Cybersecurity Dashboard - Project Proposal

1. Project Overview

A **Cybersecurity Dashboard** is a centralized platform designed to monitor, detect, and analyze security events in real time. It provides actionable insights and alerts to improve system security and protect against potential cyber threats.

2. Importance of SIEM (Security Information & Event Management)

Security Information & Event Management (SIEM) tools play a crucial role in cybersecurity by:

- **Aggregating logs** from various sources (firewalls, servers, applications, etc.).
- **Detecting anomalies and threats** through rule-based and AI-driven analytics.
- **Providing real-time alerts** to security teams.
- **Assisting in compliance** with security regulations and policies.

3. Key Features of the Cybersecurity Dashboard

a) Real-Time Log Monitoring

- Collect and analyze logs from different sources.
- Display logs in an interactive UI with filtering and search options.

b) Threat Detection & Alerts

- Detect suspicious activities using predefined security rules.
- Send alerts via email, SMS, or dashboard notifications.

c) User Access & Authentication Monitoring

- Track login attempts and unauthorized access.
- Implement multi-factor authentication (MFA) logging.

d) Incident Response & Reporting

- Provide a response plan for detected threats.
- Generate reports for security audits and compliance.

e) Real-Time Analytics & Visualization

- Interactive graphs and charts to analyze security trends.
- Customizable dashboards for different security use cases.

4. Technology Stack

Component	Technology Choices
Backend API	Python (Django)
Frontend	HTML / CSS
Database	MySQL
Log Processing	Graylog
Authentication	OAuth, JWT, MFA Implementation
Cloud/Hosting	Azure
Containerization	Docker

5. Objectives

- Develop a **user-friendly and secure dashboard** for cybersecurity professionals.
- Enable **real-time monitoring and alerting** for security threats.
- Improve **incident response efficiency** with automated threat detection.
- Provide **scalability and flexibility** by integrating with cloud and on-premise environments.

6. Next Steps

1. **Design Wireframes & Architecture** for the dashboard.
2. **Set Up the Development Environment** with chosen tech stack.
3. **Implement Log Monitoring Module** for data collection.
4. **Develop Threat Detection Mechanisms** and integrate with alerting systems.
5. **Build Frontend UI** for visualization and analytics.
6. **Testing & Deployment** in a real-world scenario.

7. Conclusion

This **Cybersecurity Dashboard** will provide an efficient and centralized way to manage security logs, detect threats, and enhance cybersecurity posture. With **SIEM integration and real-time analytics**, it will be a valuable tool for security teams.