IDEATION PHASE
BRAINSTORM AND IDEA PRIORITIZATION

DATE	17 October 2023
TEAM ID	TEAM 2.11
PROJECT NAME	MALWARE DETECTION AND CLASSIFICATION
MAXIMUM MARKS	4 MARKS

Team Members – Shashibhushan Das, Athibhan Pruthvi, Hiya Sharma, Mohan Raj

Step 1: Team Gathering, Collaboration and Select the Problem Statement

This step involves bringing together a team of experts with different backgrounds, such as cybersecurity, machine learning, and data science. The team will then collaborate to define the problem statement, which should be specific, measurable, achievable, relevant, and time-bound. In this case the problem statement is defined as 'Using AI for Malware Detection and Classification'.

Step 2: Brainstorm, Idea Listing and Grouping

Brainstorming:

- Use AI to develop new malware detection algorithms.
- Use AI to improve existing malware detection algorithms.
- Use AI to classify malware.
- Use AI to automate tasks related to malware detection and classification.

Idea Listing:

- Use deep learning to develop malware detection algorithms.
- Use natural language processing to develop malware detection algorithms.
- Use AI to develop malware classification algorithms.
- Use AI to automate the analysis of large amounts of data to identify potential malware infections.
- Use AI to automate the generation of reports on malware infections.
- Use AI to automate the identification and prioritization of malware threats.
- Use AI to automate the development and deployment of new malware detection and classification algorithms.

Grouping:

- Malware detection algorithms: deep learning, natural language processing
- Malware classification algorithms: AI
- Task automation: analysis of large amounts of data, generation of reports, identification and prioritization of threats, development and deployment of new algorithms

Step 3: Idea Prioritization

The following ideas are prioritized based on their potential impact and feasibility:

1. Use AI to develop new malware detection algorithms.
2. Use AI to improve existing malware detection algorithms.
3. Use AI to automate the analysis of large amounts of data to identify potential malware infections.
4. Use AI to automate the generation of reports on malware infections.
5. Use AI to automate the identification and prioritization of malware threats.
6. Use AI to develop malware classification algorithms.
7. Use AI to automate the development and deployment of new malware detection and classification algorithms.