
Algorithmic Trading System
Security & Compliance
3 preventive | 0 detective
L5 — Evaluation and Observability
Portfolio Manager (Human)
human-in-the-loop · reactive
C2 H11 M9
L3 — Agent Frameworks
Order Execution Router
task-oriented · reactive
C7 H16 M11
L1 — Foundation Models
CL-prompt-to-leak (2 layers)
CL-poison-and-pivot (2 layers)
Algo Trading Agent
task-oriented · self-modifying
C19 H19 M17
Risk Oversight Agent
task-oriented · deliberative
C12 H21 M16
Compliance Agent
task-oriented · deliberative
C13 H16 M15
CL-vertical-full: Adversarial input -> poisoned model -> data exfil -> infra pivot -> log cover -> impersonation
T-CL-006: Cascade Failure Propagation
T-CL-005: Goal Misalignment Cascade
T-CL-003: Cross-Layer Privilege Escalation