LABRADOR LABS

Labrador OSS 솔루션 소개

2023

01

오픈소스 사용 현황

소프트웨어 보안취약점 자동분석 시스템

AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

1.1 오픈소스 사용 현황

비대면 및 디지털 전환에 의한 오픈소스 SW 활용 급등

오픈소스 SW 적극 활용추세

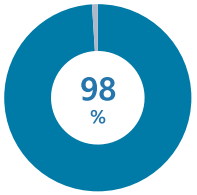
✓ **스마트폰 80% 이상 리눅스 기반 안드로이드**
(디지털데일리 2020년 9월)

✓ **금융권 운영체제의 80% 이상이 리눅스 및 유닉스**
(금융보안원 2016년)

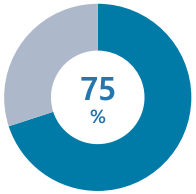
✓ **'2020년 사이버 보안 이슈 전망 보고서 ' 는 "금융권의 디지털 전환을 위해서는 오픈소스의 활용이 필수불가결함 " 을 발표**
(금융보안원 2020년)

4차 산업혁명 도래와 더불어 AI, 클라우드, 빅데이터, IoT 등 융합분야 활용 가속화 중

글로벌 오픈소스 사용 현황



기업의 98%
오픈소스 활용



개발 코드의 75%
오픈소스로 구성
(시놉시스 2021)

2021년 글로벌 **2억**개의
오픈소스 프로젝트

하루 1만개 이상 프로젝트 생성

국내 오픈소스 사용 현황

오픈소스 거버넌스 구축에 많은 어려움을 겪고 있는 상황

- 커뮤니티 수는 0.2%, 개발자 수는 0.05%, 글로벌 프로젝트 수는 1.2% 수준
- 개발자들은 본인이 오픈소스 코드를 사용하고 있는지 자각하지 못하고 있는 상황

〈표 2〉 국내외 오픈소스 SW 커뮤니티 및 인력 현황 비교

구분	해외	국내
개발자 수 (커미터 수)	약 20,000,000명 (약 40,000 명)	약 15,323명 (약 780 명)
커뮤니티 수	약 167,000 개	약 370 개
글로벌 프로젝트 수	약 800 건	약 10 건

자료 : 정보통신산업진흥원 ('19.07)

1.2 오픈소스 사용 위험 현황

“ 오픈소스 적극 활용 추세에 따라 보안 취약점, 라이선스 리스크 확대

보안 위협 현황

✓ **2~4년 전 배포된 리눅스 커널 기반으로 최신 기기가 운영되며, 평균 200~300개의 취약점을 내포하고 있음**
(LABRADOR LABS 자체조사결과)

✓ **알려진 취약점인 CVE가 14만개 이상 공개 되었으며, 매일 50개 이상의 새로운 취약점이 발견**
(www.cvedetails.com)

✓ **전세계 금융거래의 50%이상이 오픈소스를 통해 처리되고 있으며, 전체 오픈소스 75%에 한 개 이상의 취약점 보유**
(코스콤 2021년)

오픈소스 취약점 발생 사례

오픈소스명	발생시기	내용
아파치 스트럿츠	'17.5월	· 미국의 신용평가기관인 에퀴팩스(Equifax)는 웹 애플리케이션 개발 오픈소스인 아파치 스트럿츠의 원격코드 실행 취약점 공격으로 약 1억 4천만 명의 개인정보 유출
MySQL	'19.5월	· 오픈소스 데이터베이스인 MySQL 서버의 기본 포트를 통해 암호화 되어있지 않은 서버를 확인하고 랜섬웨어 공격을 시도
쿠버네티스	'19.6월	· 쿠버네티스에서 파일 복사 시 경로 조작을 통해 악성 파일 실행이 가능한 취약점이 발견되어 디렉토리 탐색 공격[18] 발생

*CVE: Common Vulnerabilities and Exposures

라이선스 위반 현황

삼성전자, 한컴 등 오픈소스 라이선스 규정 위반으로 손해배상

- 삼성전자는 리눅스 커널의 코드 및 BusyBox 사용 시, 라이선스 위반으로 손해배상 판결
- 2018년 한컴오피스 듀얼라이선스 미인지로 인해 23억원 지불

LG CNS 오픈소스 라이선스 규정 위반으로 법정 공방

- 2008년 LG CNS가 구매한 GS인증 제품의 판매사가 라이선스를 위반하여, 양사가 고소를 당함으로 LG CNS 대표가 체포된 사례가 있음

(금융보안원)

금융권, OSS 리스크 관리 안되고 있어...법적 분쟁/보안사고 발생 우려 ↑

- 금융권이 대부분 애플리케이션 내 오픈소스에 대한 법적 고지의무 등 기본적인 라이선스 규정도 지키지 않는 상황

(데일리시큐 2020년 07월)

1.3 오픈소스 사용 리스크 대응

> 오픈소스 적극 활용에 따른 취약점, 라이선스 이슈 증가로 이에 대한 효율적인 리스크 해결 방안 마련이 필요

조직 내부 Pain Point

- ✓ 오픈소스, 취약점 수동 관리에 따른 비효율성
- ✓ 취약점 발견 시 개발 담당자 확인 어려움
- ✓ 취약점 조치여부 확인 및 후속 관리 곤란
- ✓ 특정 취약점 발견 시 해당 프로젝트 확인 애로

→ 취약점 수동 관리에 따른 비효율 및 애로사항 발생

자동화된 OSS 취약점 관리 시스템 필요

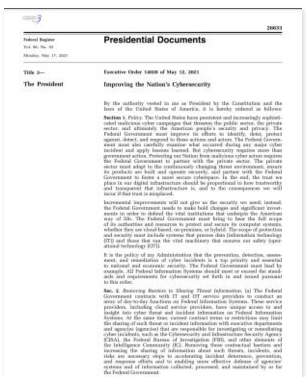
SBOM은 S/W 구성요소의 정보 및 공급 관계 추적 가능하여 취약성을 탐지하고 문제 발생시 신속한 수정을 지원

SBOM (Software Bill of Materials) 동향

SBOM이란?

- 식품 성분 명세서와 같이, 개발 결과물의 모든 SW 구성 항목 정보 제공
- 취약점, 라이선스 이슈 정보 포함

SBOM의 제도화 추세



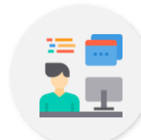
미 대통령 행정명령
(2021.05.12.)

Section 4
소프트웨어 공급망의 안전보장 향상
-
국가기관 납품 소프트웨어의
SBOM 제공 의무화 명시 ('22.12)

SBOM의 시장 파급 효과

- 미국 관공서에 납품하는 모든 소프트웨어는 SBOM 의무 제공
- 미국 제조사 납품 국내 협력 회사에도 SBOM 제공 요구 중
- 미국 FDA 의료기기 제품 출시 전, SBOM 제공 권고 중

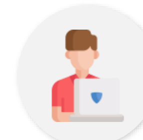
Labrador SBOM 대응



Developer

- 오픈소스 소프트웨어 자동관리
- 안전한 소프트웨어 재사용 가능

SBOM
소프트웨어 목록관리
라이선스 점검
보안취약점 검증



User

- 높은 신뢰도의 소프트웨어 사용
- 이슈 발생시 대응 용이

Labrador

✓ 분석 특허 알고리즘 활용, 정확한 SBOM 생성

✓ 국내 최초로 SBOM 표준 Export 기능 제공(SPDX/CycloneDX)

사례
미국 Intuitive사, SBOM 솔루션으로 Labrador 도입(2023)

LABRADOR LABS

02

래브라도랩스 소개

소프트웨어 보안취약점 자동분석 시스템

AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

2.1 LABRADOR LABS 소개

> ‘18년 설립 이후 오픈소스 소프트웨어의 사용 리스크 자동 탐지 및 관리 솔루션 제공

기업 개요

LABRADOR LABS

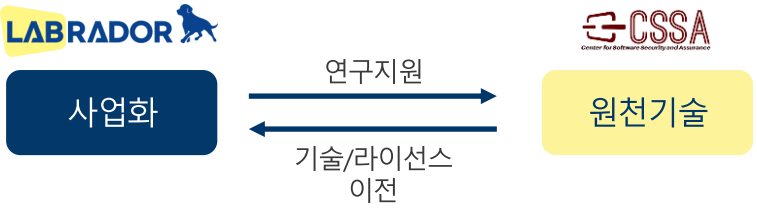
“Find all bugs with Labrador”

【회사 소개】

래브라도랩스는 소프트웨어 보안취약점을 찾아내는 자동화된 분석 시스템을 구축하기 위한 학술 연구 협력 프로젝트로 부터 시작했습니다. 연구실에서 발현된 참신하고 혁신적인 기술을 사용하여 국내외 소프트웨어 개발 환경에 기여하고자 회사를 설립하게 되었습니다

현재 보안취약점 자동분석 기술을 기반으로 소프트웨어 보안과 라이선스 분석 자동화 제품인 래브라도를 출시하여 국내외 다양한 사이트에 서비스를 제공하고 있습니다.

설립일	2018. 3월
위치	서초구 반포대로 53, 4~5F
대표자	이희조, 김진석
임직원 수	31명



- 회사와 연구소간 공동 DB TF 운영
- 보안 및 오픈소스 거버넌스 컨설팅 TF 운영
- Chief Scientist 제도 운영

* CSSA
(Center for Software Security and Assurance)

고려대학교 컴퓨터학과 4개 연구실을 중심으로
미국 카네기멜론, 영국 옥스포드, 스위스 ETH 대학의 연구팀이 모여
2015년 설립한 연구센터

2.2 주요 연혁 및 특허 현황

주요 연혁 & IP(지적재산권) 현황

- **2023** 03월 삼성증권 오픈소스 취약점 관리체계 구축 수주
- **2022** 06월 신SW상품대상(과기부장관상)수상
  GS인증(1등급) 획득
  04월 삼성화재 IVAS 구축 사업 수주
- **2021** 12월 Labrador Fuzzer 1.0 Beta 런칭
  08월 Labrador OSS 2.0 런칭
  03월 Series-A 40억 투자 유치(기업은행 외 3개사)
- **2020** 12월 국방부 통합 분석 플랫폼 구축 완료
  07월 2020 제14회 상반기 대한민국 우수특허 대상 IT 부분 선정
- **2019** 08월 제3회 LABRADOR LABS 컨퍼런스 개최, 래브라도 1.0 런칭
  05월 고려대 스마트팩토리 융합보안대학원 협업 체계 확립 (https://sec.korea.ac.kr)
- **2018** 10월 중소기업벤처부 TIPS 선정 (고려대 기술지주 자회사 TIPS 1호)
  03월 고려대 기술지주자회사 ㈜래브라도랩스 설립 (CSSA 스핀오프)

No.	구분	출원국	출원 및 등록 번호	지식재산권(특허)명
1	Application	대한민국	10-1568224	소프트웨어 취약점 분석 방법 및 분석장치
2	Open Source	미국	10-146532	APPARATUS AND METHOD FOR DETECTING CODE CLONING OF SOFTWARE
3	Open Source	대한민국	10-1780233	소프트웨어의 코드 클론 탐지 장치 및 방법
4	Binary	대한민국	10-2104295	탐색 전략을 자동으로 생성하는 방법 및 자동으로 생성된 탐색 전략을 사용한 콘콜릭 테스팅 수행 방법
5	Binary/ Protocol	대한민국	10-2104610	네트워크 프로토콜의 취약점을 탐지하는 퍼징 방법 및 장치
Moverly		다양한 코드 형상으로 전파된 취약코드를 높은 정확도로 탐지하는 탐지 기술		
xVDB		NVD의 reference 링크 위주로 고려하던 기존 접근법보다 더욱 확장된 취약점 DB 수집 기술		

2.3 제품 사용 사례

국내외 유수기관 및 업체가 래브라도의 우수성을 인정하고 있음

01 삼성전자 보안 내재화 (2018)

개발된 소스 코드의 보안 취약점 자동 검사

SAMSUNG ELECTRONICS

02 수술용 로봇 업체와 계약 (2022~)

국내 최초로 글로벌 시장에 SBOM 제공 솔루션 수출

03 삼성화재 오픈소스 취약점 점검 솔루션 구축 (2022~)

보험업계 1위 사업자, 동종업계 최초로 **IVAS** 도입

삼성화재

* IVAS : Integrated Vulnerability Analysis System

04 삼성증권 오픈소스 취약점 관리체계 구축(2023~)

증권사 TOP 3 사업자, 동종업계 최초로 **IVAS** 도입

삼성증권

* IVAS : Integrated Vulnerability Analysis System

05 국방 무기체계 SW 안전성 검증 (2020~)

국방부 통합 취약점 분석 플랫폼 구축

대한민국 국방부
Ministry of National Defense

06 KT 기기 보안 검증 (2020~2021)

KT의 IoT 기기 보안성 검증(취약점 검출)

kt

07 국가보안기술연구소 드론 취약점 분석 (2021~)

RVDB* 축적 및 연구 협력

NSR 국가보안기술연구소

* RVDB : Robot Vulnerability Database

08 아우토크립트 오토모빌 취약점 보안 검증(2021~)

대형 오토모빌 제조업체의 보안 검증에 활용

AUTOCRYPT

LABRADOR LABS

03

Labrador OSS 소개

소프트웨어 보안취약점 자동분석 시스템

AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

3.1 Labrador OSS 특장점

Labrador 솔루션은 3-Layer 취약점 분석과 같이 차별화 기술을 통해 높은 분석 정확도를 제공하며, 고객사의 사용 환경에 최적화된 솔루션 제공

3-Layer 분석

- 컴포넌트/파일/함수 단위의 3중 분석 통한 90% 이상의 정밀도
- 함수 단위의 미세 분석 기반으로 정확한 SBOM 정보 제공

공신력 있는 기관의 경쟁력 입증

- 한국과학기술원 주관 평가에서 경쟁사 대비 우수한 평가 획득
- 취약점 및 컴포넌트 탐지 등 기능, 사용성 측면에서 경쟁 우위

쉽고 편리한 취약점 해결방안 제공

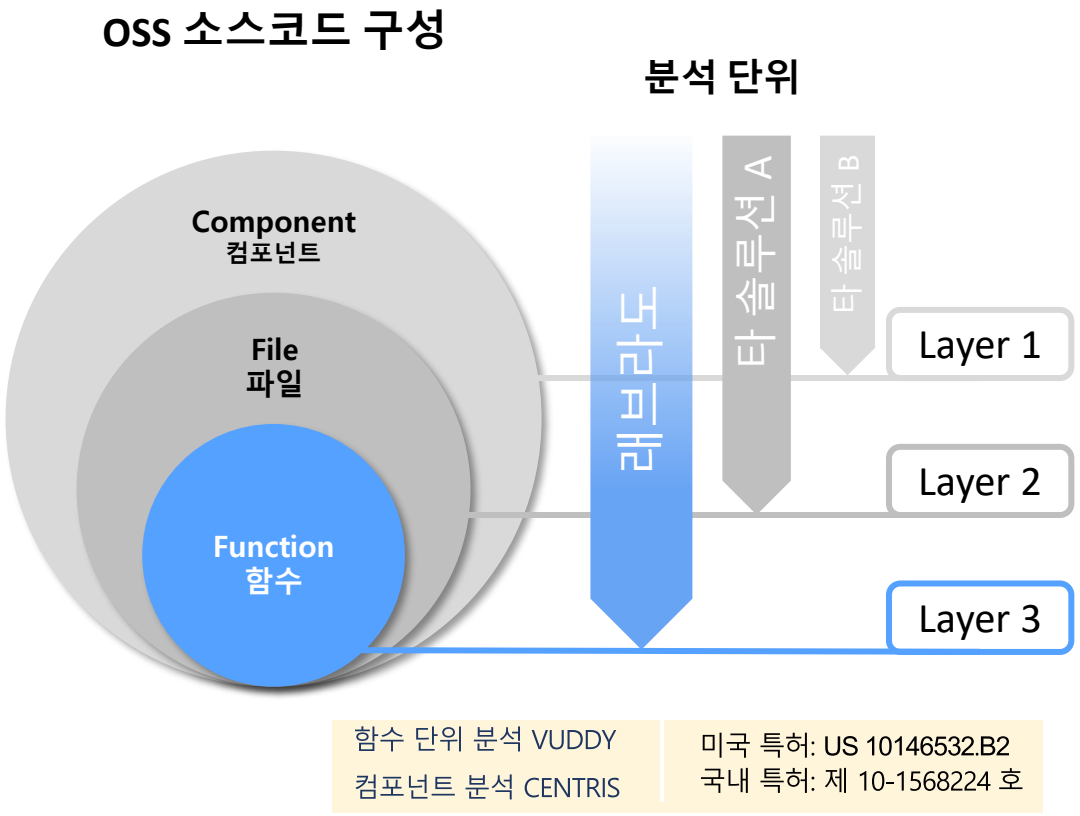
- Pin Point 패치정보 제공
- 취약점 우선순위 정보 제공

IVAS 플랫폼 구축 경험

- 2019년 국방부 및 2022년 삼성화재 IVAS 플랫폼 구축 경험을 통한 신뢰도 높은 시스템 구축 가능

3-Layer 분석 개요

래브라도는 3-Layer 취약점 분석을 근간으로 오픈소스 소프트웨어의 구성요소(SBOM)를 정확히 탐지하고, 이를 기준으로 쉽고 편리한 취약점 분석 및 해결 방법을 제공



함수 단위 분석 VUDDY
컴포넌트 분석 CENTRIS

미국 특허: US 10146532.B2
국내 특허: 제 10-1568224 호

3-Layer Analysis, Only 래브라도 !!

1 정확한 SBOM 제공

✓ 다양한 디펜던시 분석으로 정확한 소프트웨어 구성 요소 탐지

2 획기적인 취약점 탐색 정확도 제공

✓ 함수 단위 미세분석으로 오탐 및 과탐 발생율 제로 수준

3 취약점만 해결 가능한 백포팅 해법 제공

✓ 문제되는 취약점 부분만 해결 가능한 검증된 패치정보 제공

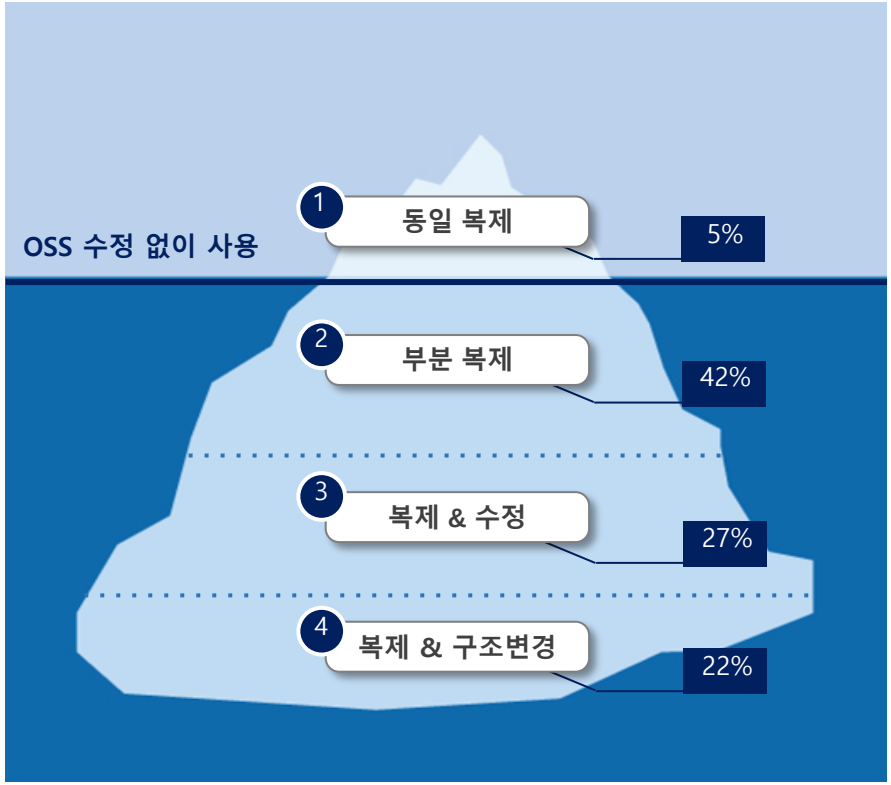
4 사용자 정의 취약점 등록 및 관리 가능

✓ 컴포넌트 단위 포함, 함수단위의 자체 취약코드 등록 및 탐지 기능으로 자체취약점 관리

3-Layer 분석 특성

오픈소스 소프트웨어 활용 시, *95%의 오픈소스 소프트웨어가 부분 복제되거나, 수정 및 변경되어 재사용되고 있습니다.
3-Layer 취약점 분석 방식은 컴포넌트, 파일 및 함수 단위까지의 취약점 분석을 실행하기 때문에 다양한 활용 형태에 대응 가능하여 오탐 및 과탐을 최소화합니다.

분석 대상 사용자 S/W 활용 형태



3-Layer 분석 방식

OSS 활용 형태	**컴포넌트** 단위 취약점 매칭 (Layer 1)	**파일** 단위 취약점 매칭 (Layer 2)	**함수** 단위 취약점 매칭 (Layer 3)
1 동일 복제	○	○	○
2 부분 복제	△ 일부 탐지 가능	○	○
3 복제 & 수정	X	X	△ 일부 탐지 가능
4 복제 & 구조변경	X	△ 일부 탐지 가능	△ 일부 탐지 가능

"CENTRIS: A Precise and Scalable Approach for Identifying Modified Open-Source Software Reuse" IEEE/ACM Int'l Conf. on Software Engineering (ICSE), May 2021.
https://ccs.korea.ac.kr/pds/ICSE21.pdf

04

Labrador OSS 주요 기능

소프트웨어 보안취약점 자동분석 시스템

AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

4.1 다양한 Scan Mode 제공

사용자의 환경을 고려하여 다양한 소스코드 스캔 방식 제공

Option 1

CLI

사용자 시스템의 Command Line에서 소스코드 스캔 후 결과 확인
(코드 프라이버시가 보장되는 Hashed 암호파일 업로드)

Option 2

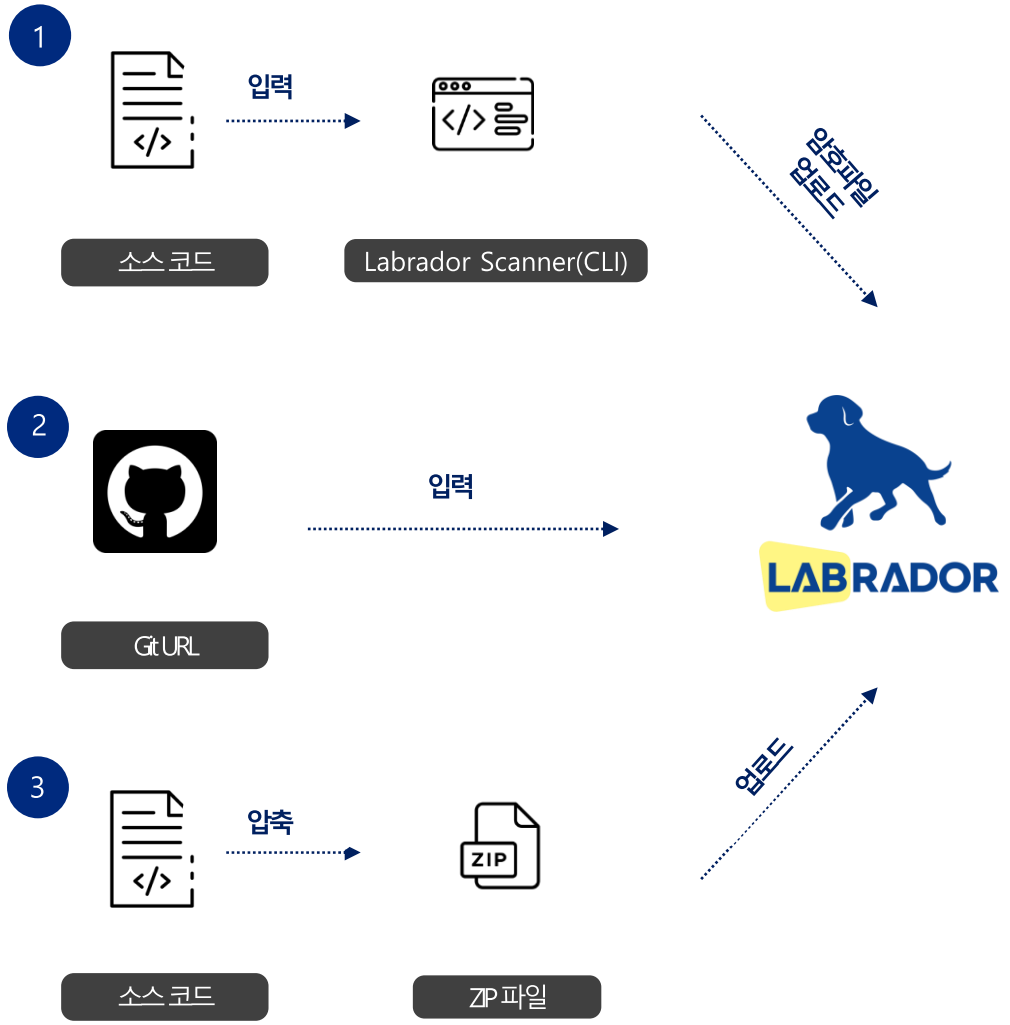
Git URL

Public/Private 저장소의 소스코드 URL을 입력하면
자동 스캔 및 분석

Option 3

ZIP Upload

분석대상 소스코드를 압축해서 업로드 후
자동 스캔 및 분석



4.2 오픈소스 라이선스 컴플라이언스 관리

> 소스코드 심층 분석 통해 오픈소스 라이선스 정보 수집 및 컴플라이언스 이슈에 대한 사전 대응

라이선스 컴플라이언스 관리

- 오픈소스 라이선스 이슈 정보 제공 통해 컴플라이언스 리스크 제거
- 검출된 라이선스의 고지문 예제 자동 생성

오픈소스 취약점 정보 제공 기능

01 정확한 취약점 정보 제공

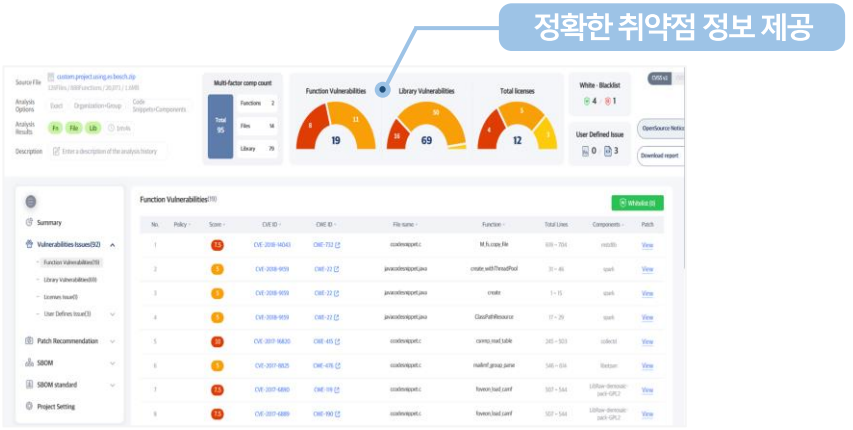
- 취약점에 대한 3-Layer 분석 기반 90% 이상의 정밀도
- 변경된 소스코드에 대해서도 정확한 분석 가능

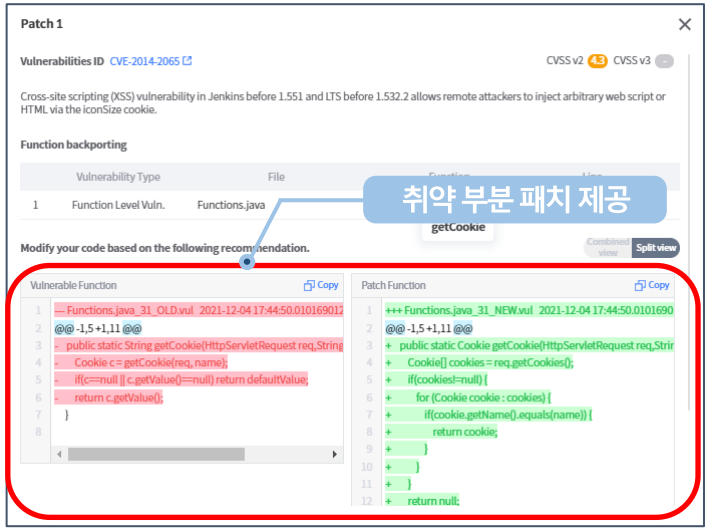
02 Pinpoint 패치정보 제공

- 취약한 부분의 코드만 수정하여 개발 효율 극대화
- 단순 버전 업그레이드와 달리, 부작용 사전 방지 가능

03 취약점 우선순위 정보 제공

- CVSS 기준 위험 스코어 정보 제공
- CWE Top 25별 추천 패치 우선 순위 정보 제공





오픈소스 프로젝트의 분석 이력 자동 관리

01 회사 내 그룹별 사용 지원

- 그룹 및 프로젝트 별 독립된 사용환경 및 이력 관리 제공
- 최상위 관리자의 통합 관리 기능 제공

02 분석 이력 관리

- 프로젝트 취약점, 라이선스 이슈 및 조치 이력 확인
- 프로젝트 버전 별 비교 분석 기능 제공

03 다양한 보고서 제공

- PDF 형식의 요약 보고서 제공
- 엑셀 형식의 상세 보고서 제공

4.5 조직 내 소프트웨어 거버넌스 정책 자동 관리

소프트웨어 거버넌스에 대한 다양한 정책 및 자동화 지원

01 자체 취약점 및 컴포넌트 관리

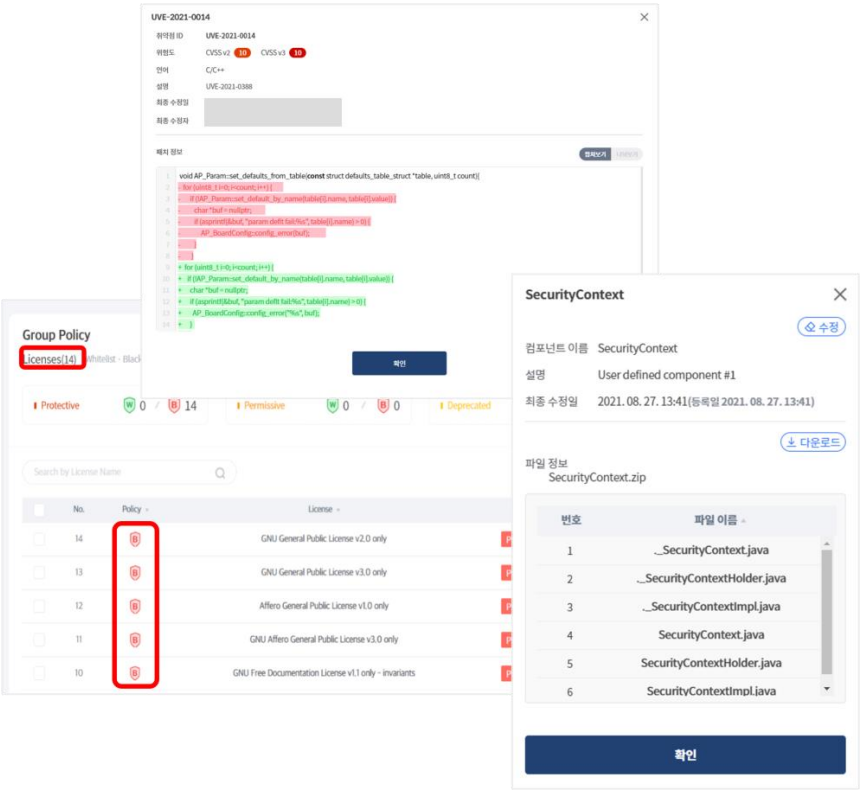
- 자체 개발한 소스코드의 취약점 자동 관리 기능 제공
- 조직 내 사용금지 된 컴포넌트 자동 필터링 기능 제공

02 Whitelist / Blacklist 관리

- 특정 CVE / CWE / 컴포넌트 / 라이선스에 대한 조직내 정책 자동 관리 기능 제공

03 미등록된 취약점 관리

- CVE에 미등록된 취약점 등록 및 관리 기능 제공



4.6 SBOM 국제 표준 포맷 제공

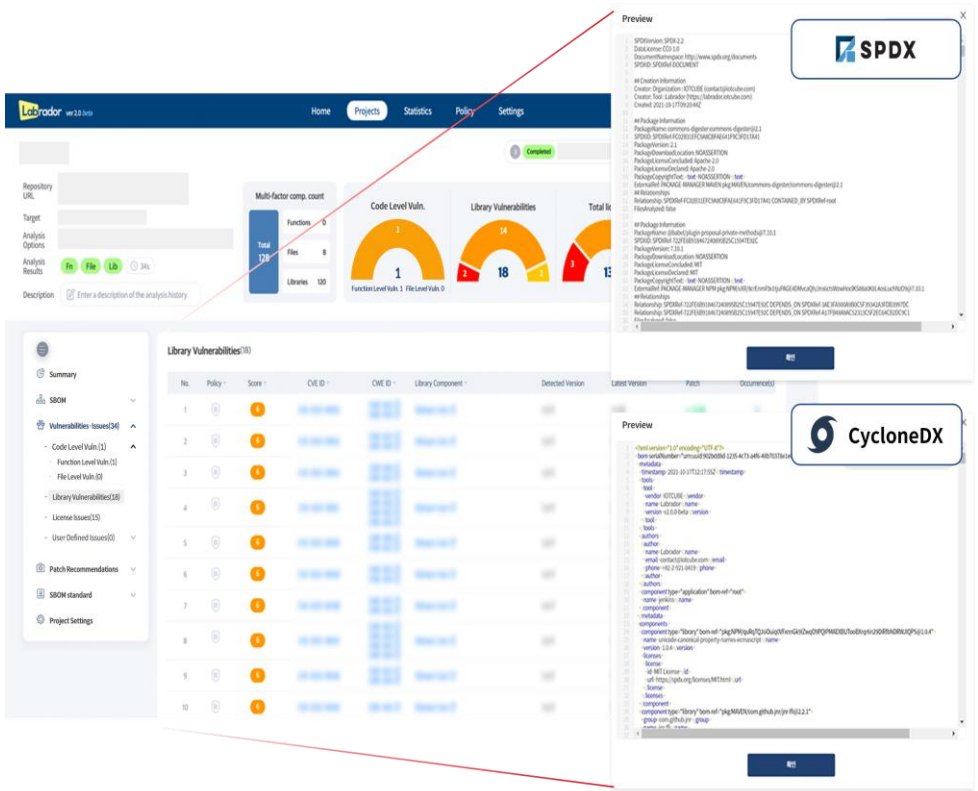
SPDX & CycloneDX 국제 표준 포멧 제공

01 국제 표준 포맷 지원

- 안전하고 투명한 소프트웨어 공급망 관리를 위해 SBOM 국제 표준인 SPDX, CydoneDX 지원

02 S/W 공급망 관리 지원

- SDLC 전 단계에서 S/W 구성요소 추적관리
- 협력업체를 포함한 3rd party S/W 구성요소 관리
- 구성요소 관리를 통한 S/W 공급망 공격 예방



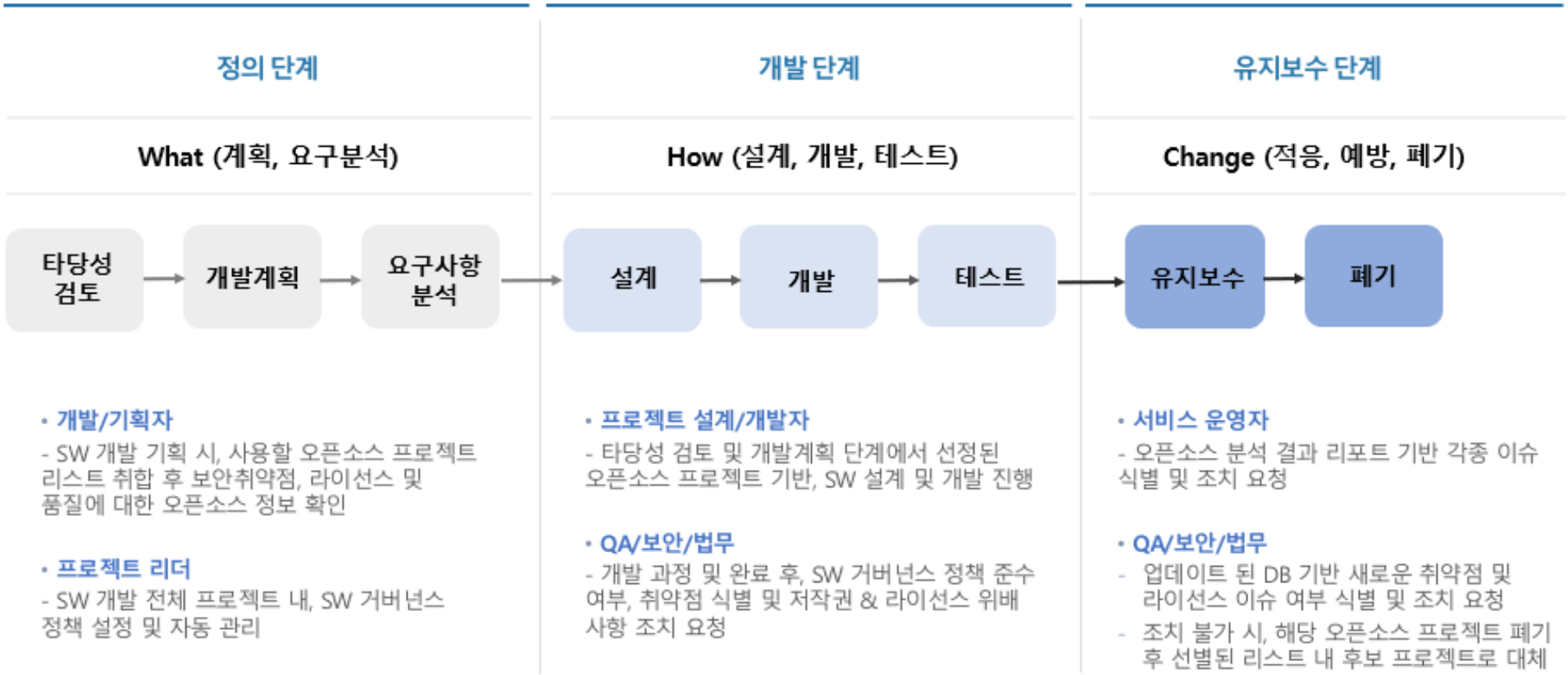
LABRADOR LABS

05
Labrador 운영 환경

소프트웨어 보안취약점 자동분석 시스템
AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

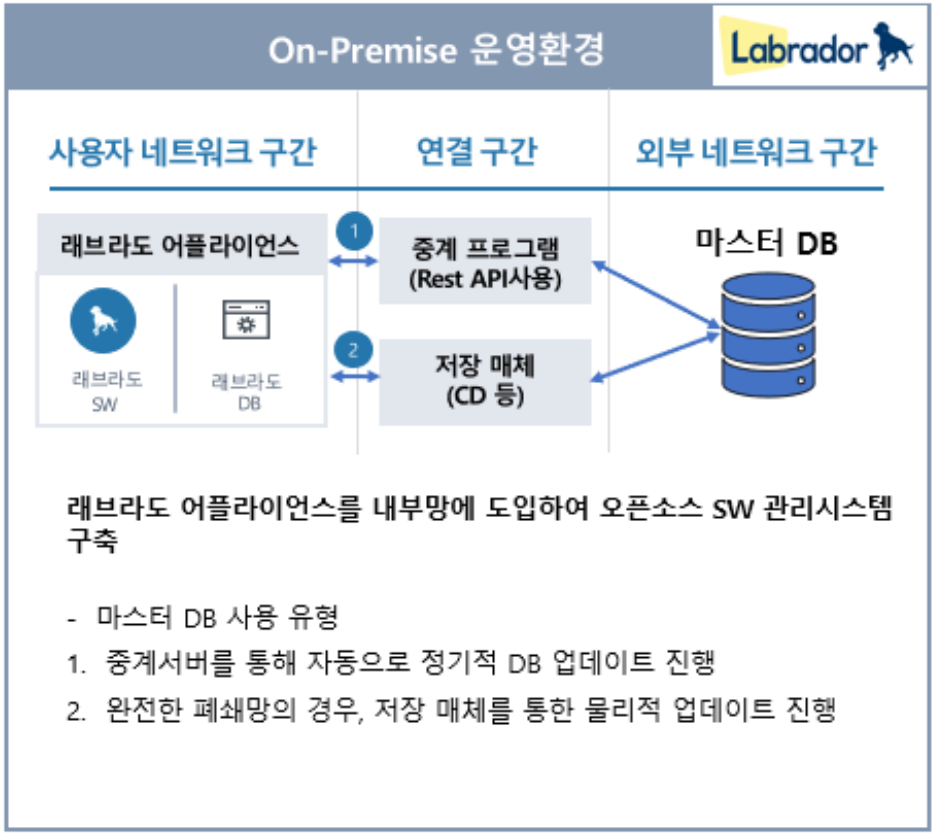
5.1 SDLC 단계별 오픈소스 관리 운영 방안

SDLC의 정의 단계, 개발 단계 및 유지보수 전 단계에 걸쳐 오픈소스 관리 지원



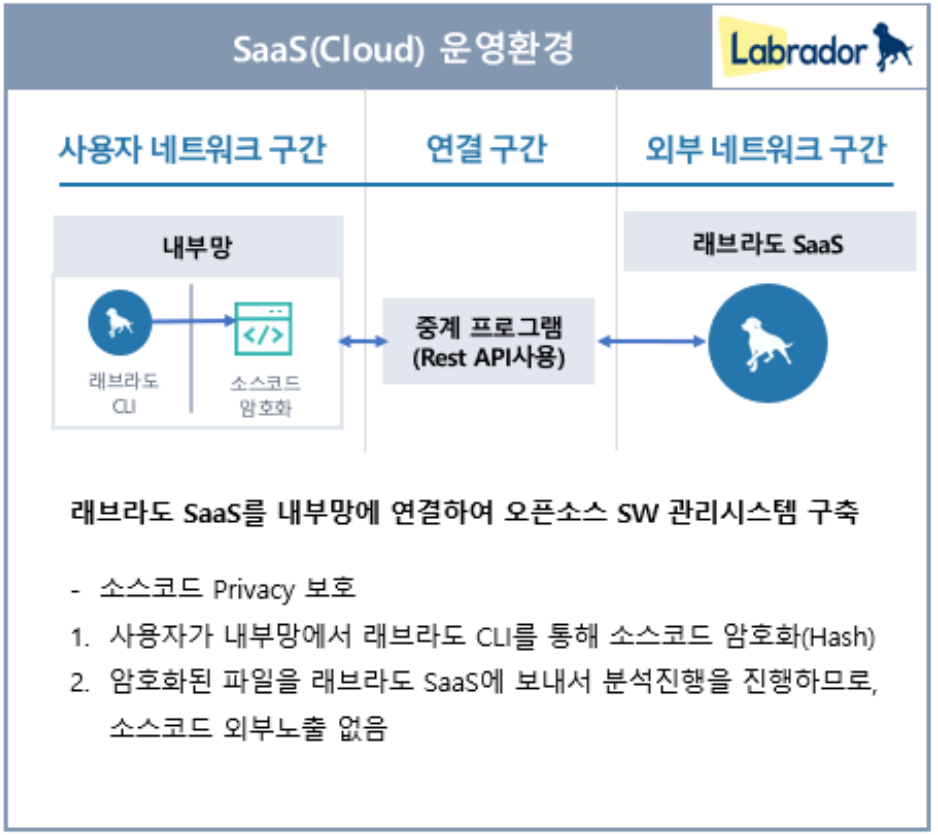
5.2 래브라도 구축 환경

On-Premise 및 SaaS 방식의 운영환경 제공



래브라도 어플라이언스를 내부망에 도입하여 오픈소스 SW 관리시스템 구축

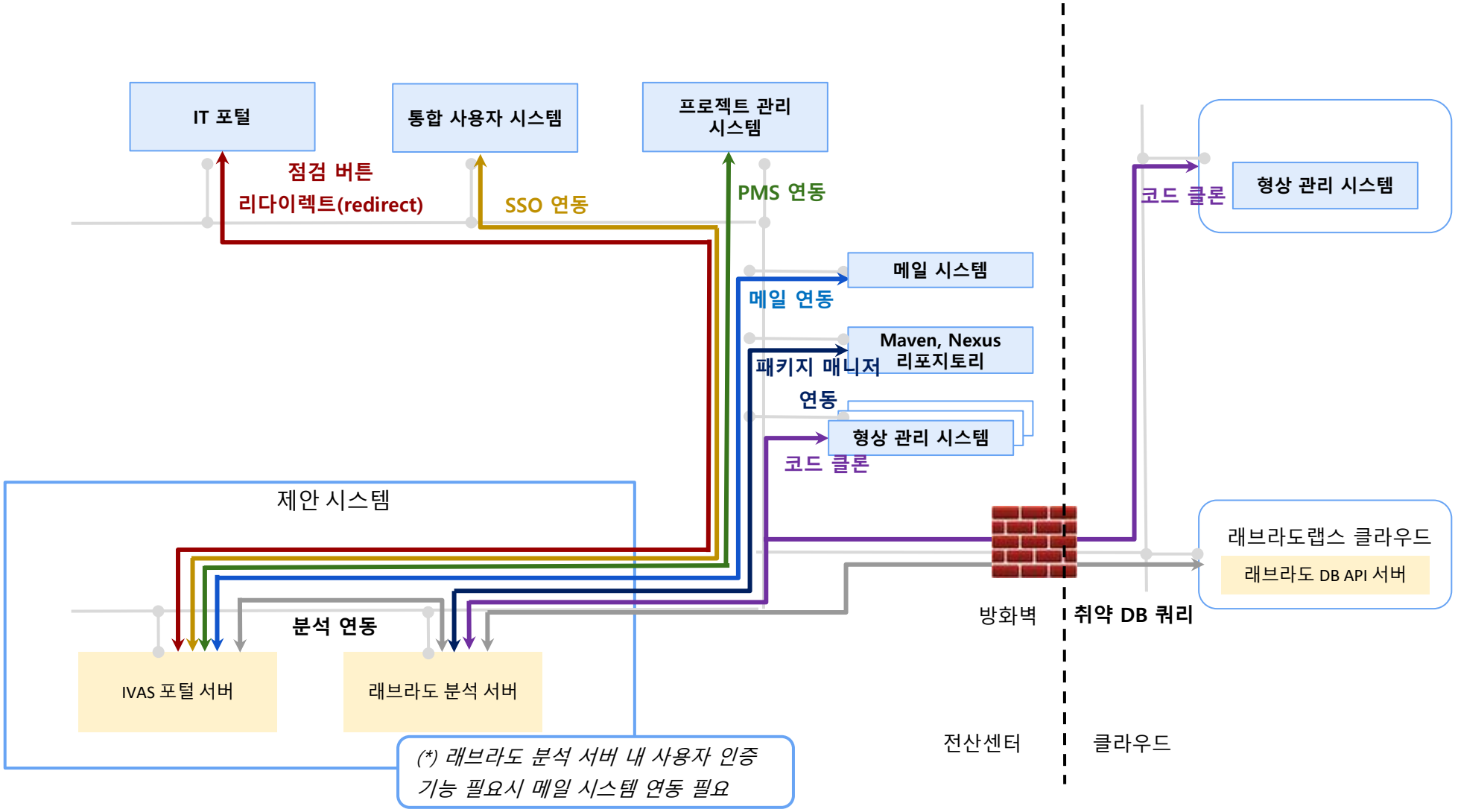
- 마스터 DB 사용 유형
1. 중계서버를 통해 자동으로 정기적 DB 업데이트 진행
2. 완전한 폐쇄망의 경우, 저장 매체를 통한 물리적 업데이트 진행



래브라도 SaaS를 내부망에 연결하여 오픈소스 SW 관리시스템 구축

- 소스코드 Privacy 보호
1. 사용자가 내부망에서 래브라도 CLI를 통해 소스코드 암호화(Hash)
2. 암호화된 파일을 래브라도 SaaS에 보내서 분석진행을 진행하므로, 소스코드 외부노출 없음

래브라도 SW 보안성 검증 체계 시스템 개념도



06

Labrador IVAS

소프트웨어 보안취약점 자동분석 시스템

AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

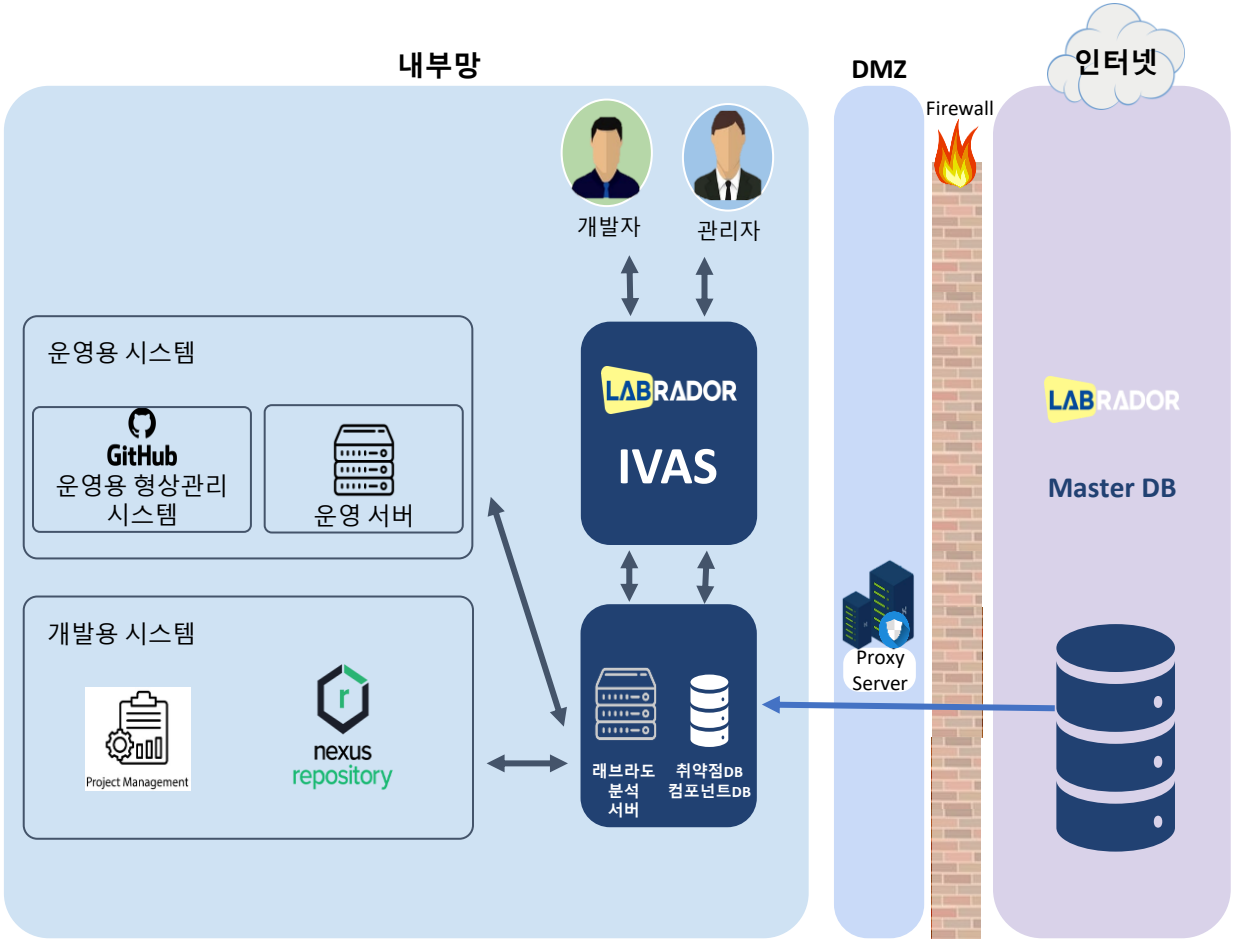
LABRADOR LABS

6.1 래브라도 IVAS 개요

IVAS는 래브라도에서 분석한 오픈소스의 취약점 분석 결과를 고객사 내부 시스템과 연동하여 보다 쉽고 편리하게 취약점을 관리할 수 있는 고객 중심의 통합 시스템 입니다.

IVAS 특징

1. 고객 운영시스템 SW 취약점 자동분석
2. 분석 결과에 대한 단계별 조치 관리
3. 조치 담당자에 대한 자동 통보 및 후속 현황 관리
4. 취약점에 대한 중요도별 필터링 기능
5. 특정 취약점에 대한 통합 검색 기능
6. 고객 환경에 맞는 유연한 대응 구조



6.2 래브라도 IVAS 화면 구성

> IVAS는 형상 관리, 프로젝트지원센터 등 내부 저장소와 연동하여 자동 분석이 가능하며,
> 별도 수동 분석이 필요한 사용자의 니즈에 맞춰 자가 분석 기능도 제공합니다.

형상 관리 분석

현재 오픈되어 운용 중인 서비스에 대한 오픈소스 정기 분석

- 분석 결과
- 통합 점검
- 취약점 조치 현황
- 라이선스 사용 현황
- 관리자 설정

자가 분석

개발자 및 담당자 필요에 따른 자발적인 분석 진행 가능

- 소스코드
- 바이너리
- 컨테이너

프로젝트지원센터 연동분석

개발 진행 중인 서비스에 대한 오픈소스 분석

관리자 설정

분석 대상 시스템 관리 및 점검 정책 관리

- 담당자 관리
- 형상 관리 시스템 관리
- 조치 대상 필터링
- 자가 분석 통계
- 삭제 관리

6.3 래브라도 IVAS 조치 관리 지원

> IVAS는 분석한 오픈소스의 분석 결과에 대해 사용자가 효율적이고 쉽게 관리할 수 있도록 조치 관리, 조치 정책, OSS 관리 등의 기능을 제공합니다.

01 조치 계획 관리 지원

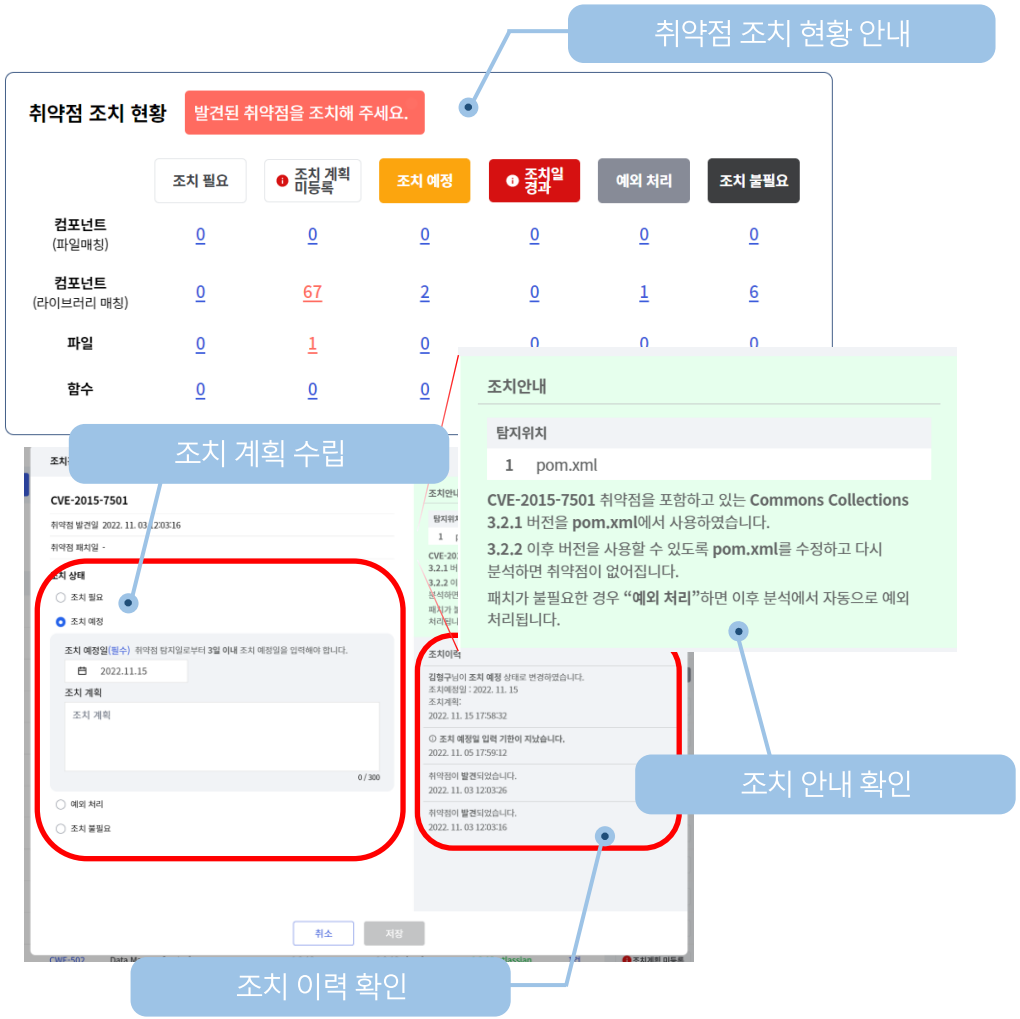
- 발견된 취약점에 대한 담당자 조치 계획 관리 지원
- 조치 예정일 경과 / 조치 상태 변경 등의 조치 이력 표시

02 조치 현황 안내

- 조치 현황 파악에 용이한 단계별 현황 노출
- 예외처리 / 계획이 미등록된 취약점 구분

03 조치 안내 확인

- 탐지된 취약점에 대한 조치 안내 정보 제공
- 보다 정확한 조치를 위해 탐지 위치 정보 제공



6.4 래브라도 IVAS 조치 정책 지원

01 조치 대상 필터링

- 조치 대상을 필터링하여 효율적인 패치 작업 지원
- 취약점 위험도 기준 / CWE 기준 설정 가능

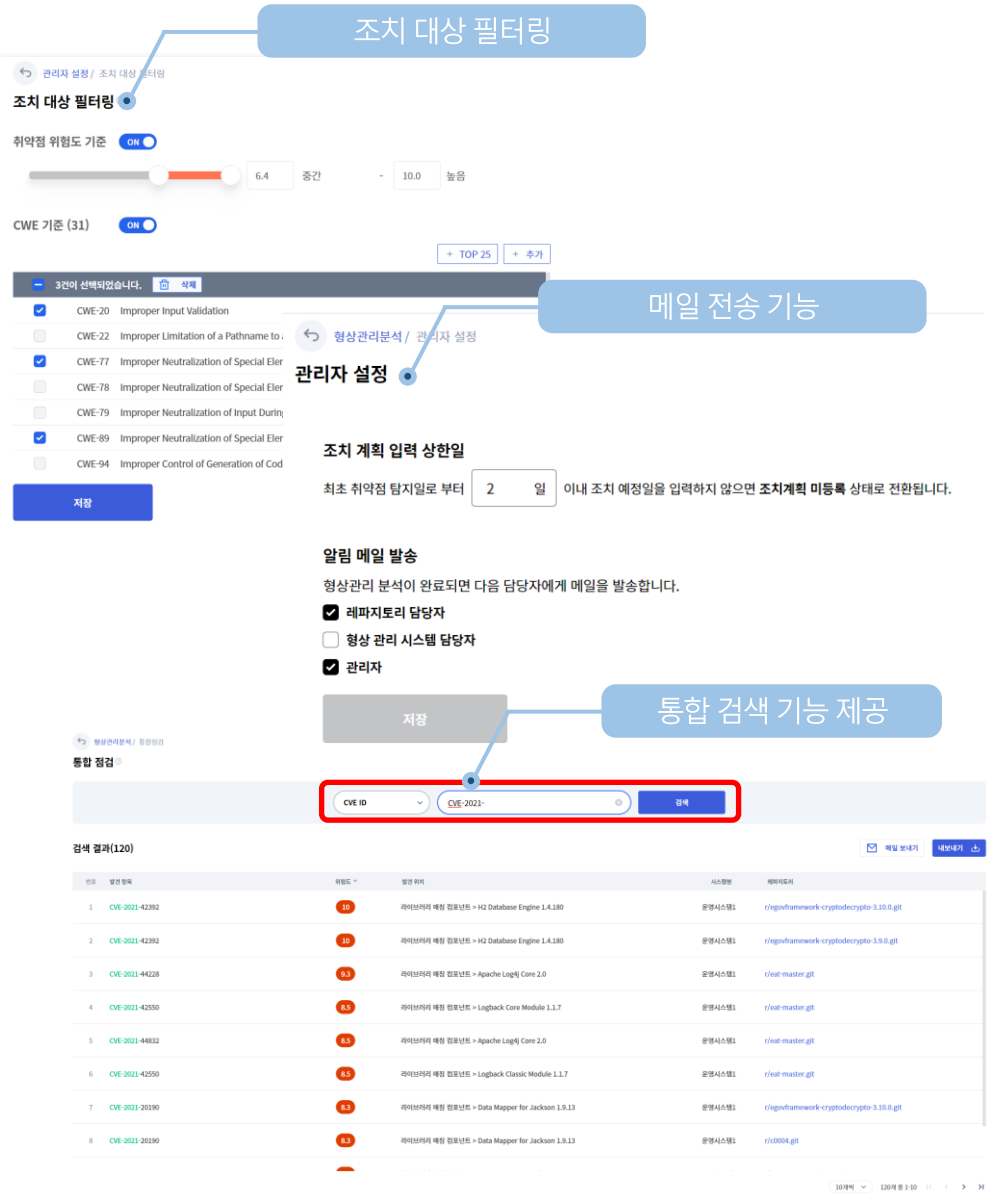
02 담당자 권한에 따른 메일 발송

- 형상관리 시스템 내 저장소에 대한 취약점 조치 메일 자동 발송
- 형상관리 시스템 내 저장소에 대한 분석 결과 메일 자동 발송

03 통합 검색 기능 제공

- 특정 취약점*에 대한 통합 검색 기능 제공 (프로젝트명, 담당자명)
- 조치예외 처리한 취약점에 대해서도 검색 가능
  (프로젝트명, 담당자명)

* 조직에서 관리하고자 하는 취약점(ex)Log4j 등)



LABRADOR LABS

6.5 래브라도 IVAS OSS 관리 지원

01 통계화면 제공

- 사용된 OSS 컴포넌트의 취약점 및 사용현황에 대한 통계화면 제공
- OSS가 사용된 목적을 쉽게 파악할 수 있도록 키워드 정보 제공

02 OSS 사용관리 지원

- 버전별 OSS 관리로 안전한 OSS 버전 선택 가능
- 정확한 SBOM 정보를 제공하여 사용된 OSS 컴포넌트 관리 지원

감사합니다

㈜래브라도랩스 http://www.labradorlabs.ai

서울특별시 서초구 반포대로 53 기아빌딩 5층

02-921-0419

LABRADOR LABS