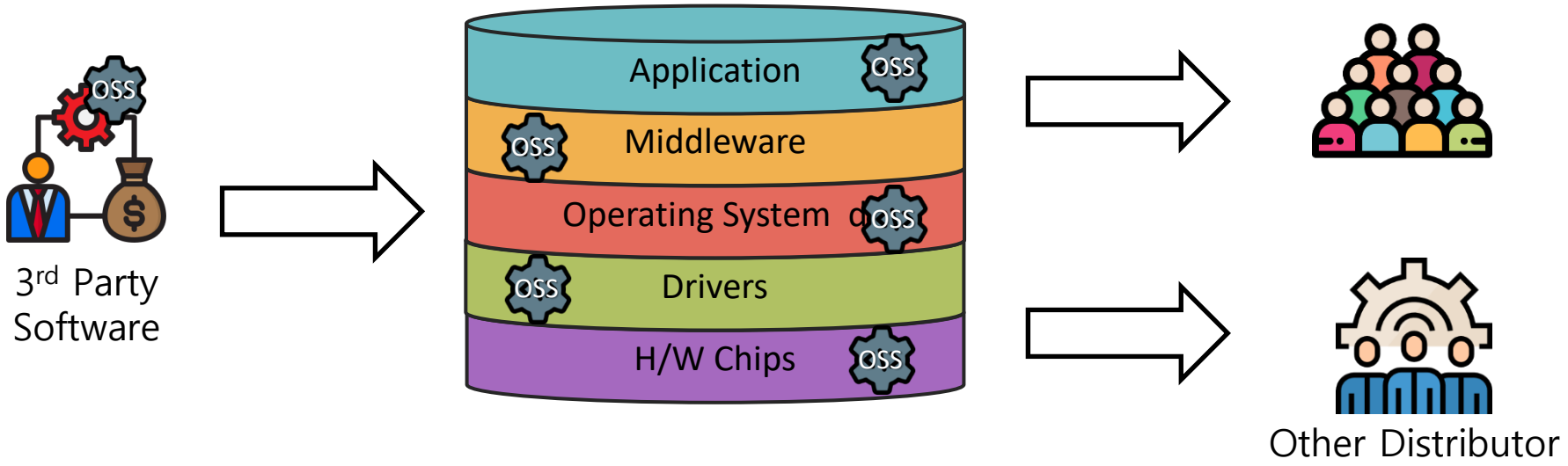
SBOM Tool Essentials

LG Electronics, Kyoungae Kim

LG Open Source

SBOM Tool

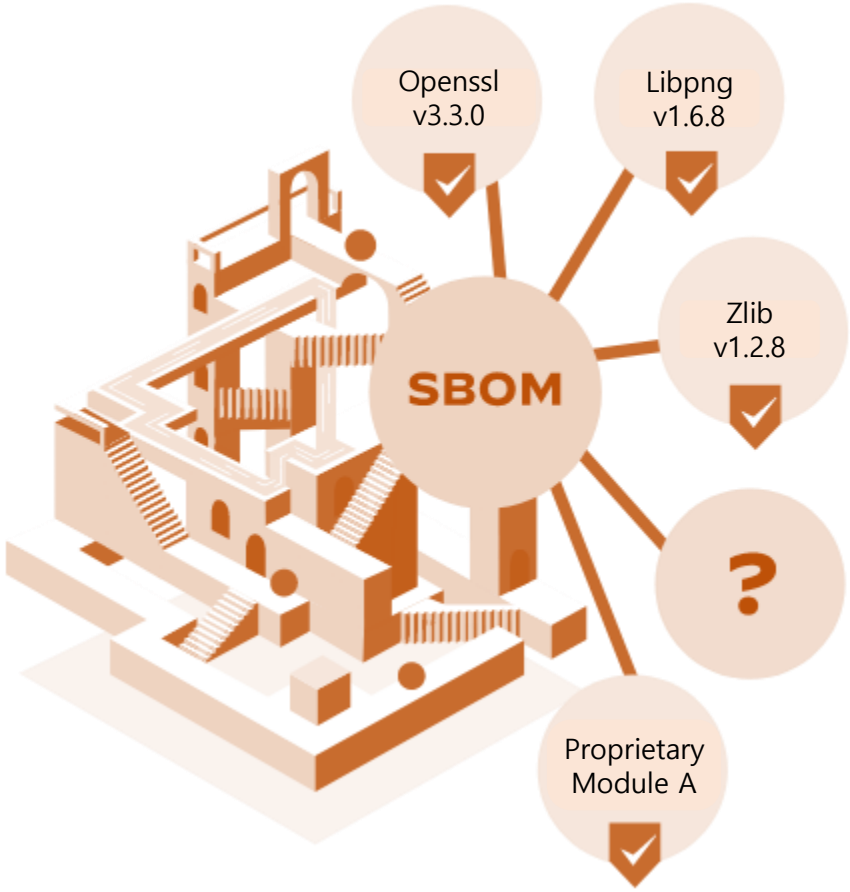
Supply Chain Software



SBOM (Software Bill Of Materials)

Baseline Software Component Information

- Supplier Name
- Component Name
- Component Version
- Unique Identifier
- Dependency Relationship
- Data Author Name
- Timestamp
- Licenses
- Vulnerabilities



Automation Support

SBOM Creation Automation

SBOM Document Auto Creation
(ex. SPDX, CycloneDX, SWID Tags)

CLI/API Support for Automation

Dependency Support

- Dependency Scanning
- Support Transitive Dependency
- Ex. Support SPDX Document Field “relationships”

Component Identification

Many different component names should be managed by one

Ex. Apache tomcat, tomcat, apache-tomcat

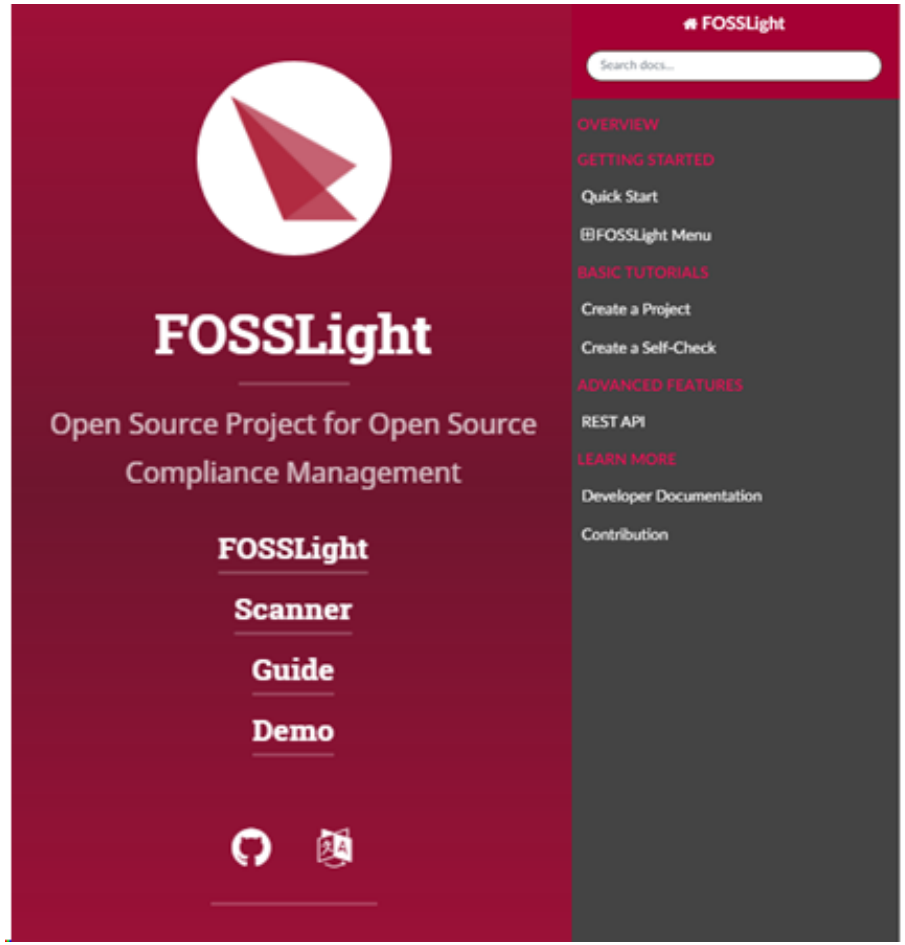
-> One component

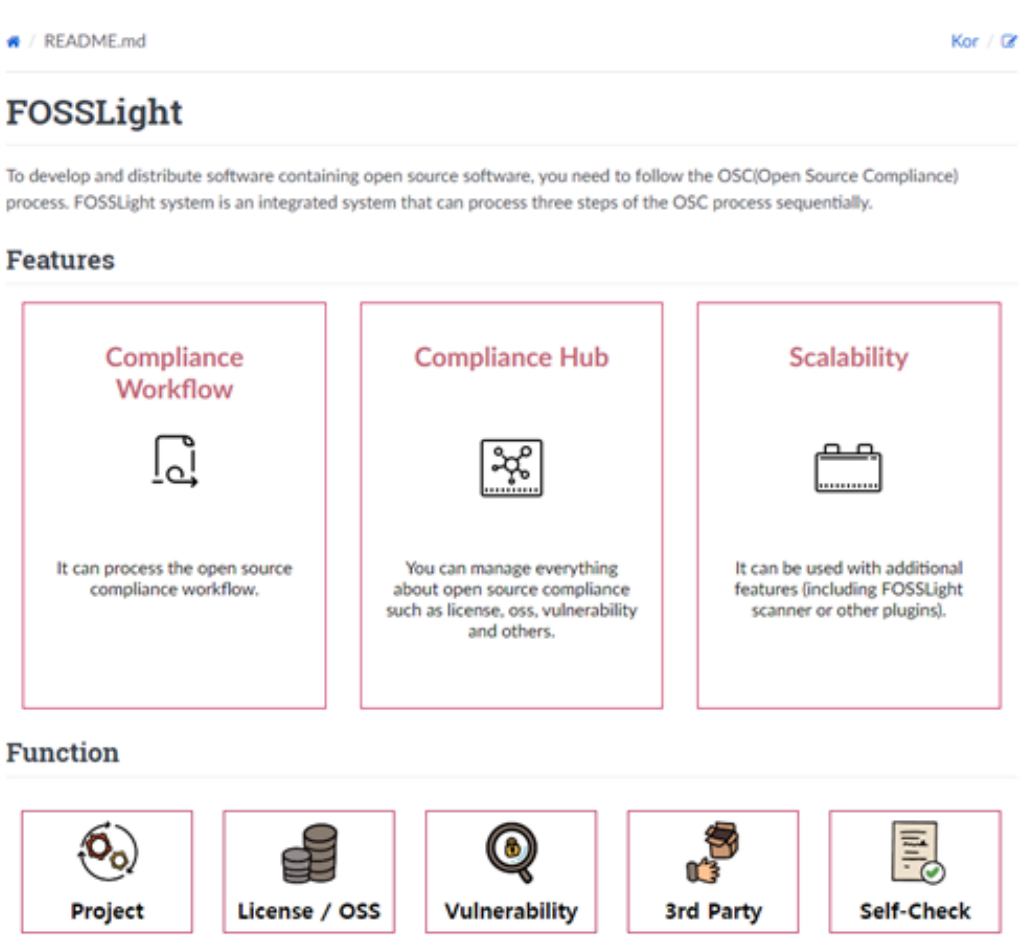
Operation

- Support SBOM search
- Tracking SBOM Changes
- Real-time Notification

FOSSLight

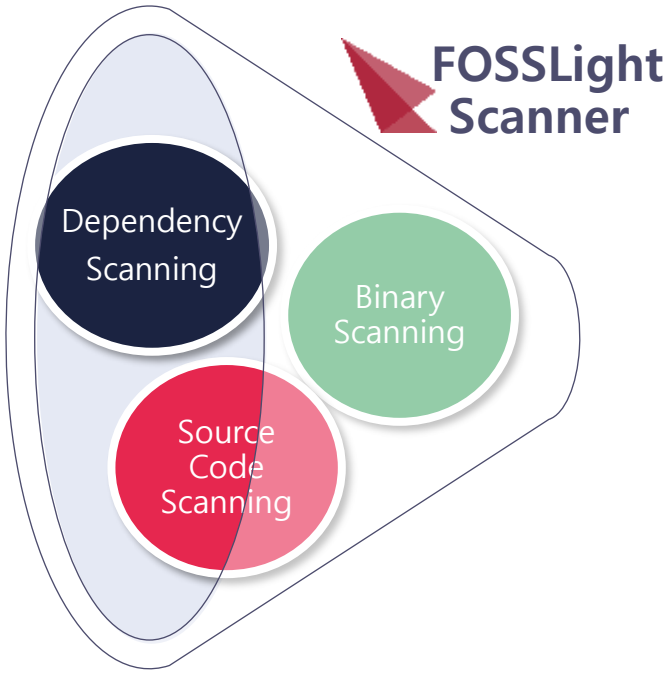
FOSSLight Open Source Project





https://fosslight.org

FOSSLight Scanner + FOSSLight Hub



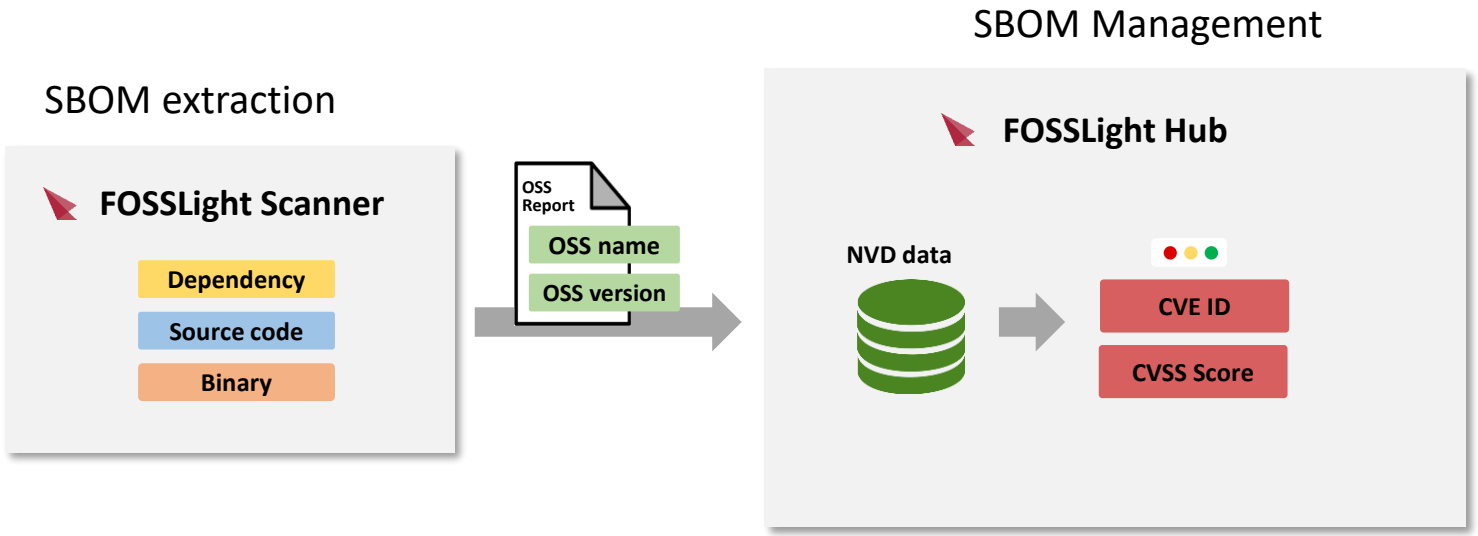
OSS BOM

ID	Source Name or Path	OSS Name	OSS Versio	License	Download Location	Homepage	Copyright Text
-	[Name of the Source File or Path /	[Name of the OSS used	[Version Nu	[License of the OSS. Use	[Download URL or a spe	[Web site that serves as	[The copyright holde
1	/src/tools/busybox/	busybox	1.4	GPL-2.0	https://busybox.net/dow	https://www.busybox.net	Copyright (c) 1999-2
2	/src/framework/curl/	curl	7.50.3	curl	https://github.com/curl/	http://curl.haxx.se	Copyright (c) 1996 -
3	/src/application/calendar/view.c	-		BSD-3-Clause			Copyright (c) 2016, N

SBOM Management

FOSSLight Hub

FOSSLight + Vulnerability

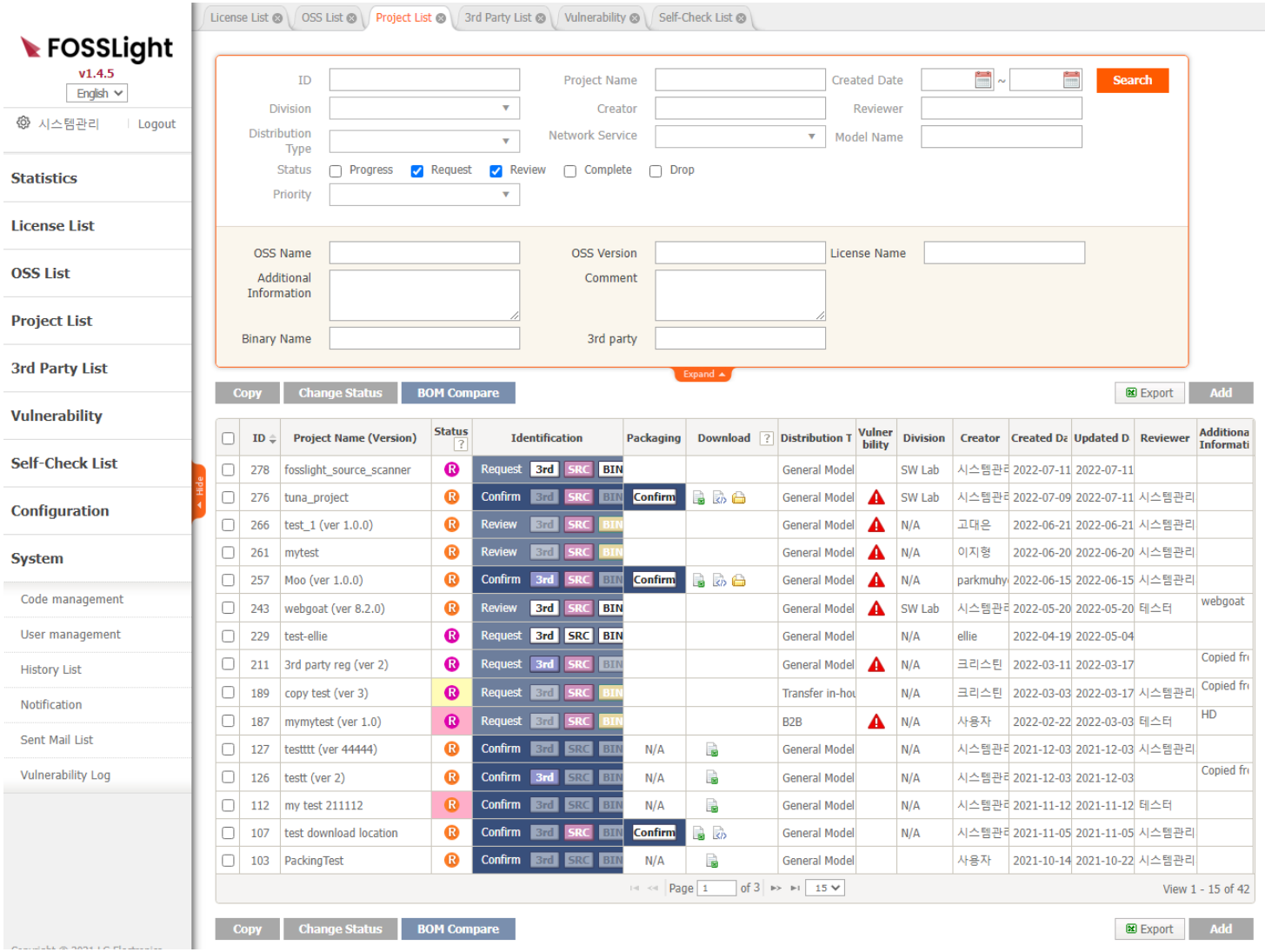


	OSS Name	Version	Score	CVE ID	Published Date
1	aiohttp	3.6.2	6.1	CVE-2021-21330	2022-08-11

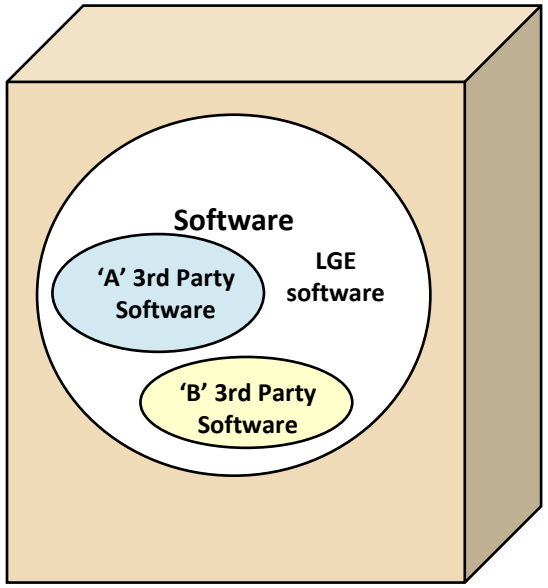
FOSSLight Hub

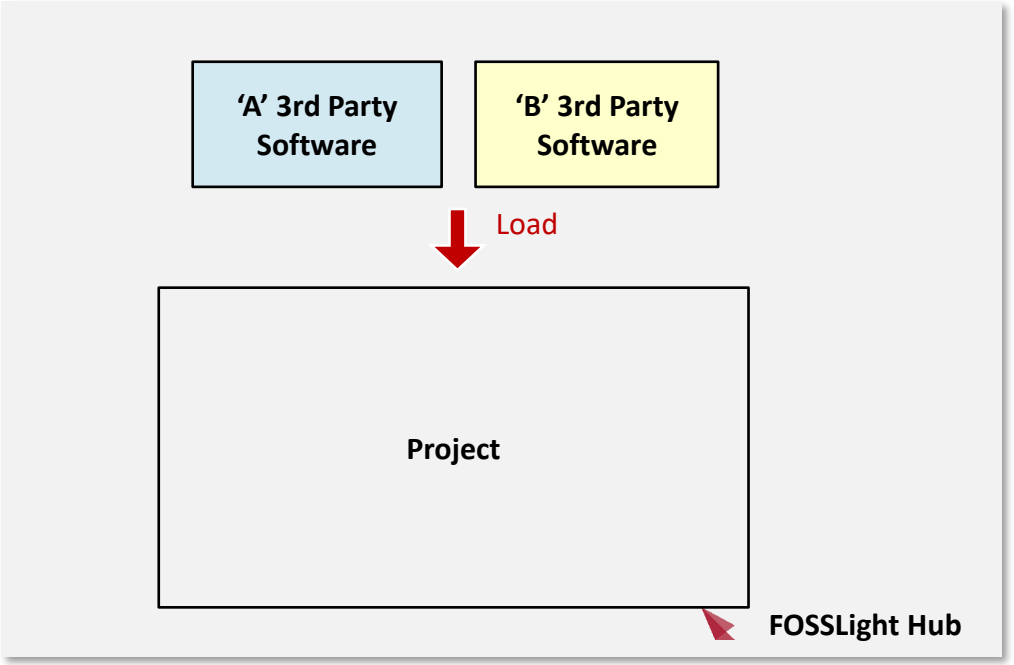
Essential for

SBOM Management



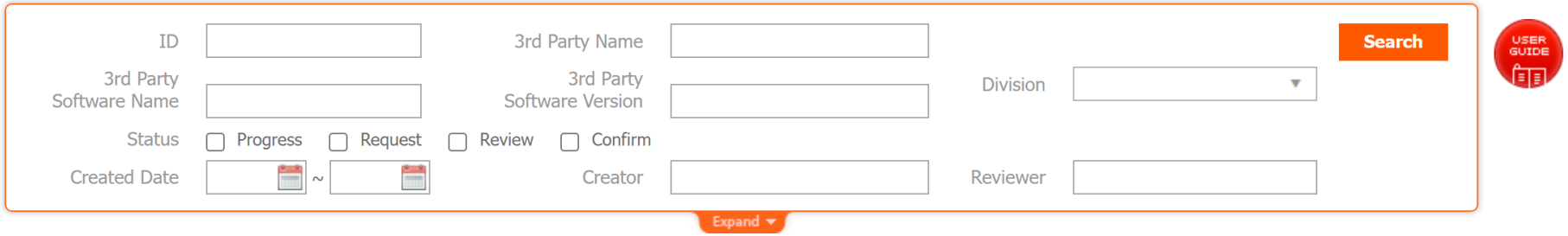
Supply Chain Management





Supply Chain Management

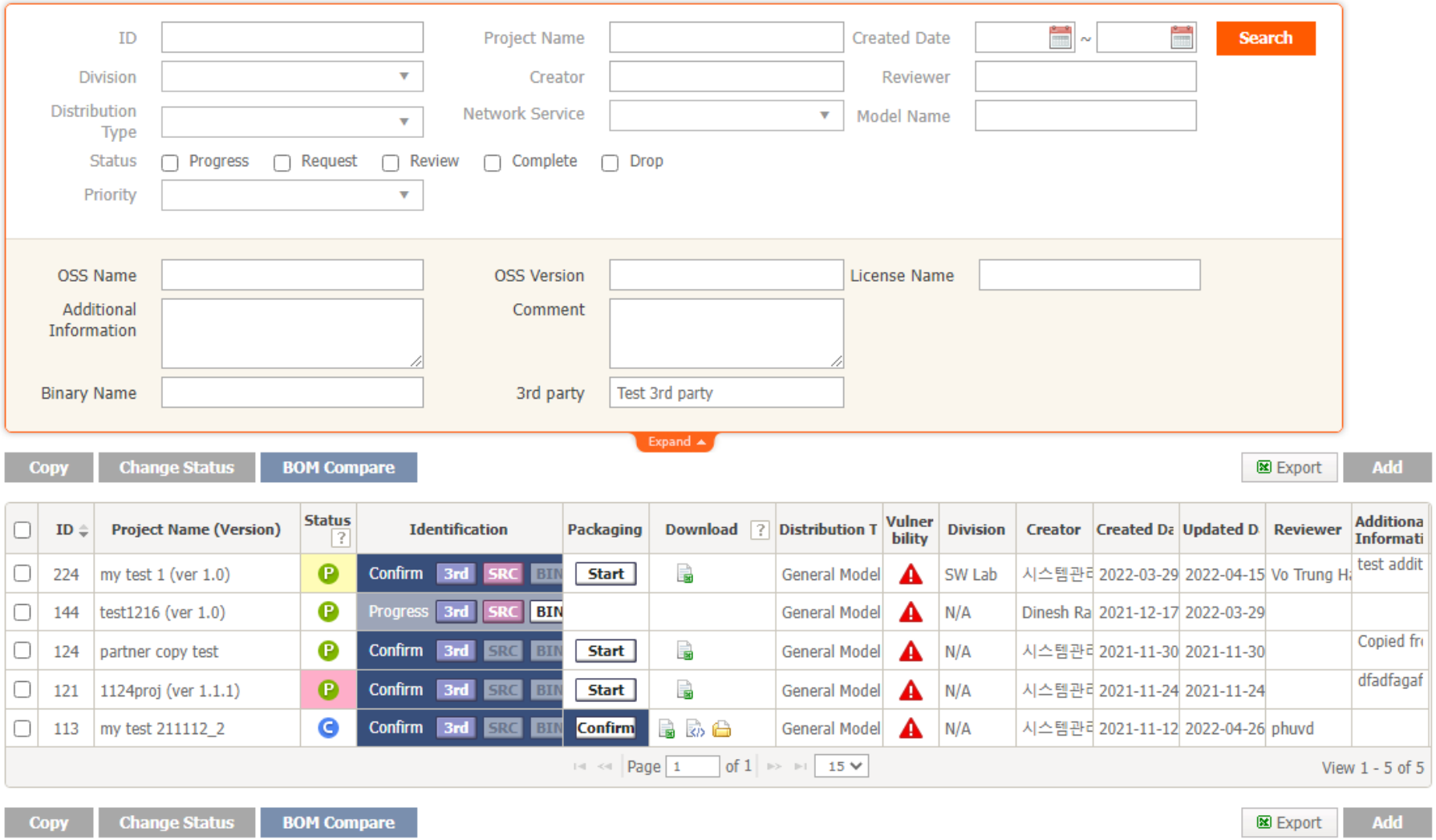
❑ Using “3rd Party List”



ID	3rd Party Name	Software Name (Version)	Status	Delivery Form	Description	Vulnerability	Division	Creator	Created Date	Updated Date	Reviewer
539	seongsik89.kim_Company	Training device app (ver 1.	C	B	3rd party 정보입니다.	⚠	CTO 컨버전스센터	김성식/선임연구원	2021-09-07	2022-02-24	김경애/Task Leader/S
538	Brian_Moon_Company	Training device app	C	S		⚠	VS 스마트개발센터	문경귀/책임연구원	2021-09-07	2022-02-24	김경애/Task Leader/S
537	red.kim_he	Training device app	C	S		⚠	HE CAV	김영기/책임/HE서	2021-09-07	2022-02-24	석지영/선임연구원/S
535	hosc-1104	Sample_software_from_3r	P	S			CTO SW센터	일반박원재	2021-09-03	2022-02-24	박원재/선임연구원/S
534	OSC-1756 test	(test)170308_pwj_3rdParty	R	S		⚠	CTO SW센터	시스템관리자	2021-08-03	2022-02-24	시스템관리자
533	test	Sample_software_from_3r	R	S			CTO SW센터	시스템관리자	2021-08-03	2022-02-24	시스템관리자
532	한글로 작성된 경우 테스트	한글로 작성된 경우 테스트	P	S		⚠	CTO SW센터	시스템관리자	2021-05-12	2022-02-24	
531	test 3rd party item	좋은 소프트웨어	C	S		⚠	CTO SW센터	시스템관리자	2021-04-26	2022-02-24	시스템관리자
530	Test_JK_3rd	SW_3rd_JK_Test (ver 0.0.1	C	S	Test		CTO SW센터	방재권/선임연구원	2021-04-16	2022-02-24	김소임/선임연구원/S
528	delete 3rd party test	mail_plugin	C	S			CTO SW센터	시스템관리자	2020-11-26	2022-02-24	시스템관리자

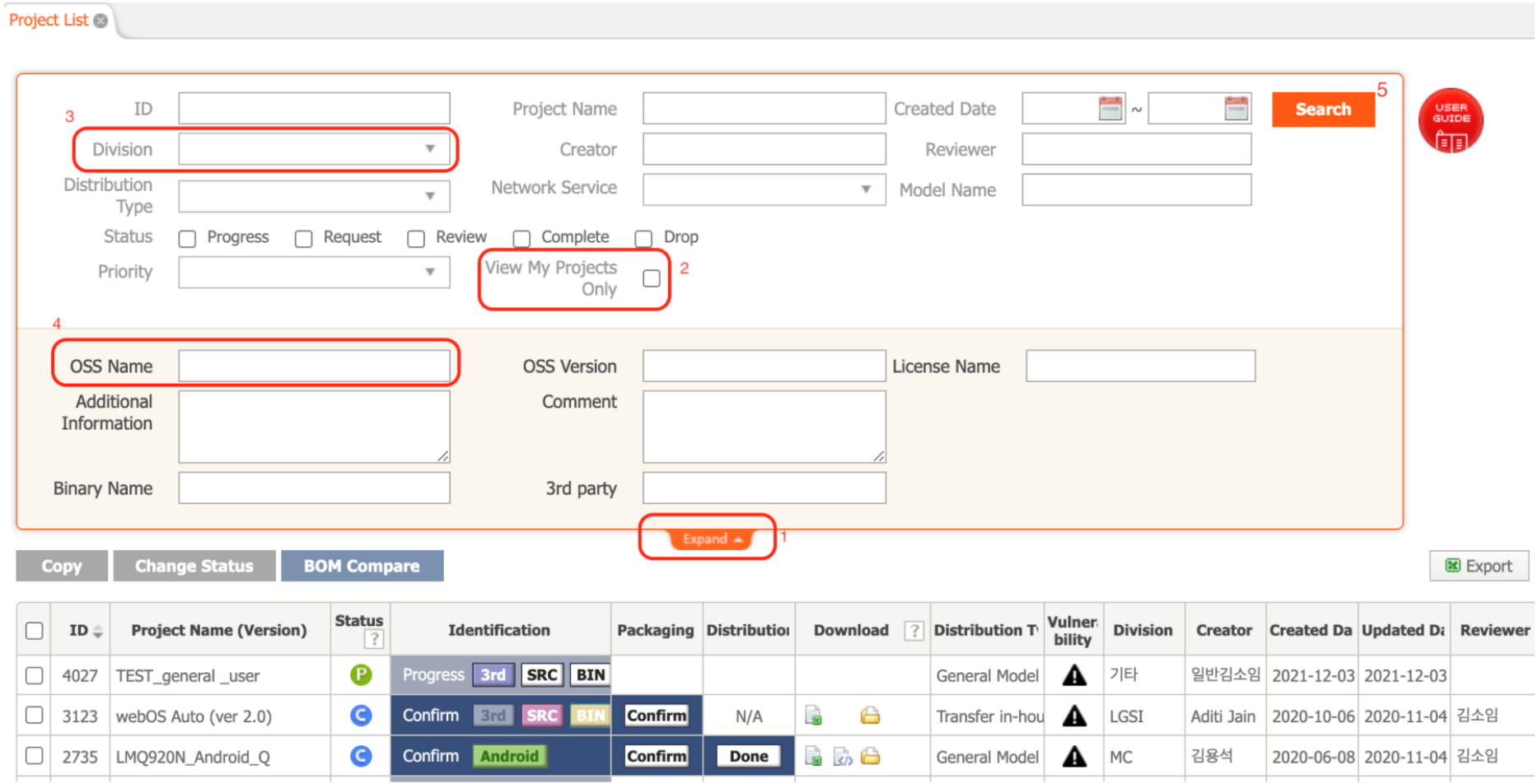
SBOM with Supply Chain

Can manage product SBOM including supply chain



SBOM Search

Search for specific component/version



SBOM Tracking

Support SBOM Compare

Copy | Change Status | BOM Compare

Before Project id: 1602 | After Project id: 1604 | Search

Excel download

Status	OSS_Before	License_Before	OSS_After	License_After
add			cJSON (1.7.10)	MIT
add			openssl (1.1.1f)	OpenSSL
delete	base-files (3.0.14)	GPL-2.0-only		
delete	lcdtest (2.0)	GPL-2.0-only, GPL-3.0, MPL-1.1		
change	cairo(1.12.12)	GPL-3.0	cairo(1.12.14)	GPL-3.0, MPL-1.1
change	apmd(3.2.2-14)	GPL-2.0-only	apmd(3.2.2-14)	GPL-2.0
change	BusyBox	GPL-2.0-only	BusyBox	GPL-2.0
change	usbutils(007)	GPL-2.0-only	usbutils(008)	GPL-2.0

Page 1 of 1 | 15 | View 1 - 8 of 8

Vulnerability Review

❑ Vulnerability Review for product

ID	Project Name (Version)	Status	Identification	Packaging	Download	Security	Vulnerability	Distribution Type	Division	Creator	Created Date	Updated Date	Reviewer	Additional Information
499	newOne	P	Start					General Model	SW Lab	Admin	2023-05-08	2023-05-08		
498	mytestproject12345	P	Confirm 3rd SRC BIN BOM	Start		SEC	⚠	General Model	SW Lab	Admin	2023-05-03	2023-05-03	Admin	
497	cdh_test	R	Confirm 3rd SRC BIN BOM	Confirm		SEC	⚠	General Model	SW Lab	Admin	2023-04-25	2023-04-25	Admin	
496	txtxt	P	Progress 3rd SRC BIN BOM			SEC		General Model	SW Lab	사용자	2023-04-21	2023-04-21		

❑ Security Review Tab

Total | Fixed | Not Fixed

Show Comment History | Comment Edit

Export | Save

OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerabilty Link
Protocol Buffers		CVE-2015-5237	8.8	2017-09-25	Unresolved	https://nvd.nist.gov/vuln/detail/
Protocol Buffers		CVE-2021-3121	8.6	2021-01-11	Unresolved	https://nvd.nist.gov/vuln/detail/
SnakeYAML	1.27	CVE-2022-1471	9.8	2022-12-01	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	5.3.1	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	5.3.1	CVE-2022-22965	9.8	2022-04-01	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	4.3.30	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/

Vulnerability Real-time Notification

FOSSLight Hub Notification

[OSC] Vulnerability Discovered

« Vulnerability Information »

OSS ID	OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
22869	json-smart-v2	2.2.1	CVE-2021-27568	9.1	An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as demonstrated by NumberFormatException. When it is not caught, it may cause programs using the library to crash or expose sensitive information.	2021-02-23	2022-05-12
15690	json-smart-v2	2.3	CVE-2021-27568	9.1	An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as demonstrated by NumberFormatException. When it is not caught, it may cause programs using the library to crash or expose sensitive information.	2021-02-23	2022-05-12

* This mail was sent by osc.lge.com

Takeaways and Conclusions

- ❑ Automation for SBOM generation and management is important
- ❑ It is difficult to determine the minimum unit of SBOM component.

Suggestions for SG17

- ❑ Consider to make a guideline for SBOM component unit such as the necessary for commercial software or self-developed software and so on.