Member 1: Apurba Das

During Week 1, I engaged in the effective launching of the project, and I directed my attention to defining the expectations described in the project brief and sharing these expectations with other team members clearly. I suggested an initial online meeting where I could ask what possible cybersecurity issues I could work on and make sure that it aligns with the unit learning outcomes. Some practical problems that I proposed were challenging, like detecting phishing attacks and aggregating threat intelligence, and these led to helpful discussions.

I initiated the process of checking the marking rubric, requirements of the project, and deliverables because we wanted to be fully equipped with what was expected. Then, I started to make the first version of our project charter and Gantt chart, which will lead us through the working process. I also made a shared Google Drive folder with articles of research, notes of team meetings, and documentation.

Also, I started with the initial stage of the literature review by selecting the last cybersecurity articles in IEEE and ACM. One of the things that I paid special attention to is ways of tapping the attack seen in social engineering, and it appears that it is also a potential subject of our group. I gave the team summaries of the papers to aid us in coming up with a direction to take in our research.

Finally, I assisted with the determination of initial roles on the basis of the strengths and experience of each member, as well as participated in the drafting of the team contribution form. Week 1 went well, and I have a strong feeling that the groundwork we have established will help us sail through an easy research and development process.

Member 2: Hemant Adhikari

With the first week of work on our cybersecurity group project, I focused on group organization and management. I led a kickoffmeeting of our team and took down notes of what was discussed in a shared notes file. My role was to gather individual availability and schedule a meeting every week so that everything is going in the right direction.

Interpretation of the assessment brief was also done and shared with the team to resolve any confusions. I proposed the following ideas regarding the practical cybersecurity problems of multi-factor authentication vulnerabilities and secure cloud infrastructure. These talks were useful in enabling us to focus on the area of concern in the project. I also assisted Apurba during the review of scholarly databases to identify the possible research gaps, and I provided three literature reviews of current articles.

There is another task that I managed—organization of our feasibility analysis. I started my research on the availability of data, tools, and platforms, as I had to understand which of the shortlisted topics could be successfully worked on. As an example, I researched free APIs to identify the phishing and studied the possibility of using open-source threat databases to support our study.

I also initiated the development of the preliminary abstract and the proposed problem statement of our report. It is still in progress, but this has provided our group a foundation to build on and improve as we complete our topic.

In short, Week 1 focused on the establishment of the foundation of the project, the agreement on responsibilities, and starting research on the background of the project. I made sure that the team was well-organized, our conversations were effective, and records were up-to-date. Since this is Week 1, in the future, I expect to be more active during Week 2 to further perfect the structure of our research and write the essay about the introduction to the report.

Member 3: Aman Basnet

This week, I concentrated, first of all, on the technical practicability and initial planning of the methodology of our project. We brainstormed a few different challenges in the field of cybersecurity, after which I offered to assess the level of technical complexity of our top three ideas. Feasibility A rapid feasibility assessment was also carried out to identify which ideas could work in reality within the constraint of the project.

I also searched the tools and platforms that could be used in its implementation, e.g., Python libraries to detect phishing, Wireshark to examine a network, and OWASP ZAP to break into it. I wrote down my findings and shared them at our second group meeting, so the team started working in the direction of the topic, which is not only non-obsolete but also capable of realization in technical terms.

At the same time, I started writing the early architecture of a prototype system that we could develop. According to our rough plan, I drew a block diagram of a very basic data flow: using a front end (user input), a backend detection module (ML-based), and a database. I also interpreted possible datasets on Kaggle and open threat intelligence on feeds that could be used in possible training, in case it is necessary.

Hemant and I started testing some of the non-functional requirements, such as scalability, performance, and data privacy. I also indicated some of the performance measures that we might apply in the future—accuracy, false positive rate, and response time were some of the examples.

By providing a chance to be involved in the technical preparation of our project, Week 1 enabled me to form a clear idea of the parameters of the project and be an active participant in it. In Week 2, I will complete our methodology section and start working with prototyping testing on the small scale to ensure our research direction is correct.

Member 4: Sanjeev Oli

My task during Week 1 was to complete the primary literature review and to prepare the reference material in preparation for the project. After narrowing down the potential research avenues by our group, I initiated the process of gathering research articles and studies in academia and industry that discussed comparable issues. I relied on the peer-reviewed articles of journals such as IEEE, ACM, and Springer, as well as on white papers of the well-known cybersecurity companies.

I have synthesized five important articles that explored the phishing detection methods, anti-zero-trust architectures, and network anomaly detection. In my summaries, I added the methodology, findings, limitations, and tools. This has assisted our group to review that which has already been done and where we can have a new contribution. It was also my suggestion that we do the analysis of the current methods and their results with a literature review matrix, which the team agreed with as well.

Simultaneously, I made a contribution in the establishment of a reference management system via Zotero, where we can collectively structure the citations to our report. I also secured all the sources by applying the APA style of referencing as indicated in the brief.

As well, I volunteered to help Apurba write the purpose of the project and assisted in the definition of the problem statement by way of structuring it around the current threats and gaps in cybersecurity and their ethical under- and overtones.

Week 1 was fruitful and interesting. My current comprehension of the technical and research direction of our project supported by literature has been improved. Next week, I will proceed with the literature review, defining the limitations of the available tools in more detail, and start working on the first draft of the related works part of our report.