APH10

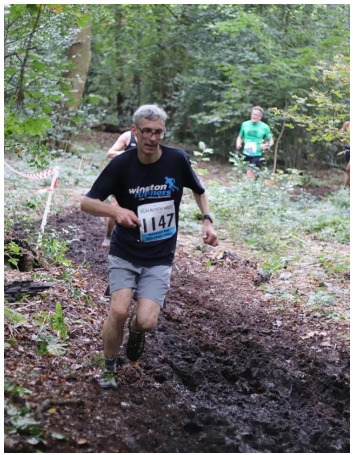
Taming the Supply Chain

September 2024

Anthony Harrison (Founder)
anthony@aph10.com

APH10

- A career delivering mission critical solutions across multiple sectors
- Founder and Director APH10
- Open Source Software
- STEM Ambassador
- Mentor



CoderDojo

A supply chain is a network of companies and people that are involved in the production and delivery of a product or service.

Supply Chain Diagram

Raw Materials → Supplier → Manufacturer → Distributor → Retailer → Consumer

Software Supply Chain

THE APACHE SOFTWARE FOUNDATION

ECLIPSE FOUNDATION

Microsoft

THE LINUX FOUNDATION

aws

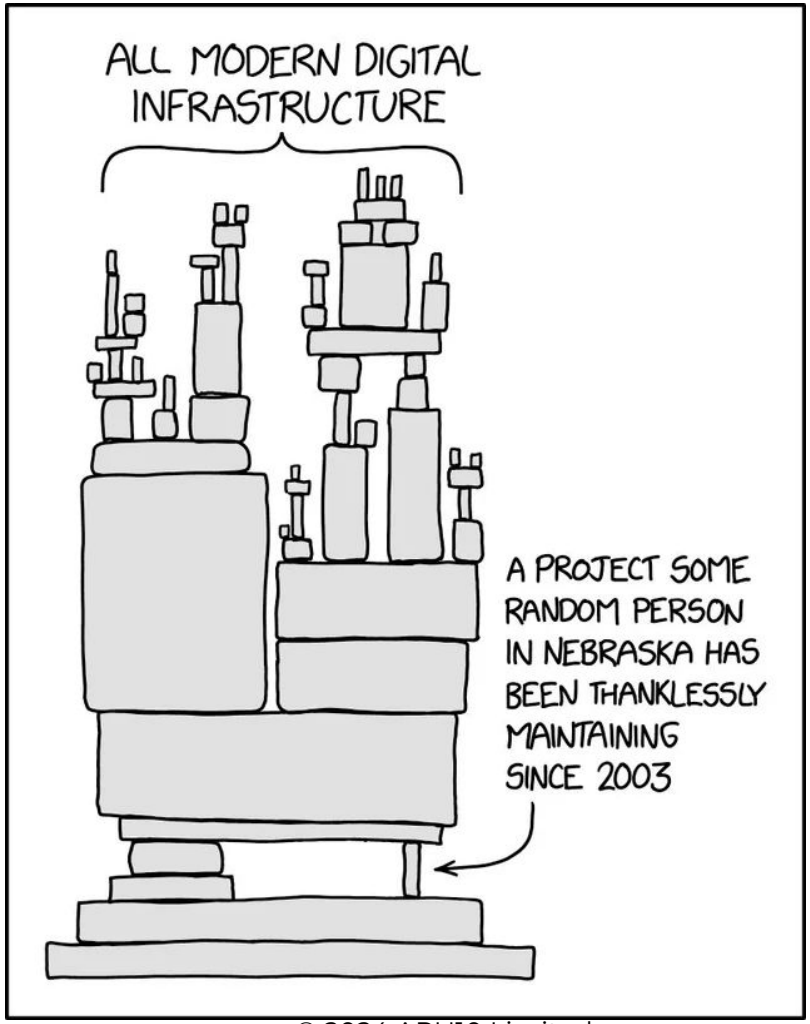
Developer / Foundation / Consolidator -> Integrator -> Customer

How can the supply chain be disrupted?

Traditional Supply Chain	Software Supply Chain

How can the supply chain be disrupted?

Traditional Supply Chain	**Software Supply Chain**
Harvest failure	
Transport disruption	
Strikes	



https://xkcd.com/2347/

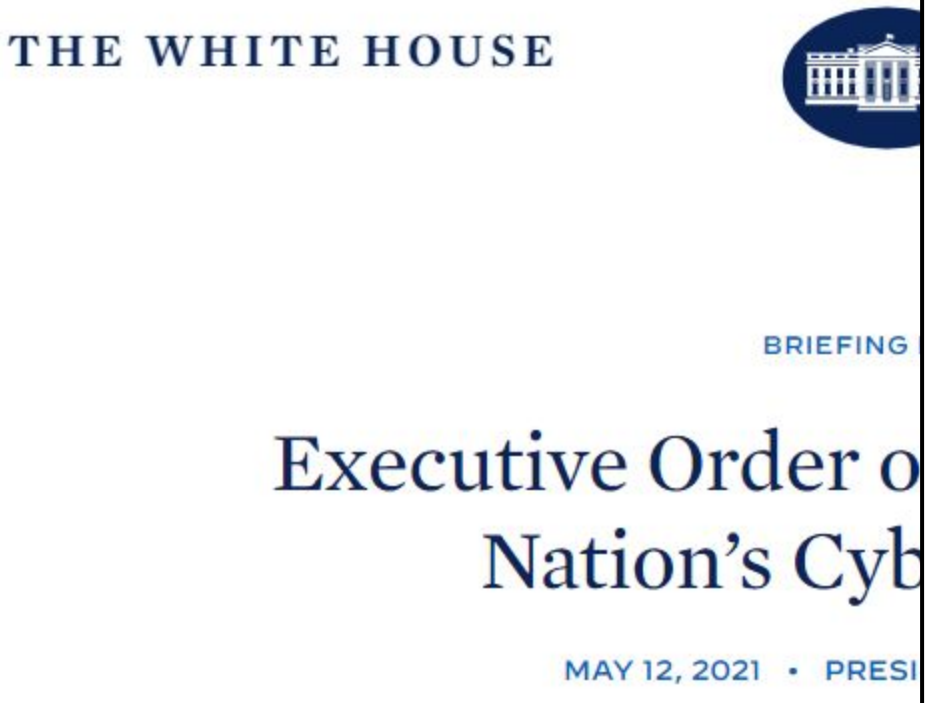
TLP:WHITE

National Institute of Standards and Technology
U.S. Department of Commerce

Defending Against Software Supply Chain Attacks

April 2021

Regulation



- Improve Software Supply Chain Security
  - The EO will improve the security of software by establishing baseline security standards for development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available.
  - It also creates a pilot program to create an "energy star" type of label so the government — and the public at large — can quickly determine whether software was developed securely.

Software Bill of Materials (SBOMs)

APH10

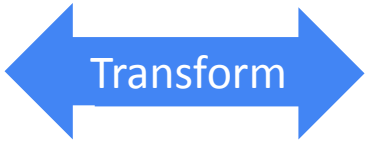
APH10

What is an SBOM?

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

APH10

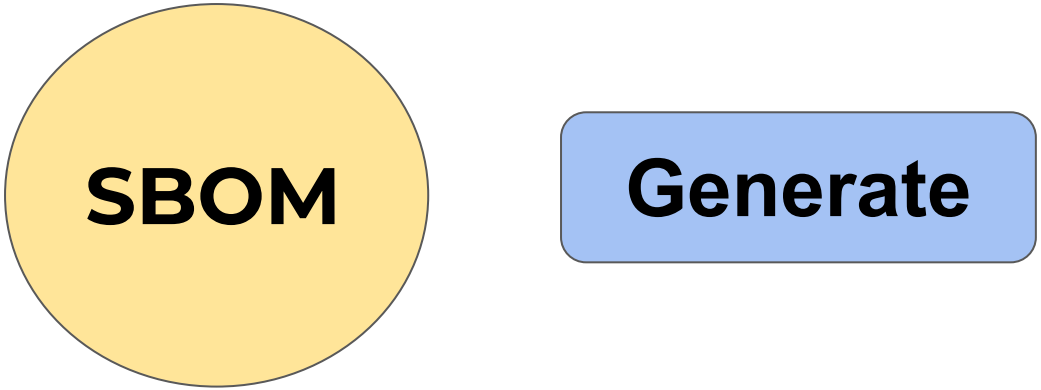
Two primary standards and formats….



https://spdx.org/

https://cyclonedx.org/

SBOM Lifecycle



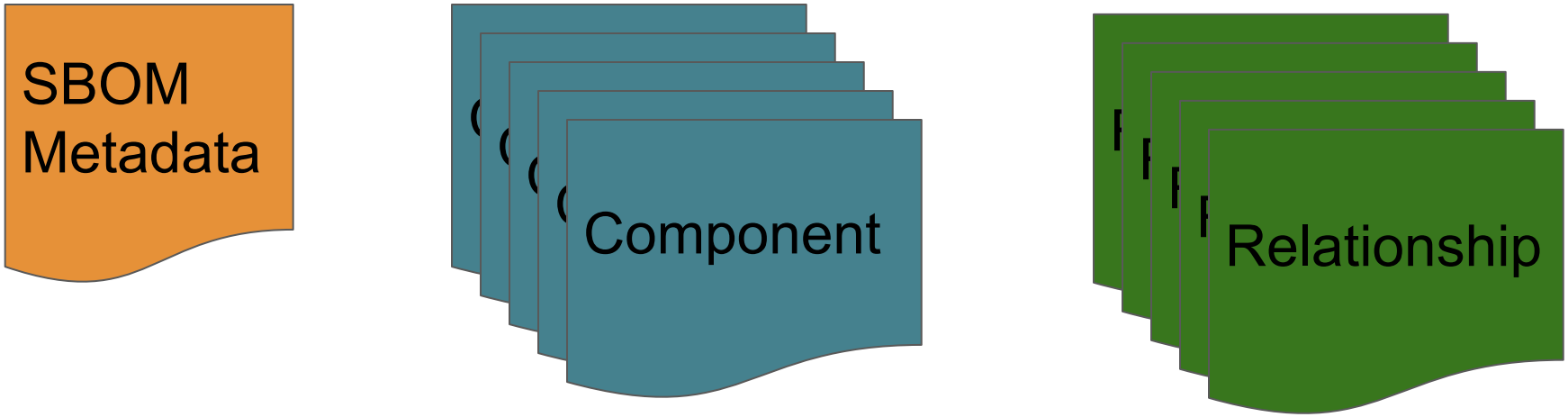
Workshop setup

git clone https://github.com/anthonyharrison/bsideslancs2024.git

cd bsideslancs2024

sh install.sh

SBOM Content



APH10

sbom4files

```
sbom4files [-h] [-d DIRECTORY] [-p PROJECT] [-r] [-i IGNORE] [--debug]
[--sbom {spdx,cyclonedx}] [--format {tag,json,yaml}] [-o OUTPUT_FILE] [-V]

Input:

-d DIRECTORY, --directory DIRECTORY                Directory to be scanned

-p PROJECT, --project PROJECT                      Name of project

-r, --recurse                                      Recurse directories

-i IGNORE, --ignore IGNORE      Comma separated list of extensions to ignore
```

sbom4files

```
sbom4files [-h] [-d DIRECTORY] [-p PROJECT] [-r] [-i IGNORE] [--debug]
[--sbom {spdx,cyclonedx}] [--format {tag,json,yaml}] [-o OUTPUT_FILE] [-V]

Output:

--sbom {spdx,cyclonedx} specify type of sbom to generate (default: spdx)

--format {tag,json,yaml} format for SPDX software bill of materials (sbom)
(default: tag)

-o OUTPUT_FILE, --output-file OUTPUT_FILE output filename (default: output
to stdout)
```

sbom4files

```
sbom4files –directory example1 –project “BSides Test1”
```

METADATA

```
SPDXVersion: SPDX-2.3
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: BSides-Test1
DocumentNamespace: http://spdx.org/spdxdocs/BSides-Test1-90c37dee-a7c9-4788-a9c5-d42bc442ddb2
LicenseListVersion: 3.22
Creator: Tool: sbom4files-0.4.0
Created: 2024-03-18T11:09:57Z
CreatorComment: <text>This document has been automatically generated.</text>
#####
```

https://pypi.org/project/sbom4files/

APH10

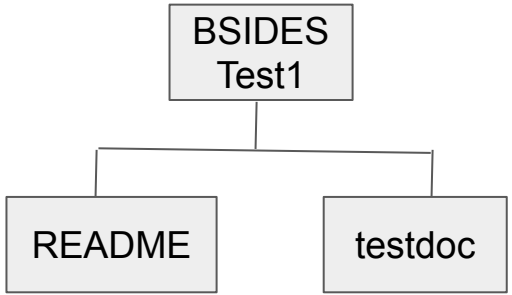
COMPONENTS

```
FileName: ./example1/README.md
SPDXID: SPDXRef-File-1-README
FileChecksum: SHA1: d98c486cc67e3eea0c51a75d0e71863b39069085
FileChecksum: SHA256: 92d7b6709621cd5ba40a2dc0e26a510111b34397638a7454b1f7bfa76b24eeef
FileChecksum: SHA512:
1e7478ce2ed5493a3b3a6f6ee3e07581547eabb7c2e4716c57b79000da09565daa4275f7f70a4bebba521abcf0e
2147994c9f1ed86caec1953098506520cde0a
FileType: DOCUMENTATION
FileType: TEXT
LicenseConcluded: NOASSERTION
LicenseInfoInFile: NONE
LicenseComments: <text>Unable to determine license from the file.</text>
FileCopyrightText: NOASSERTION
#####
```

https://pypi.org/project/sbom4files/

RELATIONSHIPS

```
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Package-BSides-Test1-files
Relationship: SPDXRef-Package-BSides-Test1-files CONTAINS SPDXRef-File-1-README
Relationship: SPDXRef-Package-BSides-Test1-files CONTAINS SPDXRef-File-2-testdoc
```



https://pypi.org/project/sbom4files/

sbom4files

```
sbom4files -directory example1 -project "BSides Test1" -sbom
cyclonedx -format json
```

METADATA


```
"$schema": "http://cyclonedx.org/schema/bom-1.5.schema.json",
 "bomFormat": "CycloneDX",
 "specVersion": "1.5",
 "serialNumber": "urn:uuid:e338186c-ee06-4060-9e51-4e7c7099ddac",
 "version": 1,
 "metadata": {
   "timestamp": "2024-03-18T11:13:55Z",
   "tools": {
     "components": [
       {
         "name": "sbom4files",
         "version": "0.4.0",
         "type": "application"
       }
     ]
   },
   "component": {
     "type": "application",
     "bom-ref": "CDXRef-DOCUMENT",
     "name": "BSides Test1"
   }
 },
```

COMPONENTS


```
      "type": "file",
      "bom-ref": "1-README",
      "name": "example1/README.md",
      "hashes": [
        {
          "alg": "SHA-1",
          "content": "d98c486cc67e3eea0c51a75d0e71863b39069085"
        },
        {
          "alg": "SHA-256",
          "content": "92d7b6709621cd5ba40a2dc0e26a510111b34397638a7454b1f7bfa76b24eeef"
        },
        {
          "alg": "SHA-512",
          "content":
"1e7478ce2ed5493a3b3a6f6ee3e07581547eabb7c2e4716c57b79000da09565daa4275f7f70a4bebba521abcf0e2147994c9f1ed86caec1953098506520cde0a
"
        }
      ],
      "properties": [
        {
          "name": "License Comments",
          "value": "Unable to determine license from the file."
        }
      ]
```

RELATIONSHIPS

```
"dependencies": [
    {
      "ref": "CDXRef-DOCUMENT",
      "dependsOn": [
        "1-BSides-Test1-files"
      ]
    },
    {
      "ref": "BSides-Test1-files",
      "dependsOn": [
        "1-README",
        "2-testdoc"
      ]
    }
  ]
```

sbom4files

```
sbom4files -directory example1 -project "BSides Test1" -sbom
cyclonedx -format json -recurse
```

COMPONENTS

```
"type": "file",
"bom-ref": "7-Java",
"name": "example1/testfiles/Java.java",
"hashes": [
  …
],
"licenses": [
  {
    "license": {
      "id": "Apache-2.0",
      "url": "https://www.apache.org/licenses/LICENSE-2.0"
    }
  }
],
"copyright": "(C) 2024 Anthony Harrison",
"properties": [
  {
    "name": "License Comments",
    "value": "This information was automatically extracted from the file."
  },
  {
    "name": "Comment",
    "value": "Source is Java"
  }
]
```

sbom4python

```
sbom4python [-h] [-m MODULE] [-r REQUIREMENT] [--system] [--exclude-license]
[--include-file] [--include-service] [-d] [--sbom {spdx,cyclonedx}]
[--format {tag,json,yaml}] [-o OUTPUT_FILE] [-g GRAPH] [-V]

Input:

-m MODULE, --module MODULE    identity of python module

-r REQUIREMENT, --requirement REQUIREMENT    name of requirements.txt file

--exclude-license             suppress detecting the license of components

--include-file                include reporting files associated with module
```

sbom4python

```
sbom4python [-h] [-m MODULE] [-r REQUIREMENT] [--system] [--exclude-license]
[--include-file] [--include-service] [-d] [--sbom {spdx,cyclonedx}]
[--format {tag,json,yaml}] [-o OUTPUT_FILE] [-g GRAPH] [-V]

Output:

--sbom {spdx,cyclonedx} specify type of sbom to generate (default: spdx)

--format {tag,json,yaml} format for SPDX software bill of materials (sbom)
(default: tag)

-o OUTPUT_FILE, --output-file OUTPUT_FILE output filename (default: output
to stdout)

 -g GRAPH, --graph GRAPH     filename for dependency graph
```

APH10

sbom4python

```
sbom4python —requirement requirements.txt
```

```
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-1-lib4package
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-2-lib4sbom
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-3-sbom2dot
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-4-sbom4files
```

https://pypi.org/project/sbom4python/

sbom4python

```
sbom4python –module sbom4python
```

```
PackageName: sbom4files
SPDXID: SPDXRef-13-sbom4files
PackageVersion: 0.4.4
PrimaryPackagePurpose: LIBRARY
PackageSupplier: Person: Anthony Harrison (anthony.p.harrison@gmail.com)
PackageDownloadLocation: https://pypi.org/project/sbom4files/0.4.4/#files
FilesAnalyzed: false
PackageHomePage: https://github.com/anthonyharrison/sbom4files
PackageLicenseDeclared: Apache-2.0
PackageLicenseConcluded: Apache-2.0
PackageCopyrightText: NOASSERTION
PackageSummary: <text>SBOM generator for files in a directory</text>
ExternalRef: PACKAGE_MANAGER purl pkg:pypi/sbom4files@0.4.4
ExternalRef: SECURITY cpe23Type
cpe:2.3:a:anthony_harrison:sbom4files:0.4.4:*:*:*:*:*:*:*
#####
```

https://pypi.org/project/sbom4python/

APH10

```
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Package-1-sbom4python
Relationship: SPDXRef-Package-1-sbom4python DEPENDS_ON SPDXRef-Package-12-sbom2dot
Relationship: SPDXRef-Package-1-sbom4python DEPENDS_ON SPDXRef-Package-13-sbom4files
Relationship: SPDXRef-Package-1-sbom4python DEPENDS_ON SPDXRef-Package-2-lib4package
Relationship: SPDXRef-Package-1-sbom4python DEPENDS_ON SPDXRef-Package-8-lib4sbom
Relationship: SPDXRef-Package-12-sbom2dot DEPENDS_ON SPDXRef-Package-8-lib4sbom
Relationship: SPDXRef-Package-13-sbom4files DEPENDS_ON SPDXRef-Package-14-python-magic
Relationship: SPDXRef-Package-13-sbom4files DEPENDS_ON SPDXRef-Package-8-lib4sbom
Relationship: SPDXRef-Package-2-lib4package DEPENDS_ON SPDXRef-Package-3-requests
Relationship: SPDXRef-Package-3-requests DEPENDS_ON SPDXRef-Package-4-certifi
Relationship: SPDXRef-Package-3-requests DEPENDS_ON SPDXRef-Package-5-charset-normalizer
Relationship: SPDXRef-Package-3-requests DEPENDS_ON SPDXRef-Package-6-idna
Relationship: SPDXRef-Package-3-requests DEPENDS_ON SPDXRef-Package-7-urllib3
Relationship: SPDXRef-Package-8-lib4sbom DEPENDS_ON SPDXRef-Package-10-pyyaml
Relationship: SPDXRef-Package-8-lib4sbom DEPENDS_ON SPDXRef-Package-11-semantic-version
Relationship: SPDXRef-Package-8-lib4sbom DEPENDS_ON SPDXRef-Package-9-defusedxml
```

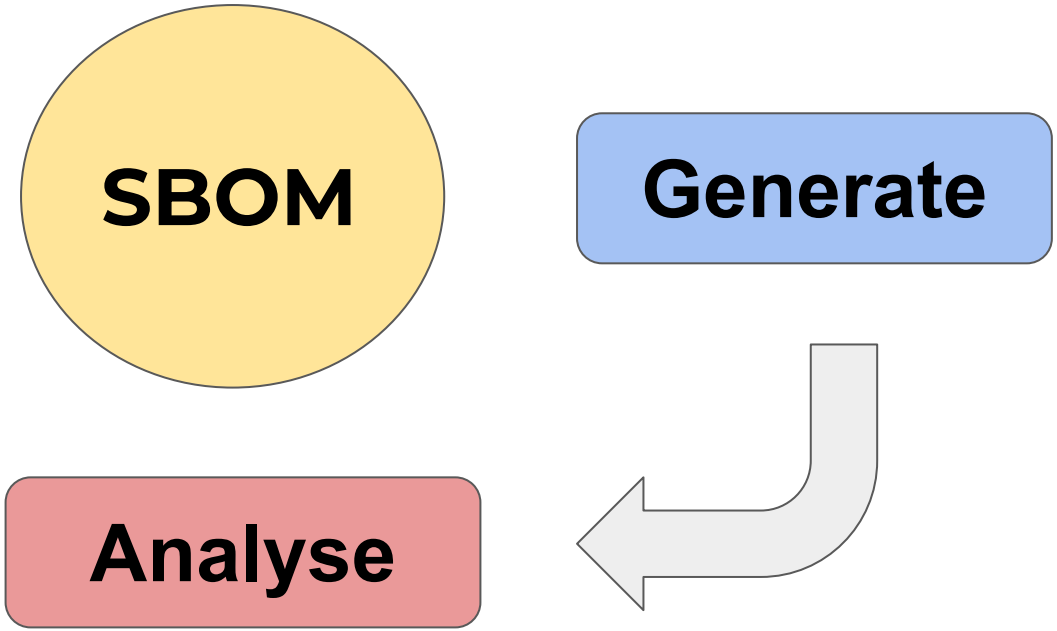
https://pypi.org/project/sbom4python/

APH10

sbom4python

```
sbom4python –module sbom4python –include-file
```

SBOM Lifecycle



What can go wrong with the software supply chain?

What can go wrong with the software supply chain?

- Vulnerable component
- Out of date component
- Using unmaintained package
- Insufficient information provided (e.g. licence)
- Violation of development policy
- SBOM quality fails to met standards

sbomaudit

```
usage: sbomaudit [-h] [-i INPUT_FILE] [--offline] [--cpecheck] [--purlcheck]
[--disable-license-check] [--age AGE] [--maxage MAXAGE] [--allow ALLOW]
[--deny DENY] [--verbose] [--debug] [-o OUTPUT_FILE] [-V]

Input:

  -i INPUT_FILE, --input-file INPUT_FILE            Name of SBOM file

  --cpecheck             check for CPE specification

  --purlcheck            check for PURL specification

  --disable-license-check disable check for SPDX License identifier
```

sbomaudit

```
usage: sbomaudit [-h] [-i INPUT_FILE] [--offline] [--cpecheck] [--purlcheck]
[--disable-license-check] [--age AGE] [--maxage MAXAGE] [--allow ALLOW]
[--deny DENY] [--verbose] [--debug] [-o OUTPUT_FILE] [-V]

Input:

  --age AGE             minimum age of package (as integer representing
days) to report (default: 0)

  --maxage MAXAGE       maximum age of package (as integer representing
years) to report (default: 2)

  --allow ALLOW         Name of allow list file

  --deny DENY           Name of deny list file
```

sbomaudit

```
sbomaudit  -i example2/sboms/sbom1.spdx
```

```
┌─────────────────┐
| Package Summary |
└─────────────────┘
[ ] License included for package python-dateutil: MISSING
[ ] License included for package urllib3: MISSING
[ ] Using latest version of package colorama: Version is 0.4.4; latest is 0.4.6
[ ] Using old version of package colorama: Age of release is 1252 days
[ ] License included for package docutils: MISSING
[ ] Using latest version of package docutils: Version is 0.16; latest is 0.20.1
[ ] Using old version of package docutils: Age of release is 1527 days
[ ] Using latest version of package rsa: Version is 4.7.2; latest is 4.9
[ ] Using old version of package rsa: Age of release is 1118 days
```

https://pypi.org/project/sbomaudit/

APH10

Dependency Pining

Strategy	Pros	Cons
Fixed versions		
Dynamic version		

Dependency Pining

Strategy	Pros	Cons
Fixed versions	Stable known baseline Predictability	Defects not resolved Less portable
Dynamic version	Defects resolved	Unknown baseline Rogue package deployment Dependency Hell

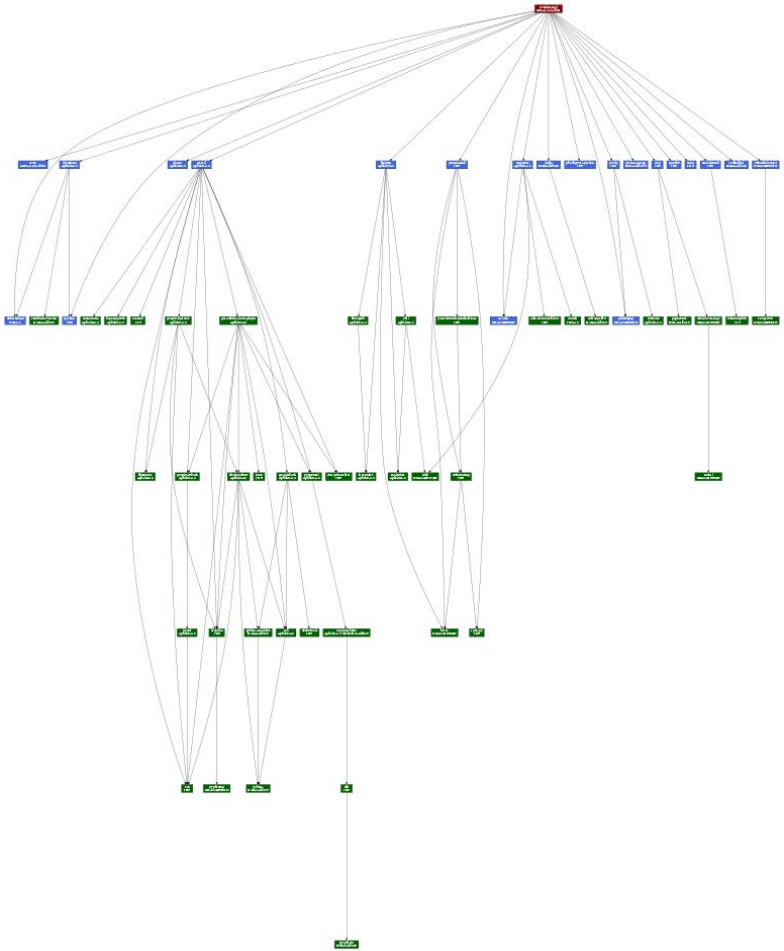
Dependencies

- Dependencies are software constraints - what the software needs to execute
  - Direct components **explicitly** used by the software
  - Transitive components **implicitly** required by other dependencies
- Typically 2 to 10 transitive dependencies for each direct dependency
  - Programming language dependent
- Multiple ways of specifying dependency
  - Can optionally include version of dependency
  - Explicit version numbers v. open (not specified) version numbers
- Conflicting dependencies

Direct dependencies

```
aiohttp[speedups]>=3.7.4
beautifulsoup4==4.1.2
cvss
defusedxml
distro
gsutil
importlib_metadata>=3.6; python_version < "3.10"
importlib_resources; python_version < "3.9"
```

APH10



sbomaudit

```
sbomaudit  -i example2/sboms/sbom1.spdx -deny
example2/policy/project.conf
```

```
[ ] License included for package python-dateutil: MISSING
[ ] Denied License check for package python-dateutil: NOASSERTION not allowed
[ ] Denied Package check for package six: six not allowed
[ ] License included for package urllib3: MISSING
[ ] Denied License check for package urllib3: NOASSERTION not allowed
[ ] Using latest version of package colorama: Version is 0.4.4; latest is 0.4.6
[ ] Using old version of package colorama: Age of release is 1252 days
[ ] License included for package docutils: MISSING
[ ] Denied License check for package docutils: NOASSERTION not allowed
[ ] Using latest version of package docutils: Version is 0.16; latest is 0.20.1
[ ] Using old version of package docutils: Age of release is 1527 days
[ ] Denied Package check for package rsa: rsa not allowed
[ ] Using latest version of package rsa: Version is 4.7.2; latest is 4.9
[ ] Using old version of package rsa: Age of release is 1118 days
```

https://pypi.org/project/sbomaudit/

APH10

Change Happens….

sbomdiff

```
usage: sbomdiff [-h] [--sbom {auto,spdx,cyclonedx}] [--exclude-license] [-d]
[-o OUTPUT_FILE] [-f {text,json,yaml}] [-V] FILE1 FILE2

SBOMDiff compares two Software Bill of Materials and reports the
differences.

positional arguments:

  FILE1                 first SBOM file

  FILE2                 second SBOM file
```

sbomdiff

```
sbomdiff  example2/sboms/sbom1.spdx
example2/sboms/sbom2.json
```

```
[LICENSE] python-dateutil: License changed from NOASSERTION to NOT FOUND
[LICENSE] urllib3: License changed from NOASSERTION to NOT FOUND
[LICENSE] docutils: License changed from NOASSERTION to NOT FOUND
[VERSION] rsa: Version changed from 4.7.2 to 4.9

Summary
-------
Version changes:  1
License changes:  3
Removed packages: 0
New packages:     0
```

https://pypi.org/project/sbomdiff/

APH10

sbom2doc

```
usage: sbom2doc [-h] [-i INPUT_FILE] [--debug] [--include-license] [-f
{console,excel,json,markdown,pdf}] [-o OUTPUT_FILE] [-V]

Input:

  -i INPUT_FILE, --input-file INPUT_FILE            Name of SBOM file

Output:

--debug               add debug information

--include-license     add license text

-f {console,excel,json,markdown,pdf}, --format {console,excel,json,markdown,pdf}

-o OUTPUT_FILE, --output-file OUTPUT_FILE
```

APH10

sbom2doc

```
sbom2doc -i example2/sboms/sbom1.spdx
```

SBOM Summary

Item	Details
SBOM File	example2/sboms/sbom1.spdx
SBOM Type	spdx
Version	SPDX-2.3
Name	Python-awscli
Creator	Tool:sbom4python-0.10.3
Created	2024-03-18T14:58:32Z
Files	0
Packages	12
Relationships	13

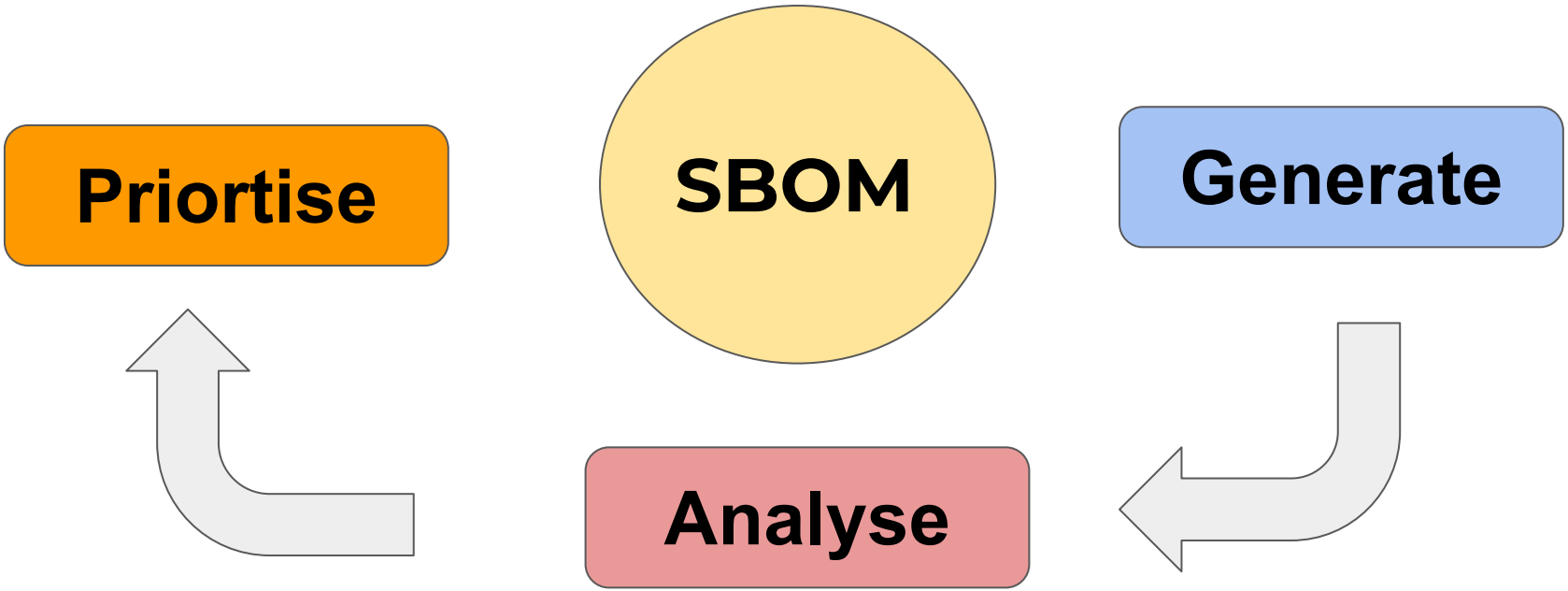
Package Summary

Name	Version	Type	Supplier	License
awscli	1.32.64	APPLICATION	Amazon Web Services	Apache-2.0
botocore	1.34.64	LIBRARY	Amazon Web Services	Apache-2.0
jmespath	1.0.1	LIBRARY	James Saryerwinnie (js@jamesls.com)	MIT
python-dateutil	2.9.0.post0	LIBRARY	Gustavo Niemeyer (gustavo@niemeyer.net)	NOASSERTION
six	1.16.0	LIBRARY	Benjamin Peterson (benjamin@python.org)	MIT
urllib3	2.2.1	LIBRARY	Andrey Petrov (andrey.petrov@shazow.net)	NOASSERTION
colorama	0.4.4	LIBRARY	Jonathan Hartley (tartley@tartley.com)	BSD-3-Clause
docutils	0.16	LIBRARY	David Goodger (goodger@python.org)	NOASSERTION
pyyaml	6.0.1	LIBRARY	Kirill Simonov (xi@resolvent.net)	MIT
rsa	4.7.2	LIBRARY	Sybren A. Stuvel (sybren@stuvel.eu)	Apache-2.0
pyasn1	0.5.1	LIBRARY	Ilya Etingof (etingof@gmail.com)	BSD-2-Clause
s3transfer	0.10.1	LIBRARY	Amazon Web Services (kyknapp1@gmail.com)	Apache-2.0

https://pypi.org/project/sbom2doc/

APH10

SBOM Lifecycle



Data Sources
- NVD, OSV

Scoring
- CVSS, EPSS

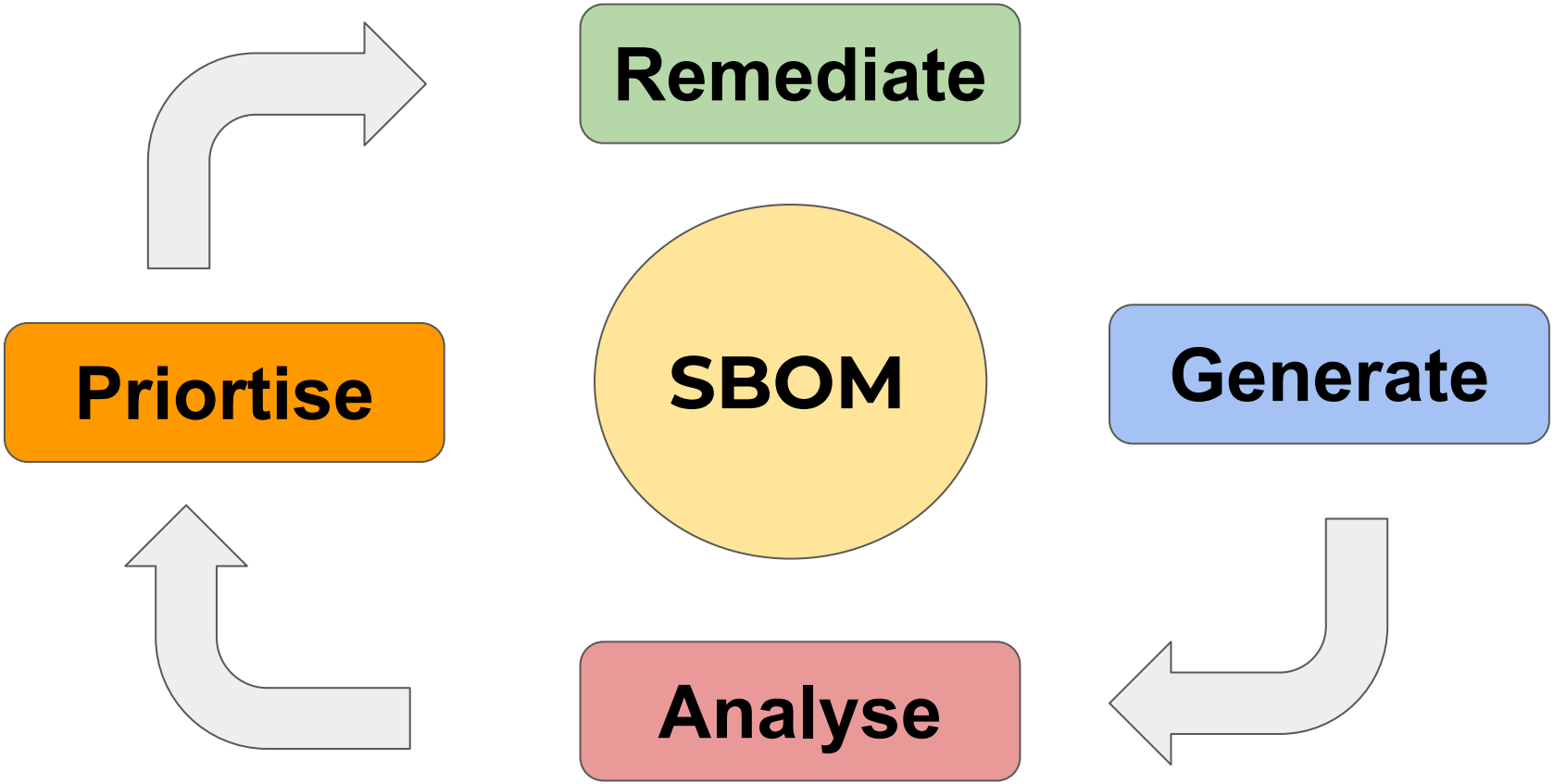
Known Exploits
- KEV

Vulnerabilities
- VDR, VEX, CSAF

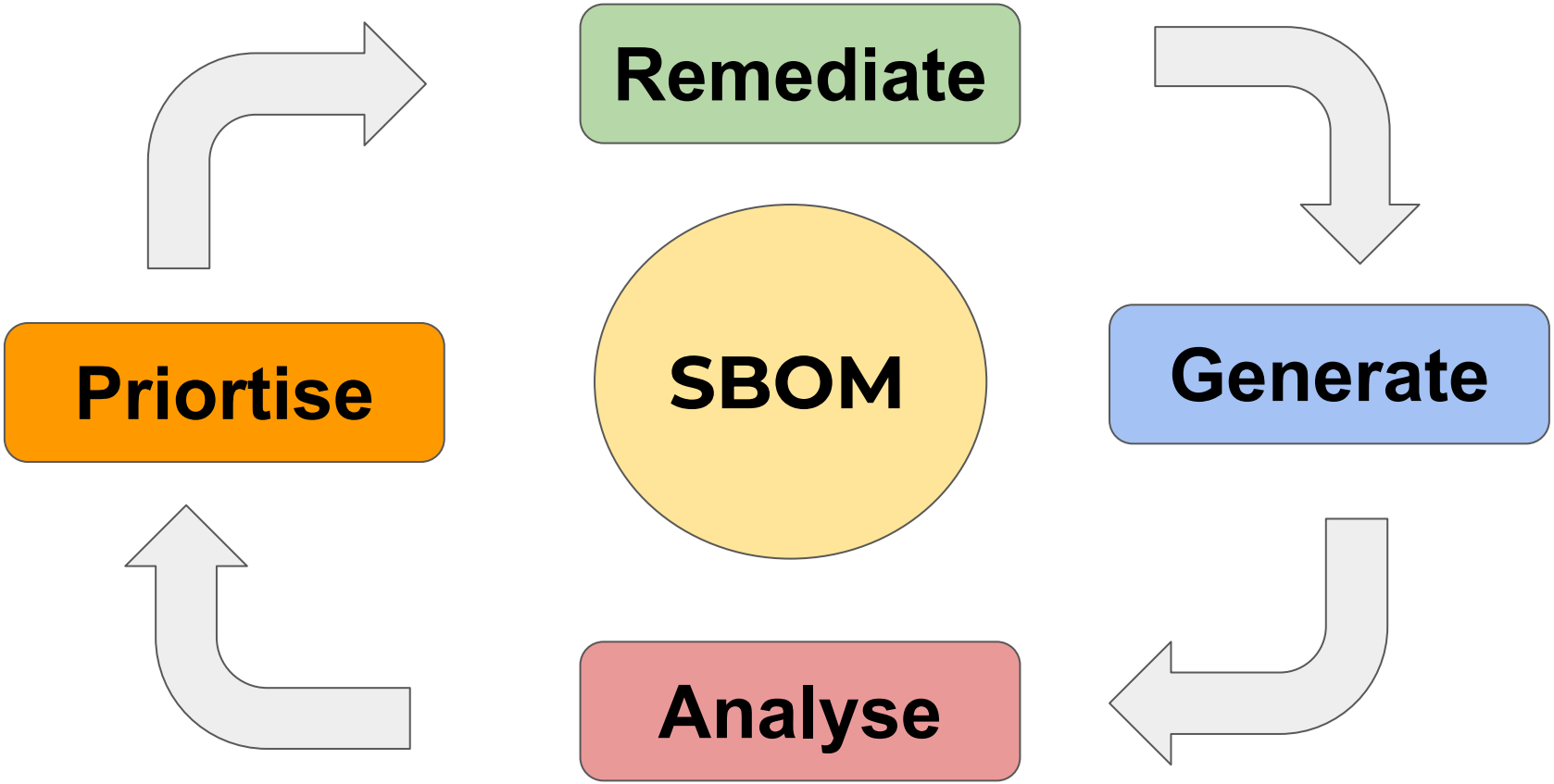
https://dependencytrack.org/

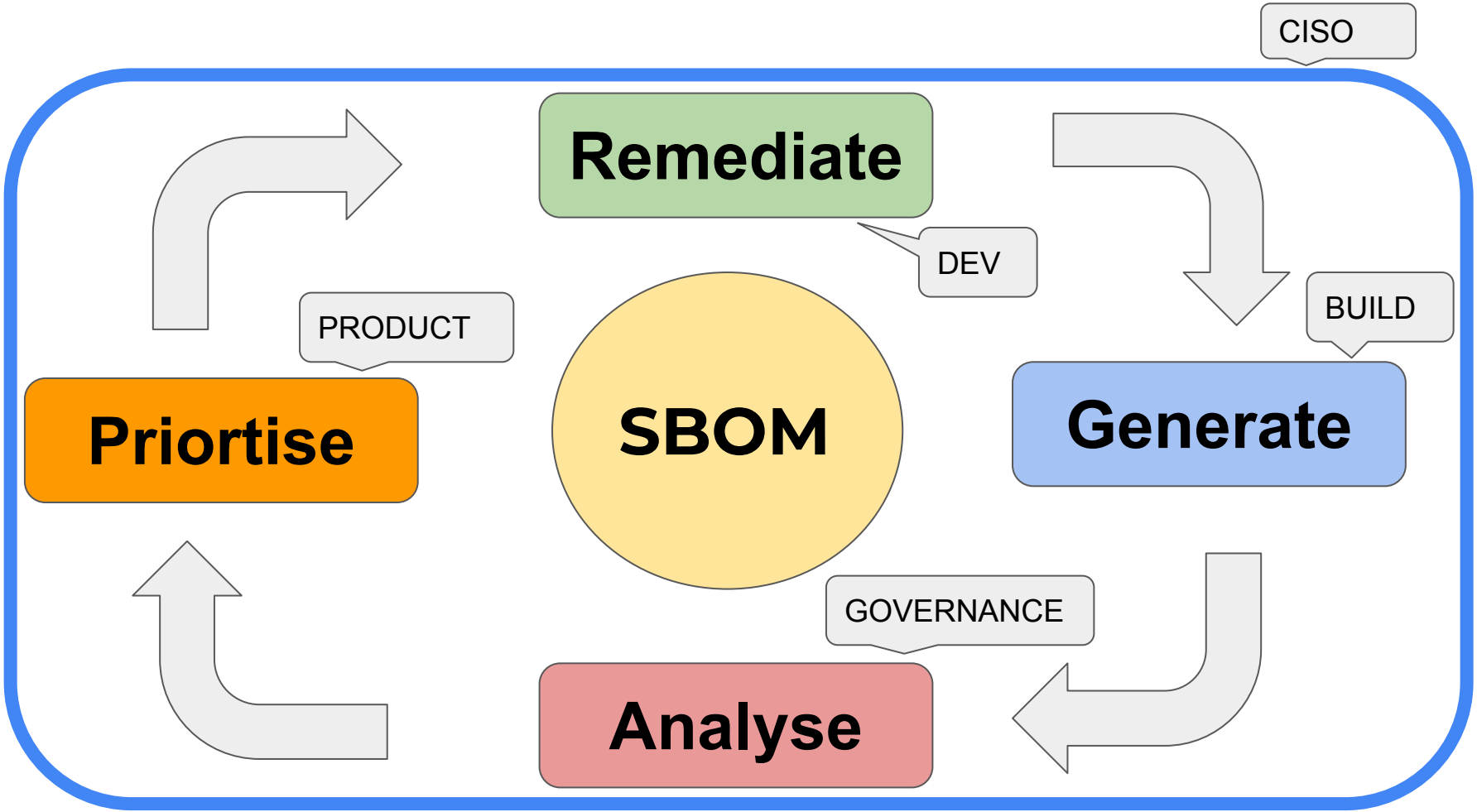
APH10

SBOM Lifecycle

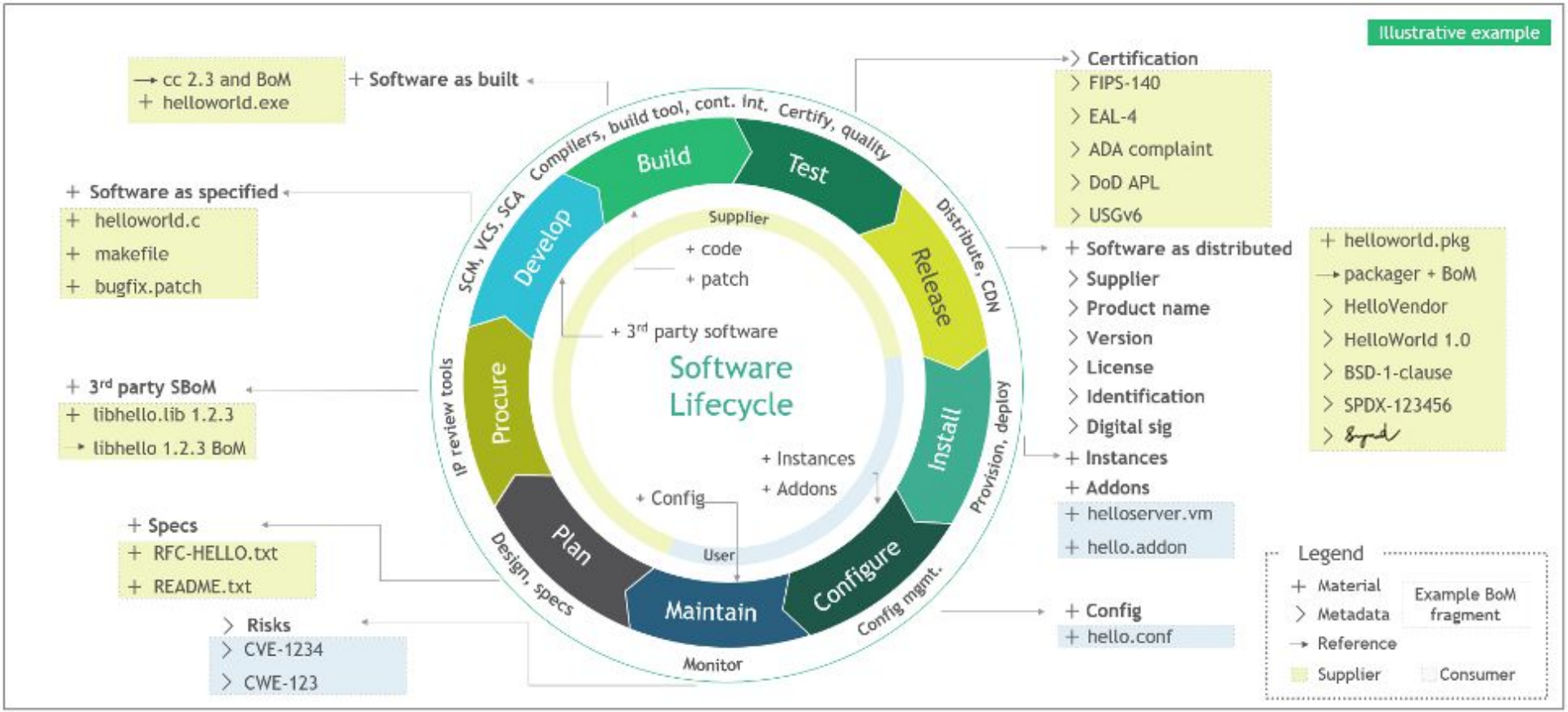


SBOM Lifecycle





Software lifecycle

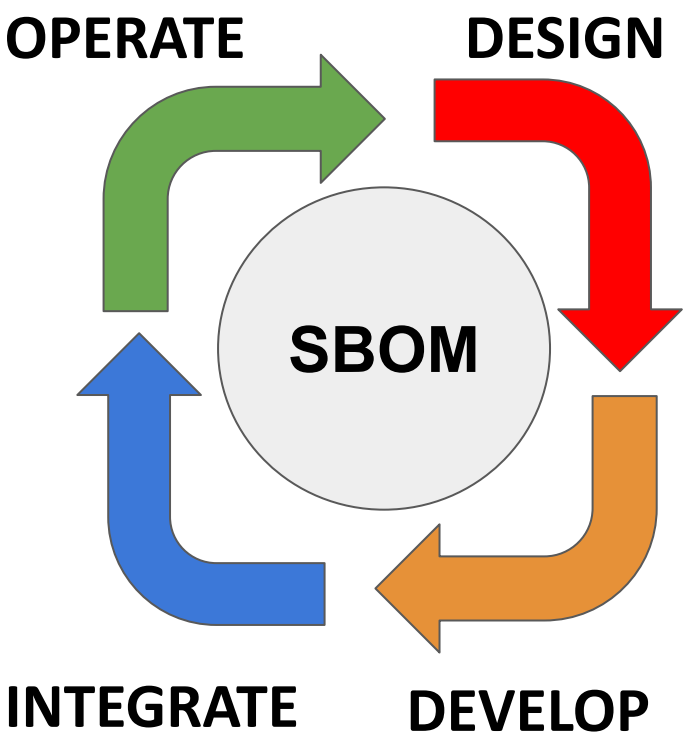


https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1

SBOM Types

- Design
  - Represents the software to be produced
- Source
  - Created from source repository. Often produced as part of SCA tool chain
- Build
  - Represents a releasable product resulting from a build process (e.g. an executable)
- Analysed
  - Represents a set of products e.g., executables, packages, containers, and virtual machine images after a build
- Deployed
  - Represents an inventory of all artefacts installed onto a system
- Runtime
  - Identifies the components executing within a system

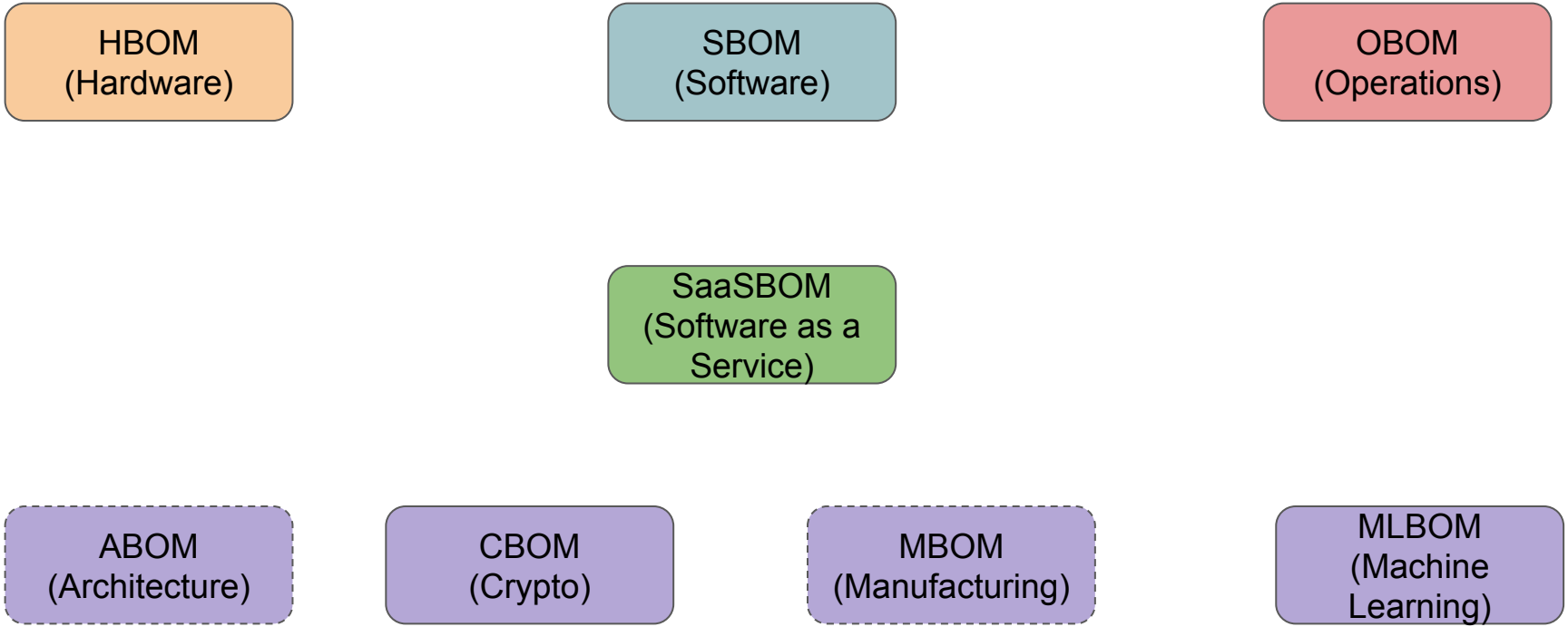
SBOMs are used throughout the lifecycle



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

APH10

SBOMs in the wider context



APH10

National Cyber Security Centre

ABOUT NCSC | CISP | REPORT AN INCIDENT | CONTACT US

Home | Information for... | Advice & guidance | Education & skills | Products & services | News, blogs, events...

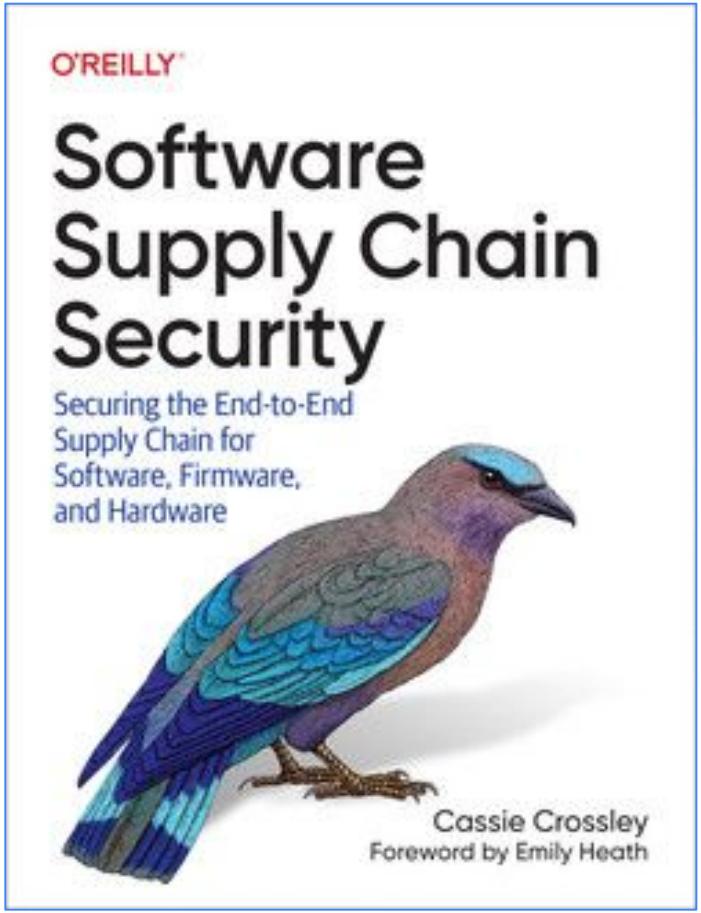
GUIDANCE

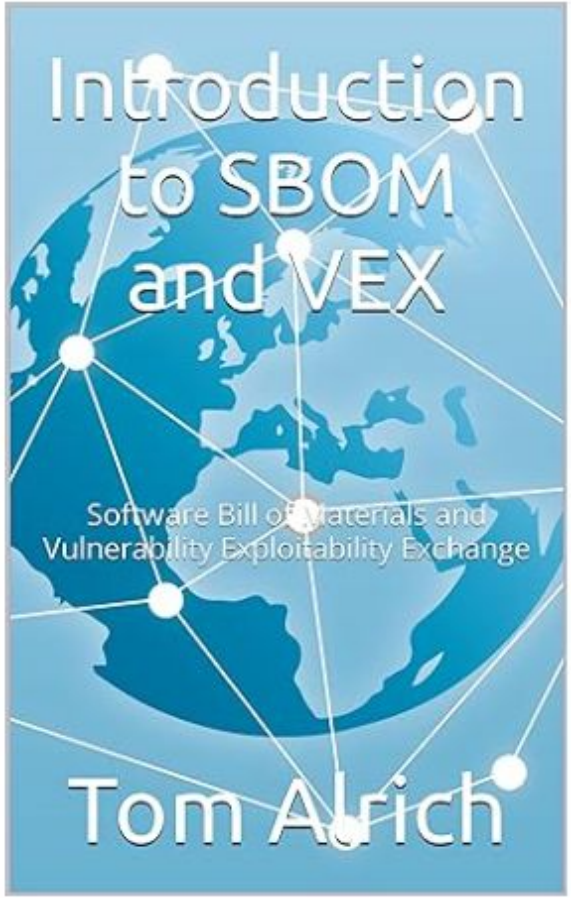
Supply chain security guidance

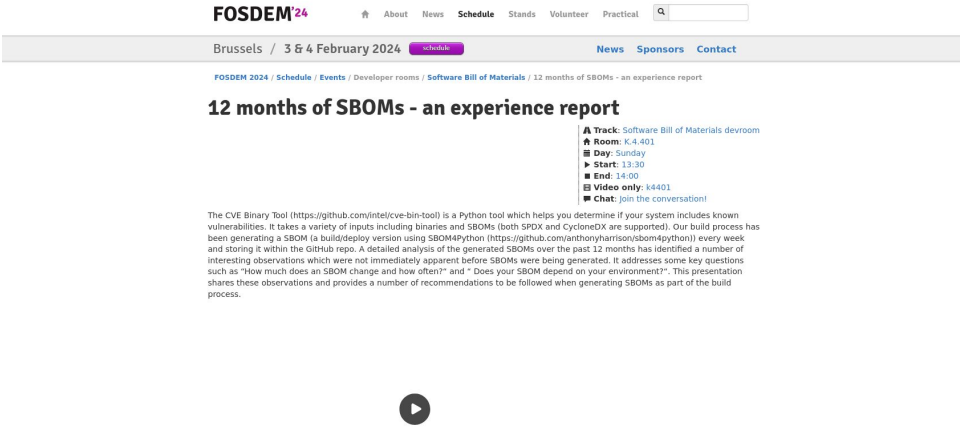
Proposing a series of 12 principles, designed to help you establish effective control and oversight of your supply chain.

Pages

PAGE 1 OF 14







https://www.youtube.com/watch?v=WrUVKqKaq1Y

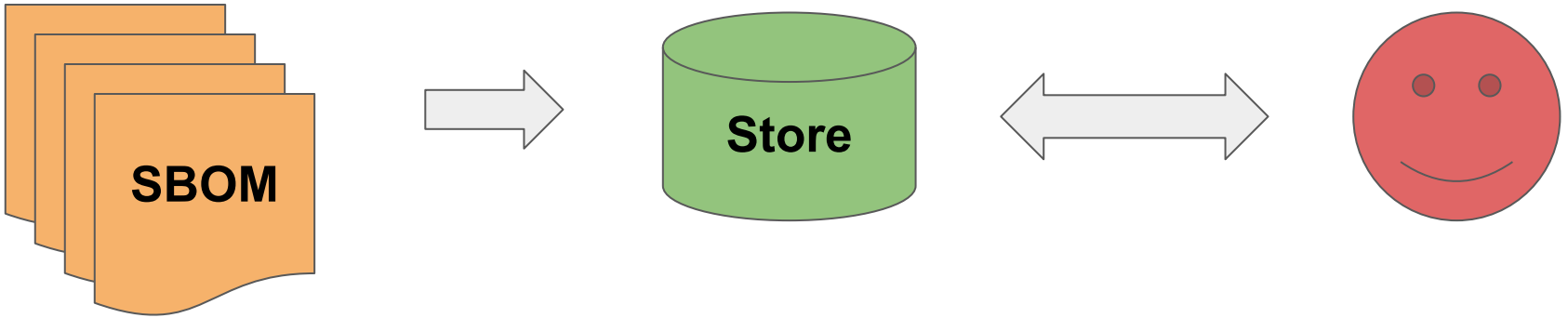
https://fosdem.org/2024/schedule/event/fosdem-2024-1896-12-months-of-sboms-an-experience-report/

GitHub

LinkedIn

APH10

Anthony Harrison
anthony@aph10.com




```
sbom-manager --module pyyaml
SBOM                    Project          Description     Product  Version   License
=============================================================================
matcha-ml.spdx          Matcha-ML        Release 2.3     pyyaml   5.4.1     MIT
cve-bin-tool-py3....    Release_3.2.1    Not specified   pyyaml   6.0       MIT
sbom4python.spdx        sbom4python      Release 0.8.0   pyyaml   6.0       MIT

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

https://pypi.org/project/sbom-manager/

APH10