Using Python to manage Software Bill of Materials

Who am I?

STILL LEARNING NEW TECHNIQUES, TECHNOLOGIES, …

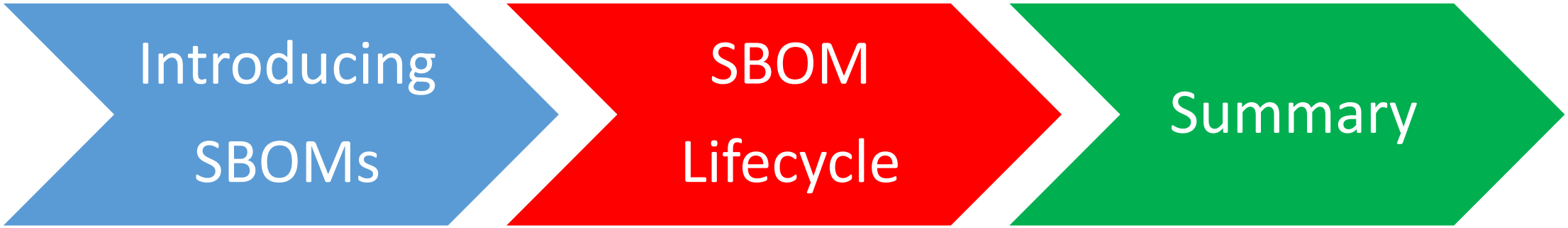
CEng

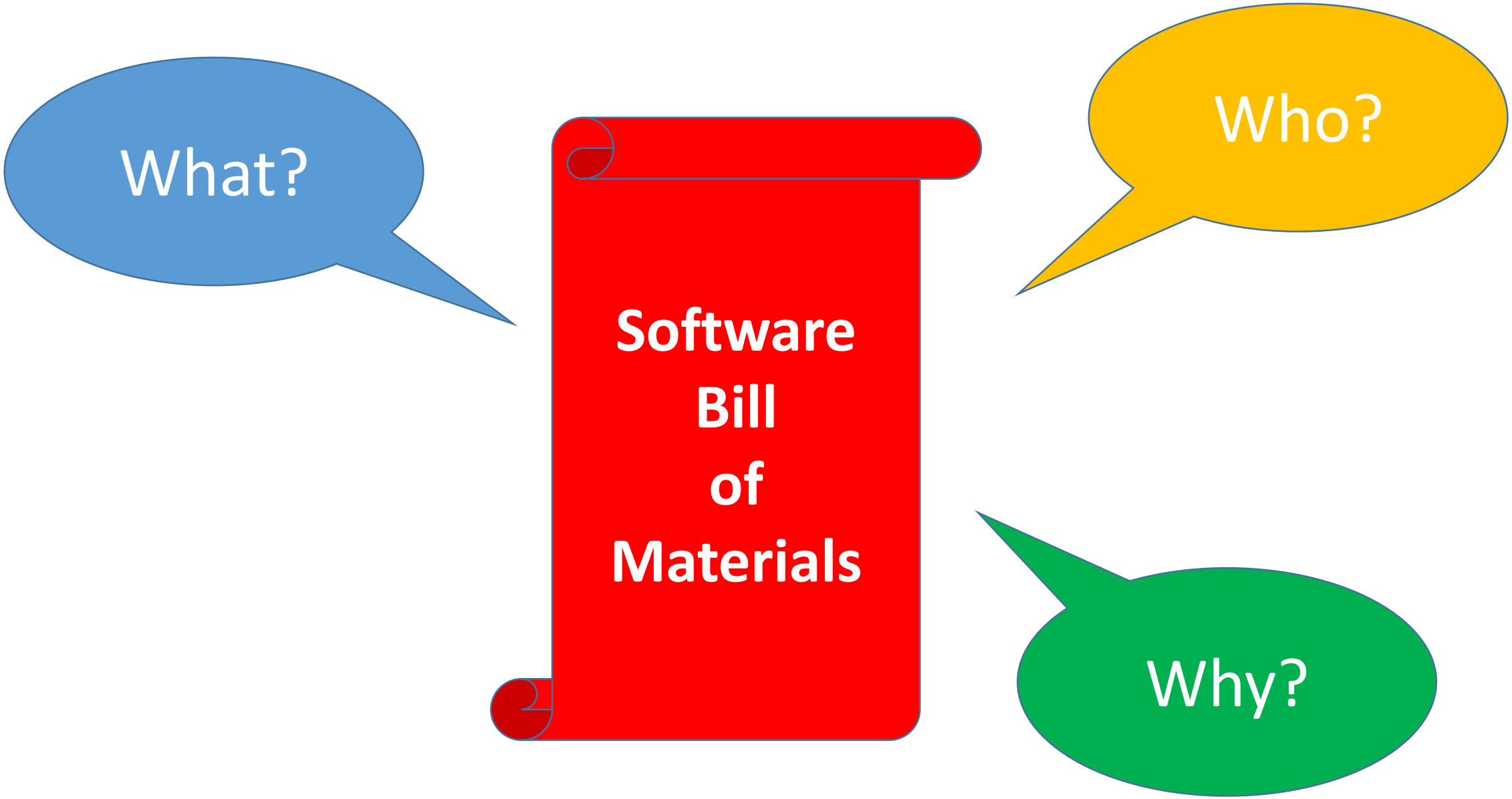
bcs Fellow

STEM AMBASSADORS

CoderDojo

Agenda





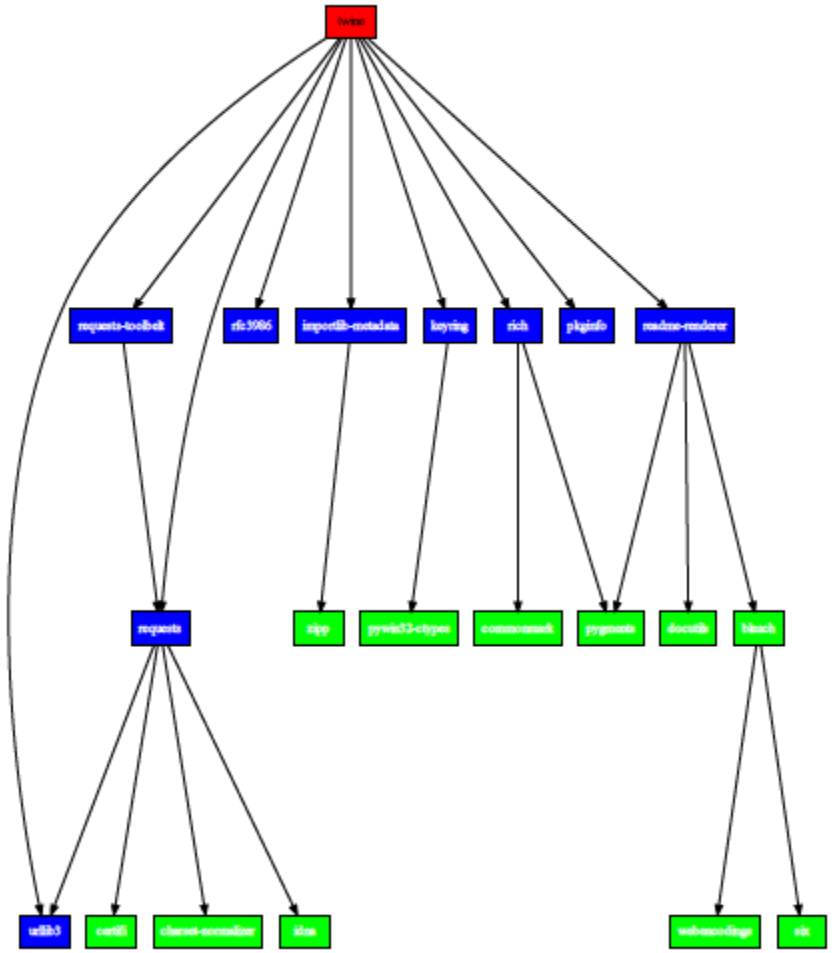
SBOMs

- A SBOM is a **formal set of machine-readable metadata**
- SBOMs are designed to be **shared across organizations**
- SBOMs are an important part of a **cybersecurity strategy**

Industry Mandate

May 2021	Dec 2021	Feb 2022	May 2022	2022/23

LOG4J

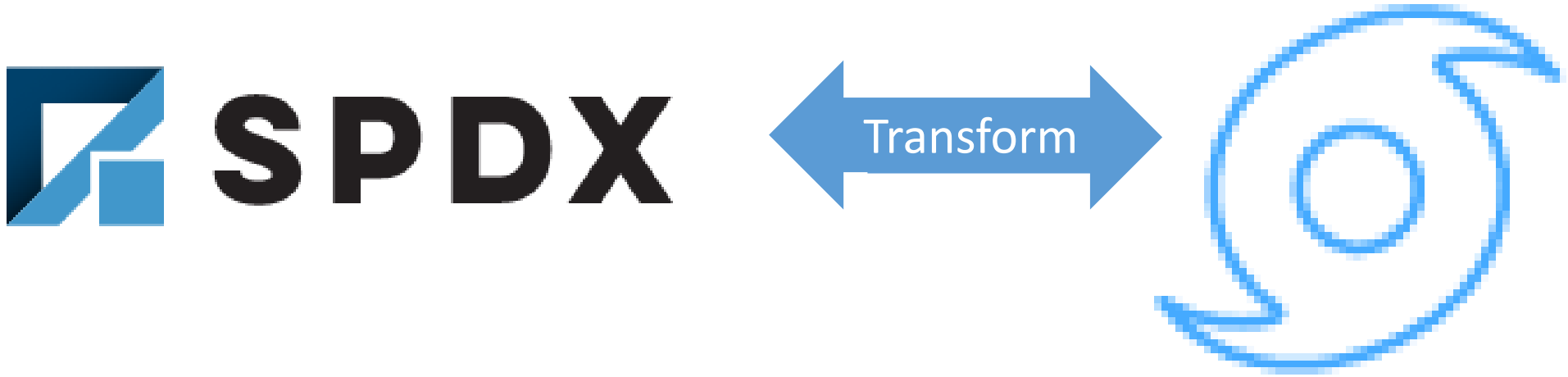


Minimum Elements in a SBOMs

- Product Name
- Version/Release
- Supplier Name

- Dependency Relationships
- Author of SBOM Data
- Timestamp

Two standards and formats….



Create

SBOM Creation

- Package dependencies
- Using the Python language ecosystem
- Processing and generating content

- Explicit Dependencies

- Implicit Dependencies

```
$ pip show pytest
Name: pytest
Version: 7.1.2
Summary: pytest: simple powerful testing with Python
Home-page: https://docs.pytest.org/en/latest/
Author: Holger Krekel, Bruno Oliveira, Ronny Pfannschmidt, Floris Bruynooghe, Brianna …
Author-email:
License: MIT
Location: c:\users\ap_ha_000\appdata\local\programs\python\python310\lib\site-packages
Requires: atomicwrites, attrs, colorama, iniconfig, packaging, pluggy, py, tomli
Required-by: pytest-asyncio, pytest-cov, pytest-forked, pytest-xdist
```


SBOM4Python

- Generates SBOM file for an installed Python module
- Compliant with SBOM minimum content
- Choice of machine readable format (SPDX or CycloneDX)

Licence Metadata

- Apache 2.0
- Apache License, Version 2.0
- Apache 2
- **Apache-2.0**

SPDX licence list

- Apache License 2.0 (Apache-2.0)

- **MIT**
- **MIT License**
- **MIT license**

SPDX licence list

- MIT License (MIT)

Supplier Identification

- Individual
- Organisation

```
$ sbom4python -module pip
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: pip
DocumentNamespace: http://spdx.org/spdxdocs/pip-9bfaa9e4-327c-42e8-bfc9-1b32ab3a3155
LicenseListVersion: 3.9
Creator: Tool: SBOM4PYTHON_Generator-0.1.0
Created: 2022-07-03T19:14:00Z
CreatorComment: <text>This document has been automatically generated.</text>
#####

PackageName: pip
SPDXID: SPDXRef-Package-1-pip
PackageSupplier: Organization: The pip developers
PackageVersion: 22.1.2
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
##### Reported license MIT
PackageLicenseConcluded: MIT
PackageLicenseDeclared: MIT
PackageCopyrightText: NOASSERTION
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Package-1-pip
```

Create

Manage

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?

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.

Am I impacted by a vulnerability?

Vulnerability Details : CVE-2021-3156

Sudo before 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.

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

The happy day Log4j query….

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

Create

Manage

Scan

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

- Report Generated: 2022-01-08 14:13:28
- Time of last update of CVE Data: 2022-01-07 22:52:22

CVE SUMMARY

Severity	Count
CRITICAL	12
HIGH	43
MEDIUM	17
LOW	4

NewFound CVEs

Vendor	Product	Version	CVE Number	Severity	Score (CVSS Version)
alpinelinux	apk-tools	2.10.4	CVE-2021-30139	HIGH	7.5 (v3)
busybox	busybox	1.30.1	CVE-2018-1000500	HIGH	8.1 (v3)
busybox	busybox	1.30.1	CVE-2021-42374	MEDIUM	5.3 (v3)
busybox	busybox	1.30.1	CVE-2021-42376	MEDIUM	5.5 (v3)
busybox	busybox	1.30.1	CVE-2021-42378	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42379	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42380	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42381	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42382	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42384	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42385	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42386	HIGH	7.2 (v3)

sbom4python

sbom-manager

cve-bin-tool

Summary

- SBOMs are becoming a growing and important part of software development
- Better dependency management
- Key role to supporting better vulnerability management

New Pip Install?

```
$ newpip install <module>
```

```
pip install <module>
sbom4python --module <module> --output <module>.spdx
sbom-manger --add <module>.spdx --project $PROJECT_NAME
cve-bin-tool --sbom <module>.spdx --output <module>_vuln.txt
```

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

Thank You