FOSDEM 2023
Partial Event Report

Philippe Ombredanne, AboutCode.org nexB Inc.

Philippe Ombredanne

- Project lead and maintainer for VulnerableCode, **ScanCode** and AboutCode
- Creator of **Package URL**, co-founder of SPDX, ClearlyDefined
- FOSS veteran, long time **Google Summer of Code** mentor
- Co-founder and CTO of nexB Inc., makers of DejaCode
- Weird facts and claims to fame
  - Signed off on the **largest deletion of lines of code** in the **Linux kernel** (but these were only comments)
  - Unrepentant **code hoarder**. Had 60,000+ GH forks now down only to 20K forks
- pombredanne@nexb.com irc:pombreda

FOSDEM in Brussels, Belgium

- All volunteers led
- Free as in beer and freedom!
  - Just walk in: no registration required (none possible either)
- 8,000 to 10,000 people on a university campus over a weekend
- Many events "on the fringe" before and after FOSDEM
- My trip report
  - The day before FOSDEM
  - Highlights of the Legal + Policy devroom and SBOM devroom
- Key takeaways

nexB

The day before

- Many "Fringe" events
- My workshop

FOSS license and security compliance tools developers and users workshop

- Morning: FOSS developers presented their plans
- Afternoon: Users exposed their requirements
- 60 registrations, about 55 attendees showed up

Represented tools

- AboutCode/ScanCode
- BANG Binary Analysis
- Eclipse Onioro Compliance tooling/toolchain
- Flict
- Hermine
- Opossum
- ORT
- Osselot and OSADL license obligations list
- REUSE
- SPDX tools for Python
- Trustsource
- YesIscan

Key insights (1): Share the data!

"I would like to have automation to avoid repeat work when re-running tools"
"Let's avoid re-running scans, share them and reuse them instead"

- Everyone wants to share and reuse data from scans, and origin and license
  - Avoid redoing the scans
  - Avoid redoing the same review either inside my org or across orgs
- But "It is hard to overcome lawyers objections to share data such as license conclusions and curations"
- And how to trust the scans and curations? And deal with different policies and standards for conclusions and curations? (specifically about licensing)
- What is the motivation and ease for public data sharing?
- We should share raw scanners/tools outputs first
- We should fix upstream licensing issues, upstream

Key insights (2) Licensing != Security?

License and Vulnerability are like oil and vinegar

- Even if core process is code origin determination, constituents are not the same (yet)
  - License folks care less about Vulnerabilities
  - Security folks care less about licensing
- FOSS projects that cater to both should provide differentiated documentation for each audience
- Core tools are the same: users are different
- Expect a convergence of the two aspects more and more

nexB

Key insights (3) License Compatibility

Multiple projects try to solve license compatibility

- FLICT, OSADL, Hermine Oniro
- Automating license conflicts/compatibility checks is a real problem at scale
- Projects may work together and eventually some conventions will emerge on
- Key domains
  - Help legal understand/zoom in on key license concerns
  - What is the effect of multiple licenses?
  - How to surface license compatibility issues

Follow up collaboration opportunities?

- Collaborate: License conflicts/compatibility checking projects on data and standards
- Create: A live inventory of all the FOSS tools and their capabilities
- Share: Approaches to dependency detection/resolution/processing
- Define: Evolve a standard/schema for tools-to-tools technical scan data sharing
- DATA: Exchange data!

FOSDEM Proper

- Too many devrooms to count!

- BSD
- Binary Tools
- Collaboration and Content Management
- Community
- Confidential Computing
- Containers
- Continuous Integration and Continuous Deployment
- DNS
- Declarative and Minimalistic Computing
- Distributions
- Embedded, Mobile and Automotive
- Emulator Development
- Energy
- Erlang, Elixir and Friends
- FOSS Educational Programming Languages
- FOSS on Mobile Devices
- Fast and Streaming Data
- Friends of OpenJDK
- Go
- Graph Systems and Algorithms
- HPC, Big Data and Data Science
- Haskell
- Image-based Linux and Secure Measured Boot
- JavaScript
- Kernel
- Kotlin
- LLVM
- Legal and Policy Issues
- LibreOffice Technology Development Platform
- MariaDB, MySQL and Friends
- Matrix
- Microkernel and Component-based OS
- Monitoring and Observability
- Mozilla
- Network
- Nix and NixOS
- Open Media
- Open Research Tools and Technology
- Open Source Design
- Open Source Firmware, BMC and Bootloader
- PostgreSQL
- Public Code and Digital Public Goods
- Python
- RISC-V
- Railways and Open Transport
- Real Time Communications
- Rust
- Security
- Software Bill of Materials
- Software Defined Storage
- Sovereign Cloud
- Test
- Testing and Automation
- Translations

nexB

The FOSDEM fun

- In person! And deliciously crowded and packed
- Running around from room to room
- Along the way, meet some great people, stop and chat
  - And never reach the place you had planned to go
- Beer and fries!
- Fringe events, before and after and parties.

Key devrooms: legal+policy

- On the legal + policy dev room: https://fosdem.org/2023/schedule/track/legal_and_policy_issues/

- IANAL and "unlicensed practice of law" https://fosdem.org/2023/schedule/event/foss_law/

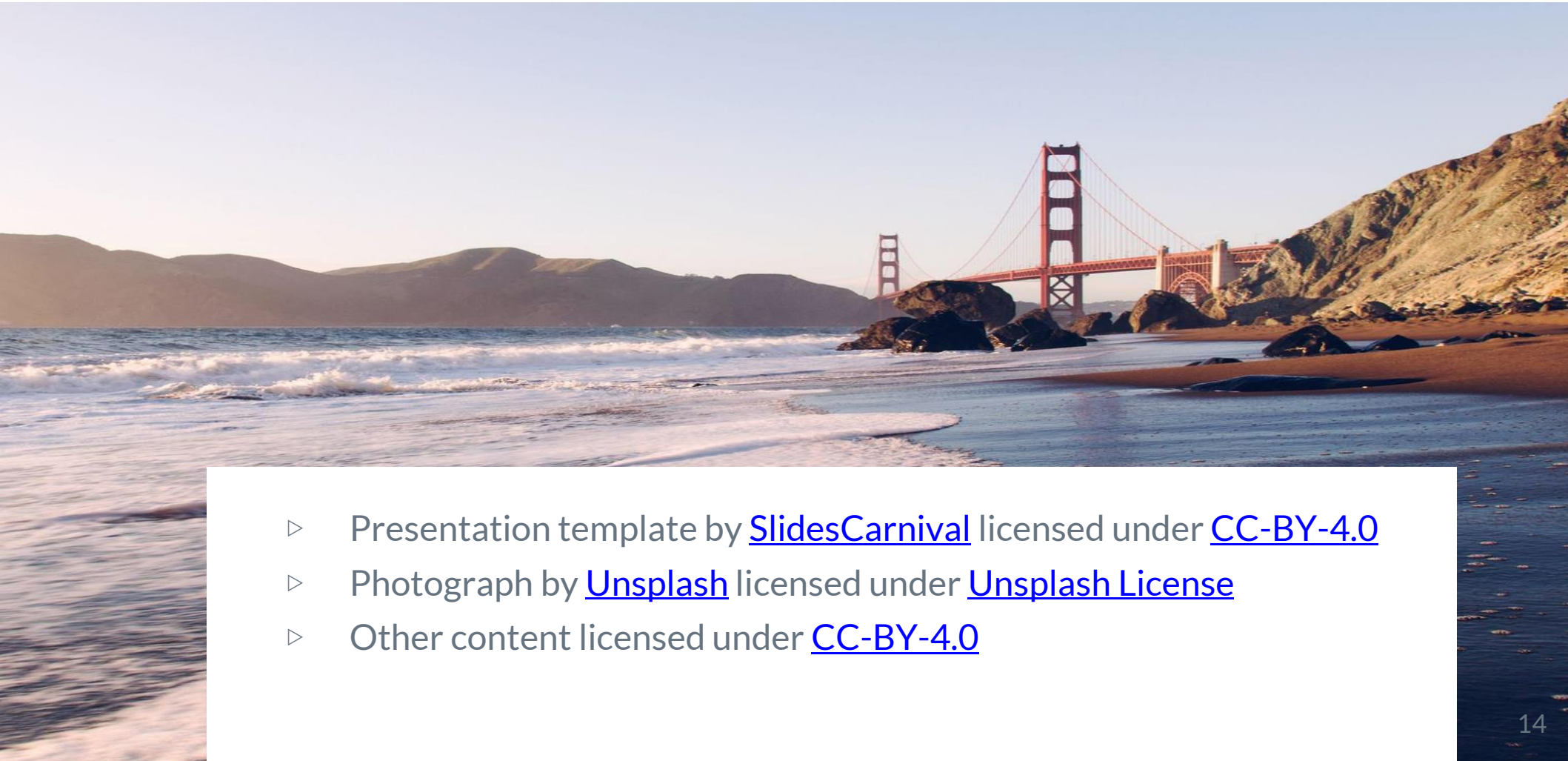
- Dangers to FOSS of upcoming European legislation "CRA"

Key devrooms: SBOM

- https://fosdem.org/2023/schedule/track/software_bill_of_materials/
- Lots of SPDX, but not exclusively
- Many presentation on how tools can produce SBOMs
- Embedded build tools are integrating SBOMs (Yocto and Buildroot)
- Standardized SBOM formats are necessary but not sufficient
  - Accuracy, trust and being actionable are under heavy discussion
- Few tools and fewer team can/do consume SBOMs???
  - There may be supply/demand imbalance issue
- Large orgs are evolving their own processes and conventions
  - (e.g., Siemens BOM on CycloneDX)
- VEX may emerge as more important than SBOMs
- Package URL/PURL is mostly everywhere

nexB

Credits



- Presentation template by SlidesCarnival licensed under CC-BY-4.0
- Photograph by Unsplash licensed under Unsplash License
- Other content licensed under CC-BY-4.0