OSS Review Toolkit

Project Update
About me

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

@tsteenbe
linkedin.com/in/tsteenbe
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
**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**

- **SW project source code change**
- **.ort.yml**
- **analyser**
- **downloader**
- **scanner**
- **evaluator**
- **advisor**
- **Reporter**

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

- **SW360**
- Upload (curated) package metadata and licenses
- **ClearlyDefined**
- Curated FOSS metadata
- **ScanCode**
- Retrieve all source code
- Dependencies graph
- **FOSSID**
- Detect licenses / copyrights in source code
- **Security advisories**
- Vulnerabilities database
- **Policy violations**
- OSS used **OK** or **NOT OK** based on computable rules
- **Ticket based review process**
- Issue resolutions

- **Curated FOSS metadata**
- **Vulnerabilities databases**

**Legend:**
- Local
- Under development

**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.

Join the ORT community at [github.com/oss-review-toolkit/ort](https://github.com/oss-review-toolkit/ort)

Copyright HERE Europe B.V. CC-BY-4.0
‘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

Copyright HERE Europe B.V. CC-BY-4.0
Thank you
Merci
Dank je wel

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