OSS Review Toolkit

Using FOSS tools for FOSS reviews in a CI/CD world

Thomas Steenbergen
Head of Open Source - HERE Technologies

Open Source Summit North America 2019
About me

Head of Open Source at HERE Technologies
global location cloud company

© 2019 HERE

[Image of Thomas Steenbergen]

Active contributor

- thomas.steenbergen@here.com
- @tsteenbe
- linkedin.com/in/tsteenbe

[200+ countries mapped]

HERE Maps on board of

[100M vehicles and counting]

9,000+ employees in 56 countries

OSS Review Toolkit
http://oss-review-toolkit.org

SPDX
OSS Tooling Group
European Chapter

OpenChain
FOSS reviews is Firefighting in most Organizations

Challenges

Awareness and understanding

Tens of build/dependency tools in use

Lack of technical consistency

Large volume of scan results

Missing package metadata

Declared ≠ detected licenses

Security vulnerabilities
Build or Share?
Assessing Market Solutions

Tested more than 20+ commercial and FOSS solutions on the market which include review workflows, tooling, etc. ...

You can just buy solutions, build few missing pieces and be done, right?

Modern SW dev practices are not fully supported by current FOSS review tooling available on the market.
Started building a new tool 3 years ago…

OSS Review Toolkit

but challenges are too big for single company…

We work together on open source standards and tools ecosystem
How to automate?

- **Counsel:** Found OSS with Apache-2.0, BSD-3-Clause, CC-BY-SA-3.0 and GPL-2.0 licenses. Apache-2.0 and GPL-2.0 are incompatible with each other. Please explain...

- **Engineer:** Our code includes BSD-3-Clause and we depend on Apache-2.0 test library. GPL-2.0 is build tools and CC-BY-SA-3.0 is docs from StackOverflow

- **Counsel:** So what is distributed to our customers?
- **Engineer:** An executable with only our code and BSD-3-Clause
- **Counsel:** OK, but you must include open source notices to comply with BSD-3-Clause license

**OK / NOT OK = code context + legal context + product context**

- Source code, docs, example, test or build tools?
- What are the licenses and resulting obligations?
- What is released to customers? Artifact, service or website?
- How is it included? Which scope? Linking? Did we change the code?
- Patents? Freedom to operate?
- What does the contract say?
OSS Review Toolkit: scaling OSS reviews in CI/CD (Q3 2019)

Goal: enable review during source creation by providing easy, open-source & scalable tooling for developers to do basic compliance and share results in open standard formats.
Thank you

Contact
Thomas Steenbergen
HERE Open Source Office

thomas.steenbergen@here.com
@tsteenbe
linkedin.com/in/tsteenbe

OSS Review Toolkit
https://github.com/heremaps/oss-review-toolkit

Welcome your feedback and contributions