

Sprint Retrospective Meeting Minutes:

Date: 1/25/2026

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

Start time: 5:30pm

End time: 6:00pm

1. Sprint Goals Review

- **Goal:** Complete SIEM Dashboards & Detection Rules (User Story #4) and verify accurate visualization of SIEM events.
- **Status:** Completed — Dashboards were finalized, detection rules were tuned, and all visualizations correctly displayed correlated events.
- **Note:** All other sprint stories are complete except for User Story #5, which is in progress.

2. What Went Well

- SIEM remained stable and responsive during dashboard validation.
- Dashboard panels accurately displayed port scan, brute-force, and data exfiltration events.
- Detection rules were refined and produced consistent alerting.
- Team collaborated effectively to complete dashboard formatting and testing.
- Improvements to scripts allowed quicker event generation for validation.

3. Challenges / What Went Wrong

- Some dashboard widgets required multiple formatting passes to align correctly.
- Correlation logic for less common attack patterns needed extra tuning.
- Documentation of detection rule updates took longer than planned.

4. Action Items / Improvements

- Begin drafting risk assessment details for User Story #5 (still in progress).
- Improve automation scripts for dashboard testing and validation.

- Continue tuning correlation thresholds for edge-case events.
- Ensure documentation includes finalized dashboard configurations and 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.