LG Electronics Open Source Program Office

# FOSSLight 현재와 미래

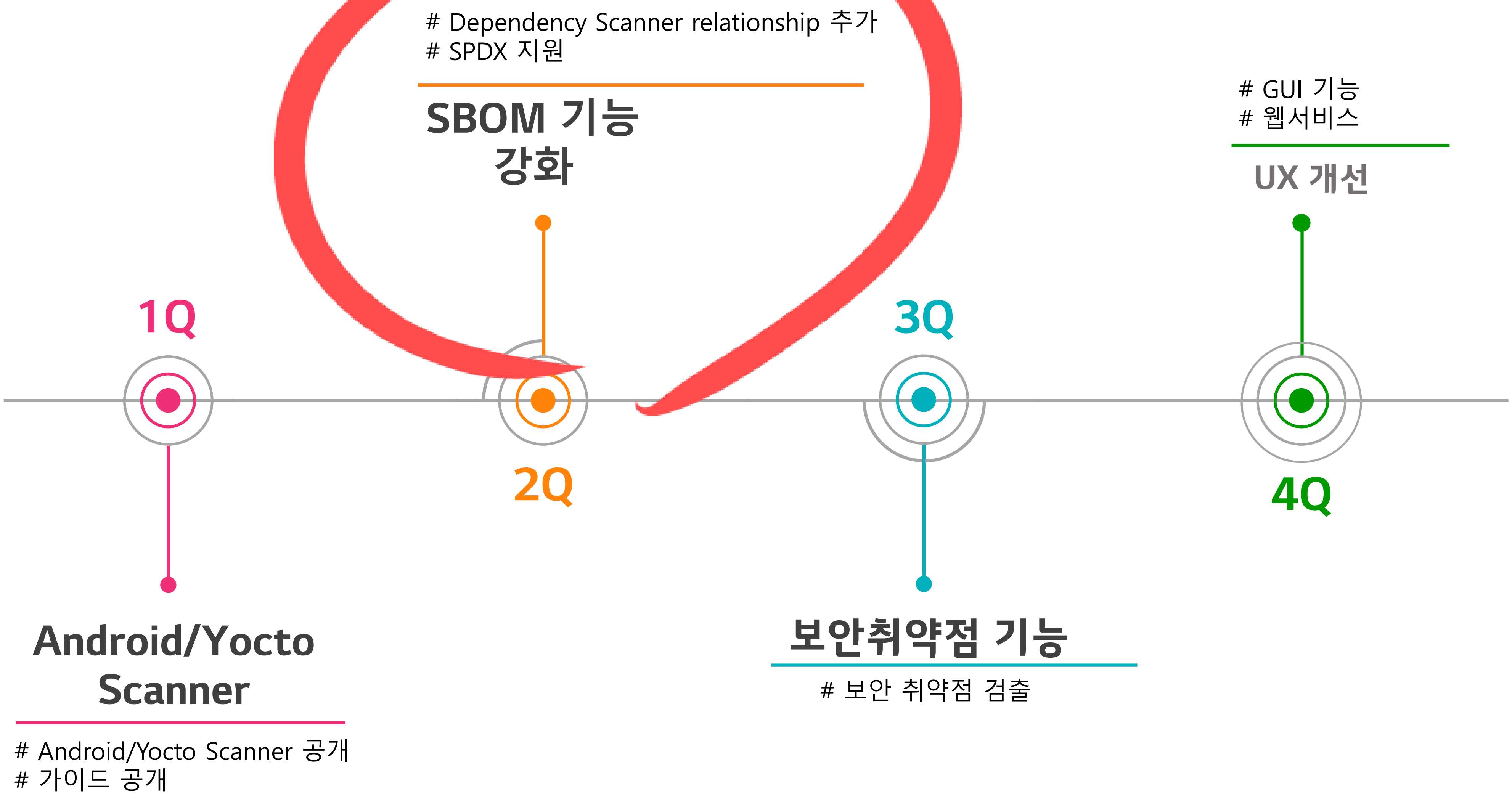
LG전자 김경애

LG Open Source

# CONTENTS

- FOSSLight SBOM 지원
- 2024 FOSSLight 로드맵

# FOSSLight Scanner 2023 로드맵



**1Q**

**Android/Yocto Scanner**

# Android/Yocto Scanner 공개
# 가이드 공개

**2Q**

**SBOM 기능 강화**

# Dependency Scanner relationship 추가
# SPDX 지원

**3Q**

**보안취약점 기능**

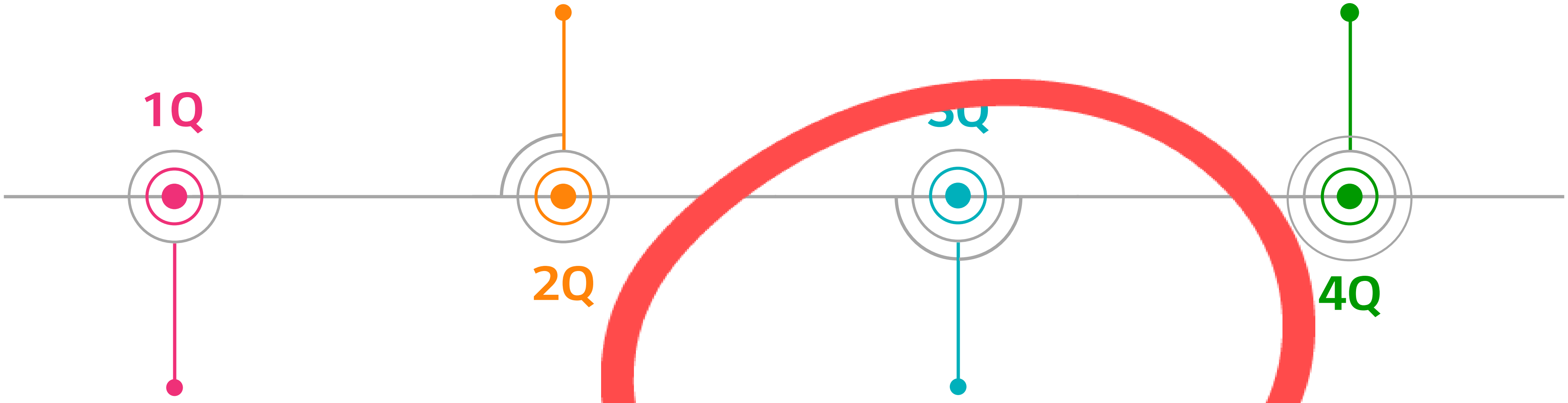
# 보안 취약점 검출

**4Q**

**UX 개선**

# GUI 기능
# 웹서비스

# FOSSLight Hub 2023 업데이트 일정



**요구사항 분석 및 설계**

**보안취약점 기능 개선**

- # NVD Data Feed > REST API 변경
- # CVE 목록 출력
- # 패치 링크 출력
- # 패치 적용된 CVE 제외 max score 출력

**SBOM 기능 강화**

- # 고지 의무 상관없이 고지문 출력
- # 종속성 관계 추가
- # CycloneDX 양식 지원

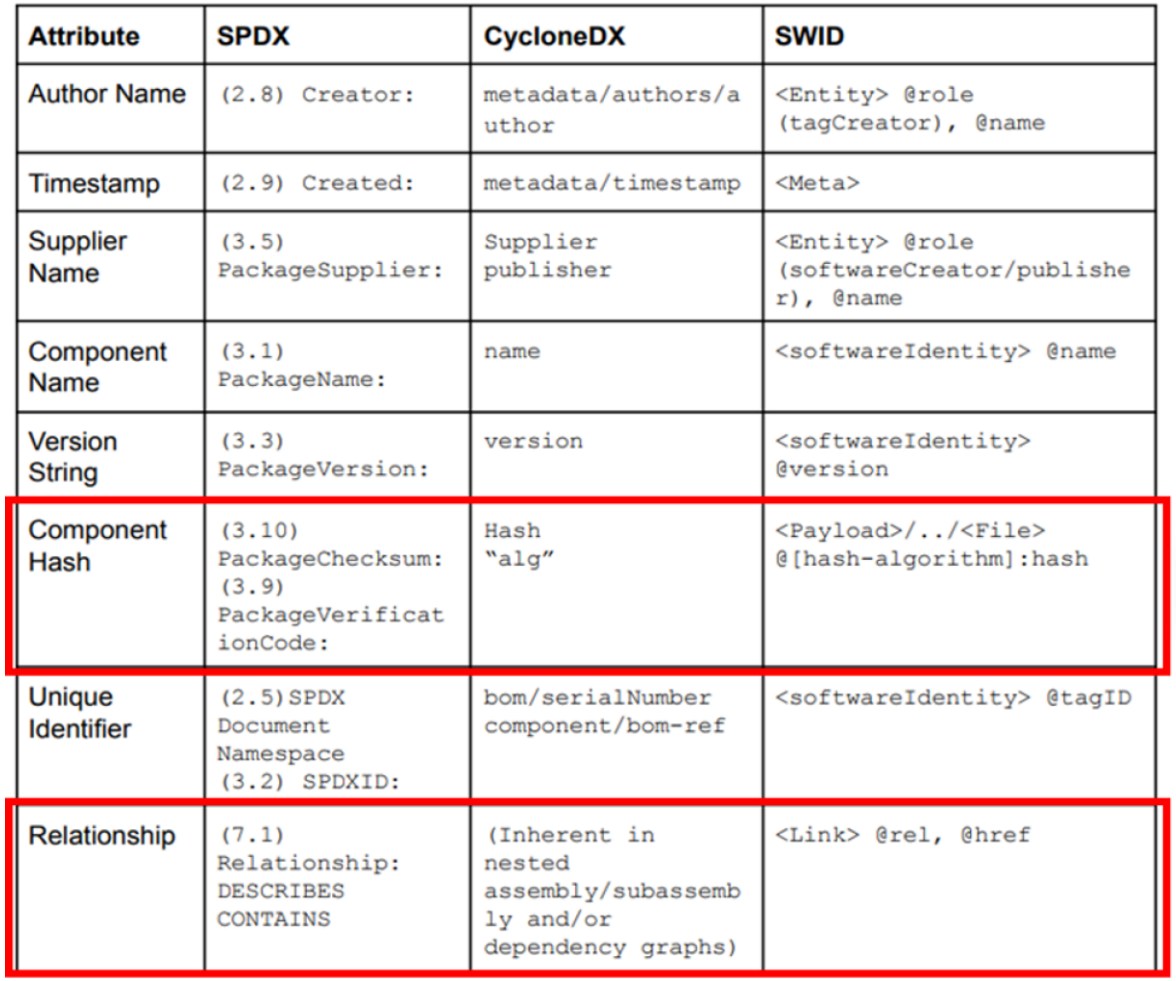
**UX 개선**

- # UI 업그레이드
- # Dashboard 개선

LG Electronics Open Source Program Office

# FOSSLight SBOM 지원

# Baseline Attributes of SBOM



| Attribute | SPDX | CycloneDX | SWID |
|---|---|---|---|
| Author Name | (2.8) Creator: | metadata/authors/author | <Entity> @role (tagCreator), @name |
| Timestamp | (2.9) Created: | metadata/timestamp | <Meta> |
| Supplier Name | (3.5) PackageSupplier: | Supplier publisher | <Entity> @role (softwareCreator/publisher), @name |
| Component Name | (3.1) PackageName: | name | <softwareIdentity> @name |
| Version String | (3.3) PackageVersion: | version | <softwareIdentity> @version |
| Component Hash | (3.10) PackageChecksum:<br>(3.9) PackageVerificationCode: | Hash “alg” | <Payload>/../<File> @[hash-algorithm]:hash |
| Unique Identifier | (2.5)SPDX Document Namespace<br>(3.2) SPDXID: | bom/serialNumber<br>component/bom-ref | <softwareIdentity> @tagID |
| Relationship | (7.1) Relationship:<br>DESCRIBES<br>CONTAINS | (Inherent in nested assembly/subassembly and/or dependency graphs) | <Link> @rel, @href |

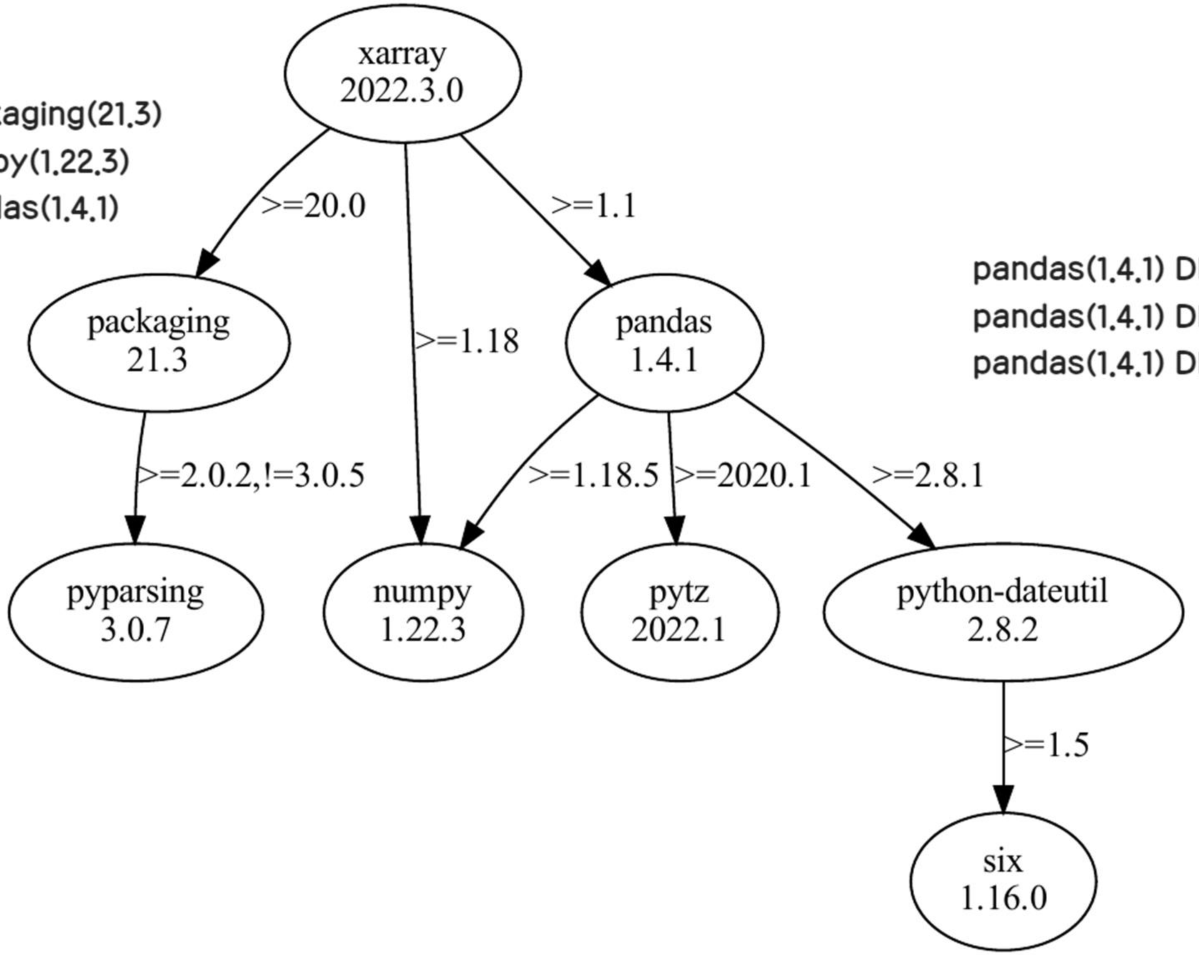
Table 1: Mapping baseline component information to existing formats

추가 지원 필요

# Relationship 정보

- 각 패키지의 dependencies 정보 필요

xarray(2022.3.0) DEPENDS_ON packaging(21.3)
xarray(2022.3.0) DEPENDS_ON numpy(1.22.3)
xarray(2022.3.0) DEPENDS_ON pandas(1.4.1)



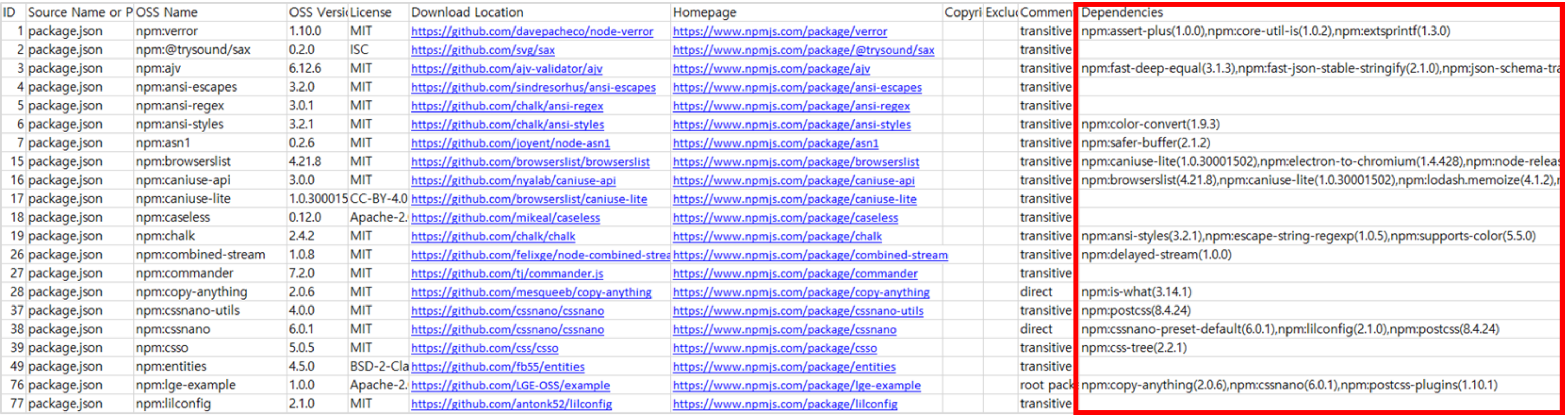
pandas(1.4.1) DEPENDS_ON numpy(1.22.3)
pandas(1.4.1) DEPENDS_ON pytz(2022.1)
pandas(1.4.1) DEPENDS_ON python-dateutil(2.8.2)

LG Electronics Open Source Program Office

# FOSSLight Scanner Dependencies

# FOSSLight Dependency Scanner

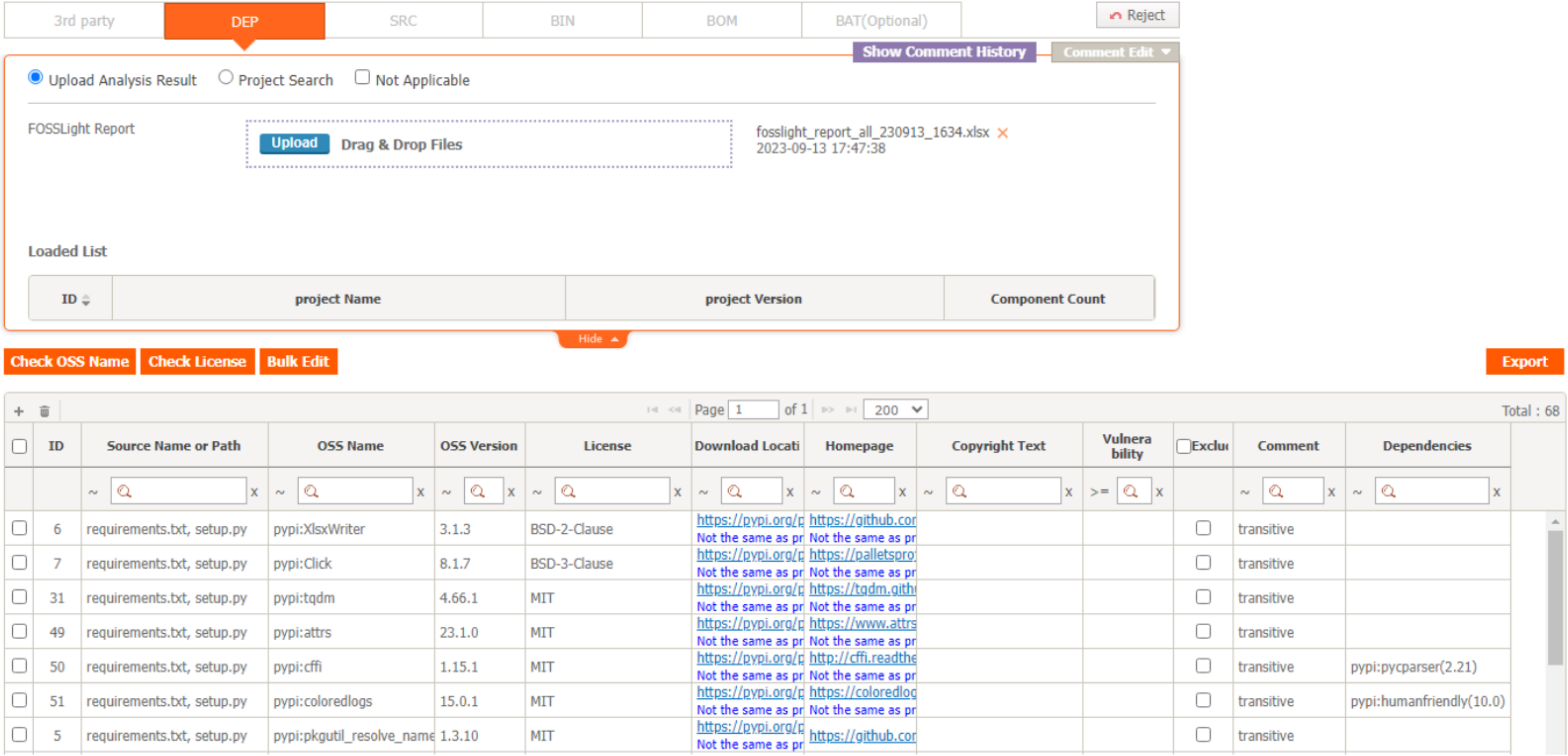
- **FOSSLight Dependency Scanner dependencies 정보 추가**



| ID | Source Name or P | OSS Name | OSS Versi | License | Download Location | Homepage | Copyri | Exclu | Commen | Dependencies |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | package.json | npm:verror | 1.10.0 | MIT | https://github.com/davepacheco/node-verror | https://www.npmjs.com/package/verror | | | transitive | npm:assert-plus(1.0.0),npm:core-util-is(1.0.2),npm:extsprintf(1.3.0) |
| 2 | package.json | npm:@trysound/sax | 0.2.0 | ISC | https://github.com/svg/sax | https://www.npmjs.com/package/@trysound/sax | | | transitive | |
| 3 | package.json | npm:ajv | 6.12.6 | MIT | https://github.com/ajv-validator/ajv | https://www.npmjs.com/package/ajv | | | transitive | npm:fast-deep-equal(3.1.3),npm:fast-json-stable-stringify(2.1.0),npm:json-schema-tra |
| 4 | package.json | npm:ansi-escapes | 3.2.0 | MIT | https://github.com/sindresorhus/ansi-escapes | https://www.npmjs.com/package/ansi-escapes | | | transitive | |
| 5 | package.json | npm:ansi-regex | 3.0.1 | MIT | https://github.com/chalk/ansi-regex | https://www.npmjs.com/package/ansi-regex | | | transitive | |
| 6 | package.json | npm:ansi-styles | 3.2.1 | MIT | https://github.com/chalk/ansi-styles | https://www.npmjs.com/package/ansi-styles | | | transitive | npm:color-convert(1.9.3) |
| 7 | package.json | npm:asn1 | 0.2.6 | MIT | https://github.com/joyent/node-asn1 | https://www.npmjs.com/package/asn1 | | | transitive | npm:safer-buffer(2.1.2) |
| 15 | package.json | npm:browserslist | 4.21.8 | MIT | https://github.com/browserslist/browserslist | https://www.npmjs.com/package/browserslist | | | transitive | npm:caniuse-lite(1.0.30001502),npm:electron-to-chromium(1.4.428),npm:node-releas |
| 16 | package.json | npm:caniuse-api | 3.0.0 | MIT | https://github.com/nyalab/caniuse-api | https://www.npmjs.com/package/caniuse-api | | | transitive | npm:browserslist(4.21.8),npm:caniuse-lite(1.0.30001502),npm:lodash.memoize(4.1.2),n |
| 17 | package.json | npm:caniuse-lite | 1.0.300015 | CC-BY-4.0 | https://github.com/browserslist/caniuse-lite | https://www.npmjs.com/package/caniuse-lite | | | transitive | |
| 18 | package.json | npm:caseless | 0.12.0 | Apache-2. | https://github.com/mikeal/caseless | https://www.npmjs.com/package/caseless | | | transitive | |
| 19 | package.json | npm:chalk | 2.4.2 | MIT | https://github.com/chalk/chalk | https://www.npmjs.com/package/chalk | | | transitive | npm:ansi-styles(3.2.1),npm:escape-string-regexp(1.0.5),npm:supports-color(5.5.0) |
| 26 | package.json | npm:combined-stream | 1.0.8 | MIT | https://github.com/felixge/node-combined-strea | https://www.npmjs.com/package/combined-stream | | | transitive | npm:delayed-stream(1.0.0) |
| 27 | package.json | npm:commander | 7.2.0 | MIT | https://github.com/tj/commander.js | https://www.npmjs.com/package/commander | | | transitive | |
| 28 | package.json | npm:copy-anything | 2.0.6 | MIT | https://github.com/mesqueeb/copy-anything | https://www.npmjs.com/package/copy-anything | | | direct | npm:is-what(3.14.1) |
| 37 | package.json | npm:cssnano-utils | 4.0.0 | MIT | https://github.com/cssnano/cssnano | https://www.npmjs.com/package/cssnano-utils | | | transitive | npm:postcss(8.4.24) |
| 38 | package.json | npm:cssnano | 6.0.1 | MIT | https://github.com/cssnano/cssnano | https://www.npmjs.com/package/cssnano | | | direct | npm:cssnano-preset-default(6.0.1),npm:lilconfig(2.1.0),npm:postcss(8.4.24) |
| 39 | package.json | npm:csso | 5.0.5 | MIT | https://github.com/css/csso | https://www.npmjs.com/package/csso | | | transitive | npm:css-tree(2.2.1) |
| 49 | package.json | npm:entities | 4.5.0 | BSD-2-Cla | https://github.com/fb55/entities | https://www.npmjs.com/package/entities | | | transitive | |
| 76 | package.json | npm:lge-example | 1.0.0 | Apache-2. | https://github.com/LGE-OSS/example | https://www.npmjs.com/package/lge-example | | | root pack | npm:copy-anything(2.0.6),npm:cssnano(6.0.1),npm:postcss-plugins(1.10.1) |
| 77 | package.json | npm:lilconfig | 2.1.0 | MIT | https://github.com/antonk52/lilconfig | https://www.npmjs.com/package/lilconfig | | | transitive | |

# FOSSLight Hub DEP 추가

# FOSSLight Hub DEP 탭 추가



● Upload Analysis Result ○ Project Search □ Not Applicable

FOSSLight Report

fosslight_report_all_230913_1634.xlsx ✕
2023-09-13 17:47:38

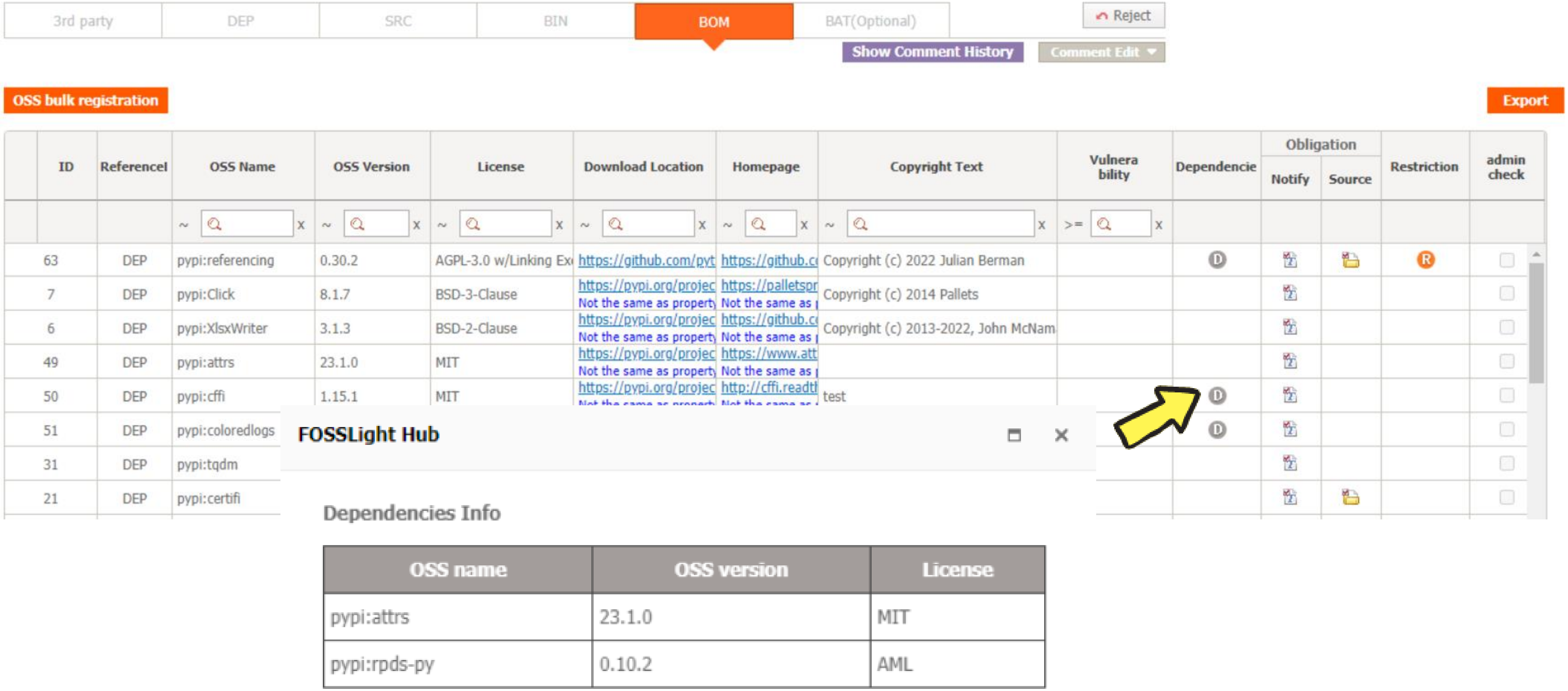
Loaded List

| ID | project Name | project Version | Component Count |
|---|---|---|---|

Page 1 of 1 200 Total : 68

| □ | ID | Source Name or Path | OSS Name | OSS Version | License | Download Locati | Homepage | Copyright Text | Vulnera bility | □Excluc | Comment | Dependencies |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 6 | requirements.txt, setup.py | pypi:XlsxWriter | 3.1.3 | BSD-2-Clause | https://pypi.org/p<br>Not the same as pr | https://github.cor<br>Not the same as pr | | | □ | transitive | |
| □ | 7 | requirements.txt, setup.py | pypi:Click | 8.1.7 | BSD-3-Clause | https://pypi.org/p<br>Not the same as pr | https://palletspro<br>Not the same as pr | | | □ | transitive | |
| □ | 31 | requirements.txt, setup.py | pypi:tqdm | 4.66.1 | MIT | https://pypi.org/p<br>Not the same as pr | https://tqdm.githu<br>Not the same as pr | | | □ | transitive | |
| □ | 49 | requirements.txt, setup.py | pypi:attrs | 23.1.0 | MIT | https://pypi.org/p<br>Not the same as pr | https://www.attrs<br>Not the same as pr | | | □ | transitive | |
| □ | 50 | requirements.txt, setup.py | pypi:cffi | 1.15.1 | MIT | https://pypi.org/p<br>Not the same as pr | http://cffi.readthe<br>Not the same as pr | | | □ | transitive | pypi:pycparser(2.21) |
| □ | 51 | requirements.txt, setup.py | pypi:coloredlogs | 15.0.1 | MIT | https://pypi.org/p<br>Not the same as pr | https://coloredlog<br>Not the same as pr | | | □ | transitive | pypi:humanfriendly(10.0) |
| □ | 5 | requirements.txt, setup.py | pypi:pkgutil_resolve_name | 1.3.10 | MIT | https://pypi.org/p<br>Not the same as pr | https://github.cor | | | □ | transitive | |

# BOM 탭 Dependencies 정보



| | ID | Referencel | OSS Name | OSS Version | License | Download Location | Homepage | Copyright Text | Vulnerability | Dependencie | Obligation | | Restriction | admin check |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Notify | Source | | |
| | | | ~ x | ~ x | ~ x | ~ x | ~ x | ~ x | >= x | | | | | |
| | 63 | DEP | pypi:referencing | 0.30.2 | AGPL-3.0 w/Linking Ex | https://github.com/pyt | https://github.c | Copyright (c) 2022 Julian Berman | | Ⓓ | 📄 | 📁 | Ⓡ | □ |
| | 7 | DEP | pypi:Click | 8.1.7 | BSD-3-Clause | https://pypi.org/projec<br>Not the same as property | https://palletspr<br>Not the same as | Copyright (c) 2014 Pallets | | | 📄 | | | □ |
| | 6 | DEP | pypi:XlsxWriter | 3.1.3 | BSD-2-Clause | https://pypi.org/projec<br>Not the same as property | https://github.c<br>Not the same as | Copyright (c) 2013-2022, John McNam | | | 📄 | | | □ |
| | 49 | DEP | pypi:attrs | 23.1.0 | MIT | https://pypi.org/projec<br>Not the same as property | https://www.att<br>Not the same as | | | | 📄 | | | □ |
| | 50 | DEP | pypi:cffi | 1.15.1 | MIT | https://pypi.org/projec | http://cffi.readt | test | | Ⓓ | 📄 | | | □ |
| | 51 | DEP | pypi:coloredlogs | | | | | | | Ⓓ | 📄 | | | □ |
| | 31 | DEP | pypi:tqdm | | | | | | | | 📄 | | | □ |
| | 21 | DEP | pypi:certifi | | | | | | | | 📄 | 📁 | | □ |

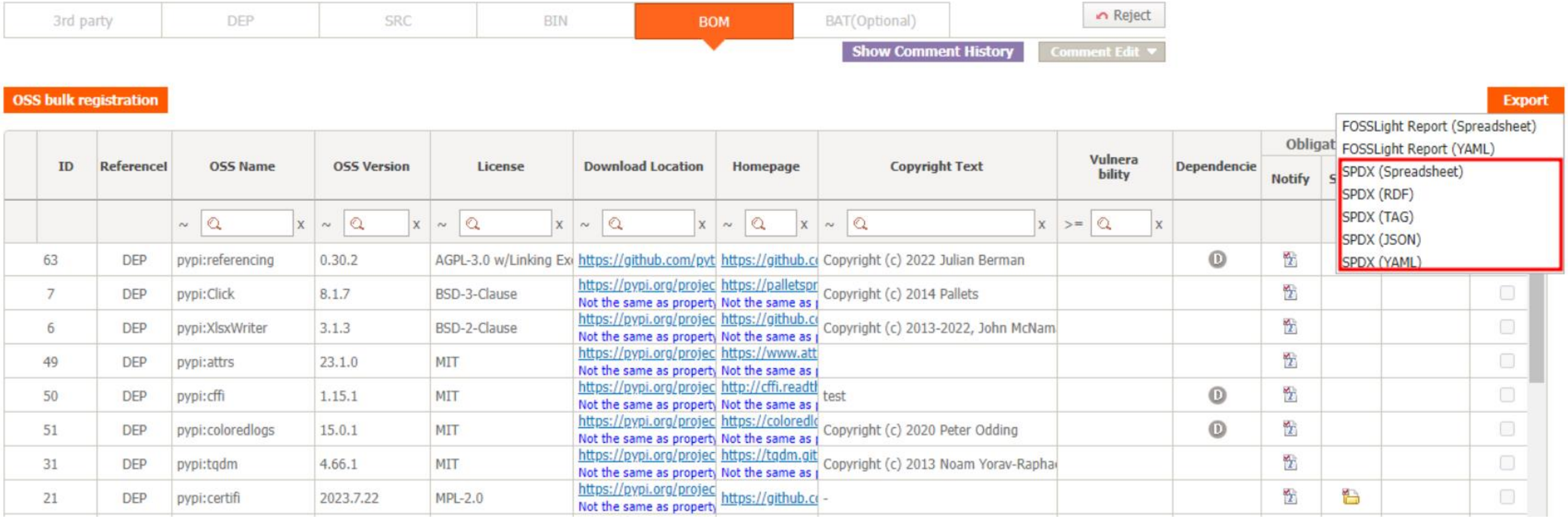
**FOSSLight Hub**

Dependencies Info

| OSS name | OSS version | License |
|---|---|---|
| pypi:attrs | 23.1.0 | MIT |
| pypi:rpds-py | 0.10.2 | AML |

LG Electronics Open Source Program Office

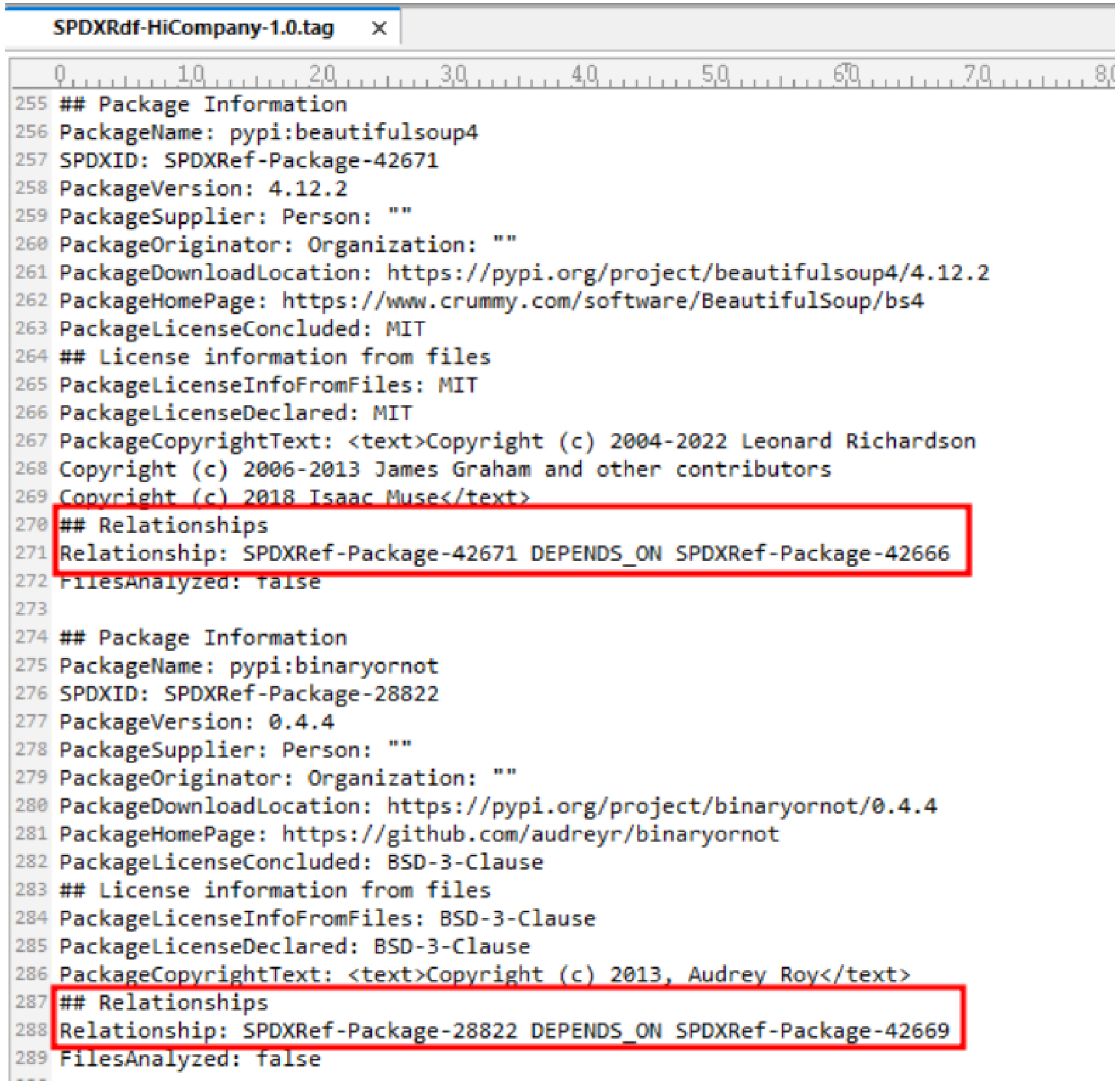
# SPDX Relationship 정보 추가



| ID | ReferenceI | OSS Name | OSS Version | License | Download Location | Homepage | Copyright Text | Vulnera bility | Dependencie | Obligat | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Notify | S | |
| | | ~ x | ~ x | ~ x | ~ x | ~ x | ~ x | >= x | | | | |
| 63 | DEP | pypi:referencing | 0.30.2 | AGPL-3.0 w/Linking Ex | https://github.com/pyt | https://github.c | Copyright (c) 2022 Julian Berman | | D | | | |
| 7 | DEP | pypi:Click | 8.1.7 | BSD-3-Clause | https://pypi.org/projec<br>Not the same as propert | https://palletspr<br>Not the same as | Copyright (c) 2014 Pallets | | | | | □ |
| 6 | DEP | pypi:XlsxWriter | 3.1.3 | BSD-2-Clause | https://pypi.org/projec<br>Not the same as propert | https://github.c<br>Not the same as | Copyright (c) 2013-2022, John McNam | | | | | □ |
| 49 | DEP | pypi:attrs | 23.1.0 | MIT | https://pypi.org/projec<br>Not the same as propert | https://www.att<br>Not the same as | | | | | | □ |
| 50 | DEP | pypi:cffi | 1.15.1 | MIT | https://pypi.org/projec<br>Not the same as propert | http://cffi.readtl<br>Not the same as | test | | D | | | □ |
| 51 | DEP | pypi:coloredlogs | 15.0.1 | MIT | https://pypi.org/projec<br>Not the same as propert | https://coloredlc<br>Not the same as | Copyright (c) 2020 Peter Odding | | D | | | □ |
| 31 | DEP | pypi:tqdm | 4.66.1 | MIT | https://pypi.org/projec<br>Not the same as propert | https://tqdm.git<br>Not the same as | Copyright (c) 2013 Noam Yorav-Rapha | | | | | □ |
| 21 | DEP | pypi:certifi | 2023.7.22 | MPL-2.0 | https://pypi.org/projec<br>Not the same as propert | https://github.c | - | | | | | □ |

LG Electronics Open Source Program Office

# SPDX Relationship 정보 출력

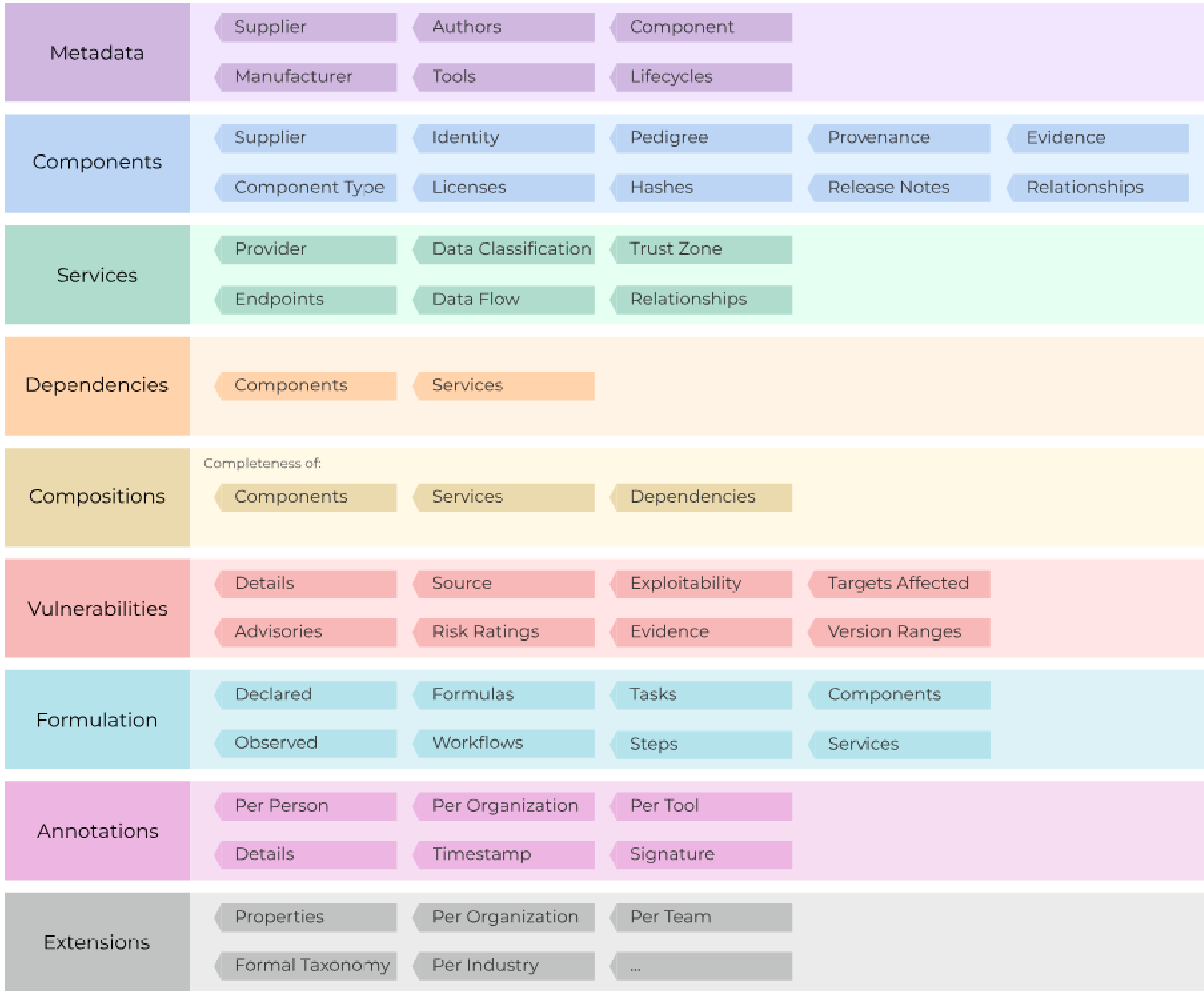


```
## Package Information
PackageName: pypi:beautifulsoup4
SPDXID: SPDXRef-Package-42671
PackageVersion: 4.12.2
PackageSupplier: Person: ""
PackageOriginator: Organization: ""
PackageDownloadLocation: https://pypi.org/project/beautifulsoup4/4.12.2
PackageHomePage: https://www.crummy.com/software/BeautifulSoup/bs4
PackageLicenseConcluded: MIT
## License information from files
PackageLicenseInfoFromFiles: MIT
PackageLicenseDeclared: MIT
PackageCopyrightText: <text>Copyright (c) 2004-2022 Leonard Richardson
Copyright (c) 2006-2013 James Graham and other contributors
Copyright (c) 2018 Isaac Muse</text>
## Relationships
Relationship: SPDXRef-Package-42671 DEPENDS_ON SPDXRef-Package-42666
FilesAnalyzed: false

## Package Information
PackageName: pypi:binaryornot
SPDXID: SPDXRef-Package-28822
PackageVersion: 0.4.4
PackageSupplier: Person: ""
PackageOriginator: Organization: ""
PackageDownloadLocation: https://pypi.org/project/binaryornot/0.4.4
PackageHomePage: https://github.com/audreyr/binaryornot
PackageLicenseConcluded: BSD-3-Clause
## License information from files
PackageLicenseInfoFromFiles: BSD-3-Clause
PackageLicenseDeclared: BSD-3-Clause
PackageCopyrightText: <text>Copyright (c) 2013, Audrey Roy</text>
## Relationships
Relationship: SPDXRef-Package-28822 DEPENDS_ON SPDXRef-Package-42669
FilesAnalyzed: false
```

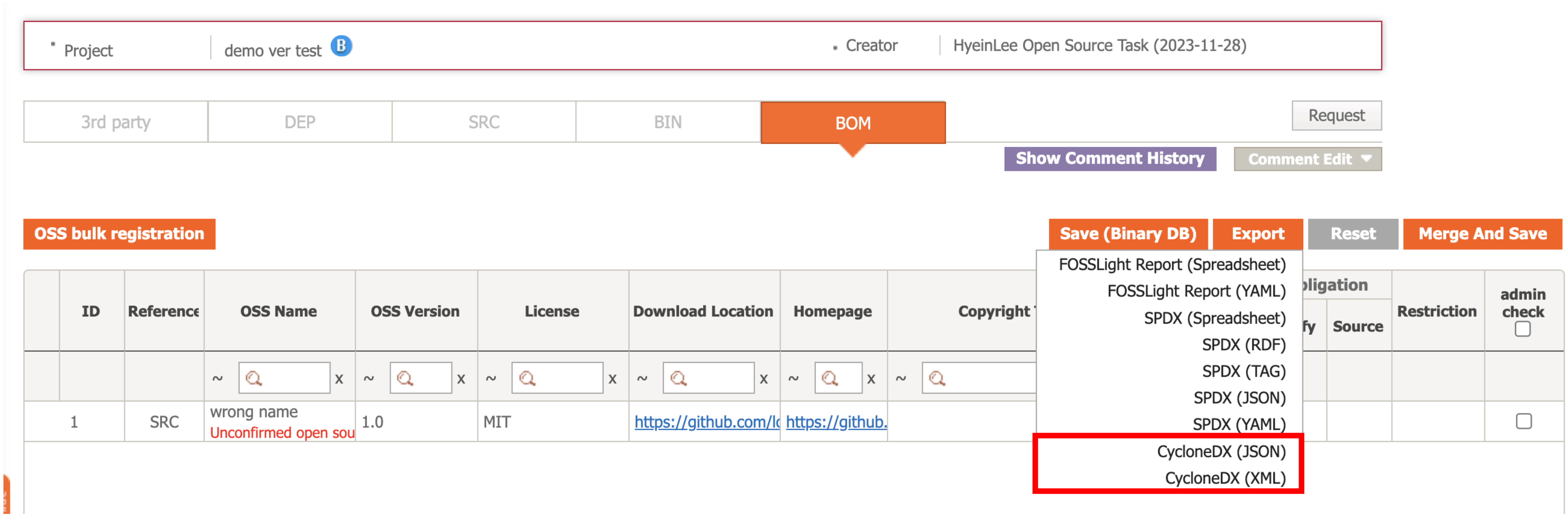
# FOSSLight Hub CycloneDX 지원

# CycloneDX 양식 지원



| | | | | | |
|---|---|---|---|---|---|
| Metadata | Supplier | Authors | Component | | |
| | Manufacturer | Tools | Lifecycles | | |
| Components | Supplier | Identity | Pedigree | Provenance | Evidence |
| | Component Type | Licenses | Hashes | Release Notes | Relationships |
| Services | Provider | Data Classification | Trust Zone | | |
| | Endpoints | Data Flow | Relationships | | |
| Dependencies | Components | Services | | | |
| Compositions | Completeness of: | | | | |
| | Components | Services | Dependencies | | |
| Vulnerabilities | Details | Source | Exploitability | Targets Affected | |
| | Advisories | Risk Ratings | Evidence | Version Ranges | |
| Formulation | Declared | Formulas | Tasks | Components | |
| | Observed | Workflows | Steps | Services | |
| Annotations | Per Person | Per Organization | Per Tool | | |
| | Details | Timestamp | Signature | | |
| Extensions | Properties | Per Organization | Per Team | | |
| | Formal Taxonomy | Per Industry | ... | | |

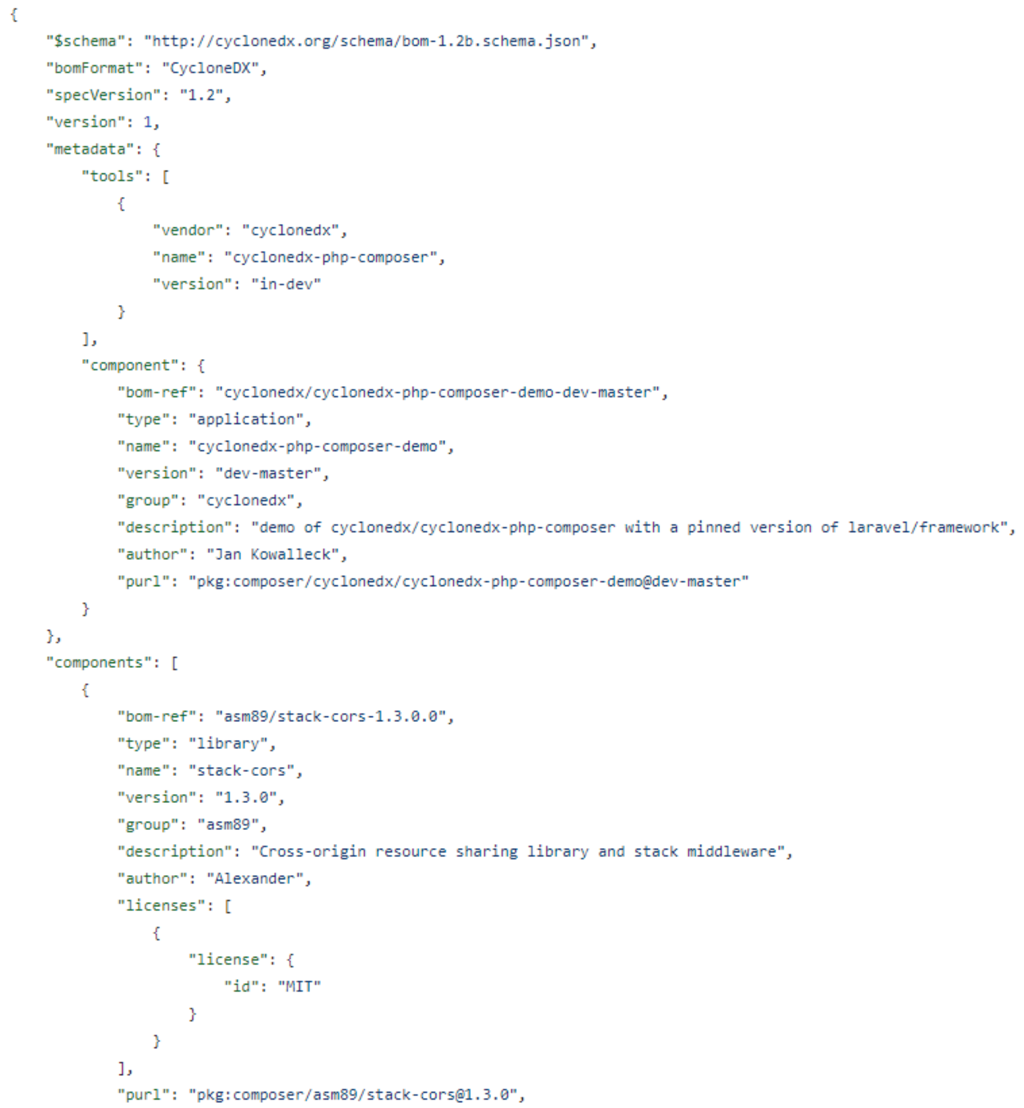
# CycloneDX 양식 지원



- Project: demo ver test
- Creator: HyeinLee Open Source Task (2023-11-28)

| | ID | Reference | OSS Name | OSS Version | License | Download Location | Homepage | Copyright | fy | Source | Restriction | admin check |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | SRC | wrong name<br>Unconfirmed open sou | 1.0 | MIT | https://github.com/l | https://github. | | | | | □ |

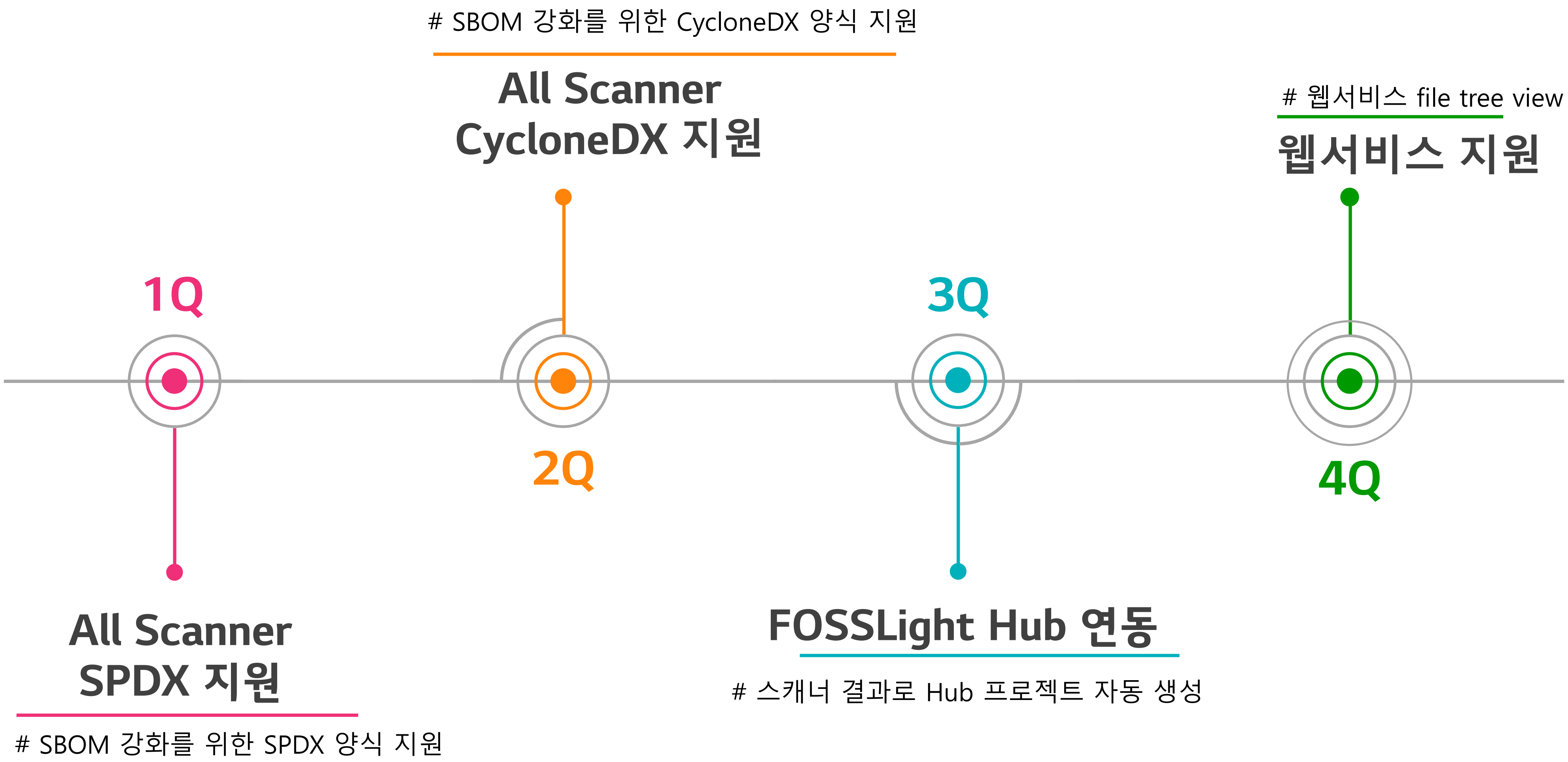
# CycloneDX 예



```json
{
    "$schema": "http://cyclonedx.org/schema/bom-1.2b.schema.json",
    "bomFormat": "CycloneDX",
    "specVersion": "1.2",
    "version": 1,
    "metadata": {
        "tools": [
            {
                "vendor": "cyclonedx",
                "name": "cyclonedx-php-composer",
                "version": "in-dev"
            }
        ],
        "component": {
            "bom-ref": "cyclonedx/cyclonedx-php-composer-demo-dev-master",
            "type": "application",
            "name": "cyclonedx-php-composer-demo",
            "version": "dev-master",
            "group": "cyclonedx",
            "description": "demo of cyclonedx/cyclonedx-php-composer with a pinned version of laravel/framework",
            "author": "Jan Kowalleck",
            "purl": "pkg:composer/cyclonedx/cyclonedx-php-composer-demo@dev-master"
        }
    },
    "components": [
        {
            "bom-ref": "asm89/stack-cors-1.3.0.0",
            "type": "library",
            "name": "stack-cors",
            "version": "1.3.0",
            "group": "asm89",
            "description": "Cross-origin resource sharing library and stack middleware",
            "author": "Alexander",
            "licenses": [
                {
                    "license": {
                        "id": "MIT"
                    }
                }
            ],
            "purl": "pkg:composer/asm89/stack-cors@1.3.0",
```

# 2024 FOSSLight Roadmap

# FOSSLight Scanner 2024



1Q

**All Scanner SPDX 지원**

# SBOM 강화를 위한 SPDX 양식 지원

2Q

**All Scanner CycloneDX 지원**

# SBOM 강화를 위한 CycloneDX 양식 지원

3Q

**FOSSLight Hub 연동**

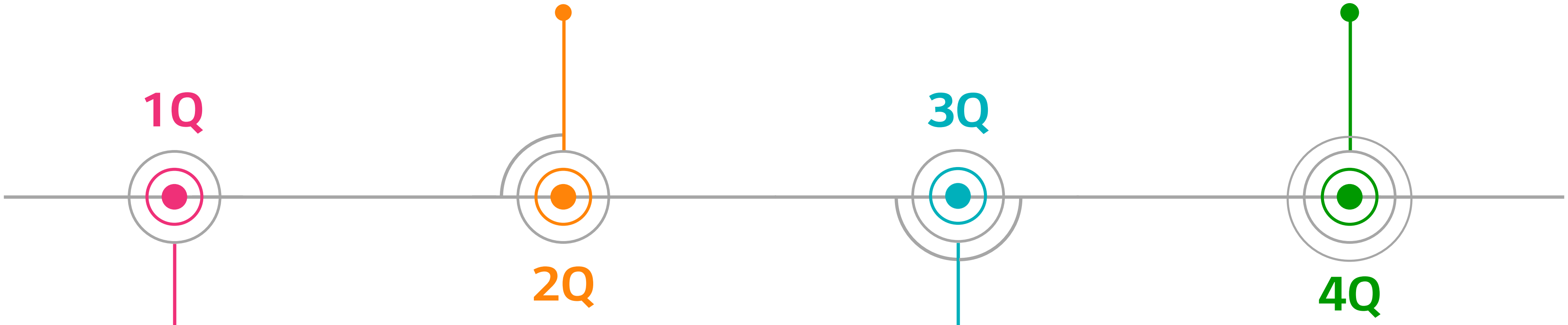
# 스캐너 결과로 Hub 프로젝트 자동 생성

4Q

**웹서비스 지원**

# 웹서비스 file tree view

# FOSSLight Hub 2024



1Q

## DB Migration

# OSORI DB Integration

2Q

## SBOM 기능 강화

# 3rd Party SBOM
# 프로젝트 내 SBOM Compare 기능

3Q

## 보안 리뷰 기능 향상

# SEC Tab 편집 강화
# 보안 담당자 기능 추가

4Q

## 품질 향상

# Vulnerability 정확도 향상
# 코드 리팩토링

# Thank You!