Technology Stack

Overview

The technology stack consists of various tools and frameworks required to build and deploy the real-time security intelligence system.

Key Components

1. **Data Collection** - Logstash, Kafka, Syslog, API Integrations.
2. **Data Processing** - Apache Spark, Elasticsearch, SIEM tools.
3. **AI & Machine Learning** - TensorFlow, PyTorch, Scikit-learn.
4. **Threat Intelligence** - Open Threat Exchange (OTX), STIX/TAXII.
5. **Automation & Orchestration** - Ansible, SOAR Platforms.
6. **Cloud & Infrastructure** - AWS, Azure, Kubernetes.
7. **Monitoring & Analytics** - Grafana, Kibana, Splunk.

Technology Integration

Each of these technologies plays a crucial role in ensuring real-time threat detection, data correlation, and automated responses.