

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:

- Recent CloudTrail events extracted and formatted - recent CloudTrail events were extracted and formatted into a consistent schema. This prepared data for consumption by both detection logic and the UI for visual representation.
- Realistic test actors and simulated CloudTrail activity - test actors were created, and simulated CloudTrail activity was generated to validate anomaly detection logic.
- Rule-based anomaly detection logic - initial rule-based detection logic was implemented to flag suspicious identity behaviors.

Rejected User Stories:

- Structured AI explanations for detected incidents - structured AI explanations were partially explored but not finalized. Additional development is needed to generate understandable insights for each detected incident.
- UI updates - the UI update was not completed for this sprint. Visual integration of real-time events and incident data will continue in the next sprint.