

Project Design Phase-I
Proposed Solution Template

Date	19 September 2022
Team ID	PNT2022TMIDxxxxxx
Project Name	Malware Detection and Classification
Maximum Marks	2 Marks

Proposed Solution:

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	The problem we aim to address is the escalating complexity of cyber threats and the need for innovative solutions to enhance cybersecurity. Specifically, we intend to develop a log-based malware detection and classification system that provides real-time reports to firewall development companies and testers, helping them identify and categorize malware within their networks swiftly and accurately.
2.	Idea / Solution description	Our solution, the "Malware Detection and Classification" system, leverages advanced AI and cybersecurity techniques to monitor network traffic, detect malware, and classify it in real-time. Detailed malware detection and classification. User-friendly interface. Real-time communication with an AI assistant. IoT protection. Integration with other apps. User education on cybersecurity. Privacy control. Incident response integration. Feedback mechanism. Data analysis for data leak prevention.
3.	Novelty / Uniqueness	Our system's uniqueness lies in its comprehensive approach to malware detection and classification, real-time communication with an AI assistant, integration with other apps, IoT protection, and user education. The ability to provide detailed explanations in real-time sets us apart, as does our commitment to user feedback and continuous improvement.

4.	Social Impact / Customer Satisfaction	Our system's impact extends to both individual users and organizations. It empowers users to navigate the digital landscape safely and educates them about cybersecurity. For businesses and developers, it enhances firewall testing by offering real-time malware monitoring and classification. Rapid threat identification allows for timely responses to potential breaches, ultimately increasing the security of digital assets. By prioritizing user satisfaction and offering a user-friendly interface, we aim to create a safer and more user-centric digital environment.
5.	Business Model (Revenue Model)	We propose a subscription-based revenue model with tiered pricing. Users can access a basic version of our system for free, while premium features, such as IoT protection and advanced analytics, are available through paid subscriptions. Additionally, we can offer enterprise-level licenses for firewall development companies and testers. Advertising partnerships and data analysis services can provide supplementary revenue streams.
6.	Scalability of the Solution	Our solution is highly scalable. As the digital landscape continues to evolve, we can expand our malware database, enhance AI algorithms, and add new features to adapt to emerging threats. We can also scale up our infrastructure to accommodate a growing user base and ensure reliable service. Collaborations with other apps and integration with various devices and systems make our solution versatile and ready for integration into different environments. Our commitment to continuous improvement ensures long-term scalability and relevance.