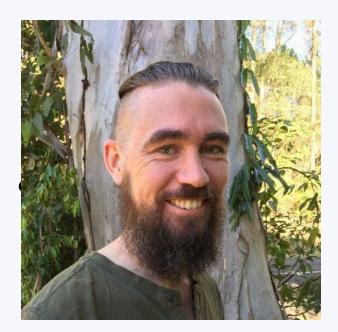
CycloneDX

Software Bill of Materials Standard





Patrick Dwyer



@coderpatros



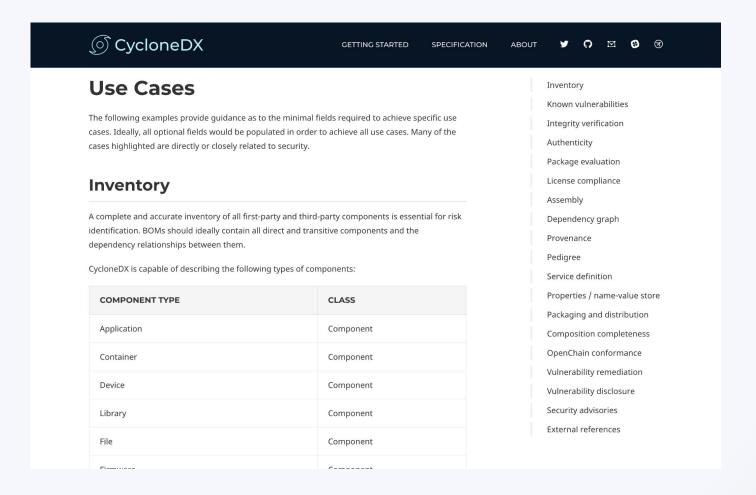
patrick.dwyer@owasp.org

- Co-Leader of OWASP CycloneDX
- Contributor to multiple SBOM related projects and tools
- OSS Maintainer
- Software Development Lead (Government)

Introducing CycloneDX

- Flagship OWASP standards project
- Lightweight, simplicity over complexity easy to implement and adopt
- Optimized for highly automated processes
- Purpose built as a BOM format for cybersecurity use cases
- Designed in May 2017
- Initial release March 2018
- Yearly releases since
- Formal governance and standards process
- Recommended by multiple world government agencies
- Large and growing industry and vendor support
 - https://cyclonedx.org/about/supporters/
- Estimated to be in use at 100k organizations

Use Case Examples



A collection of common use cases achievable with CycloneDX along with concrete examples in XML and JSON.

https://cyclonedx.org/use-cases/

BOM Metadata

```
"bomFormat": "CycloneDX",
"specVersion": "1.3",
"serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
"version": 1,
"metadata": {
    "timestamp": "2020-04-13T20:20:39+00:00",
    "tools": [ ... ],
    "authors": [ ... ],
    "manufacture": { ... },
    "supplier": { ... },
    "component": { ... }
```

Component Inventory

Supports:

- Applications
- Libraries
- Frameworks
- Containers
- Operating systems
- Firmware
- Devices
- Files
- Services

Known vulnerabilities

```
"components": [
   "type": "library",
    "group": "org.apache.logging.log4j",
    "name": "log4j2-core",
    "version": "2.14.1",
    "cpe": "cpe:2.3:a:apache:log4j:2.14.1",
    "purl": "mvn:org.apache.logging.log4j/log4j-core@2.14.1",
    "swid": { ... }
```

Integrity

```
"components": [
   "type": "library",
    "group": "org.apache.logging.log4j",
   "name": "log4j2-core",
    "version": "2.14.1",
    "hashes": [
     {"alg": "SHA3-512", "content": "..." }
```

Authenticity

- XML Signature
- JSON Web Signature (JWS)
- JSON Signature Format (JSF)
- Digital signatures can be applied to a BOM or to an assembly within a BOM
- Signatures can be external to the BOM or enveloped (included within)

Component Pedigree

```
"pedigree": {
  "ancestors": [
      "type": "library",
      "group": "org.apache.logging.log4j",
      "name": "log4j2-core",
      "version": "2.14.1"
  "patches": [
      "type": "backport",
      "diff": { ..., "resolves": [{ "type": "security", "id": "CVE-2021-44228", ... }] }
```

Provenance

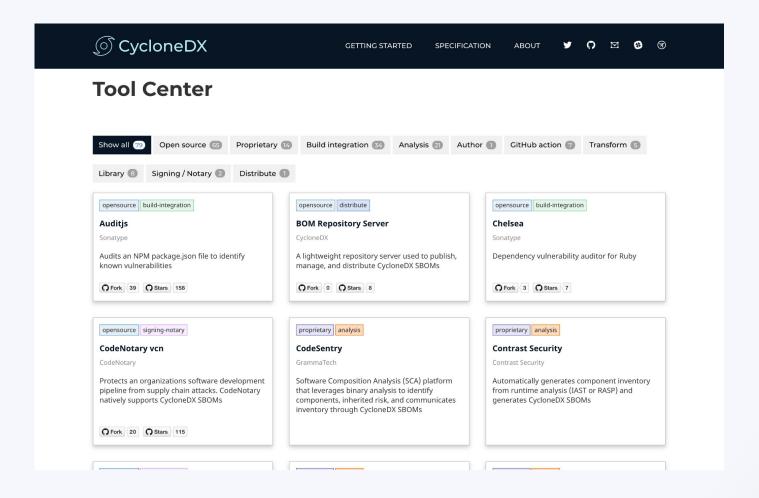
- Component downloaded location
- Supplier
- Author
- Publisher

Composition

- Assemblies
- Dependency graph
- Completeness
 - o complete
 - incomplete
 - first-party/third-party
 - unknown

and many, many more...

Tool Center



Community effort to establish a marketplace of free, open source, and proprietary tools and solutions that support CycloneDX.

https://cyclonedx.org/tool-center/

In development

- Improved hardware support
- "Vulnerability-Exploitability eXchange" format, aka VEX
- IETF URN namespace registration to deeplink between BOMs
- Schema hardening
- OWASP SBOM Maturity Model
- CycloneDX v1.4 due for release January 2022

Community Participation

- Website (introduction, use cases, tool center, and specification)
 - https://cyclonedx.org/
- GitHub
 - https://github.com/CycloneDX
- Slack
 - https://cyclonedx.org/slack
 - https://cyclonedx.org/slack/invite
- Mailing List
 - https://cyclonedx.org/discussion

Thank You

