Project Design Phase-I
Proposed Solution

Date	25 October 2023
Team ID	Team 2.6
Project Name	Project – Malware Detection and Classification
Maximum Marks	2 Marks

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Evaluate the impact of malware attacks utilizing SSL certificates with 'commonName' mismatches and propose proactive measures for mitigation.
2.	Idea / Solution description	1. **Continuous Monitoring of Certificates –** Developing a system which would do the real-time SSL certificate monitoring for common names and alerts administrators on any mismatches. 2. **Multi-Factor Authentication (MFA) and Access Controls –** Implementation of strict access controls with MFA mitigates impact of SSL certificate related attacks because it limits unauthorized access. 3. **Regular Updates and Patch management –** Keeping the certificates and softwares up-to-date minimizes the vulnerabilities which can be exploited by malware.
3.	Novelty / Uniqueness	Some of the key-factors that make this problem more unique and novel – • SSL certificates with ‘Commonname’ mismatches allows attackers to bypass many security features build into browsers and applications. • More difficult for users to detect and defend against these attacks. • Increase in the use of HTTPS gives provides attackers a larger range of potential targets. • The attacks being relatively new , there are very few ways to solutions available to mitigate them.
4.	Social Impact / Customer Satisfaction	Social Impact – Identity theft and Damage to reputation. Customer Satisfaction – Security breaches and Lack of Trust.
5.	Business Model (Revenue Model)	➢ Some possible Business/Revenue models are Selling Security solutions (like WAFs and event management systems like SIEMs) ➢ Offering security consulting services
6.	Scalability of the Solution	◆ Cloud-based solutions – easily scalable based on needs of organization. ◆ On premise solutions – Better option for larger organization with complex networks.