

Solution Requirements

Functional Requirements

1. **Real-Time Data Processing:** Ability to process security data in real-time.
2. **Threat Intelligence Integration:** Support for external threat intelligence feeds.
3. **AI-Based Threat Detection:** Machine learning models to identify anomalies.
4. **Automated Response Mechanisms:** System-triggered security actions.
5. **User Dashboards & Reports:** Real-time analytics and reporting.

Non-Functional Requirements

1. **Scalability:** Handle large volumes of security data.
2. **Security & Compliance:** Adhere to cybersecurity standards.
3. **High Availability:** Ensure minimal downtime and reliability.
4. **Integration Support:** Compatibility with existing security infrastructure.

System Constraints

- Should be cloud-compatible.
- Must support both structured and unstructured security data.
- Low-latency processing for real-time defense.