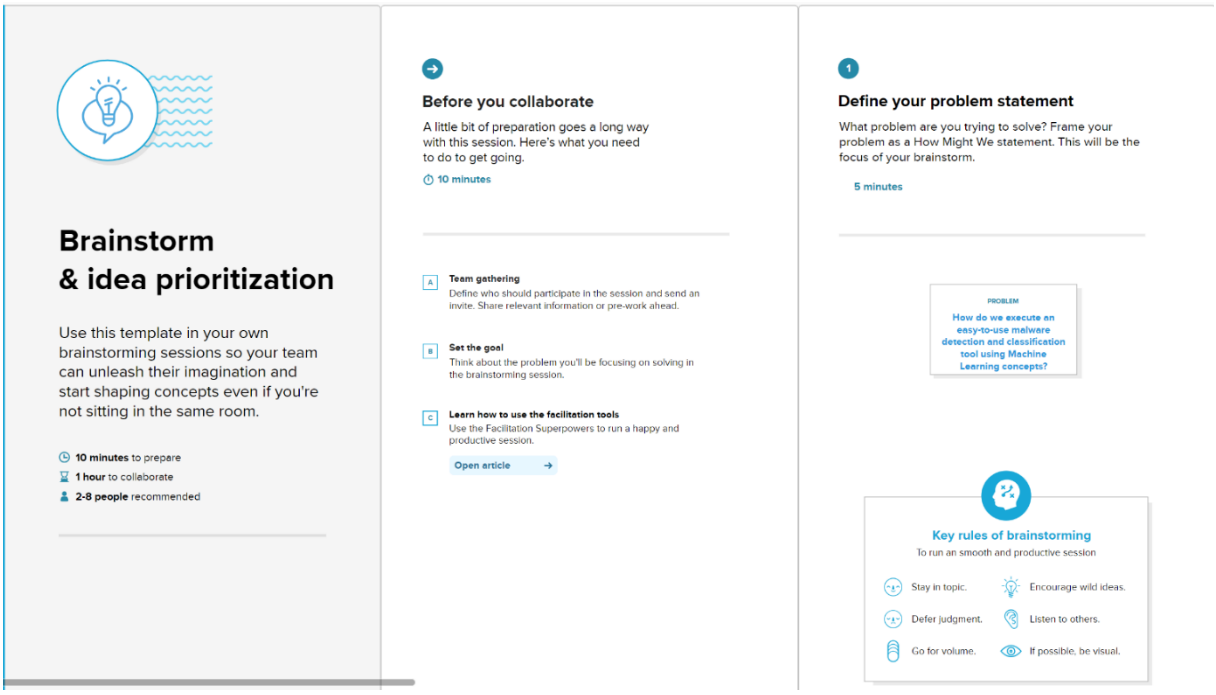
Ideation Phase
Brainstorm & Idea Prioritization Template

Date	27 September 2023
Team ID	2.3
Project Name	Malware detection and classification
Maximum Marks	4 Marks

Brainstorm & Idea Prioritization :

Mural link: https://app.mural.co/t/malwaredetectionandclassific7861/m/malwaredetectionandclassific7861/1697186707969/07ad100ef09db8f0d6f814c9d31d435b86d9e106?sender=a0132bca-2445-4b2d-b51d-77dfe78ffef6

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



Brainstorm & idea prioritization

Use this template in your own brainstorming sessions so your team can unleash their imagination and start shaping concepts even if you're not sitting in the same room.

10 minutes to prepare
1 hour to collaborate
2-8 people recommended

Before you collaborate

A little bit of preparation goes a long way with this session. Here's what you need to do to get going.

10 minutes

A **Team gathering**
Define who should participate in the session and send an invite. Share relevant information or pre-work ahead.

B **Set the goal**
Think about the problem you'll be focusing on solving in the brainstorming session.

C **Learn how to use the facilitation tools**
Use the Facilitation Superpowers to run a happy and productive session.

Open article →

1 Define your problem statement

What problem are you trying to solve? Frame your problem as a How Might We statement. This will be the focus of your brainstorm.

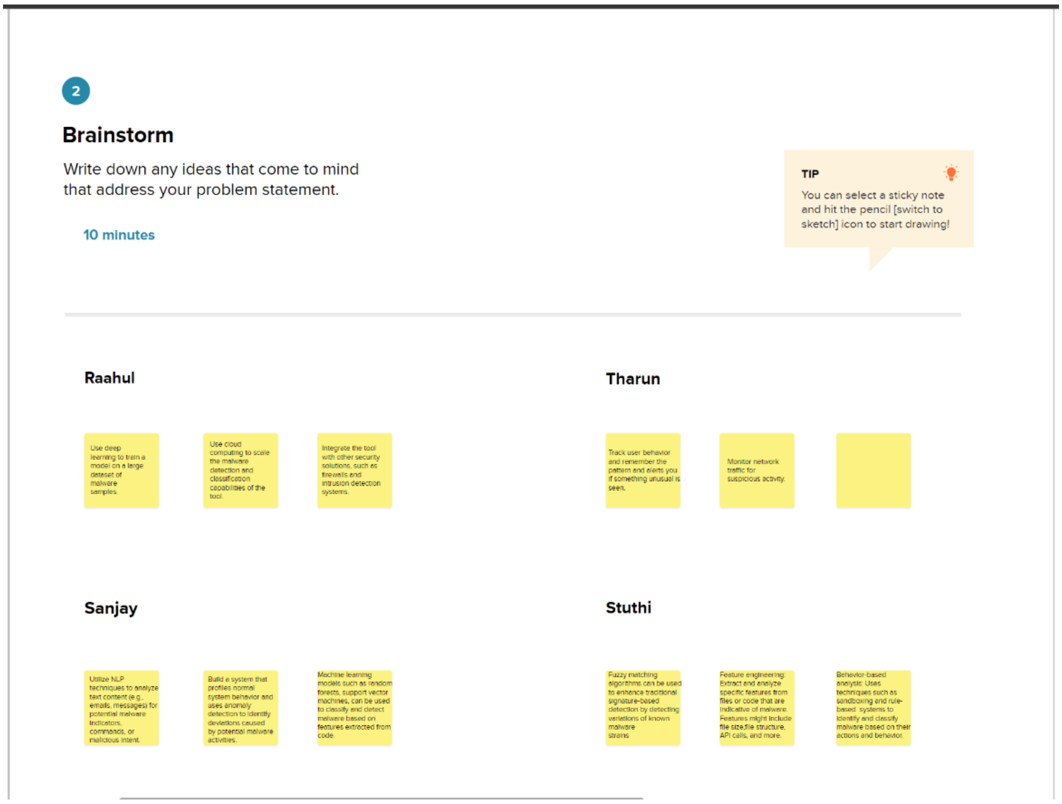
5 minutes

PROBLEM
How do we execute an easy-to-use malware detection and classification tool using Machine Learning concepts?

Key rules of brainstorming
To run an smooth and productive session

Stay in topic. Encourage wild ideas.
Defer judgment. Listen to others.
Go for volume. If possible, be visual.

Step-2: Brainstorm, Idea Listing and Grouping



2

Brainstorm

Write down any ideas that come to mind that address your problem statement.

10 minutes

TIP

You can select a sticky note and hit the pencil [switch to sketch] icon to start drawing!

Raahul

- Use deep learning to train a model on a large dataset of malware samples.
- Use cloud computing to scale the malware detection and classification capabilities of the tool.
- Integrate the tool with other security solutions, such as firewalls and intrusion detection systems.

Tharun

- Track user behavior and remember the pattern and alerts you if something unusual is seen.
- Monitor network traffic for suspicious activity.

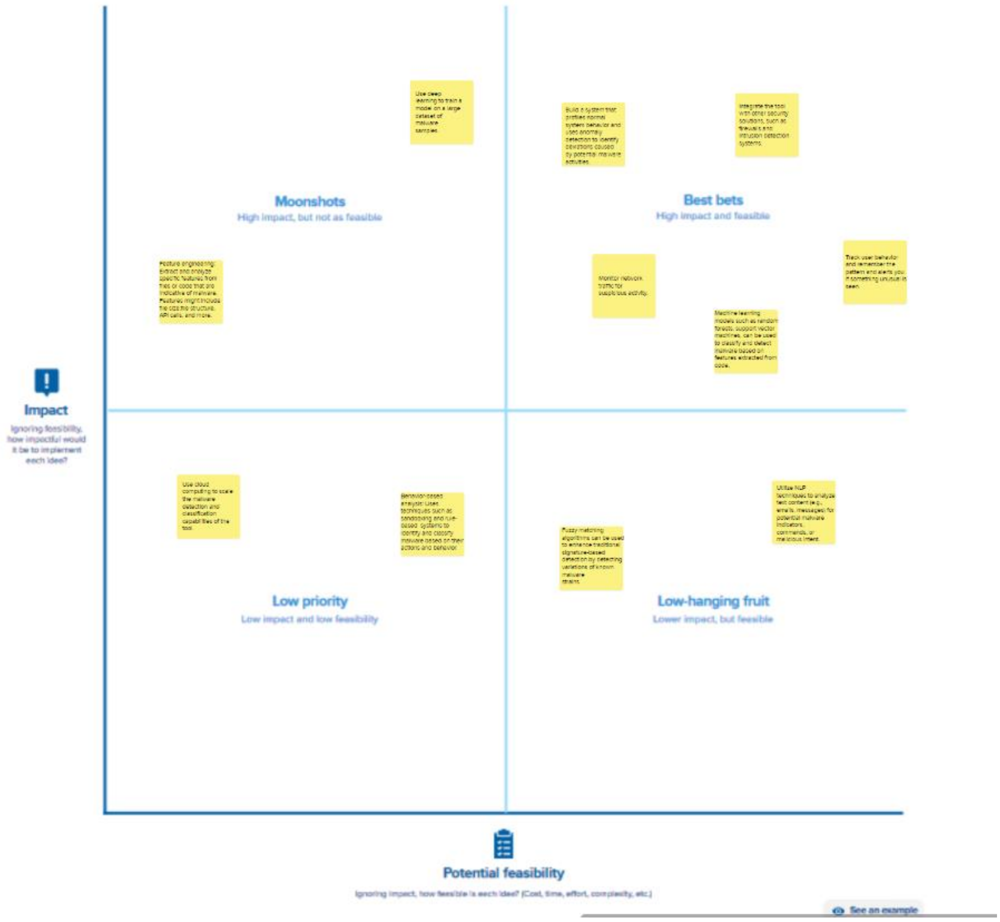
Sanjay

- Utilize NLP techniques to analyze text content (e.g., emails, messages) for potential malware indicators, commands, or malicious intent.
- Build a system that profiles normal system behavior and uses anomaly detection to identify deviations caused by potential malware activities.
- Machine learning models such as random forests, support vector machines, can be used to classify and detect malware based on features extracted from code.

Stuthi

- Fuzzy matching algorithms can be used to enhance traditional signature-based detection by detecting variations of known malware strains
- Feature engineering: Extract and analyze specific features from files or code that are indicative of malware. Features might include file size,file structure, API calls, and more.
- Behavior-based analysis: Uses techniques such as sandboxing and rule-based systems to identify and classify malware based on their actions and behavior.

Step-3: Idea Prioritization


Moonshots
High impact, but not as feasible
Best bets
High impact and feasible
Low priority
Low impact and low feasibility
Low-hanging fruit
Lower impact, but feasible
Impact
Ignoring feasibility, how impactful would it be to implement each idea?
Potential feasibility
Ignoring impact, how feasible is each idea? (Cost, time, effort, complexity, etc.)
See an example

Use deep learning to train a model on a large dataset of malware samples.

Feature engineering: Extract and analyze specific features from files or code that are indicative of malware. Features might include file size,file structure, API calls, and more.

Build a system that profiles normal system behavior and uses anomaly detection to identify deviations caused by potential malware activities.

Integrate the tool with other security solutions, such as firewalls and intrusion detection systems.

Monitor network traffic for suspicious activity.

Track user behavior and remember the pattern and alerts you if something unusual is seen.

Machine learning models such as random forests, support vector machines, can be used to classify and detect malware based on features extracted from code.

Use cloud computing to scale the malware detection and classification capabilities of the tool.

Behavior-based analysis: Uses techniques such as sandboxing and rule-based systems to identify and classify malware based on their actions and behavior.

Fuzzy matching algorithms can be used to enhance traditional signature-based detection by detecting variations of known malware strains

Utilize NLP techniques to analyze text content (e.g., emails, messages) for potential malware indicators, commands, or malicious intent.