OpenChain KWG Tooling & Legal Group 24th meeting

“Shift-Left에서 SBOM까지: 툴 통합 기반 오픈소스 거버넌스 모델”

오에스비씨 이준수

OSBC

Shift-Left에서 SBOM까지: OpenChain 연계 거버넌스 구조도

OpenChain Core Principles: Policy → Review → Verification → Supplier Assurance → Evidence

Snyk Shift-Left Review & Awareness	FossID Verification of Use	Insignary Clarity Supplier Assurance	OSiMS (CSC) Record & Evidence Mgmt.

SBOM / SPDX & CycloneDX / Policy & Evidence Hub

조직 거버넌스 체계 (Policy / Responsibility / Review / Education / External Response)

OSBC

SBOM 관리의 일관성을 위한 조직적/기술적 기반

조직 거버넌스 구조 (Policy & Governance Framework)

- 역할/책임 정의 (Role & Responsibility)
- 검토/승인 절차 (Process & Review Flow)
- 교육·의사소통 (Education & External Response)

SBOM / SPDX 기반 기술 표준화 (Technical Layer)

- SBOM 생성 도구 간의 공통 언어 확보
- 내부/외부 SBOM 간 비교·검증 체계 구축
- 변경 추적 및 Evidence 관리

거버넌스 구현 플랫폼 예시 (예: OSiMS, Fosslight Hub 등)

- SBOM 데이터 가시화 및 병합
- 정책 기반 모니터링 및 리스크 인사이트 제공

OSBC

오에스비씨 솔루션 라인업

제품명	주요 특징	주요 사용자	운영방식	비고
AI기반 DevSecOps 보안플랫폼 **Snyk**	IDE, CI/CD, 배포/운영 등 개발 전 주기 맞춤형 다양한 연동 체계 지원, DevSecOps 적용 및 자동화 강점 AI 코딩 어시스턴트 통합(MCP) 제공	오픈소스 담당자 개발자, 보안담당자	SaaS	
공급망 관리 특화 SCA **Insignary Clarity**	강력한 바이너리 분석 기능 지원, 공급망 관리 및 다양한 개발 및 운영 환경 대응	오픈소스 담당자 개발자, QA, 법무 등	하이브리드 온프레미스 SaaS	
스니펫 단위 정밀 분석 SCA **FossID**	소스코드 라인별 비교 분석을 통한 오픈소스 식별, 모든 언어 분석 지원, 라이선스 컴플라이언스 관리 중점, 보안취약점 확장	오픈소스 담당자 개발자, QA, 법무 등	하이브리드 온프레미스	
SBOM 통합관리 플랫폼 **OSiMS**	Clarity, FossID 연동 사용 또는 SBOM 검증 용도로 단독 사용 가능, SBOM 통합 관리 플랫폼	모든 사용자	온프레미스	

OSBC

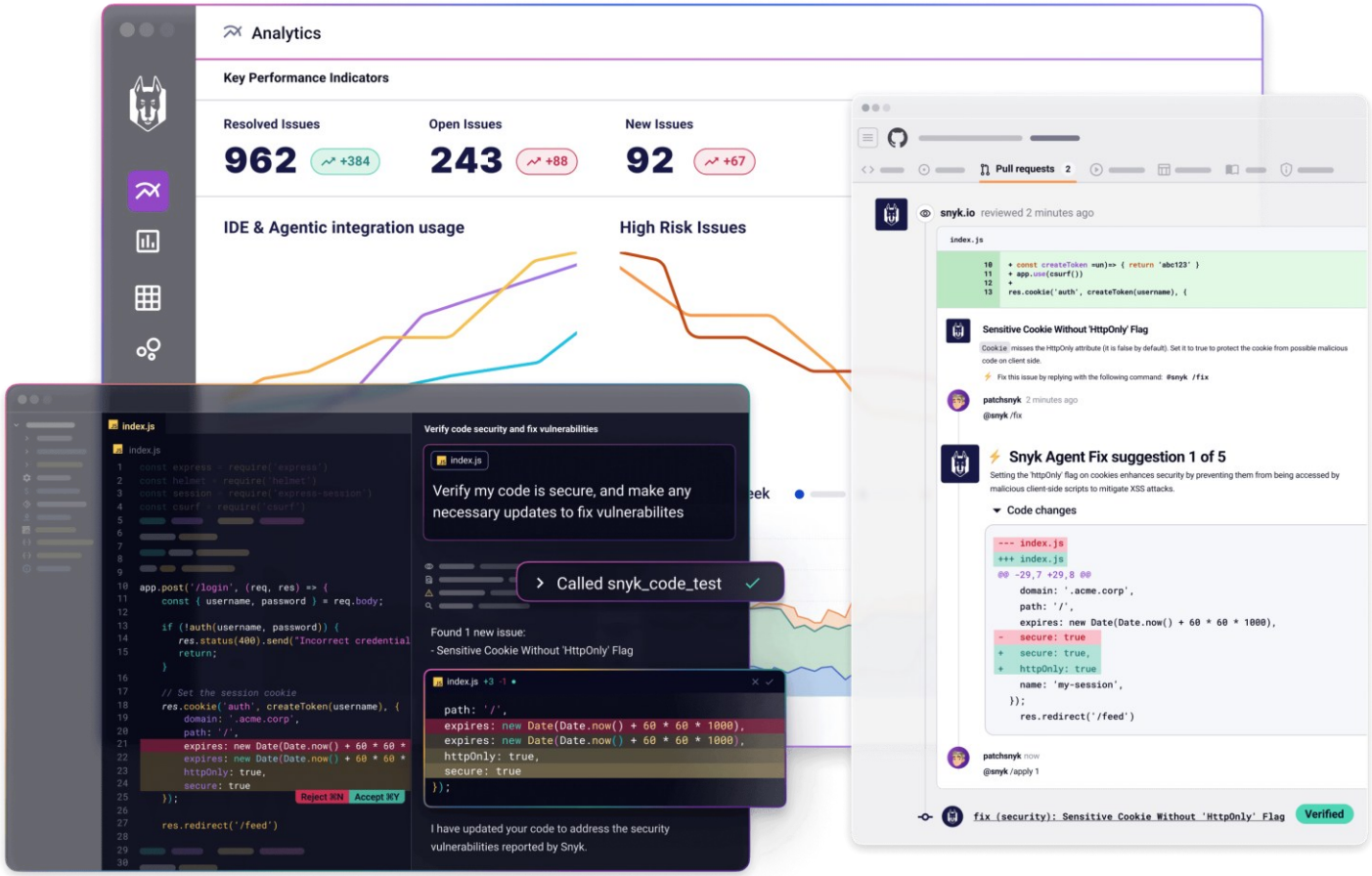
Snyk

AI 시대의 신뢰, 코드 한 줄에서 부터

AI 코드 생성과 오픈소스 사용이 폭발적으로 증가하는 지금,
Snyk은 보안과 신뢰의 기준이 됩니다.

AI가 생성한 코드,
인터넷에서 복사한 스니펫,
외부 패키지와 오픈소스 라이브러리...

보이지 않는 보안 리스크는
코드 한 줄에서 시작됩니다.
Snyk은 코드 한 줄부터
취약점, 라이선스 위험 및 정책위반을 실시간
분석하고 자동 수정까지 지원합니다.



Gartner 2025년
매직쿼드런트 – 애플리케이션
보안 테스팅툴(AST) 리더

Gartner Peer Insights
Customers' Choice
선정(2022)

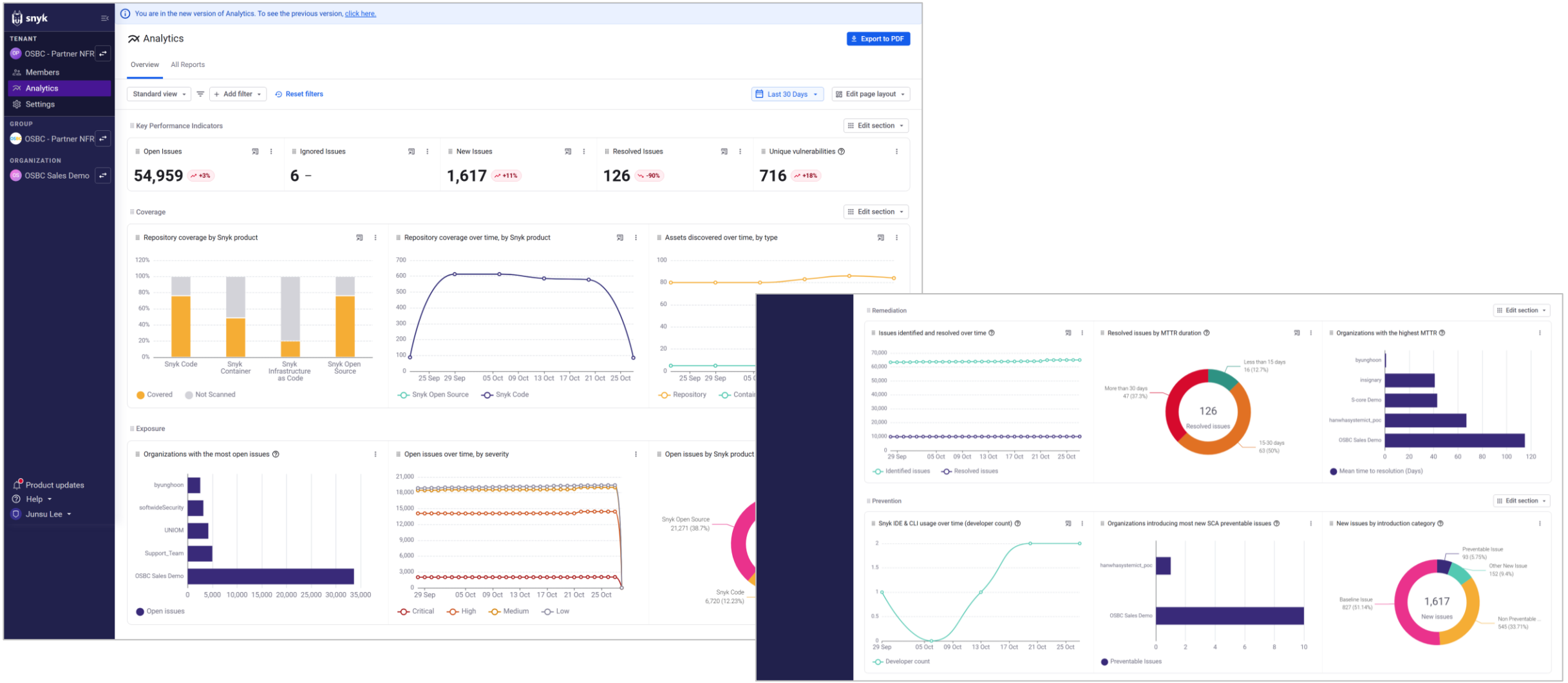
Forrester Wave
2024년 SCA 도구 리더 선정

OSBC

개발 전체 라이프사이클을 안전하게 보호하는 Snyk

OSBC

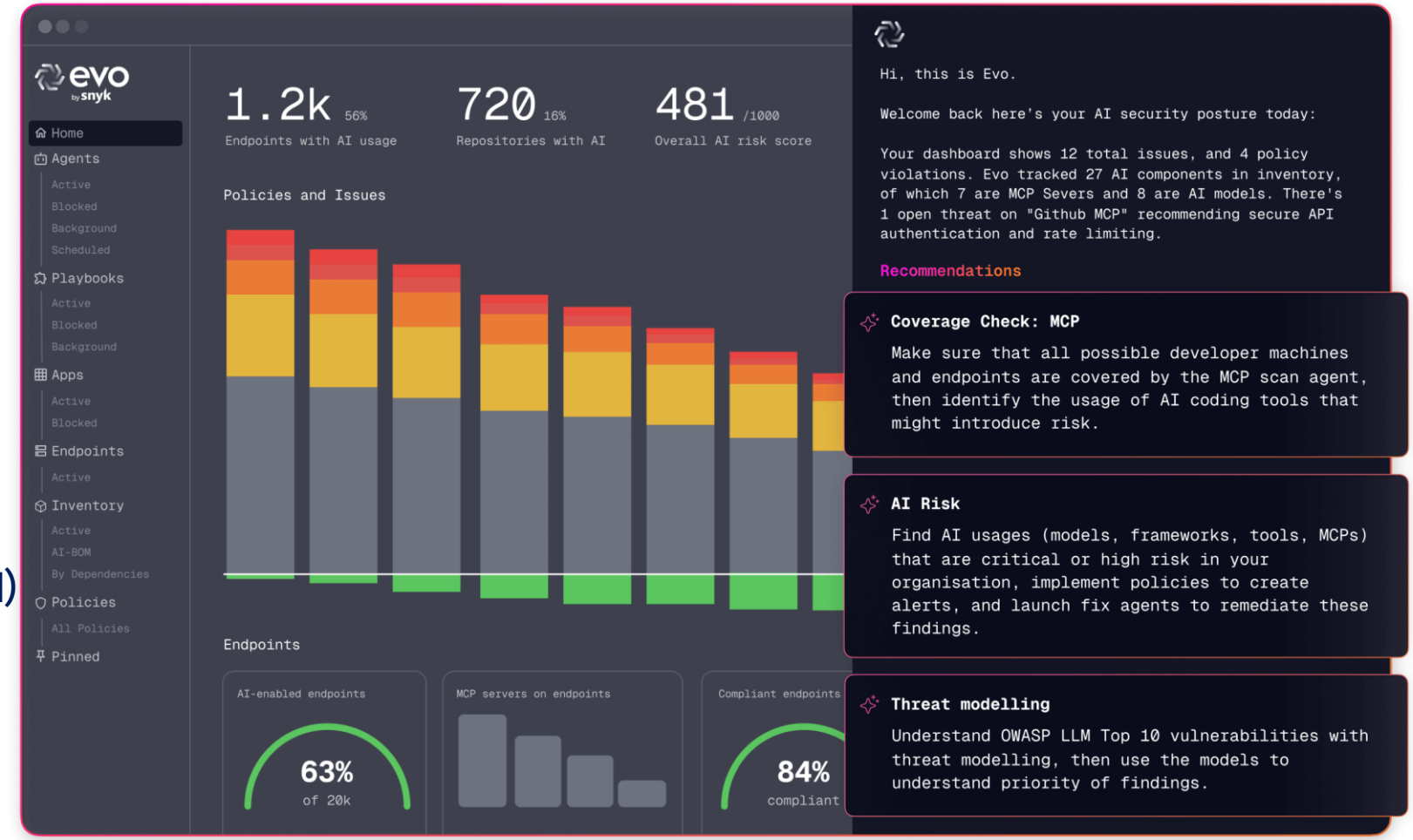
Snyk Analytics, 최상위 레벨 통합 대시보드



OSBC

Evo by Snyk - 에이전틱 보안 오케스트레이션의 시작

AI-native 애플리케이션은 매일 새로운 위협에 노출됩니다.Evo는 수동 점검 대신, 보안 에이전트가 스스로 탐지·평가·조치하는 체계를 제공합니다.코드, 모델, 에이전트, API까지 — AI 생애주기 전체를 실시간으로 모니터링하고 방어합니다.



Evo는 Snyk의 AppSec 플랫폼 위에서 작동하는AI 보안 오케스트레이션 시스템입니다.

- **AI 구성요소 자동 탐지 및 위협 모델링 (AI-BOM)**
- **정책 기반 에이전트 오토메이션 (Adaptive Policy & Workflow)**
- **모델 리스크 스코어링 및 지속 모니터링복잡한 보안 워크플로우를 자동화하고, AI 혁신 속도를 지키면서 신뢰를 강화합니다.**

OSBC

Insignary Clarity

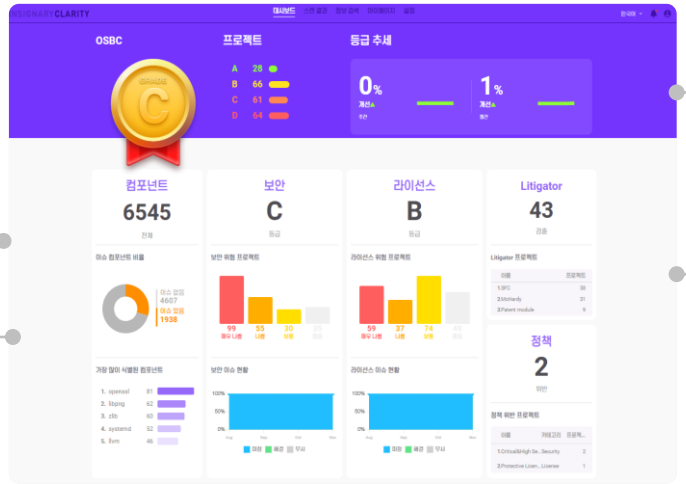
바이너리·소스코드 기반, SBOM·공급망 관리 특화 SCA 도구

오픈소스 검증목록 구축(SBOM)

- SPDX, CycloneDX, NIS-SBOM, VEX

보안취약점 탐지/모니터링

- 알려진 취약점 + 새로운 CVE 자동 탐지
- CVSS 점수 기반 위험도 표시, 조치 가이드
- NVD + CNVD 지원, EPSS 지원(예정)



라이선스 탐지 및 Litigator Code 식별

- 라이선스 유형 자동 분류
- 법적 분쟁 우려 있는 Litigator Code 별도 경고

Deep Fingerprinting 기술 (특허 보유)

- 해시 매칭 대비 장점, 오탐률 낮춤
- 리버스엔지니어링 불필요

바이너리 분석

소스코드 없이 바이너리 만으로 파일 내 오픈소스 식별

소스코드 분석

다양한 개발언어를 지원하는 소스코드 검증 기능

직관적인 UI

직관적인 UI를 통한 분석결과 가시화, 다국어 지원

범용적 지원

다양한 임베디드 환경(ARM, Intel 등)을 범용적으로 지원

낮은 오탐율

String Fingerprint 기반의 정확한 분석

맞춤형 배포방식

클라우드, SaaS 및 온프레미스 운영 지원

OSBC

Insignary Clarity

바이너리·소스코드 기반, SBOM·공급망 관리 특화 SCA 도구

01

소스코드 및 바이너리 모두 지원하는
정확한 오픈소스 식별

02

Deep Fingerprinting 기반의 정확한 분석
(특허 기술 기반의 낮은 오탐율)

03

소스코드 및 SBOM
검증을 통한 취약점 관리

04

SBOM 표준 완벽 지원 및
공급망 투명성 확보

05

다양한 운영환경 지원
(클라우드, SaaS 및 On-Premise 대응)

06

글로벌 및
국내 대표기업의 검증된 레퍼런스

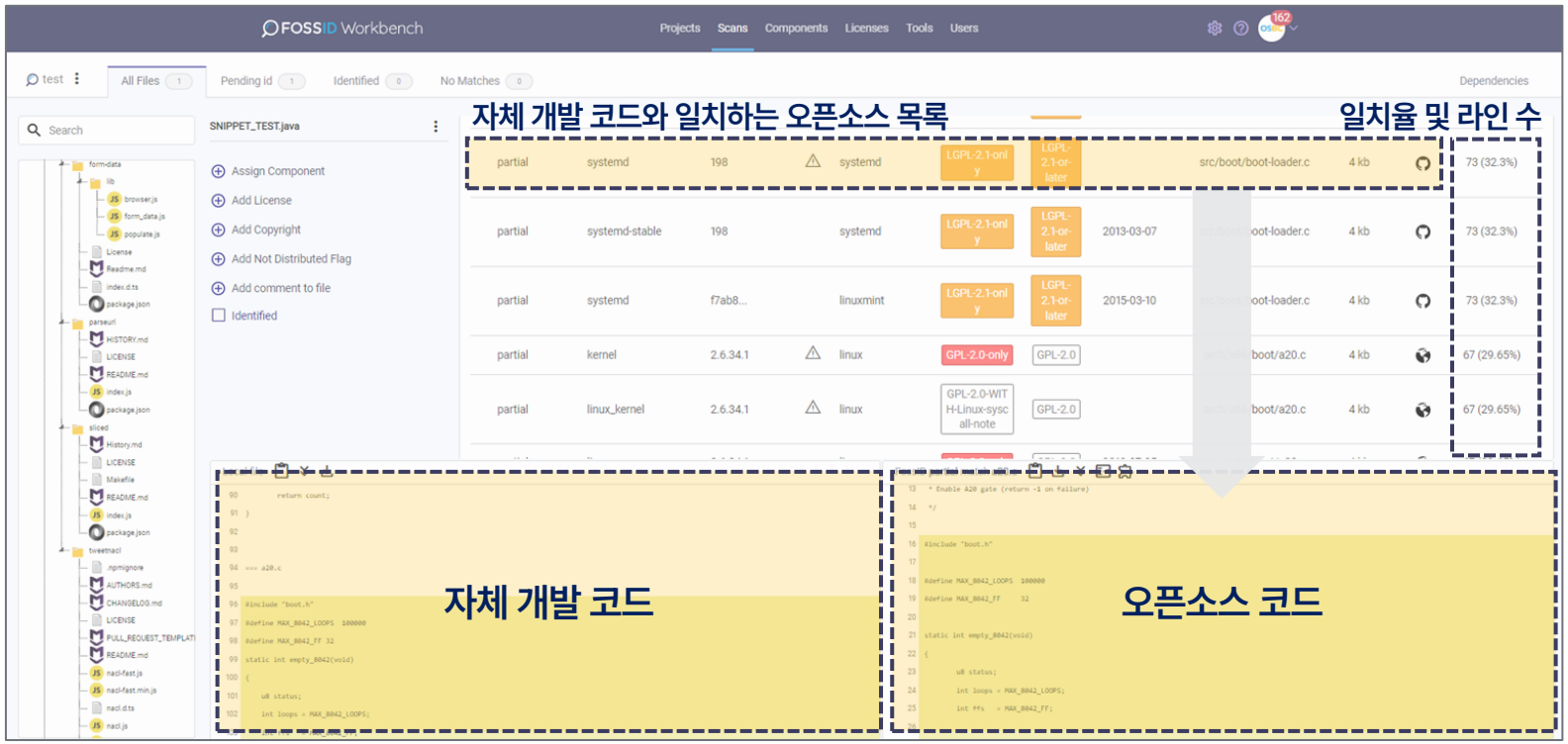
OSBC

FossID

AI 생성 코드 대응, 스니펫 단위 오픈소스 정밀 식별 플랫폼

FossID Workbench 오픈소스 검증 프로세스

프로젝트 생성	소스코드 분석	오픈소스 검증 진행	오픈소스 내역(SBOM) 산출
프로젝트 기본 정보 입력	파일 업로드 또는 Git 지정	코드 비교 및 출처 식별작업 진행	자체 보고서 및 SPDX/CycloneDX 출력



다양한 오픈소스 탐지 방식

폴더, 라이브러리, 압축파일, 바이너리 등 전체 컴포넌트, 수정된 코드, AI 생성 코드 등의 탐지를 위한 스니펫 단위까지 모두 식별

단계적 분석 방식으로 포괄적인 분석 결과 제공

1단계 시그니처 분석, 2단계 AI 기반 필터링, 3단계 라이선스 및 저작권 정보 추출, 4단계 의존성 분석을 통한 종합 결과 제공

Side-by-side 비교 기능 제공

매칭 수준을 직관적으로 비교할 수 있는 작업 화면을 제공. 자체 개발 코드와 오픈소스 코드의 일치 블록을 명확하게 식별 가능

보안취약점 특화 기능

컴포넌트 단위 보안취약점 관리의 과오탐 방지 및 취약 코드 라인 정확히 탐지. 취약점 영향 여부를 기록 및 관리하는 VEX 지원

OSBC

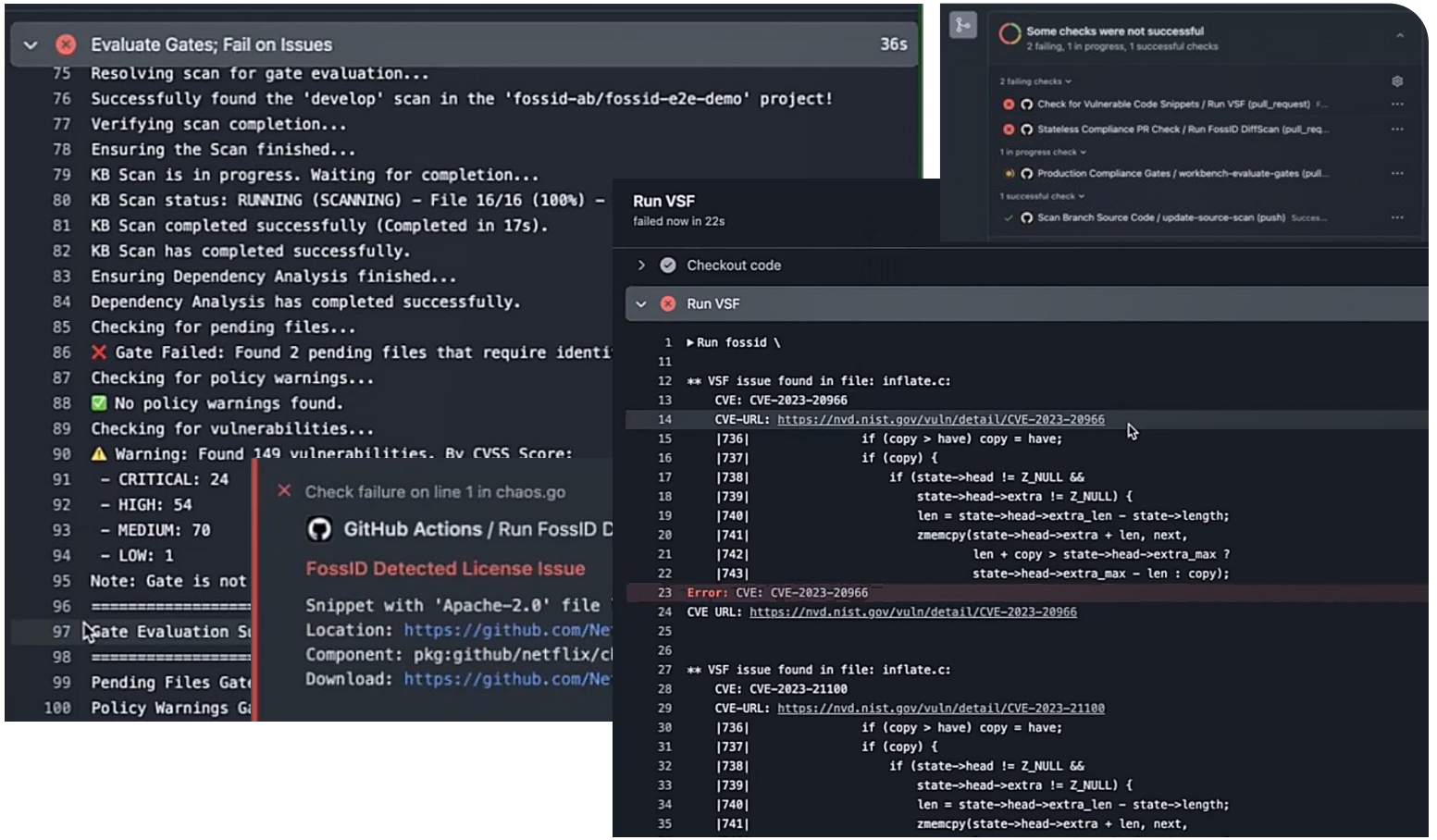
FossID

코드 한 줄, 작은 스니펫 속에도 숨어있는 라이선스·보안 리스크

CI/CD 환경에서 코드 빌드 단계까지 정밀 검증하는
오픈소스 SCA 솔루션

개발 파이프라인 전 과정에서, 코드 속 라이선스와 보안 리스크는 언제든 발견될 수 있습니다.

FossID는 GitHub Actions, GitLab CI/CD 등 파이프라인에 연계되어 PR Check 등을 통해 스니펫 단위까지 오픈소스를 정밀 검증하고 SBOM, 라이선스 및 취약점 정보를 신속하게 제공합니다.



OSBC

OSiMS (CSC)

SBOM 통합관리 플랫폼

OSBC

OSiMS (CSC)

SBOM 통합관리 플랫폼

OSBC

감사합니다.

이준수

jslee@osbc.co.kr

jslee@opensource.or.kr

OSBC