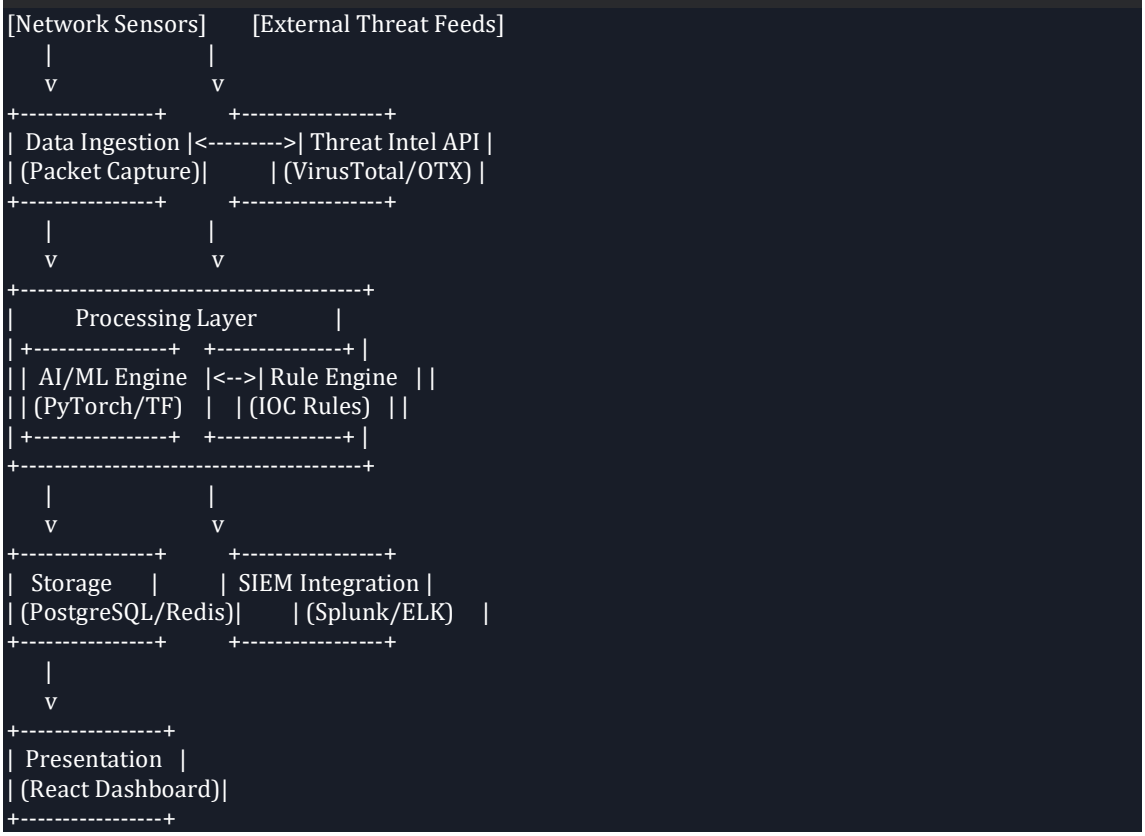
SecureFlow Architecture Diagram

System Overview



Component Breakdown

1. Data Ingestion Layer

- **Network Sensors**: PacketBeat, Zeek, custom PCAP collectors
- **Formats**: PCAP, NetFlow, IPFIX
- **Throughput**: 10Gbps capable

2. Processing Layer

Component	Technology	Function
AI/ML Engine	PyTorch, ONNX	Anomaly detection models
Rule Engine	CEL, YARA	Real-time IOC matching
API Service	FastAPI	REST/gRPC endpoints

3. Storage Layer

- **PostgreSQL**: Threat intelligence database
- **Redis**: Real-time alert caching
- **S3/MinIO**: PCAP archival

4. Integration Layer

- **SIEM Connectors**: Splunk HEC, Elasticsearch
- **Threat Feeds**: MISP, VirusTotal, AlienVault OTX
- **Notification**: SMTP, Slack, PagerDuty

Data Flow Sequence

1. **Collection**: Network traffic captured via sensors
2. **Normalization**: Convert to unified JSON format
3. **Analysis**:
    - Rule-based IOC matching
    - ML model inference (100ms latency)
4. **Storage**:
    - Alerts → PostgreSQL
    - Raw PCAP → S3
5. **Visualization**:
    - Real-time dashboard updates
    - SIEM alert forwarding

Security Controls

```mermaid
graph TD
  A[HTTPS Encryption] --> B[RBAC]
  B --> C[JWT Authentication]
  C --> D[Rate Limiting]
  D --> E[Input Validation]
  E --> F[Audit Logging]
```

Scalability Features

- **Horizontal Scaling**: API workers auto-scale to 100 instances
- **Model Serving**: Triton Inference Server
- **Stream Processing**: Kafka queues buffer traffic spikes

- **Geo-Distribution**: Multi-region deployment support