核心技术 I - Embedding 选型与调优

挑战：通用模型不懂“风控黑话”。

选型策略：强基座 + 领域微调

- 基座模型：**BAAI/bge-m3**
    - 优势：支持多语言（跨境风控）、支持长文本、支持稠密+稀疏双重检索（关键词+语义并重）。
- 微调方案 **(Fine-tuning)**：
    - 数据构造：构建 <Query, Positive, Negative> 三元组。
    - *Query*：“账户深夜小额高频转账”
    - *Positive*：“命中跑分洗钱特征，关联地下钱庄”
    - *Negative*：“用户海外商旅正常消费”

Slide 5: 核心技术 II - 专家经验的混合存储

理念：向量解决“是什么”，图谱解决“关联谁”。

存储结构设计：

1. **Vector DB (Milvus/ES)**：
    - 存储内容：黑产画像描述、专家分析报告全文。
    - 作用：回答 RAG 语义提问（如“这种手法以前出现过吗？”）。
2. **Graph DB (Neo4j/Nebula)**：
    - 存储内容：账户 -> IP -> 设备 -> 黑产团伙。
    - 作用：发现深层关联，支撑可视化渲染。
3. **Timeline Store**：
    - 存储内容：专家研判步骤序列 (JSON)。
    - 作用：指导 Agent 学习标准的分析步骤。

Slide 6: Agent 运作机制 - ReAct 范式

Agent 如何像专家一样思考？

工作流 **(Workflow)**：

1. 感知 **(Observation)**：接收警报，如“账户 A 突发异常交易”。
2. 思考 **(Thought - CoT)**：
   - “我需要先查一下它的关联环境。”
   - “环境有异常，我需要检索知识库看看像哪种攻击。”
3. 行动 **(Action - Tools)**：
   - 调用 get_graph_relation() 获取图谱。
   - 调用 search_knowledge_base() 检索相似案例。
4. 响应 **(Response)**：
   - 输出定性结论：“疑似杀猪盘资金归集”。
   - 输出依据：引用召回的 Knowledge ID。

Slide 7: 前端可视化交互设计 (UI/UX)

设计理念：宏观链路与微观证据的自由切换。

双视图模式 **(Dual-View Mode)**：

- 视图 **A**：风险关联图谱 **(Graph View)**
  - 技术栈：AntV G6。
  - 功能：展示资金流向、团伙挖掘、红黑节点高亮。
  - 场景：用于判断案件的波及范围和团伙规模。
- 视图 **B**：知识库证据列表 **(Table View)**
  - 技术栈：HTML/React Table。
  - 功能：展示 RAG 召回的 Top-N 相似案例、SOP 文档、匹配度得分。
  - 场景：用于确认 Agent 定性的理论依据。

Slide 8: 案例演示 - 针对“跑分洗钱”的研判

(此处可以放置生成的 HTML 截图)

场景复盘：

1. 输入：账号 123 凌晨突发 50 笔快进快出交易。
2. **Agent** 动作：
   - 检索图谱 -> 发现共用 IP 关联已知黑产团伙。
   - 检索向量 -> 命中“休眠户突发交易”SOP 文档。
3. 系统输出：

- 左侧：渲染出该账号与黑产团伙的连接图。
- 右侧：列出《休眠账户处置规范》原文，并高亮匹配条款。
- 结论：建议“只收不付”。

Slide 9: 实施路线图 (Roadmap)

Phase 1: 知识工程 **(M0-M1)**

- 收集历史工单、SOP文档。
- 清洗数据，设计 Graph Schema。

Phase 2: 模型构建 **(M2-M3)**

- BGE-M3 模型微调。
- 搭建 RAG 检索链路与 Agent Tool 接口。

Phase 3: 系统集成 **(M4-M5)**

- 开发前端可视化工作台 (Graph + Table)。
- 专家介入进行 RLHF (反馈优化 Agent 回答)。

Slide 10: 总结与展望

核心价值：

- 提效：初级分析师借助 Agent 达到中级专家水平。
- 沉淀：将流动的专家经验固化为企业的数字资产。
- 精准：通过图谱+语义的双重校验，降低误报率。

Q&A

💡 演讲建议 **(Speaker Notes)**：

1. 在讲 **Slide 4 (Embedding)** 时：强调为什么要微调。可以举例子：“通用模型觉得‘买茶叶’是购物，但在我们风控场景，特定的语境下‘买茶叶’可能是欺诈话术。只有微调能解决这个问题。”
2. 在讲 **Slide 7 (前端)** 时：强调“可解释性”。告诉听众，我们不仅给结果，还把 Agent 查到的“文档原文”摆在桌面上（表格视图），这让业务人员敢用、敢信。
3. 在讲 **Slide 8 (案例)** 时：直接把之前生成的 HTML Demo 打开展示，动态切换一下图谱和表格，效果会非常震撼。