

## Technology Stack

### AI-Based Threat Intelligence Platform

Date: 23 August 2025  
Name :Mansi Chougule

---

#### Components s Technologies Used

S.No	Component	Description	Technology (Used)
1	User Interface	Analyst dashboard, search, KPIs, reports	<b>Streamlit</b> , Plotly
2	Data Collection	Fetching threat data from external API	<b>AlienVault OTX API</b> (via Python requests)
3	Database	Store collected threat indicators	<b>SQLite</b>
4	Data Preprocessing	Normalization C cleaning	<b>Pandas</b>
5	Data Analysis	Frequency counts, distribution, anomaly detection	<b>Pandas</b> , <b>scikit-learn</b> ( <b>IsolationForest</b> )
6	Visualization	Charts C maps for threats and trends	<b>Plotly Express</b>
7	Export	Download processed data	CSV export using Pandas

---

#### Application Characteristics

S.No	Characteristic	Implementation
1	Open-Source Frameworks	Streamlit, Pandas, Plotly, scikit-learn
2	Security	API key stored via environment variable (OTX API)
3	Data Scope	Threat feeds limited to AlienVault OTX (100 indicators per request)
4	Scalability	Prototype scale (local database, single API feed)
5	Features	Date range filter, KPIs, anomaly detection toggle, search, CSV export