2022-01-10 - Software Bill of Materials - ONAP story

Topic Leader(s)

- Muddasar Ahmed
- Pawel PawlakS

Topic Description

30m Muddasar Ahmedand Pawel Pawlak

SBOM is a software inventory and related descriptive information, a list of ingredients that make up software components. We will share with other LFN projects ONAP SBOM story

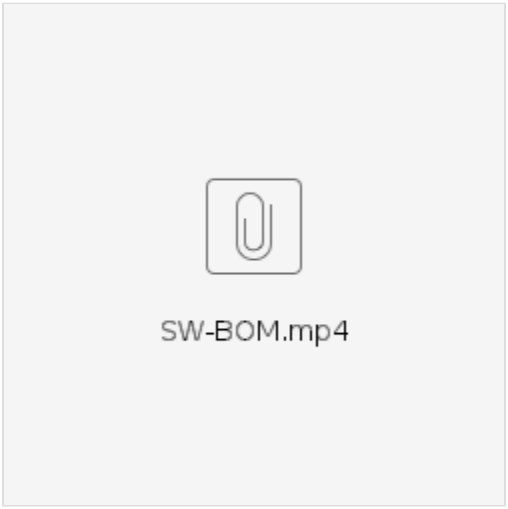
Topic Overview

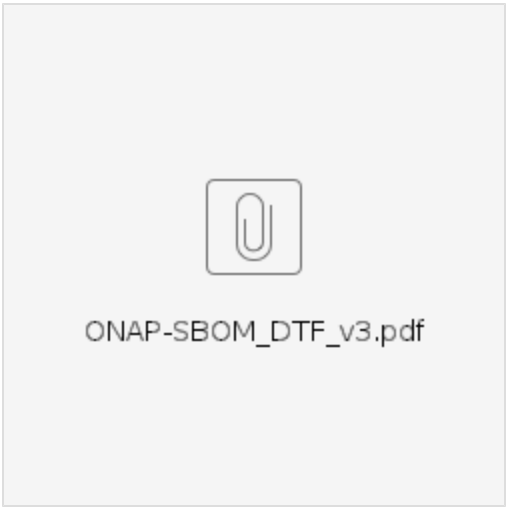
An SBOM is a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships. These inventories should be comprehensive – or should explicitly state where they could not be. There are several benefits of creating and using SBOM include reducing cost, security risk, license risk, and compliance risk. SBOMs helps in improving software development, supply chain management, vulnerability management, asset management, procurement, and high assurance processes.

We will describe available formats, and why we selected SPDX. We will review real ONAP SBOM and discuss SBOM generation in LFN CI pipeline.

Slides & Recording

Live Interactive Session





Agenda

- What is SBOM
- SBOM vs. HBOM
- SBOM formats
- ONAP SBOM review

Minutes

SBOMs available formats were reviewed with an explanation of selected SPDX as ISO standard for an ONAP SO pilot and real ONAP SBOM generation in LFN CI pipeline. Adding SBOM capability in the pipeline has no roadblocks, call for action was to implement it sooner as it does not require a lot of efforts on project teams.

Action Items

- [ ]