Week 3 – Dashboard Development for Real-Time Threat Monitoring

Objectives:

- Convert model outputs and traffic logs into actionable visuals.
- Help security analysts detect patterns, anomalies, and threats faster.
- Create a usable dashboard using Python Dash/Plotly.

Deliverables Included:

1) cyber_dash_app.py (Dash app)
2) dashboard_data.csv (sample/refreshable dataset)
3) Four PNG screenshots of key visuals
4) This PDF report describing metrics and workflow

Metrics Visualized:

- Traffic by Protocol: Stacked counts of Benign vs Attack per protocol.
- Top Malicious IPs: Top 10 source IPs with most intrusion attempts.
- Detection Rates: Distribution of Benign vs Attack as a pie chart.
- Time-Series of Intrusions: Minute-resolution attack counts, highlighting peaks.

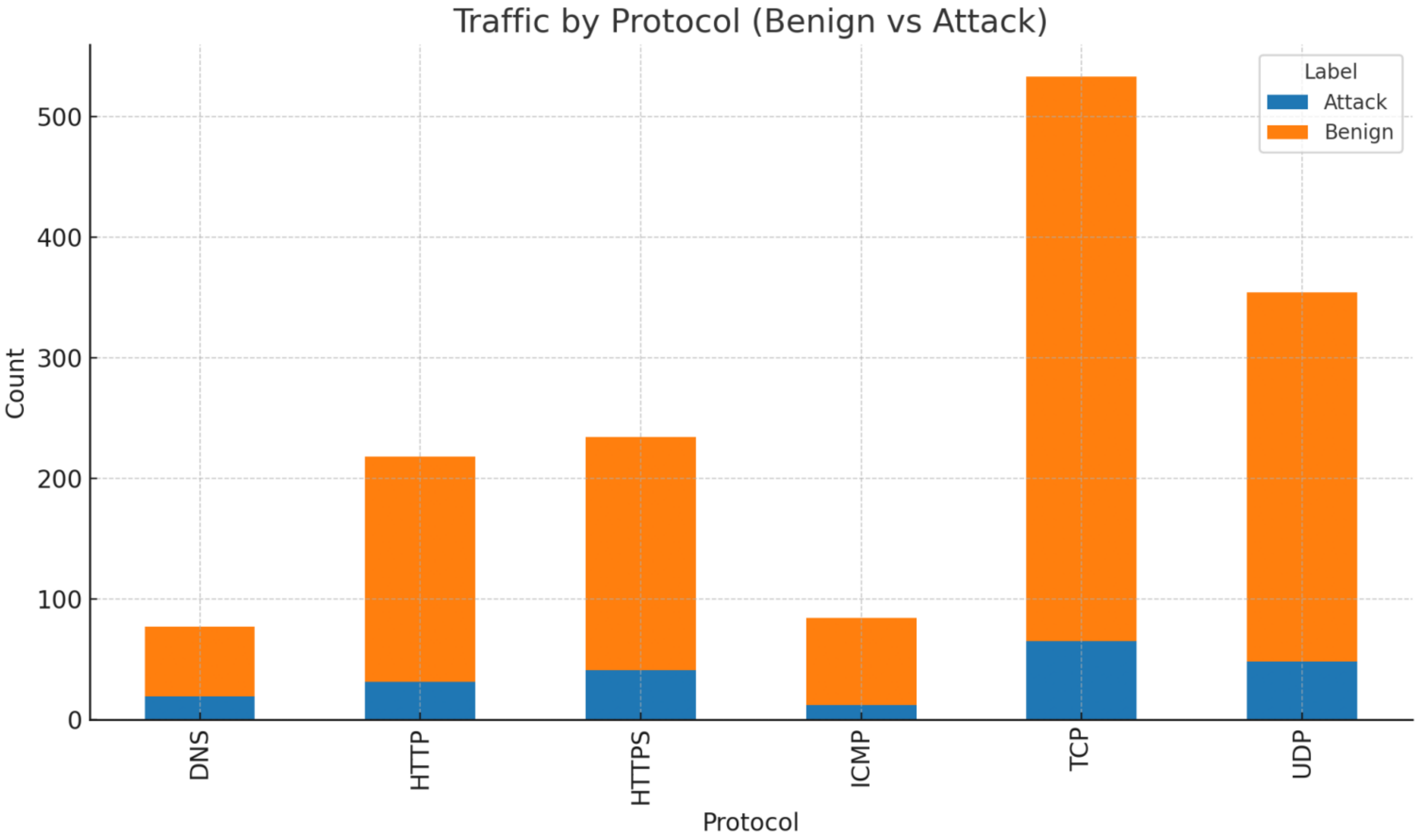
Search & Query Functionality:

- Search by IP/domain/subnet via the search box in the Dash header.
- Filters by protocol and date range; highlights and narrows visuals and logs.

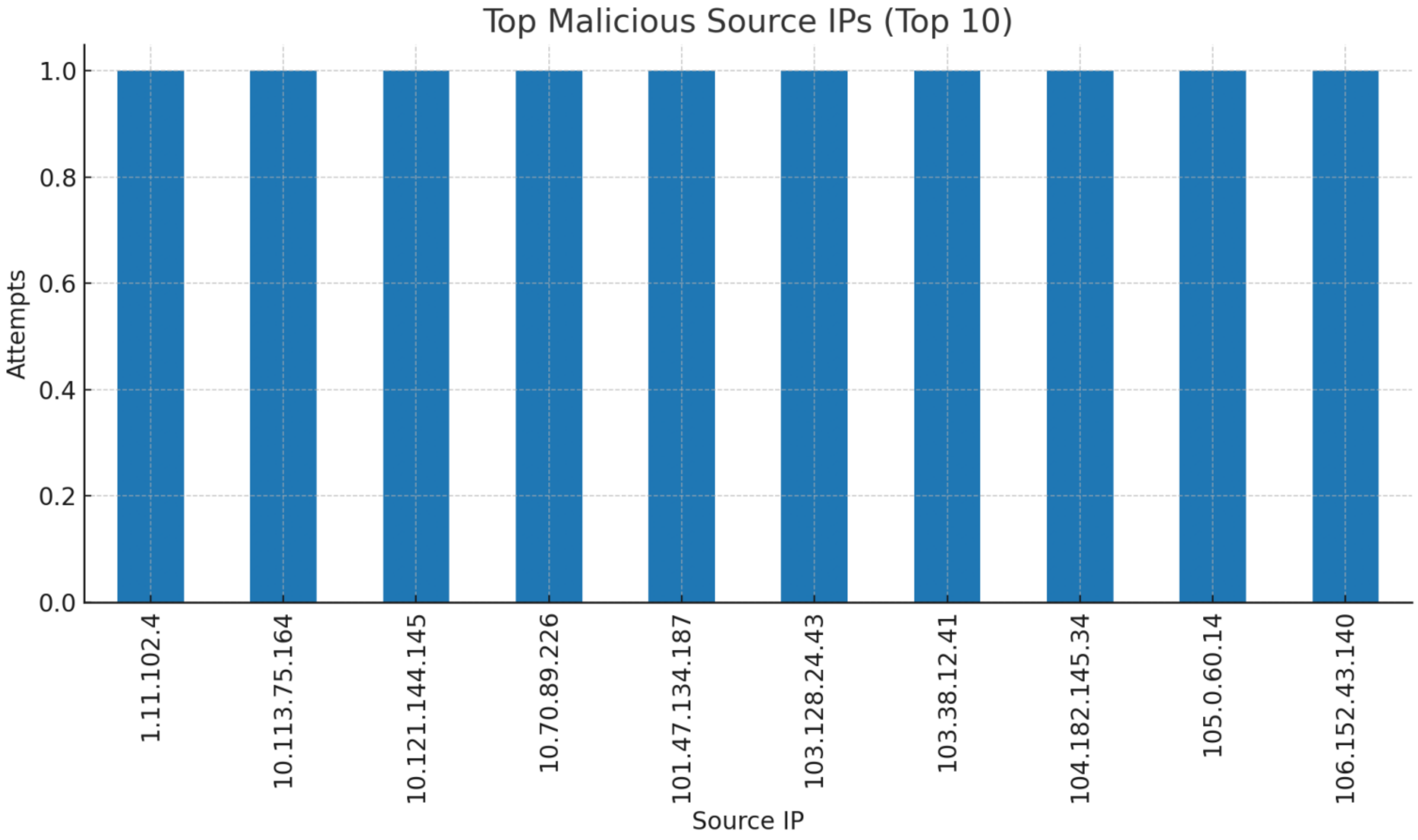
Real-Time Behavior:

- Dashboard reloads data every 15 seconds from dashboard_data.csv.
- Replace the CSV periodically or stream-append to simulate real-time.

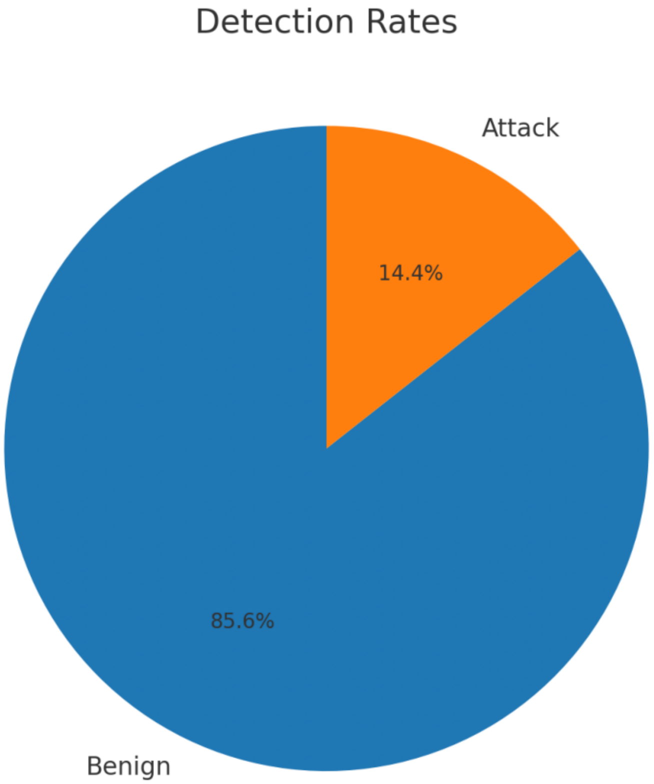
Traffic by Protocol (Benign vs Attack)



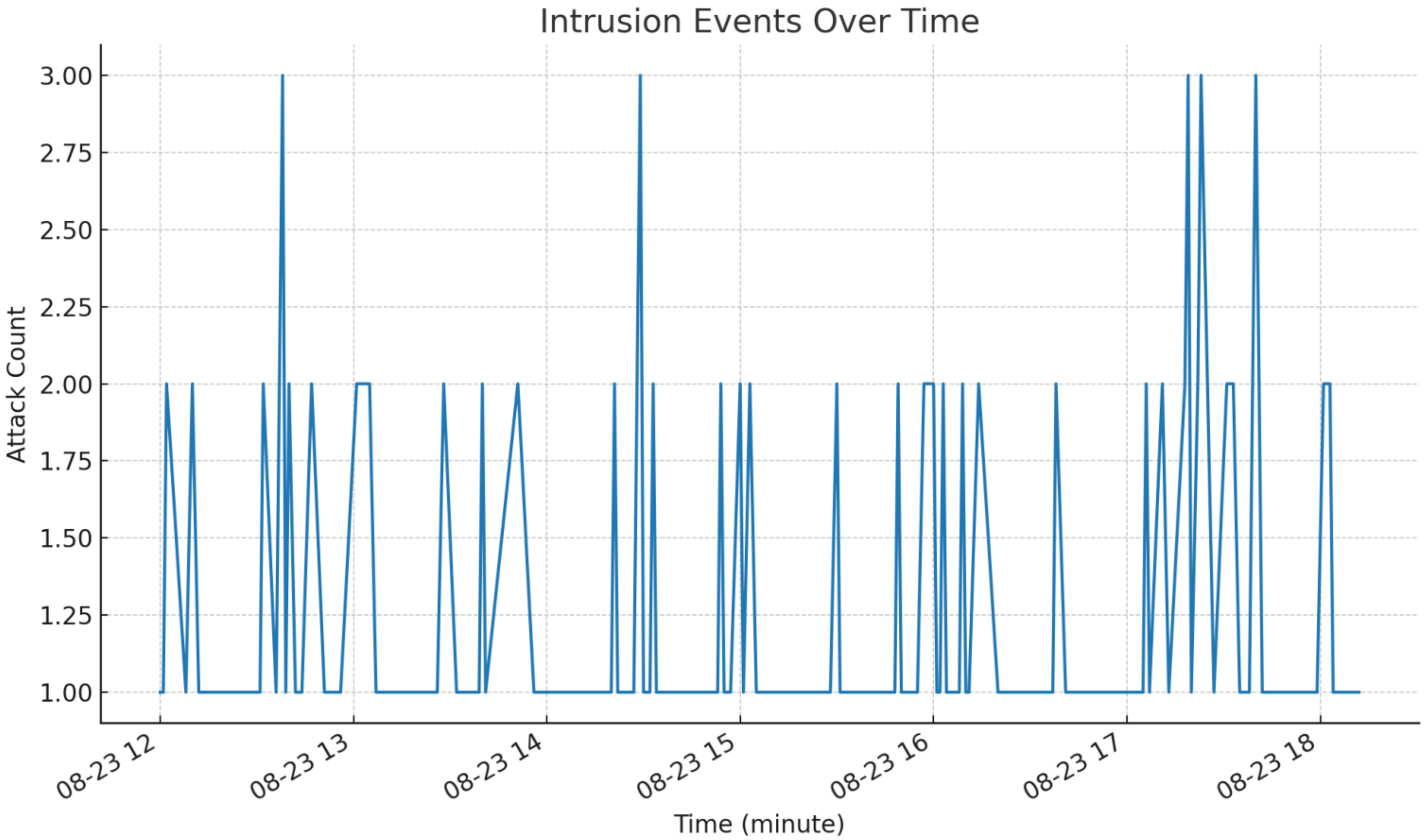
Top Malicious Source IPs



Detection Rates



Intrusion Events Over Time



Intrusion Events Over Time
Attack Count
Time (minute)