## User Story:

As a cybersecurity specialist, I need a system that can instantly identify and respond to security threats using AI-driven network analysis, so that organizations can stay protected against new and evolving cyber attacks.

## Sprint Backlog Tasks:

|  |  |  |
| --- | --- | --- |
| Task # | Task Description | Estimated Hours |
| 1 | Set up the project environment and initialize a Node.js server with Express | 3 hours |
| 2 | Design a simple frontend dashboard using HTML and CSS to display threat alerts | 6 hours |
| 3 | Configure MongoDB to securely store event logs and user activity | 4 hours |
| 4 | Build a basic machine learning model with TensorFlow or Scikit-learn for threat detection | 7 hours |
| 5 | Create backend APIs to handle network traffic data and send it for AI analysis | 5 hours |
| 6 | Implement real-time visual updates on the dashboard for newly detected threats | 6 hours |
| 7 | Develop secure login and role-based access control for users and admins using JWT or Passport.js | 5 hours |
| 8 | Set up a real-time notification system for immediate threat alerts | 6 hours |
| 9 | Perform testing to handle special cases like unusual traffic spikes or system recovery after downtime | 5 hours |
| 10 | Fine-tune machine learning models and optimize backend APIs for better performance | 6 hours |
| 11 | Conduct final integration testing, clean up code, prepare project documentation, and update the GitHub repository with a README file | 4 hours |