Using SW360 for OSS Compliance Management Process

Kouki Hama  kouki1.hama@toshiba.co.jp
Software Engineering & technology center
Open Source Technology Department
Thursday July 18, 2019 16:50 - 17:30

**Hall B (4)**
Open Source Leadership

Experience Level **Beginner**

https://events.linuxfoundation.jp/events/open-source-summit-japan-2019/program/schedule/
Summary

SW360 is an OSS tool used for centrally managing software component information, license information, vulnerability information, and etc. This tool also allows you to associate project information with many software components.

Toshiba has begun centralizing information management of open source software by SW360. This made it possible to share open source information across departmental barriers. On the other hand, feedback from users obtained various issues.

Kouki will explain how Toshiba has promoted the use of open source by SW360 and will explain how to approach issues. These include issues that originate from Japan domestic requirement and issues that need to be solved beyond the boundaries of a company. Moreover, Kouki will report on what kind of open source compliance management system Toshiba aims for.
Who am I?

Kouki Hama (濱 功樹)

• Toshiba Corporation (2016~now)
• Research and Development OSS Compliance / Management Tool
  • SW360, Fossology, GitLab, spdx tool, …

• Hobby
  • Playing with my cats
  • Mathematics (Research Nonlinear Optimization Algorithm)
  • Pokémon Go

Hi I am Hama
Today’s presentation consists of 5 points

• Difficulty of Open Source Software compliance management
• How to manage OSS with SW360 property?
• OSS SW360 Ecosystem
• Live demonstration
• Q & A
Difficulty of Open Source Software compliance management
Need to confirm a lot of OSS information before Using OSS

- Version
- License
- Vulnerability
- ECCN
- User history
- Author
- etc

I use OSS_A
OSS spreading like mushrooms around the world

- Version
- License
- Vulnerability
- ECCN
- User History
- Author
- etc

OSS_A
And we need to clarify a lot of OSS related information

- Version
- License
- Vulnerability
- ECCN
- User History
- Author
- etc

OSS_A

I check OSS_A, OSS_B, …
In addition we need to prepare a lot of OSS related documents.

Vulnerability
License
ECCN
Version
User History
Author

I make document about OSS_A, OSS_B, ...
Occasionally, Reusing other department/product’s OSS related documentation should look good.
However, reusing other product/project OSS information is challenging

WHY?
Answer 1.
Finding property information from a lot of other products is tedious.
Answer 2.
Different products have their own respective OSS information

Where is OSS_A License Information?

- Vulnerability
- License
- ECCN
- Version
- History
- Author
Answer 3.
Different products have unique OSS version information.
Moreover

Software dependency is a significant factor, however can be complex.
We need put together OSS information

- OSS review requires a certain amount of time
- Avoid checking the same OSS information numerous times
The best approach is Utilizing the OSS compliance tool. 

https://github.com/eclipse/sw360
What is SW360?

https://github.com/eclipse/sw360

A software component catalogue application – designed to work with FOSSology.
SW360 Management and Associate Project Information With OSS related Component

Project register snapshot

Component register snapshot

Name, Version, Project visibility, Project type, Group, Project owner, etc

Project visibility, Project type, Group, Project owner, etc

Linked each other

Name, Vendor, Version, Programming Languages, Operating System, Contributors, Download URL, License, CPE ID, etc

OSS Information
You can also say that SW360 is the “Bill of Material” Management Tool

SW360 integrates all “Bill of Materials” in your company
How to manage OSS with SW360 property?

Make it possible with OSS Management Process
Example Enterprise Process

- Review and approve compliance record of Open Source software components
- Compile notices for publication
- Post publication verifications

- Queued for Process
  - Own Proprietary Software
  - 3rd Party Software
  - Open Source

- Identification
- Audit
- Resolve Issues
- Reviews
- Approvals
- Registration
- Notices
- Verifications
- Distribution
- Verifications

- Outgoing Software
- Notices & Attributions
- Written Offer

- Identify Open Source components for review
- Scan or audit source code – and – Confirm origin and license of source code
- Resolve any audit issues in line with company Open Source policies
- Record approved software/versions in inventory per product and per release
- Verify source code packages for distribution – and – Verify appropriate notices are provided
- Publish source code, notices and provide written offer

Example of Compliance Management End-to-End Process

(Ref) https://www.openchainproject.org/resources
SW360 assists OSS management

- Queued for Process
  - Own Proprietary Software
  - 3rd Party Software
  - Open Source

Identification -> Audit -> Resolve Issue -> Review -> Approval -> Registration -> Notice -> Verification -> Distribution -> Verification

- Outgoing Software
- Notices & Attributions
- Written Offer

- Identify Open Source components for review
- Scan or audit source code – and – Confirm origin and license of source code
- Record approved software/version in inventory per product and per release
- Compile notices for publication

© 2019 Toshiba Corporation
Identification

Identify Open Source components for review

SW360 supports:
- Register to use OSS
- Search Used history of each OSS components
Audit

Scan or audit source code — and — Confirm origin and license of source code

SW360 supports:
- Register OSS Source code (with version)
- License scan (License information from Fossology)
- Register CPE ID (For detecting Vulnerability)
- Register ECC (Export Control) Information

SW360 assists OSS management
Record approved software/version in inventory per product and per release

SW360 supports:
- Check OSS (Name, Version, Person in charge, etc.)
- And Projects (Name, Project Version, etc.)
SW360 supports:
- Create user-friendly copyright and license list
- Register the format of the product attachment to be displayed on the document.
TOSHIBA OSS Management System Goal!

Project Start → Survey internal User history → SW360, GitLab, FOSSology, CVE-Search → OSS Community

OSS Management Process

Export Control & Customs
Vulnerability
License

OSS Community

Develop OSS Source Code → License Documents → Customers

© 2019 Toshiba Corporation
Changing perspectives

Why do OSS related companies such as Toshiba need to utilize the OSS management system?
One company's improper use of the OSS resonates throughout all the supply chain.
OSS SW360 Ecosystem
A lot of members will have access to discussions related to SW360 publicly.

- Open Chain Japan WG: https://wiki.linuxfoundation.org/openchain/openchain-japanese-working-group

Open Chain Japan Work Group

• OpenChainJapan has Tooling Sub Group
• Try to discuss how to improve sw360’s interface for non-English speakers / Japanese users.
  • Apply for Japanese vulnerability information
    • JVN = Japan Vulnerability Notes
  • Translate to Japanese language
    • Not only Japanese but also others
  • etc

Interpret in the Japanese language while sharing information with all OSS related connections in the world.
In conclusion

• OSS management can be daunting

• Centering OSS information by SW360 is viable

• SW360 assists by complying with the OpenChain Process

• More people are showing interest in SW360
Try SW360

I'm going to give a live demonstration on how to use SW360 Create Project information which includes component information
Create Software Component

[Components]-[Add Component]
Register Component  Release Information

Register Version etc…
[Components]-[Edit]-[Add Release]
Register project Information

Create Project Information which include Component information
[Projects]-[Add Project]
## Create License Document

[Projects]-[Linked Releases And Projects]-[Generate License Info]

### Project: Vim_test_project

<table>
<thead>
<tr>
<th>Name</th>
<th>Project state</th>
<th>Relation</th>
<th>Type</th>
<th>Clearing State</th>
<th>Main Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>tarb 4.3-11+deb8u2</td>
<td>Unknown</td>
<td></td>
<td>OSS</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>Vim_test 2.7</td>
<td>Unknown</td>
<td></td>
<td>OSS</td>
<td>New</td>
<td></td>
</tr>
</tbody>
</table>

- Projects only
- Export Spreadsheet
- Generate License Info
- Generate Source Code Bundle
Confirm Vulnerabilities

Check OSS Vulnerabilities
[Components]-[Vulnerabilities]
Q & A

kouki1.hama@toshiba.co.jp
Thank You