ARRAY

HUAWEI

OPEN SOURCE COMPLIANCE INTEGRATED IN DEVELOPMENT

Alberto Pianon, Carlo Piana – **Array**

Linaro connect - 8 September 2021

IN GENERAL

WHY

Compliance is required for many reasons:

- Legal
- Social (R-E-S-P-E-C-T!)
- Ecosystem

HOW (IN A NUTSHELL)

Different levels:

- Making sure you are compliant
    - What’s inside your code base (what are you reusing)
    - What is the licensing of inbound-outbound
    - Through a *process*
- Making your downstream *aware* you are compliant, facilitate adoption:
    - SPDX
    - Software Bill of Materials
    - REUSE https://www.reuse.software
    - OpenChain (ISO 5230) https://www.openchainproject.org/

WHEN

Two main appraches:

- *Post-mortem*
- Continuous (CI/CD/CC) ✓

ENTER ALLSCENARIOS (CODENAME)

WHAT (CHALLENGES)

- An entire multikernel OS (mainly portable, IoT devices etc.)
- Based on Yocto / Bitbake
- For different target platforms
- Thousand packages, all in one

OUR APPROACH

- OS in full open since day #1
- Compliance, OpenChain fundamental building blocks
- The first step of a long journey
- An example for others

WHO

- Started as an internal project at Huawei
- Nearly entirely rebuilt from scratch (HarmonyOS → OpenHarmony → AllScenariOS (working title)
- Soon to be donated to Eclipse Foundation (not official)
- Working Group already established
- Development team fully briefed and on board with the process
- Noi Techpark Bolzano
- Array

HOW

- Scancode → Fossology
- Integrated in a CI/CD (Via a Gitlab CI Pipeline)
- Audit Team
- Aliens4Friends
- SPDX
- REUSE
- **Not** Clearly Defined
- Dashboard

FOSSOLOGY

- what it does and what it help us to do
- what it *doesn't* do:
    - **code snippets?** yes, but it's no anti-plagiarism tool
- it's *not* a comprehensive tool:
    - needs input (source packages) from some other tool
    - some other tool has to collect output, generate SBOM and elaborate stats

FOSSOLOGY: THE PROBLEM

- Fossology requires a lot of human work (auditors)
  - hundreds of packages, hundreds of thousands of files
  - hundreds of man-days (auditing)
- Do it the Open Source way, avoiding reinventing the wheel and reusing others’ (trusted) work

THE SOLUTION: DEBIAN MATCHING

- Debian is like a **trusted “friend”** that vouches for the **“alien” packages**
- reuse copyright/license information which has already been collected and maintained by **humans@Debian**, and are machine readable (DEP5)
- DEP5 specs: every file must have a copyright and a license in the `debian/copyright` file of the Debian package
- `debian/copyright` is machine readable, we can reuse all metadata!

THE SOLUTION: DEBIAN MATCHING

- it does not solve everything:
  - not always a full match in Debian
  - not all packages may be found in Debian
  - not all debian/copyright files are machine readable :(
- but it really helps and **saves a substantial amount of human work**

BACK TO THE COMMUNITY

- Aliens4Friends (open source)
- All compliance documents, procedures, artifacts
- Dashboard
- All under Apache license, where permitted
- Including SBOM
- Database of decisions
- Upstream to ClearlyDefined (very likely)
- Upstream REUSE fix / MR

thank
you