Interactive Cyber Threat Analysis & Visualization Architecture
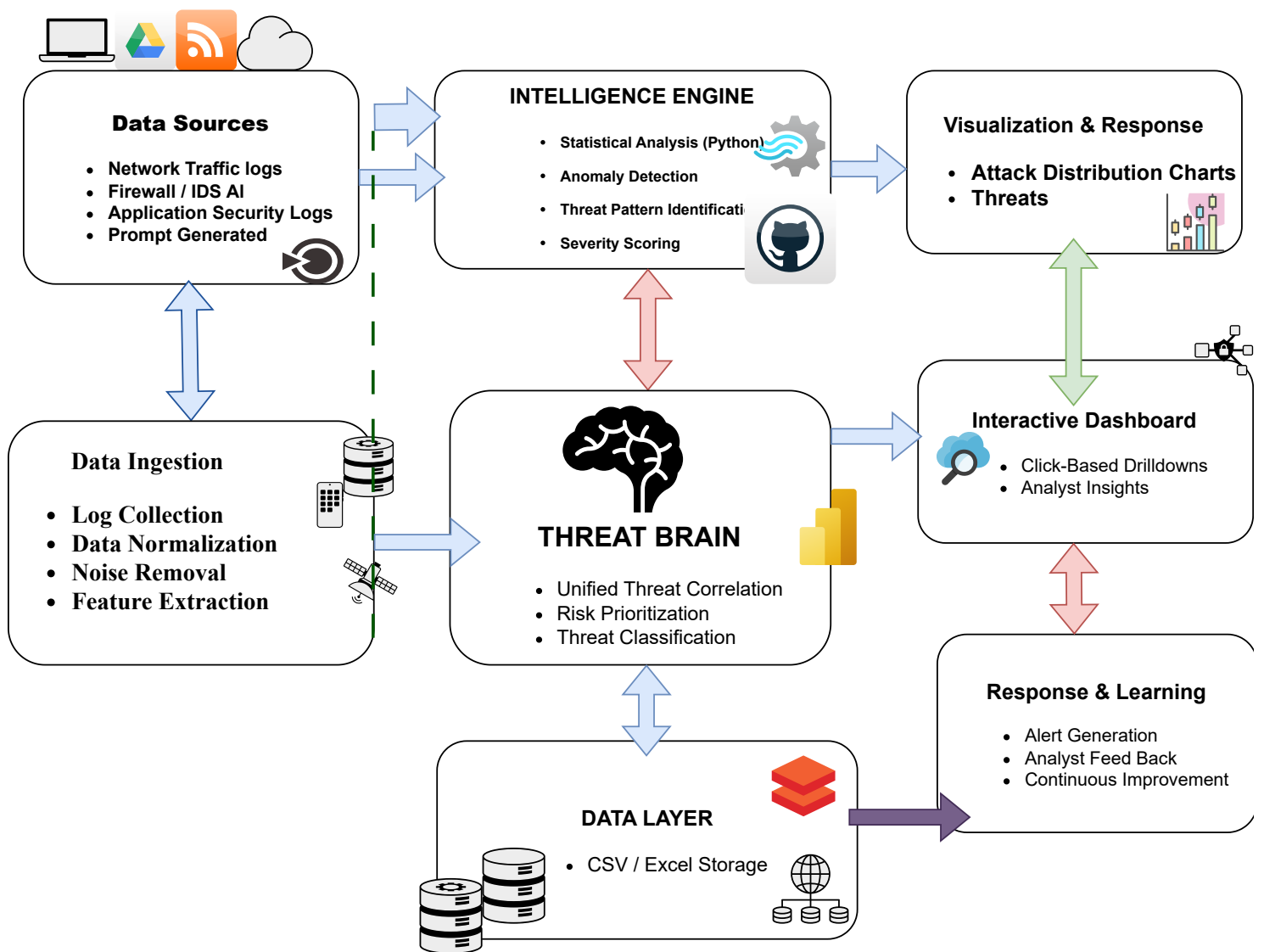

Data Sources

- Network Traffic logs
- Firewall / IDS AI
- Application Security Logs
- Prompt Generated

INTELLIGENCE ENGINE

- Statistical Analysis (Python)
- Anomaly Detection
- Threat Pattern Identification
- Severity Scoring

Visualization & Response

- Attack Distribution Charts
- Threats

Data Ingestion

- Log Collection
- Data Normalization
- Noise Removal
- Feature Extraction

THREAT BRAIN

- Unified Threat Correlation
- Risk Prioritization
- Threat Classification

Interactive Dashboard

- Click-Based Drilldowns
- Analyst Insights

DATA LAYER

- CSV / Excel Storage

Response & Learning

- Alert Generation
- Analyst Feed Back
- Continuous Improvement