Proposed Solution Template

- **Date**: 29 April 2025
- **Project Name**: AI-Based Threat Intelligence Platform
- **Maximum Marks**: 2 Marks

SR.NO	Parameter	Description
1	Problem Statement (Problem to be solved)	The increasing sophistication of cyber threats poses a significant challenge to organizations, particularly in detecting and responding to threats in real-time. This project aims to create a platform that uses AI and machine learning to detect and respond to emerging cyber threats by aggregating data from diverse sources and providing actionable intelligence to security teams.
2	Idea / Solution description	The solution involves an AI-based platform that continuously monitors network traffic, system logs, and endpoint activities. It uses machine learning algorithms to detect potential threats such as malware, phishing, ransomware, and insider threats. The platform will also aggregate and correlate data from various sources and deliver real-time alerts and visualizations to security analysts for prompt threat mitigation.
3	Novelty / Uniqueness	The platform utilizes machine learning models tailored specifically to detect emerging and sophisticated threats that traditional rule-based systems often miss. Its integration with external threat intelligence feeds (open-source, dark web, etc.) and internal data sources creates a comprehensive, dynamic defense mechanism, which enhances the ability to predict and prevent cyberattacks proactively.

4	Social Impact / Customer Satisfaction	This solution will significantly improve the cybersecurity posture of organizations by providing real-time, actionable insights into threats. It will enable security teams to respond more effectively, reducing the impact of cyberattacks and protecting sensitive data. The increased security will contribute to a safer digital ecosystem, benefiting both businesses and consumers by reducing data breaches and loss of trust.
5	Business Model (Revenue Model)	The platform will follow a **SaaS (Software as a Service)** model, offering subscription-based pricing to businesses. The pricing tiers will depend on the number of endpoints monitored, the volume of data processed, and the advanced features like predictive analytics and custom integrations. There may also be opportunities for enterprise-level customization at a premium cost.
6	Scalability of the Solution	The platform is designed to scale as organizations grow. It can accommodate increased data volumes, new data sources, and additional security tools without significant changes to the infrastructure. The use of cloud services for data processing ensures that the platform can handle the growing needs of large organizations, while also being adaptable for smaller companies that require fewer resources.