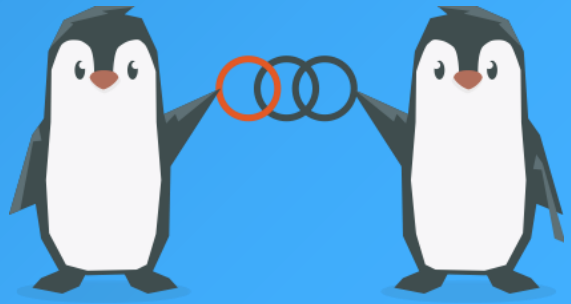
OpenChain SBOM WG

2026-02-18

THE LINUX FOUNDATION

OPENCHAIN



Anti-Trust Policy Notice

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.
- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/ antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

FOSS license and security compliance tools workshop

FOSDEM 2026 Fringe Event

- **A workshop designed to facilitate dialogue between tool developers and users. By sharing development plans and practical feedback, participants will identify synergies to enhance the lifecycle of SBOM creation and utilization.**

FOSDEM 2026 Fringe: FOSS license and security compliance tools workshop Fri, Jan. 30, 2026

Interested in open source license and security compliance? Join us for a one-day workshop for developers and users of open source compliance tools on Friday, January 30th, 2026 in Brussels just before FOSDEM 2026.

Our goal is for open source developers, users, and contributors to exchange requirements, plans, and collaboration opportunities around FOSS tools for software provenance detection, vulnerability management, license detection and regulatory compliance like CRA, code scanning, package dependency analysis, container analysis, SBOM creation and consumption, and license or vulnerability databases - basically, all the tools you need to figure out which FOSS code you use, where it is from, what is license, how to comply with the license, and whether it contains vulnerable code.

Previous attendees include developers from ORT, ScanCode, ClearlyDefined, FOSSology, Tern, FSFE REUSE, SW360, BANG, Hermine, Opossum, SPDX tools, DoubleOpen, OpenChain, and AboutCode projects along with users from leading technology and industrial companies, open source foundations, and government institutions worldwi
Whether you are a developer or user interested in the tools for Software Supply Chain and SBOMs, a FOSS license-savvy lawyer, a compliance or security analyst, or an OSPO member: **you will be warmly welcomed**.

<https://workshop.aboutcode.org/>

Schedule – All times CET (UTC+1)

The day will be split in two:
1) The morning will focus on **tool developers** to announce and share their plans, and discuss opportunities for collaboration across projects.
2) The afternoon will focus on **tool users** to share their concerns, problems and requirements, and address these in the represented projects.

8:30 Registration with coffee and light breakfast

9:00 Welcome and introductions

9:30 FOSS compliance tool developers, present your plans!

Each open source project will present their plans for releases and upcoming features with a 5 minute lightning talk.
We likely already know what your tool does, though a short intro is OK. We will use flip charts, big post-its, and markers to support the presentations and discussions – there will not be a projector/beamer, so do not plan for it.

11:15 Discuss collaboration opportunities

How can we work together to overcome shared challenges, and make tools interoperable and compatible so we can deliver better value to all our users?

12:15 Lunch break

This is funded by attendees and our generous sponsors!

13:15 FOSS compliance tool users, give us your requirements!

Each user presents their concerns, problems and requirements

15:00 Coffee break

15:30 Discuss collaboration and joint development opportunities

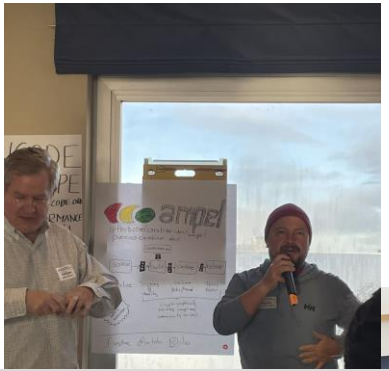
16:30 Workshop conclusion and recap

17:00 Drinks at rooftop bar (inside)

THE LINUX FOUNDATION

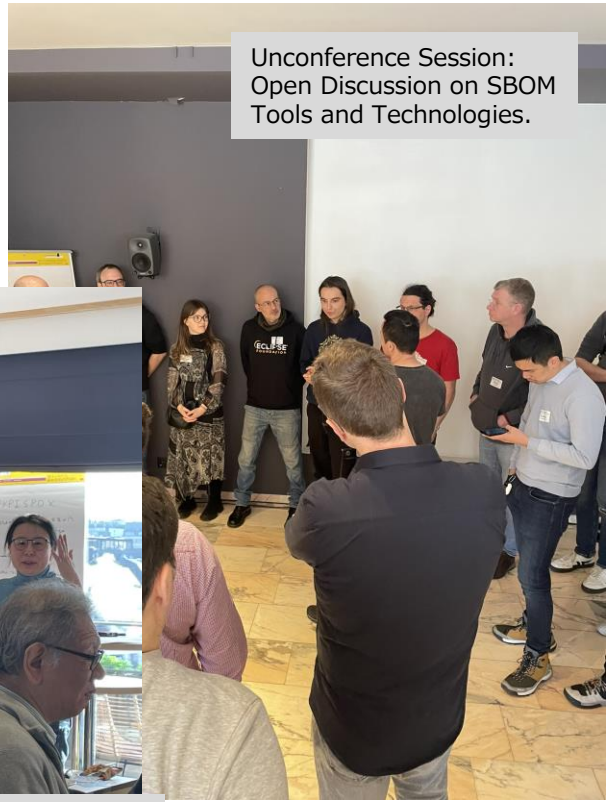
OPENCHAIN

FOSS license and security compliance tools workshop (AboutCode workshop)



Adolfo -san presents Ampel, a tool designed to assess SBOM quality and visualize the results through clear signals.

Qing -san on ClearlyDefined: Understanding its role and impact.



Unconference Session: Open Discussion on SBOM Tools and Technologies.

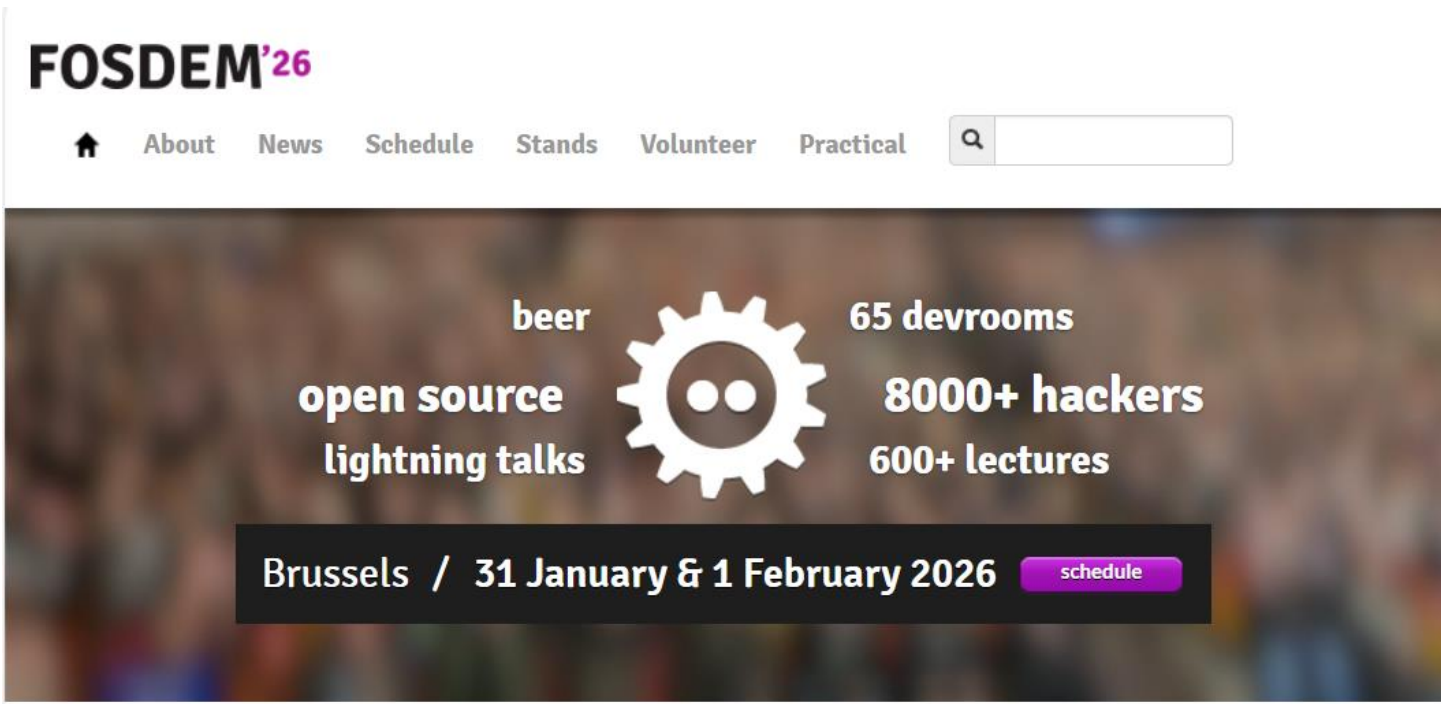
Daniel –san on Curl
Greg K.H. –san on linux kernel

Workshop Summary: From "Users" to "Active Contributors“ This three-part workshop featured OSS tool demos, an unconference on current challenges, and a final keynote from a prominent developer.

The Key Message:
The OSS community has no obligation to fix vulnerabilities.
The Risk: With the Cyber Resilience Act (CRA) approaching, relying solely on the community for security patches is now a fatal risk.
The Action: We must shift from being mere "users" to "active contributors" who take ownership of vulnerability fixes. Our top priority is to improve internal processes and build a development framework that collaborates directly with OSS communities.

THE LINUX FOUNDATION
OPENCHAIN

<https://fosdem.org/2026/>



Our Focus Areas: SBOM and Supply Chain, CRA in Practice, Legal & Policy

THE LINUX FOUNDATION

OPENCHAIN

On-site at FOSDEM

Survival Guide: Venue & Food
The event takes place at ULB, a massive 12-hectare campus. Since there are few nearby hotels, most attendees commute 30 minutes from the city center. Be prepared for packed buses and trams. While food trucks are available, buying lunch can be difficult due to the crowds. We highly recommend bringing your own food and drinks.

Stands (Community Booth): Extremely Crowded

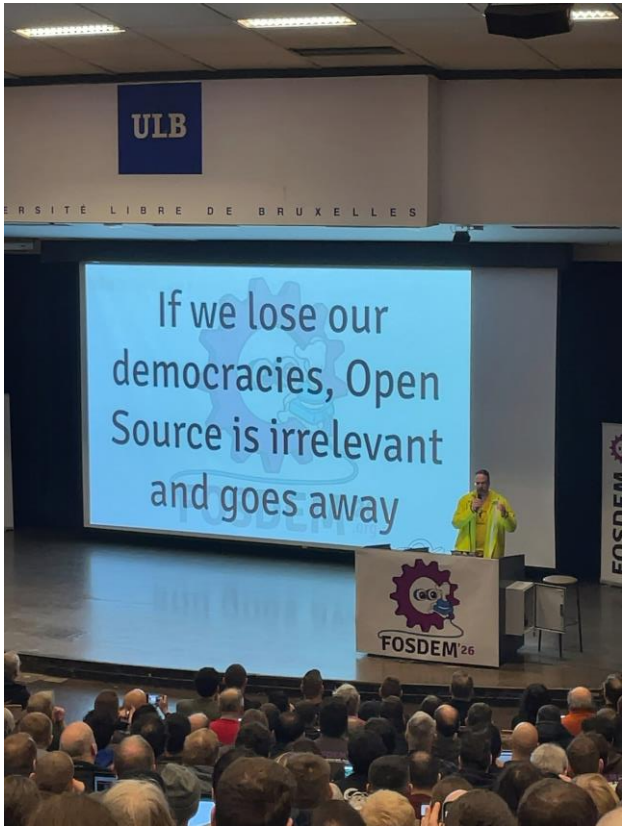
Overwhelming Crowd at the Keynote (1,500+ People)

THE LINUX FOUNDATION

OPENCHAIN

Opening Keynote

https://fosdem.org/2026/schedule/event/SFKNTZ-welcome_to_fosdem_2026/



The Essence of FOSDEM: Beyond the Session

The heart of FOSDEM lies in the "Hallway Track." While the opening keynote on Digital Sovereignty and Democracy drew thunderous applause from over 1,500 attendees, the real magic happens in the corridors.

This is a massive, autonomous ecosystem: 1,000+ sessions and 100+ community stands, all operated by volunteers and provided free of charge. From the custom Wi-Fi to the privacy-focused Matrix protocol, everything is built by the community, for the community.

On-site, you see students, executives, and families discussing Open Source as equals. It is clear that OSS is no longer just a tool, it is the essential social infrastructure nurturing Europe's next generation.

Beyond gaining technical knowledge, this experience proved the vital importance of touching the raw passion of the open-source community firsthand.

THE LINUX FOUNDATION

OPENCHAIN

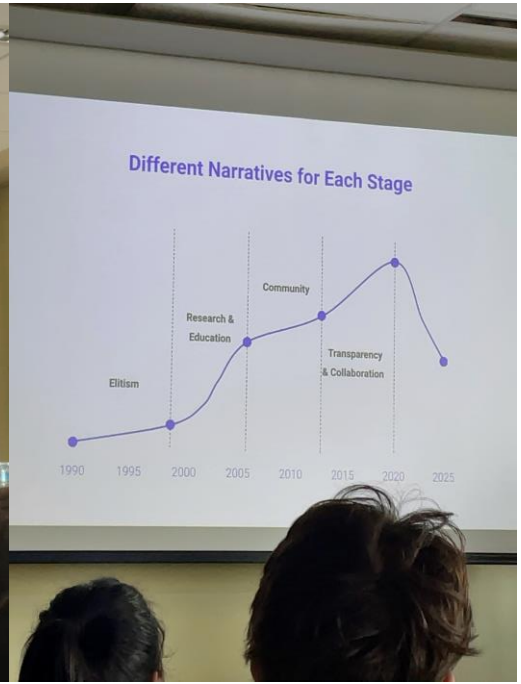
Legal &Policy Devroom

It really feels like 2026, with the full enforcement of the CRA just around the corner next year. I'd heard the Legal & Policy devroom wasn't that crowded last year, but this time it was packed. Despite the legal nature of the discussions, I was impressed by how much the organizers seemed to be enjoying themselves.

In a context separate from SBOMs, I had breakfast with Matthias-san from the FSFE, one of the devroom organizers, to talk about things like the translation of Ada & Zangemann. It was a great way to start the day before diving into the legal sessions.

https://fosdem.org/2026/schedule/event/9HAMJC-fork_the_government_the_back_and_forth_open_source_advocacy_road_in_taiwan/

Fork the Government : The Back and Forth Open Source Advocacy Road in Taiwan

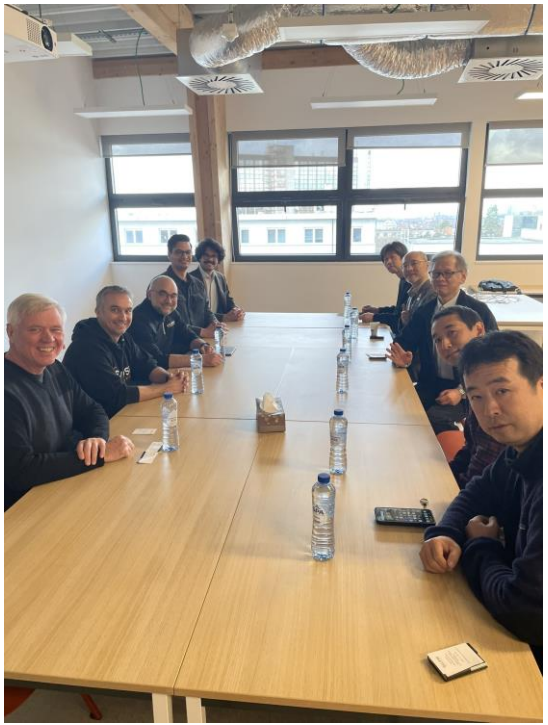


Rosalind Liu-san analyzed how Taiwan's open-source movement evolved from its 1990s roots into a force for digital democracy through g0v and the 2014 Sunflower Movement, yet now faces a strategic mismatch between its ideals and the hardware economy **due to fragmented narratives across cost, transparency, and sovereign technology**.

THE LINUX FOUNDATION

OPENCHAIN

Meetup with Eclipse Foundation



Overview
A strategic deep-dive with **NEC/CNCF (Muto-san) and Renesas (Ito-san) from OpenChain Japan** regarding the **Eclipse Foundation's ORC WG** and the impact of the **Cyber Resilience Act (CRA)**.

Strategic Pillars
Alignment: Defining the roles of CRA vs. Eclipse ORC WG in the global ecosystem.
Responsibility: Analyzing supply chain impact and the division of liability.
Implementation: Moving from SBOM theory to practical, automated toolchains.

Technical Focus
Granularity: Determining the necessary depth of dependency tracking and provenance.
Evidence: Establishing documentation standards for regulators and partners.
Synergy: Collaborating with **OCCTET** and **OpenChain SBOM WG** for Quality Guide etc.

Call to Action
Community lead and Corporate OSPOs should lead these cross-industry and cross-community initiatives and escalate findings to executive management to drive compliance readiness.

THE LINUX FOUNDATION
OPENCHAIN

SBOM Devroom

We attended an all-day SBOM session held in a reserved auditorium. As expected from the advance buzz, the venue was packed. While we could enter without waiting during the early morning hours, once we stepped out, getting back in meant waiting for quite some time.

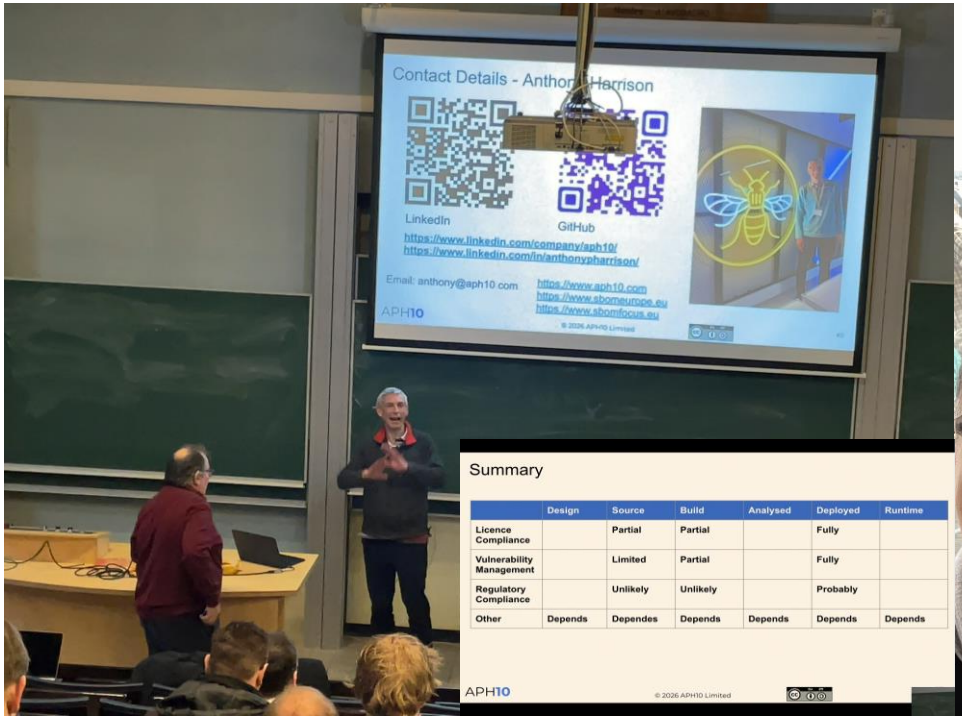
Among the participants, I only saw a few acquaintances from Japan, which made me feel that greater participation from the Asian community especially from the Japanese community would be valuable.

THE LINUX FOUNDATION

OPENCHAIN

https://fosdem.org/2026/schedule/event/DVPCJC-the_day_in_a_life_of_a_sbom/

The day in a life of a SBOM



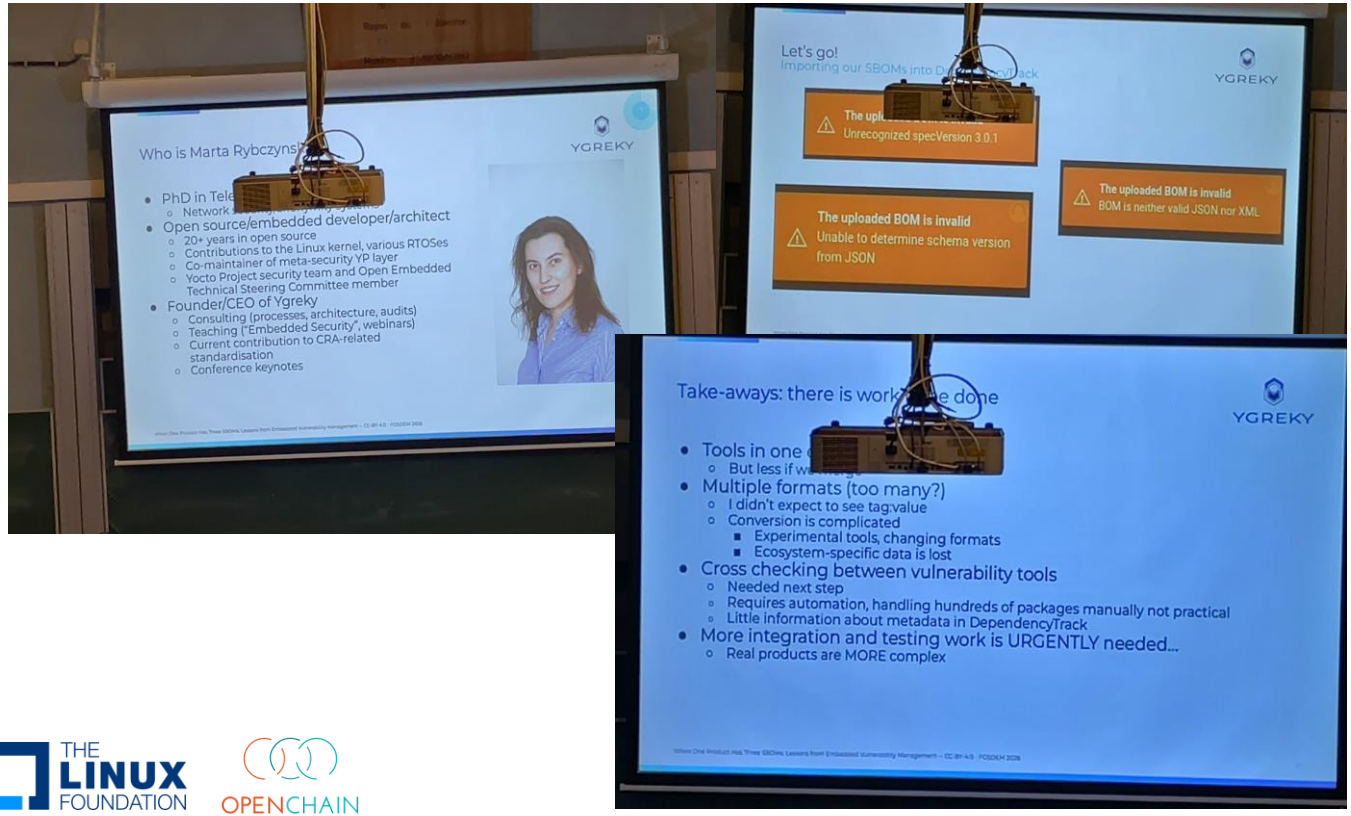
The first session was by Anthony Harrison - san, whom I was finally able to meet in person.

Due to train congestion, I wasn't able to join the session in real-time, but I have since watched the recording. While ‘Build SBOM’ Type remain the primary focus of current discussions, **his talk highlighted why Deployed SBOMs are so essential**.

THE LINUX FOUNDATION
OPENCHAIN

https://fosdem.org/2026/schedule/event/7YG9H7-embedded-product-with-three-sboms/

When One Product Has Three SBOMs: Lessons from Embedded Vulnerability Management

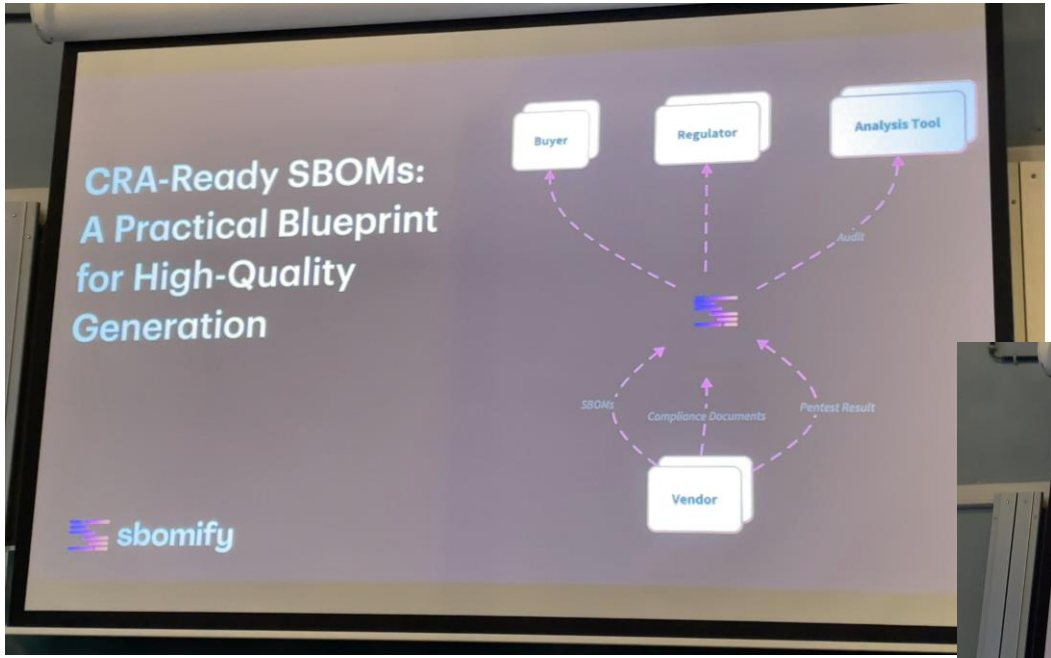


Real-world efforts to operationalize SBOMs generated by Kernel, Yocto, and Zephyr were shared. A primary challenge is **the format disparity between embedded-focused SBOMs (SPDX/CycloneDX) and information loss during conversion.** Missing package names or versions lead to incomplete dependency mapping and inaccurate vulnerability analysis. To mitigate this, speakers recommended prioritizing native SBOM output from tools and cross-checking converted data across multiple scanners to verify integrity. The session **emphasized the ongoing need for community-driven interoperability improvements and integrated testing**.

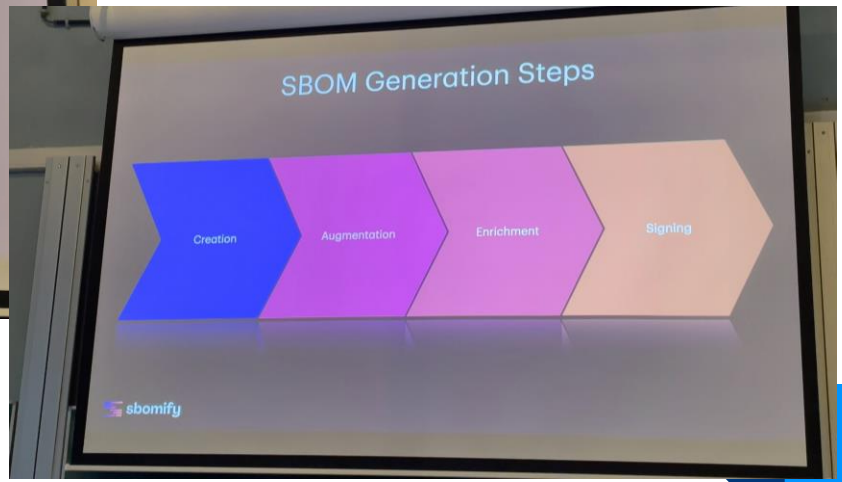
THE LINUX FOUNDATION
OPENCHAIN

https://fosdem.org/2026/schedule/event/UYTGWA-sbom-generation/

CRA-Ready SBOMs: A Practical Blueprint for High-Quality Generation



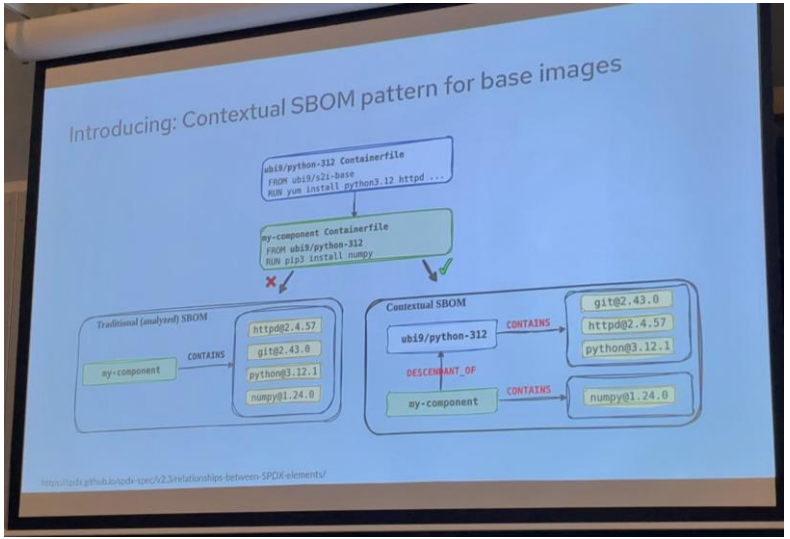
The session emphasized **a pragmatic "30-minute start" over legal idealism or perfection**. While it offers **a great first step for immediate CRA alignment, the lack of supply chain considerations is a concern from my view**. The approach focuses on individual artifacts, potentially overlooking the deeper dependency risks and upstream verification required for true supply chain security.



THE LINUX FOUNDATION
OPENCHAIN

https://fosdem.org/2026/schedule/event/8R99HP-contextual-sbom/

Contextual SBOMs and impact on vulnerability management



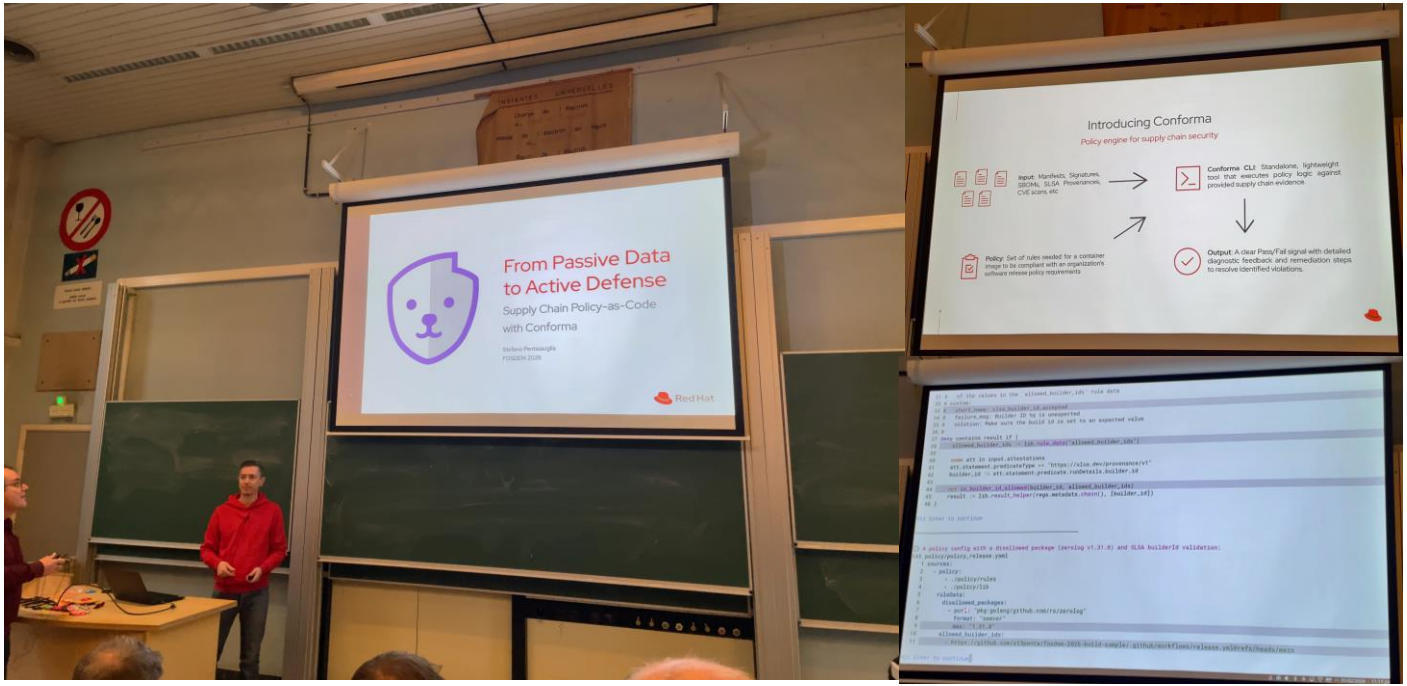
The session had suggested applying the use of SPDX relationships such as DESCENDANT_OF to clarify the origin of the package (base/builder image) and define clear boundaries of responsibility.

THE LINUX FOUNDATION

OPENCHAIN

https://fosdem.org/2026/schedule/event/UGRZNA-conforma-supply-chain-policy-as-code/

From Passive Data to Active Defense: Supply Chain Policy-as-Code with Conforma

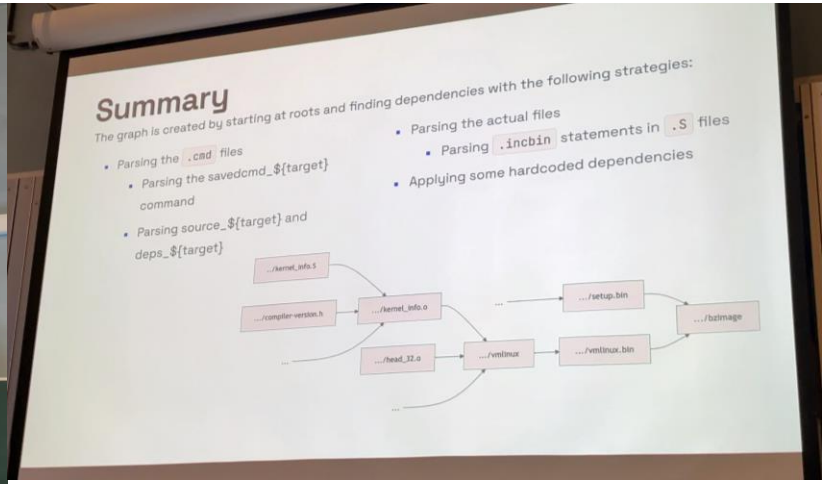


The session that interested me focused on "Conforma" a policy engine that automatically validates SBOMs and attestations generated in the software supply chain, providing Pass/Fail judgments in pipelines along with human-readable violation details. The presentation included both the mechanism and a demonstration.
When I shared this with the Japanese community, we learned about a similar tool called OPA, which is being utilized at AGL Assessment Automation.

THE LINUX FOUNDATION
OPENCHAIN

https://fosdem.org/2026/schedule/event/938CKB-how_to_create_the_sbom_for_the_linux_kernel/

How to create the SBOM for the Linux kernel

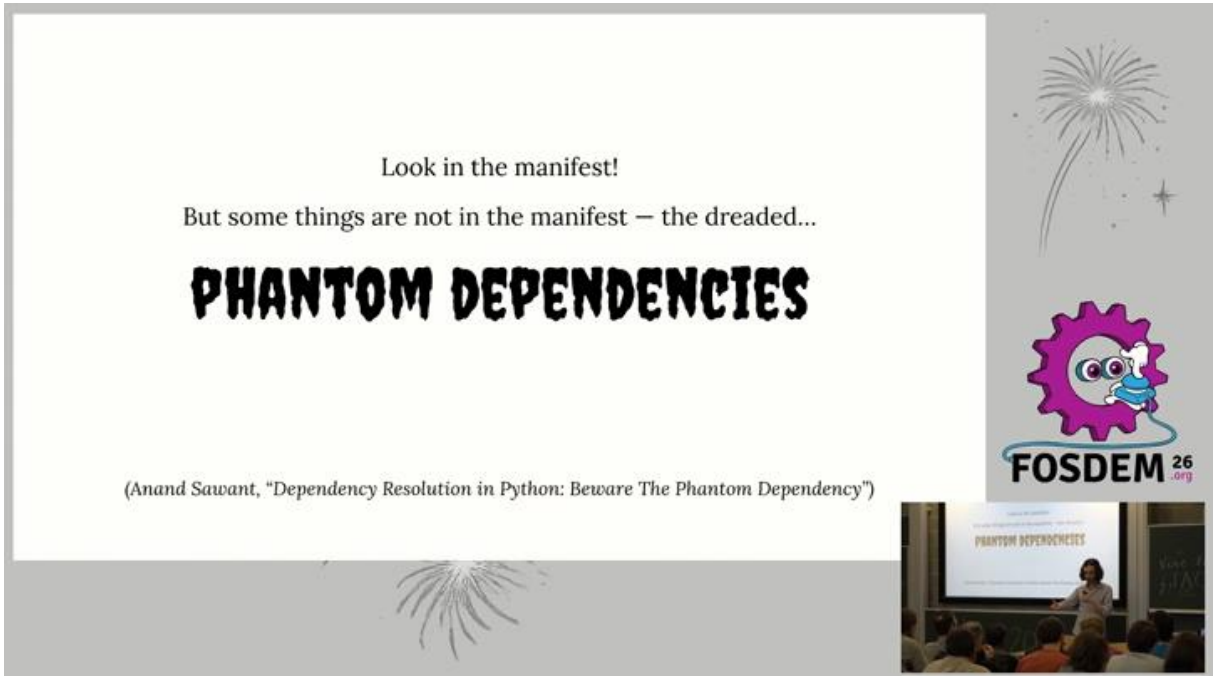


This session **introduced kernel SBOM**, generated using SPDX v3.0.1. To our knowledge, **Yocto and kernel are currently among the most accurate tools for representing SPDX v3.0.1**. However, we observed **some challenges regarding tool interoperability**.
For instance, build options are documented in the Comment field, which could lead to information loss during format conversions between different tools. This is an area that may need further refinement.

THE LINUX FOUNDATION
OPENCHAIN

https://fosdem.org/2026/schedule/event/7NQJNU-binary_dependencies_identifying_the_hidden_packages_we_all_depend_on/

Binary Dependencies: Identifying the Hidden Packages We All Depend On



After returning to Japan, I was introduced to this session and watched the recording.

While the presenter was using Python, they discussed how it's crucial and extremely challenging to trace dependencies **not just at the package manager level, but all the way down to the C/C++ layer**. Their talk focused on how to tackle this problem.

This is recognized as **a major challenge within OpenChain Japan SBOM SG as well**, do others see it the same way?

CISA SBOM

We were surprised to run into Victoria-san and Jono-san from CISA at the AboutCode workshop.

We learned that CISA SBOM is now operational, and they're working hard to respond to public comments in April and release a new version.