Better Together using Observability tools for SIEM and Analytics

- **Speakers**: Mathias Palmersheim, Josh Lee
- **Room**: CC 236
- **Time**: Sun 2:00 pm – 2:30 pm

- **Format**: Lecture (30 Min + Q&A)
- **Difficulty**: Some experience required
- **Track**: Security / Privacy
- **Additional Tags**: DevOps
- **Presenter Location**: In-person
- **Experience**: several-th time speaking

Description:

Finding root causes during outages or security incidents is hard enough — but it becomes far more difficult when every team uses a different toolset. This talk explores why observability and SIEM tools are **better together**, and how unifying them can dramatically improve communication, reduce toil, and cut costs.

Mathias and Josh explain how, despite different stakeholders (SRE, Security, Business Analysts), the underlying data problem is the same: collecting, streaming, processing, storing, and analyzing events. They show how a **unified pipeline** can serve all these needs while improving user experience and reducing operational friction.

Attendees will learn:

- Why combining observability and SIEM tools creates better outcomes
- The challenges of merging toolchains and how to overcome them
- How to design a unified observability solution that delivers the right data to every stakeholder

The result: SRE, Security, and Business teams can all get what they need from a shared, coherent data ecosystem.

Target Audience:

- SRE practitioners
- Security practitioners