Exploring Software Bills of Materials (SBOMs)

chip

First, what even is a SBOM?

A Software Bill of Materials (SBOM) is a formal record of all software packages and components used in a software project. These packages and components include all third-party and open-source code, such as libraries, languages, APIs, etc. Essentially, SBOMs contain everything your software relies on that you didn't write yourself.

Why do we need SBOMs?

Because **components** rely on other components, SBOMs are built in a hierarchical nature and show the **dependencies**, or relationships, between different components. SBOMs also include information on **vulnerabilities**, or identified risky software, and thus can add transparency to a project.

With that in mind, let us introduce the

Centralized Hub for Inventories Platform

A simple way to create, vizualize, and manage SBOMs

SBOM Generation

Four different scripts that can run on any OS to create an SBOM for your app.

- SBOMs created in the **CycloneDX** format, a popular company standard.
- Dependencies & metadata created with **CDXGen** and vulnerabilities added through **Grype.**

SBOM Storage

One place to efficiently view and store all your SBOMs.

- A streamlined database to ensure a **fast user experience.**
- A sleek view page to **search, upload, and update** your SBOMs.
- A complete list of all **vulnerabilities** present in a SBOM.

SBOM Visualization

A simple tree to help visualize the dependency relations of your app.

- Uses **D3-vizualization** for a tree graph based on the SBOM for your app
- Increased visibility for dependencies with **vulnerabilities**

Thank you to our sponsors at Cisco, our stakeholders at Duke ITSO, and our team leads Alexis Sparko and Julie Biaunie and mentors at Duke Innovation Co-lab.