NTIA Software Component Transparency
February 13, 2020

Formats & Tooling WG

JC Herz
Kate Stewart

Agenda

- Workgroup Goals
- Overview Document
- Tooling Information being collected per Format
    - Template and Example
- Feedback Request
- Next Steps

Formats and Tooling Workgroup Goal

Wrapping up from phase I, we identified for the need for:

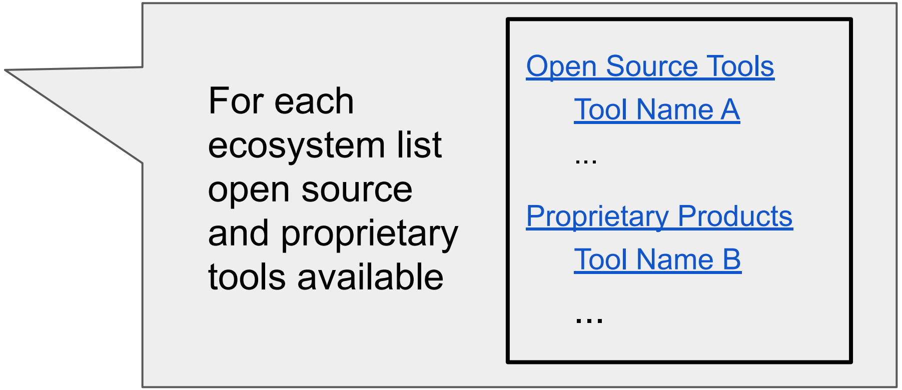
- Tooling
  - Documenting tooling
  - Identifying tooling gaps
  - Documenting processes
  - Turnkey universal translation tools

Formats and Tooling workgroup is focusing on addressing these items.

Overview Document

Overview of Tooling that supports Automation working with Software Bill of Materials Formats.

- Introduction
- Definitions
- Tooling Ecosystem for Key Formats
  - SWID
  - SPDX
  - CycloneDX
- Conclusions



For each ecosystem list open source and proprietary tools available

- Open Source Tools
  - Tool Name A
  - ...
- Proprietary Products
  - Tool Name B
  - ...

An initial breakdown of types of tools

Author - sharing information useful for risk assessment.

- Human/Manual Inspection - creation from manual
- Build/Creation - organization and role creating data
- PostBuild/Audit/SCA - service provider (accuracy, completeness, precision)

Consume - understand and inspect

- View - human readable - picture, figures, tables, text.   Impact on business process
- Diff - comparison of two documents inside of a given format.   Version comparison as an example.
- Analyze SBOM component data

Transform - consume and re-author

- Translate
- Merge/Analysis/Audit - two different sources of information
- Tool support: Libraries, APIs

Information to Collect per Tool

Tool Template

Format Support	Author, Consume, Transform
Functionality	
Location	Website: Source:
Installation instructions	
How to use	

Example: FOSSology

Support	Author(SCA, Human), Consume, Transform(REST API)
Functionality	FOSSology is an open source license compliance software system and toolkit allowing users to run license, copyright and export control scans from a REST API. As a system, a database and web UI are provided to provide a compliance workflow. As part of the toolkit multiple license scanners, copyright and export scanners are tools available to help with compliance activities.
Location	Website: https://www.fossology.org/ Source: https://github.com/fossology
Installation instructions	https://www.fossology.org/get-started/
How to use	https://www.fossology.org/get-started/basic-workflow/

Feedback Request

- Will proposed approach meet need?
    - Is this approach to categorizing tools useful? Sufficient?
    - Template: right level of information?
    - What other information is being looked for?
    -
- Know a tool to be added to each ecosystem document? Please let the document owner know about it, so it can be added.
    - SWID: TBD
    - SPDX: kstewart@linuxfoundation.org
    - CycloneDX: steve.springett@owasp.org
- Priorities for next steps?

Questions?

More Info…

Co-Chairs:

- J. C. Herz (Ion Channel) jc.herz@ionchannel.io
- Kate Stewart (Linux Foundation) kstewart@linuxfoundation.org

Mailing List: ntia-sbom-formats@linuxfoundation.org

Subscribe at: https://lists.linuxfoundation.org/mailman/listinfo/ntia-sbom-formats

Shared Drive: https://drive.google.com/drive/folders/1KAQ7AWlWMKcSFnRc_S-7XB76xFRRWLmT