

Sprint Review Meeting Minutes

Attendees: Aykhan Pashayev, Charlie Iglesias, Cheng Zhang, Alex Linghay Eng, Nicolas Su Nobrega

Start Time: 6:50 PM EST

End Time: 7:25 PM EST

Meeting Notes:

We met with the product owner to go over what we worked on this sprint. Feedback was given after each team member presented the work they had been given. Stories that need more work will be put back into the backlog for improvement, while completed stories were accepted into the increment.

Accepted User Stories:

- Detection pipeline operational - The end-to-end pipeline for parsing CloudTrail logs, normalizing data into the defined schema, and applying rule-based anomaly detection is now functional. Incidents are successfully generated based on suspicious identity behaviors.
- Flask API implementation - A REST API was created using Flask to expose detected incidents. The API allows the frontend to pull structured incident data, preparing the system for UI integration and demo testing.
- Schema finalization - The internal incident schema was finalized to ensure consistency between detection logic, API responses, and future UI consumption. This ensures reliable data flow across system components.

Rejected User Stories:

- Frontend integration with API - Although the UI has been developed, integration with the Flask API has not yet been completed. The frontend still needs to connect to the API to dynamically pull and display incident data.
- AI chatbot integration using Gemini - The AI chatbot feature, which will allow users to ask questions about detected incidents and receive handling recommendations, has not yet been implemented. This feature is planned for the next sprint after successful demo validation of the detection system.