Report:

Title Page:

- Title: Retrospective Sprint 2 of Group AttackFlow1
- Building a dataset of real-world cyber-attacks with Attack Flow
- List of team members with their a-numbers:
  - Se Jin Yoon: a1706219
  - Ting-Wei Chin: a1782423
  - Faisal Hawsawi: a1822781
  - Lina Nehme: a1802697
  - Ran Qi: a1675122
  - Joseph Toubia: a1753547
  - Zemin Wong: a1780385
  - Jixing Ye: a1798631
  - Yu Zheng: a1739446

Snapshots (Group):

I attended the initial sprint planning meeting on August 16 with the teammates, Here is the documentation:

Product Backlog (See Figure)

Task Board (See Figure)

Sprint Backlog (See Figure)

User Stories & DoD

During the first sprint, most of the work is to understand client's requirements and deduce user stories. After meeting with the clients, we selected the most important user stories, which are the key feature of our product:

"As a data annotator, I want to upload an incident report, annotate it and save it so that users can use the file later for analysis."

"As a user, I want to be able to visualize the attack flows in a graphical format so that I can easily understand the patterns and trends in the data."

Based on the user stories, we derived below tasks:

- Research on attack flow (sample files, current projects, tools available, etc)
  - DoD: testing MITRE attackflow builder & visualization tool and discuss the experience in sprint 1 meeting 2

- Propose software architecture
    - DoD: A UML graph showing the software architecture
- Research tech stack and code standards
    - produce a list of technologies to be used for the front end and back end, with justification

Summary of Changes:

In this initial snapshot, we have laid the foundation for our project by defining the user stories based on the project's objectives. The team has been actively collaborating to set up the product backlog , task board, meeting schedules, communication platforms, etc. Preliminary discussions with Associate Professor Hung Nguyen have provided valuable insights, guiding our approach. The team is motivated and committed to ensuring the project's success.

Changes in this week's snapshot:

- Defined a list of user stories, functional & non-functional requirements.
- Decided on the platform (web app) and proposed software architecture accordingly.
- Decided on the tech stack (database, framework, coding language, IDE)

What went well in the sprint (Individually Written)?

In the recent sprint, our ensemble embarked on a journey to comprehend the intricate requirements of our client, culminating in the derivation of pivotal user stories. A quintessential example of this endeavor was the user story: "As a data annotator, I want to upload an incident report, annotate it, and subsequently save it, facilitating users to later utilize the file for meticulous analysis." This narrative not only elucidated the core functionalities our software should possess but also provided a roadmap for our developmental trajectory.

Furthermore, our collective efforts were channeled into researching the multifaceted realm of attack flow. This exploration was not a mere academic exercise; it was a strategic initiative to ensure our software would be equipped to handle real-world challenges. The Definition of Done (DoD) for this task was particularly enlightening: testing the MITRE attack flow builder & visualization tool and subsequently discussing the experience in our sprint meeting. Such endeavors ensured that our software would not only be functional but also resonate with the needs of the cybersecurity community.

What could be improved (Individually Written)?

One of the salient observations postulated from our kick-off meeting was the potential for a more profound preparatory phase. While the meeting was rife with insights, a more in-depth perusal of the provided documentation prior to the meeting could have been advantageous. Such a preparatory act would have equipped us with a repertoire of incisive questions, thereby extracting maximal value from our interactions. For instance, our query regarding the incorporation of a tool for document annotation could have been more nuanced, had we delved deeper into the project's intricacies beforehand.

Furthermore, while our user stories were meticulously crafted, reflecting the project's objectives, there lies an opportunity to refine them further. The essence of a user story is not just to delineate functionalities but to resonate with the end-users' aspirations. A more immersive engagement with potential users, perhaps through focus group discussions or surveys, could elucidate nuances that might currently elude us.

What will the group commit to improve in the next sprint (Individually Written)?

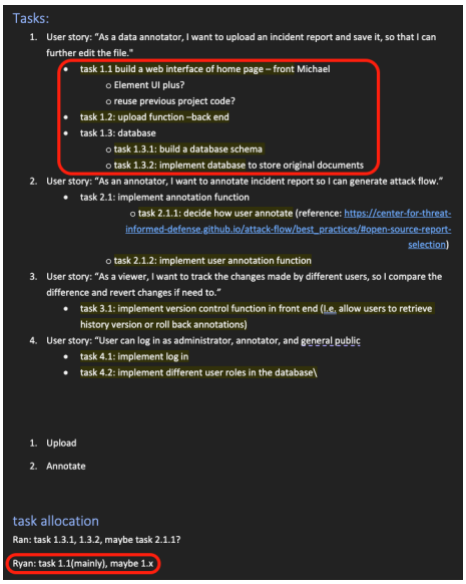
A salient commitment revolves around the interface design. Given the revelation that the initial interface will commence as a hand-drawn sketch, it becomes imperative to ensure that this rudimentary representation is both comprehensive and resonant with user aspirations. This sketch will serve as the bedrock upon which subsequent design iterations will be predicated. Thus, meticulous attention to detail, coupled with feedback from potential users, will be paramount. This endeavor will not just enhance the user experience but will also expedite subsequent developmental phases, ensuring that the software's architecture and functionalities are in harmony with the interface.

Furthermore, addressing the previously identified need for a more profound preparatory phase, our team will institute a regimen of pre-meeting readings and discussions. This will not only optimize our interactions with stakeholders but also engender a culture of proactive inquiry, ensuring that every team member is not just a passive participant but an active contributor to the project's trajectory.

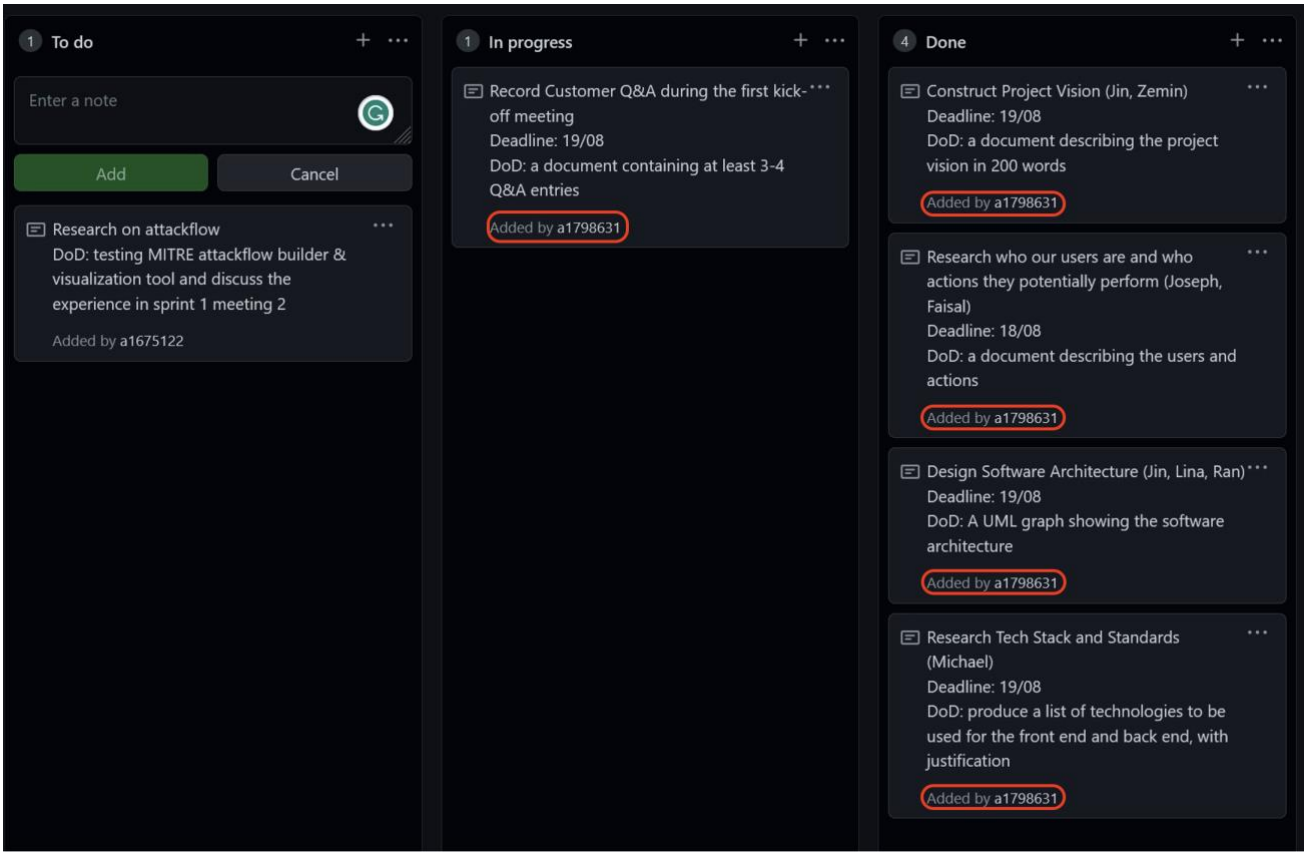
Comment on your progress this sprint (Individually Written)

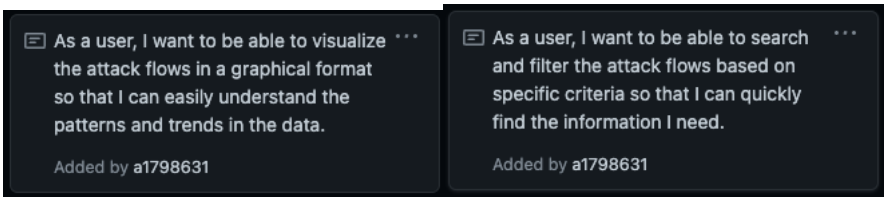
What I have done:

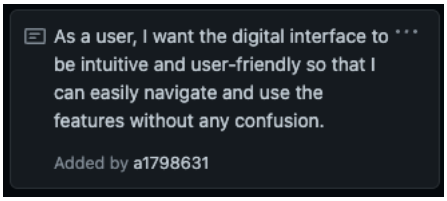
1. Participated in all the meetings and engaged in discussions.
2. Would be in charge of building web interface.



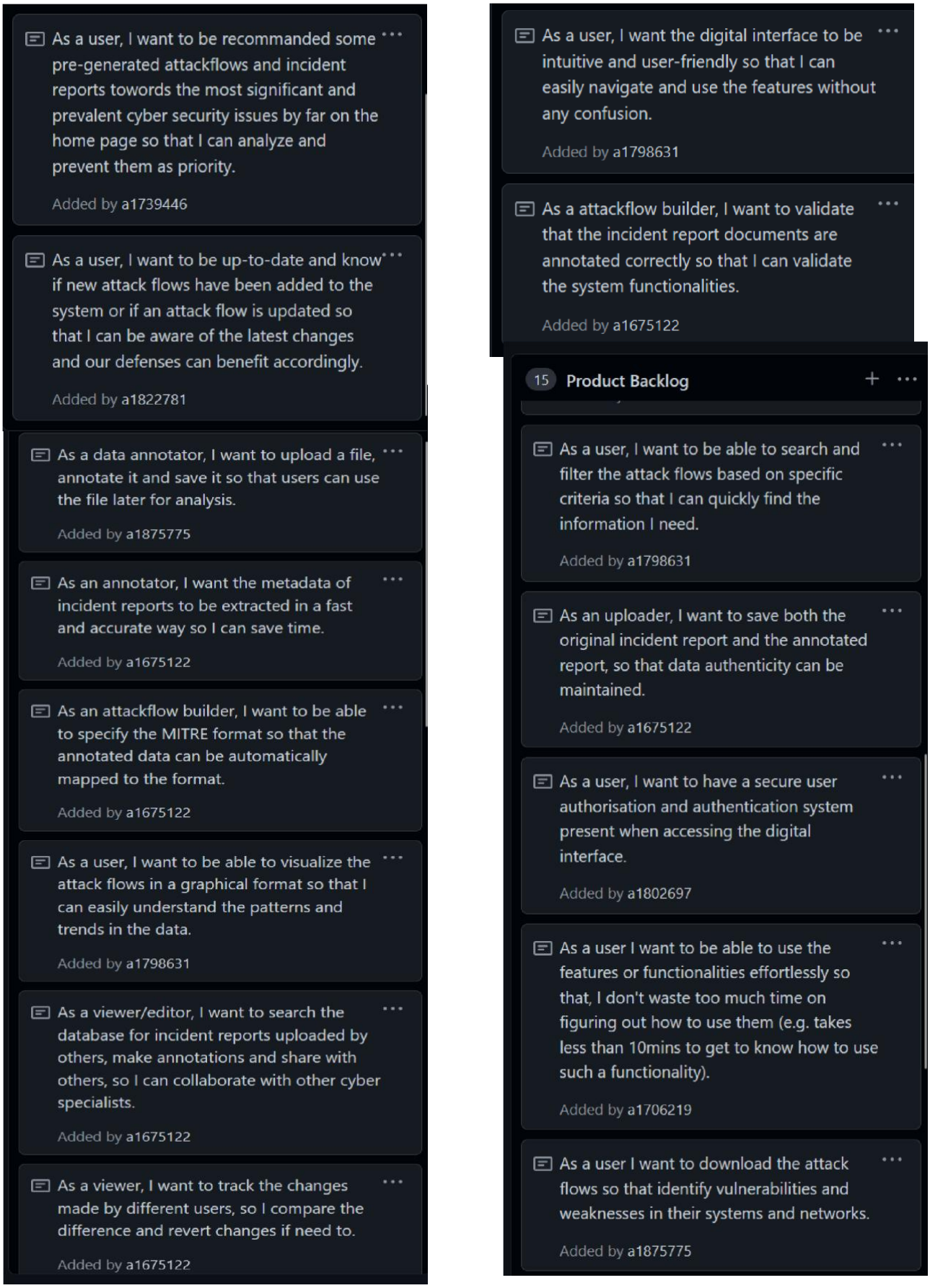
3. Contributed to posting on GitHub backlogs and task board.







Appendix


As a user, I want to be recommanded some pre-generated attackflows and incident reports towords the most significant and prevalent cyber security issues by far on the home page so that I can analyze and prevent them as priority.
Added by a1739446
As a user, I want to be up-to-date and know if new attack flows have been added to the system or if an attack flow is updated so that I can be aware of the latest changes and our defenses can benefit accordingly.
Added by a1822781
As a data annotator, I want to upload a file, annotate it and save it so that users can use the file later for analysis.
Added by a1875775
As an annotator, I want the metadata of incident reports to be extracted in a fast and accurate way so I can save time.
Added by a1675122
As an attackflow builder, I want to be able to specify the MITRE format so that the annotated data can be automatically mapped to the format.
Added by a1675122
As a user, I want to be able to visualize the attack flows in a graphical format so that I can easily understand the patterns and trends in the data.
Added by a1798631
As a viewer/editor, I want to search the database for incident reports uploaded by others, make annotations and share with others, so I can collaborate with other cyber specialists.
Added by a1675122
As a viewer, I want to track the changes made by different users, so I compare the difference and revert changes if need to.
Added by a1675122
As a user, I want the digital interface to be intuitive and user-friendly so that I can easily navigate and use the features without any confusion.
Added by a1798631
As a attackflow builder, I want to validate that the incident report documents are annotated correctly so that I can validate the system functionalities.
Added by a1675122
15 Product Backlog
As a user, I want to be able to search and filter the attack flows based on specific criteria so that I can quickly find the information I need.
Added by a1798631
As an uploader, I want to save both the original incident report and the annotated report, so that data authenticity can be maintained.
Added by a1675122
As a user, I want to have a secure user authorisation and authentication system present when accessing the digital interface.
Added by a1802697
As a user I want to be able to use the features or functionalities effortlessly so that, I don't waste too much time on figuring out how to use them (e.g. takes less than 10mins to get to know how to use such a functionality).
Added by a1706219
As a user I want to download the attack flows so that identify vulnerabilities and weaknesses in their systems and networks.
Added by a1875775