LGE Internal Use Only

LG Electronics Open Source Program Office

FOSSLight Hub + Scanner 연동 사례

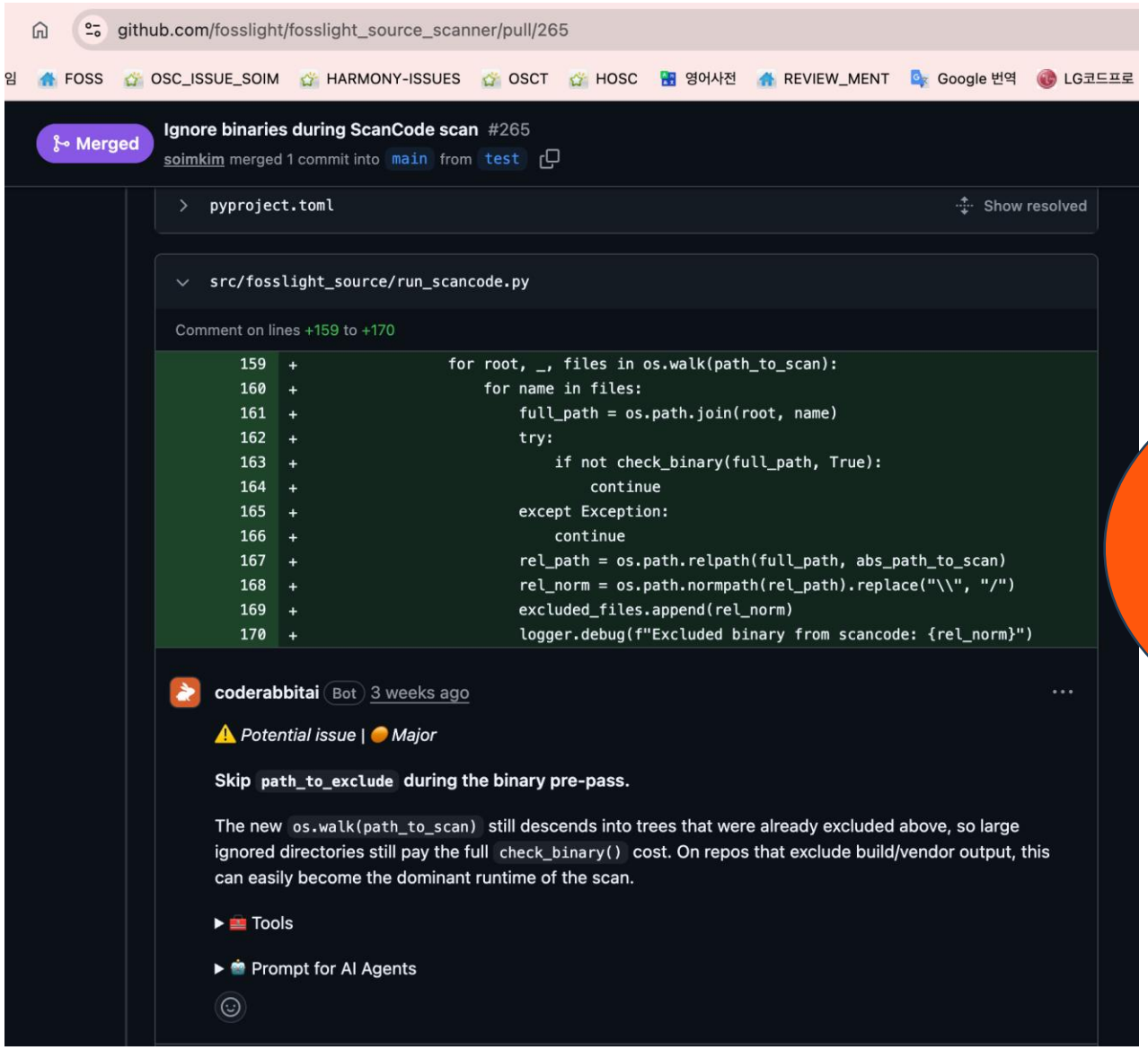
LG전자 Open Source Task 김소임

LG Open Source

CONTENTS

FOSSLight Scanner Updates

Pull Request - coderabbitai 리뷰 받기



자동으로
리뷰
받으세요

CodeRabbit

-e (exclude) 옵션: 분석 제외

- -e <pattern> : 파일 또는 폴더를 분석에서 제외

```
fosslight –e “dev/” “*.jar”
```

FOSSLight Scanner 유용한 옵션

FOSSLight Scanner – 실행 모드 선택

Modes

all (default)	Run all modes (Source, Dependency, Binary)
source	Run FOSSLight Source analysis only
dependency	Run FOSSLight Dependency analysis only
binary	Run FOSSLight Binary analysis only
compare	Compare two FOSSLight reports

분석

오픈 소스 분석

툴을 선택하여
실행 가능

Compare

SBOM
(FOSSLight Report)
비교

-s <parameter 정의 파일>

- 스캐너별 세부 옵션 설정

```
fosslight –s setting.json –p .
```

fosslight_scanner / tests / setting.json

woocheol-lge Update setting.json

Code | Blame | 22 lines (22 loc) · 510 Bytes

```
{
  "mode": ["binary", "source"],
  "path": ["tests"],
  "dep_argument": "",
  "output": "test_result_dir",
  "format": ["excel"],
  "link": "",
  "db_url": "",
  "timer": false,
  "raw": true,
  "core": -1,
  "no_correction": false,
  "correct_fpath": "",
  "ui": false,
  "exclude": ["test", "sample_license.txt"],
  "selected_source_scanner": "scancode",
  "source_write_json_file": true,
  "source_print_matched_text": true,
  "source_time_out": 120,
  "binary_simple": false,
  "recursive_dep": false
}
```

40524 B436 7EC 0AE92E4D

https://github.com/fosslight/fosslight_scanner/blob/main/tests/setting.json

분석 결과에 오검출이?

OSS Name : fosslight_scanner, OSS Version : 1.0, License : Apache-2.0

fosslight_scanner / src / fosslight_scanner / cli.py

dd-jy Add dependency recursive mode

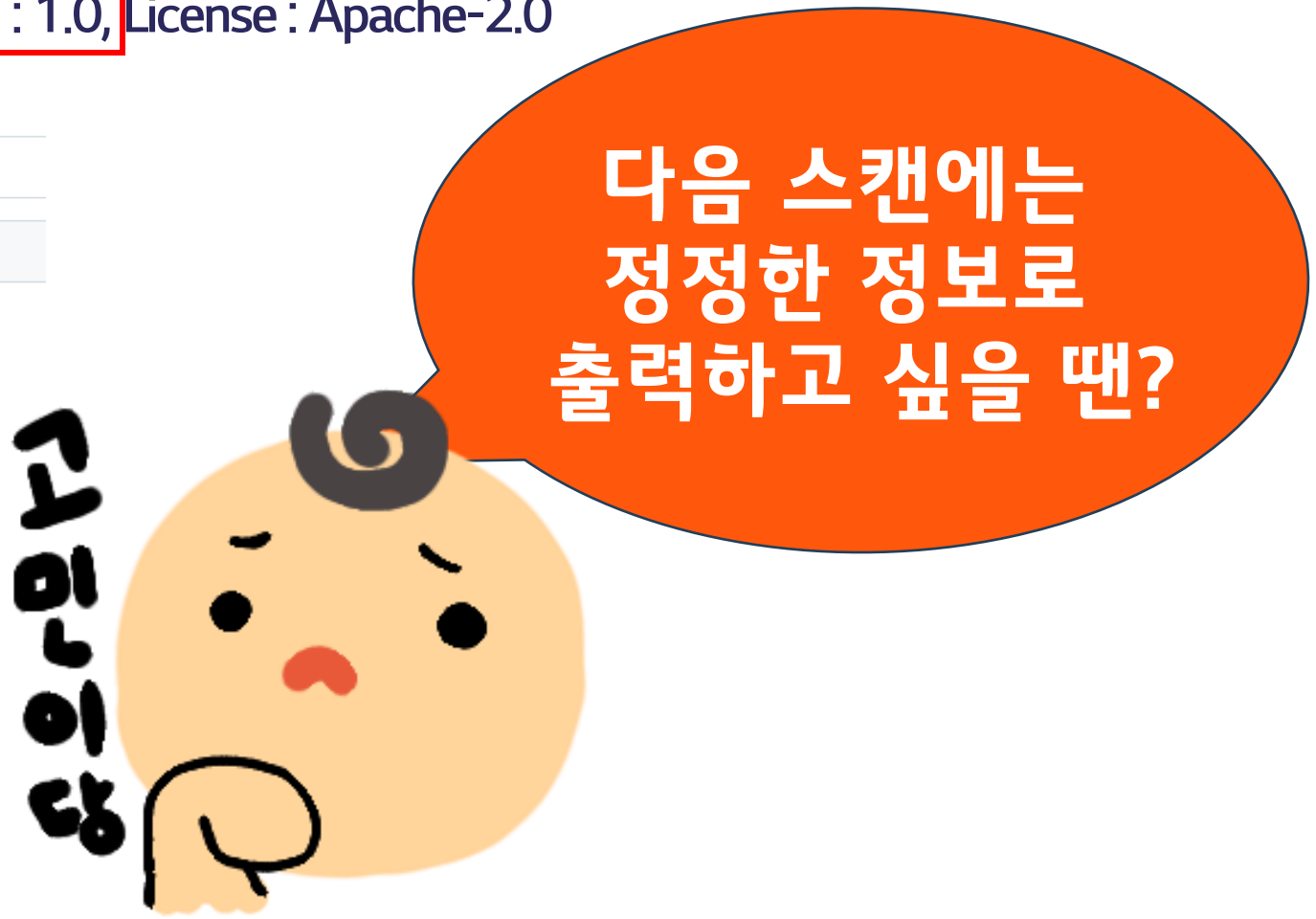
Code Blame 138 lines (123 loc) · 6.75 KB

```python
#!/usr/bin/env python
# -*- coding: utf-8 -*-
# Copyright (c) 2022 LG Electronics Inc.
# SPDX-License-Identifier: Apache-2.0
import sys
import json
import os
import os.path
from argparse import ArgumentParser

from ._help import print_help_msg
from .fosslight_scanner import run_main, PKG_NAME
from ._parse_setting import parse_setting_json
from fosslight_util.help import print_package_version


def set_args(mode, path, dep_argument, output, format, link, db_url, timer,
             raw, core, no_correction, correct_fpath, ui, setting, exclude_path,
             recursive_dep):

    selected_source_scanner = "all"
    source_write_json_file = False
    source_print_matched_text = False
    source_time_out = 120
    binary_simple = False
```



LG Electronics Open Source Program Office

sbom-info.yaml

스캔 결과 정정/제외 설정 방법
단, FOSSLight Dependency Scanner에는 적용되지 않음

- sbom-info.yaml 이 분석 Top directory 에 위치하면 이 정보를 우선 적용

```yaml
libidn: # 오픈소스인 경우
- version: "1.5"
  source name or path:
  - "src/libidn/*"
  - "b.c"
  license:
  - "GPL-3.0"
  - "LGPL-2.1"
  download location: "http://ftp.gnu.org/gnu/libidn"
  homepage: "https://www.gnu.org/software/libidn"
  copyright text: "Copyright 2002-2007, Simon Josefsson"
```

```yaml
'-': # 특정 경로를 스캔 결과에서 제외하는 경우
- version: ''
  exclude: True
  source name or path:
  - "build/*"
  - "test/*"
```

- Sbom-info.yaml 적용하지 않고자 할 땐, --no_correction
- 다른 파일명으로 적용할 땐 –correct_fpath <path>

https://fosslight.org/fosslight-guide/scanner/etc/sbom_info.html?highlight=sbom-info.yaml

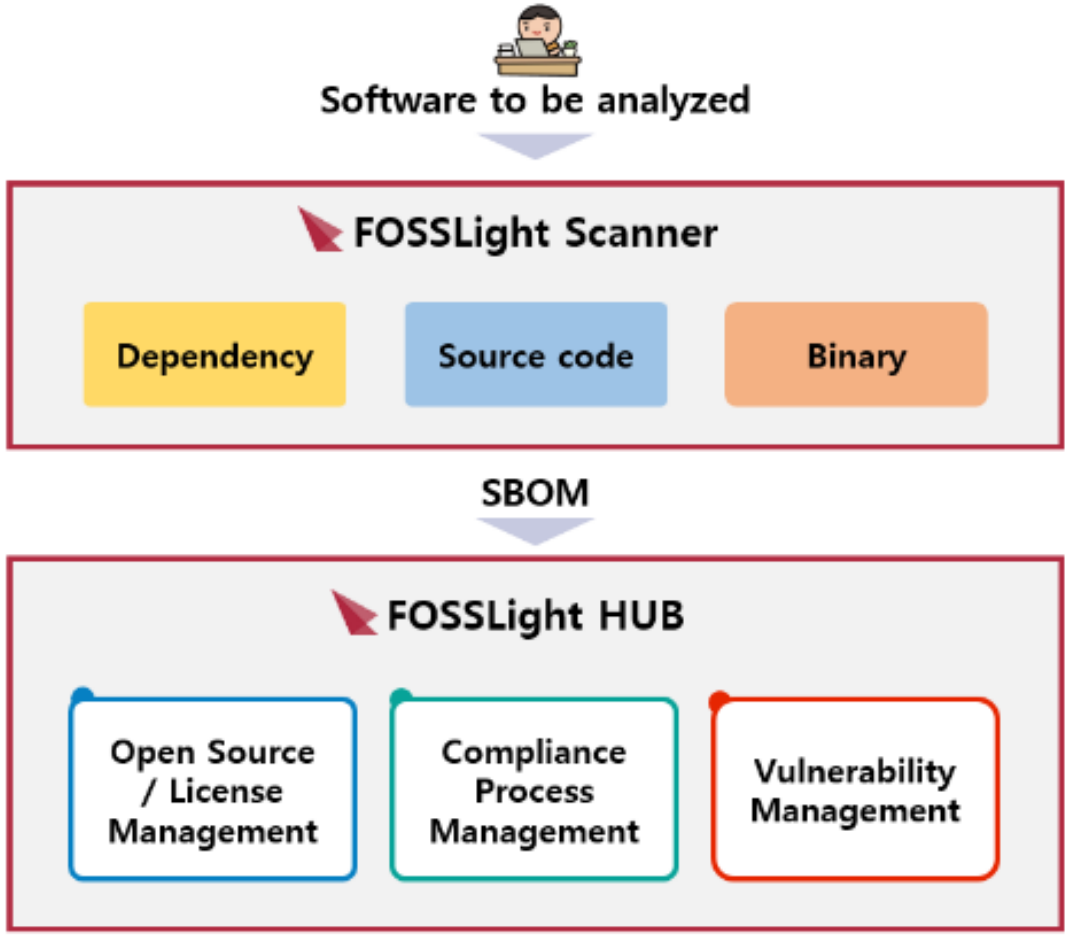
-w <url>

- Git clone 또는 wget 가능한 링크를 입력
- 소스를 다운로드 받아 분석 결과 추출

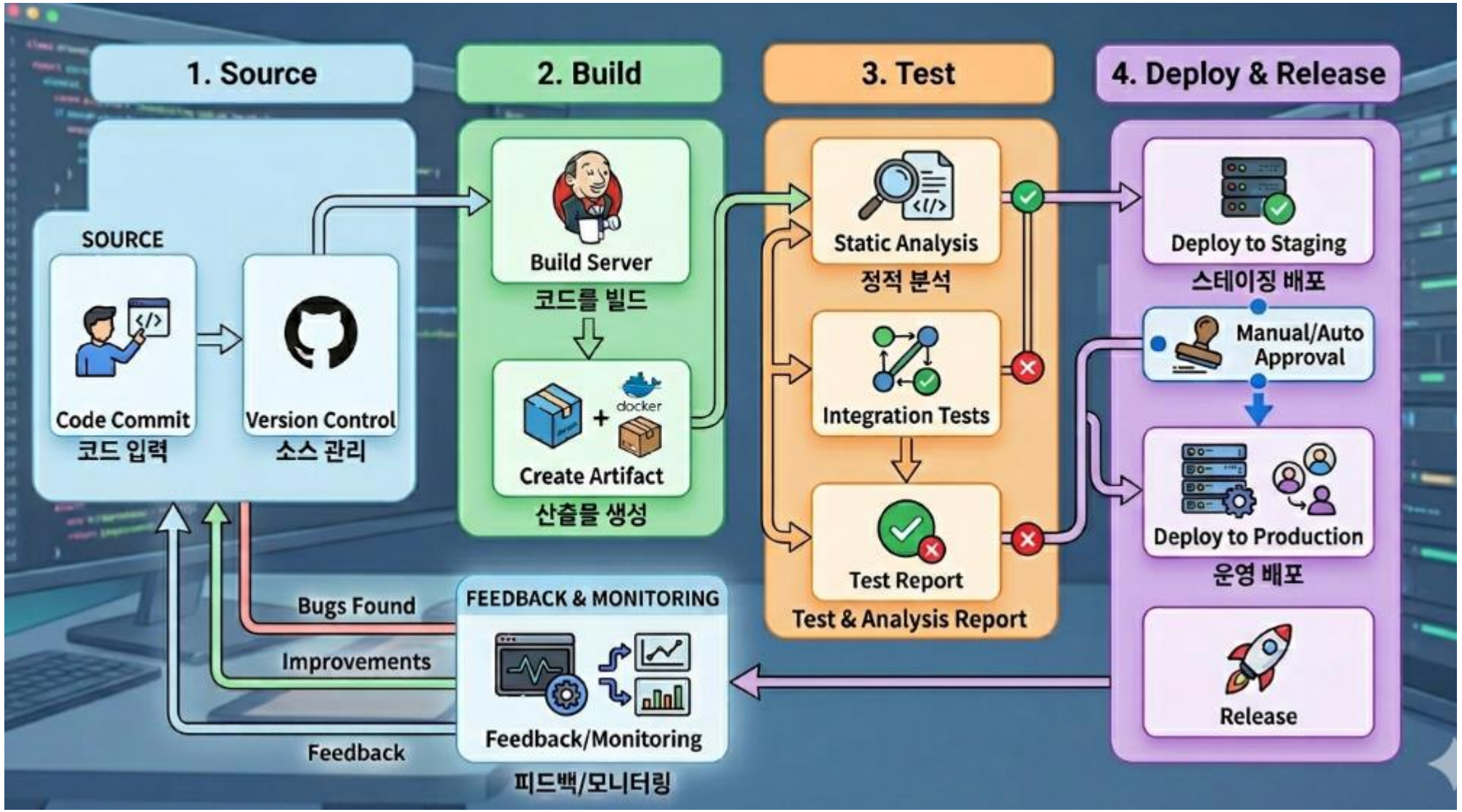
```
fosslight –w “http://github.com/fosslight/fosslight_scanner”
```

FOSSLight Scanner + Hub 연동

FOSSLight Scanner와 FOSSLight Hub 연동

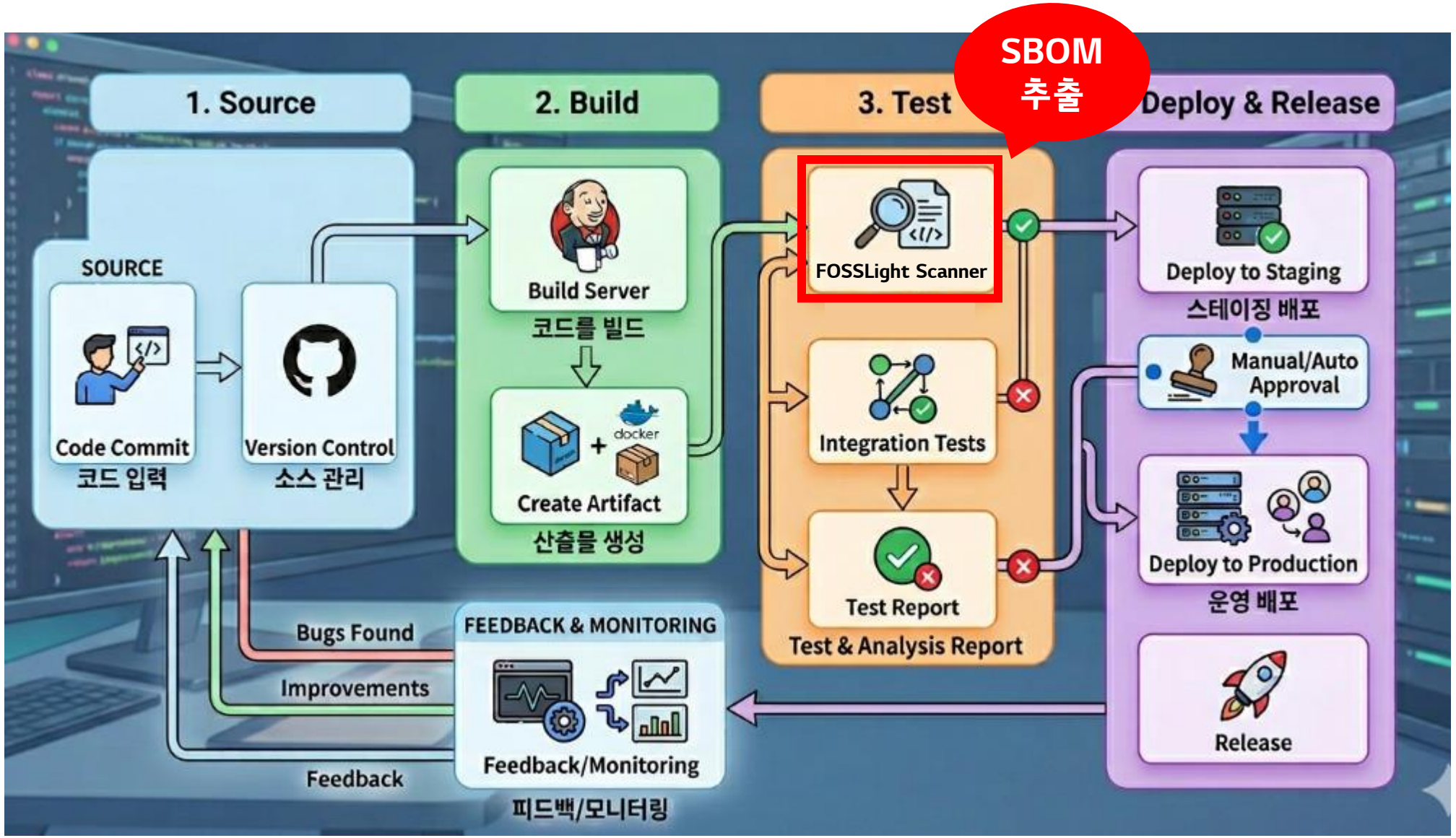


CI/CD 통상적인 구조



LG Electronics Open Source Program Office

CI/CD with FOSSLight



SBOM 추출

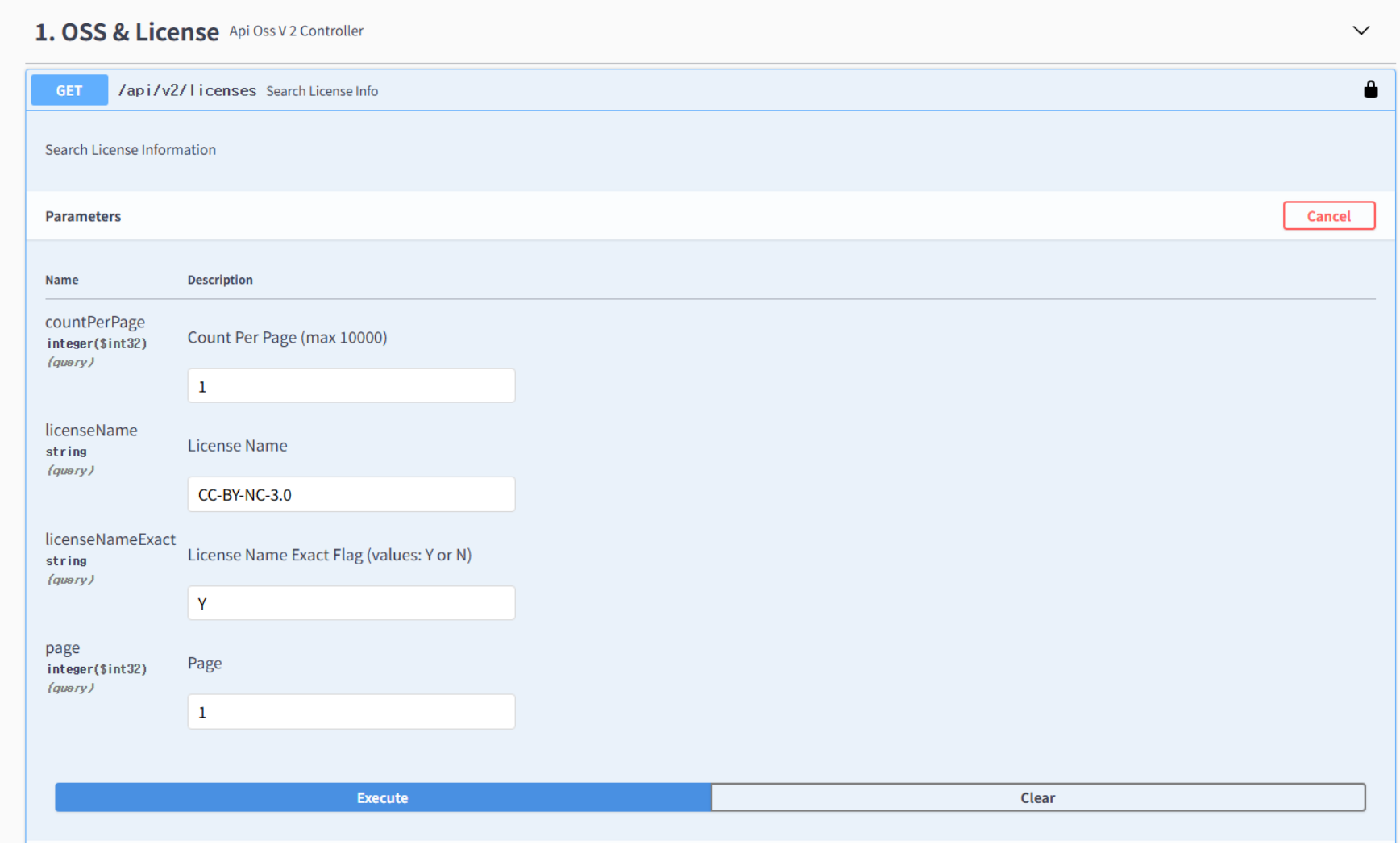
- OSS Name, Version, License, Download location 추출

Package URL	OSS Name	OSS Version	License	ownload	Homepag	Copyright	Exclude	Comment	Depends On
pkg:npm/%40types/node@9.6.57	npm:@types/node	9.6.57	MIT	ttps://gith	https://www.npmjs.com/package/			direct	
pkg:npm/agent-base@6.0.2	npm:agent-base	6.0.2	MIT	ttps://gith	https://www.npmjs.com/package/			transitive	pkg:npm/debug@4.3.6
pkg:npm/asap@2.0.6	npm:asap	2.0.6	MIT	ttps://gith	https://www.npmjs.com/package/			transitive	
pkg:npm/axios@0.21.4	npm:axios	0.21.4	MIT	ttps://gith	https://www.npmjs.com/package/			direct	pkg:npm/follow-redirects@1.15.6
pkg:npm/buffer-equal-constant-time@1.	npm:buffer-equal-constant-time	1.0.1	BSD-3-Cla	ttps://gith	https://www.npmjs.com/package/			transitive	
pkg:npm/dayjs@1.11.12	npm:dayjs	1.11.12	MIT	ttps://gith	https://www.npmjs.com/package/			direct	
pkg:npm/debug@4.3.6	npm:debug	4.3.6	MIT	ttps://gith	https://www.npmjs.com/package/			transitive	pkg:npm/ms@2.1.2
pkg:npm/define-data-property@1.1.4	npm:define-data-property	1.1.4	MIT	ttps://gith	https://www.npmjs.com/package/			transitive	pkg:npm/es-define-property@1.0.0,pkg:npm/es-errors@1.3.0,pkg:npm/gopd@1.0.1
pkg:npm/ecdsa-sig-formatter@1.0.11	npm:ecdsa-sig-formatter	1.0.11	Apache-2.	ttps://gith	https://www.npmjs.com/package/			transitive	pkg:npm/safe-buffer@5.2.1
pkg:npm/es-define-property@1.0.0	npm:es-define-property	1.0.0	MIT	ttps://gith	https://www.npmjs.com/package/			transitive	pkg:npm/get-intrinsic@1.2.4

LG Electronics Open Source Program Office

FOSSLight Hub API

- License name으로 License 정보 조회



https://fosslight.org/hub-guide/advanced/2_rest_api_2.html

FOSSLight Hub API

- API > License 조회
  - Restriction 여부를 체크

Request URL

```
https://osc.lge.com/api/v2/licenses?countPerPage=1&licenseName=CC-BY-NC-3.0&licenseNameExact=Y&page=1
```

Server response

Code | Details

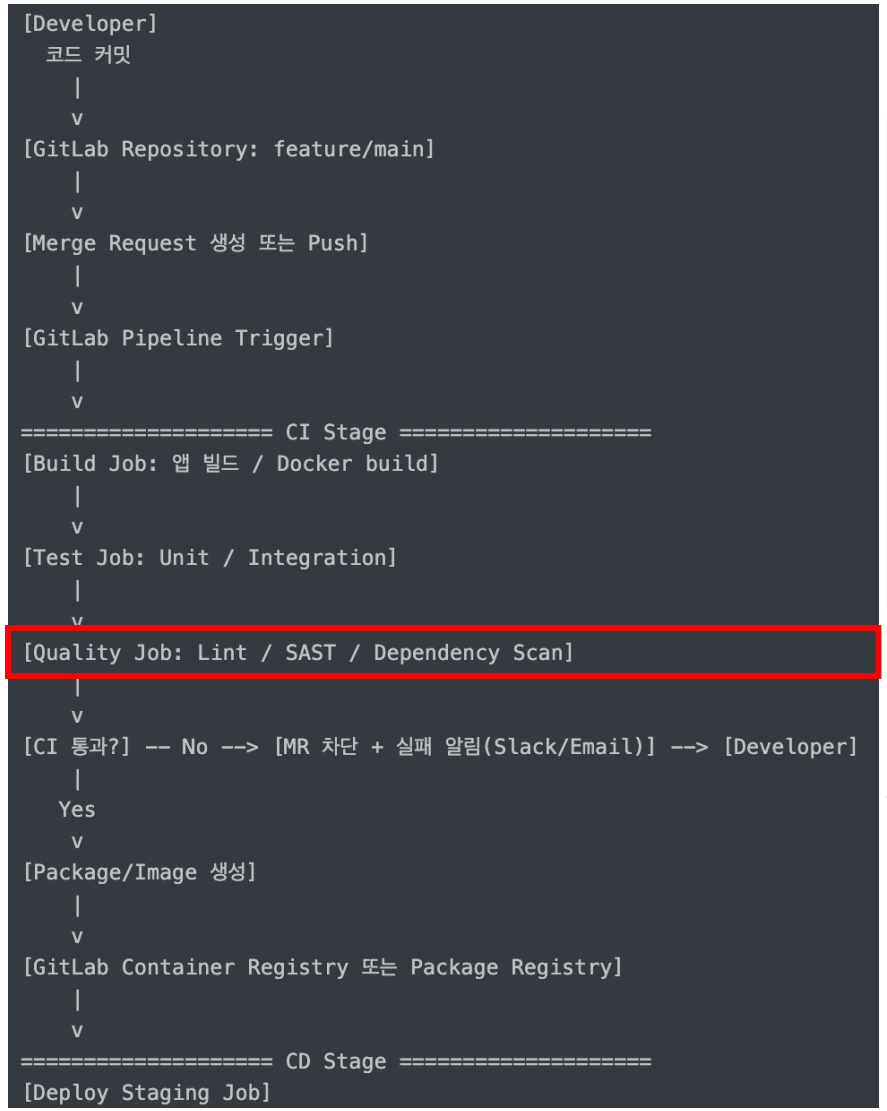
200

Response body


```
License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.₩r₩n₩r₩nExcept for the limited purpose of indicating to the public that the Work is licensed under the CCPL, Creative Commons does not authorize the use by either party of the trademark ₩"Creative Commons₩" or any related trademark or logo of Creative Commons without the prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time. For the avoidance of doubt, this trademark restriction does not form part of the License.₩r₩n₩r₩nCreative Commons may be contacted at http://creativecommons.org/.₩r₩n₩r₩nStandard License Header₩r₩nThere is no standard license header for the license",
      "licenseIdentifier": "CC-BY-NC-3.0",
      "homepageUrl": "https://spdx.org/licenses/CC-BY-NC-3.0.html",
      "description": "Cannot USE because of non-commercial ",
      "creator": "박원재/책임연구원/SW공학(연)Open Source Task",
      "modifier": "김소임/책임연구원/SW공학(연)Open Source Task",
      "created": "2017-05-10 19:21:50",
      "modified": "2024-08-05 11:16:57",
      "restrictions": [
        "Non-commercial only"
      ],
      "licenseNickname": "CC BY NC 3.0",
      "obligations": [
        "Y",
        "N"
      ],
      "attribution": ""
    }
```


https://fosslight.org/hub-guide/advanced/2_rest_api_2.html

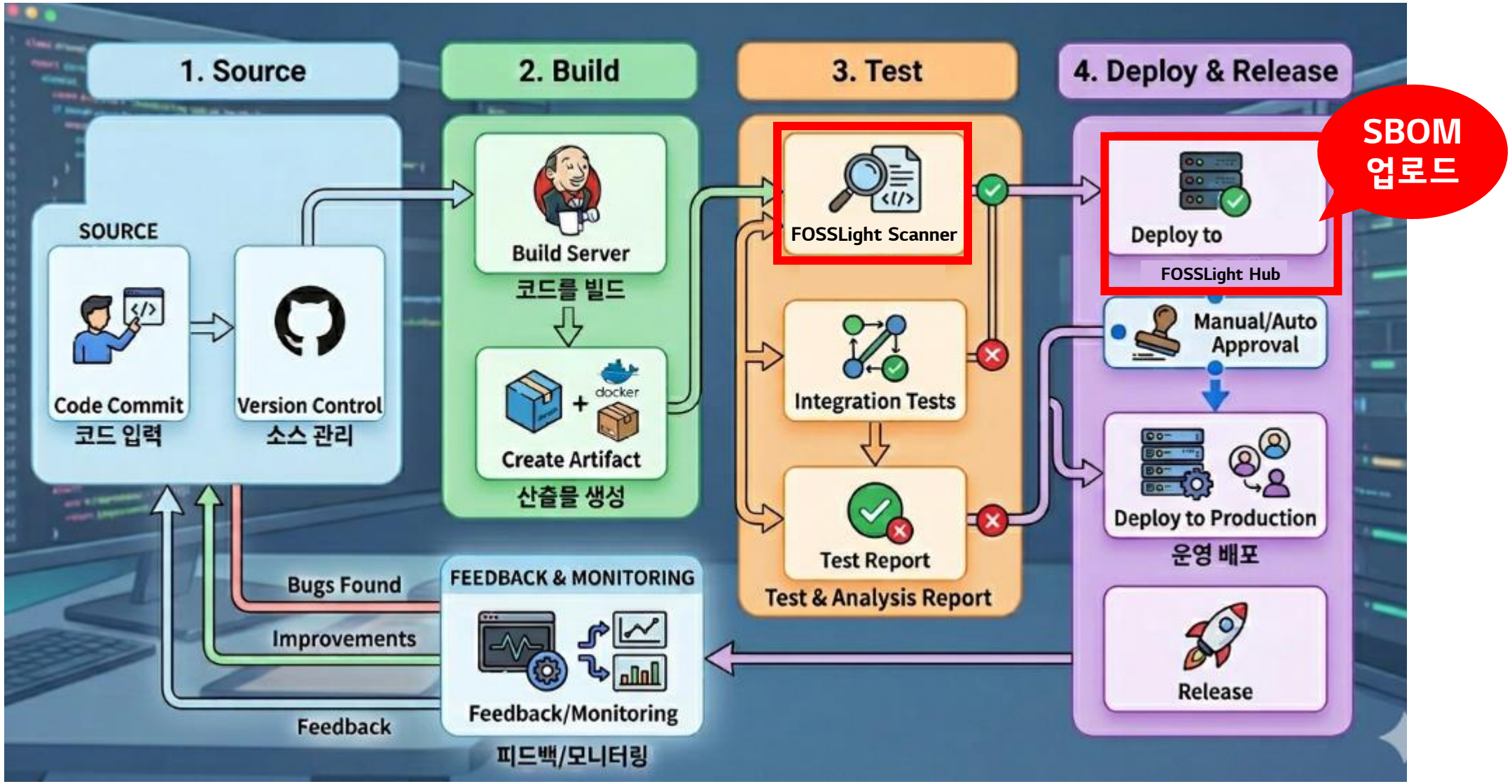
CI/CD with FOSSLight



FOSSLight Scanner 분석 › SBOM 추출

API로 License 정보 조회하여
Restriction 있는 License (ex. Non-commercial) 알림

CI/CD with FOSSLight



CI/CD with FOSSLight

```
[Developer]
  코드 커밋
    |
    v
[GitLab Repository: feature/main]
    |
    v
[Merge Request 생성 또는 Push]
    |
    v
[GitLab Pipeline Trigger]
    |
    v
==================== CI Stage ====================
[Build Job: 앱 빌드 / Docker build]
    |
    v
[Test Job: Unit / Integration]
    |
    v
[Quality Job: Lint / SAST / Dependency Scan]
    |
    v
[CI 통과?] -- No --> [MR 차단 + 실패 알림(Slack/Email)] --> [Developer]
    |
   Yes
    v
[Package/Image 생성]
    |
    v
[GitLab Container Registry 또는 Package Registry]
    |
    v
==================== CD Stage ====================
[Deploy Staging Job]
```

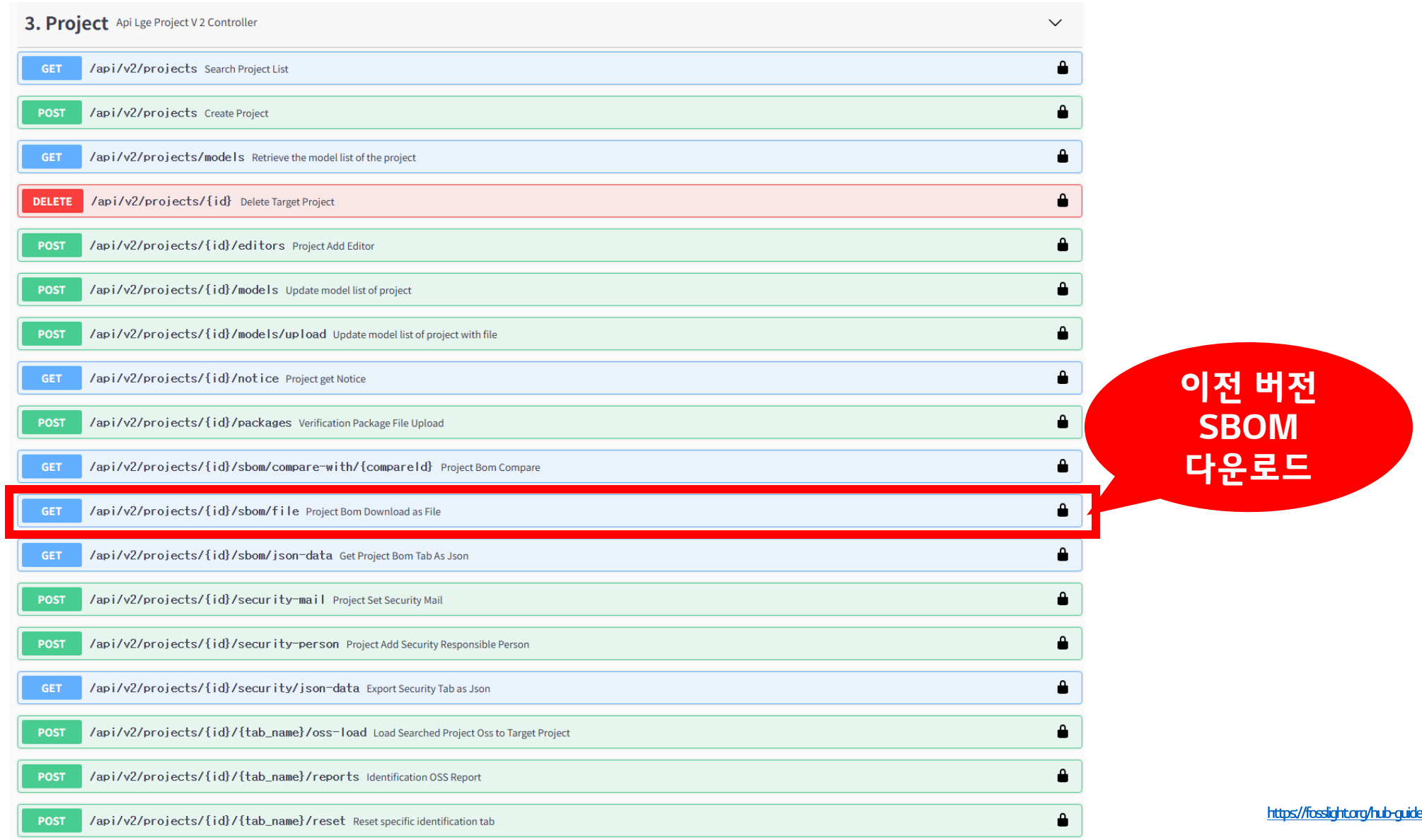
FOSSLight Hub API를 이용한 SBOM 릴리즈

1. 이전 버전의 SBOM 파일 다운로드

2. FOSSLight Scanner SBOM Compare 기능으로
이전 버전 대비 **OSS 변경 사항** 메일 알림

3. 신규 SBOM을 업로드

FOSSLight Hub API



이전 버전 SBOM 다운로드

https://fosslight.org/hub-guide/advanced/2_rest_api_2.html

FOSSLight Hub API

3. Project Api Lge Project V 2 Controller

GET	/api/v2/projects	Search Project List
POST	/api/v2/projects	Create Project
GET	/api/v2/projects/models	Retrieve the model list of the project
DELETE	/api/v2/projects/{id}	Delete Target Project
POST	/api/v2/projects/{id}/editors	Project Add Editor
POST	/api/v2/projects/{id}/models	Update model list of project
POST	/api/v2/projects/{id}/models/upload	Update model list of project with file
GET	/api/v2/projects/{id}/notice	Project get Notice
POST	/api/v2/projects/{id}/packages	Verification Package File Upload
GET	/api/v2/projects/{id}/sbom/compare-with/{compareId}	Project Bom Compare
GET	/api/v2/projects/{id}/sbom/file	Project Bom Download as File
GET	/api/v2/projects/{id}/sbom/json-data	Get Project Bom Tab As Json
POST	/api/v2/projects/{id}/security-mail	Project Set Security Mail
POST	/api/v2/projects/{id}/security-person	Project Add Security Responsible Person
GET	/api/v2/projects/{id}/security/json-data	Export Security Tab as Json
POST	/api/v2/projects/{id}/{tab_name}/oss-load	Load Searched Project Oss to Target Project
POST	/api/v2/projects/{id}/{tab_name}/reports	Identification OSS Report
POST	/api/v2/projects/{id}/{tab_name}/reset	Reset specific identification tab

최신 버전
SBOM
업로드

https://fosslight.org/hub-guide/advanced/2_rest_api_2.html

SBOM Compare

- OSS 변경 내역을 Html 포맷으로 추출하여 메일에 첨부

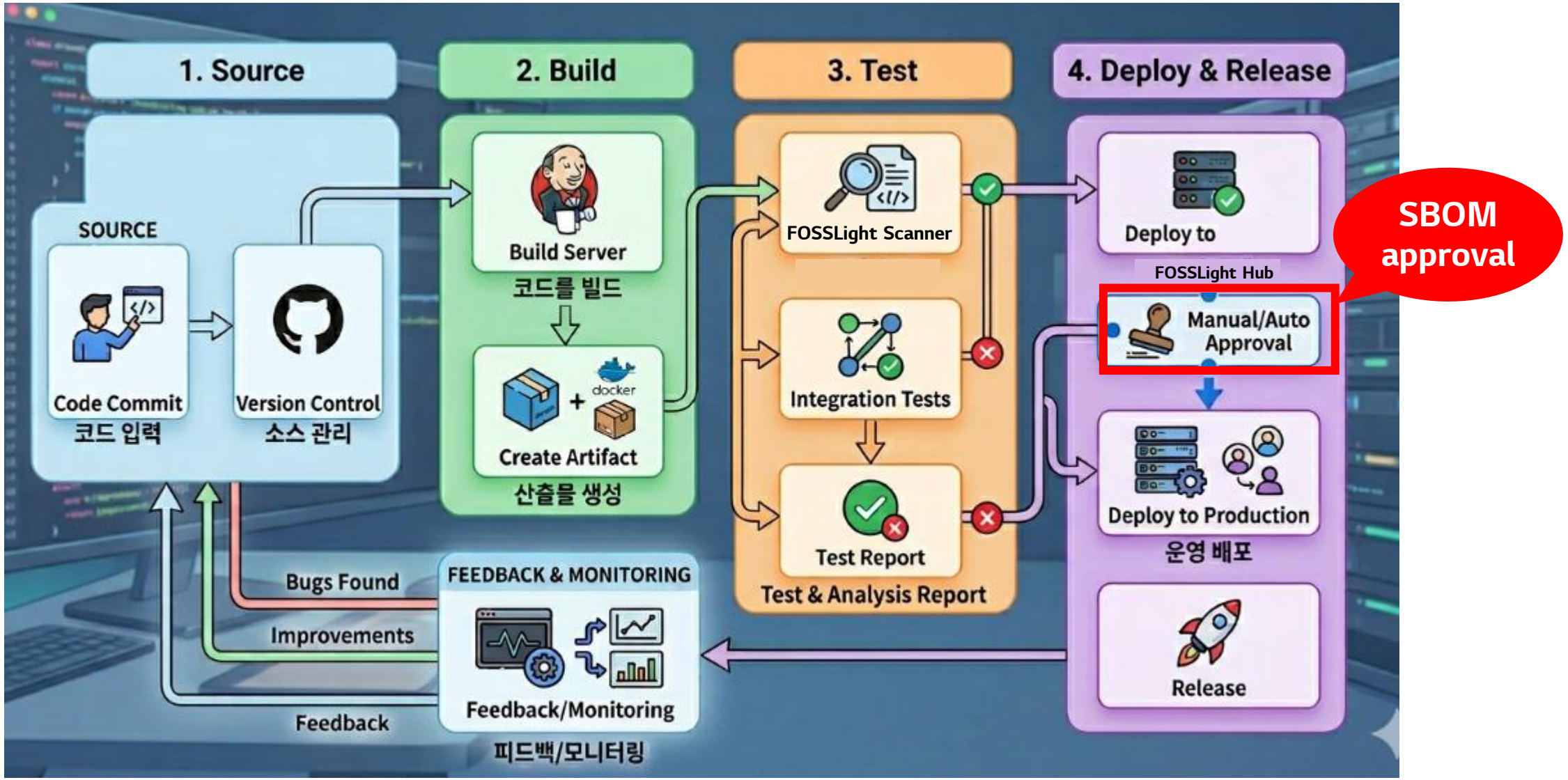
FOSSLight Scanner Compare Result

BOM Compare Result

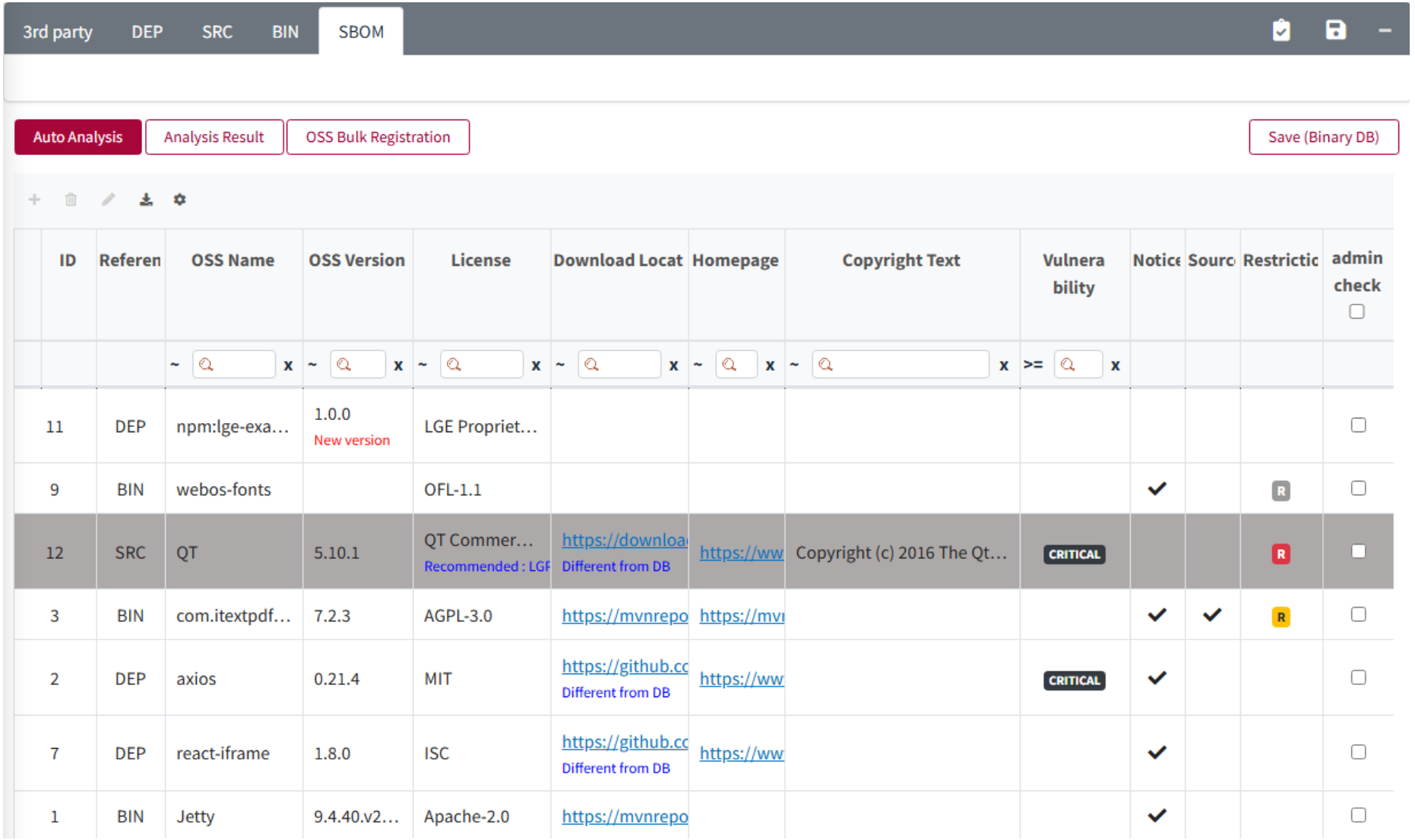
- Before FOSSLight Report file: /home/soim/git/scanner/fosslight_scanner/tests/fosslight_raw_data/fosslight_report_230308_prj-5204.yaml
- After FOSSLight Report file: /home/soim/git/scanner/fosslight_scanner/tests/fosslight_raw_data/fosslight_report_230308_prj-5203.yaml

Status	OSS_Before	License_Before	OSS_After	License_After
add			FFT	FFT License
delete	JsonCPP(1.8.4)	MIT		
change	gson(2.8.2)	Apache-2.0	gson(3.1)	Apache-2.0

CI/CD with FOSSLight

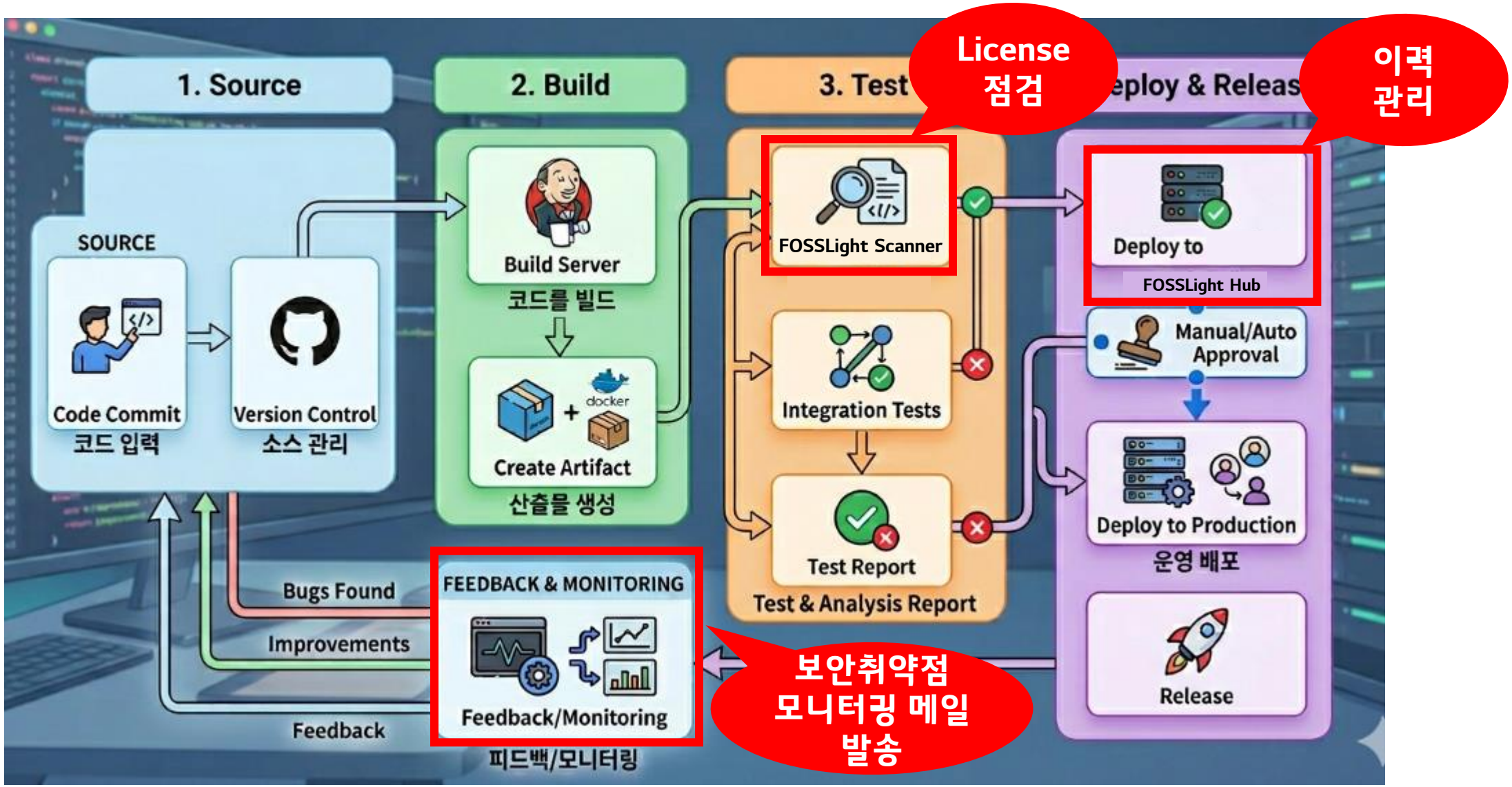


SBOM 리뷰 & Approval



ID	Referen	OSS Name	OSS Version	License	Download Locat	Homepage	Copyright Text	Vulnera bility	Notice	Sourc	Restrictic	admin check
11	DEP	npm:lge-exa…	1.0.0 New version	LGE Propriet…								
9	BIN	webos-fonts		OFL-1.1					✓		R	
12	SRC	QT	5.10.1	QT Commer… Recommended : LGF	https://downloa Different from DB	https://ww	Copyright (c) 2016 The Qt…	CRITICAL			R	
3	BIN	com.itextpdf…	7.2.3	AGPL-3.0	https://mvnrepo	https://mvı			✓	✓	R	
2	DEP	axios	0.21.4	MIT	https://github.cc Different from DB	https://ww		CRITICAL	✓			
7	DEP	react-iframe	1.8.0	ISC	https://github.cc Different from DB	https://ww			✓			
1	BIN	Jetty	9.4.40.v2…	Apache-2.0	https://mvnrepo				✓			

CI/CD with FOSSLight



보안취약점 모니터링 메일

FOSSLight Hub Notification

[TEST][OSC] Vulnerability Discovered : "(5230)user-test-android (3.0)"

Comment

이 프로젝트에서 사용된 Open Source 중 다음과 같은 보안 취약점이 발견되었습니다.

	Registered Data
Project Name	user-test-android
Project Version	3.0
Security Mail	Enable
Security Responsible Person	
Operating System	Linux
Distribution Type / Network Service Only?	General / N
Distribution Site	opensource.lge.com
OSS Notice	Platform-generated
Priority	P2
Creator	CTO SW센터 시스템관리자(oscAdmin)
Division	CTO SW센터
Reviewer	CTO SW센터 시스템관리자(oscAdmin)

« Vulnerability Information »

OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
ffmpeg	4.4.1	CVE-2026-40962	9.8	FFmpeg before 8.1 has an integer overflow and resultant out-of-bounds write via CENC (Common Encryption) subsample data to libavformat/mov.c.	2026-04-16	2026-04-20

Coming Soon...

- FOSSLight Scanner 네버 엔딩 레볼루션


Hello FOSSLight

Q&A