FOSDEM'21
Software Composition Dev Room

OSS
Review Toolkit

Project Update

About me

🐦 @tsteenbe
🔗 linkedin.com/in/tsteenbe

Head of Open Source

- HERE Open Source Office (OSO) is a team of 7 people
- Supporting 9k+ employees in 56 countries on all things Open Source together with our legal counsels
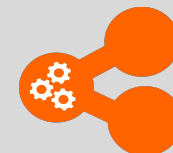
Active contributor to:

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

SPDX

Open Source Tooling Group

OPENCHAIN

ClearlyDefined

TODO
European Chapter
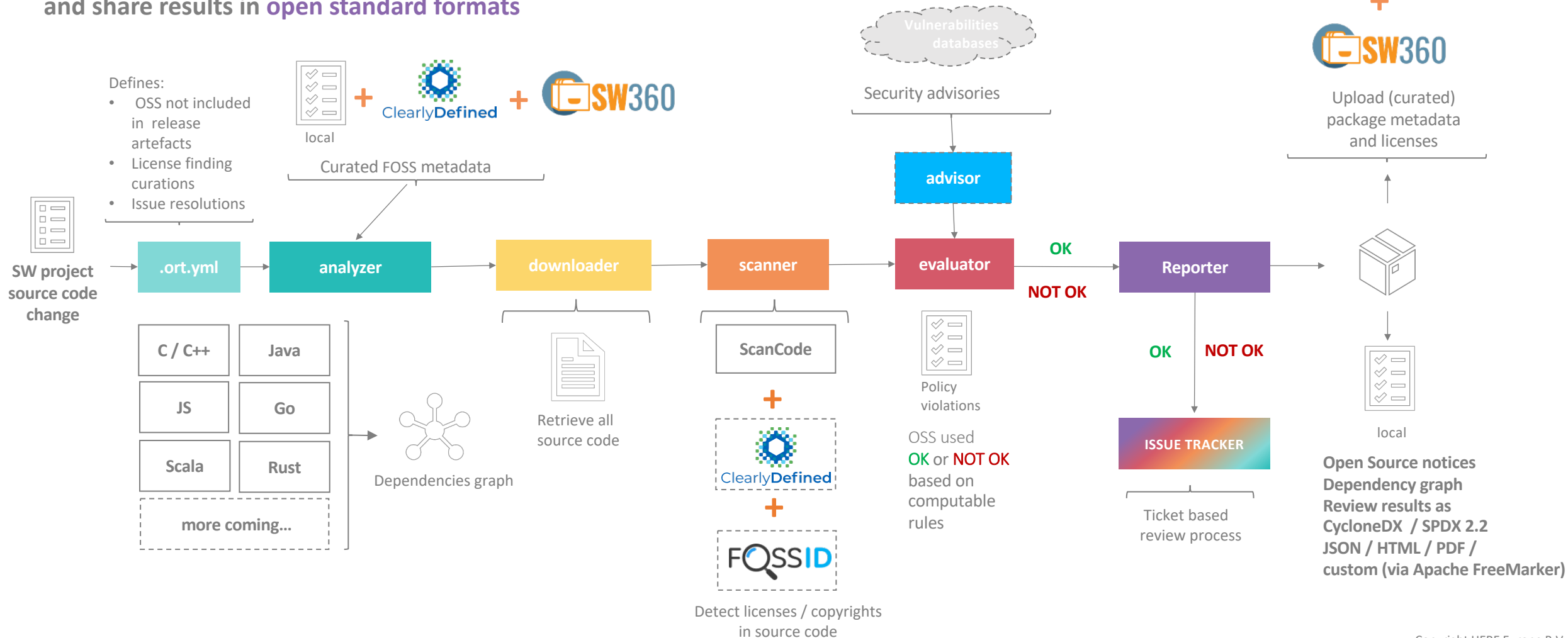
OSS Review Toolkit

Highlights of 2020:

- New Advisor component - add security data to your scans
- Reporter improvements:
    - Customizable AsciiDoc files and PDFs
    - Customizable notices via Apache Framemaker
    - GitLabLicense model to display license findings in GitLab's UI
    - Context-aware 'how to fix' for violations and errors
- Support for SPDX manifest to manually define SW packages
- Ability to use the 'WITH' operator to classify licenses
- Ability to override the declared license for a specific package
- New configuration options and improvements such as proxy support, SW360 storage
- Performance improvements to reduce scan times
- Partnership with FossID - use ORT in FossID or vice versa

Questions? Interested in collaborating? Chat with us using the ort-talk Slack channel, see **github.com/oss-review-toolkit/ort**

OSS Review Toolkit (Q1 2021)

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**

Defines:
- OSS not included in release artefacts
- License finding curations
- Issue resolutions

local

Curated FOSS metadata

+ **ClearlyDefined** + **SW360**

Security advisories

Vulnerabilities databases

advisor

ClearlyDefined
+
SW360

Upload (curated) package metadata and licenses

SW project source code change

.ort.yml → **analyzer** → **downloader** → **scanner** → **evaluator** → **OK** / **NOT OK** → **Reporter**

C / C++	Java
JS	Go
Scala	Rust

more coming...

Dependencies graph

Retrieve all source code

ScanCode

+

ClearlyDefined

+

FOSSID

Detect licenses / copyrights in source code

Policy violations

OSS used **OK** or **NOT OK** based on computable rules

OK **NOT OK**

ISSUE TRACKER

Ticket based review process

local

Open Source notices Dependency graph Review results as CycloneDX / SPDX 2.2 JSON / HTML / PDF / custom (via Apache FreeMarker)

Join the ORT community at **github.com/oss-review-toolkit/ort**

Hands-on Demo

- 'How To Fix' texts for violations and errors

- Handling large scan results using ort helper cli

- How to add package metadata to code using SPDX manifests

OSS Review Toolkit

Features planned for 2021:

- Support for making license choices
- Support for additional security vulnerability providers such as VulnerableCode
- SPDX 3.0 SBOM generation
- Further improvements to:
  - Performance
  - GitLab integration
  - Documentation

Questions? Interested in collaborating? Chat with us using the ort-talk Slack channel, see **github.com/oss-review-toolkit/ort**

Thank you
Merci
Dank je wel

Thomas Steenbergen

🐦 @tsteenbe

in linkedin.com/in/tsteenbe

OSS Review Toolkit

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

Starting and Scaling an Open Source Office

ORT Slack

Related OSS Projects

https://oss-compliance-tooling.org

https://clearlydefined.io

https://spdx.org

https://www.openchainproject.org

https://www.doubleopen.org

https://www.eclipse.org/sw360