

# 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

GETTING STARTEDSPECIFICATIONABOUTTwitterGitHubEmailDiscordYouTube

## Use Cases

The following examples provide guidance as to the minimal fields required to achieve specific use cases. Ideally, all optional fields would be populated in order to achieve all use cases. Many of the cases highlighted are directly or closely related to security.

### Inventory

A complete and accurate inventory of all first-party and third-party components is essential for risk identification. BOMs should ideally contain all direct and transitive components and the dependency relationships between them.

CycloneDX is capable of describing the following types of components:

COMPONENT TYPE	CLASS
Application	Component
Container	Component
Device	Component
Library	Component
File	Component
Firmware	Component

Inventory

Known vulnerabilities

Integrity verification

Authenticity

Package evaluation

License compliance

Assembly

Dependency graph

Provenance

Pedigree

Service definition

Properties / name-value store

Packaging and distribution

Composition completeness

OpenChain conformance

Vulnerability remediation

Vulnerability disclosure

Security advisories

External references

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

```
{  
  ...  
  "components": [  
    {  
      "type": "library",  
      "group": "org.apache.logging.log4j",  
      "name": "log4j2-core",  
      "version": "2.14.1"  
    }  
  ]  
}
```

## 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
  - complete
  - incomplete
  - first-party/third-party
  - unknown

**and many, many more...**

# Tool Center

The screenshot shows the CycloneDX Tool Center interface. At the top is a dark navigation bar with the CycloneDX logo and links for GETTING STARTED, SPECIFICATION, ABOUT, and social media icons. Below this is a 'Tool Center' header. A filter bar allows users to show all tools (79) or filter by license (Open source: 65, Proprietary: 14) and function (Build integration: 34, Analysis: 21, Author: 1, GitHub action: 7, Transform: 5). Further filters include Library (8), Signing / Notary (2), and Distribute (1). The main area displays tool cards for Auditjs, BOM Repository Server, Chelsea, CodeNotary vcn, CodeSentry, and Contrast Security, each with its license, description, and GitHub metrics.

Tool Name	License	Function	Description	Forks	Stars
Auditjs	Open source	Build integration	Audits an NPM package.json file to identify known vulnerabilities	39	158
BOM Repository Server	Open source	Distribute	A lightweight repository server used to publish, manage, and distribute CycloneDX SBOMs	0	8
Chelsea	Open source	Build integration	Dependency vulnerability auditor for Ruby	3	7
CodeNotary vcn	Open source	Signing / Notary	Protects an organizations software development pipeline from supply chain attacks. CodeNotary natively supports CycloneDX SBOMs	20	115
CodeSentry	Proprietary	Analysis	Software Composition Analysis (SCA) platform that leverages binary analysis to identify components, inherited risk, and communicates inventory through CycloneDX SBOMs	-	-
Contrast Security	Proprietary	Analysis	Automatically generates component inventory from runtime analysis (IAST or RASP) and generates CycloneDX SBOMs	-	-

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**

