FOSSLight Hub 2.0

지금까지의 관리 툴은 잊어라!!

—

민경선 책임 연구원
LG 전자

CONTENTS

01
FOSSLight Hub

01 FOSSLight Hub란?

- Open Source Compliance/Security Process를 위한 오픈소스 통합 관리 시스템
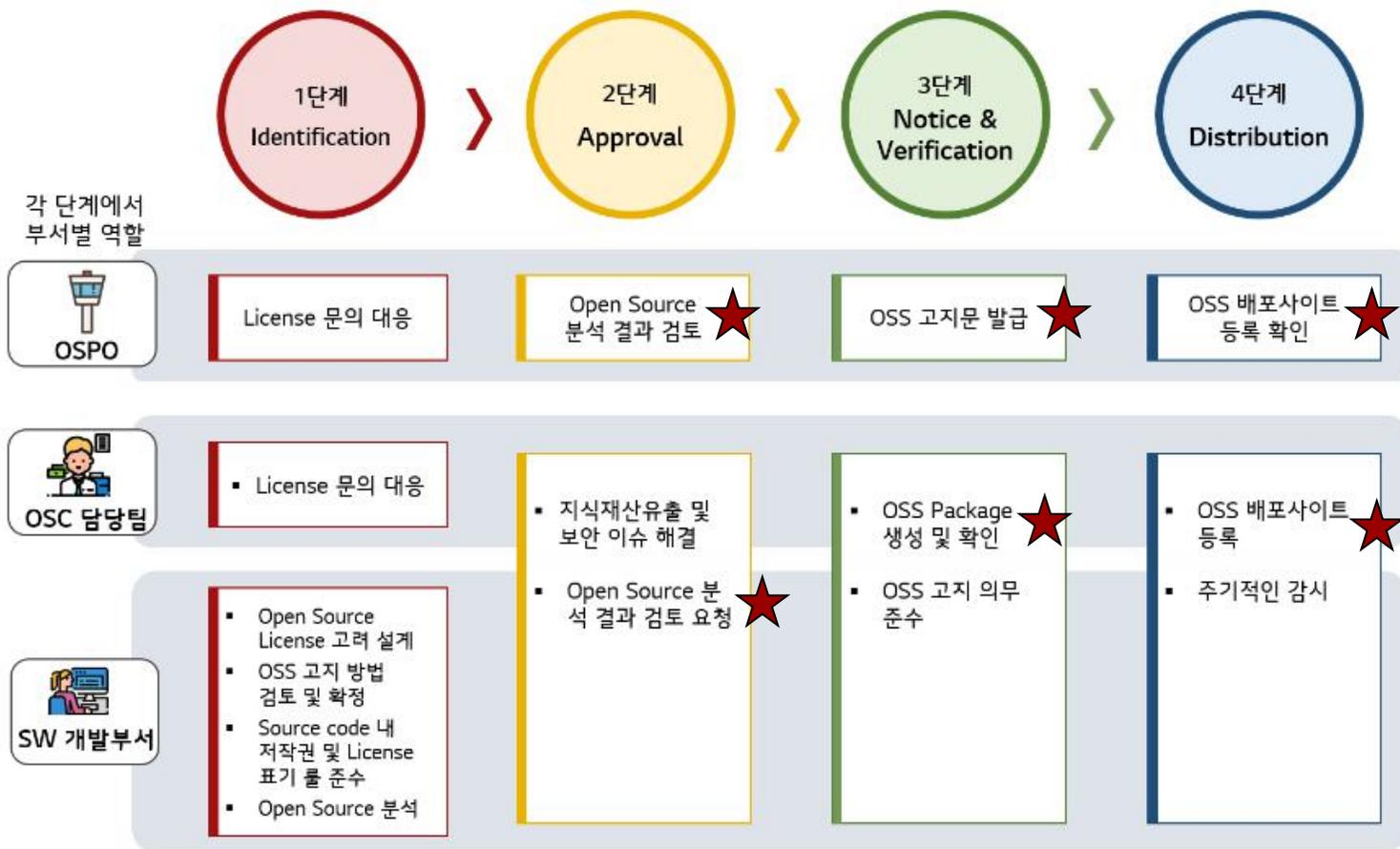
01 OSC Process
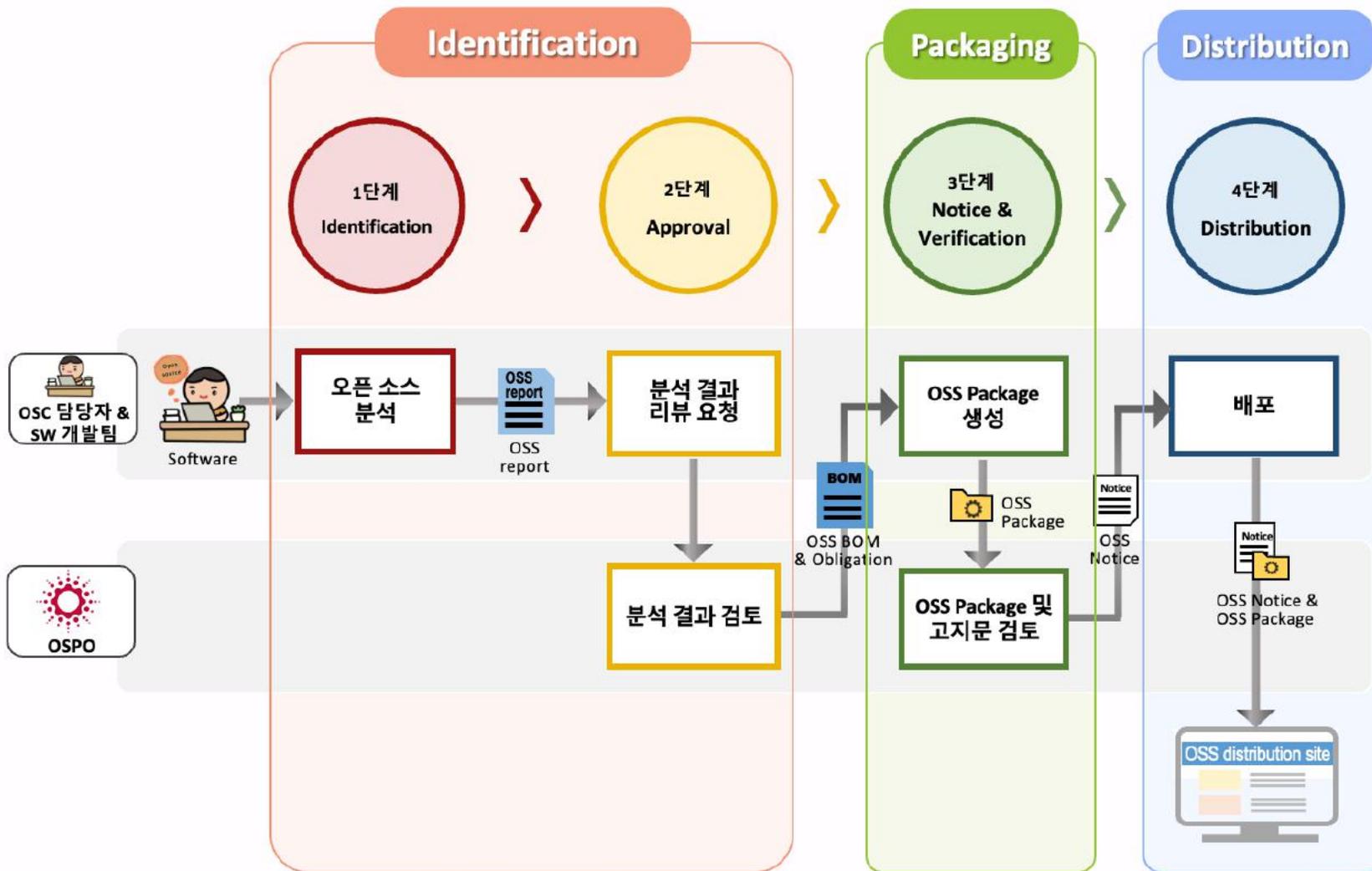
01 FOSSLight Hub 주요 기능

검토 및 진단

오픈소스, 라이선스 관리
- 오픈소스 정보 통합 관리
- 라이선스 의무 사항 및 제약 사항 확인
- 오픈 소스 일괄 등록

보안 취약점 관리
- 프로젝트별 발견된 보안취약점 관리
- 프로젝트별 보안취약점 변경사항 모니터링 및 자동 메일 알림
- 보안취약점 조회

보고 및 조치

컴플라이언스 프로세스 관리
- OSS 고지문 발급
- 다양한 형태의 고지문 제공 (HTML, TEXT, SPDX)
- 연계 배포 사이트 자동 업로드

SBOM 작성 및 관리
- SPDX, CycloneDX 문서 지원
- 다양한 내보내기 형식 지원 (PDF, HTML, TEXT)
- SBOM 변경사항 추적 가능

예방

공급망 관리
- 3rd party로부터 전달받은 Software의 오픈소스 정보 (SBOM) 등록 및 관리
- 오픈소스 확약서 관리
- 프로젝트 자동 연계

사전 점검
- 오픈소스 자동 분석
- 라이선스 자동 검출
- 라이선스 의무사항 및 보안취약점 알림

02 FOSSLight Hub 2.0 Policy

enterprise.fosslight.org

02 FOSSLight Hub 2.0 UI

03
Dependency

03 PURL 정보 제공

03 PURL 정보 제공

Open Source Information

OSS Name ⓘ	aiokafka
Nickname	pypi:aiokafka
OSS Version	0.12.0
Vulnerability Info ◂	
OSS Type	

Declared License

	License	Restricti
	Apache-2.0	

Detected License	
Restriction	
License Type	Permissive
Obligation	🗎
Download Location	https://pypi.org/project/aiokafka (pkg:pypi/aiokafka)
Home Page	https://github.com/aio-libs/aiokafka
Copyright	Copyright 2016 Taras Voinarovskyi
Summary Description	
Important Notes	
Attribution	

03 Dependen

The Dependency Tree supports a maximum depth of 5 levels.

Dependency Tree (Package Url)	+ Expand All	− Collapse All

	pkg:pypi/pillow@10.4.0
−	pkg:pypi/fastapi@0.115.8
−	> pkg:pypi/starlette@0.45.3
−	> pkg:pypi/anyio@3.7.1
	pkg:pypi/sniffio@1.3.0
	pkg:pypi/idna@3.4
	pkg:pypi/exceptiongroup@1.1.3
−	> pkg:pypi/pydantic@2.4.2
	pkg:pypi/annotated-types@0.6.0
−	> pkg:pypi/pydantic-core@2.10.1
	pkg:pypi/typing-extensions@4.8.0
	pkg:pypi/typing-extensions@4.8.0
	pkg:pypi/typing-extensions@4.8.0
	pkg:pypi/jsondiff@2.0.0
−	pkg:pypi/requests@2.31.0
	pkg:pypi/certifi@2025.1.31
	pkg:pypi/urllib3@1.26.18
	pkg:pypi/idna@3.4
	pkg:pypi/charset-normalizer@3.3.0

Page 1 of 1   200 ▾   Count : 62

3rd party | DEP | SRC | BIN | BOM

FOSSLight Report   fosslight_re
2025-09-30

	ID	Package URL	OSS Name
☐		~ 🔍	x ~ 🔍
☐	39	pkg:pypi/pillow@10...	pillow
☐	5	pkg:pypi/aioitertool...	aioitertools
☐	47	pkg:pypi/pymysql@...	PyMySQL
☐	52	pkg:pypi/rsa@4.9.1	python-rsa
☐	3	pkg:pypi/aiobotocor...	aiobotocore
☐	24	pkg:pypi/fastapi@0....	fastapi
☐	32	pkg:pypi/jsondiff@2...	jsondiff
☐	51	pkg:pypi/requests@...	requests

04
Security

04 Security 탭

- 프로젝트별 보안취약점 관리

ID	Project Name	Status	OSC Process	Download ⓘ	Security
747	datafile collector	Progress	Identification > Packaging		Need to resolve(9.8)
737	test_sec_mail	Request	Identification > Packaging		Discovered(N/A)
736	Test empty project (1.0)	Request	Identification > Packaging		Discovered(N/A)
735	dep-test (1)	Request	Identification > Packaging		Discovered(N/A)
734	qwer (1.0)	Request	Identification > Packaging		Discovered(N/A)
733	test prj	Request	Identification > Packaging		Need to resolve(9.9)
732	my project coffee	Request	Identification > Packaging		Need to resolve(9.8)
731	a123sdfs	Progress	Identification > Packaging		Need to resolve(7.5)

- Need to resolve(XX) : 기준 점수 이상 보안취약점이 존재하는 경우
- Discovered(XX) : 기준 점수 이상 보안취약점이 존재하지 않는 경우
- Resolved(XX) : Need to resolve탭 기준 점수 이상 취약점이 모두 'Fixed' resolution인 경우
- BOM탭 기준임. 각 상태 (XX) 안에서 프로젝트 내 vulnerability max score 확인 가능함

04 Security - Overview

전체 CVE ID의 Vulnerability 점수 구간 별 Count

Vulnerability Resolution 그래프
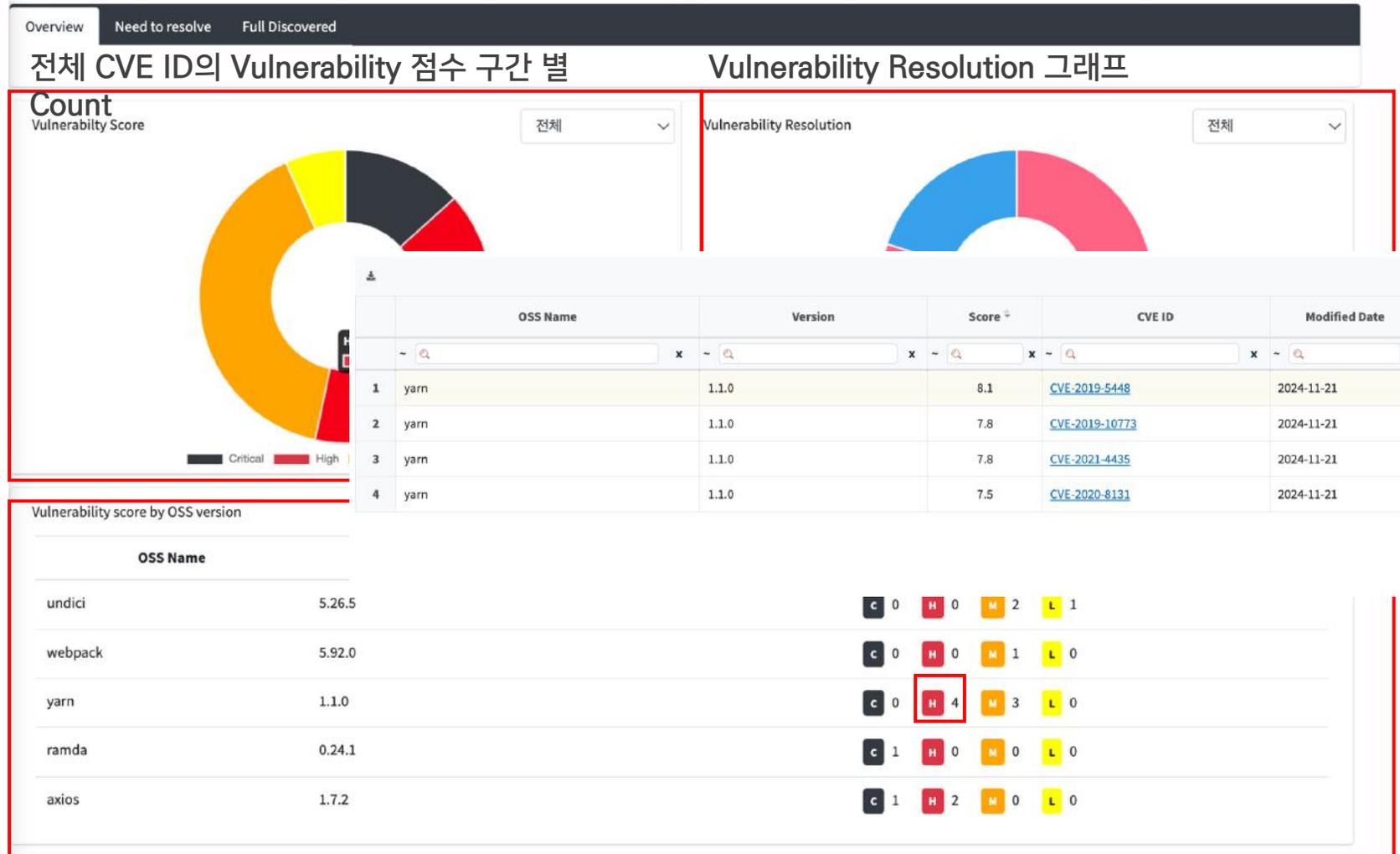
OSS 버전별로 Vulnerability 점수에 대한 count 및 상세 정보 제공

04 Security - Need to resolve / Full discovered

- Need to resolve : 기준 점수 이상인 CVE ID 목록 확인 가능

- Full Discovered : 검출된 전체 CVE ID 목록

04 신규 보안취약점 발견시 메일 발송

- Security Vulnerability Score 이상인 신규 보안취약점 발견시, 알림 메일 발송

04 보안취약점 메일링 및 담당자 설정

- 메일링 Enable/Disable 설정 가능
- Security 담당자 설정 가능

04 보안취약점 데이터 베이스 수집

- 일 1회, NVD에서 제공되는 REST API를 통해 데이터 취득하여 DB에 저장

04 보안취약점 데이터 베이스와 OSS 매칭

- NVD CPE 데이터에서 product, version 값을 각각 OSS name(또는 nickname), OSS version 과 매칭하여 보안취약점 검출

04 보안취약점 버전 관리

- NVD에서 제공하는 버전과 FOSSLight Hub에서 관리하는 버전을 매핑시켜 보안취약점 검출이 가능하도록 기능 제공

FOSSLight Hub

7.81.0-1ubuntu1.1.8 버전

=

NVD

7.81.0 버전
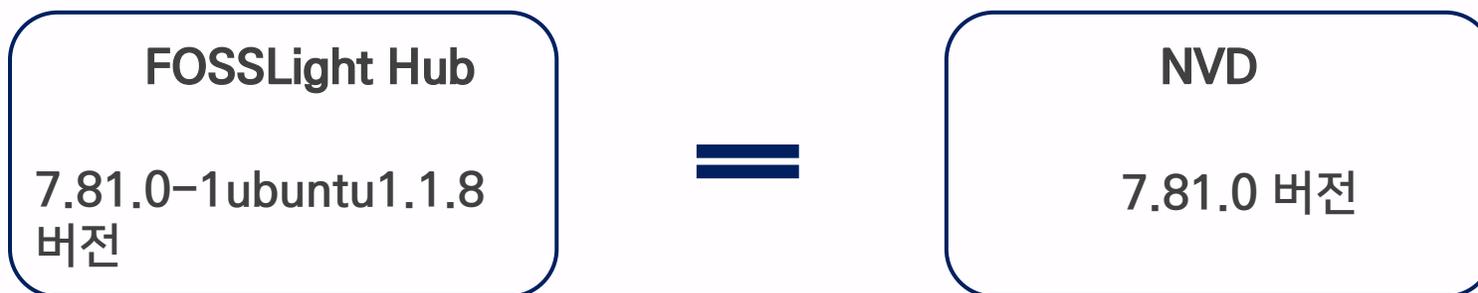
04 Include CPE

- OSS에 매핑이 누락된 보안취약점 정보를 추가하는 기능 제공
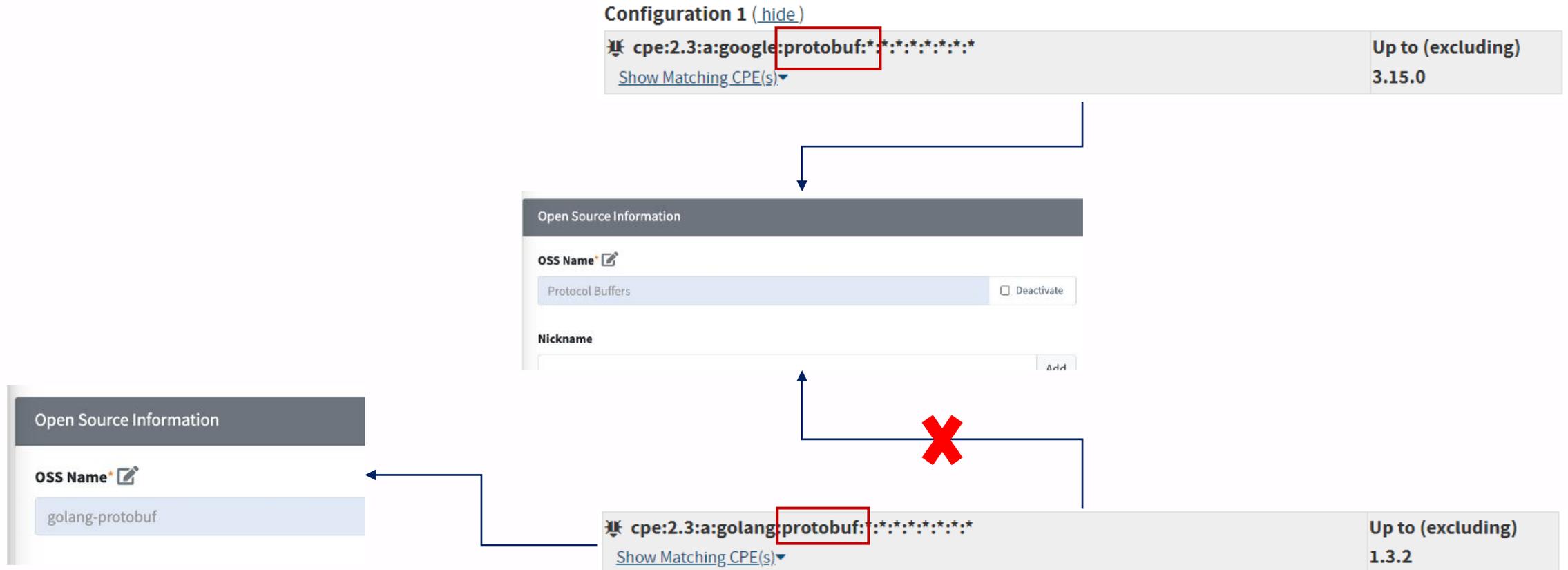
04 Exclude CPE

- OSS에 잘못 매핑된 보안취약점 정보를 제외하는 기능 제공

05
CoReviewer

05 CoReviewer 이전의 리뷰 과정
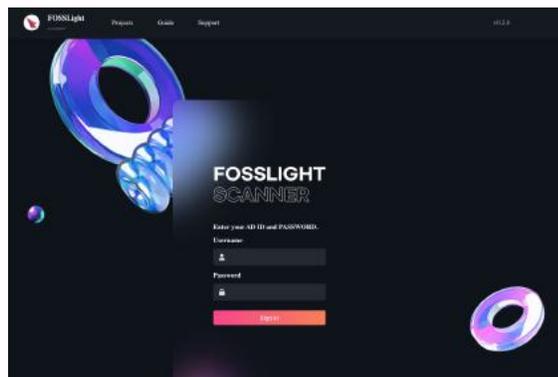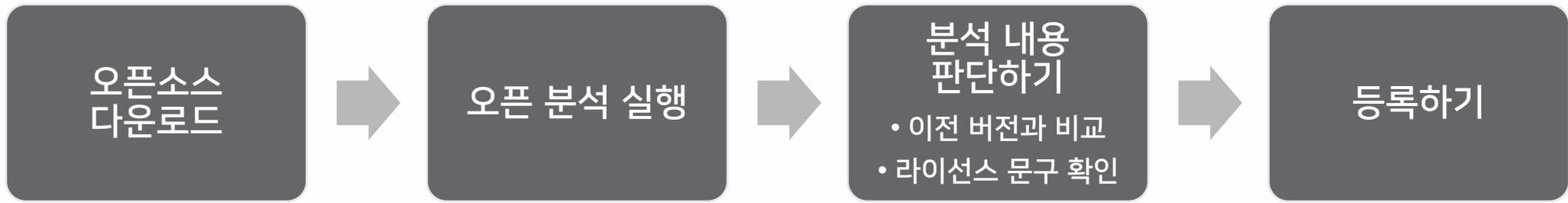
| 오픈소스 다운로드 | → | 오픈 분석 실행 | → | 분석 내용 판단하기 · 이전 버전과 비교 · 라이선스 문구 확인 | → | 등록하기 |
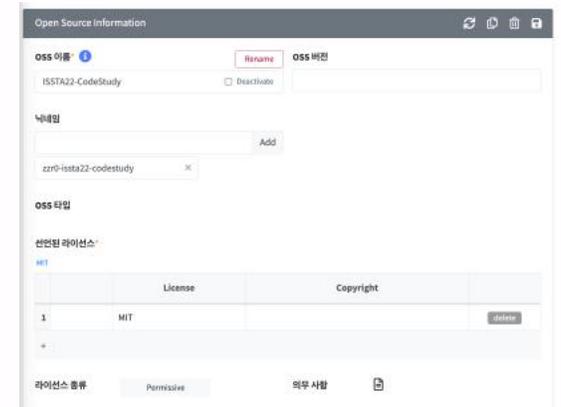
05 CoReviewer 도입

- 오픈소스 리뷰의 자동화 도입

05 CoReviewer 실행 방법

05 CoReviewer 결과 리포트

[CoReviewer] FAIL

등록 실패

1. grpc (2.72.0)
   reason : [Existed] grpc ()
2. microsoft-TemplateStudio (fd7db0a)
   reason : [New] [generic-cla, proprietary-license, unknown]
3. microsoft-wdkmetadata (0.12.8-experimental)
   reason : [Not Included in License Text] MS-PL
4. win32metadata (61.0.15-preview)
   reason : [Not Included in License Text] MS-PL
5. windowsappsdk (1.7.250606001)
   reason : [Existed] windowsappsdk ()

[CoReviewer] SUCCESS (NEED TO CHECK)

등록 성공, 검토 필요

http://collab.lge.com/main/x/DZYppg

1. GuidMapping (1.3.0)
   infoMsg : [Saved] NO_LICENSE_DETECTED
2. dotnet-runtime (9.0.7)
   infoMsg : [Dectected] Unknown-License-Reference
   [Same Need Review] dotnet-runtime (9.0.2)
3. dotnet-runtime (9.0.5)
   infoMsg : [Dectected] Unknown-License-Reference
   [Same Need Review] dotnet-runtime (9.0.7)
4. log4net (3.1.0)
   infoMsg : [Dectected] Unknown-License-Reference
   [Saved diff Version] Checkout : rel/3.1.0 / Saved : 3.1.0

[CoReviewer] SUCCESS

등록 성공

1. CsWin32 (0.3.183)
2. ExtensionBlocks (1.4.2)
3. Lnk (1.5.1)
4. WinUIEx (2.6.0)
5. grpc-dotnet (2.71.0)
6. WinUI-Gallery (2.6.0)
7. serilog (4.3.0)

05 CoReviewer를 통해 등록된 OSS

- 분석 결과를 확인 할 수 있도록 comment로 제공

05 등록 실패 케이스 저장 방법

- 분석된 결과를 저장할 수 있는 UI 제공

	Title	Result	OSS Name	OSS Version	OSS NickName	Declared License Name	Copyright	Download Location	Homepage	Description	Comment
☑	취합정보		binaryornot	0.4.3 New version	pypi:binaryornot	bsd-new New license	Copyright (c) 2013, Audrey Roy	https://pypi.org/project/binaryornot, https://pypi.org/project/binaryornot/0	https://github.com/binaryornot/bi...		[Scancode License Analysis] Declared L
☐	┗ binaryornot (0.4.4) 최신 등록 정보		binaryornot	0.4.3 New version	pypi:binaryornot	BSD-3-Clause		https://pypi.org/project/binaryornot, https://pypi.org/project/binaryornot/0	https://pypi.org/project/binaryorn...		[Scancode License Analysis] Declared L
☐	┗ 사용자 작성 정보		pypi:binaryornot New open source	0.4.3	pypi:binaryornot Duplicate.	0BSD		https://pypi.org/project/binaryornot OSS with the similar link already exists.	https://github.com/binaryornot/bi...		[Scancode License Analysis] Declared L
☐	┗ License text파일 분석 결과		binaryornot	0.4.3 New version	pypi:binaryornot	bsd-new New license		https://pypi.org/project/binaryornot, https://pypi.org/project/binaryornot/0	https://github.com/binaryornot/bi...		[Scancode License Analysis] Declared L
☐	┗ Scancode 분석 결과		binaryornot	0.4.3 New version	pypi:binaryornot	bsd-new New license	Copyright (c) 2013, Audrey Roy	https://pypi.org/project/binaryornot, https://pypi.org/project/binaryornot/0	https://github.com/binaryornot/bi...		[Scancode License Analysis] Declared L

Page 1 of 1   15   Count : 1

Panel 1

Title

취합정보 ▼

OSS Name ⓘ

binaryornot

OSS Version

0.4.3

New version

Nickname

[   ] Add

pypi:binaryornot ✕

Vulnerability Info ＞

Declared License

bsd-new

	License	Copyright	
1.	bsd-new		delete

+ |

Detected License

[   ] Add

Restriction

Copyright

Copyright (c) 2013, Audrey Roy

License Type

Obligation

Download Location

[   ] Add

https://pypi.org/project/binaryornot ✕
pkg:pypi/binaryornot

https://pypi.org/project/binaryornot/0.4.3 ✕
pkg:pypi/binaryornot

Home Page

https://github.com/binaryornot/binaryornot

Summary Description

Important Notes

Comment

[Scancode License Analysis]
Declared License: bsd-new(1)
Full scan: bsd-new(5.0)

Save

Panel 2

Title

License text파일 분석 결과 ▲

[   ]

취합정보

binaryornot (0.4.4) 최신 등록 정보

사용자 작성 정보

License text파일 분석 결과

Scancode 분석 결과

Vulnerability Info ＞

Declared License

bsd-new

	License	Copyright	
1.	bsd-new		delete

+ |

Detected License

[   ] Add

Restriction

Copyright

License Type

Obligation

Download Location

[   ] Add

https://pypi.org/project/binaryornot ✕
pkg:pypi/binaryornot

https://pypi.org/project/binaryornot/0.4.3 ✕
pkg:pypi/binaryornot

Home Page

https://github.com/binaryornot/binaryornot

Summary Description

Important Notes

Comment

[Scancode License Analysis]
Declared License: bsd-new(1)
Full scan: bsd-new(5.0)

Save

Panel 3

Title

binaryornot (0.4.4) 최신 등록 정보 ▼

OSS Name ⓘ

binaryornot

OSS Version

0.4.3

New version

Nickname

[   ] Add

pypi:binaryornot ✕

Vulnerability Info ＞

Declared License

BSD-3-Clause

	License	Copyright	
1.	BSD-3-Clause		delete

+ |

Detected License

[   ] Add

Restriction

Copyright

License Type

Obligation

Download Location

[   ] Add

https://pypi.org/project/binaryornot ✕
pkg:pypi/binaryornot

https://pypi.org/project/binaryornot/0.4.3 ✕
pkg:pypi/binaryornot

Home Page

https://pypi.org/project/binaryornot/0.4.3

Summary Description

Important Notes

Comment

[Scancode License Analysis]
Declared License: bsd-new(1)
Full scan: bsd-new(5.0)

Save

05 등록 실패 케이스 저장 방법

- 오픈소스 별 FOSSLight Source Scanner 분석 결과 파일 제공

#		파일명	크기	수정일시	다운로드
1		125608840_EasternJournalist-utils3d_0.0.2.xlsx	7.5 KB	2025-10-01 10:55	⬇
2		125608843_PyYAML_6.0.3.xlsx	7.6 KB	2025-10-01 10:55	⬇
3		125608849_anyio_4.11.0.xlsx	7.6 KB	2025-10-01 10:55	⬇
4		125608851_boto3_1.38.18.xlsx	12.1 KB	2025-10-01 10:55	⬇
5		125608852_botocore_1.38.46.xlsx	24.9 KB	2025-10-01 10:57	⬇
6		125608855_click_8.3.0.xlsx	7.8 KB	2025-10-01 10:55	⬇
7		125608867_fonttools_4.60.0.xlsx	19.3 KB	2025-10-01 10:56	⬇
8		125608869_hf-xet_1.1.10.xlsx	11.2 KB	2025-10-01 10:55	⬇
9		125608870_huggingface_hub_0.35.1.xlsx	14.2 KB	2025-10-01 10:55	⬇
10		125608872_iopath_0.1.10.xlsx	8.3 KB	2025-10-01 10:55	⬇
11		125608880_mysql-connector-python_9.2.0.xlsx	51.8 KB	2025-10-01 10:55	⬇
12		125608882_ninja_1.13.0.xlsx	17.8 KB	2025-10-01 10:56	⬇
13		125608890_portalocker_3.2.0.xlsx	8.2 KB	2025-10-01 10:56	⬇

05 CoReviewer 효과

- 2025년 오픈소스 등록 기준

OSPO
13%
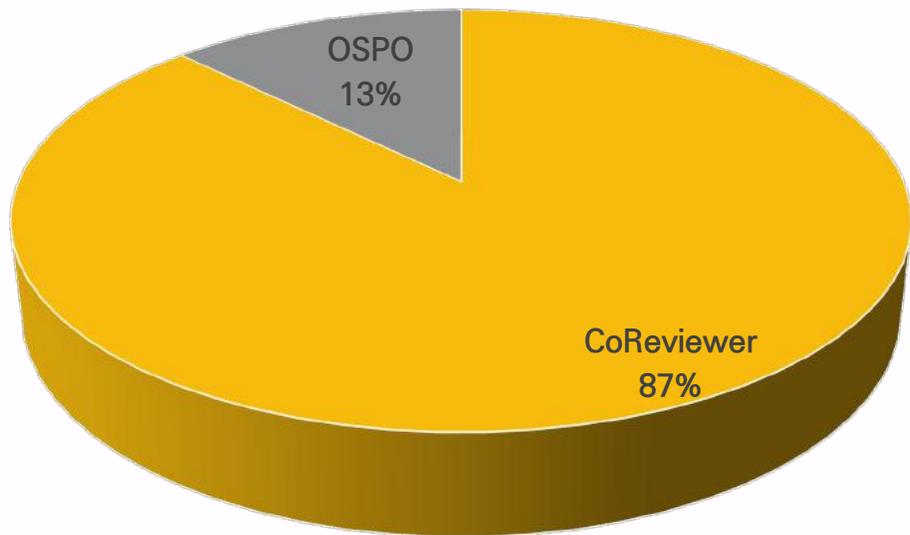
CoReviewer
87%

■ CoReviewer   ■ OSPO

OSPO는 반복작업을 단순화
리뷰시간 단축 OSPO의 확인이
필요한 부분에 좀 더 집중 가능

Requestor는 리뷰 시간이
단축되어 프로세스 진행
소요시간이 감소됨

감사합니다

FOSSLight Hub 2.0