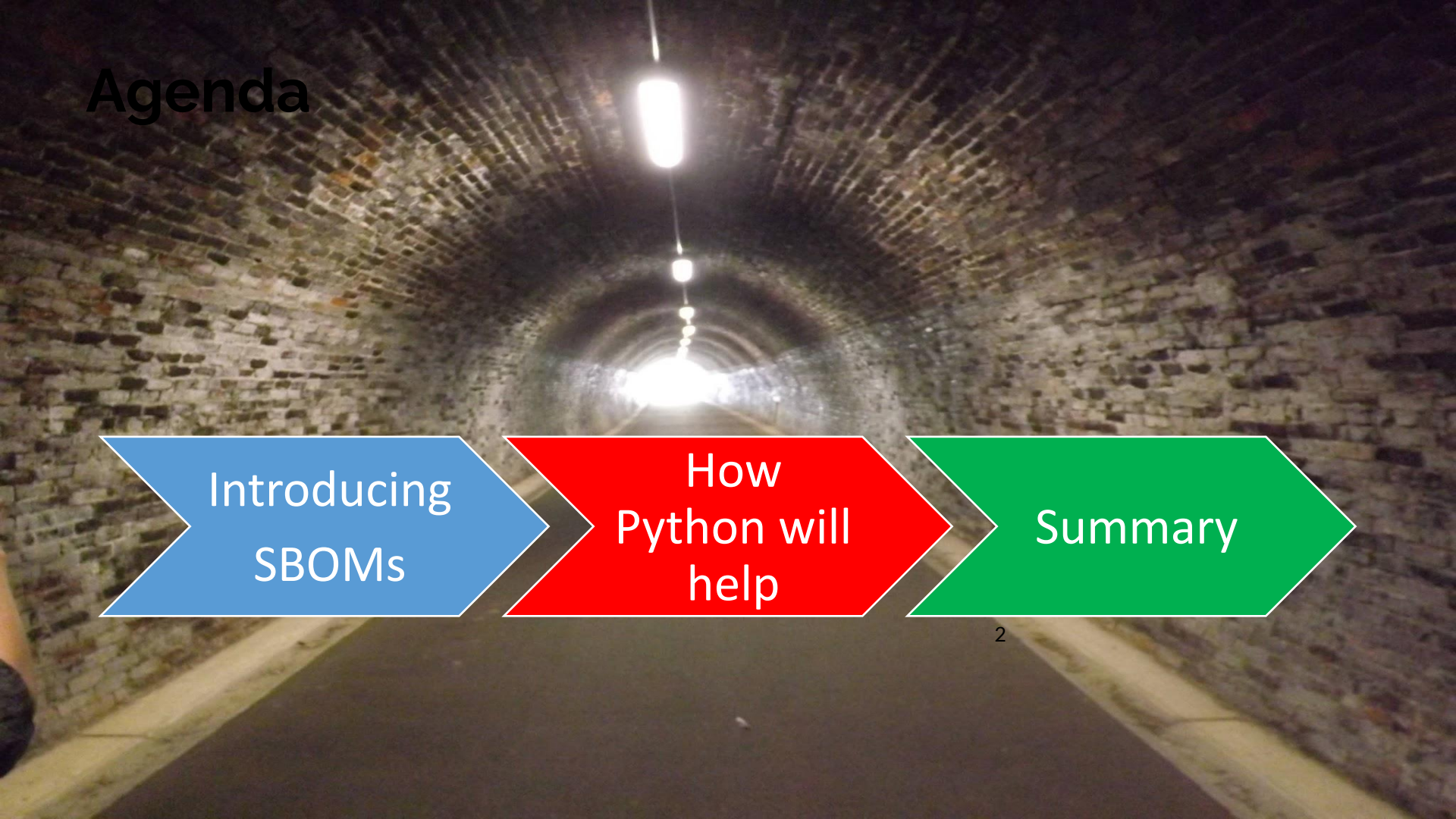
SBOMs are coming

How will Python help?

Anthony Harrison

PyCascades 2023 - March 2023

Agenda



Independent Consultant

Open Source enthusiast

Using Python since 2013

Runner

STEM AMBASSADORS

CoderDojo

Can you answer these?

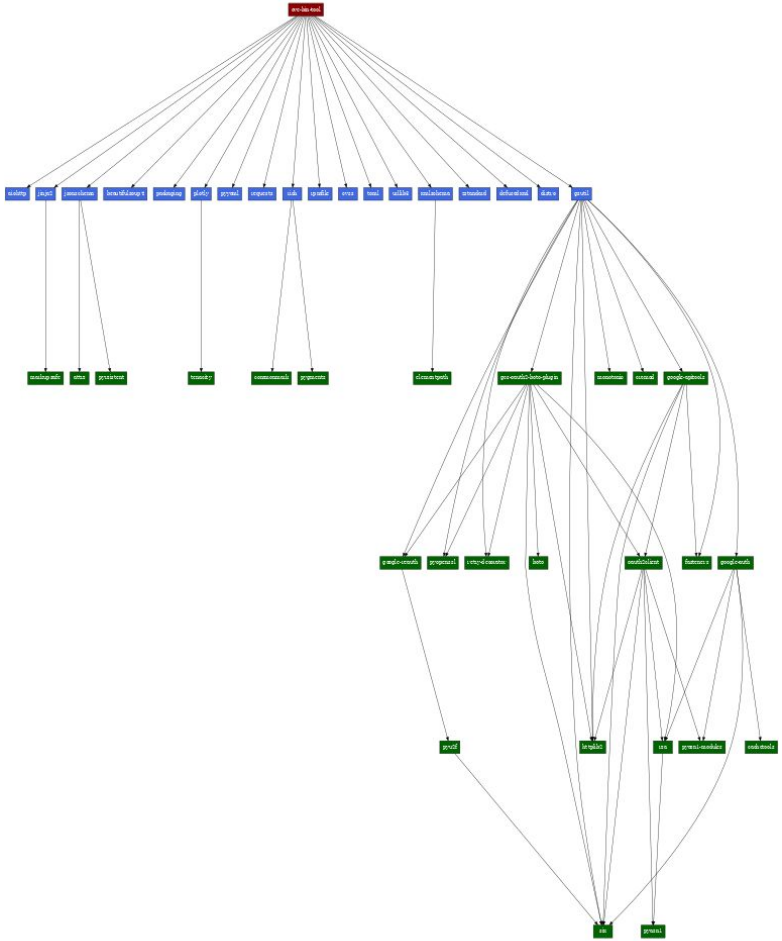
Why do I need to an SBOM?

How do I create an SBOM?

What can I do with an SBOM?

Why do we now need Software Bill of Materials if we haven't needed them in the past?

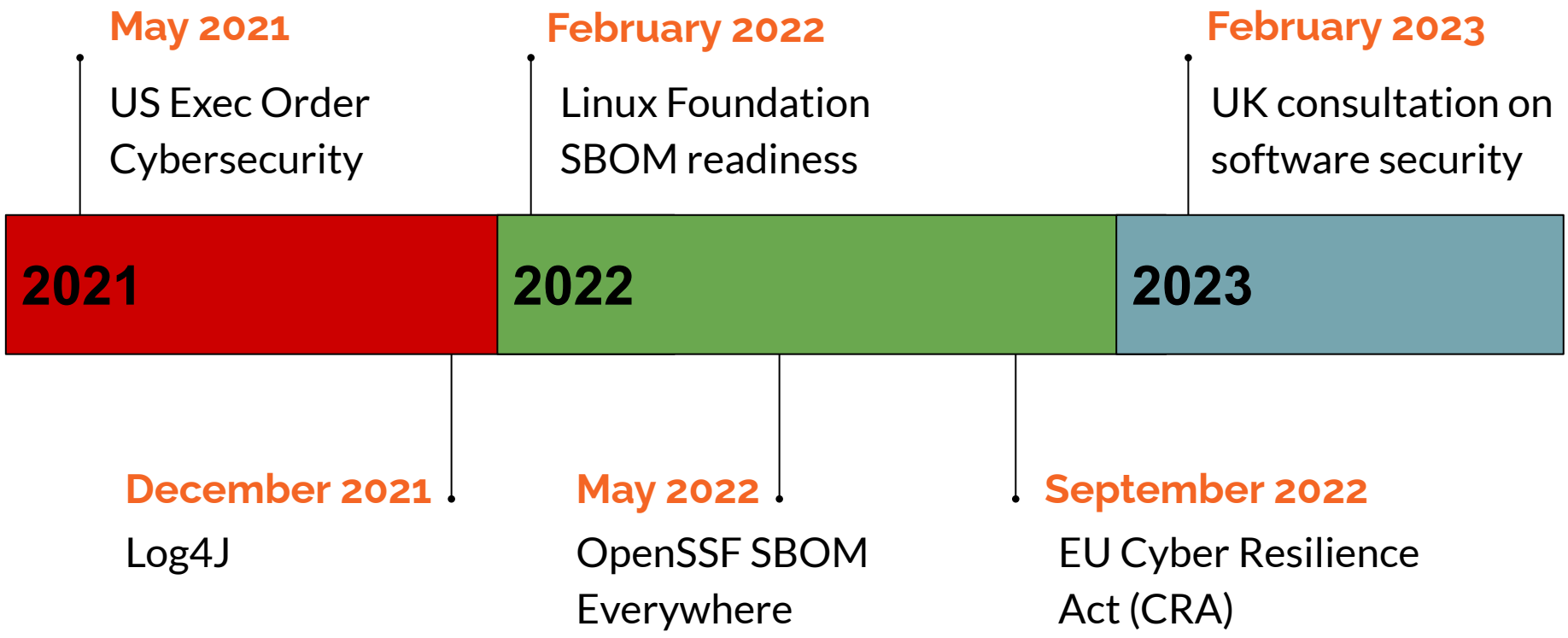
We no longer **understand** how our software is **constructed** or works



A Python application has 18 direct dependencies but requires another 25 packages through transitive dependencies

- A SBOM is a **formal set of machine-readable metadata** describing your software application
- SBOMs are designed to be **shared within and across organizations**
- SBOMs form an important part of a software **risk strategy**

Increasing awareness of SBOMs

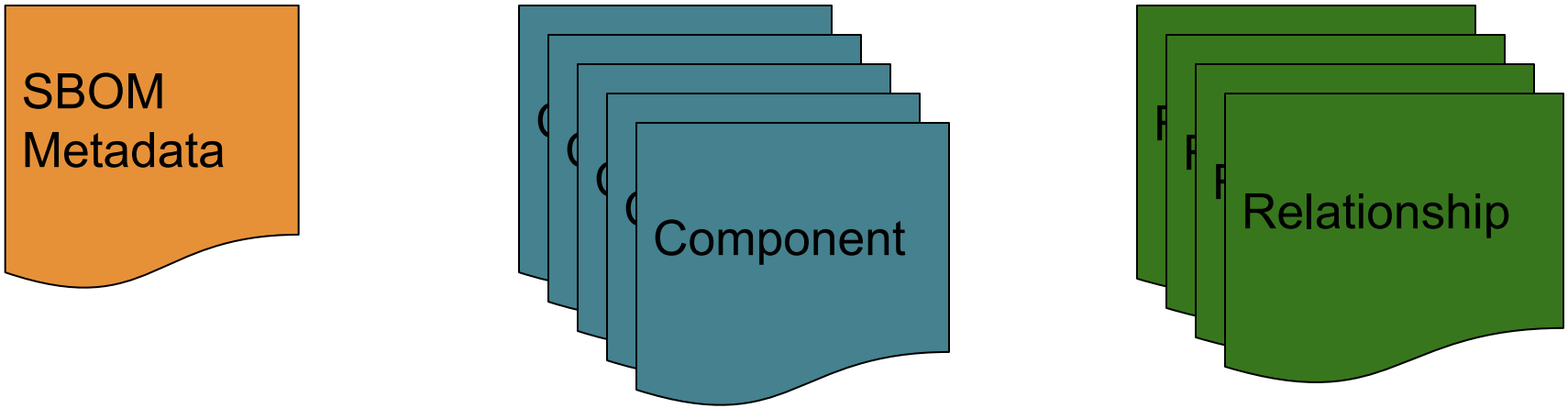


Two primary standards and formats….

https://spdx.org/

https://cyclonedx.org/

SBOM Content

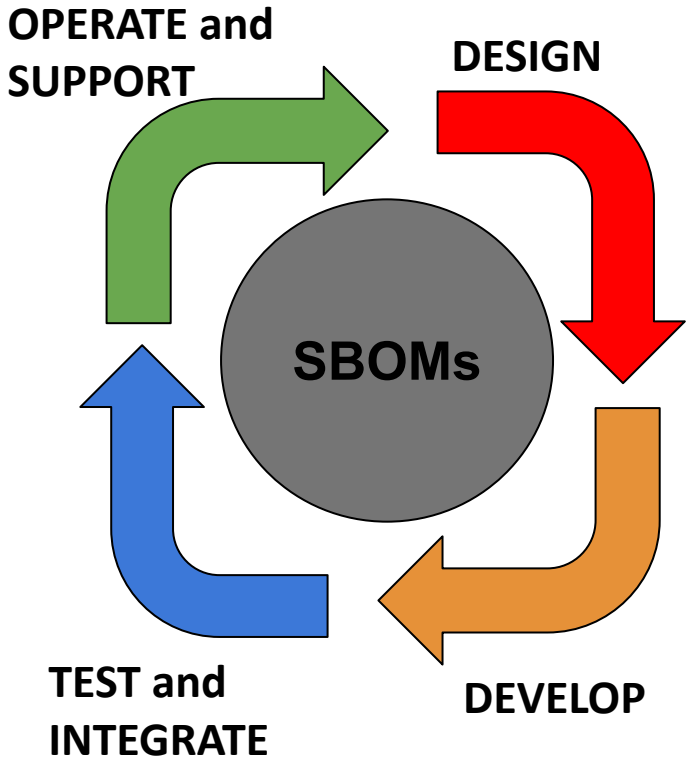


```
PackageName: sbom4files
SPDXID: SPDXRef-Package-1-sbom4files
PackageVersion: 0.2.0
PackageSupplier: Person: Anthony Harrison (antho
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
PackageHomePage: https://github.com/anthonyharri
PackageLicenseConcluded: Apache-2.0
PackageLicenseDeclared: Apache-2.0
PackageCopyrightText: NOASSERTION
PackageSummary: SBOM generator for files in a di
ExternalRef: PACKAGE-MANAGER purl pkg:pypi/sbom4
ExternalRef: SECURITY cpe23Type cpe:2.3:a:anthon
```

Component Metadata

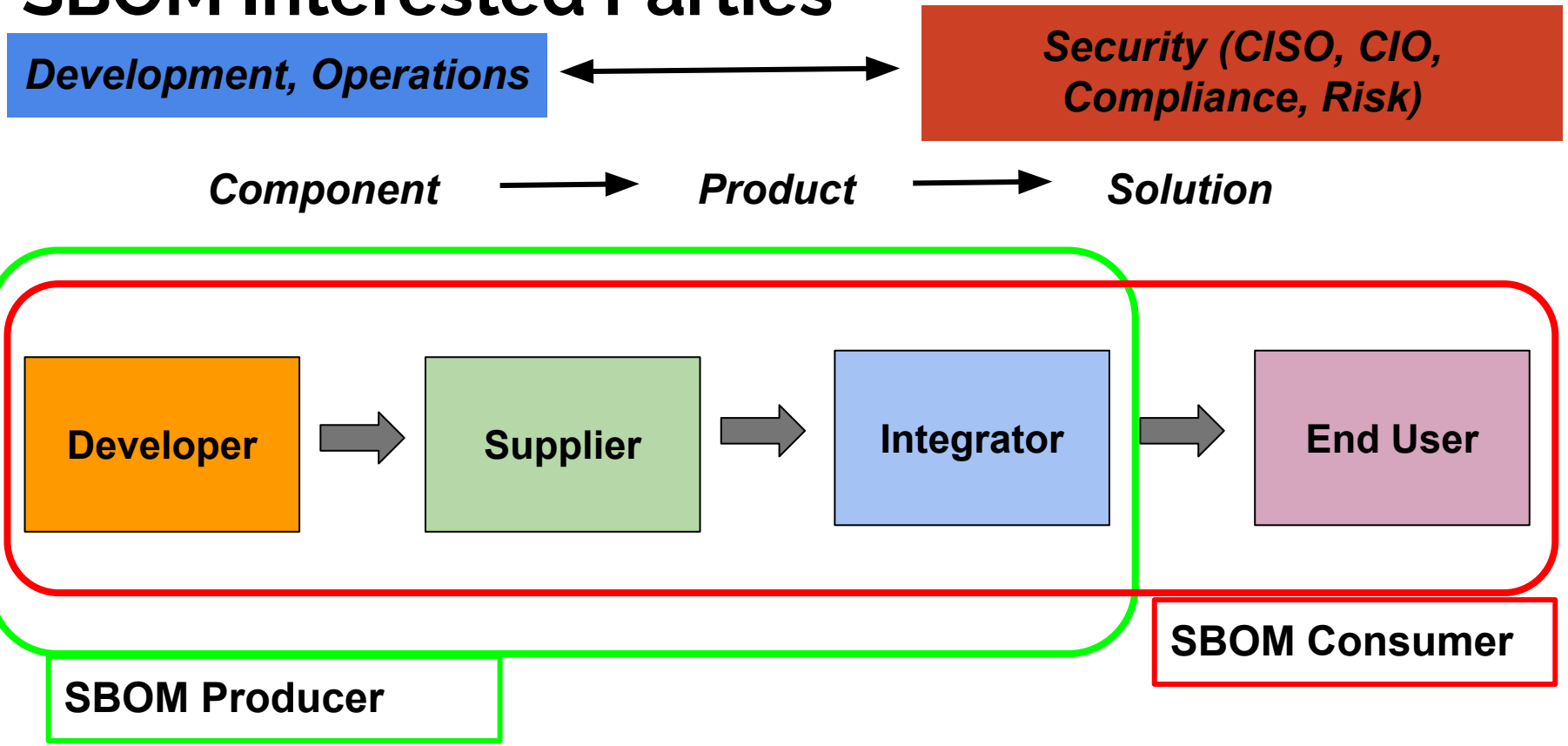
- Component Name
- Component Supplier
- Component Version
- Component License

SBOMs are used throughout the lifecycle



- 3rd party component selection
- Source files in build
- Applications built
- Component dependencies
- Build composition
- Build integrity
- Change Management
- Vulnerability Monitoring
- Obsolete software detection

SBOM Interested Parties



SBOM Tooling

SBOM Creation

sbom4files

sbom4python

distro2sbom

sbom4files

- Licence, copyright information, checksum, type of file

```
FileName: ./sbom4files/cli.py
SPDXID: SPDXRef-File-2-cli
FileChecksum: SHA1: bc045c292bac3175f80e9b2a0101c32cf5ac4792
FileChecksum: SHA256: dac51da8c922e22d8007152e29dd0fafa7fbef90e59e9f06ec1c2c98ff58f138
FileChecksum: SHA512: 225a4c66726a6c6c5185bbb1326e23343dac15530debbae028e45913b4cc66c13cf5f
FileType: SOURCE
FileType: TEXT
LicenseConcluded: Apache-2.0
LicenseInfoInFile: Apache-2.0
LicenseComments: <text>This information was automatically extracted from the file.</text>
FileCopyrightText: (C) 2023 Anthony Harrison
```

sbom4python

- Direct and transitive dependencies, supplier and licences

```
PackageName: sbom4files
SPDXID: SPDXRef-Package-1-sbom4files
PackageVersion: 0.2.0
PackageSupplier: Person: Anthony Harrison (anthony.p.harrison@gmail.com)
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
PackageHomePage: https://github.com/anthonyharrison/sbom4files
PackageLicenseConcluded: Apache-2.0
PackageLicenseDeclared: Apache-2.0
PackageCopyrightText: NOASSERTION
PackageSummary: SBOM generator for files in a directory
ExternalRef: PACKAGE-MANAGER purl pkg:pypi/sbom4files@0.2.0
ExternalRef: SECURITY cpe23Type cpe:2.3:a:anthony_harrison:sbom4files:0.2.0:*:*:*:*:*:*:*
```

distro2sbom

- SBOM for Installed modules (RPMs, Debian, Windows)

```
PackageName: bash
SPDXID: SPDXRef-Package-2-bash
PackageVersion: 5.1.8
PackageSupplier: Organization: AlmaLinux Packaging Team (packager@almalinux.org)
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
PackageHomePage: https://www.gnu.org/software/bash
PackageLicenseConcluded: GPLv3+
PackageLicenseDeclared: GPLv3+
PackageCopyrightText: NOASSERTION
PackageSummary: The GNU Bourne Again shell
```

Lack of consistency of License Metadata

Apache 2.0	
Apache License, Version 2.0	
Apache 2	
Apache	
Apache-2.0	**Valid SPDX License identifier**

Component Naming

- Multiple ways of specifying component name
- CPE (Common Platform Enumeration) e.g. ***cpe:2.3:a:djangoproject:django:3.2.1:*:*:*:*:*:*:****
- PURL (Package URL) e.g. ***pkg:pypi/django@3.2.1***

Supplier

- Where did the component come from?
- Need to distinguish between developer, a distributor or integrator

SBOM Management

sbom-manager

sbomdiff

sbomaudit

Managing SBOMs – Typical Use Cases

- Does my project/product use version X of component Y?
- What version(s) of component Y is being used?
- Is my organisation impacted by a vulnerability with component X?
- What vulnerabilities exist within my product?
- Has anything changed?
- How good is the SBOM?

sbom-manager

- Manage a collection of SBOMs in a number of formats
- Identify the set of components included in a software release.
- Tools to support a number of common use cases.

```
$ sbom-manager --module sudo
SBOM          Project     Description     Product     Version
=============================================================================================
centos.files  Centos      Version 7       sudo        1.8.23
```

```
$ sbom-manager --module log4j
No data found
```

sbomdiff

- Changed license, new (or deleted) components, changed version

```
[REMOVED] ucf: (Version 3.0043)
[VERSION] coreutils: Version changed from 9.1 to 8.32
[LICENSE] coreutils: License changed from NOASSERTION to GPLv3+
[REMOVED] sensible-utils: (Version 0.0.17)
[REMOVED] libxext6: (Version 2)
[VERSION] shared-mime-info: Version changed from 2.2 to 2.1
[LICENSE] shared-mime-info: License changed from NOASSERTION to GPLv2+
[VERSION] libxml2: Version changed from 2.9.14 to 2.9.13
[LICENSE] libxml2: License changed from NOASSERTION to MIT
[REMOVED] libtext-glob-perl: (Version 0.11)
[REMOVED] debianutils: (Version 5.7)
[ADDED  ] bash: (Version 5.1.8)
[ADDED  ] filesystem: (Version 3.16)
[ADDED  ] setup: (Version 2.13.7)
[ADDED  ] python3: (Version 3.9.14)
[ADDED  ] python3-libs: (Version 3.9.14)
```

sbomaudit

- Included SPDX licence, minimum contents, latest version (Python)

```
Package Summary

[x] Allowed Package check for package click
[x] Supplier included for package click
[x] Version included for package click
[x] License included for package click
[x] SPDX Compatible License id included for package click
[ ] Allowed License check for package click: BSD-3-Clause not allowed
[ ] Using latest version of package click: Version is 8.1.2; latest is 8.1.3
[x] NTIA compliant
```

SBOM Governance

cve-bin-tool

sbom2dot

sbom2doc

cve-bin-tool

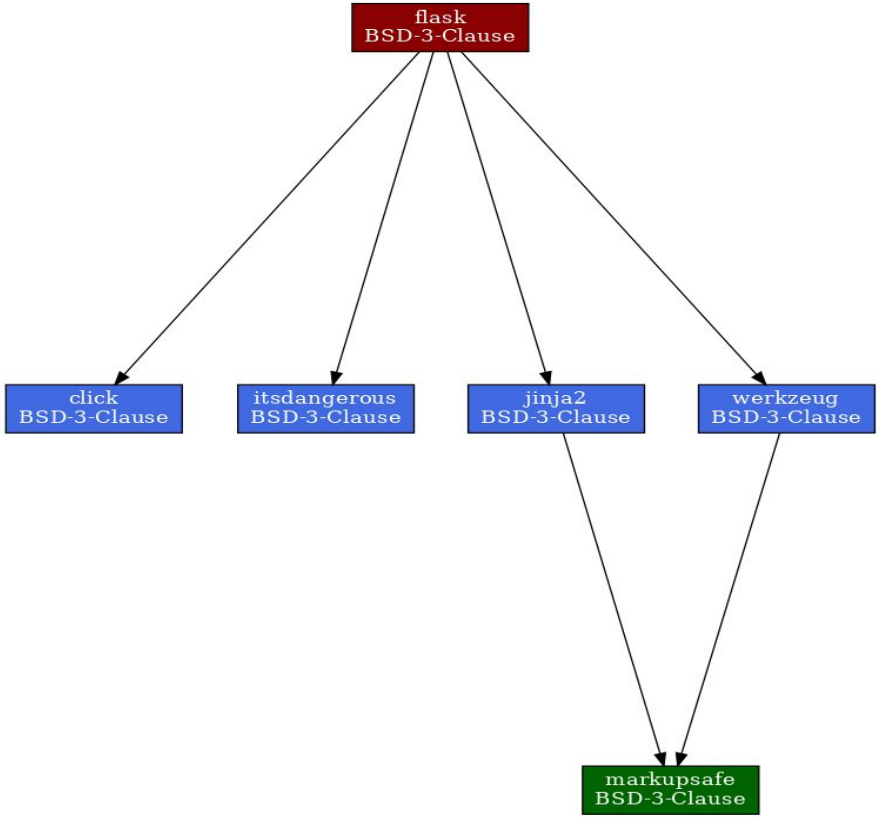
- A binary scanner which helps determine which packages/libraries are vulnerable
- Scans SBOMs for vulnerabilities
- Produces a list of components with reported CVEs and associated severity

sbom2dot

Dependencies

Relationships

Licenses



sbom2doc

PDF

Markdown

Console

SBOM Summary

Item	Details
SBOM File	/tmp/click.json
SBOM Type	cyclonedx
Version	1.4
Name	Python-click
Creator	tool:sbom4python
Created	2023-03-02T11:58:30Z
Files	0
Packages	1
Relationships	1

Package Summary

Name	Version	Supplier	License
click	8.1.2	Armin Ronacher	BSD-3-Clause

License Summary

License	Count
BSD-3-Clause	1

Summary

- SBOMs are becoming a growing and important part of the **software development lifecycle**
- SBOMs provide enhanced **dependency management**
- SBOMs provide a key role to supporting better **risk management**

SBOMs are only as good as the data which is provided. Everyone is responsible for improving this data.

Can you answer these now?

Why do I need to an SBOM?

How do I create an SBOM?

What can I do with an SBOM?

Resources/Links

https://www.linuxfoundation.org/tools/the-state-of-software-bill-of-materials-sbom-and-cybersecurity-readiness/

https://openssf.org/oss-security-mobilization-plan/

https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom

https://github.com/anthonyharrison

https://github.com/intel/cve-bin-tool

https://www.bcs.org/articles-opinion-and-research/manage-risk-with-a-software-bill-of-materials/

Questions?

anthonypharrison

@APH_GB

All Pictures © A.P. Harrison