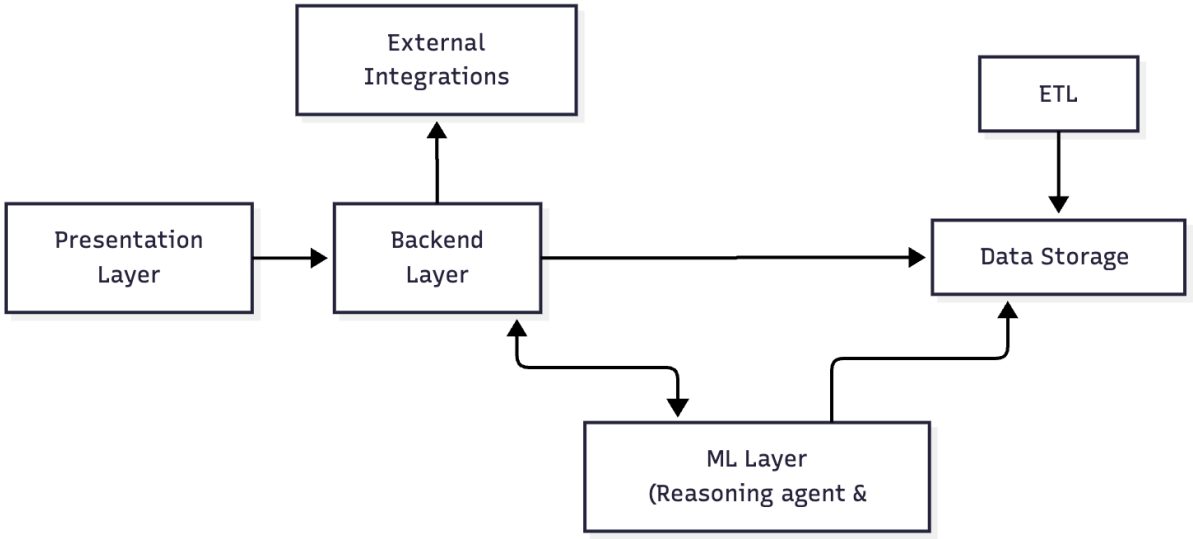
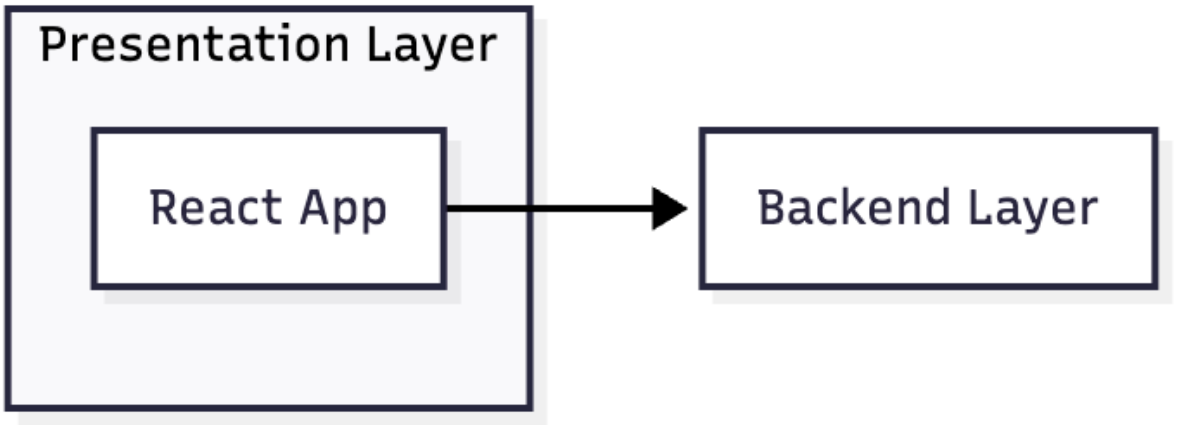
AI Agent for Network Intrusion Detection & Response - Diagrams backbone

High-level diagram:

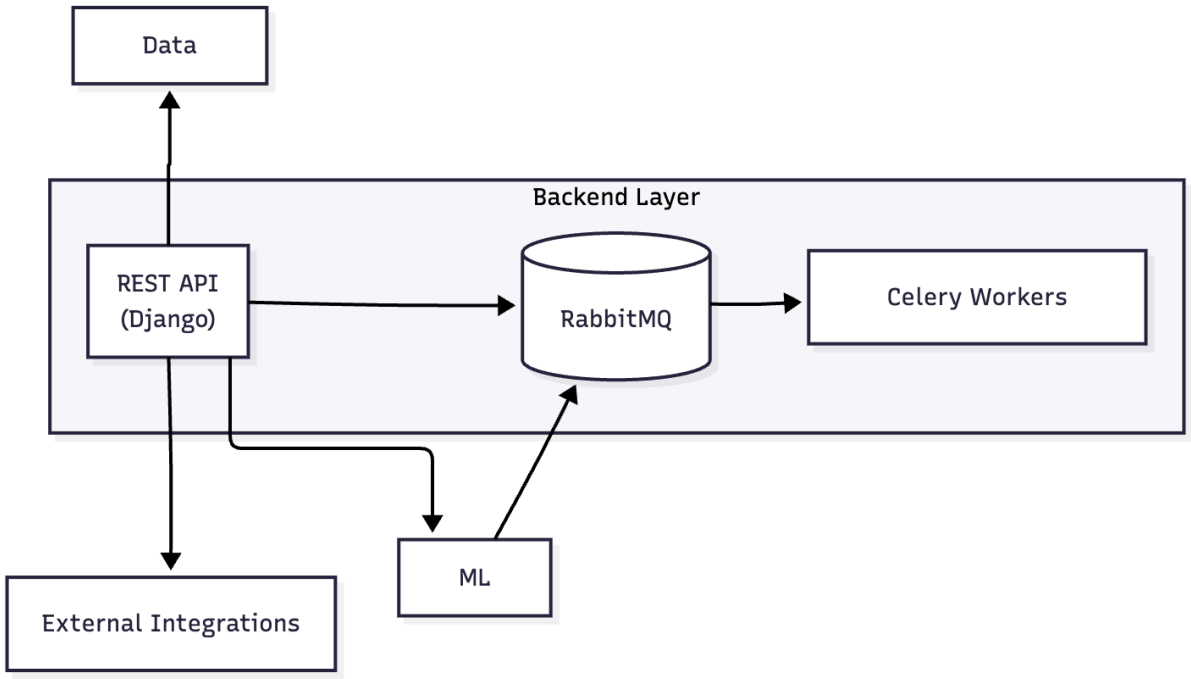


Presentation Layer Diagram:



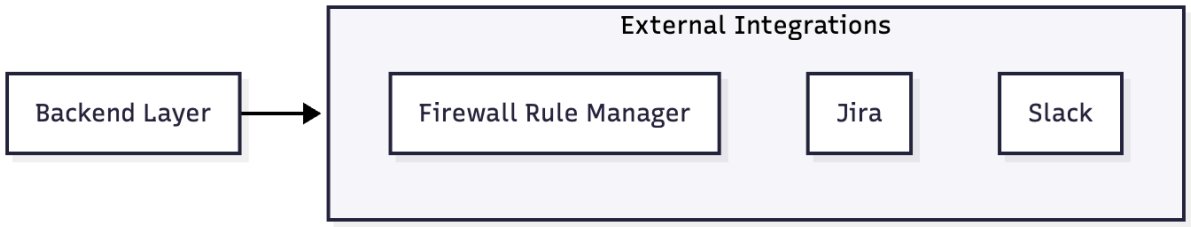
- **React App** → A TypeScript-based frontend. It visualizes alerts, system health, incident timelines, dashboards, and agent decisions.

Backend Layer Diagram:



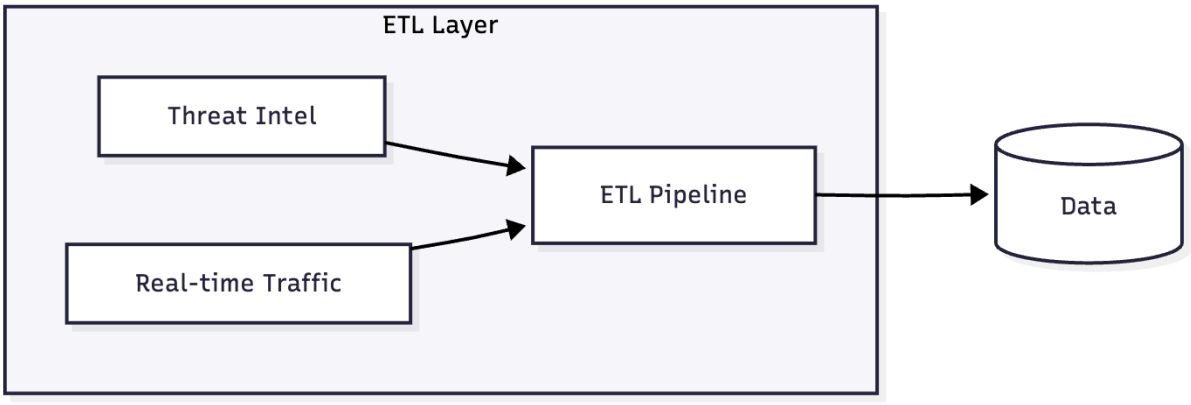
- **REST API (Django)** → Authentication, endpoints, business logic, incident submission, data retrieval, and on-request triggers to AI models.
- **RabbitMQ (Message Broker)** → Decouples API from long-running processes.
- **Celery Workers** → Trigger external integrations.

External Integrations Diagram:



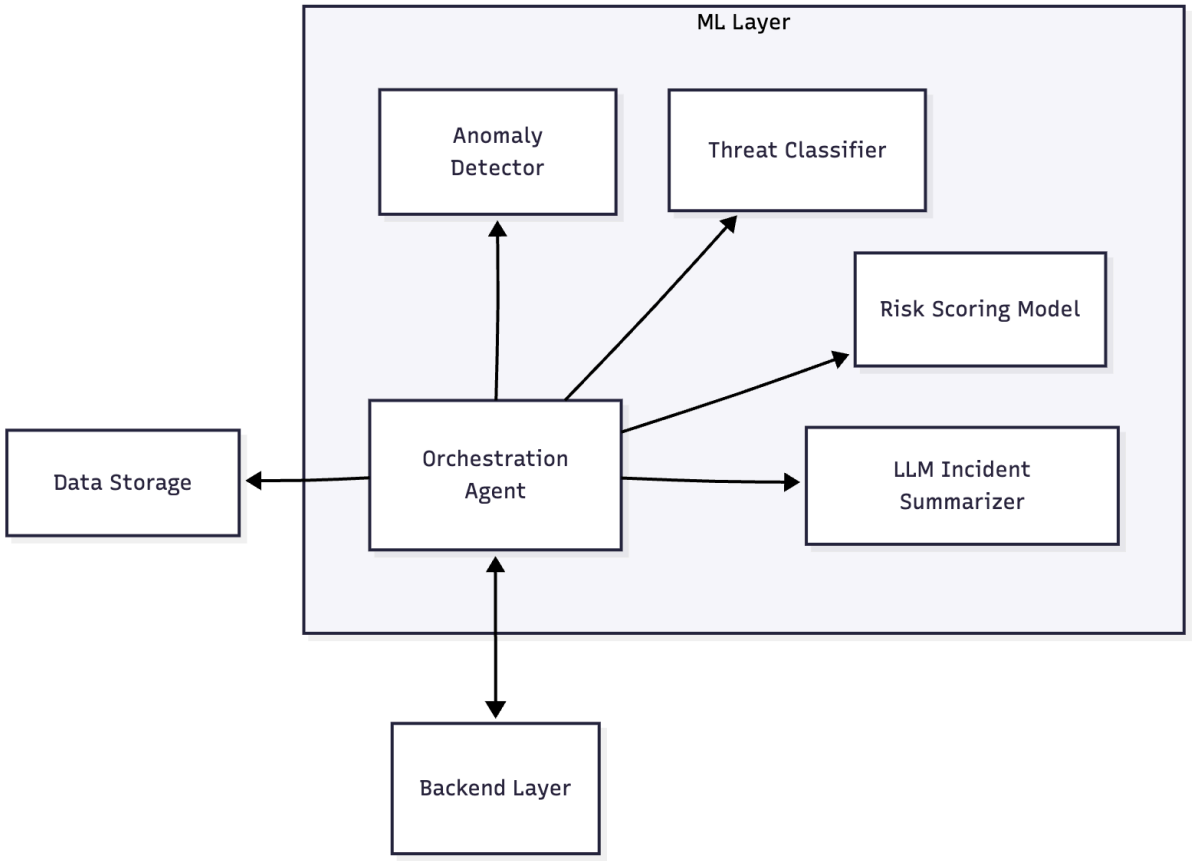
- **Firewall Rule Manager** → Used by the agent to automatically block or unblock IPs. Acts as the active defense layer.
- **Jira Integration** → Creates incident tickets with context produced by the agent.
- **Slack Integration** → Sends real-time alert notifications.

ETL Layer Diagram:



- **Threat Intelligence Source** → Feeds IP reputation and domain scores.
- **Real-Time Traffic Simulation** → Simulated packet/flow-level telemetry.
- **ETL Pipeline** → performs:
    - normalization
    - feature extraction
    - enrichment with threat intel
    - writes to the vectorial database

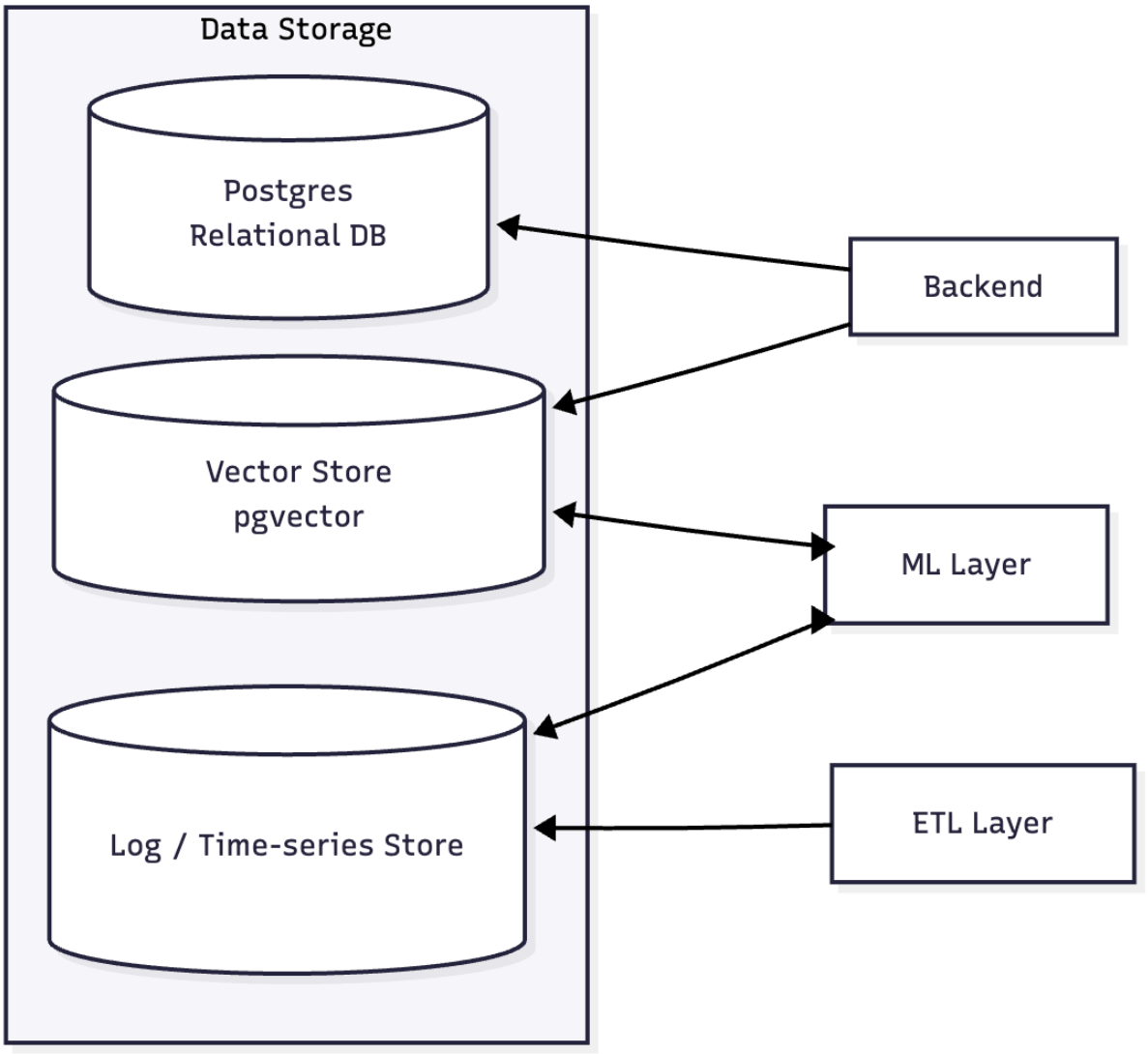
ML Layer Diagram:



- **Orchestration Agent** → the “brain”:
  - calls other models
  - retrieves data from storage
  - calculates severity
  - selects response actions
  - returns decisions to the backend via the messaging queue

- **Anomaly Detector** → Flags unusual flows. (Supervised: Model: ??)
- **Threat Classifier** → Model that assigns attack types: DDoS, Port Scan, Brute Force. (Supervised: ANN)
- **Risk Scoring Model** → Computes the risk based on threat classification and context (Supervised: Regression?)
- **LLM Incident Summarizer** → summarizes incidents in a human-readable way for UI and Jira tickets and Slack messages

Data Storage Diagram:



- **Postgres (Relational DB):**
  - user accounts
  - Incidents
  - model outputs
  - agent decisions
- **Vector Store (pgvector):**
  - incident summaries
  - anomaly patterns
  - historical context for similarity search

- **Log / Time-Series Store:**
  - network traffic records
  - Internal platform activity.