About me

Head of Open Source at HERE Technologies
HERE TechnologiesのOpen Source責任者

A location data and technology platform company
位置データとテクノロジープラットフォームの企業

Active contributor 以下のプロジェクトへの貢献活動中

- OSS Review Toolkit
  - http://oss-review-toolkit.org
- SPDX
- Open Source Tooling Group
- OPENCHAIN
- TODO
- ClearlyDefined

thomas.steenbergen@here.com
@tsteenbe
linkedin.com/in/tsteenbe
Work In Progress

OSS Review Toolkit is pre-release software

First release planned for Q1 of 2020
The OpenChain Project helps to identify and share the core components of a Free and Open Source Software (Open Source) compliance program.

A key element to an Open Source Compliance Program is an Open Source Review process.

https://www.openchainproject.org
Why: Open Source Compliance Program
オープンソースのコンプライアンスプログラムを推進する理由

• **Know your obligations.** You should have a process for identifying and tracking Open Source components that are present in your software

• **Satisfy license obligations.** Your process should be capable of handling Open Source license obligations that arise from your organization’s business practices

Benefits of a robust Open Source Compliance program include:

• Increased understanding of the benefits of Open Source and how it impacts your organization

• Increased understanding of the costs and risks associated with using Open Source

• Increased knowledge of available Open Source solutions

• Reduction and management of infringement risk, increased respect of Open Source developers/owners’ licensing choices

• Fostering relationships with the Open Source community and Open Source organizations

Source: OpenChain training slides: https://github.com/OpenChain-Project/curriculum
What information do you need to gather?
どのような情報を収集する必要があるか？

When analyzing Open Source usage, collect information about the identity of the Open Source component, its origin, and how the Open Source component will be used. This may include:

使用するオープンソースを解析する場合、オープンソースが何であるか、どこから入手したか、および、どのようにコンポーネントが利用されるかの情報を収集する必要がある。詳細としては以下の情報：

- Package name
- Status of the community around the package (activity, diverse membership, responsiveness)
- Version
- Download or source code URL
- Copyright owner
- License and License URL
- Attribution and other notices and URLs
- Description of modifications intended to be made

- List of dependencies
- Intended use in your product
- First product release that will include the package
- Location where the source code will be maintained
- Possible previous approvals in another context
- If from an external vendor:
  - Development team’s point of contact
  - Copyright notices, attribution, source code for vendor modifications if needed to satisfy license obligations

Source: OpenChain training slides: https://github.com/OpenChain-Project/curriculum
How: Source Code Scanning Tools
どのように、ソースコードスキャンツールを使うか。

• There are many different automated source code scanning tools.
• 自動のソースコードスキャンツールは複数存在
• All of the solutions address specific needs and - for that reason - none will solve all possible challenges
• それぞれのツールによるソリューションは皆、特定のニーズを満たすものであり、したがって、可能性のある要求事項をすべて満たすツールは無い
• Companies pick the solution most suited to their specific market area and product
• それぞれの企業は、自らの市場と製品に最も適したソリューションを選択する
• Many companies use both an automated tool and manual review
• 多くの企業は、自動化されたツールと人手でのレビューを共有している

Source: OpenChain training slides: https://github.com/OpenChain-Project/curriculum
We work together on open source standards and tools ecosystem

No solution satisfied our needs so in 2017 we created a new tool...

そのツールがOSS Review Toolkit

but challenges are too big for single company so...

OSS Review Toolkitが目指すところは、HERE Technologies 1社で開発するにはあまりに壮大、なので

われわれは、OSSコンプライアンスの標準と、複数のツールそれぞれのエコシステムと協働することにした
Main types of tools in the area of license compliance include (but are not limited to):

- **License scanning**: Identifies licenses and license relevant statements, can also copyright statements, author statements, acknowledgements
- **Binary scanning**: Identifies used software packages in software binaries, can also determine the versions of software packages
- **Source code scanning**: Can identify published origin of source code and other files
- **Dev Ops integration**: Uses the information from building the software to determine OSS used
- **Component management**: Collect information about used software components and their use in products or projects is centrally collected and can be reused

Source: OpenChain training slides: https://github.com/OpenChain-Project/curriculum
OSS Review Toolkit

Features:

- **License scanning** ライセンスの検出(scan)
  Identifies copyrights and licenses by wrapping existing license / copyright scanners like ScanCode to detect findings in local source code directories.

- **Best practices / company standards scanning** 標準的な手法/社内標準に従っているかの検出
  Align software projects across the organization.

- **Policy violations rule engine** 設定したポリシーへの違反検出
  Perform highly customizable policy checks against scan results.

- **Software Bill of Materials / Notices** ソフト部品表(SBOM) および共有形式（SPDX）の生成
  Generate CycloneDX, SPDX 2.2 files or plain text open source notices.

- **Dev Ops integration** Dev Opsプロセスに統合された形での動作
  Designed from the beginning for a CI/CD world.

- **Security scanning** （計画中）脆弱性スキャン
  Coming soon: integrations with OSS security vulnerabilities data feeds from various vendors.

- **Source code scanning** （計画中）ソースコードの出所特定
  Working on partnerships with vendors to develop integrations to identify published origin of source code and other files.

Collected Information

- Package name
- Version
- Source code repository URL
- Source and binary artifacts
- Copyright owner
- License and License URL
- Attribution and other notices and URLs
- List / tree of dependencies
- Location where the source code will be maintained
**OSS Review Toolkit**: scaling OSS reviews in CI/CD (Q4 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.

<table>
<thead>
<tr>
<th>SW project source code change</th>
<th>analyzer</th>
<th>downloader</th>
<th>scanner</th>
<th>evaluator</th>
<th>OK</th>
<th>NOT OK</th>
<th>Reporter</th>
<th>Open Source notices SW deliverable</th>
</tr>
</thead>
<tbody>
<tr>
<td>.ort.yml</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C / C++</td>
<td>Java</td>
<td>Go</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scala</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dependencies graph</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>more coming...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File defining OSS not included in release artefacts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Curated FOSS metadata</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Dependencies graph**
- Retrieve all source code
- Detect licenses / copyrights in source code
- OSS used OK or NOT OK based on computable rules
- Policy violations

**Security advisories**
- Fix package metadata and licenses found in SW project

**Vulnerabilities databases**
- OK
- NOT OK

**Advisor**
- OK
- NOT OK

**Review results as** CycloneDX / SPDX 2.2
- JSON / HTML / XML

**Ticket based review process**

**Open-sourced & released at** [github.com/heremaps/oss-review-toolkit](https://github.com/heremaps/oss-review-toolkit)
Open Source Tooling for Open Source Compliance

- ClearlyDefined
- Fossology
- OSS Review Toolkit
- Vulnas
- Quartermaster
- SW360

Open Source Tooling Group + SPDX + OPENCHAIN
HERE Technologies has contributed ORT to the Automated Compliance Tooling (ACT)

HERE TechnologiesはOSS Review Toolkitを、Linux Foundation配下のAutomated Compliance Tooling (ACT)プロジェクトに寄贈しました
Thank you

Thomas Steenbergen
HERE Open Source Office

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

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

ありがとうございました