Discover Dependency License Information Using SBOMs and ClearlyDefined

Jeff Mendoza, Kusari

Support from Qing Tomlinson and E. Lynette Rayle

SBOM Legal compliance

- Fields for compliance
  - Licenses, and expression
  - Discovered licenses
  - Attribution / copyright statement

Legal compliance

- Act of complying with the license of the software that you distribute or incorporate in your software
- The license is what makes OSS OSS
- Licenses have obligations, which may include
  - Attribution
  - Retain copyright statement
  - Offer for source
  - Changelog, mark changes

SBOM creation tool

- Dependency detection, identification, hierarchy
- Jack of all trades
- Package manager reported license
- Skip license

ScanCode, Apache-2.0 AboutCode

- Reads all files in a package looking for legal text
- Detailed scan data

- Other scanners as well

ClearlyDefined, MIT OSI

- Central pool of knowledge for legal information about packages of many types
- Declared vs Discovered
- Raw scan data and Definition
- SPDX license list and expressions
- Copyright, Attribution, Source Location
- Only run license scanners once
- Community based Curations
- REST API and website

cdsbom Tool

- Enhance an existing SBOM with Legal information from ClearlyDefined
- Generate NOTICE file
- CLI, and available as a Go library
- https://github.com/jeffmendoza/cdsbom
- Protobom, Apache-2.0 OpenSSF: Easy read, modify, write of SBOMs
- GUAC, Apache-2.0 OpenSSF: Library for PURL to Coordinate conversion

Join the ClearlyDefined Community

- Share SBOM + CD use cases and workflows
- Curate your dependencies
- Donate computer power
- Fix bugs, add features
- https://clearlydefined.io/