Istio and Supply Chain Security

Faseela K
Cloud Native Developer - Ericsson

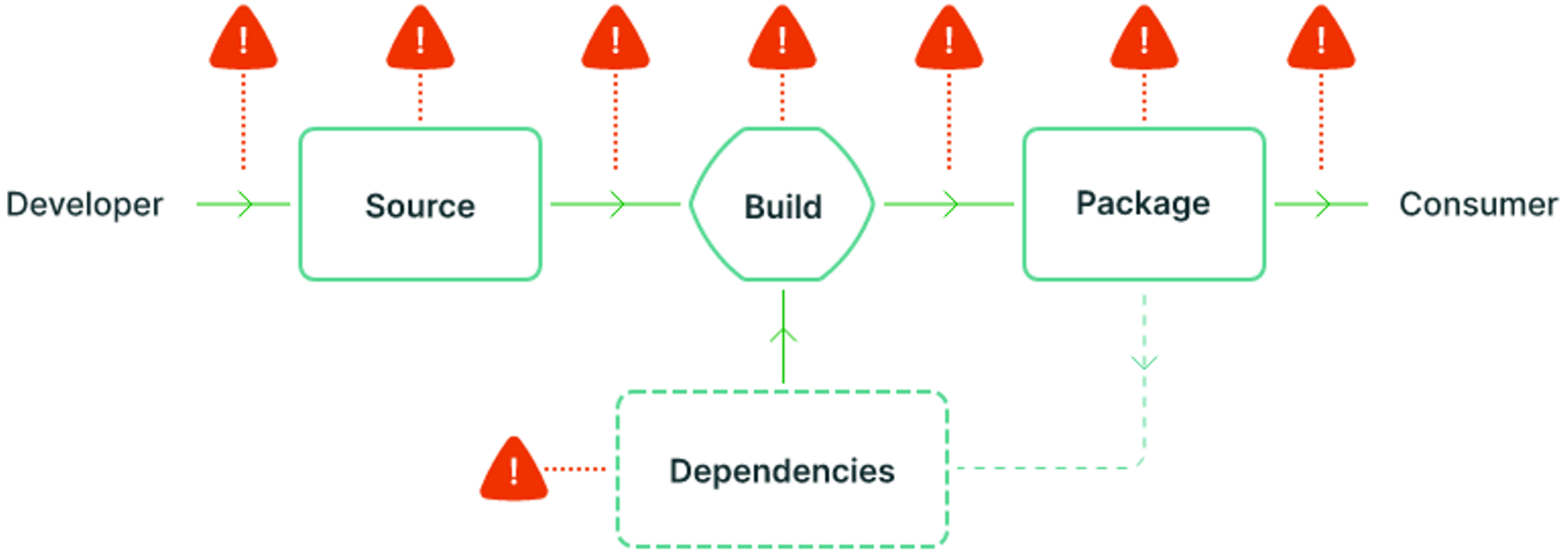
Adolfo Garcia Veytia
Staff Software Engineer - Chainguard

Agenda

- What is a Supply Chain Attack?
- Open source initiatives for Supply Chain Security
- Software Bill Of Materials
- Kubernetes BOM
- Istio Meets Kubernetes BOM
- What’s next?
- Q & A

Software Supply Chain

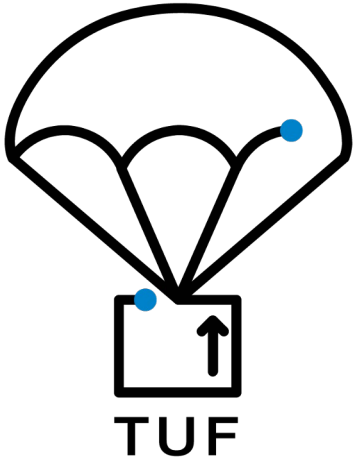
A complex, globally interconnected ecosystem that encompasses the entire life cycle of hardware, software, and managed services to compose, build and ship a software project.


Developer
Source
Build
Package
Consumer
Dependencies

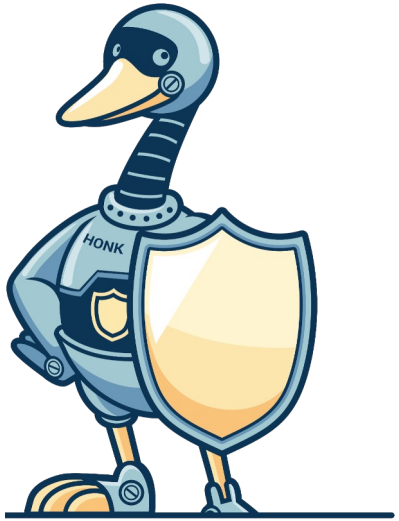
Supply Chain Attack Vectors

- Commit bad code to source
- Compromise source control platform
- build with code that is not matching source control
- Compromise build platform
- Malicious third party dependency
- Bypassing of CI/CD pipelines
- Compromised package repositories
- Make end user consume malicious package

Open Source Initiatives



Open Source Initiatives



Open Source Initiatives

Software Bill Of Materials

A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships of various components used in building software.

Source: National Telecommunications and Information Administration
https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf

SBOM

- Identifying and avoiding known vulnerabilities
- Quantifying and managing licenses
- Identifying both security and license compliance requirements
- Enabling quantification of the risks inherent in a software package
- Managing mitigations for vulnerabilities
- Lower operating costs due to improved efficiencies and reduced unplanned and unscheduled work.

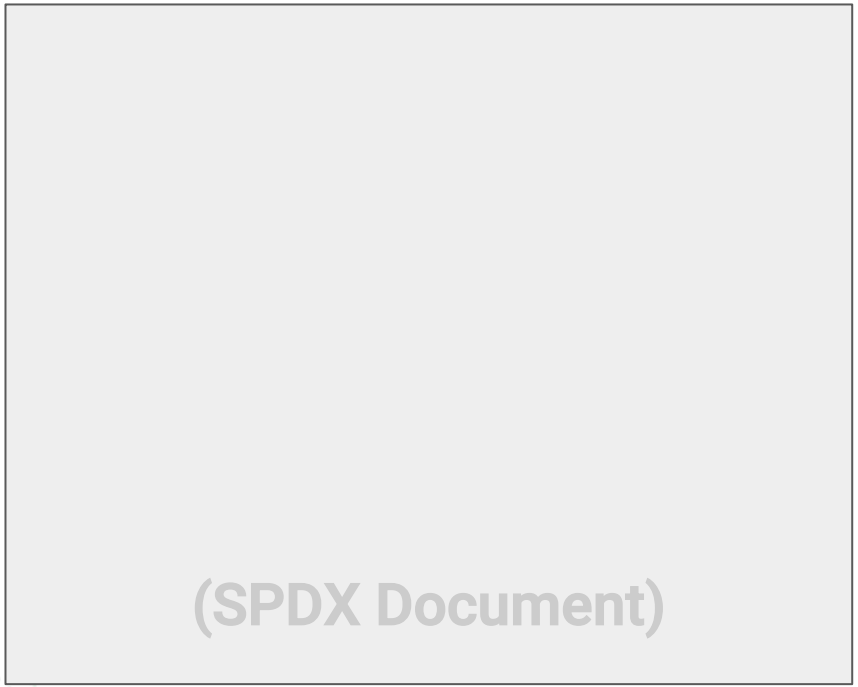
A project of the Linux Foundation

Under development for 10+ years

Codified standard ISO/IEC 5962:2021

Currently at version 2.2.1 (3.0 coming soon)

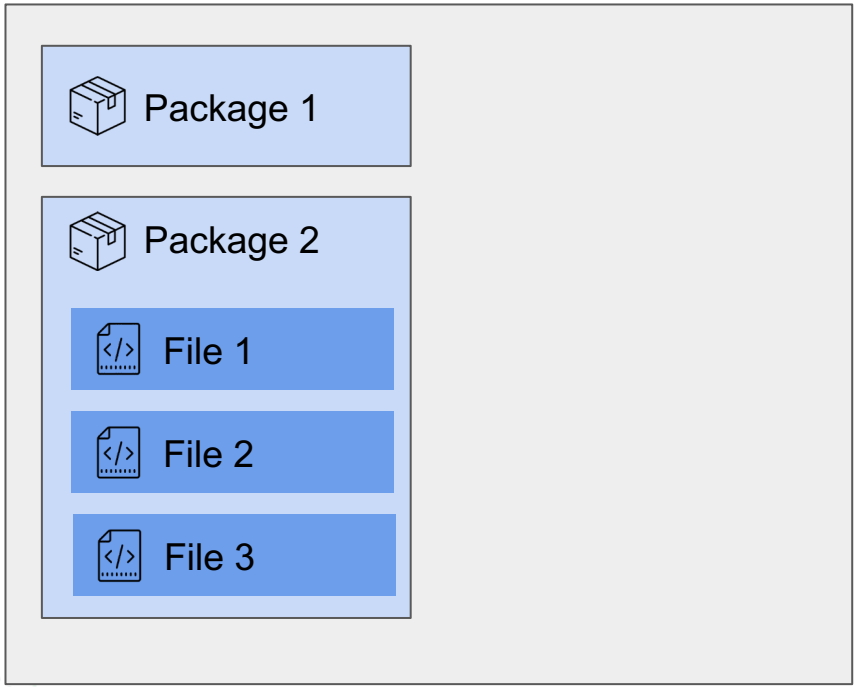
SPDX Elements



Document Metadata:

- Document ID / Namespace
- Name
- SPDX Version
- Time of creation
- Author (Person/Organization)
- Tooling Information

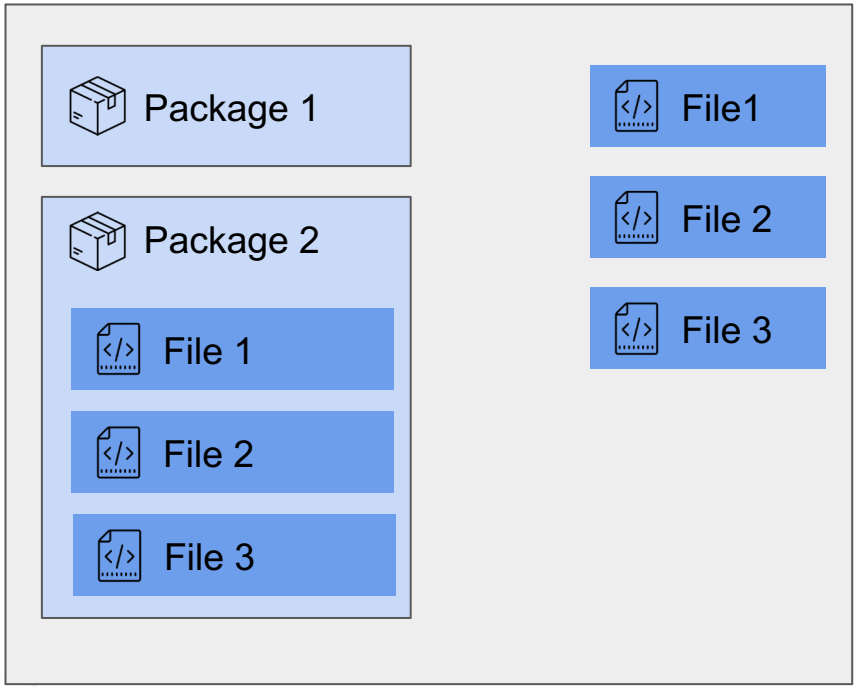
SPDX Elements



You can add a single Package …

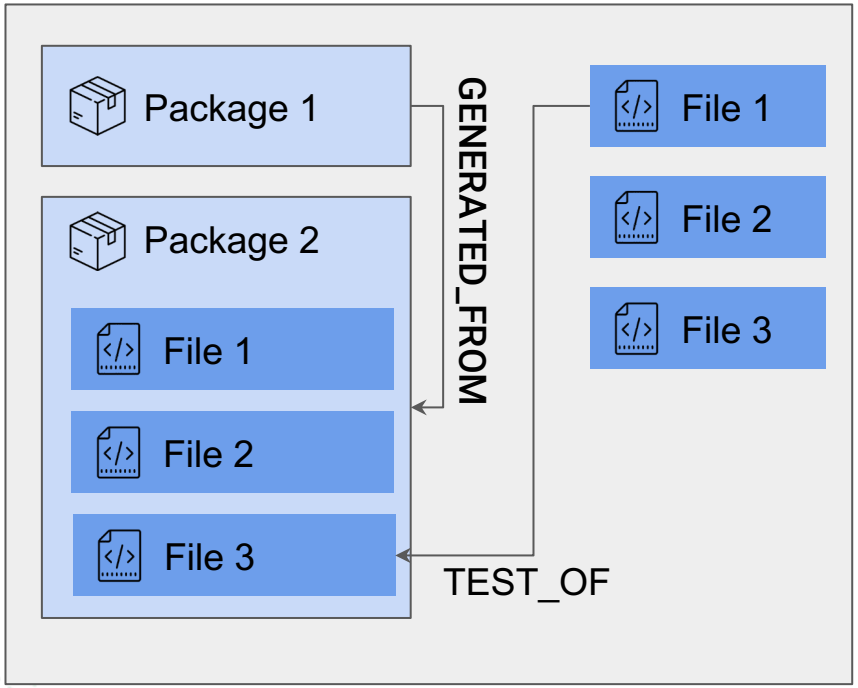
… or list its contents too

SPDX Elements



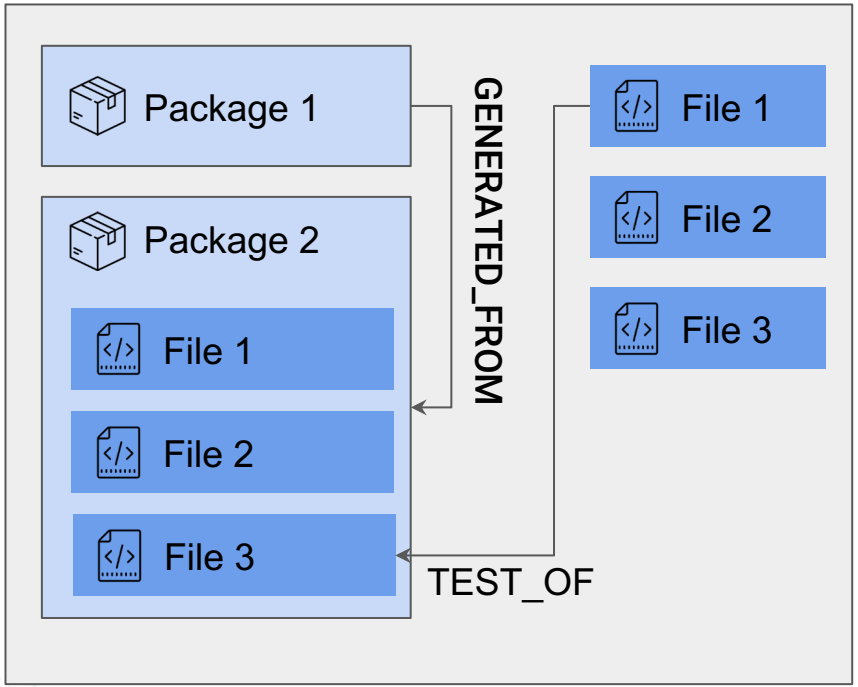
Single files can be added to the document at the top level

SPDX Elements



End every element is related to another in one or more ways.

SPDX Elements



SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: SBOM-SPDX-f2ea6055-5c60-46ea-9a56-af867552ffb0
DocumentNamespace: https://spdx.org/spdxdocs/k8s-releng-bom-f68ec784-9dc1-48b1-b1e8-78a5de60d366
Creator: Tool: sigs.k8s.io/bom/pkg/spdx
Created: 2022-01-20T22:27:10Z

Package: istio

PackageName: istio
SPDXID: SPDXRef-Package-istio
PackageDownloadLocation: NONE
FilesAnalyzed: true
PackageVerificationCode: 2cc4c44422ea3fe8498b53dda8506065076e398a
PackageLicenseConcluded: Apache-2.0
PackageLicenseInfoFromFiles: Apache-2.0
PackageLicenseInfoFromFiles: BSD-2-Clause
PackageLicenseInfoFromFiles: BSD-3-Clause
PackageLicenseInfoFromFiles: MIT
PackageLicenseInfoFromFiles: ISC
PackageLicenseInfoFromFiles: MPL-2.0
PackageLicenseInfoFromFiles: MPL-2.0-no-copyleft-exception
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION

FileName: .gitattributes
SPDXID: SPDXRef-File-istio-.gitattributes
FileChecksum: SHA1: a85000359933af3a64be09b5f2488c91a96e2a55
FileChecksum: SHA256: 425242d7373278995b688d91db1659ea90e9c8f536ddbcedf75a5ab14ee1c832
FileChecksum: SHA512:
4356493e0a8f00dc94484c12a96be4a7fb2f3a03cf260d2cc980c8c4385880730779aa03b002bb4839e7ca0a13bedc6bc9cd
b76f0b5ad74
d088e932f528b28d8
FileType: OTHER
LicenseConcluded: Apache-2.0
LicenseInfoInFile: NONE
FileCopyrightText: NOASSERTION

SPDX Elements

File captures the metadata about a any kind of file:

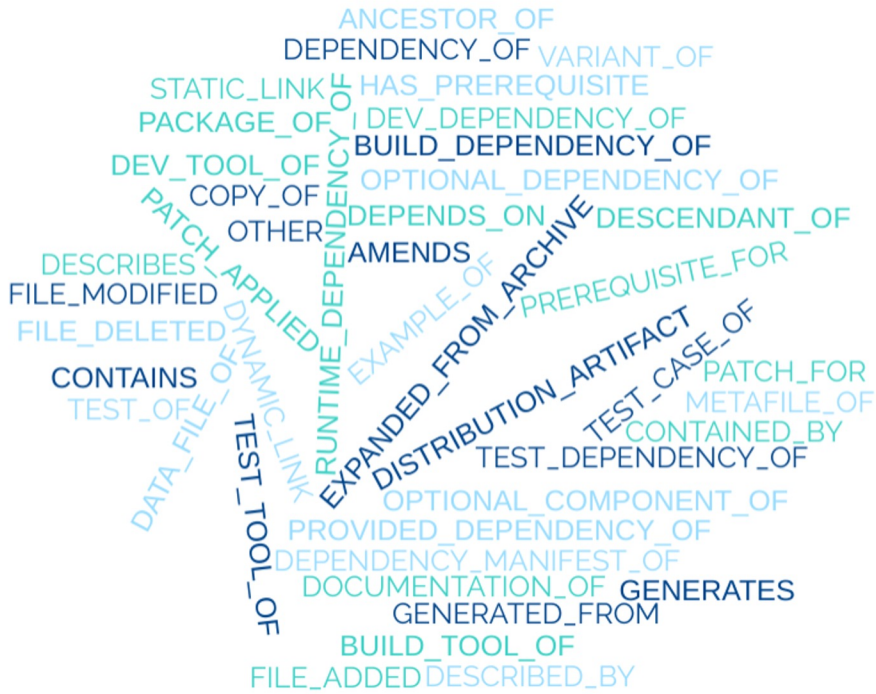
- Filename
- FileType
- Checksums
- License
- Copyright Text
- Attribution
- Contributor Data
- Notes

SPDX Elements

Package represents a group of other elements (files or packages).

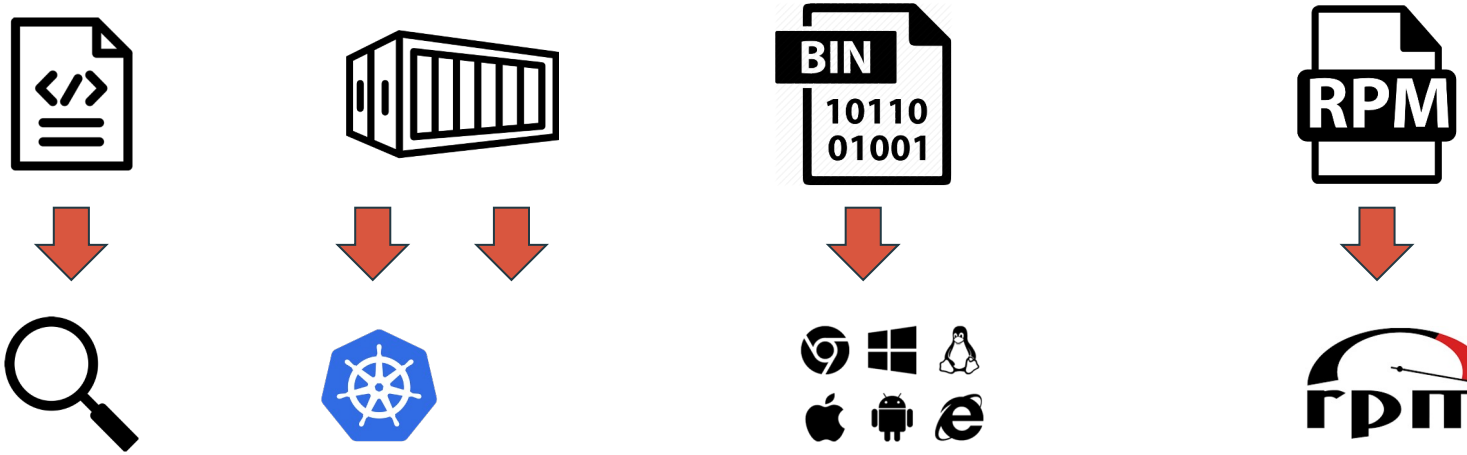
- Name
- Version
- FileName
- Supplier
- Originator
- Download location
- License (of package and contents)
- Comments

SPDX: Relationships



Artifacts: Many Types!!

SBOMs can describe different kinds of artifacts. Targeting different types of consumers

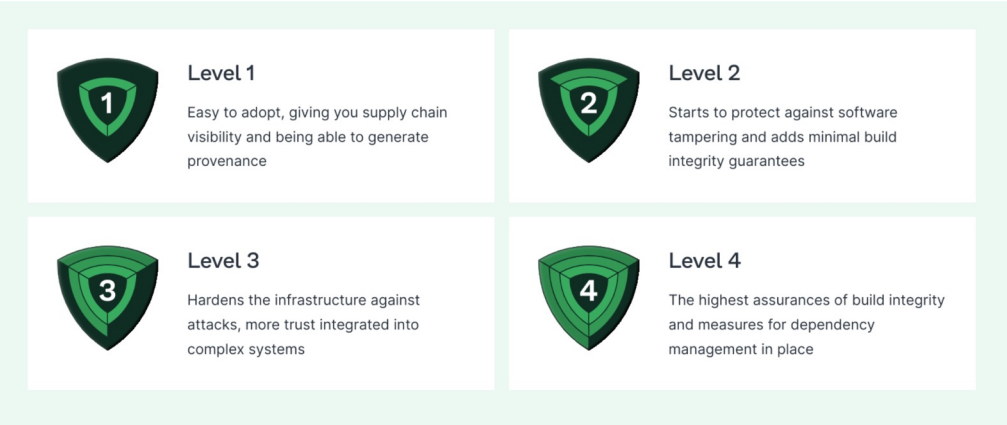


SBOMs: The Start of the Journey

SLSA: Supply chain Levels for Software Artifacts

A framework to gradually improve your supply chain security posture.

Starts with adding visibility.

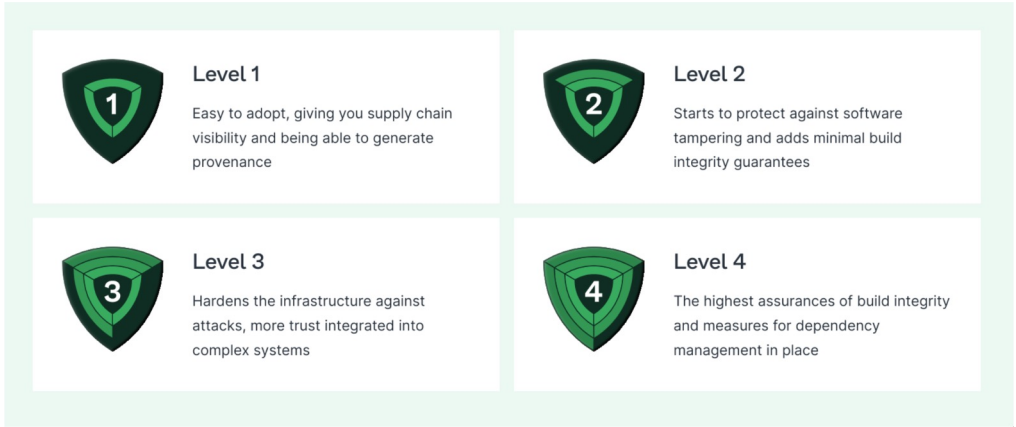


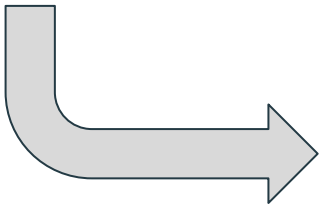
SBOMs: The Start of the Journey

SLSA: Supply chain Levels for Software Artifacts

A framework to gradually improve your supply chain security posture.

Starts with adding visibility.





SBOM!

SBOM with '*k8s bom*'

- Generate an SBOM from your git repository

```
cd istio
bom generate -n https://istio.io .
```

- Add other artifacts to your SBOM

```
bom -n https://istio.io generate \
   --dirs .  \
   --image-archives pilot.tar.gz \
   --file ./README.md  \
   --tarball istio-1.13.3-linux-amd64.tar
```


Istio Meets k8s bom

- Analyzed different bom generation tools
- Istio RFC for SBOM
- Collaboration with the Kubernetes Release Engineering Team
- SPDX Bill of Materials describing source code, dependencies and release artifacts

Istio source sbom


```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: Istio Source 1.13.3
DocumentNamespace:
https://storage.googleapis.com/istio-
release/releases/1.13.3/istio-source.spdx
Creator: Tool: sigs.k8s.io/bom/pkg/spdx
Created: 2022-04-14T16:52:19Z

##### Package: istio

PackageName: istio
SPDXID: SPDXRef-Package-istio
PackageDownloadLocation: NONE
FilesAnalyzed: true
PackageVerificationCode:
6418187297549f8757bbb1b56fe5e5af5bae8ca5
PackageLicenseConcluded: Apache-2.0
PackageLicenseInfoFromFiles: Apache-2.0
PackageLicenseInfoFromFiles: BSD-2-Clause
PackageLicenseInfoFromFiles: BSD-3-Clause
PackageLicenseInfoFromFiles: MIT
PackageLicenseInfoFromFiles: ISC
PackageLicenseInfoFromFiles: MPL-2.0
PackageLicenseInfoFromFiles: MPL-2.0-no-
copyleft-exception
```

Istio release sbom

```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: Istio Release 1.13.3
DocumentNamespace:
https://storage.googleapis.com/istio-release/
releases/1.13.3/istio-release.spdx
Creator: Tool: sigs.k8s.io/bom/pkg/spdxCreated: 2022-
04-14T16:49:15Z

##### Package: istio/pilot:1.13.3-debug
PackageName: istio/pilot:1.13.3-debug
SPDXID: SPDXRef-Package-istio-pilot-1.13.3-debug
PackageDownloadLocation: NONE
FilesAnalyzed: false
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION

##### Package:
blobs/sha256/e0b25ef516347a097d75f8aea6bc0f42
A4e8e70b057e84d85098d51f96d458f9

Relationship: SPDXRef-Package-istio-pilot-1.13.3-debug
CONTAINS SPDXRef-Package-istio-pilot-1.13.3-debug-
blobs-sha256-e0
b25ef516347a097d75f8aea6bc0f42a4e8e70b057e84d85098d51f9
6d458f9
```

What's in an istio release?

- 3 Operating systems: Linux, MacOS, Windows
- 3 architectures: amd64 armv7 arm64
- Docker images
- Other binaries
- Tarball bundles
- Source Code Tarball
- rpm + deb packages
- Licenses and Helm Charts
- Manifests
- 

SPDX compatible SBOM files

Future plans

- K8s bom
  - Linux package sources: .rpm & .deb
  - More expressive YAML definitions
  - Integration with SPDX libraries for more languages
  - Output to other SPDX formats (RDF, etc)
  - Document validation + verification
  - SPDX document visualization
  - SBOM signing and attaching capability
- Istio sbom
  - Analyze more sbom standard formats
  - Integrate to newer bom functionalities

Thank you!

- @puerco (Twitter | CNCF/Kubernetes Slack | GitHub)
- @Faseela K (Istio Slack)