Onboarding Document

The purpose of this document is to familiarize you to the development that has happened thus far with regards to SBOMs.

There is no specific language you need to know; however, a knowledge of C# might help to gain a more in depth understanding of the code for the Microsoft sbom-tool.

This document is created for a windows device. Linux or mac might require some adaptation.

SBOM

An SBOM, or a Software Bill of Materials, can be thought of as a blueprint of software. A generator tool will take in the source code of a project, will find "components" and relationships within the code, and will generate an SBOM out of this information. The SBOM can then be "consumed" with a consumption tool to get the vulnerabilities of the components of the project.

End goals:

1. Produce SBOMs for all programming languages used by USAF
2. Incorporate SBOM generation into a pipeline
3. Store SBOMs in a coherent, accessible manner
4. Allow the consumption/analysis of SBOMs

Other possible goals:

1. Automation of SBOM consumption

Current major focuses

1. Microsoft sbom-tool for SBOM generation
2. Daggerboard for SBOM consumption

Accomplishments:

1. Generate SBOM using sbom-tool for a C# project
    - sbom tool
    - sbom tool example
2. Generate SBOM using github actions
3. Using docker, experiment with sbom consumption tools
    - dependency track
    - daggerboard
4. Create a detector for the component-detection tool
    - create detector

Issues:

1. We do not have a good way of generating an SBOM for C/C++ projects
    - Look into vcpkg, since May 2022 they should generate a vcpkg.spdx.json file that can be consumed using the vcpkg experimental tool

2. Detector needs to be created for Jovial and Ada (requires `(possibly advanced)` knowledge of Jovial and Ada language and environment)
3. Dependency Track only works with CycloneDX - likely won't change
4. Daggerboard needs further development - opportunity to partner with NYPH (new york presbyterian hospital) and have large say in roadmap/development of Daggerboard

Resources:

- https://github.com/microsoft/sbom-tool
- https://github.com/microsoft/component-detection
- https://github.com/nyph-infosec/daggerboard
- https://dependencytrack.org/
- https://cyclonedx.org/
- https://spdx.dev/
- https://github.com/AppThreat/cdxgen

Contacts

Types of SBOMs

There are two major SBOM formats, SPDX and CycloneDX.

There is more to be learned about the differences between SPDX and CycloneDX. It seems that SPDX is able to contain more information than CycloneDX. CycloneDX seems to be easier for computers to parse.

Microsoft's sbom-tool currently only supports SPDX but it seems it will support CycloneDX within the near future. There are several generator tools that support CycloneDX, the most general and easiest to use that we found is cdxgen. To look for other CycloneDX generators see cyclonedx.org/tool-center/.

Daggerboard purports to support both CycloneDX and SPDX. OWASP, the designers of CycloneDX, created Dependency-track which currently supports only CycloneDX.

SBOM generation

Microsoft sbom-tool

- sbom-tool overview
- REPO:sbom-tool
- REPO:component-detection
- Tutorial - Generate SBOM for .NET project
- Advanced: Creating a Detector

cdxgen

- https://github.com/AppThreat/cdxgen

GitHub actions

- Tutorial - Create SBOM artifact using sbom-tool and GitHub Actions

Syft

- Example - SBOM generation and conversion using Syft

Consumption Tools

- Dependency Track
- Daggerboard

Create a document for new team members that guides them through the work accomplished so far on the generation and consumption tools, points them to resources and point of contacts such as those on the Microsoft Team.