Labrador 솔루션 소개

2023

㈜ 래브라도랩스

01

오픈소스 사용 현황

소프트웨어 보안취약점 자동분석 시스템

AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

1.1 오픈소스 동향

> 많은 기업들이 오픈소스를 활용하여 혁신적인 신기술·신개념 서비스 개발

오픈소스(Open Source)의 의미

■ 누구나 자유롭게 확인·수정·배포할 수 있는 프로그램 소스코드

- **목적에 맞는 오픈소스를 자유롭게** 다운로드 받아 구현 가능
- 오픈소스 활용을 통해 **개발 효율 극대화 & 신속한 대응 가능**
- 글로벌 개발자 커뮤니티와의 **문제 공유 통해 완성도 향상**

■ 오픈소스 활용 사례

Tensorflow [인공지능] | Corda [블록체인] | Linux [OS] | Kubernetes [클라우드] | ...

글로벌 기업의 오픈소스 활용·확대

* 소프트웨어정책연구소, "오픈소스 수익화의 확산-오픈소스 기반 수익화 구조"

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

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

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)

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

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

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

1.4 SBOM의 제도화 추세

> 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


Presidential Documents

Improving the Nation's Cybersecurity

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

Labrador SBOM 대응

SBOM
소프트웨어 목록관리
라이선스 점검
보안취약점 검증

Developer

- 오픈소스 소프트웨어 자동관리
- 안전한 소프트웨어 재사용 가능

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 Intuitive Surgical, SBOM 솔루션으로 Labrador 선정(2023)

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

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

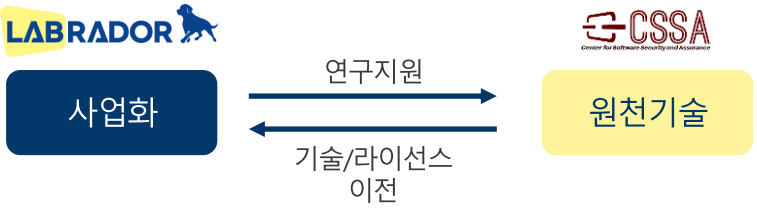
“Find all bugs with Labrador”

【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 20, 3, 4F**
대표자	**이희조, 김진석**



- 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

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

03

Labrador 소개

소프트웨어 보안취약점 자동분석 시스템

AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

LABRADOR LABS

3.1 Labrador 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

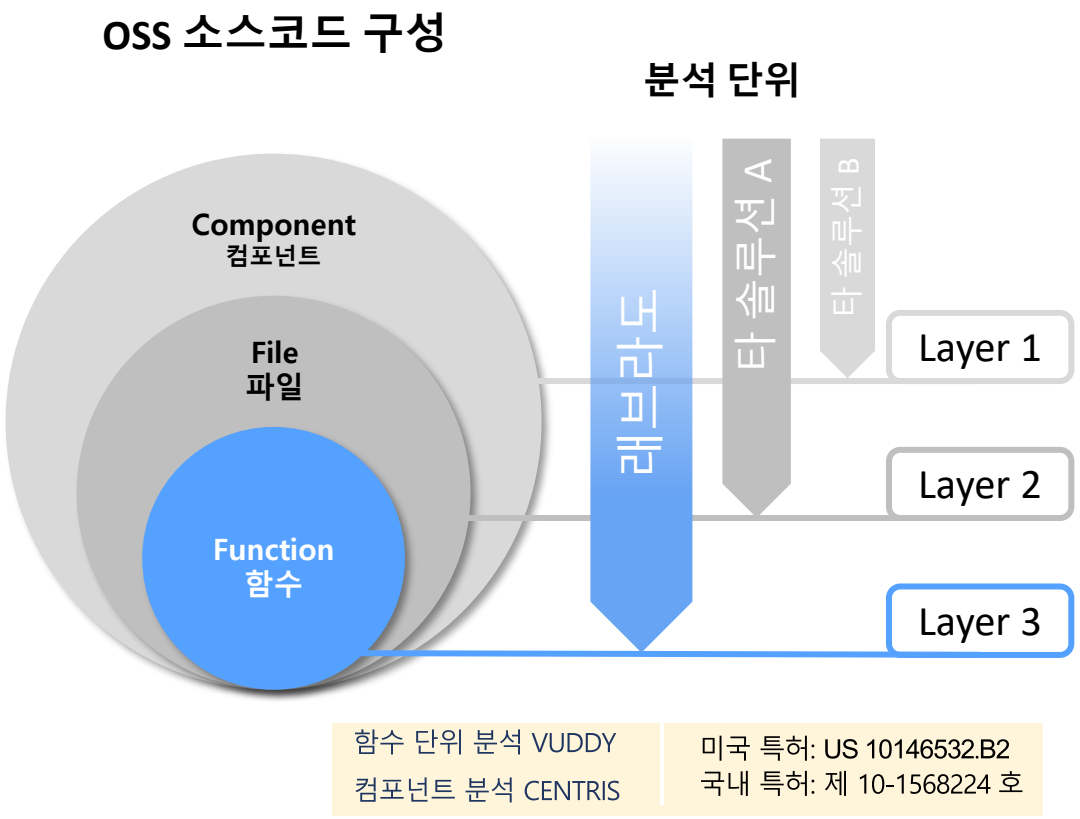
IVAS 플랫폼 구축 경험

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

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

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

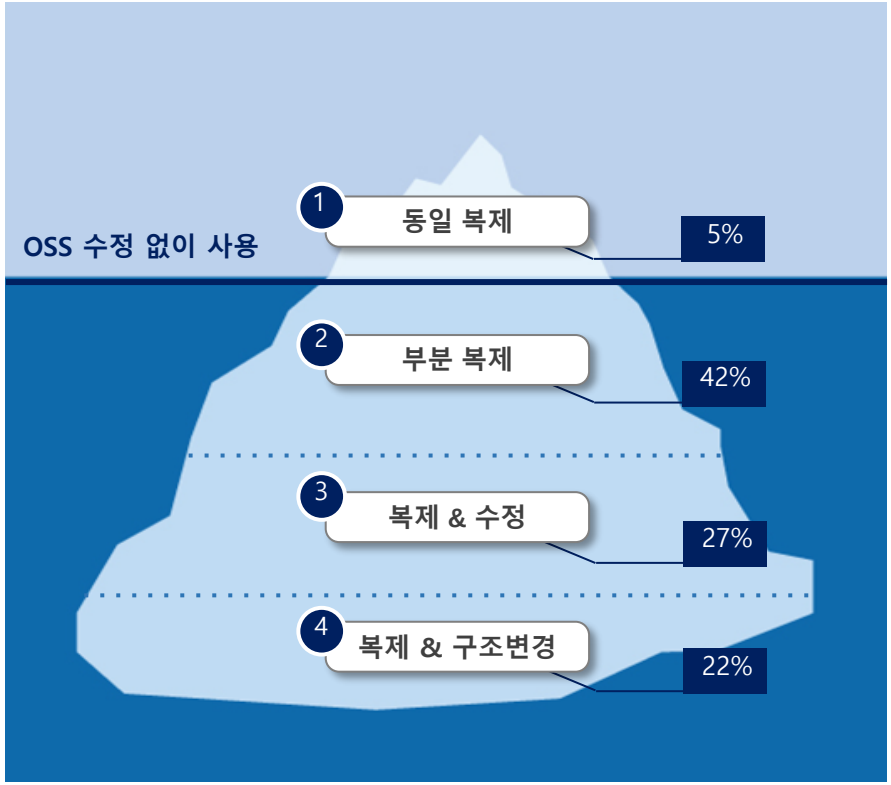
✓ 컴포넌트 단위 포함, 함수단위의 자체 취약코드 등록 및 탐지 기능으로 자체취약점 관리

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

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

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

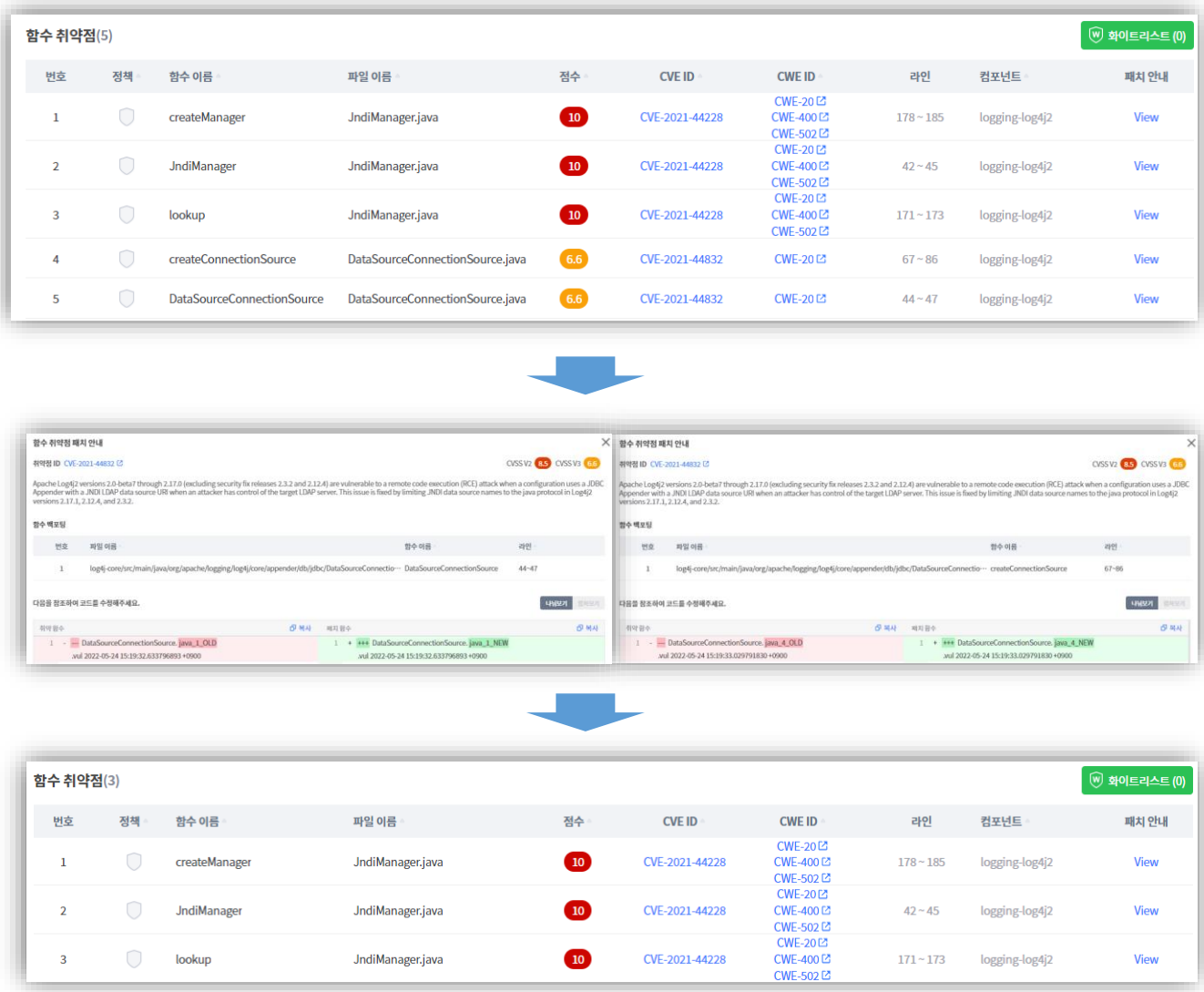
함수 취약점 탐지 및 수정 예시

1. logging-log4j2 컴포넌트 분석 진행
   - 5개의 함수 취약점 탐지
   (CVE-2021-44228, CVE-2021-44832)

2. 함수 취약점이 탐지된 파일 코드 수정
   - DataSourceConnectionSource.java
   파일의 취약한 함수 2건 수정

3. 컴포넌트 재분석 수행
   - 컴포넌트 코드 수정본 분석 수행

4. 해당 CVE 취약점 제거 확인
   - 취약점 수 변화 확인(5개->3개)
   - CVE-2021-44832 취약점 제거



Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

“ 한국과학기술원(KAIST) 사이버보안연구센터 주관 ‘오픈소스 취약점 분석 도구 평가’

래브라도는 경쟁사 대비 **최우수 평가 획득**

CSRC Weblog

[일:] 2022년 03월 04일

2021년 12월 일명 “Log4j 보안 취약점 사태” 가 발생함에 따라 오픈소스인 “Log4j”를 활용한 정보시스템을 운영하는 정부기관 및 기업들은 비상 상황에 맞닥뜨리게 되었습니다. 오픈소스는 여러 장점에도 불구하고 현재의 개발 패러다임으로 인해 소프트웨어 보안 취약점이 손쉽게 확산 될 수 있다는 문제점이 많아 오픈소스의 안전성 및 신뢰성 확보하기 위한 대응책 마련이 필요한 시점입니다. 이번 포스팅에서 오픈소스 취약점 분석 도구 소개와 오픈소스 취약점 분석 도구에 대한 평가를 작성하였습니다.

- 카이스트 블로그 : https://csrc.kaist.ac.kr/blog/2022/03/04/

연구 범위 및 내용

1. **평가 지표** : 소프트웨어진흥법 제49조 제2항 “소프트웨어 기술성 평가 기준 지침” 평가 기준에 따른 상용소프트웨어 평가항목 및 배점 참고(제3조 제2항 관련)
2. **평가 방법** : GitHub 최상위 랭크된 오픈소스 중 자주 사용되는 7개 언어로부터 생성된 프로젝트 10개 선정 후, 보안 취약점 분석 도구인 Labrador와 해외 도구 3종에 대해 컴포넌트 탐지와 취약점 분석 결과 비교
3. **평가 결과** : 종합 분석 결과, 37개 항목 중 25개 항목에서 “우수” 평가를 받아 최우수 도구로 선정됨.
4. **종합 평과 결과표**

		A	B	C	Labrador
기능성	우수	4	2	1	8
	보통	1	2	3	1
	나쁨	3	4	5	0
사용성	우수	7	10	9	14
	보통	4	1	5	4
	나쁨	6	6	7	3
유지 관리성	우수	3	2	2	3
	보통	0	0	2	1
	나쁨	2	2	3	3

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

04

Labrador 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

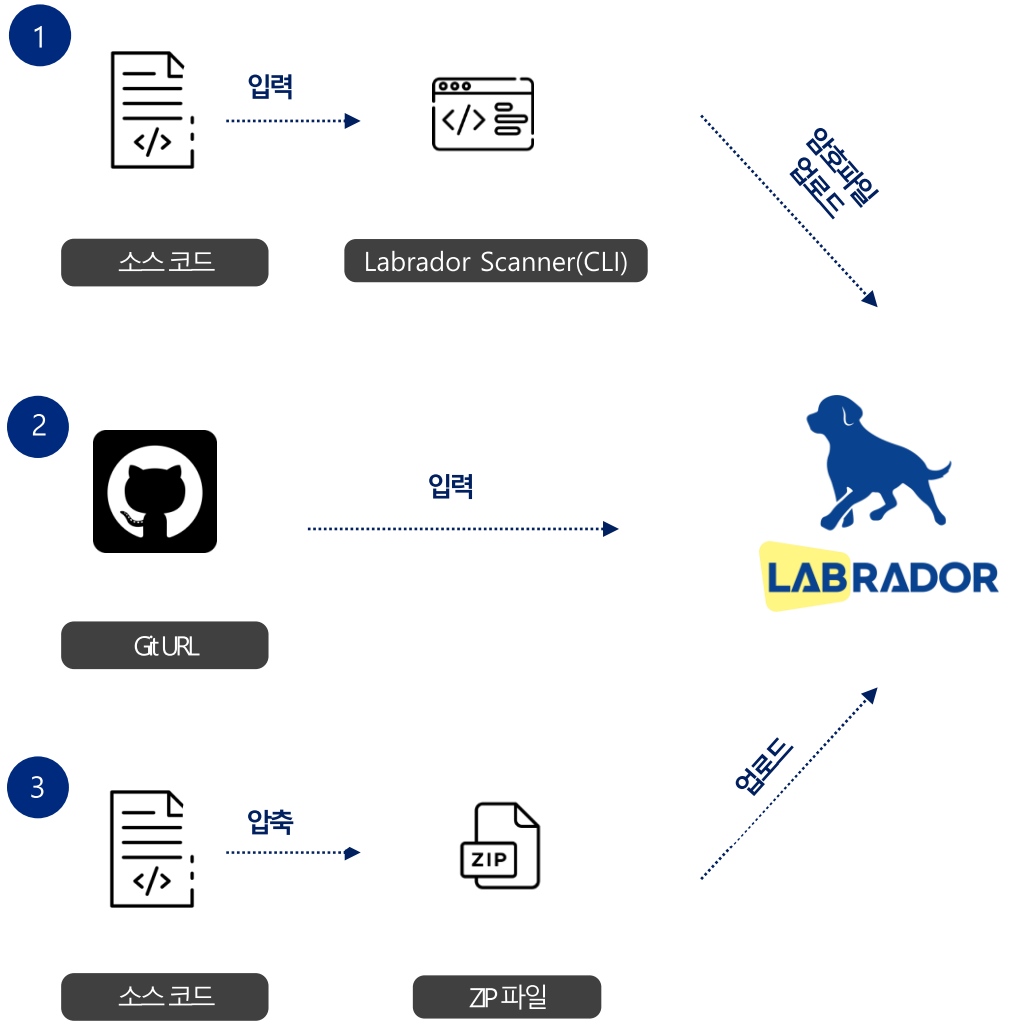
Git URL

Public/Private 저장소의 소스코드 URL을 입력하면
자동 스캔 및 분석

Option 3

ZIP Upload

분석대상 소스코드를 압축해서 업로드 후
자동 스캔 및 분석



Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

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

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

오픈소스 취약점 정보 제공 기능

01 정확한 취약점 정보 제공

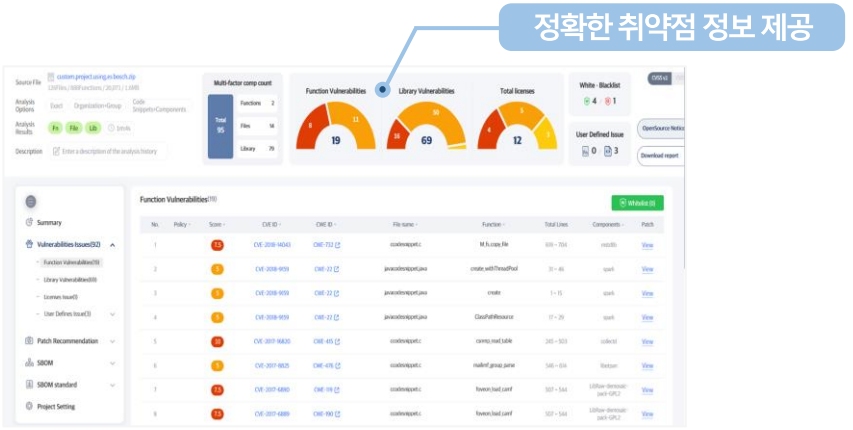
- 취약점에 대한 3-Layer 분석 기반 90% 이상의 정밀도
- 변경된 소스코드에 대해서도 정확한 분석 가능

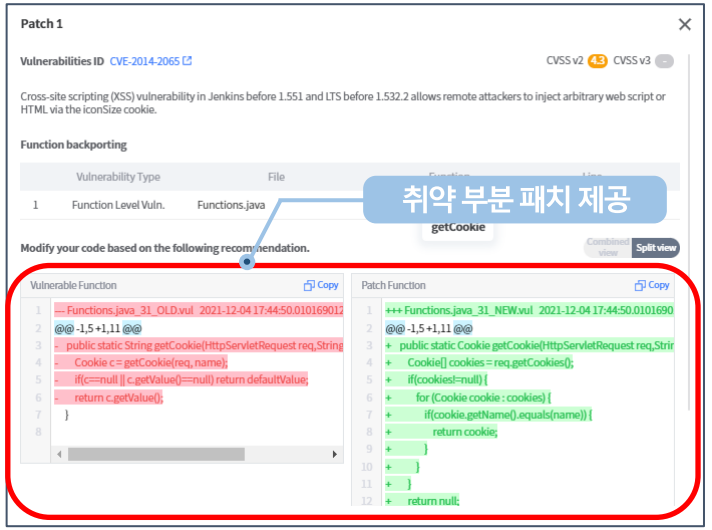
02 Pinpoint 패치정보 제공

- 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





Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

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

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

4.5 조직 내 소프트웨어 거버넌스 정책 자동 관리

소프트웨어 거버넌스에 대한 다양한 정책 및 자동화 지원

01 자체 취약점 및 컴포넌트 관리

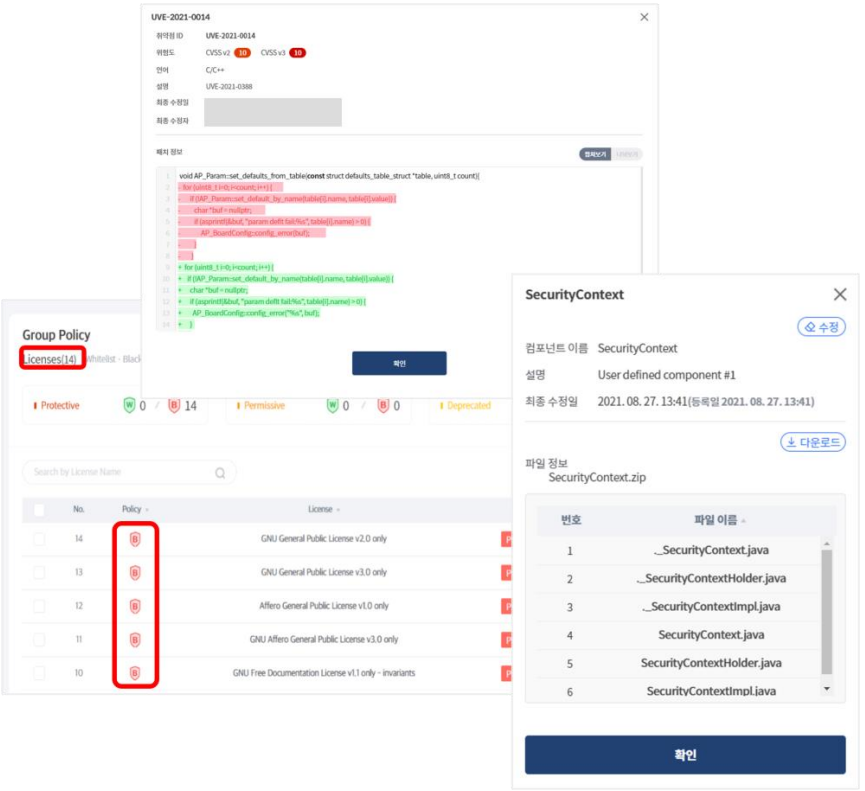
- 자체 개발한 소스코드의 취약점 자동 관리 기능 제공
- 조직 내 사용금지 된 컴포넌트 자동 필터링 기능 제공

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



Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

4.6 SBOM 국제 표준 포맷 제공

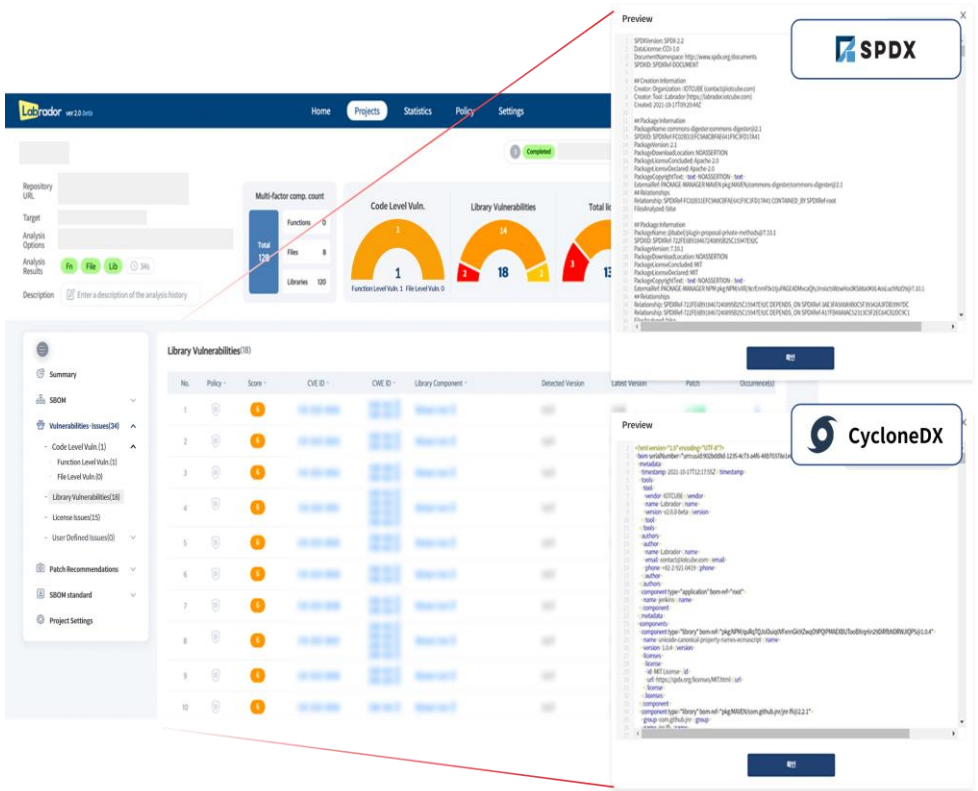
SPDX & CycloneDX 국제 표준 포멧 제공

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



Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

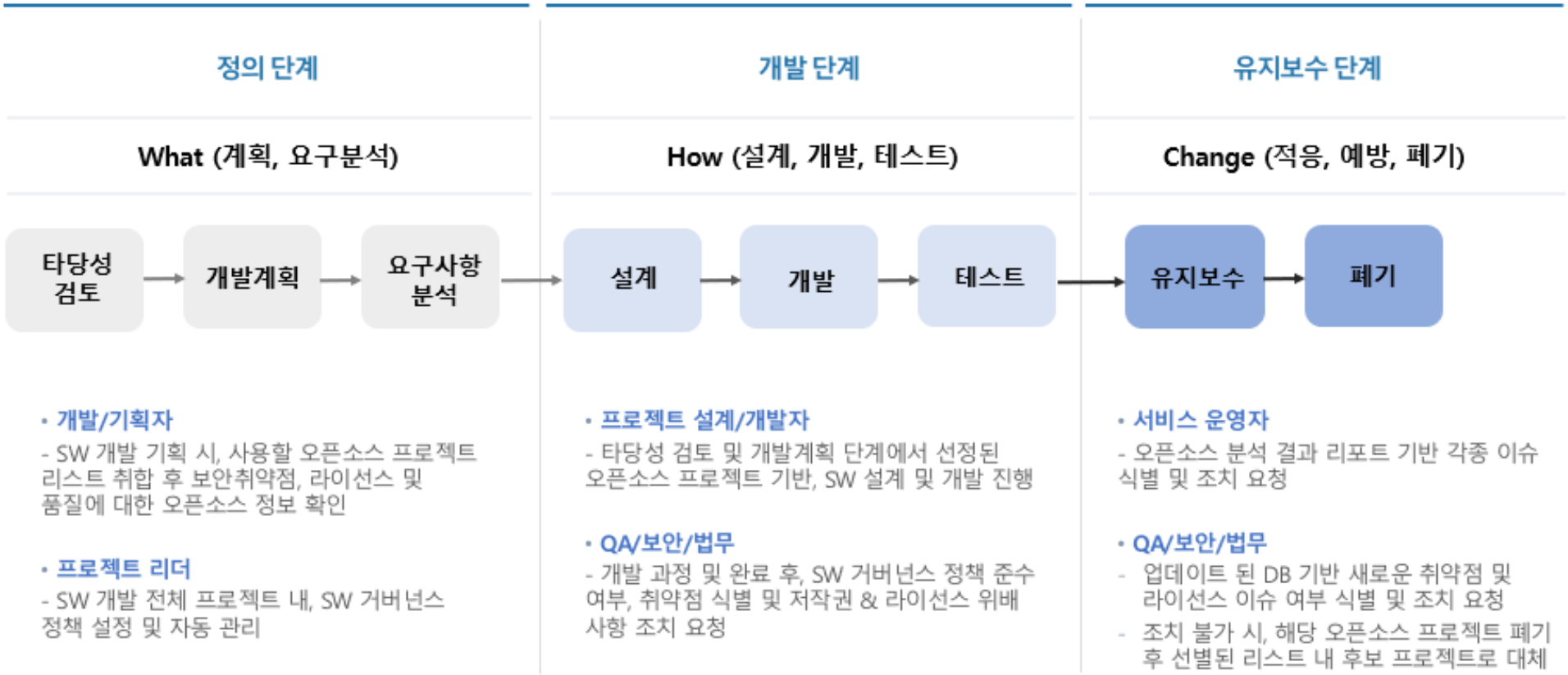
LABRADOR LABS

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



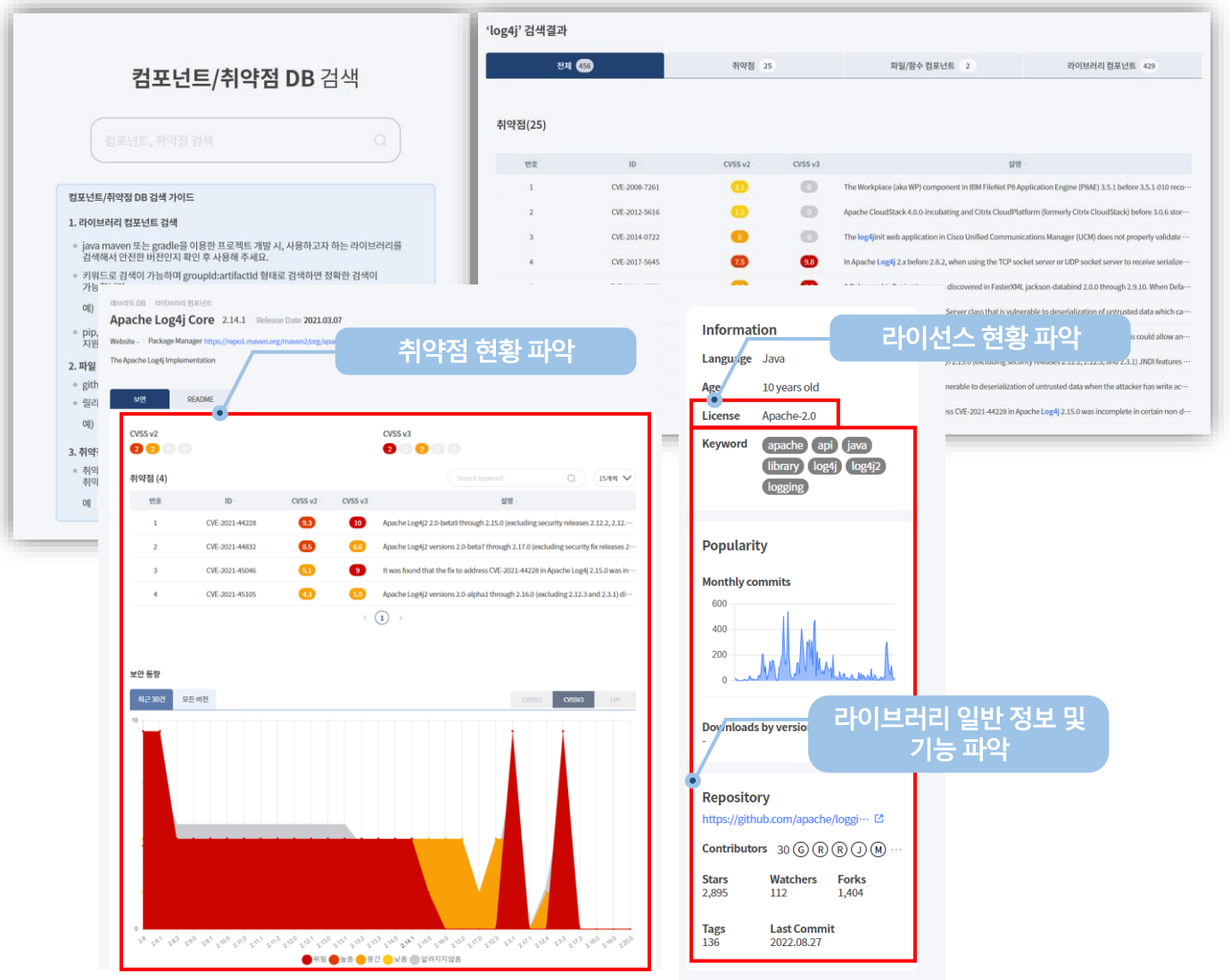
Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

5.1 SDLC 단계별 오픈소스 관리 운영 방안

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

정의 단계

- ✓ 사전 기능 점검 및 보안성 테스트를 위해 **DB 검색 기능** 제공
- ✓ DB 검색으로 찾은 컴포넌트의 **취약점 및 라이선스 이슈** 파악



Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

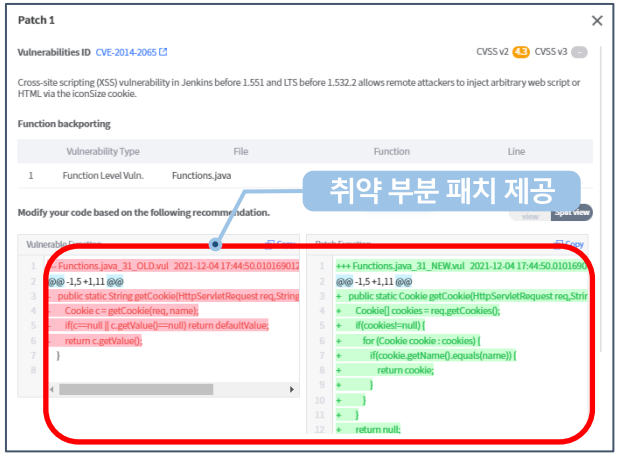
LABRADOR LABS

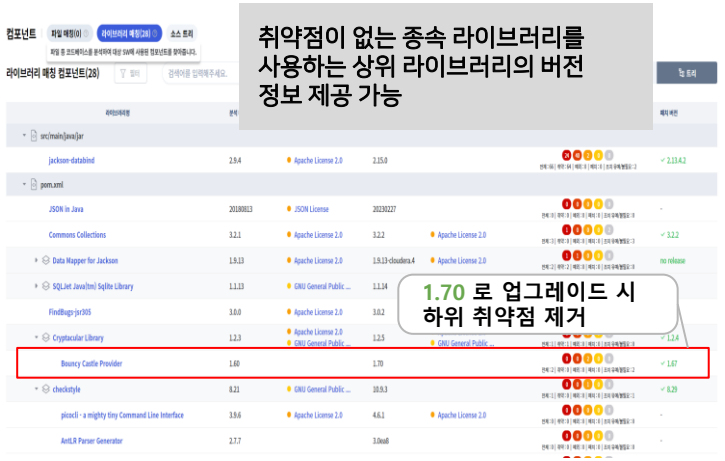
5.1 SDLC 단계별 오픈소스 관리 운영 방안

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

개발 단계

- ✓ 통합 포탈과 연동하여 **주기적인 취약점 자동 분석** 기능 제공
- ✓ 취약한 코드를 대체할 **패치 코드** 및 취약한 버전에 대한 **대체 버전** 제공
- ✓ **고려대 CSSA와의 긴밀한 협력관계 통해 전문 대응 인력 확보**





LABRADOR 사업화

연구지원

기술/라이선스이전

CSSA 원천기술

'23.10 현재 총 7개 특허 관련 기술 이관

- 취약점 DB TF 운영 중
- 공동 보안 세미나 시행
- Chief Scientist 현장 지원

CSSA와 기술이전 및 교류로 긴밀한 협력관계 유지

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

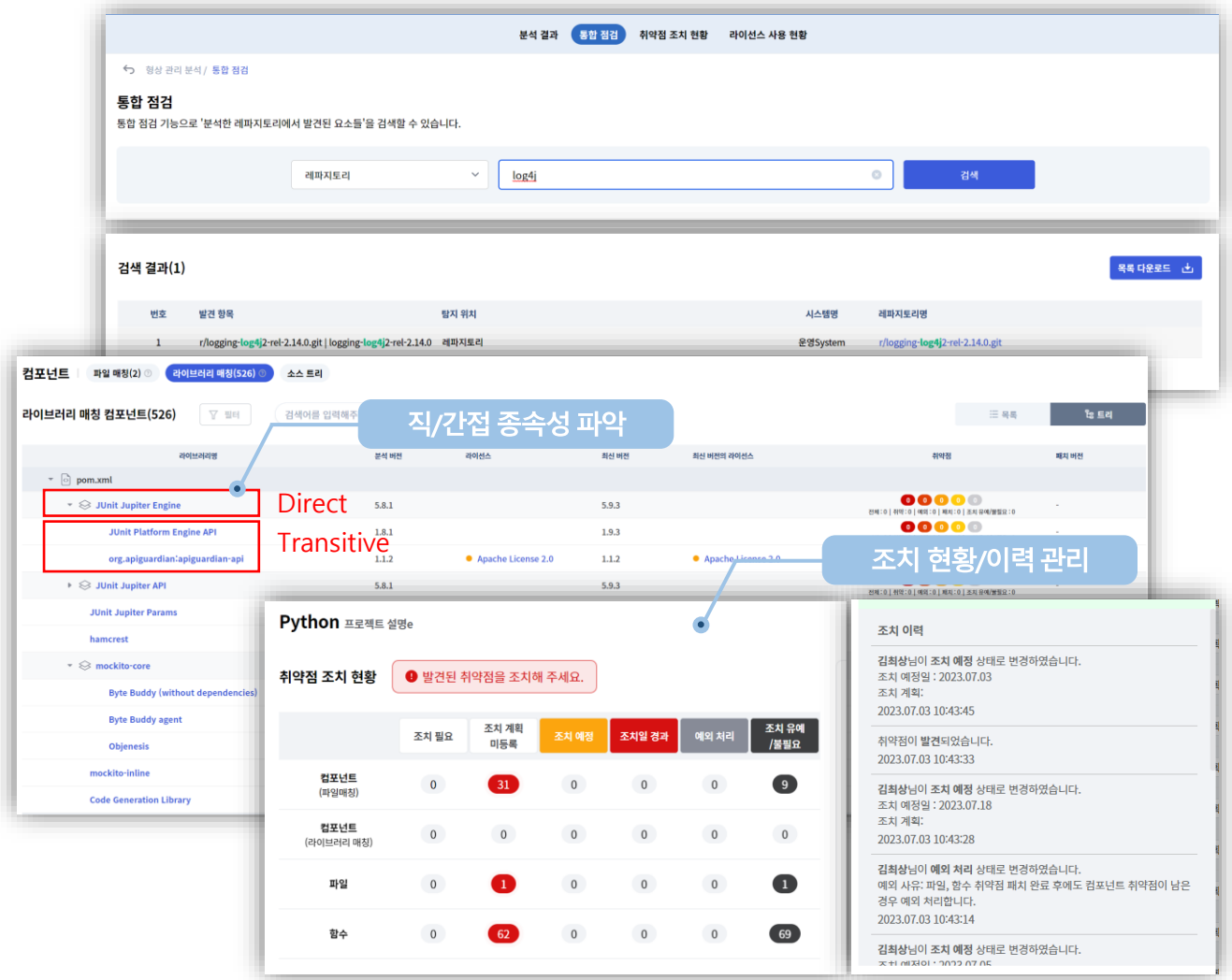
LABRADOR LABS

5.1 SDLC 단계별 오픈소스 관리 운영 방안

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

유지보수 단계

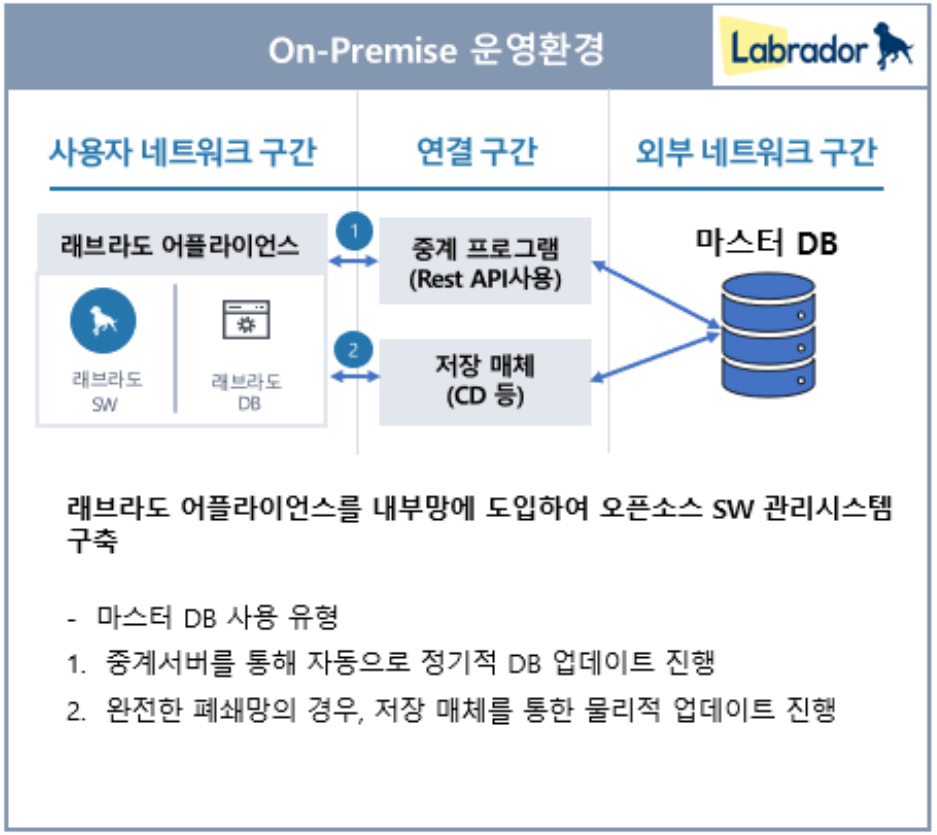
- ✓ 통합 포탈의 **통합 점검 기능**으로 개발한 소프트웨어의 **기능 및 보안성 이슈 검증**
- ✓ 소프트웨어의 **직/간접 종속성** 파악
- ✓ 조치 관리 기능 통해 **운영중인 소프트웨어 지속적으로 모니터**
- ✓ 취약한 코드를 대체할 **패치 코드** 및 취약한 버전에 대한 **대체 버전** 제공



Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

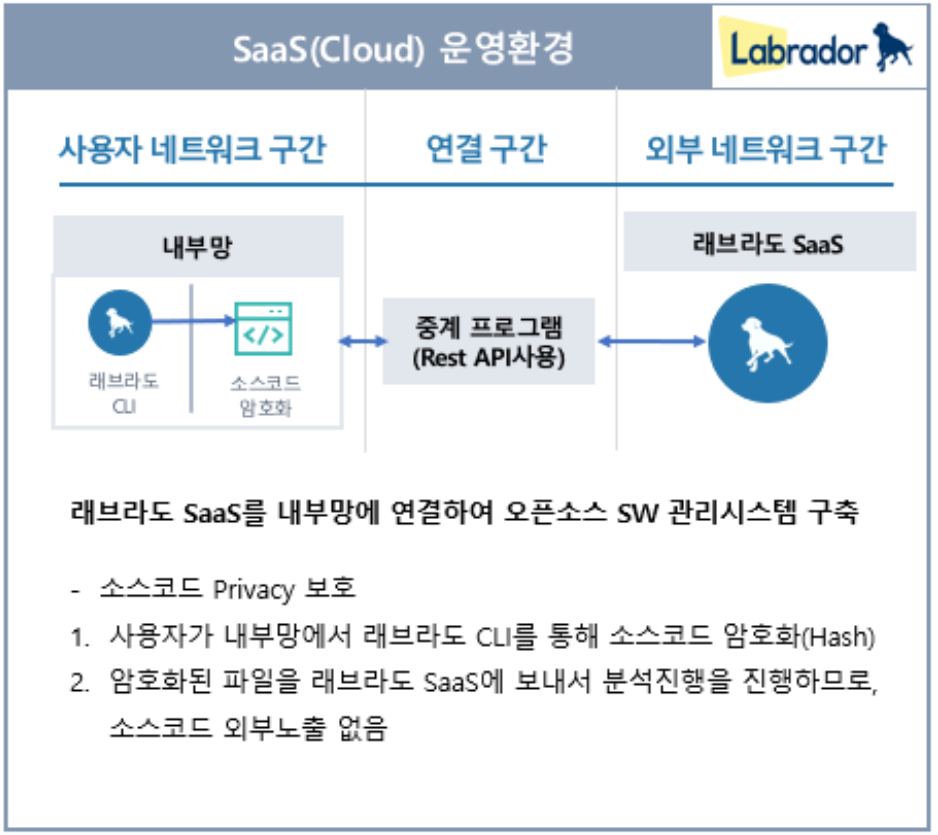
5.2 래브라도 구축 환경

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

Copyright 2023 Labrador Labs, ALL RIGHTS RESERVED

감사합니다

㈜래브라도랩스 http://www.labradorlabs.ai

서울특별시 서초구 반포대로 20 3, 4층

02-921-0419