

# Solution Architecture

## # Architecture Overview

The solution architecture consists of multiple layers working together to provide real-time security intelligence and automated threat response.

## # Components

1. **Data Ingestion Layer:** Collects logs, network data, and user activity.
2. **Threat Intelligence Engine:** Processes real-time threat feeds.
3. **AI-Based Anomaly Detection:** Uses machine learning for pattern recognition.
4. **SIEM Integration:** Correlates security events for analysis.
5. **Automated Response System:** Deploys actions such as isolating threats.

## # Workflow

- Data is collected from various sources (firewalls, endpoints, network logs).
- AI models analyze patterns and detect anomalies in real-time.
- Threat intelligence feeds provide context on new vulnerabilities.
- SIEM aggregates security events and provides alerts.
- Automated response triggers defensive measures against detected threats.