OSS Review Toolkit

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

Thomas Steenbergen

Open Source Summit EU 2019

About me

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

Head of Open Source at HERE Technologies
global location company

200+ countries mapped

HERE Maps on board of **100M** vehicles and counting

9,000+ employees in 56 countries

Active contributor

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

SPDX

OSS Tooling Group

TODO
European Chapter

OPENCHAIN

Work In Progress

OSS Review Toolkit
is pre-release software

First release planned for end of 2019

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 tooling 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, ensure your release includes open source notices to comply with BSD-3-Clause license

OK / NOT OK = code context + license context + product context

code context	license 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?	Patents? Freedom to operate?	What does the contract say?
Did we change the code?	Created by us or FOSS community?	

FOSS reviews is Firefighting in most Organizations

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

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

Why Open Source Solution?

- Solve community problem with a community solution
- CI/CD world requires compliance to move faster
- Developer-focused solution without lower compliance
- Scale cost efficiently
- Customizable to business needs
- Need for long term solution (based on open standards)
- No vendor lock-in

OK / NOT OK = code context + license context + product context

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

How is it included? Which scope? Linking?

Did we change the code?

Excludes
(.ort.yml)

+

Curations
fix local findings
(.ort.yml)

What are the licenses and resulting obligations?

Patents? Freedom to operate?

Created by us or FOSS community?

Policy Rules

+

Curations
fix metadata/findings

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

What does the contract say?

Policy Rules

+

Resolutions
manual override

OSS Review Toolkit

Demo

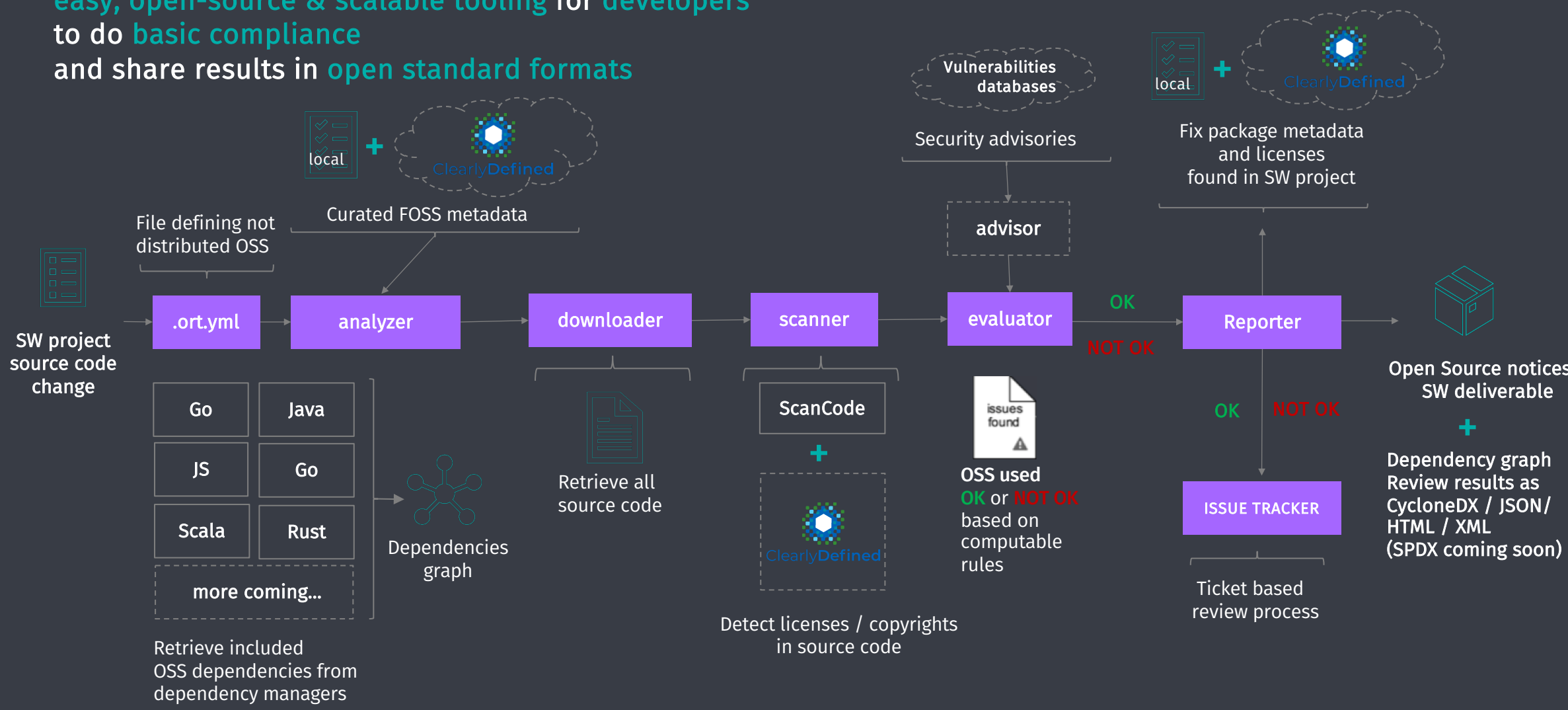
OSS Review Toolkit: scaling OSS reviews in CI/CD (Q3 2019)

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

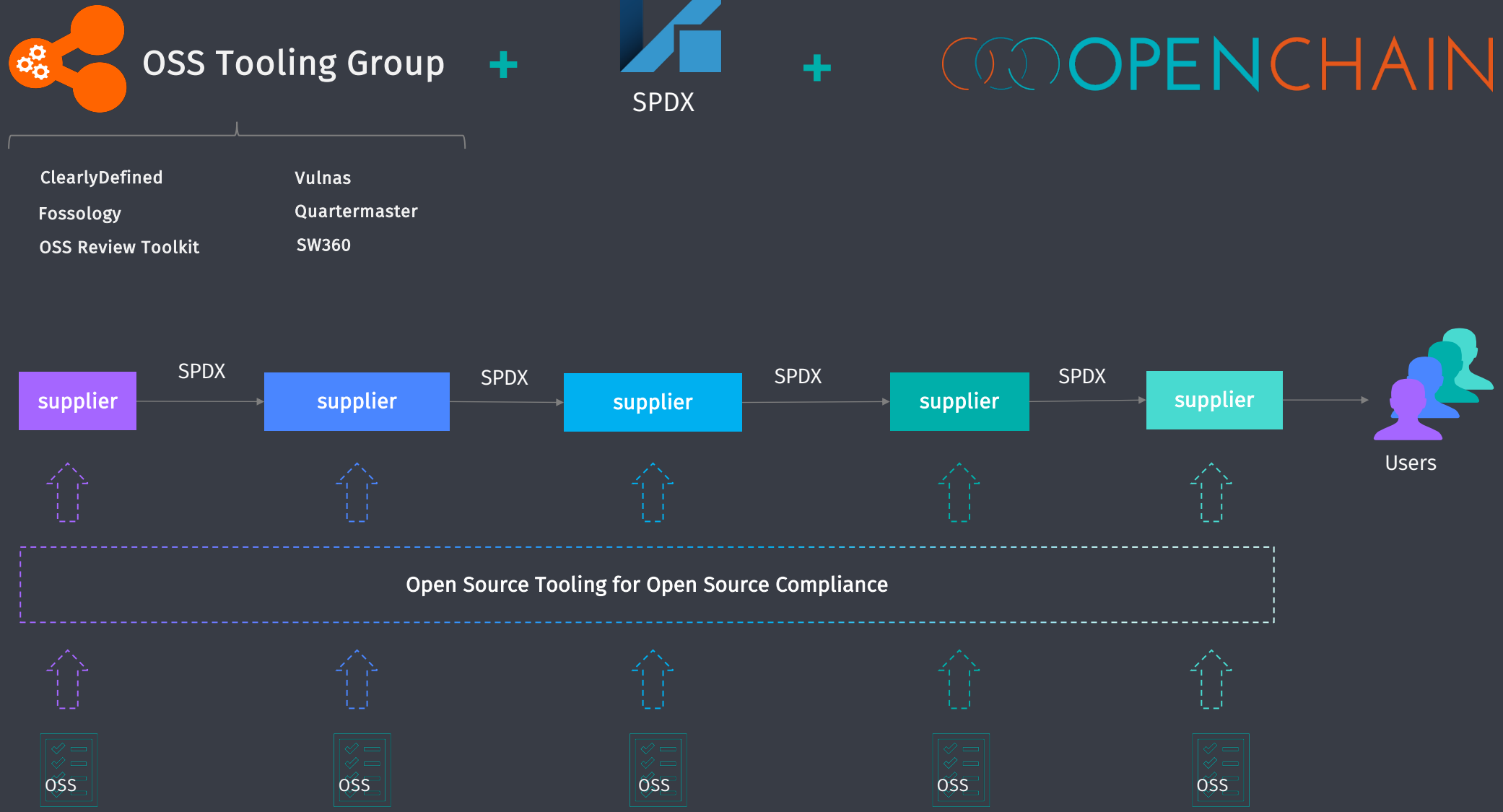
LEGEND

built

planned



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


OSS Tooling Group
+
SPDX
+
OPENCHAIN
ClearlyDefined
Fossology
OSS Review Toolkit
Vulnas
Quartermaster
SW360
supplier
SPDX
supplier
SPDX
supplier
SPDX
supplier
SPDX
supplier
Users
Open Source Tooling for Open Source Compliance
OSS
OSS
OSS
OSS
OSS

Thank you

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

Related OSS Projects

https://oss-compliance-tooling.org
https://clearlydefined.io
https://spdx.org
https://www.openchainproject.org
https://www.doubleopen.org