Tiger Team:

SBOM Generation Reference Implementations

Adolfo Carcia Veytia

Daniel Moch

Doug Dennis

Gary O'Neall

Ian Dunbar-Hall

Manoj Prasad

Ricardo Reyes

Tieg Zaharia

Viktor Petersson

sbomify

Purpose and Goal

- How do we create SBOMs for a sample project that meets both:
  - NTIA's Minimum Elements
  - Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) Third Edition
- Produce CycloneDX and SPDX SBOMs
- Publish findings in a GitHub repository
- Contribute our findings upstream if possible

Constraints

- The SBOM generation process must run in CI/CD
  - While we're using GitHub Action, it should be as agnostic as possible
- All tools must be open source

Project Phases

Phase 1

- Java Application
  - Keycloak was selected
- Container Image with Python application
  - Django was selected

Phase 2

- Go Application
- Container Image with Go application

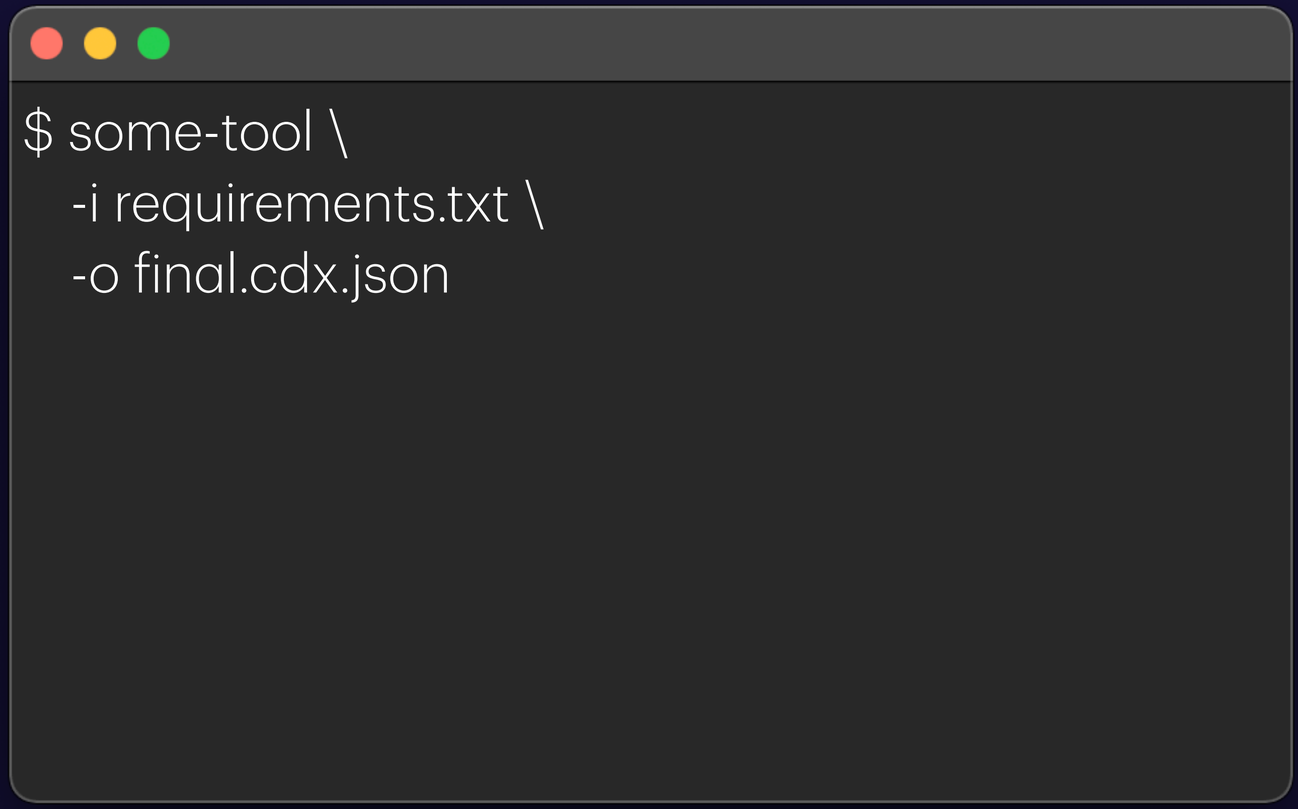
Phase 3

- "Legacy" C or C++ Application

sbomify

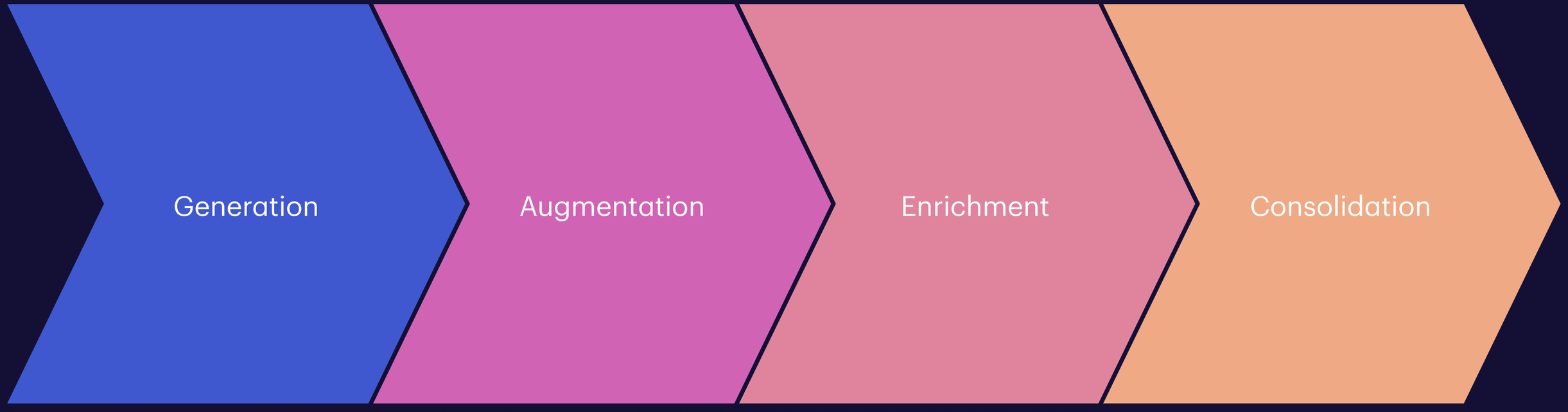
Expectation

- Run one of the many tools
- Get a valid SBOM
- Move on



sbomify

Reality: SBOM Creation Steps



sbomify

Findings so far

- Supporting both CycloneDX and SPDX creates a lot of overhead
- Meeting NTIA is a not straight forward
- Hard to benchmark framing document
- Hierarchal SBOMs are needed for even basic examples
- Source vs Build SBOMs yield very different results
- We were unable to contribute upstream to Django due to lack of proper dependency pinning

Findings so far

Tool	Format	Packages	Unique Packages	Duplication %
Syft	CycloneDX	192	172	10.42%
Trivy	CycloneDX	180	178	1.11%
Syft	SPDX	192	173	9.90%
Tvivy	SPDX	181	172	4.97%

Findings so far

Tool	Format	Packages	Unique Packages	Duplication %
cyclonedx-python	CycloneDX	3	3	0%
sbom4python	CycloneDX	3	3	0%
Syft	CycloneDX	3	3	0%
Trivy	CycloneDX	4	4	0%
sbom4python	SPDXD	3	3	0%
Syft	SPDXD	4	4	0%
Trivy	SPDXD	5	5	0%

Where are we today?

- Reusable "Blueprint" CI/CD structure is done
- Generation and Consolidation is done for phase 1*
- Augmentation and Enrichment is work in progress*

* Only for CycloneDX

Resources

- GitHub Repository
- Meeting Notes
- SBOM Resources
- SBOM Benchmarks

sbomify