



Revenue Incident Response Agent

Elastic Agent Builder Hackathon 2026 — Architecture Overview

AGENT PIPELINE (6-STEP AUTONOMOUS INVESTIGATION)



INTELLIGENCE ENGINES

Statistical Drift Detection

Z-score analysis comparing baseline vs current anomaly rates. Values exceeding $z > 3.0$ trigger investigation.

Confidence Scoring

$$C = S \times 0.4 + T \times 0.3 + D \times 0.2 + H \times 0.1$$

Weighted formula: Signal strength, Temporal alignment, Cross-signal validation, Historical deviation.

Deployment Recency

Exponential decay model correlating recent deployments with anomaly onset timing for causal inference.

TECH STACK

Elasticsearch 8.x

Node.js

Express.js

React 19

Vite

Chart.js

Lucide Icons

REST API

API ENDPOINTS (10 INTELLIGENCE ROUTES)

GET /api/health
GET /api/deployment-impact
GET /api/financial-loss
GET /api/timeline
GET /api/alerts

GET /api/anomalies
GET /api/risk-score
GET /api/business-impact
GET /api/services
GET /api/explainability

DATA ARCHITECTURE

Data Sources

- invoices (2,400+ records)
- system_events (deployments)
- transactions (payments)
- churn_events (retention)

Dual-Mode Operation

- Live Mode:** Elasticsearch queries
- Fallback:** JSON file analysis
- Transparent mode switching
- Zero data loss guarantee

Output

- Executive dashboard (React)
- Autonomous AI chat analyst
- Forensic reasoning trace
- Verifiable confidence scores