

Sprint Backlog Grooming Meeting Minutes

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

Start Time: 7:30 PM EST

End Time: 8:00 PM EST

Meeting Notes:

The team met to groom and refine backlog items related to log normalization, anomaly explanation, AI integration, and UI visualization. Responsibilities were clarified across the team to ensure smooth handoffs between backend processing, AI analysis, and frontend presentation.

User Stories Created/Discussed/Refined/Prioritized:

- Full UI–Backend Integration – As a stakeholder, I want the UI fully integrated with live backend APIs so detected incidents and CloudTrail events are displayed dynamically instead of relying on mock data.
- End-to-End System Testing – As a QA tester, I want complete end-to-end testing of the ingestion → detection → incident → UI pipeline so the team can verify that the entire system functions correctly without failures between stages.
- UI Filtering and Sorting Features – As a SOC analyst, I want filtering and sorting options in the interface so suspicious activity can be investigated quickly and efficiently.
- Structured Logging and Error Handling – As a DevOps engineer, I want structured logging and proper error handling implemented across API endpoints so system failures can be diagnosed during testing and the final demo.
- Final Demo Dataset and Test Scenarios – As a project lead, I want a finalized validation dataset and documented test scenarios so the team can demonstrate system behavior under both normal and anomalous activity conditions.

Questions & Answers:

- What does full UI–backend integration involve for the system?
The UI will connect directly to backend APIs that provide CloudTrail events, anomaly detections, and incident explanations.
- Why is end-to-end testing necessary at this stage of the project?

End-to-end testing confirms that data flows correctly through the entire pipeline, ensuring that the system works.

- How will filtering and sorting help SOC analysts?

These features allow analysts narrow down suspicious activity by focusing on specific IAM users, event types, or severity levels, improving investigation efficiency.