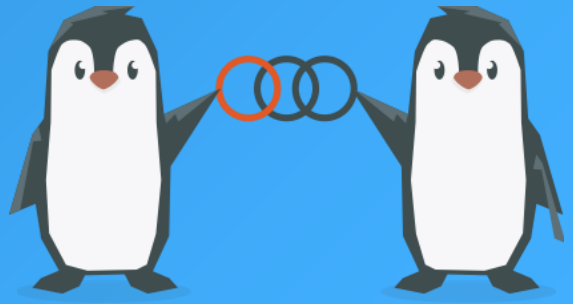
OpenChain SBOM Study Group

Kick-Off Call – Chaired by Norio Kobota from Sony – 2024-07-30

THE LINUX FOUNDATION

OPENCHAIN



Anti-Trust Policy Notice

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.
- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Agenda

- Introduce the practical considerations of using SBOMs in supply chains
- Discuss who these considerations apply to
- Talk about existing market solutions: Case Study SPDX Lite
- Have an open discussion on next steps

Welcome Our Chair for 2024

- Norio Kobota San, Senior Open Source Strategist
  Open Source Program Office
  Sony

THE LINUX FOUNDATION

OPENCHAIN

Practical Considerations: SBOM in Supply Chain

- What is necessary for compliance matters?
  - License compliance
  - Security assurance
  - Other compliance-related topics
- What regulations exist?
  - United States Executive Order
  - NTIA Minimum Requirements
  - Cyber Resilience Act
- What is necessary for efficiency?
  - Keeping overhead low
  - Ensuring suppliers can realistically produce SBOM
  - Etc.

Who These Considerations Apply To

- From our perspective:
  Everyone using the open source supply chain.

Existing Market Solutions

- Let’s have a case study on SPDX Lite as an example of a practical solution for addressing the question of “what type of approach can empower suppliers to get started with SBOM?”

- The context is:
  - Suppliers have limited resources
  - Suppliers **and** customers need minimal adjustment to deployment processes
  - Time is extremely limited for everyone

Open Discussion on Next Steps

- How often should we meet?
- How should we address topics?
- How long should the meetings be?

Initial Suggestions:

- Monthly workshop
- One case study per workshop
- One or two hours long

Goal: make sure practical "how to" information is available to everyone

Thank you everyone! See you next time!