Week 3 Dashboard Report: Intrusion Detection Dashboard

SAI NANDU POSINA

1 Overview

The **Intrusion Detection Dashboard** is a real-time cybersecurity monitoring tool designed to visualize network activity, detect malicious threats, and allow analysts to investigate suspicious behavior efficiently.

The dashboard integrates *interactive search, filtering, and graphical analysis* of protocol traffic and attack trends to enhance security monitoring.

2 Metrics Displayed

The dashboard presents key cybersecurity metrics that help analysts identify network threats:

2.1 Traffic by Protocol

- A bar chart displaying **network traffic split by protocols** (TCP, UDP, ICMP).
- Highlights **malicious vs. benign traffic** across different protocol types.
- Helps detect unusual protocol-based attack patterns (e.g., *ICMP flood attacks*).

2.2 Detection Rates

- A pie chart illustrating **benign vs. malicious detections** in network traffic.
- Helps analysts assess the **volume of potential security incidents**.

- Higher malicious rates indicate a need for **immediate threat mitigation**.

2.3 Attack Trends Over Time

- A line chart tracking **attack occurrences across time intervals**.
- Shows **hourly trends** of intrusion attempts.
- Helps security teams **prioritize response efforts** based on attack frequency.

3 Dashboard Walkthrough

3.1 User Interface & Features

The dashboard layout includes the following interactive components:

- **Search Bar** – Users can enter *protocols, attack types, or ports* to filter logs dynamically.
- **Attack Type Dropdown** – Allows filtering logs based on *Benign or Malicious* network traffic.
- **Real-Time Graphs** – Visualizes *live updates* every 5 seconds to reflect the latest network activity.

3.2 User Interactions

1. **View Protocol-Based Traffic Analysis** – Identify attack vectors using the *Traffic by Protocol* chart.
2. **Detect Malicious Patterns** – Filter *Malicious* traffic using the attack dropdown to **investigate threats**.
3. **Search Functionality** – Type `TCP`, `UDP`, `80` (or any attack-related parameter) to **retrieve specific logs**.
4. **Analyze Time-Based Trends** – Use the *Attack Trends Over Time* visualization to detect peak attack times.

4 How the Search Function Helps Analysts

The **search bar** enhances cybersecurity investigations by allowing:

- **Quick Threat Identification** – Users can enter *specific protocols, ports, or attack types* for immediate results.

- **Protocol-Based Attack Analysis** – Searching `UDP` could reveal *potential UDP flood attacks*, useful in DDoS detection.

- **Efficient Network Investigations** – Analysts can **filter logs dynamically**, speeding up security assessments.

- **Streamlined Incident Response** – Helps cybersecurity teams **act faster** on identified threats.

5 Conclusion

The **Intrusion Detection Dashboard** combines **real-time analytics, search functionality, and graphical trends** to improve cybersecurity threat detection and response. The ability to filter logs dynamically enhances **operational efficiency**, allowing analysts to **pinpoint attacks instantly and react accordingly**.

This report provides an overview of the dashboard's functionality, metrics, and how the **search and filtering features** improve cybersecurity monitoring.