Ideation Phase

Brainstorm & Idea Prioritization

Date	19 September 2022
Team ID	
Project Name	Malware Detection and Classification
Maximum Marks	4 Marks

Brainstorm & Idea Prioritization Template:

Empathy Map:
https://app.mural.co/t/cybersecurity2861/m/cybersecurity2861/1697128947242/07b5d8c1beecda3a0242ca56397da2ac7d09131b?sender=u95c8d0d9a5aba0a440917861

Brainstorming and idea prioritization template:

https://app.mural.co/t/cybersecurity2861/m/cybersecurity2861/1697198322125/34eaba9cce6aa233749f2cf8ae52976ec0ba84d4?sender=u95c8d0d9a5aba0a440917861

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

Our Team Members are –

1. **Madiraju Chaitanya Raju**
2. **Akshay Kumar Pandey**
3. **Rohit Ritesh Maini**
4. **Kunwar Khurana**

The composition of our project team for the ‘Malware Detection and Classification project’ was carefully curated to ensure that we have a well-rounded group of individuals with the right skills and expertise to tackle the complexities of this AI and cybersecurity project.

- Akshay Kumar Pandey was selected for his extensive background in cybersecurity and malware analysis. Their deep knowledge of malware behavior and classification methods makes them the ideal candidate to lead the development of the core detection and classification algorithms.

- Rohit Ritesh Maini was appointed as the project manager due to his experience in leading complex software development projects. His strong organizational skills and ability to coordinate team efforts will be essential in keeping our project on track and within budget.

- Madiraju Chaitanya Raju is an expert in software engineering with a focus on real-time data processing and logging. He will oversee the design and implementation of the logging system, which is vital for capturing and storing data related to detected malware.

- Kunwar Khurana specializes in user interface and user experience (UI/UX) design. He will ensure that the application's interface is intuitive and user-friendly, allowing security professionals to interact seamlessly with the system.

In summary, the team members were chosen based on their specific qualifications and experience that align with the project's objectives. Each team member's role was assigned to leverage their strengths and expertise in different aspects of the 'Malware Detection and Classification Logger Application,' ensuring a comprehensive and effective approach to tackling the problem."

Problem Statement –

Our objective is to deliver a log-based detection system to firewall development companies and testers, enabling them to receive hourly reports on the status and classification of detected malware within their designated network.

Why we chose this problem statement?

Our problem statement was chosen to address the cybersecurity needs of organizations. With the escalating complexity of cyber threats, there's a growing demand for innovative solutions. We selected this problem statement to enhance firewall testing by offering real-time malware monitoring and classification during the testing process to check if the firewall was working as intended. We recognized the vital importance of instant threat identification, allowing companies to swiftly respond to potential breaches and vulnerabilities.

Our team's expertise in cybersecurity, data analysis, and software development, coupled with our desire for cybersecurity innovation, uniquely positions us for this endeavor.

Step-2: Brainstorm, Idea Listing and Grouping

Pattern Creator: We thought, why not track your online behavior to help you avoid malware? It's like a GPS for safe browsing, keeping you away from digital danger zones.

Detailed Logs and Real-Time AI Communication: Ever wondered why your antivirus calls something 'bad'? We came up with an idea to provide detailed info and chat in real-time with an AI. It's like having a tech-savvy buddy explaining things when you need it.

Malware Graph Database: Imagine a map connecting different malware strains, like a family tree. It helps us analyze them better and provide you with smarter updates. It's like a detective board for cyber threats, making us better prepared for surprises.

Collaboration with Other Apps: We want to make your digital life hassle-free. So, we thought, what if our malware detector worked seamlessly with your other apps? It's like having a guardian angel that plays well with all your digital friends.

IoT Premium Feature: Your entire network becomes a fortress, guarded by our malware detection system. By loading it onto your Wi-Fi network, it's like installing a top-notch security system for all your IoT devices, protecting every corner of your digital castle.

Adblocker with Threat Notification: No one likes pesky ads, but we went a step further. How about an adblocker that also warns you about sketchy websites? It's like a digital shield, ensuring you can browse with peace of mind.

User Education Integration: Cybersecurity isn't everyone's forte, right? So, we came up with playful games that teach you to spot phishing attempts. It's like a cybersecurity boot camp, turning you into a pro at recognizing online tricks.

Privacy Beacon with Data Usage Notification: You've got the right to know how your data is used. Our Privacy Beacon ensures that. It's like having a little privacy watchdog, keeping you informed and in control of your digital life.

Incident Response Integration: When things go haywire, you want a well-coordinated response. Our idea ensures that you're in the loop and informed during a crisis. It's like having a direct line to our incident response team when you need it most.

Feedback Mechanism: Ever wished your voice could shape the services you use? With our feedback mechanism, it can. You're the expert in your experience, and we're here to listen and improve based on your insights.

Data Usage Limits and Analysis: Worried about data leaks? Our idea dives deep into where your data goes and offers solutions. It's like having a personal data detective that helps you keep your digital secrets safe.

I thought through the point of view of the user, I think that at the end of the day our app will be a product that will help users so making sure that they are satisfied is my utmost priority.

Feedback option: This option will help us on the developer side with the minor bugs that are there in the app and can eventually be solved using the user feedback.

If the user wants then we can also provide them with the scan result log files, hence better explanation on the detected malware

A static page to give some definitions on what malware is so that the user knows what why he is using the software: education

Real time scan progress: This will help the user know that the app is working and that it is not stuck, it helps the user get the idea of what is going on in real time.

Notification at the end of the scan: Will let the user know that the scan is complete if the user is working on something else and it is running in the backend.

And an extra notification if there is malware so the user doesn’t have to open the app if there is no malware: Suppose that the user is not paying attention to the scan, so at the end of the scan user will only get an extra notification if there is a malware detected.

Simple and clean UI: easy for the user to navigate through the app and be clear on what app is about.

Step-3: Idea Prioritization:
Done in the map.

Abstract:

In today's world of technology and computers, there is a big problem called "malware" that can harm the digital stuff we care about. It's like a bad guy for your computer. Our project, "Malware Detection and Classification," wants to help make your digital life safer and friendlier. We use smart computer tricks to find and sort out different kinds of malware.

We want to teach you more about keeping your stuff safe, make sure your secrets stay secret, and help when something goes wrong. Our goal is to build a strong shield against the sneaky cyber threats that are always changing. We dream of a day when you can use your computer with confidence, knowing it's protected by a smart and helpful team of digital guards.

The "Malware Detection and Classification" project is super important right now. Malware keeps getting smarter, and it can hurt your computer, steal your money, and even damage your reputation. Regular antivirus programs are good, but they only react after a problem starts, and they can't keep up with the fast changes in malware.

So, what are we doing? We're using the power of smart computers and learning from them to create a strong defense system that looks out for you. But our project is not just about safety; it's about making you feel in control of your digital world. We imagine a future where you are part of the team, and we use cool technology to make sure you're always safe and happy.

As the digital world keeps growing, so do the bad things in it. Our "Malware Detection and Classification" project is like a big step forward in the fight to protect your digital stuff. We believe that by using the latest technology, helping you, and always getting better, we can change how we think about computer safety. Our goal is to make the digital world a better and safer place for you.

Practice websites:
VirusTotal: VirusTotal offers a collection of harmless and real malware samples for testing and practice.

EICAR: The European Institute for Computer Antivirus Research (EICAR) provides test files and scenarios that mimic malware for testing antivirus software.

MalwareBazaar: This platform allows you to access a variety of malware samples for analysis and practice.

TheZoo: TheZoo is an open-source project that provides a collection of malware samples for research and practice.

Main websites:
GitHub: GitHub often hosts open-source projects and repositories that might contain real-world malware samples. Be cautious when exploring these repositories.

Vulnerable Web Applications: Websites like OWASP's WebGoat and Damn Vulnerable Web Application (DVWA) are designed for security testing and can help you practice identifying vulnerabilities and malware.

Hack The Box: This platform offers various penetration testing challenges, and some of them may involve malware analysis.

Metasploit Unleashed: Metasploit is a penetration testing tool that includes various exploits and payloads. You can use it to practice dealing with real-world malicious payloads.