**Proposed Solution Template**

Date: 24/10/2023

Team ID: 2.10

Project name: Malware Detection and Classification

Team members: Sohan, Shaz, Atharva, Pratheek

**Proposed Solution Template**

|  |  |  |
| --- | --- | --- |
| **S.No** | **Parameter** | **Description** |
| 1. | Problem Statement | We need to create a smart system that can quickly spot and categorize harmful software (malware) on computers and networks. This system has to be really good at telling the difference between malware and harmless software. It should work without slowing down your computer and be useful for regular users and big companies. To do this, we'll use advanced technology like machine learning and constantly update it to catch new types of malwares. |
| 2. | Solution description | Our approach creates a real-time malware detection system by combining dynamic analysis, machine learning models, and enhanced feature extraction. It is intended to be scalable, accurate, and quick for both people and businesses. To remain ahead of emerging malware threats, this system refreshes its database often, offering strong protection with a low number of false positives. |
| 3. | Uniqueness | Our unique system combines dynamic analysis, real-time monitoring, scalability, and advanced feature engineering. It provides a comprehensive malware detection and categorization method, guaranteeing adaptability to new threats. It stands out because of frequent updates and an emphasis on minimizing false positives and offers a thorough and efficient defense against constantly evolving malware. |
| 4. | Customer satisfaction | One of our solution's main objectives is to guarantee maximum client satisfaction:   1. Effective Protection: We put the user experience and system performance first by correctly detecting and categorizing malware while reducing false positives, which increases satisfaction. 2. User-Friendly Interface: A user-friendly interface that is straightforward and easy to use, has clear reporting, and requires little user involvement.      1. Timely Updates: We are committed to protecting users against new malware threats, which builds trust and satisfaction. Regular updates and proactive threat mitigation show this. 2. Scalability: Our system is designed to fulfil the varied needs of a wide range of customers by accommodating both individual users and large organizations. 3. Support and Assistance: By quickly resolving concerns, offering customer support and assistance for any problems or inquiries strengthens satisfaction. |
| 5. | Business Model | Our business strategy is centered on subscription-based malware detection and classification services. For both individual users and businesses, we provide tiered subscription plans that can be billed monthly or yearly. A freemium or trial version works as a conversion technique and draws in new consumers.    To increase our reach, we also work with OEMs to package our software with new products. Organizations with special demands are catered to through integration solutions and customization services. Our value proposition is improved by consulting and training services that optimize cybersecurity strategy.    In addition, we might investigate joint ventures with cybersecurity suppliers to provide our technology as an extra security measure in their suites. Services related to threat intelligence and data analytics can bring in extra money. Consistent software upgrades and customer service guarantee enduring satisfaction and subscription renewals, which in turn promotes continued business growth |
| 6. | Scalability of the solution | Because of its great scalability, our system can easily grow to meet the changing needs of both small and large businesses. Its scalability is attained by effective resource management, cloud integration, customizable APIs, multi-tiered subscription plans, worldwide support, and continuous R&D. Because of its adaptability, the system may effectively expand to accommodate the needs of a wide range of users. |