Proposed Solution

- **Date**: 8 May 2025
- **Project Name**: AI-Based Threat Intelligence Platform
- **Maximum Marks**: 2 Marks

SR.NO	Parameter	Description
1	Problem Statement (Problem to be solved)	Cybersecurity teams often struggle with delayed or missed threat detection due to limited real-time insights and inefficient manual analysis. With the rise in frequency and sophistication of cyber threats, organizations need a smarter, faster way to identify potential risks using AI-driven insights. This project addresses this need by building an AI-powered threat analysis platform that learns from traffic patterns and helps distinguish between benign and malicious behavior.
2	Idea / Solution description	The AI ThreatSense Platform is designed to process basic network threat data (such as IP addresses, alert hours, and threat scores), train machine learning models to predict potential threats, and output real-time threat classifications. The platform enables data ingestion, preprocessing, model training, and performance evaluation, all built into a lightweight yet functional system suitable for proof-of-concept and small-scale security operations.
3	Novelty / Uniqueness	Unlike traditional systems, ThreatSense is built with simplicity and educational value in mind, offering a compact yet effective model training pipeline. It features IP-based threat intelligence analysis with future scope for integration with larger datasets and external feeds. Its transparent design allows easy customization and expansion, serving as a foundation for more advanced AI security applications.

4	Social Impact / Customer Satisfaction	Although developed as a course-level project, this platform demonstrates how even limited data can be used to build a predictive cybersecurity model. It raises awareness about the practical use of AI in security and offers a starting point for institutions or small businesses to develop their own threat detection systems. The platform is open for learning, experimentation, and future enhancements, ensuring adaptability and relevance.
5	Business Model (Revenue Model)	For a real-world extension, the platform could evolve into a freemium model — offering basic real-time threat scoring for free, while charging for features like cloud hosting, API access, integration with SIEM tools, and advanced analytics. It could also be sold to cybersecurity educational institutions as a teaching kit or lab module.
6	Scalability of the Solution	The platform's codebase supports modular enhancements, allowing it to scale from handling simple threat data to ingesting large-scale enterprise-level logs. The model architecture can be upgraded to handle complex features, while its open-source foundation encourages collaborative growth, plugin integrations, and deployment on scalable cloud environments.