Security Fails at the Handoff: Rethinking Shared Responsibility in Opensource

- **Speaker**: Autumn Nash
- **Room**: HC 108
- **Time**: Sat 2:00 pm – 2:30 pm

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

Description:

The shared responsibility model is widely referenced in Linux and open-source security — but rarely understood the same way by everyone involved. Security failures often arise not from missing tools or unpatched systems, but from **broken handoffs** between policy, platform, and people.

Unless you've worked inside open-source projects, the way maintainers handle security issues, CVEs, patches, and distro maintenance can feel mysterious. This leads to false assumptions about who is responsible for what.

This talk examines where security intent gets lost as governance teams define policies, open-source politics collide, platform teams translate requirements into systems, and engineers live with the operational consequences. Attendees will gain a practical mental model for open-source security ownership:

- What belongs upstream
- What a distribution provides
- What ultimately falls on *you*

By improving handoffs and clarifying responsibility, teams can reduce risk more effectively than by adding yet another security tool.

Target Audience:

- Anyone working with open-source security
- Engineers
- Platform teams
- Security practitioners