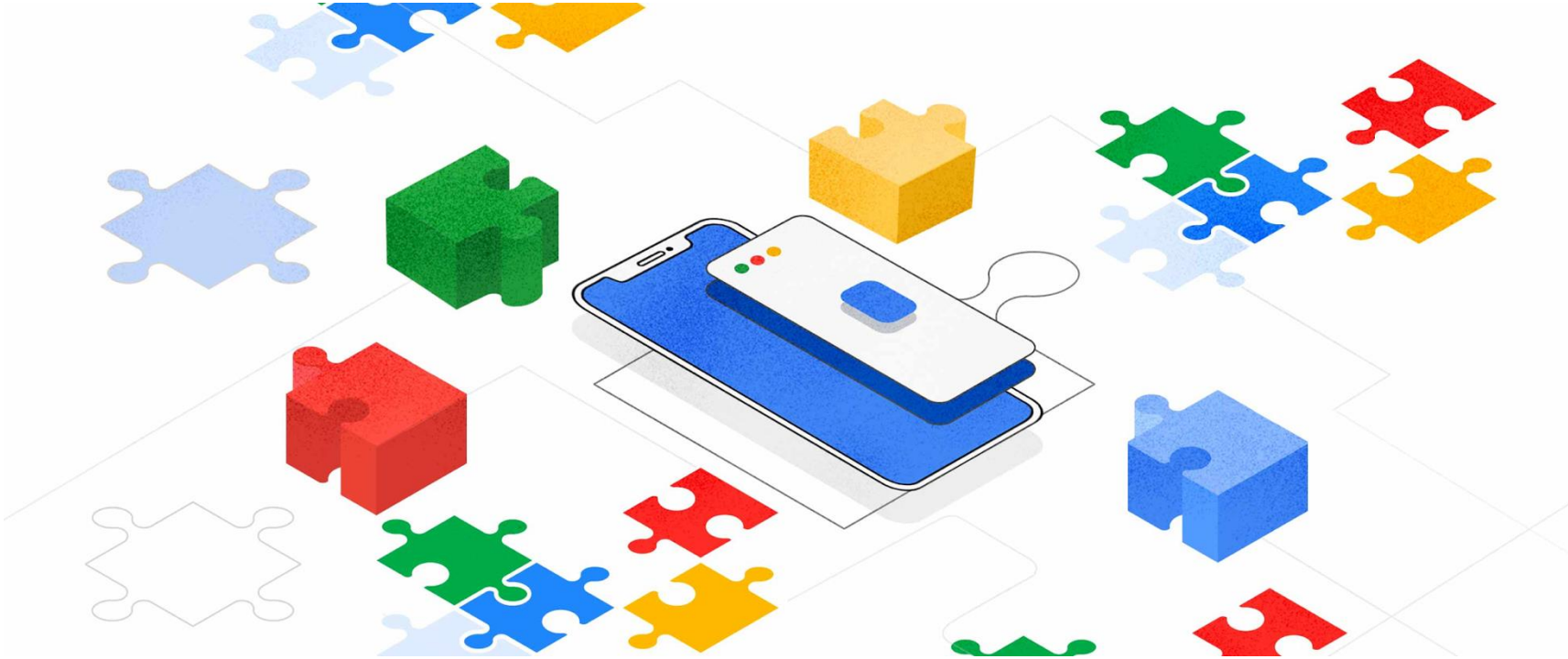
SW 공급망 관리 feat. FOSSLight

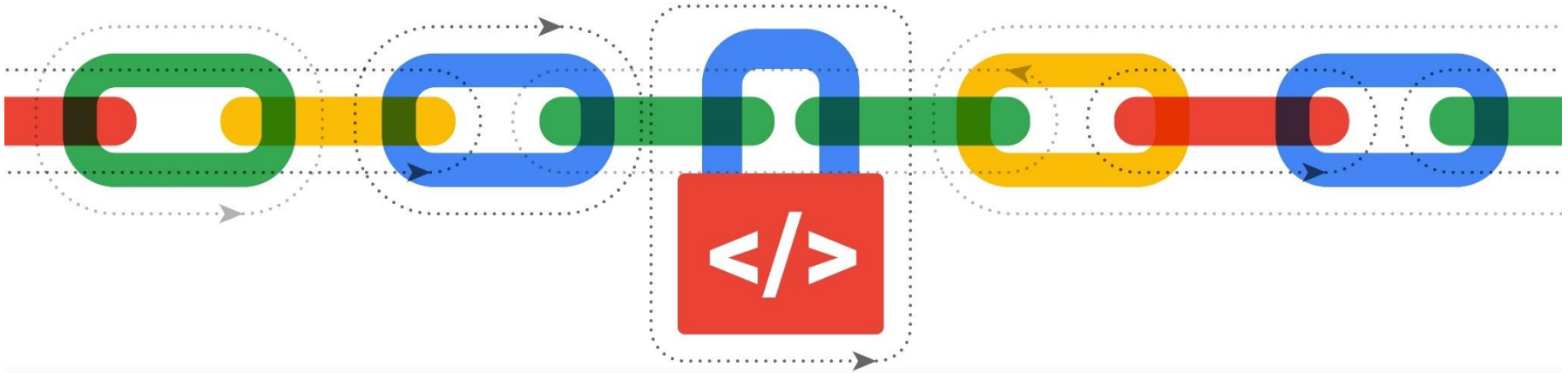
LG전자 김경애

LG Open Source

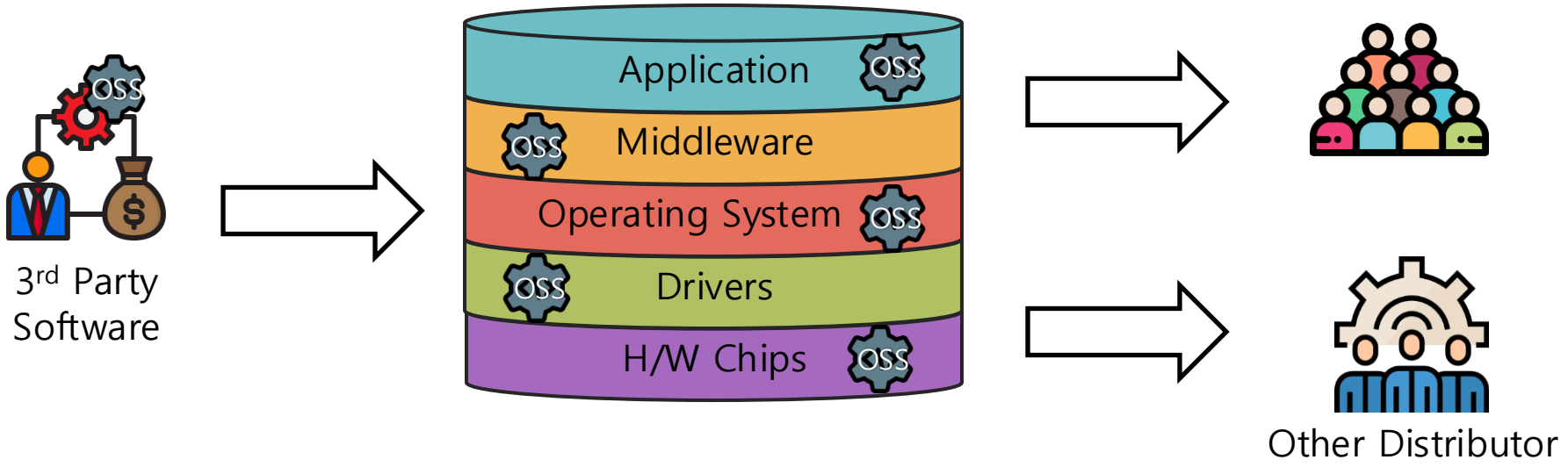
SW 공급망

SW 복잡도 증가





SW 공급망 관리 필요성


OSS
3rd Party Software
Application
OSS
OSS
Middleware
Operating System
OSS
OSS
Drivers
H/W Chips
OSS
Other Distributor

SW 공급망 공격 사례

美최대 송유관, 랜섬웨어 공격에 멈췄다‥ ·"유가 폭등 우려"

미국 최대 송유관 운영사 '콜로니얼파이프라인'이 랜섬웨어 공격을 받아 멈춰섰다. 9일(현지시간) 로이터 통신은 "송유관 재가동을 위한 회사 측의 노력에도 아직 사태가 해결되지 않았다"며 "유가 폭등 우려가 커지고 있다"고 전했다.

Pipeline spans more than 5,500 miles

이에 따르면 콜로니얼파이프라인은 8일 성명을 통해 "하루 전 자사가 사이버 공격을 받은 것을 인지했다"며 "우리는 위협을 억제하기 위해 모든 송유관 운영을 일시적으로 중단했다"고 밝혔다.

회사 측은 그러면서 "이번 사이버 공격에서 랜섬웨어를 발견했다"고 밝혔다. 랜섬웨어는 컴퓨터 시스템에 침투해 주요 데이터에 대한 접근을 차단한 뒤 몸값을 요구하는 악성 프로그램이다.

"모든 인터넷 서버 위험"…로그4j 취약점에 보안업계 비상

국내외 주요기업, 백신·취약점 대응 스캐너·시그니처 배포

김윤희 기자 | 입력 :2021/12/12 18:50 컴퓨팅

거의 모든 인터넷 서버에 대해 영향을 미칠 것으로 추정되는 치명적인 보안 취약점이 발견되면서, 국내외 보안업계에 비상이 걸렸다.

12일 보안업계는 아파치 재단이 개발한 자바 기반 오픈소스 로깅 라이브러리 '로그4j' 관련 원격 코드실행(RCE) 취약점 '로그4쉘(Log4shell)'에 대해 긴급 대응하고 있다.

로깅은 웹애플리케이션의 활동 내역을 보존하는 프로세스다. 이를 거의 모든 웹서비스에서 사용하고 있고, 발견된 취약점의 악용 난이도가 낮아 보안 조치를 신속히 취하지 않는 곳은 해킹 피해를 입을 가능성이 크다는 게 업계 분석이다.

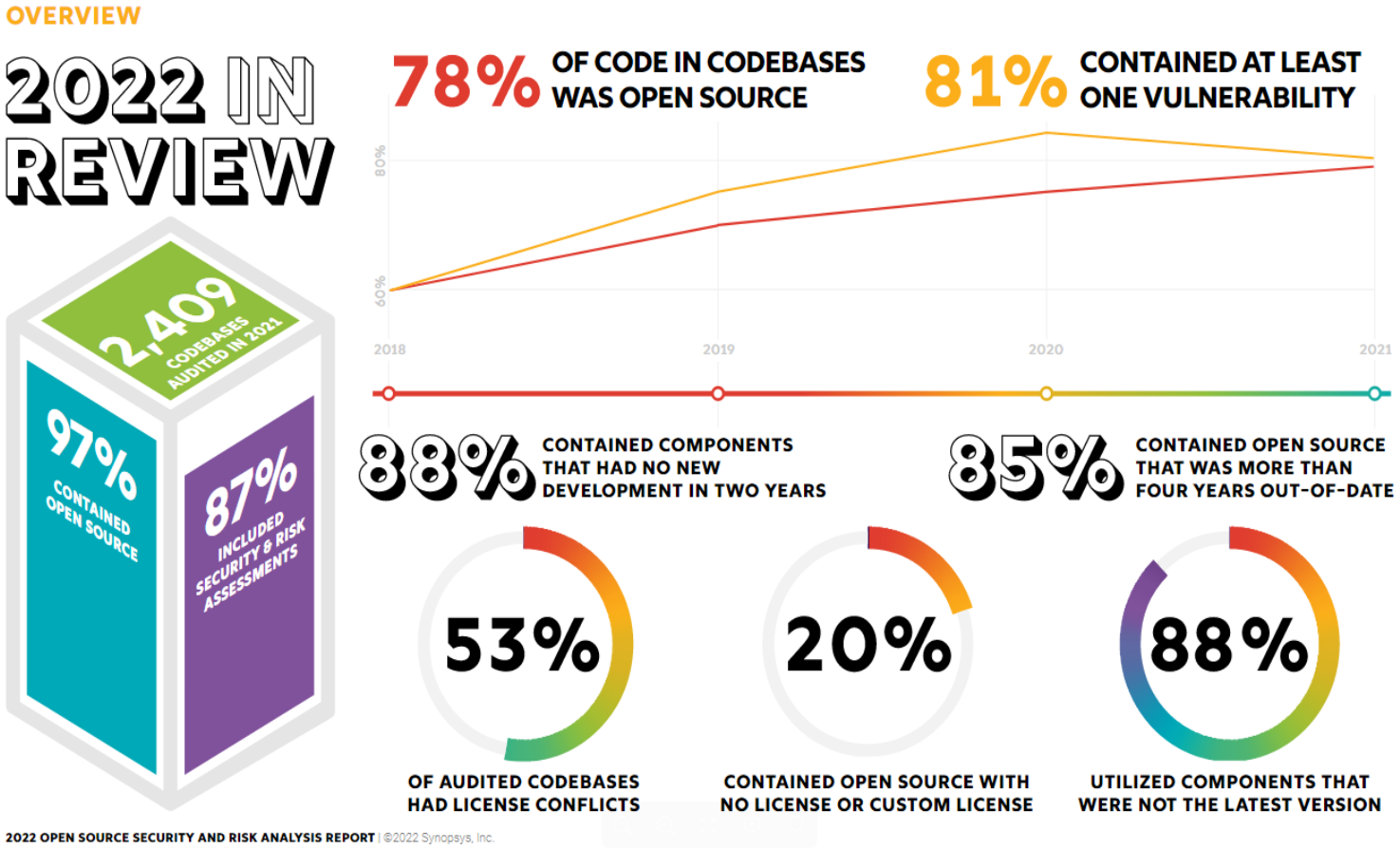
이번 취약점이 처음 알려진 것은 지난 10일이었다. 당시 마인크래프트, 아이클라우드, 스팀, 클라우드플레어 등 유명 서비스조차도 취약점 공격을 받을 수 있다는 분석이 제기됐다.

정품 VM웨어 v스피어와 상당히 유사한 악성코드 포함된 PyPI 패키지 발견

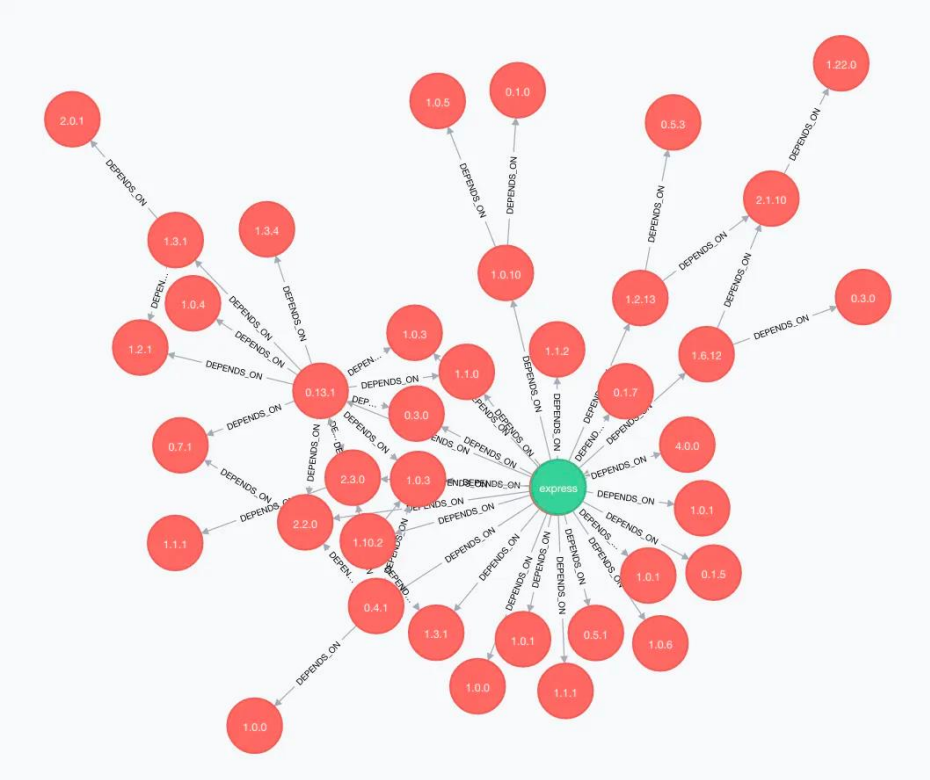
요약 : 보안 외신 SC미디어는 정품 VMware vSphere 커넥터 모듈과 매우 유사하게 설계된 'VMConnect'라는 악성 PyPI 패키지가 등장했다고 보도했다. 소나타입(Sonatype) 연구원들은 해당 악성 패키지를 'sonatype-2023-3387-237'로 명명해 할당했다. 이 악성 패키지는 정품 VMware 컨트롤러와 동일한 코드를 상당수 포함하고 있고, 이미 237번 다운로드된 것으로 나타났다. 그리고 이를 악용해 공격자들이 VMware vCenter의 중요성 및 상호 작용 방식을 알아낸 것도 확인됐다. 현재 이 패키지는 레지스트리 관리자에게 즉시 보고해 제거된 상태다.

기업의 오픈소스 활용 현황

- 21년 2,409개 SW 중 97% 오픈소스 활용, 87% 보안/라이선스 리스크



오픈소스 종속성 보안 이슈



How one developer just broke Node, Babel and thousands of projects in 11 lines of JavaScript

Code pulled from NPM – which everyone was using

Chris Williams, Editor in Chief — Wed 23 Mar 2016 // 01:24 UTC

UPDATED Programmers were left staring at broken builds and failed installations on Tuesday after someone toppled the Jenga tower of JavaScript.

A couple of hours ago, Azer Koçulu unpublished more than 250 of his modules from NPM, which is a popular package manager used by JavaScript projects to install dependencies.

Koçulu yanked his source code because, we're told, one of the modules was called Kik and that apparently attracted the attention of lawyers representing the instant-messaging app of the same name.

SBOM

SBOM 국내외 동향

미국

- 식품의약청(FDA)은 **의료기기 출시 전 안전한 제품 개발 체계의 구현 및 SBOM** 요구
- 바이든 정부는 '21년 **'국가의 사이버 보안 향상에 관한 행정 명령' 채택**으로 SBOM 관리 통한 SW 공급망 위험 낮춤
- 백악관은 연방전부 납품 SW 보안 강화 위한 '지침준수'와 '자체증명' 제출 연내 시행

유럽

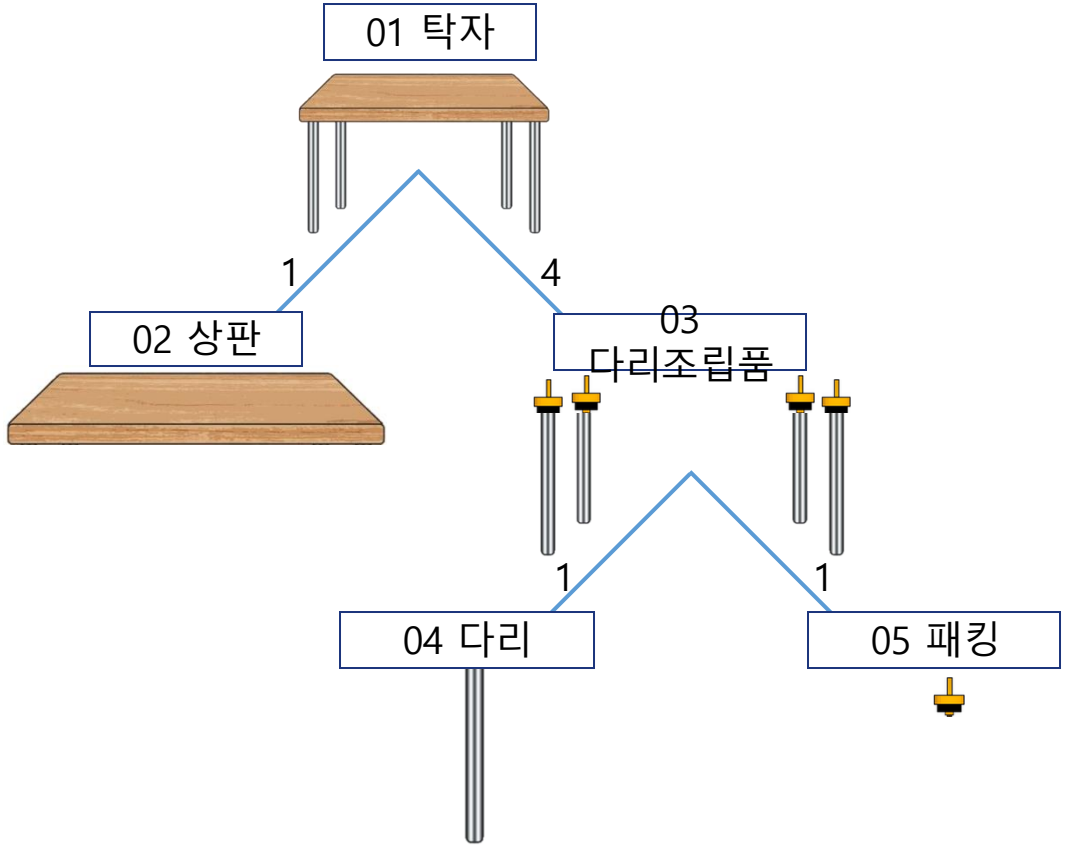
- '22년 역내 공급되는 디지털기기의 SBOM 제출을 의무화 하는 **'사이버 복원력 법 (CRA)' 제정안** 발의
- **CE마크** 부착을 위한 **기술문서에 SBOM을 포함**하고 사이버보안 적합성 평가 진행을 준비 중
- '24년 3월, 유럽의회는 CRA를 승인했으며 이사회를 거치면 '26년 하반기 효력 발생 예정

국내

- 과기정통부, **SW공급망 보안강화 사업을 내년도 예산**에 반영 계획 예정
- 과기정통부와 국정원 등은 **'24년 5월 SW 공급망 보안 가이드라인 배포**
- 가이드라인은 SBOM 기반 SW 공급망 강화 방안을 제시 등 업계 인식전환 위한 내용 수록

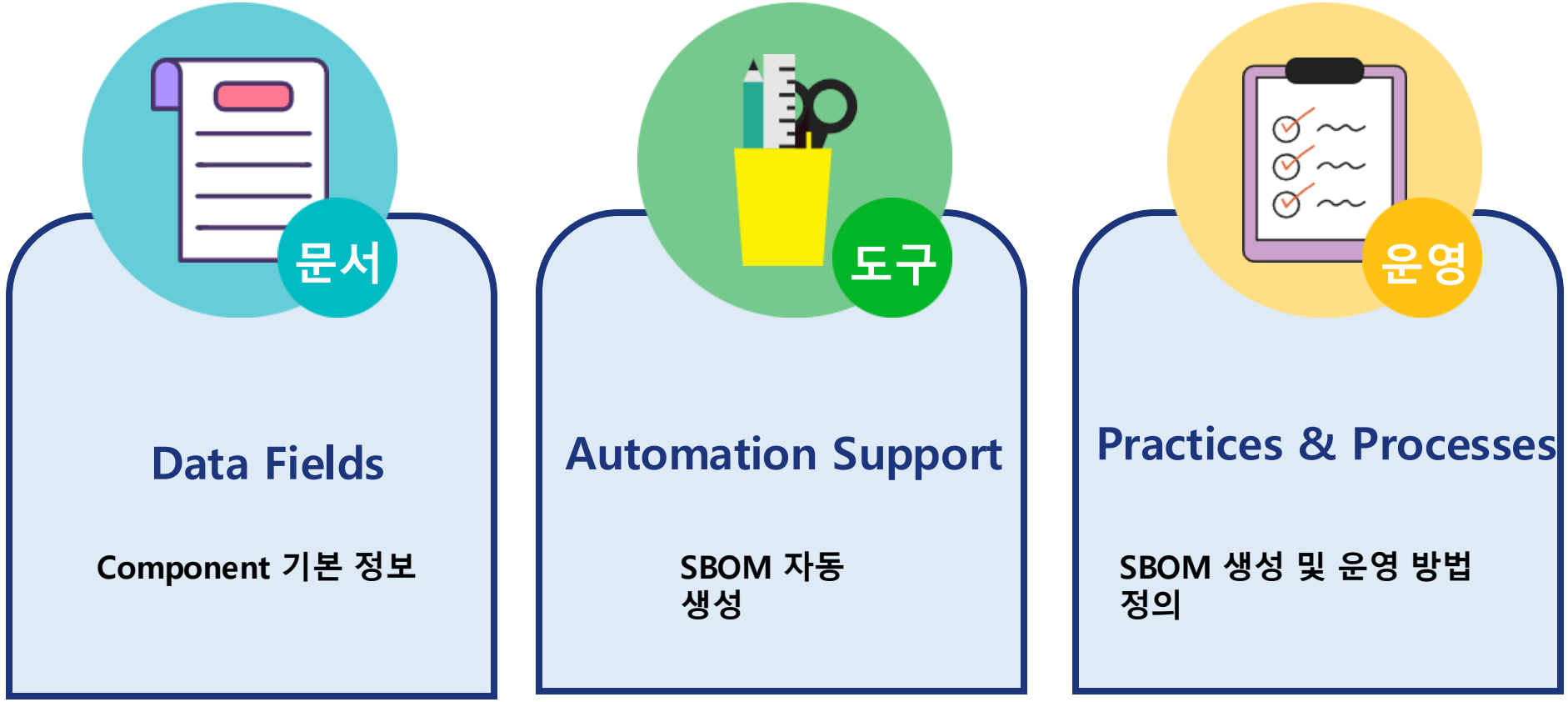
BOM(Bill Of Materials)

- 특정 제품을 만드는데 필요한 자재나 부품의 종류와 수량을 나열한 목록



SBOM (Software Bill Of Materials)

- 소프트웨어 구성 요소를 나타내는 Metadata를 의미함
- 주요 목적은 소프트웨어 구성요소와 서로의 관계를 고유하고 명확하게 식별하는 것임
- 공급되는 소프트웨어의 구성 목록을 표시하여 공급자와 사용자가 이를 기반으로 의사결정에 활용할 수 있는 환경을 조성



SBOM Data Fields

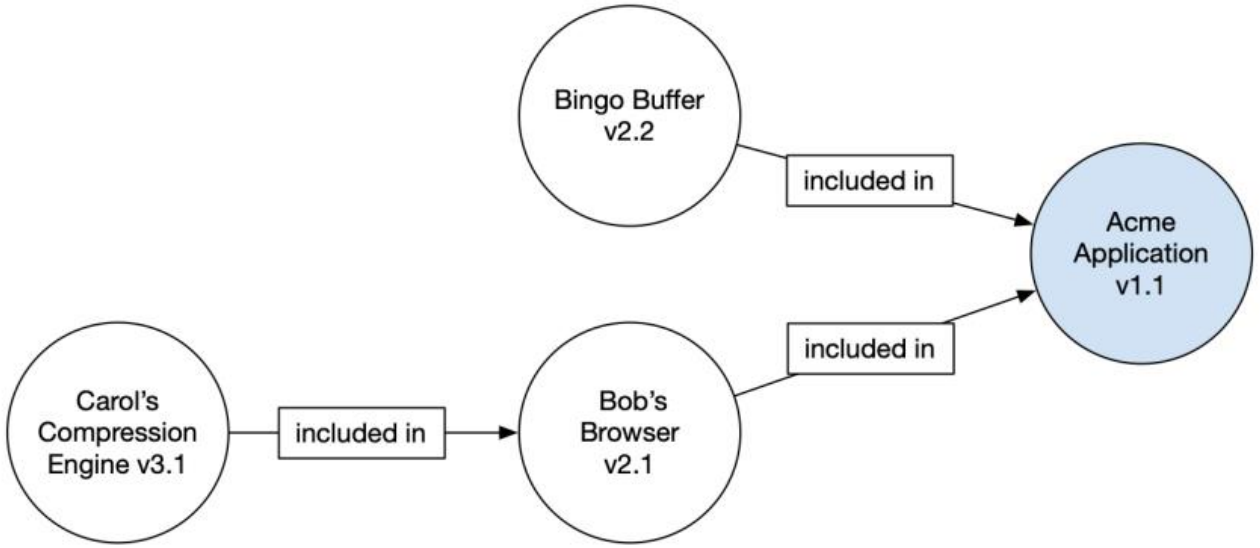


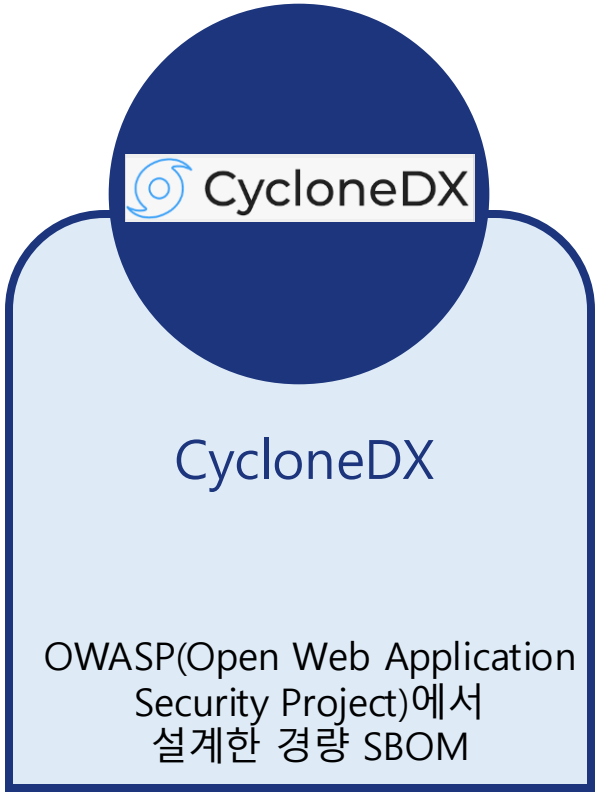
Figure 1: Conceptual SBOM graph

Component Name	Supplier	Version	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Primary
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

Table 2: Conceptual SBOM table[24]

SBOM 표준 포맷


SPDX
SPDX
(Software package data exchange)
Linux Foundation에서 설계한 표준

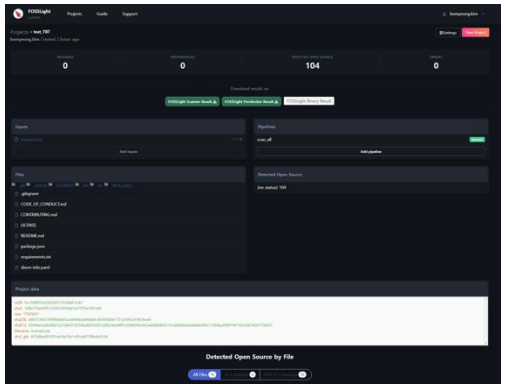

CycloneDX
CycloneDX
OWASP(Open Web Application Security Project)에서 설계한 경량 SBOM


SWID TAGS
SWID tag
(Software identification)
미국 NIST(National Institute of Standards and Technology)에서 설계한 표준

FOSSLight

FOSSLight

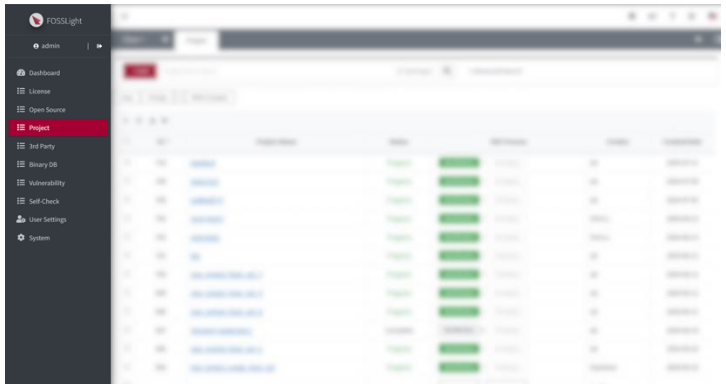
탐색 (Detect)



FOSSLight Scanner

소프트웨어에 포함된
오픈소스,
라이선스 정보와
보안취약점을
신속하고 정확하게 스캔 및 식별 하는 자동 분석 도구

관리 (Management)



FOSSLight Hub

오픈소스 소프트웨어의 **라이선스 준수와 보안 취약점 관리를 통합적으로 지원**하여, 기업의 법적 리스크 최소화와 안전한 오픈소스 사용을 돕는 통합 관리 시스템

FOSSLight Scanner 뿐만 아니라 **타사 스캐너와 연계 가능** (ex. BlackDuck, FOSSID 등)

컨설팅 (Consult)

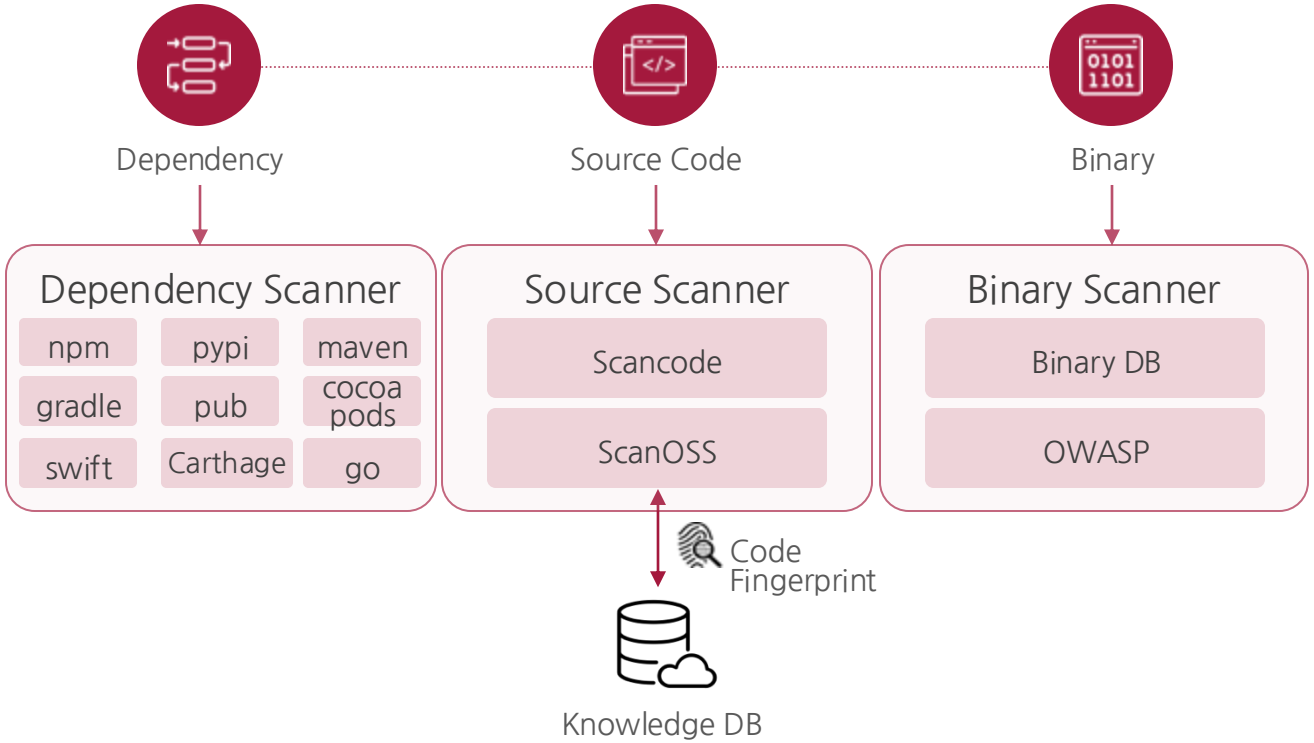
LG Open Source

FOSSLight 컨설팅

기업의 안전하고 효과적인
오픈소스 도입/관리를 위한
교육,
리뷰 등
오픈소스 전문 컨설팅 서비스

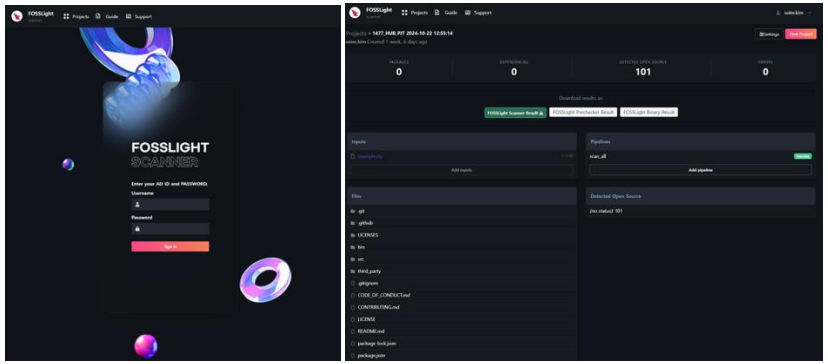
FOSSLight Scanner

독립 모듈 구성



FOSSLight Scanner 웹 서비스 Enterprise

- 번거로운 설치 과정 없이 어디서나 웹으로 서비스에 접속하여, 다양한 형태의 분석을 빠르게 실행
- 분석결과를 바로 한눈에 확인하고 다운로드 받을 수 있음
- On-Premise 사내 클라우드 구현 및 사용 가능



FOSSLight Hub

오픈소스 및 라이선스 관리

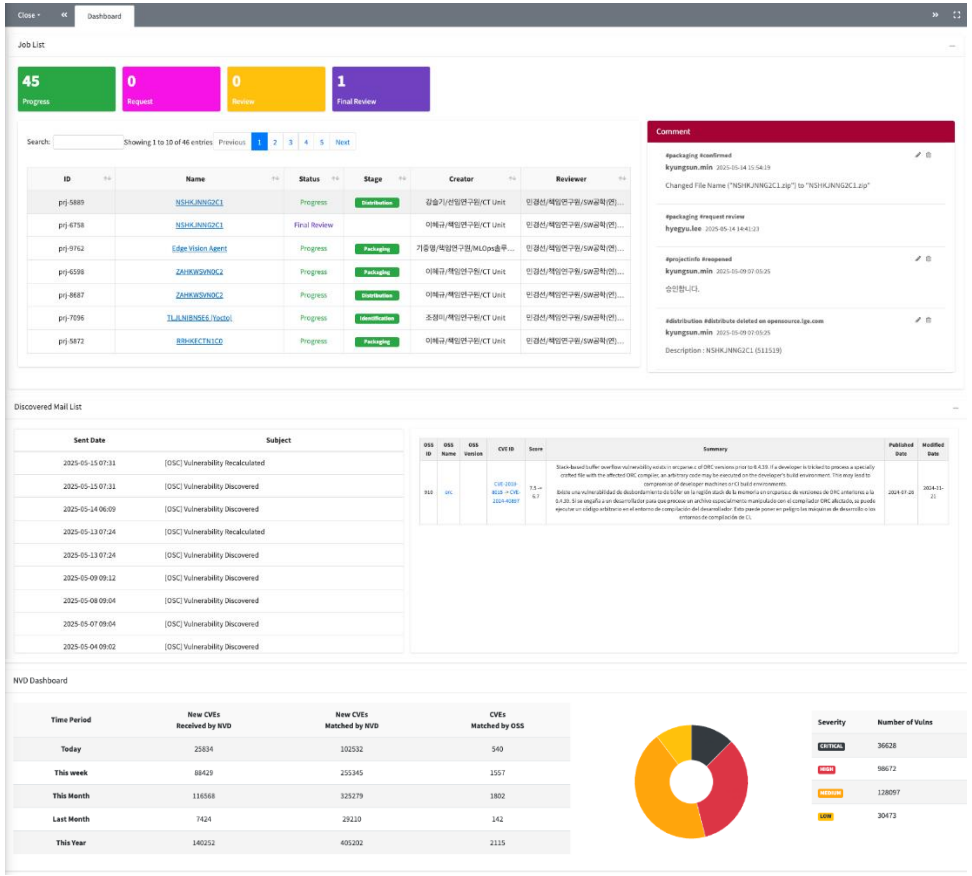
- 오픈소스 정보 통합 관리
- 라이선스 의무사항 및 제약사항 확인
- 오픈소스 및 라이선스 일괄 등록 및 대량의 라이선스 관리 가능
- 오픈소스 패키지 URL 기반 관리

컴플라이언스 프로세스 관리

- 오픈소스 식별, 취합, 배포 등 올인원 오픈소스 컴플라이언스 수행
- 고지문 자동 생성 및 커스터마이징
- 공개 의무 오픈소스 코드 검증
- HTML, TEXT, SPDX 표준의 고지문 제공
- 히스토리 및 이슈 트래킹

SBOM 관리

- 오픈소스 및 상용 소프트웨어 목록 관리
- 소프트웨어별 사용 프로젝트 검색
- 프로젝트 간 SBOM 비교 기능 및 히스토리 추적
- SPDX (ISO 표준) 및 CycloneDX 지원



보안취약점 관리

- NVD의 CVE 정보 기반 보안취약점 조회
- 프로젝트별 보안취약점 모니터링 (자동 메일 알림) 및 조치여부 및 방법에 대한 정보 공유 포털
- 보안취약점 정보에 따라 위험도 파악가능

공급망 관리

- 공급받은 타사 소프트웨어 관리
- 오픈소스 확약서 관리
- 프로젝트 자동 연계 및 프로젝트 별 3rd party 소프트웨어 사용 관리
- 외부 소프트웨어에서 발견된 보안취약점 확인

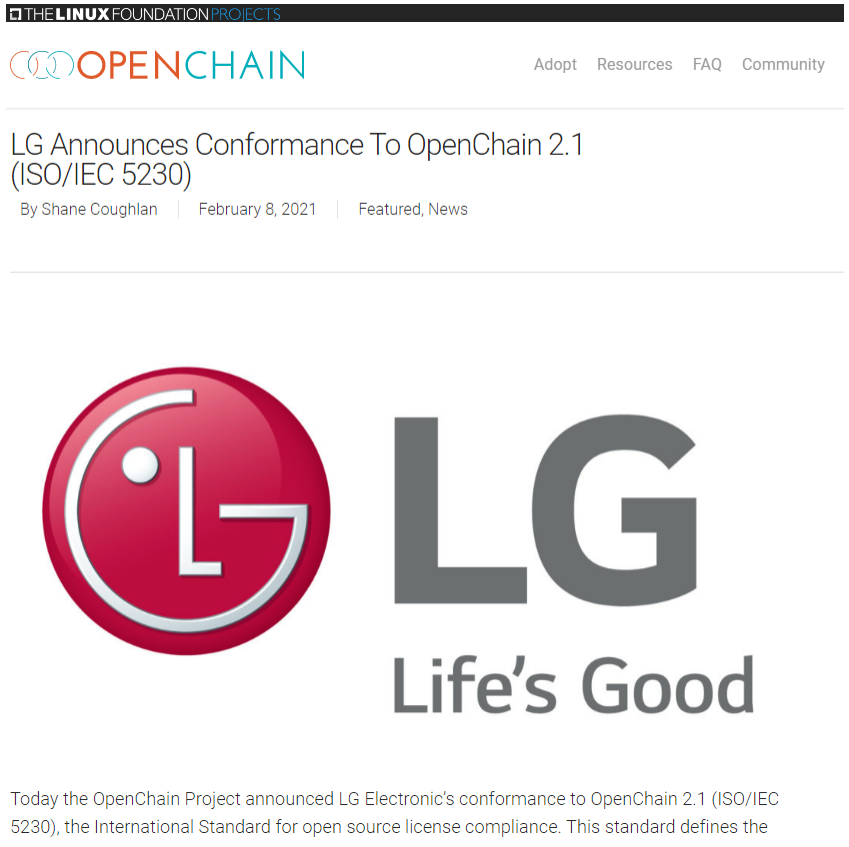
사전 점검

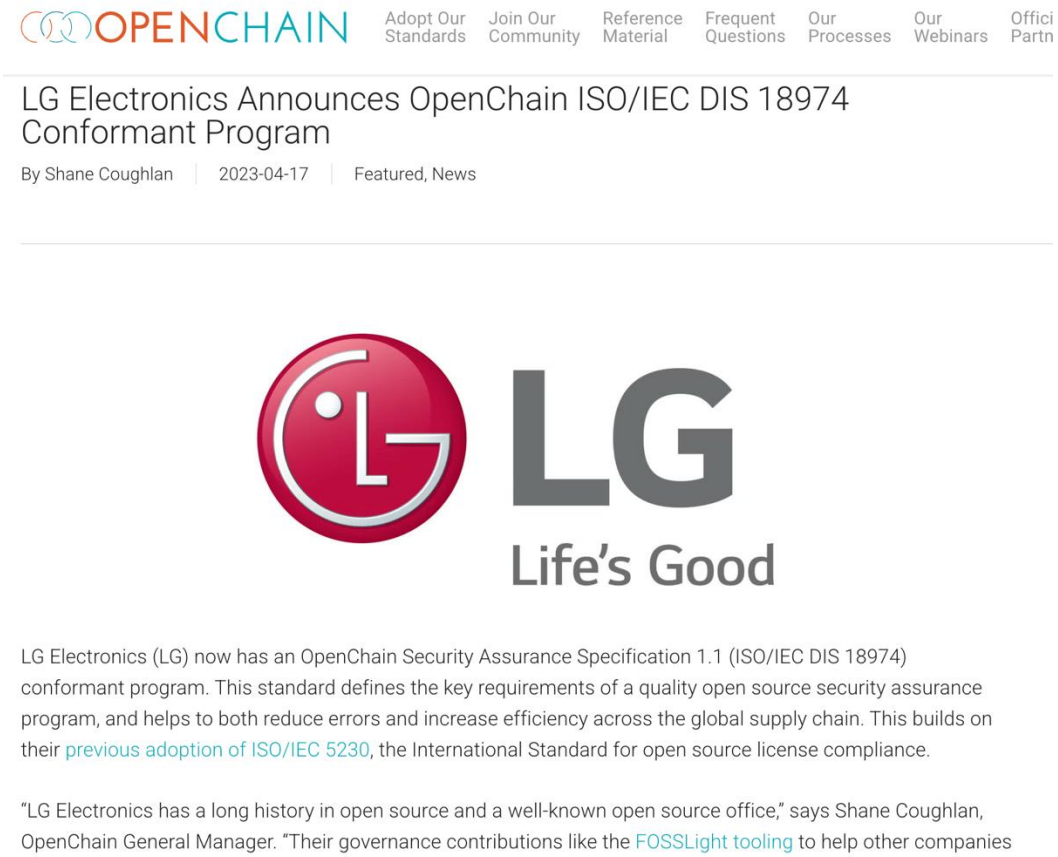
- 개발 레파지토리 URL을 통한 자동 분석
- 다운로드 주소를 통한 라이선스 자동 검출
- 라이선스 의무사항 및 보안취약점 알림
- 오픈소스 고지문 발급 및 확인

LG전자 SW 공급망 관리

OpenChain ISO 5230 / ISO 18974

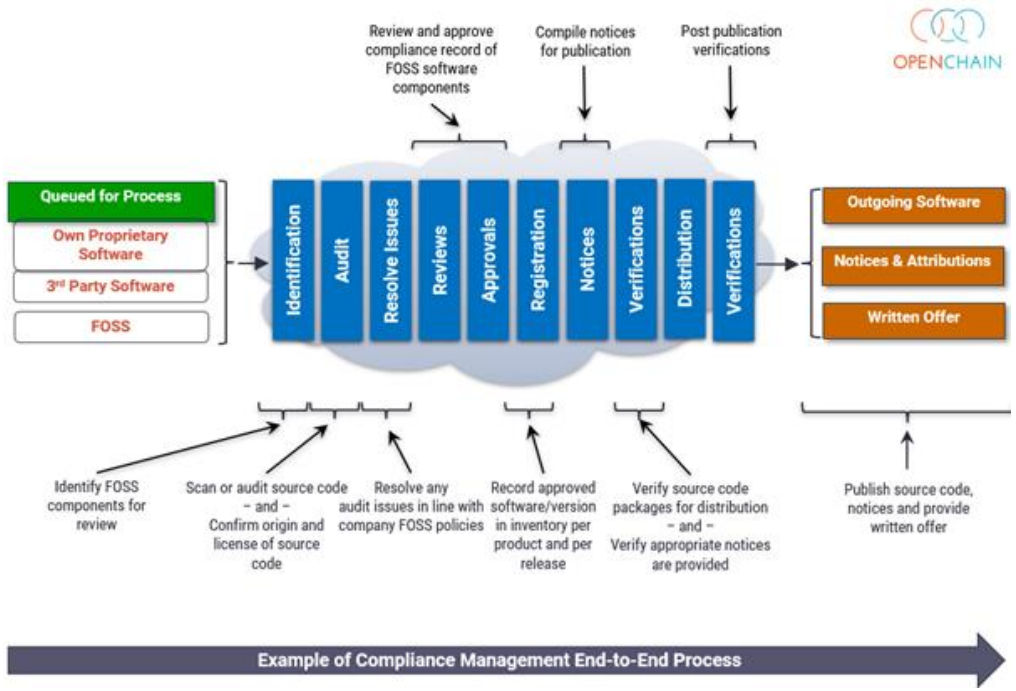
- 오픈소스 컴플라이언스/보안 표준





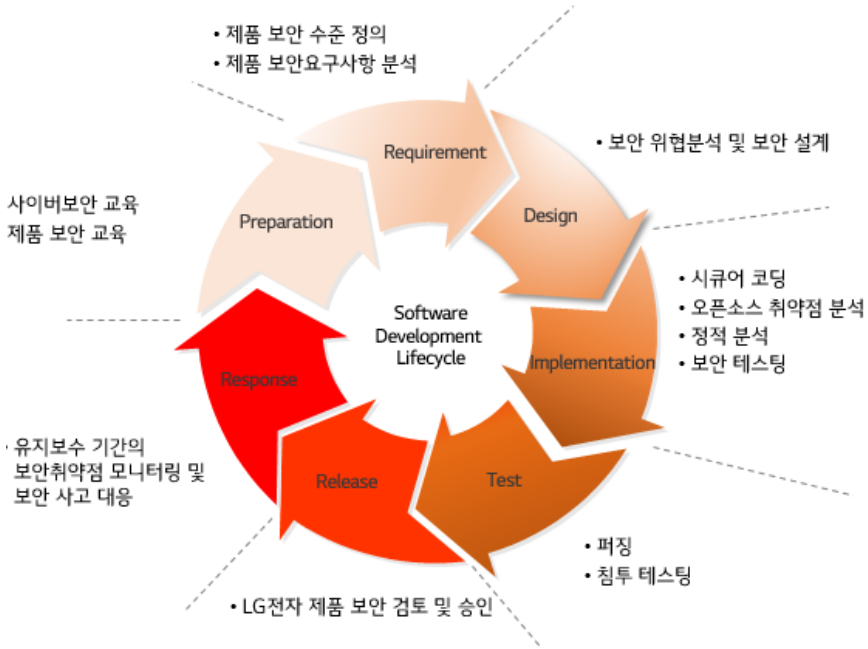
OpenChain ISO 5230 / ISO 18974

OPENCHAIN



ISO/IEC 5230 Conformance

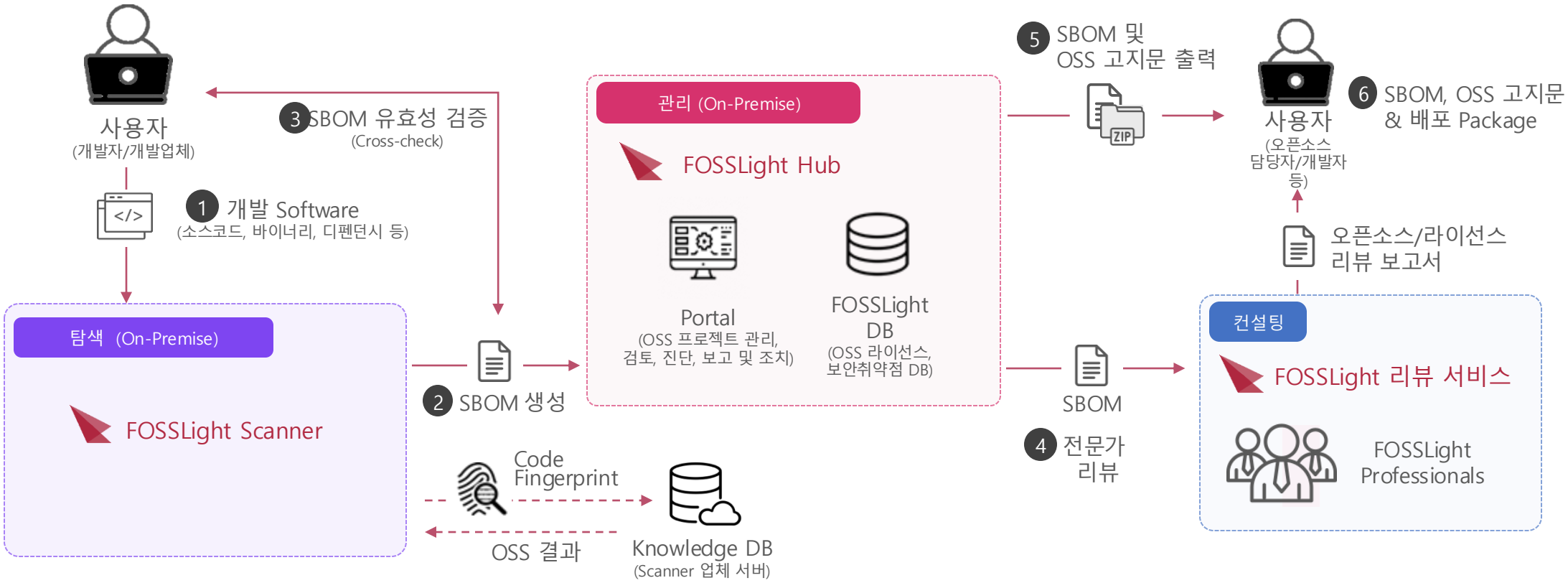
LG전자



The LG Secure Development Lifecycle

ISO/IEC 18974 Conformance

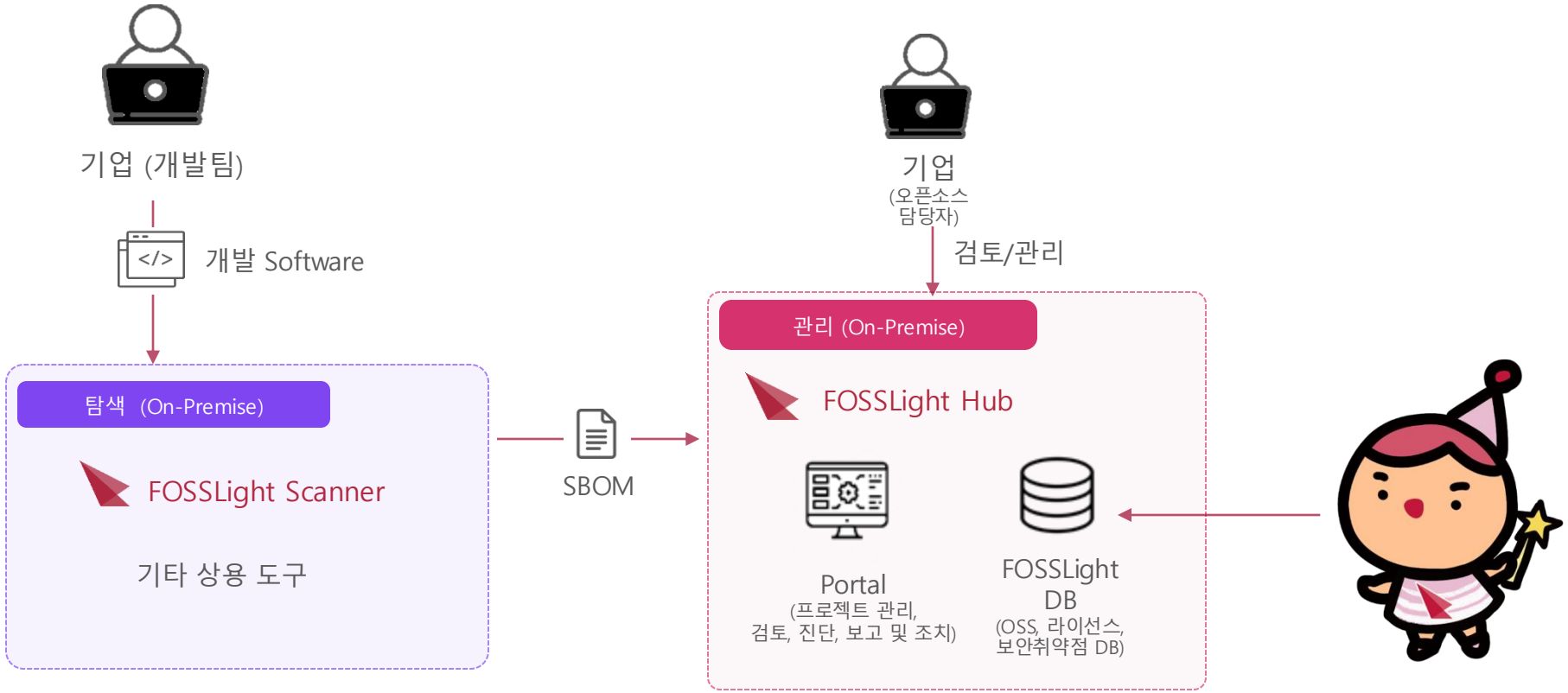
LG전자 SW 공급망 관리



공급망 보안 관리 체계 구축

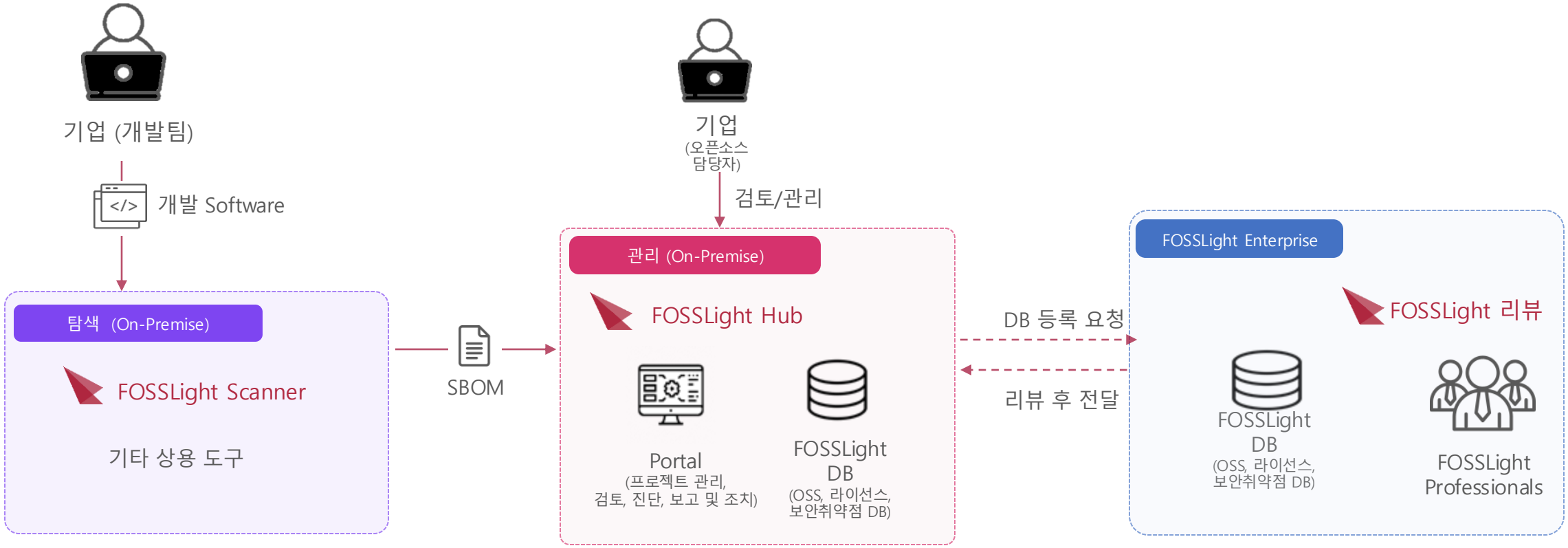
Case 1) FOSSLight Hub + CoReviewer

- **개발/관리가 가능한 오픈소스 조직이 있는 경우**



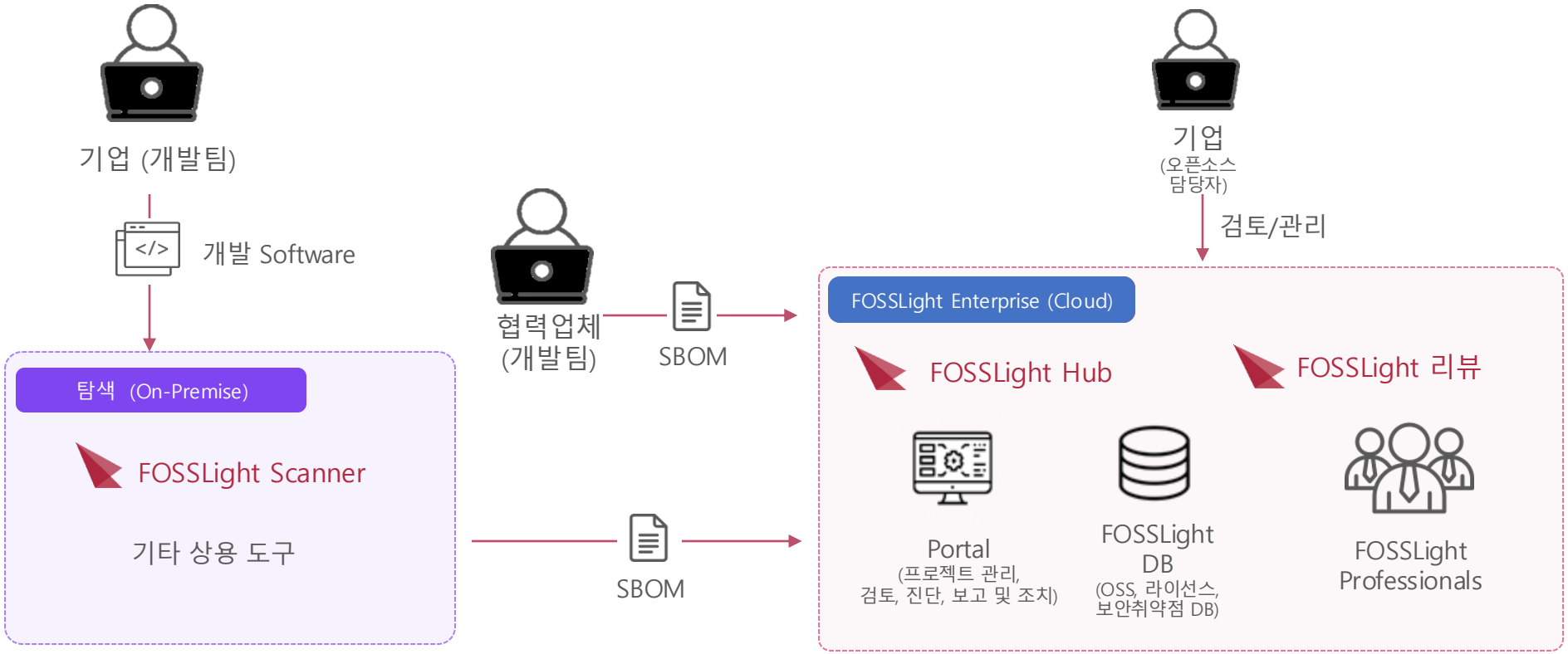
Case 2) FOSSLight Hub + DB Service

- **개발/관리가 가능한 오픈소스 조직이 있으나, 오픈소스 리뷰 부담이 되는 경우**



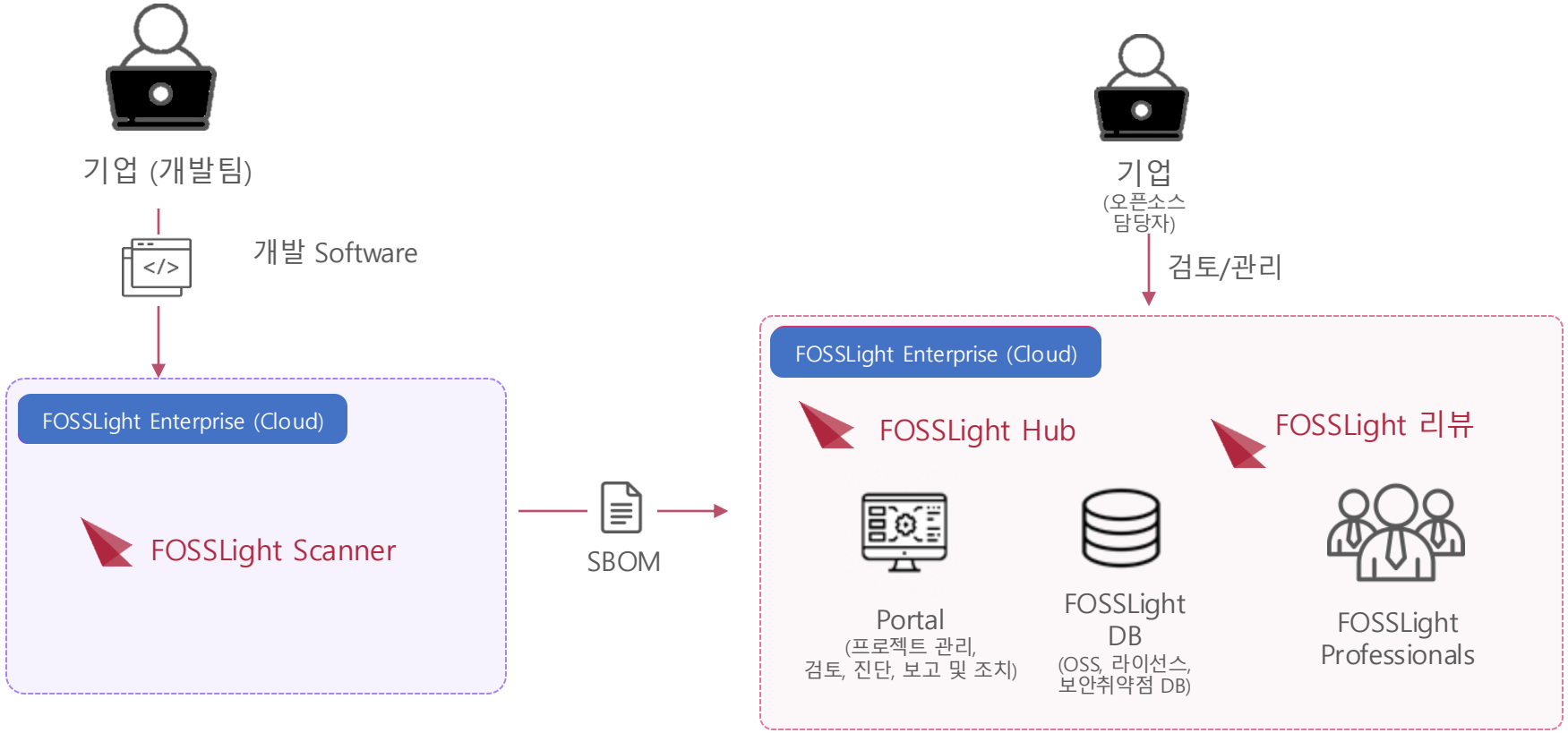
Case 3) FOSSLight Hub (Cloud)

- 개발/관리가 가능한 오픈소스 조직을 별도로 두기 부담되는 경우
- 협력업체와 함께 서비스를 이용하고 싶은 경우



Case 4) FOSSLight Scanner + Hub (Cloud)

- 개발/관리가 가능한 오픈소스 조직을 별도로 두기 부담되는 경우
- 협력업체와 함께 서비스를 이용하고 싶은 경우
- 소프트웨어 외부 반출이 가능한 경우



감사합니다