Making SBOMs work for everyone

Paris - June 2023
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 organizations.

➔ SBOMs form an important part of a software risk strategy.
Two primary standards and formats....

https://spdx.org/

Transform

https://cyclonedx.org/
SBOM Content

SBOM Metadata

Component

Relationship
Increasing awareness of SBOMs

May 2021
- US EO

February 2022
- SBOM readiness

February 2023
- UK DSIT

2021
- Log4J December 2021

2022
- SBOM Everywhere May 2022

2023
- CRA September 2022
- FDA October 2023
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
Quality

SBOM

Versioning

Naming

License
SBOM

- Users
- Quality
- Versioning
- License
- Naming
SBOM Diagram:

- Users
- Data
- Quality
- License
- Versioning
- Naming
Package Summary

[ ] License included for package attrs: MISSING
[ ] License included for package idna: MISSING
[ ] OSI Approved license for defusedxml: MISSING
[ ] Using latest version of package httplib2: Version is 0.20.4; latest is 0.22.0
[ ] License included for package pyparsing: MISSING
[ ] Using latest version of package rsa: Version is 4.7.2; latest is 4.9
[ ] Using latest version of package pyopenssl: Version is 23.1.1; latest is 23.2.0
[ ] OSI Approved license for cryptography: MISSING
[ ] Using latest version of package google-auth: Version is 2.18.1; latest is 2.19.1
[ ] Using latest version of package cachetools: Version is 5.3.0; latest is 5.3.1
[ ] Using latest version of package urllib3: Version is 1.26.15; latest is 2.0.2
[ ] OSI Approved license for packaging: MISSING
[ ] Using latest version of package packaging: Version is 21.3; latest is 23.1
[ ] Using latest version of package requests: Version is 2.30.0; latest is 2.31.0
[ ] Using latest version of package rich: Version is 13.3.5; latest is 13.4.1
[ ] NTIA compliant: FAILED

https://pypi.org/project/sbomaudit/
https://pypi.org/project/sbom2dot/
### SBOM Summary

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

### Package Summary

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Supplier</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>click</td>
<td>8.1.2</td>
<td>Armin Ronacher</td>
<td>BSD-3-Clause</td>
</tr>
</tbody>
</table>

### License Summary

<table>
<thead>
<tr>
<th>License</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSD-3-Clause</td>
<td>1</td>
</tr>
</tbody>
</table>

[https://pypi.org/project/sbom2doc/](https://pypi.org/project/sbom2doc/)
sbom-manager --module pyyaml

<table>
<thead>
<tr>
<th>SBOM</th>
<th>Project</th>
<th>Description</th>
<th>Product</th>
<th>Version</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>matcha-ml.spdx</td>
<td>Matcha-ML</td>
<td>Release 2.3</td>
<td>pyyaml</td>
<td>5.4.1</td>
<td>MIT</td>
</tr>
<tr>
<td>cve-bin-tool-py3....</td>
<td>Release_3.2.1</td>
<td>Not specified</td>
<td>pyyaml</td>
<td>6.0</td>
<td>MIT</td>
</tr>
<tr>
<td>sbom4python.spdx</td>
<td>sbom4python</td>
<td>Release 0.8.0</td>
<td>pyyaml</td>
<td>6.0</td>
<td>MIT</td>
</tr>
</tbody>
</table>

sbom-manager --module log4j
No data found

https://pypi.org/project/sbom-manager/
SBOMs provide an important part of the secure software development lifecycle.

SBOMs provide enhanced transparency and 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.