OpenSSF
OPEN SOURCE SECURITY FOUNDATION

SBOM Everywhere

SBOM-a-Rama
Winter 2024

OpenSSF Mission

OPEN SOURCE SECURITY FOUNDATION

The Open Source Security Foundation (OpenSSF)

seeks to make it easier to sustainably secure the

development, **maintenance**, and **consumption**

of the open source software (OSS) we all depend on.

This includes fostering **collaboration**, **establishing** best practices, and **developing** innovative solutions.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

SBOM Everywhere

OSSF SBOM Everywhere SIG

- TODO: Add Description

Motivation

- The initial motivation for the formation of the OSSF SBOM Everywhere SIG is born from OpenSSF's The Open Source Software Security Mobilization Plan. SBOM standardization and consensus from within the open source community is integral to adoption of universal constructs that reveal themselves via the exploration of use cases beyond a compliance check box. [Executive Order]

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

SBOM Naming Document

https://github.com/ossf/sbom-everywhere/blob/main/reference/sbom_naming.md

Consistent Naming Conventions

For SBOMs which are distributed with source tarballs or pre-built binaries as a part of a defined release of the software, the requirements for "release" files is typically a flat list of files without directories (think GitHub or GitLab Release artifacts). To meet these requirements, no directory structures should be used.

Following guidance from SLSA provenance attestations of appending a corresponding extension to the filename of the artifact that is being described. For the CycloneDX and SPDX SBOM standards and their file extension formats the guidance is as follows:

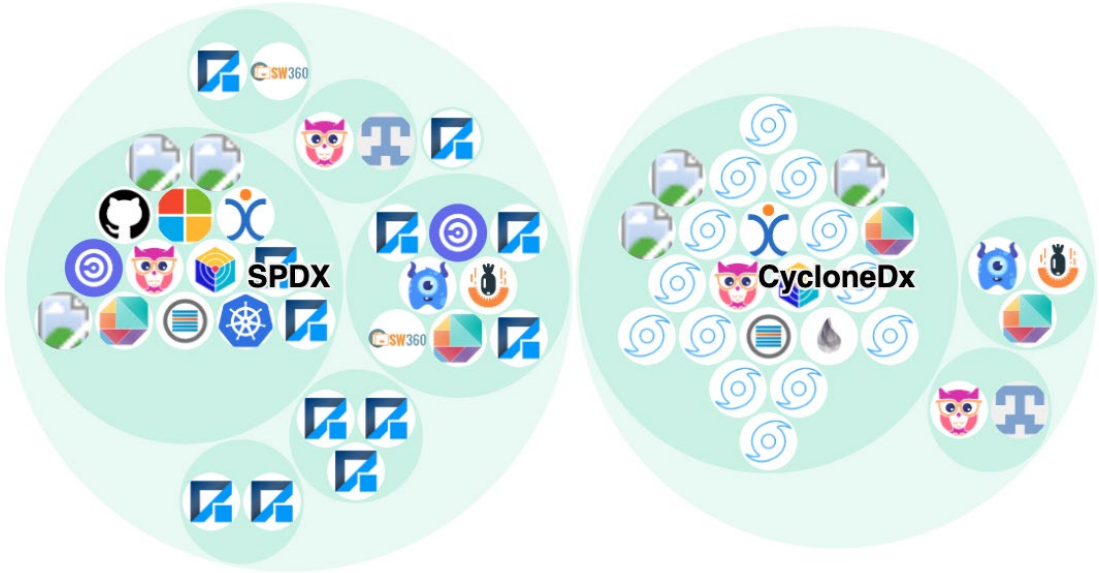
Standard + Format	Artifact Filename	SBOM Filename
CycloneDX JSON	artifact-1.0.0.tar.gz	artifact-1.0.0.tar.gz.cdx.json
CycloneDX XML	artifact-1.0.0.tar.gz	artifact-1.0.0.tar.gz.cdx.xml
SPDX TAG:VALUE	artifact-1.0.0.tar.gz	artifact-1.0.0.tar.gz.spdx
SPDX JSON	artifact-1.0.0.tar.gz	artifact-1.0.0.tar.gz.spdx.json
SPDX XML	artifact-1.0.0.tar.gz	artifact-1.0.0.tar.gz.spdx.xml
SPDX YAML	artifact-1.0.0.tar.gz	artifact-1.0.0.tar.gz.spdx.yml (or .yaml)
SPDX RDF XML	artifact-1.0.0.tar.gz	Artifact-1.0.0.tar.gz.spdx.rdf (or .rdf.xml)

The .spdx.* and .cdx.* extensions are sourced from the CycloneDX and SPDX guidance on filename extensions for SBOM documents of the corresponding standard and format.

The JSON format files should be considered a mandatory requirement and are always available. The tool support for JSON documents is considered to be better than the other file format options. If other formats are desired, the JSON SBOM should also be available.

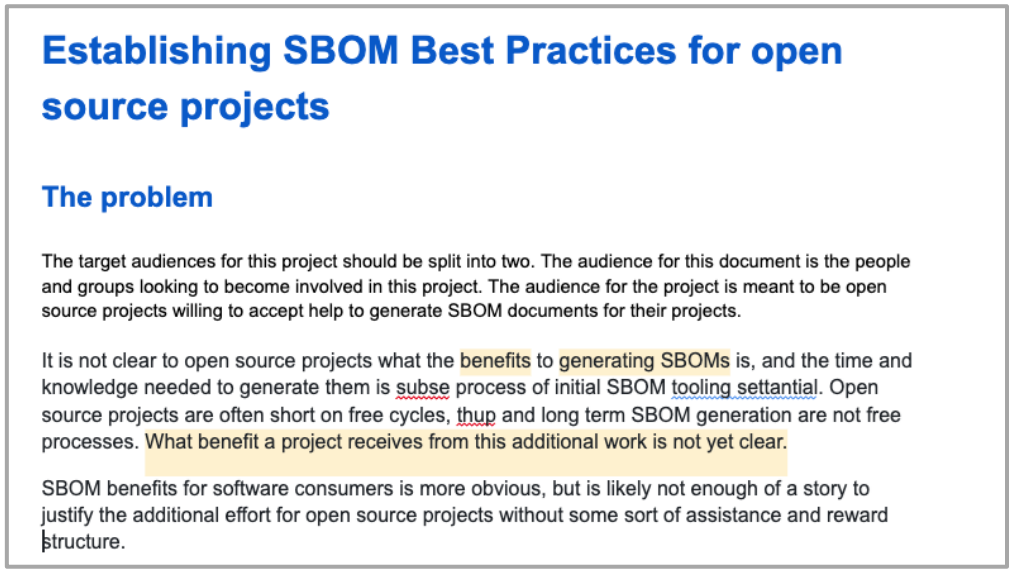
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Landscape



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

SBOM assistance



Establishing SBOM Best Practices for open source projects

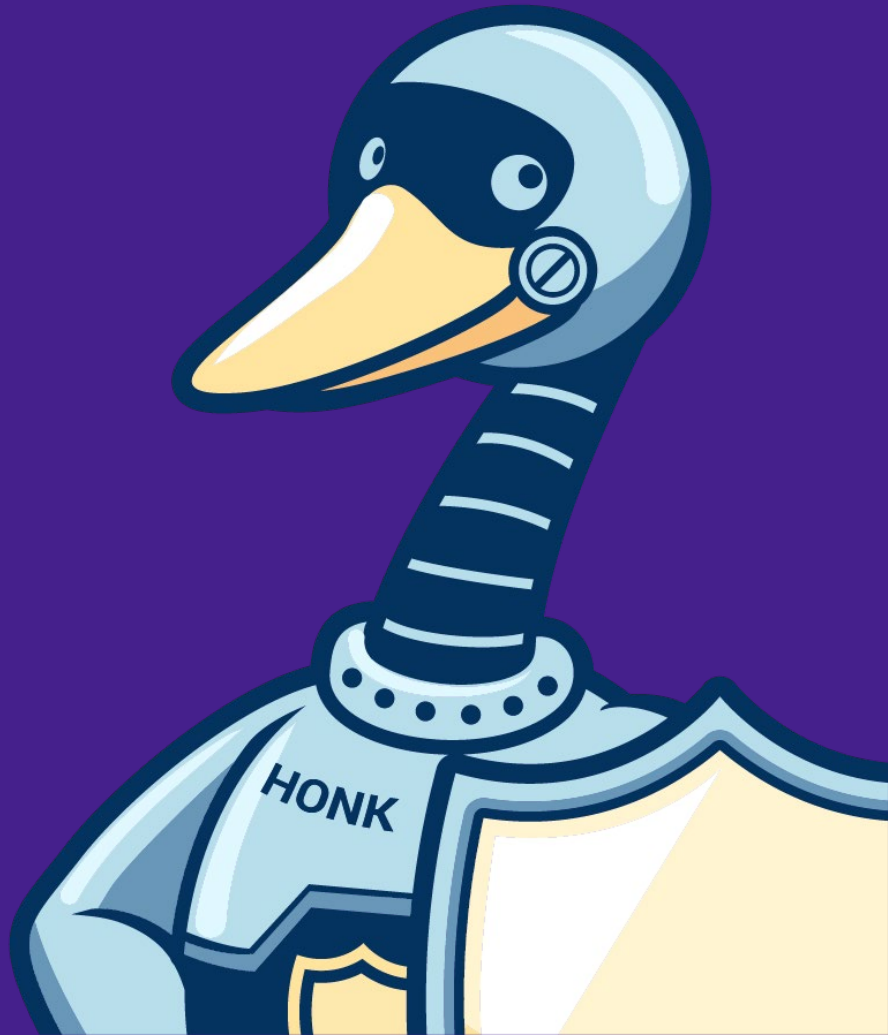
The problem

The target audiences for this project should be split into two. The audience for this document is the people and groups looking to become involved in this project. The audience for the project is meant to be open source projects willing to accept help to generate SBOM documents for their projects.

It is not clear to open source projects what the benefits to generating SBOMs is, and the time and knowledge needed to generate them is subse process of initial SBOM tooling settantial. Open source projects are often short on free cycles, thup and long term SBOM generation are not free processes. What benefit a project receives from this additional work is not yet clear.

SBOM benefits for software consumers is more obvious, but is likely not enough of a story to justify the additional effort for open source projects without some sort of assistance and reward structure.

How can you contribute?



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

https://github.com/ossf/sbom-everywhere

Instructions to join the Slack and meetings are at the bottom of the page

Get involved!

We would love your help!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Thank You!