# ClearlyDefined

Community Meeting - March 3, 2025

# Agenda

- NOASSERTION
- FOSDEM Recap
- OpenChain / ORT
- OWASP / CycloneDX
- Linux Foundation / SPDX
- Eclipse Foundation

# NOASSERTION

- NOASSERTION cases usually require special handling as they do not have a standard ID mapped to them (e.g. SPDX).
- At SAP, we usually bypass our automated processes for these cases and involve a human (30% of the total CD data).
- How other organizations handle these cases when encountered?
  - Eclipse Foundation feels the same and is using LicenseRef. Other tools like FOSSology are helpful (cross-reference).
  - GitHub: scanner issue, true ambiguity (needs human). Feedback loop beyond curation (we need a formal process to upstream).
- Recent introduction of LicenseRef has potential to help bring clarity to some of these cases.

# FOSDEM Recap

- FOSS license and security compliance tools workshop - January 31 - Brussels
- FOSDEM / SBOM - February 1-2 - Brussels **(Jeff)**
  - **Video recording available (Discover Dependency License Information Using SBOMs and ClearlyDefined)**

# Linux Foundation / SPDX

- Point of contact: Gary O’Neall and Jeff Shapiro
- Using Mendoza’s utility (cdsbom)
- Encourage data using standard format.
- May want to track an issue for the data format that you would like to see.
- Currently, license expression and SPDX identifiers are used, which are standards.
- Going forward, prefer that new data added in the standard format.

# OWASP / CycloneDX

- Point of contact: Alyssa Wright and Steve Springett
- Present ClearlyDefined to community
- Enhance our documentation
- The difference between Declared and Discovered licenses is explained in our documentation:
  - Example of different Declared and Discovered licenses
  - Example of multiple attributions

# OpenChain / ORT

- Point of contact: Shane Coughlan, Thomas Steenbergen, Marcel Kurzmann
- OpenChain event in Stuttgart (April 7-9)
- ORT Community Days is planned to be be held together
- Goals
  - Hear from industry peers as they share their open source processes and best practices.
  - Experience demonstrations from tool creators showcasing automated compliance solutions.
  - Participate in technical sessions focused on overcoming common challenges in the field.
  - Discover available support options from both the community and government resources

# Eclipse Foundation

- Point of contact: Boris Baldassari, Marcel Kurzmann
- Open Regulatory Compliance Working Group
- Eclipse Apoapsis:
- The Eclipse Apoapsis project provides a process and a reference implementation for large-scale software composition analysis (SCA). The **ORT Server** reference implementation is based on the **OSS Review Toolkit** (ORT).

ClearlyDefined

Thank you