OSS Review Toolkit

Automating FOSS reviews within CI/CD

Thomas Steenbergen & Sebastian Schuberth
Open Source Office - HERE Technologies

Bitkom Open Source Forum 2018

OSS reviews

Es geht nicht mehr per Hand!

https://pixabay.com/en/firefighter-training-590663/ (CC-0)

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

code context:

Source code, docs, example, test or build tools?

How is it included? Which scope? Linking?

Did we change the code?

legal context:

What are the licenses and resulting obligations?

Patents? Freedom to operate?

Created by us or FOSS community?

product context:

What is released to customers? Artifact, service or website?

What does the contract say?

How to automate? (2)

Usual approach

1. resolve dependencies using plugins
2. find licenses of dependencies via metadata or database
3. evaluate OK/NOT OK against approved licenses rules
4. report findings on a website
5. creation of notices

OSS
Review Toolkit

1. resolve dependencies
2. fetch all source code
3. scan for licenses & copyrights
4. cache scan results
5. evaluate OK/NOT OK using ruleset (code + licenses + product)
6. report findings within CI
7. option to exclude non-distributed OSS
8. creation of notices

Review Tooling Technical Challenges

- Missing metadata
  Source location may not be defined or found
- No sources available
  Simply missing in central repositories
- Ways of working issues
  Devs do not always follow best engineering practices resulting host issues when trying to automate
- Build/dependency tools issues
  Not designed to support FOSS reviews e.g. lacking methods or return inaccurate data
- Different build/dependency tools
  ~30 common build/dependency tools
- Large volume of scan results
  No tooling is available to automate reviewing large amounts of scan results, conclude obligations and determine any issues to be resolved within limited timeframe

MISSING DATA

MISSING TOOLING

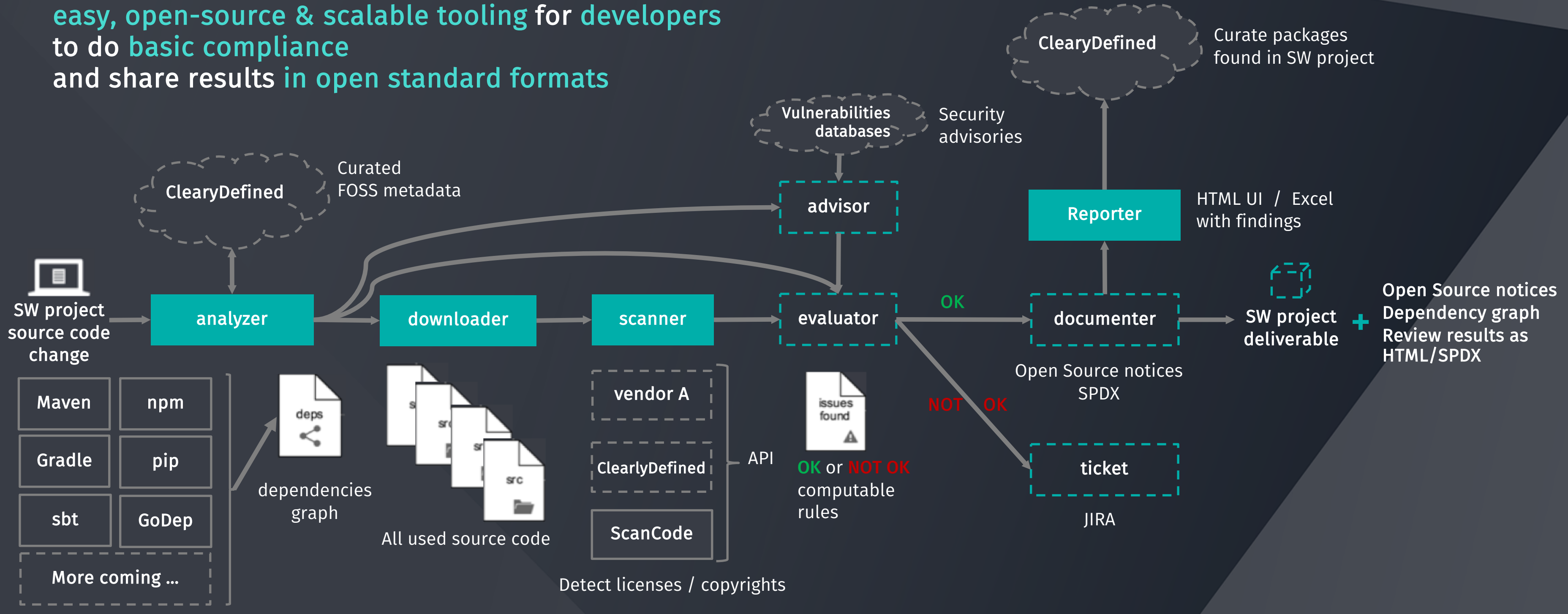
LEGEND

built

planned

OSS Review Toolkit: Scaling OSS reviews for CI/CD

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



SW project source code change

analyzer

Maven

npm

Gradle

pip

sbt

GoDep

More coming ...

ClearlyDefined

Curated FOSS metadata

dependencies graph

downloader

All used source code

scanner

vendor A

ClearlyDefined

ScanCode

API

Detect licenses / copyrights

Vulnerabilities databases

Security advisories

advisor

evaluator

OK or NOT OK computable rules

OK

NOT OK

documenter

Open Source notices SPDX

ticket

JIRA

Reporter

HTML UI / Excel with findings

ClearlyDefined

Curate packages found in SW project

SW project deliverable

+

Open Source notices
Dependency graph
Review results as HTML/SPDX

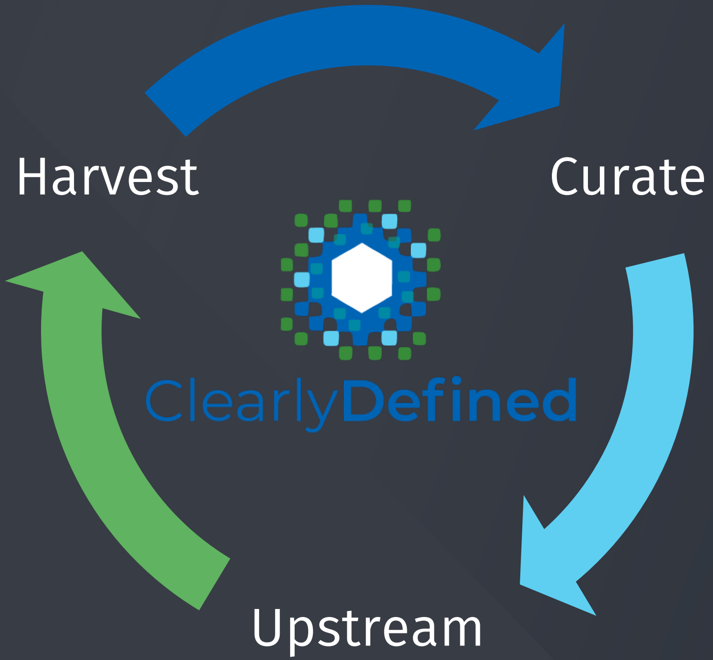
No plugins installation required within to be reviewed projects

Open-sourced & released at **github.com/heremaps/oss-review-toolkit**

Written in Kotlin + React, Apache-2.0 licensed.

OSS **Review Toolkit**

Demo



Harvest

Curate

ClearlyDefined

Upstream

Enabling FOSS project success through clearly defined license and security information

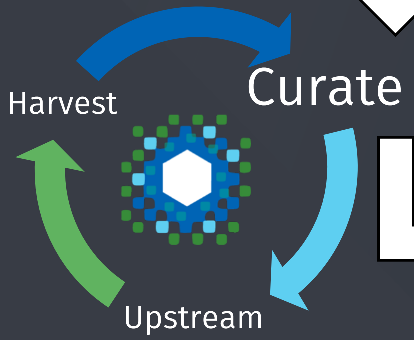
- Community solution to a community problem
- Automated scanning of released components
- Crowd-sourcing curation of ambiguous or missing information
- Contribute updates to upstream projects
- Immediate focus on license, source location, and attribution parties
- Longer-term interest in security, accessibility, localization

- Open Source Initiative incubator project
- Partners: Amazon, Eclipse, nexB, Microsoft Qualcomm, Software Heritage, SAP

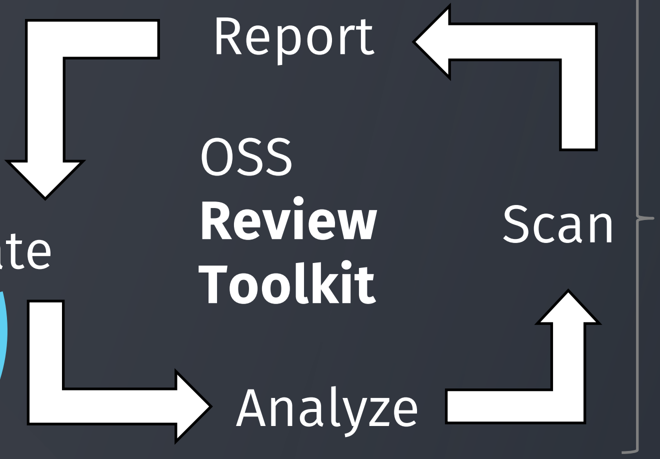
clearlydefined.io

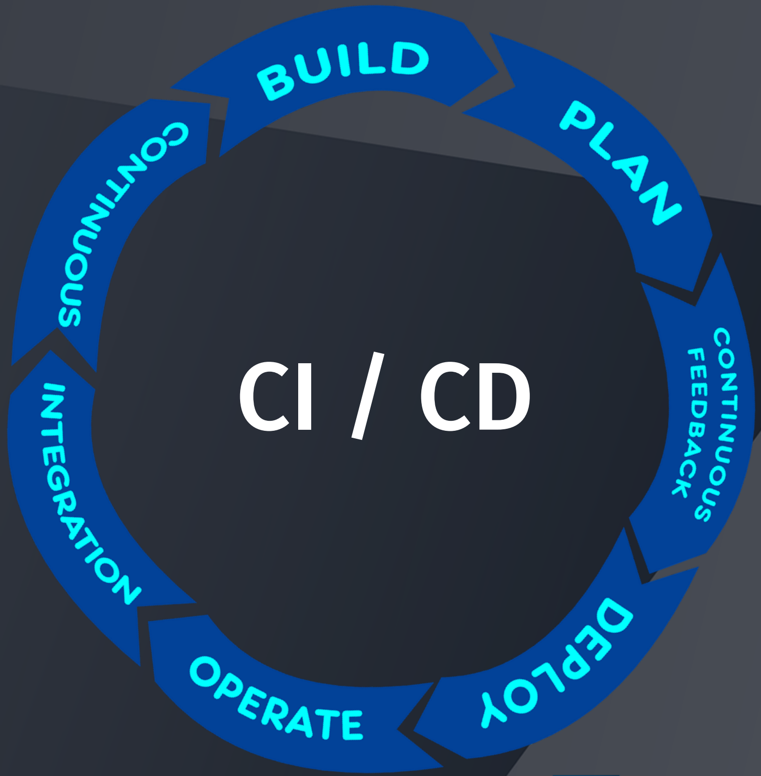
github.com/clearlydefined

How it all comes together...



Clearlydefined updating upstream OSS projects





SPDX

Exchange software bill of material

CI/CD image - https://pixabay.com/en/isolated-devops-business-3168537/ (CC-O)

OSS **Review Toolkit**

+

ClearlyDefined

Demo: fixing OSS package metadata

Note: feature no yet in master branch

Get your project ORT scanned

Want to see the ORT scan results for your project?

We will scan your project for FREE; it's as simple as 1-2-3!

1. Select up to 4 public code repositories
2. Email the list to thomas.steenbergen@here.com
3. We will reply ASAP with the scan results!

Thank you

Contact

Thomas Steenbergen
HERE Open Source Office

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

OSS Review Toolkit

https://github.com/heremaps/oss-review-toolkit

Welcome your feedback and contributions