Snapshot Week 11 of Group AttackFlow1

Building a dataset of real-world cyber-attacks with Attack Flow

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

October 23, 2023

Product Backlog

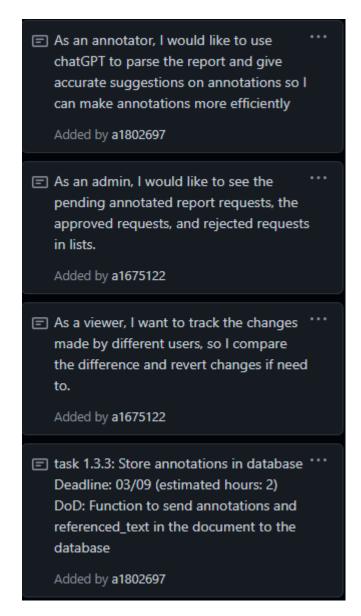


Figure 1: Product Backlog (Sprint 6) 1 of 5

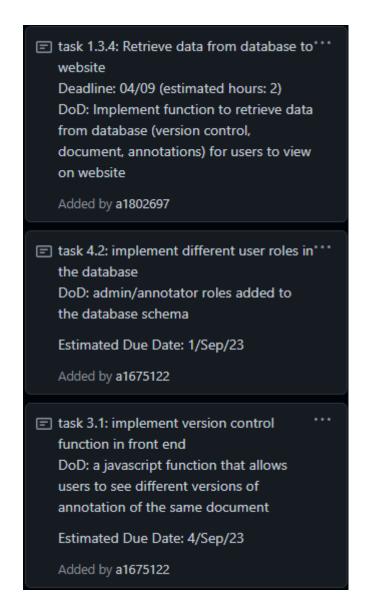


Figure 2: Product Backlog (Sprint 6) 2 of 5

■ task 1.3.2: implement database to store original documents DoD: MariaDB set up according to the database schema Estimated Due Date: 31/Aug/23 Added by **a1675122** As an annotator, I would like to check the *** status of my submitted annotations, so I can see if my annotations are approved, rejected (with reasons), or pending approval. 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

Figure 3: Product Backlog (Sprint 6) 3 of 5

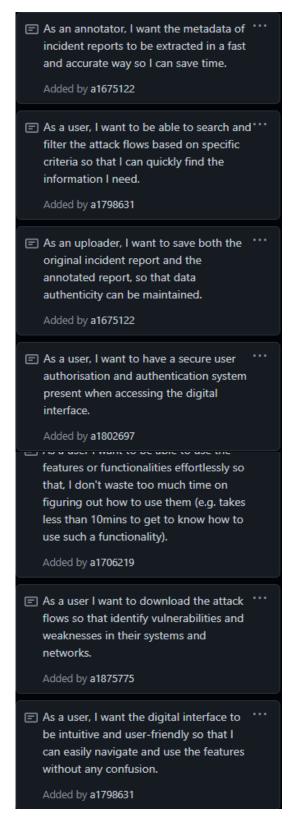


Figure 4: Product Backlog (Sprint 6) 4 of 5

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** some pre-generated attackflows and incident reports towards 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 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

Figure 5: Product Backlog (Sprint 6) 5 of 5

Task Board

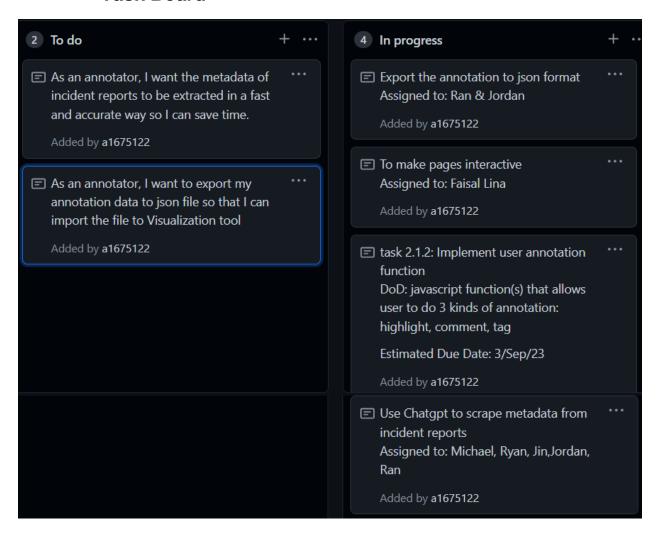


Figure 6: Task board (Sprint 6)

Sprint Backlog

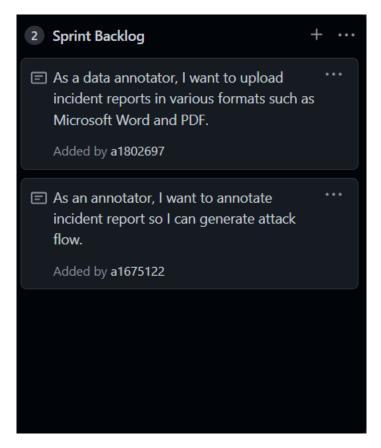


Figure 7: Sprint Backlog (Sprint 6)

User Stories

In the final weeks now and all our focus and resources are on the annotation process with ChatGPT, we are trying to utilise it as much as possible given the time frame. We have added the pre-defined tags to the annotation page as well as a highlighting function to help the annotator. Finally, we need to implement the annotator functionality including incident report management pending requests, rejected requests and approved requests, and Administrator functionality including annotator management and incident report management as with the annotator functionality.

- "As a data annotator, I want to upload an incident report and save it so that I can further edit the file."
 - Related tasks:

task 1.2: upload function

task 1.3.2: implement database to store original documents

- "As an annotator, I want to annotate incident report so I can generate attack flow."
 - Related tasks:

task 2.1.1: decide how user annotate

task 2.1.2: implement user annotation function

task 2.1.3: integrate ChatGPT to parse report and give accurate annotation suggestions

- "As an admin, I would like to see the pending annotated report requests, the approved requests, and rejected requests in lists."
 - Related tasks:

task 1.3.3: Store annotatations in database

task 4.2: Implement different user roles in the database

Definition of Done

The individual DoD of each task can be seen on the screenshot of the task board. In summary, the goals are:

- · Testing the integrated backend functions works as we expected.
- · Code is well-documented and adheres to our coding standards.
- Explain and ensure that all the scrum members understand the specifics of the tasks and how to construct the implementation.

Summary of Changes

The upload and annotate functions are still under the spotlight to get the best possible functionality and we are still trying to get the most functionality out of ChatGPT. Both Administrator and Annotator user roles are still the main focus as suggested above, however, some functionality has been implemented.

- Annotation function to be completed. We will continue with the
 annotate functionality including how to annotate? How to use
 keywords/tags? How to use predefined keywords/tags? How to incorporate
 keywords from Mitre Att&ck? Must identify tags and be able to manually
 search from drop down menu to define relevant tag as well as profile
 functionality.
- This snapshot re-enstates the major role of ChatGPT to extract metadata. We have now decided to utilise the ChatGPT as much as possible in our web application to extract metadata.
- Administrator functionality to be implemented. The administrator functionality needs to be implemented including annotator management (delete annotator from the database and else) incident report management (pending request, approved request, rejected request).