2022 LFN Security whitepaper

Document outline:

- Intro / overview of recent LF efforts, OpenSSF project
- LFN-specific actions and how they align to all-up LF efforts to secure OSS
    - Committee and sub-committe
    - Best practices
        - CII badging
        - SBOM
    - Sampling of projects and their specific approach to security
        - ONAP
            - SBOM
                - ONAP is updating its processes so that Software Bill of Materials (SBOMs) are automatically generated and distributed with ONAP software releases. SBOMs are files that record the components (e.g., libraries, packages, etc.) of a software product. These records provide many benefits: it makes it easier to track changes between versions of a release, it can help in debugging dependency errors in an installation, and it can help identify whether a product contains libraries that have known software vulnerabilities. All of this makes it easier to deploy, maintain, and secure software.

                  Once fully implemented, ONAP's build processes will automatically create the SBOMs for each release. Like many environments today, ONAP's build tools include the ability to compile the components included in the build process and output this information in SBOM files. As such, there are no additional steps for developers and project owners. The result is a "free" way to make ONAP easier to use and manage. Interest in SBOMs has been growing over the years and today many organizations have procurement requirements that stipulate that SBOMs be delivered and numerous software developers have taken the step to include them with their software. The ONAP project is proud to join the list of projects that supports this valuable enhancement.
        - ODL
        - TF
        - EMCO
- Closing summary + invitation to join