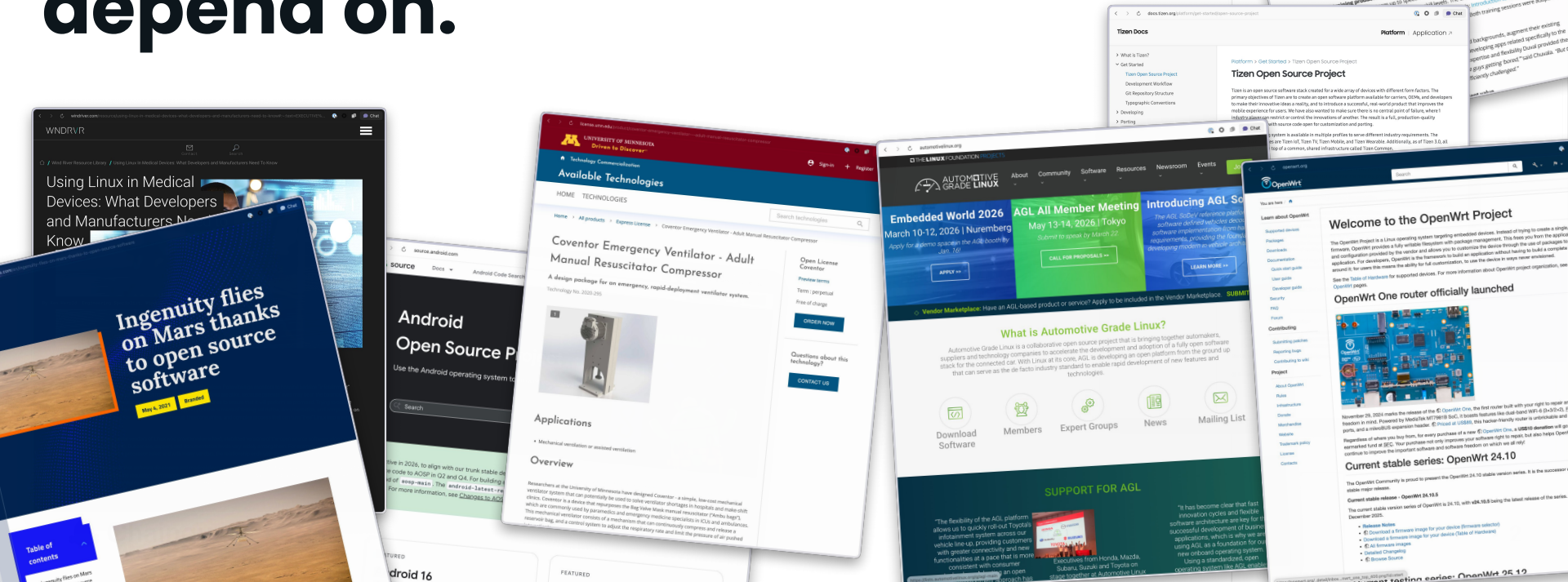
$ whoami › Kalle Westerling

Currently, **Senior Developer Relations Engineer** at **Chainguard**, leading self-paced training initiative at **courses.chainguard.dev**

Previously in engineering & product-oriented roles in **national open science research institutions in the UK and US**

linkedin.com/in/kallewesterling

Open source isn’t just software we use; it’s infrastructure we depend on.



Open source is an ecosystem or an operating model

- Open licenses → legal permission to use, modify, share
- Community activity → actual people (increasingly also bots + agents) maintaining, reviewing, responding
- Infrastructure → build systems, signing, release, trust

How is a piece of software produced and updated?

How do code fixes actually reach users, and can do they trust them?

How is trust established when there is no single person is in charge?

What happens when something breaks downstream?

What has changed?

- ~~There's more open source~~
- We consume OSS differently: Software is assembled automatically
  - Code pulls in dependencies on its own
  - Systems rebuild and redeploy constantly
  - Updates flow through, sometimes without a human ever touching them
  - And the latest news: code-authoring AI tools are dreaming up completely new codebases.

...but our trust model hasn't really changed. We still rely on:

- Manual + human reviews
- Best effort maintenance
- Diffused responsibility

What has changed?

Can we use open source safely?

How do we responsibly depend on open source?

Who and what systems are accountable?

How quickly can we fix problems that appear?

How do downstream users know what or who to trust?

Open source as critical infrastructure

- **Shared maintenance** instead of everyone patching alone
- **Building from source**, not trusting opaque binaries
- **Clear provenance** and **repeatable builds**
- **Fast (automated?) remediation** when issues appear
- ***Making the secure path the default***, not the exception

Overall goal: Make trust boring, automated, and reliable

Safe open source is a community responsibility

Open source isn't just something we use, open source is something we all rely on. As such, it is critical infrastructure.

The challenge becomes not ~~Can we use open source safely?~~ but How do we responsibly depend on open source?

linkedin.com/in/kallewesterling