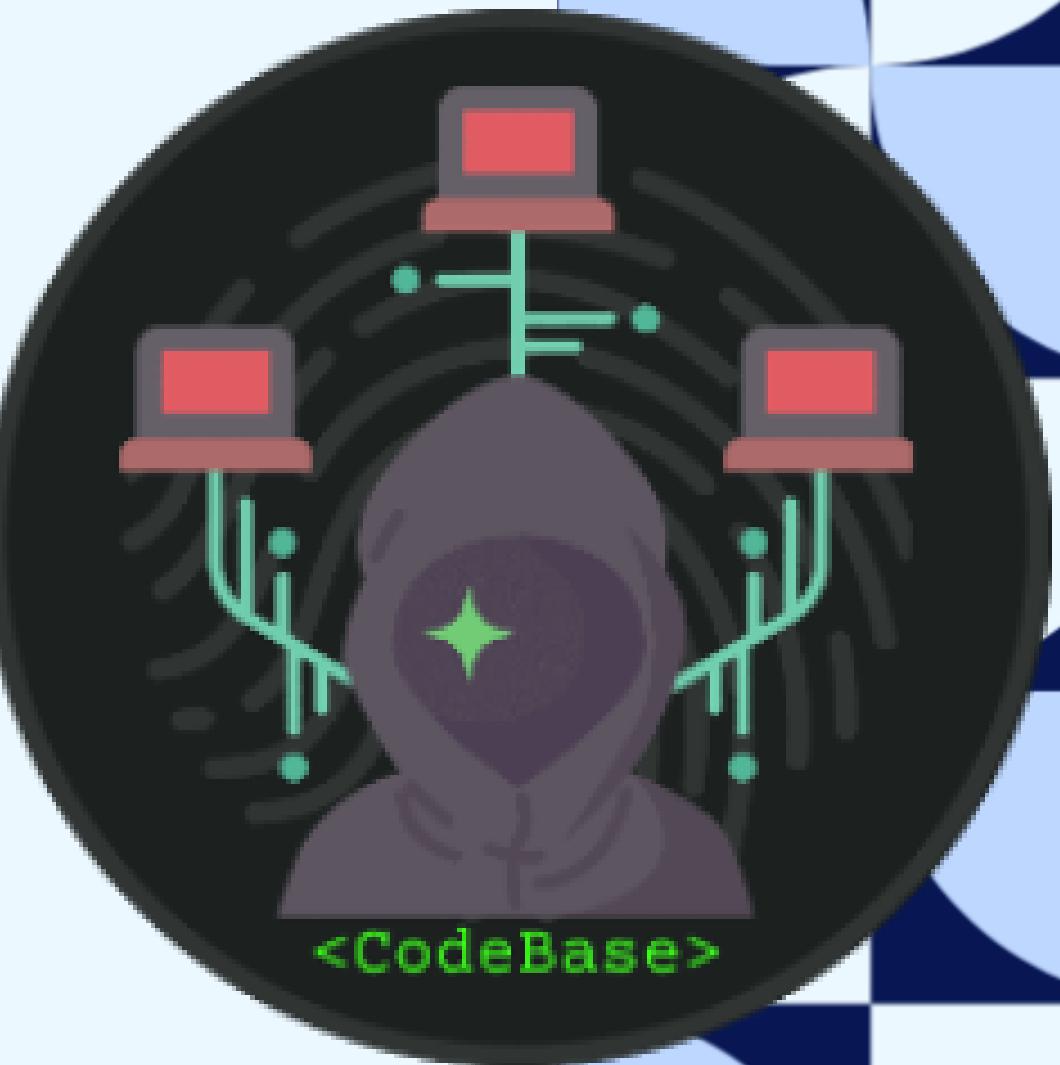
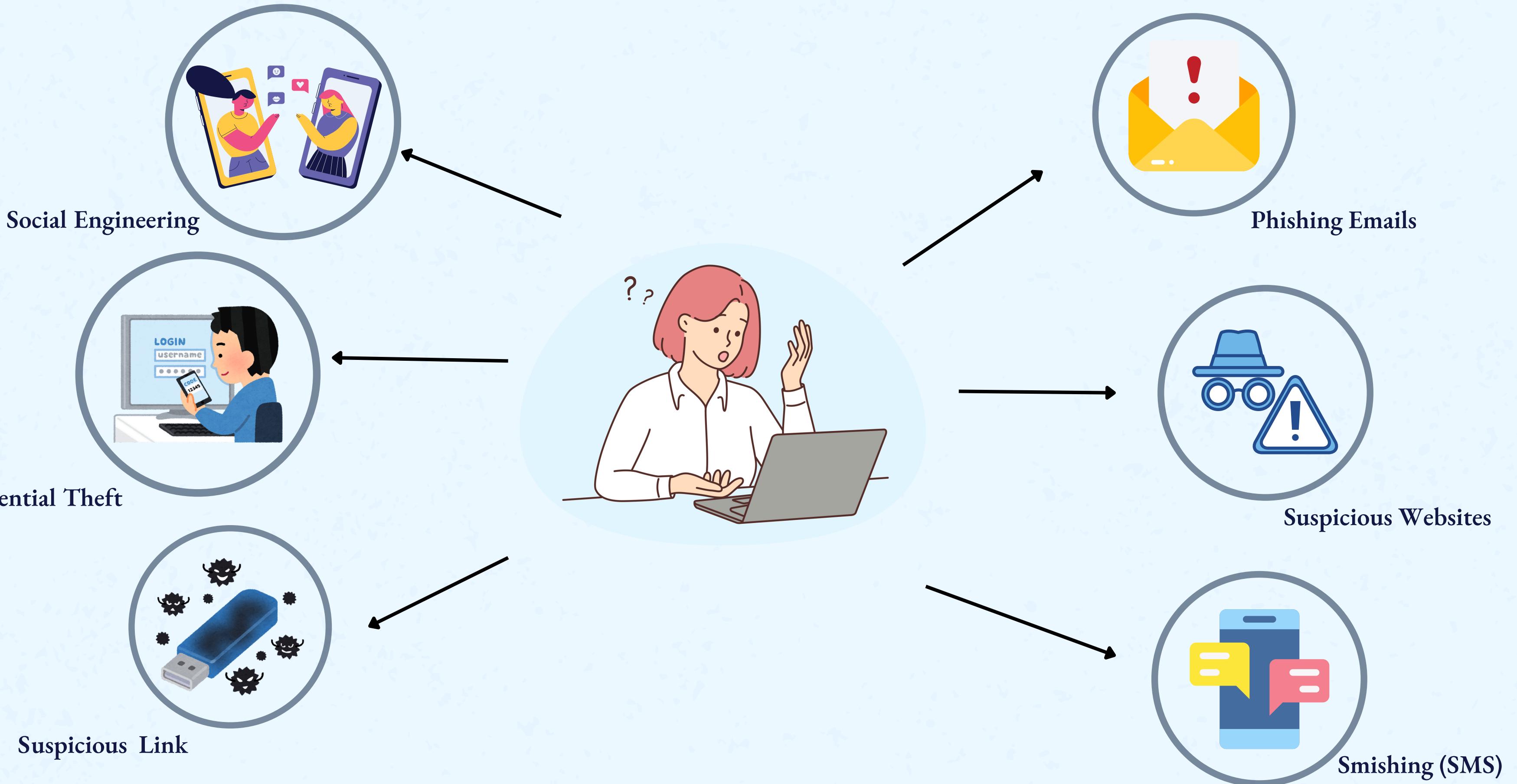


Smart India Hackathon

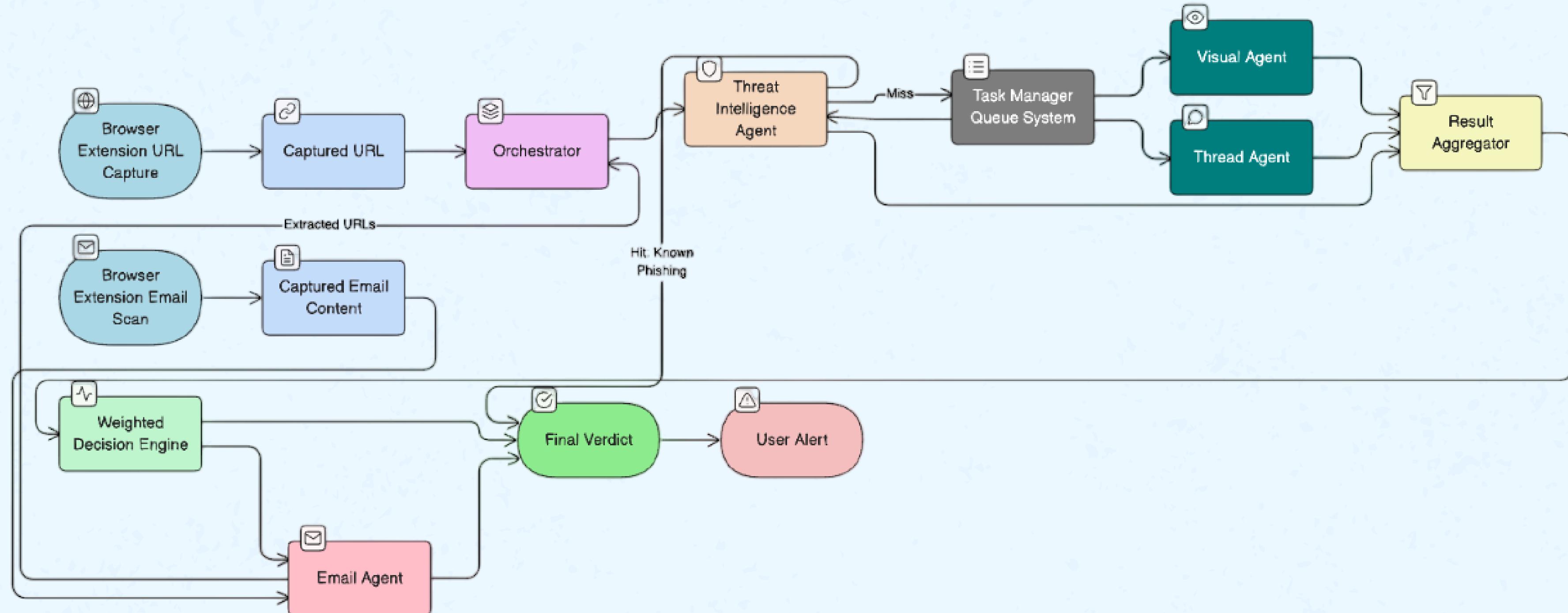
- Problem Statement ID: 25154
- Problem Statement Title: Real-Time AI/ML Based Phishing Detection and Prevention System
- Team Name: CodeBase



Visual Representation of Problem



Overall Workflow of Solution



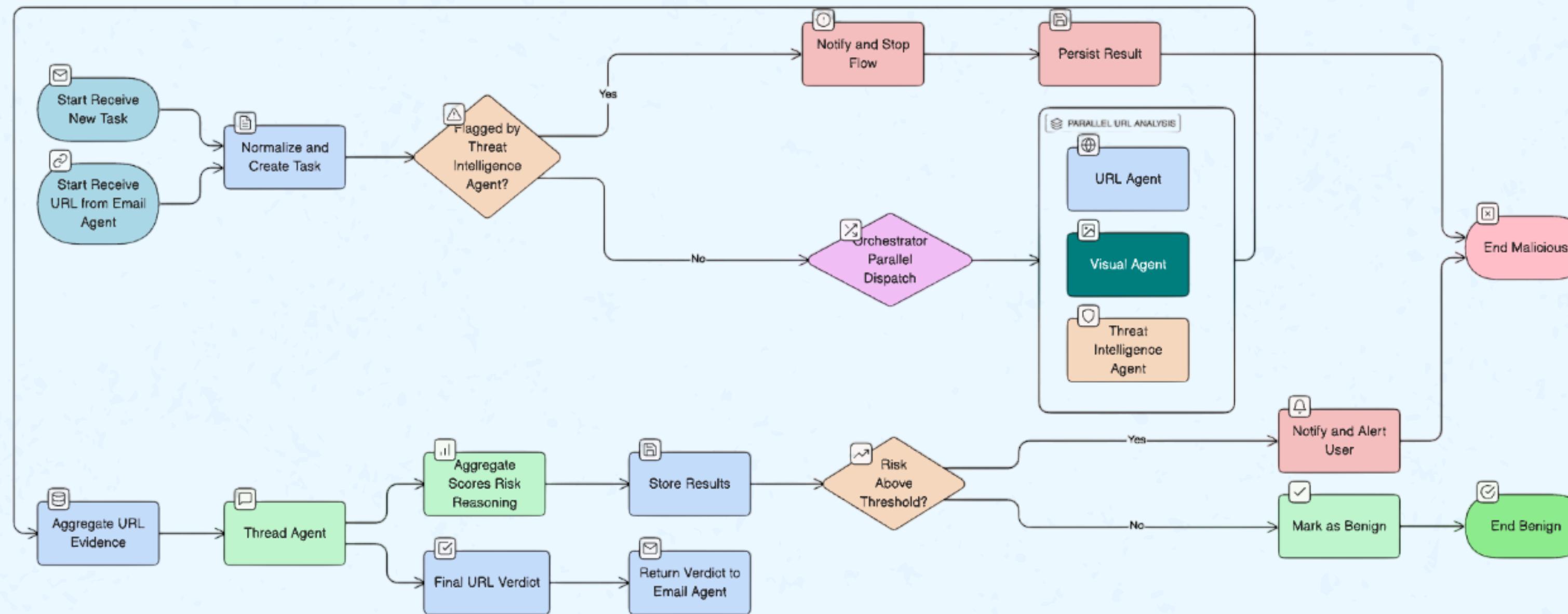
Multi Agent Analysis

1. Orchestrator Agent
2. Threat Intelligence Agent
3. URL Agent
4. Visual Agent
5. Thread Agent
6. Email Agent

Orchestrator Agent

- The central controller that dispatches tasks to all agents in parallel.
- Aggregates their outputs, applies risk thresholds, and decides whether to stop, alert, or mark as safe.

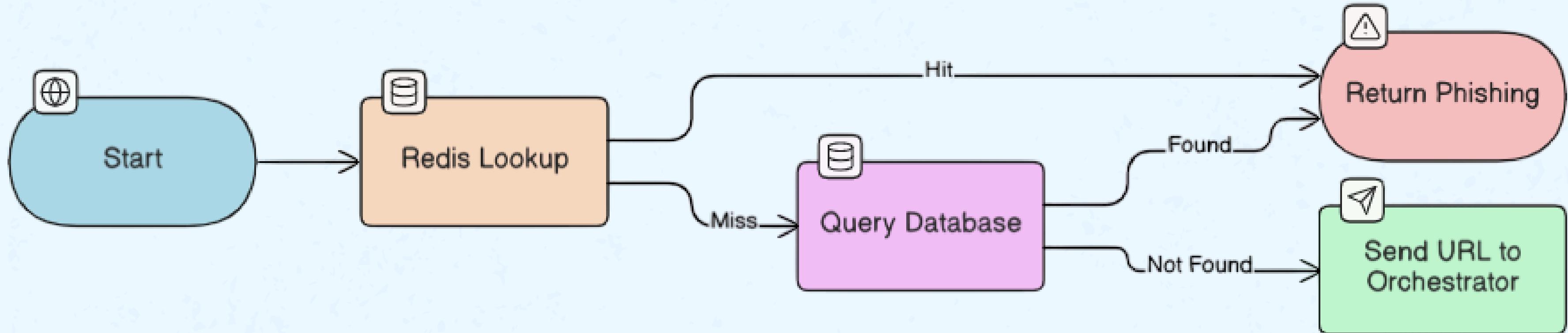
Flowchart



Threat Intelligence Agent

- Quickly checks if a URL is already known as phishing or safe using stored intelligence.
- If unknown, forwards the URL for deeper analysis by other agents.

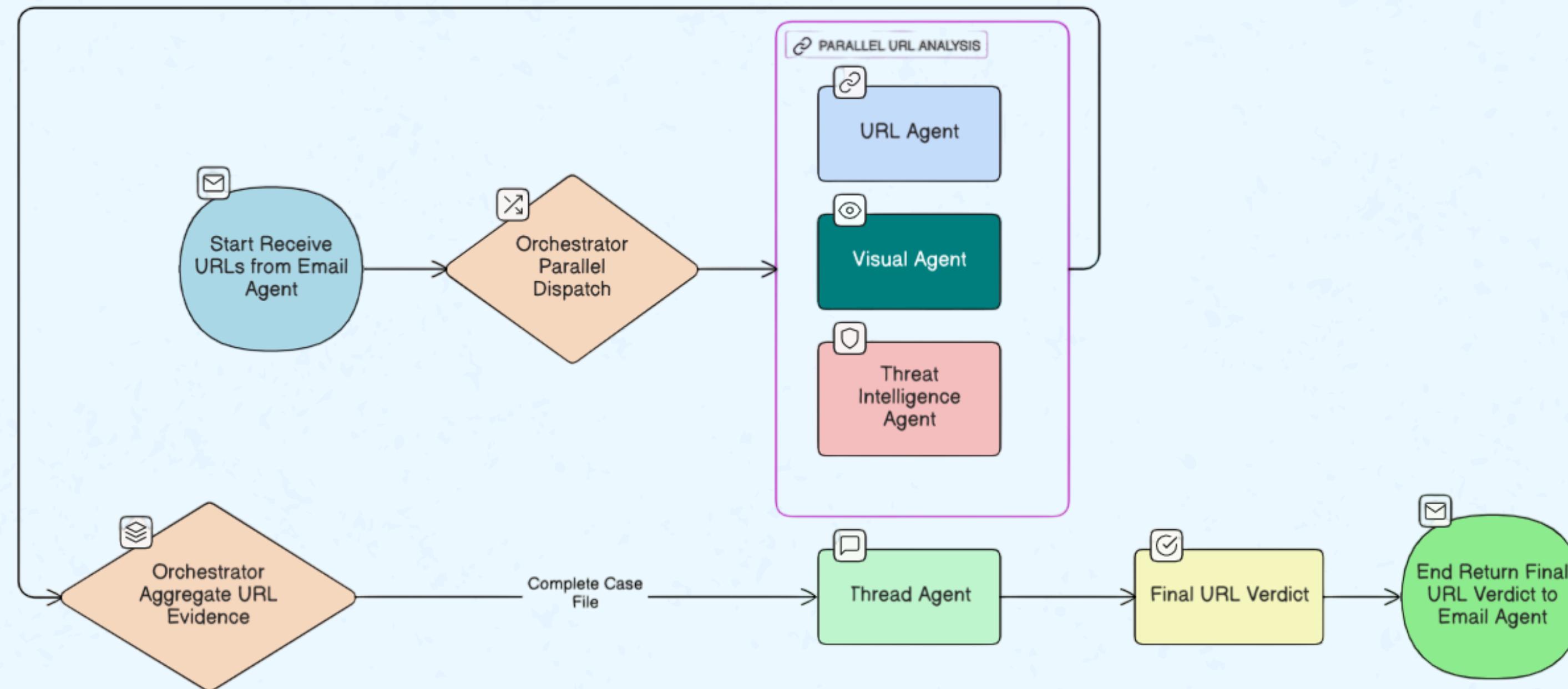
Flowchart



URL Agent

- Performs direct analysis of the URL by extracting lexical, domain, certificate, and page-content features.
- Combines these signals into a classification verdict with score and reasoning, which is later aggregated by the orchestrator.

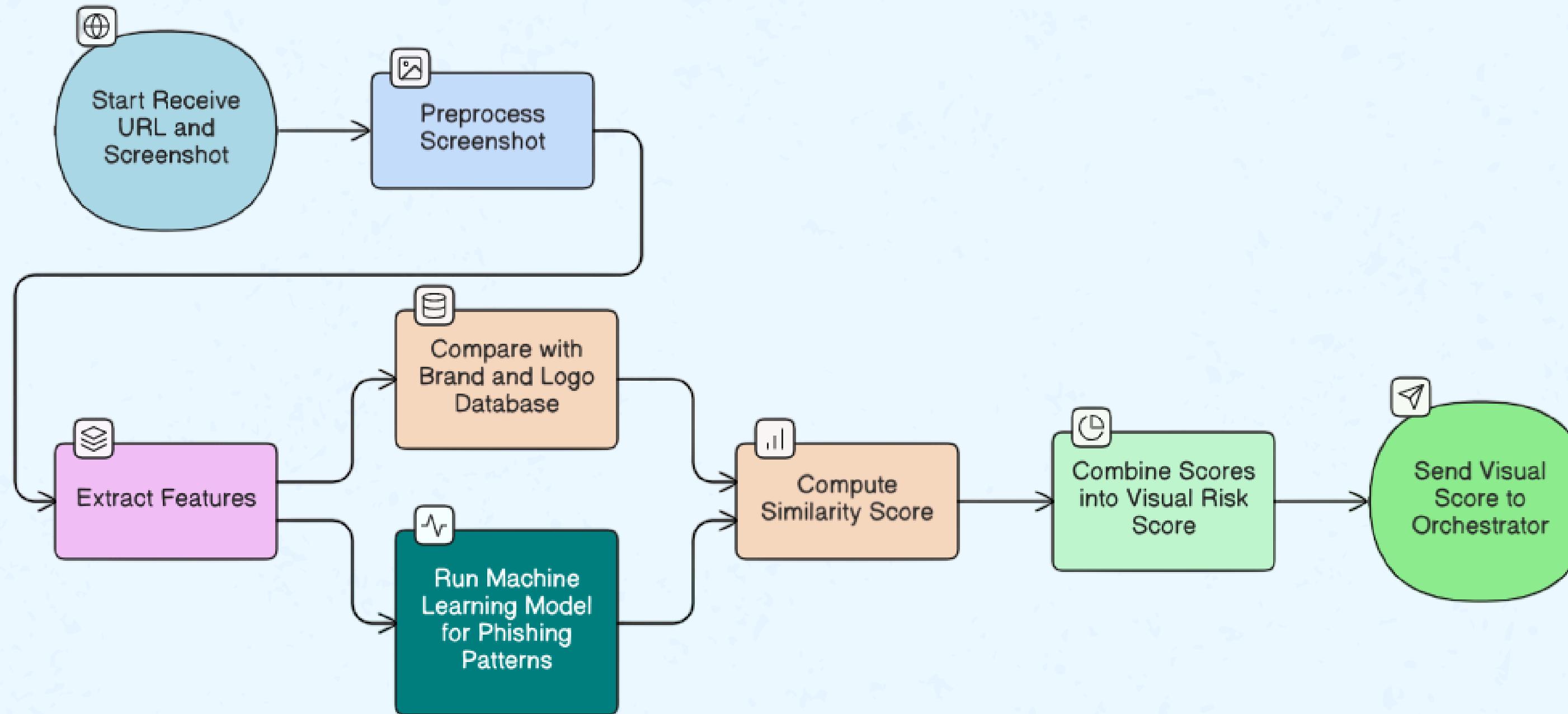
Flowchart



Visual Agent

- Analyzes webpage screenshots to detect brand impersonation and phishing patterns.
- Generates a visual risk score by combining similarity checks and ML-based detections.

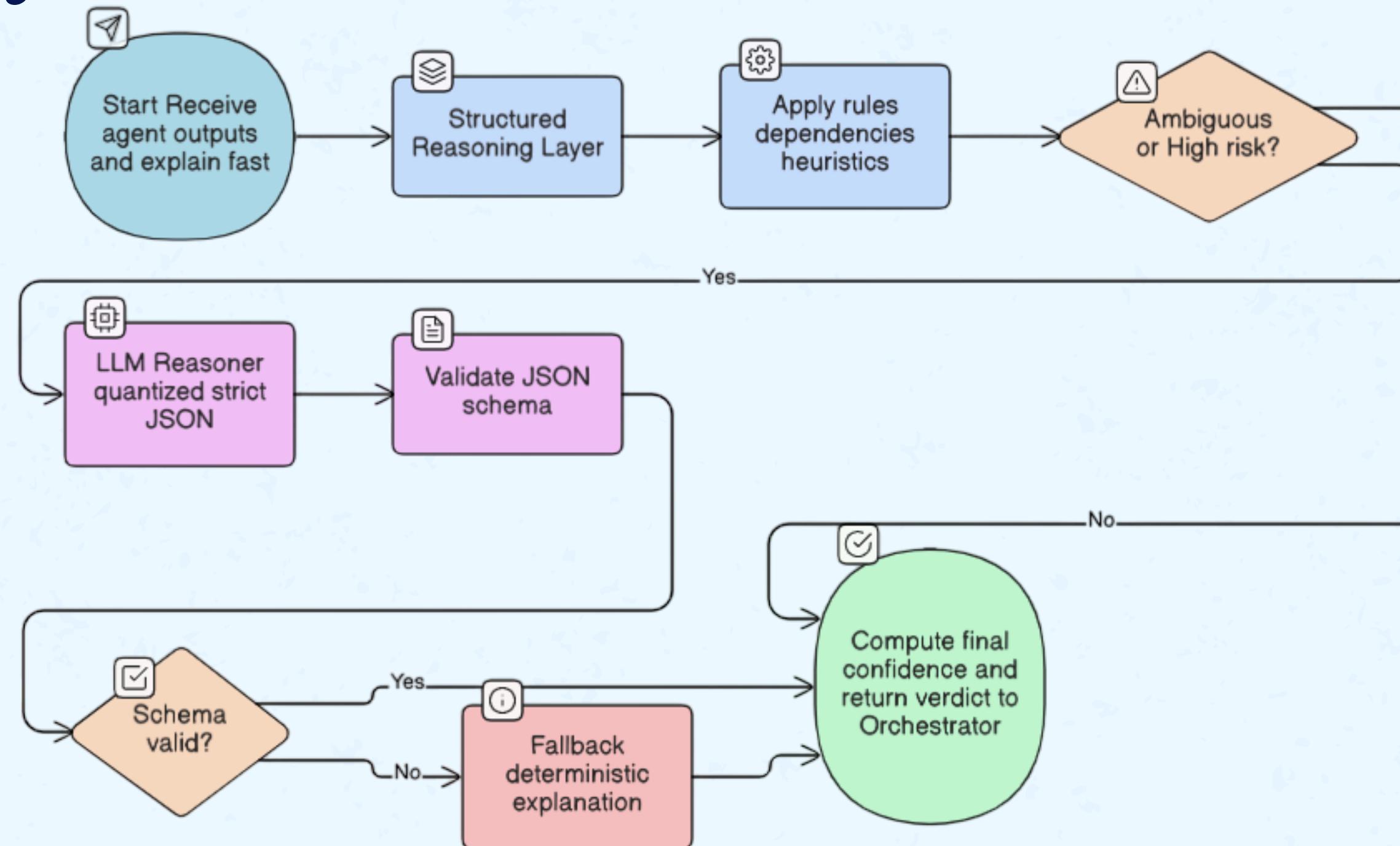
Flowchart



Thread Agent

- Aggregates and reasons over outputs from all agents, applying rules and heuristics for consistency.
- Handles ambiguous or high-risk cases with deeper reasoning before finalizing the verdict.

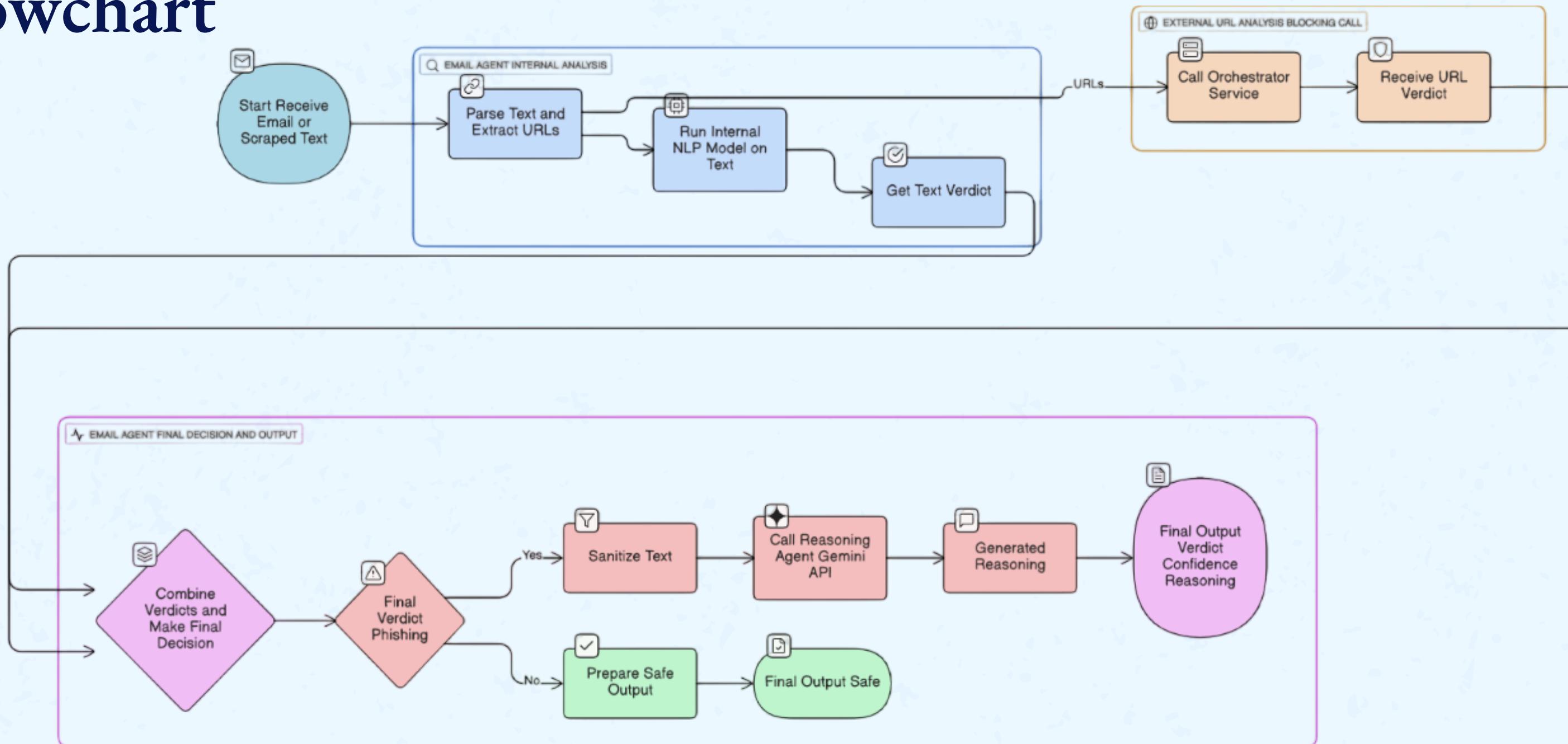
Flowchart



Email Agent

- Parses email text to extract URLs and applies internal analysis (NLP-based) for phishing detection.
- Combines internal verdict with URL analysis, then outputs a final decision with reasoning or marks as safe.

Flowchart



Scalability



- Modular multi-agent design enables independent scaling of each agent.
- Cloud-native deployment supports elastic scaling under high phishing traffic.
- Asynchronous task queues ensure efficient parallel processing.
- Extensible architecture for easy integration with enterprise systems.
- Real-time parallel analysis minimizes latency even as traffic grows.

GitHub Repos



MVP Link

**THANK
YOU**

