

Sprint Retrospective Meeting Minutes:

Date: 2/8/2026

Attendees: Max Gleiberman, Julian Hernandez, Nathan Mahabeer, Elizabeth Hechavarria

Start time: 3:00pm

End time: 3:20pm

1. Sprint Goals Review

- **Goal:** Complete SIEM Dashboards & Detection Rules (User Story #4) and begin progress on Risk Assessment & Documentation (User Story #5).
- **Status: User Story #4:** Completed — SIEM dashboards were finalized, detection rules were tuned, and visualizations accurately displayed correlated security events. **User Story #5:** In progress — Initial planning and outlining have begun, but full documentation and risk assessment are not yet complete.
- **Note:** All other sprint stories are complete except for User Story #5, which is in progress.

2. What Went Well

- SIEM platform remained stable and responsive during dashboard validation and testing.
- Dashboard panels accurately visualized port scans, brute-force attacks, and data exfiltration events.
- Detection rules were refined and produced consistent, reliable alerts.
- Team collaboration was strong during dashboard formatting, testing, and tuning.
- Improved automation scripts enabled faster event generation for validation purposes.

3. Challenges / What Went Wrong

- Some dashboard widgets required multiple formatting passes to ensure proper alignment and readability.
- Correlation logic for less common or edge-case attack patterns required additional tuning.

- Documentation updates, particularly for detection rules and dashboards, took longer than anticipated.

4. Action Items / Improvements

- Continue developing the risk assessment and supporting documentation for **User Story #5**.
- Further improve automation scripts to streamline dashboard testing and validation.
- Continue refining correlation thresholds for edge-case events.
- Ensure final documentation includes complete dashboard configurations and detection rule mappings.
-

5. Team Performance

- **Strengths:** Strong teamwork, improved troubleshooting efficiency, solid SIEM and dashboard configuration work.
- **Improvements:** Increase speed of documentation creation and dashboard polish.

6. Previous Retrospective Issues

- Noise issues from advanced detection logic largely resolved.
- Dashboard accuracy and formatting issues from prior sprint fully addressed.