

“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.

개발

운영

SBOM / SPDX & CycloneDX / Policy & Evidence Hub

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

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

오에스비씨 솔루션 라인업

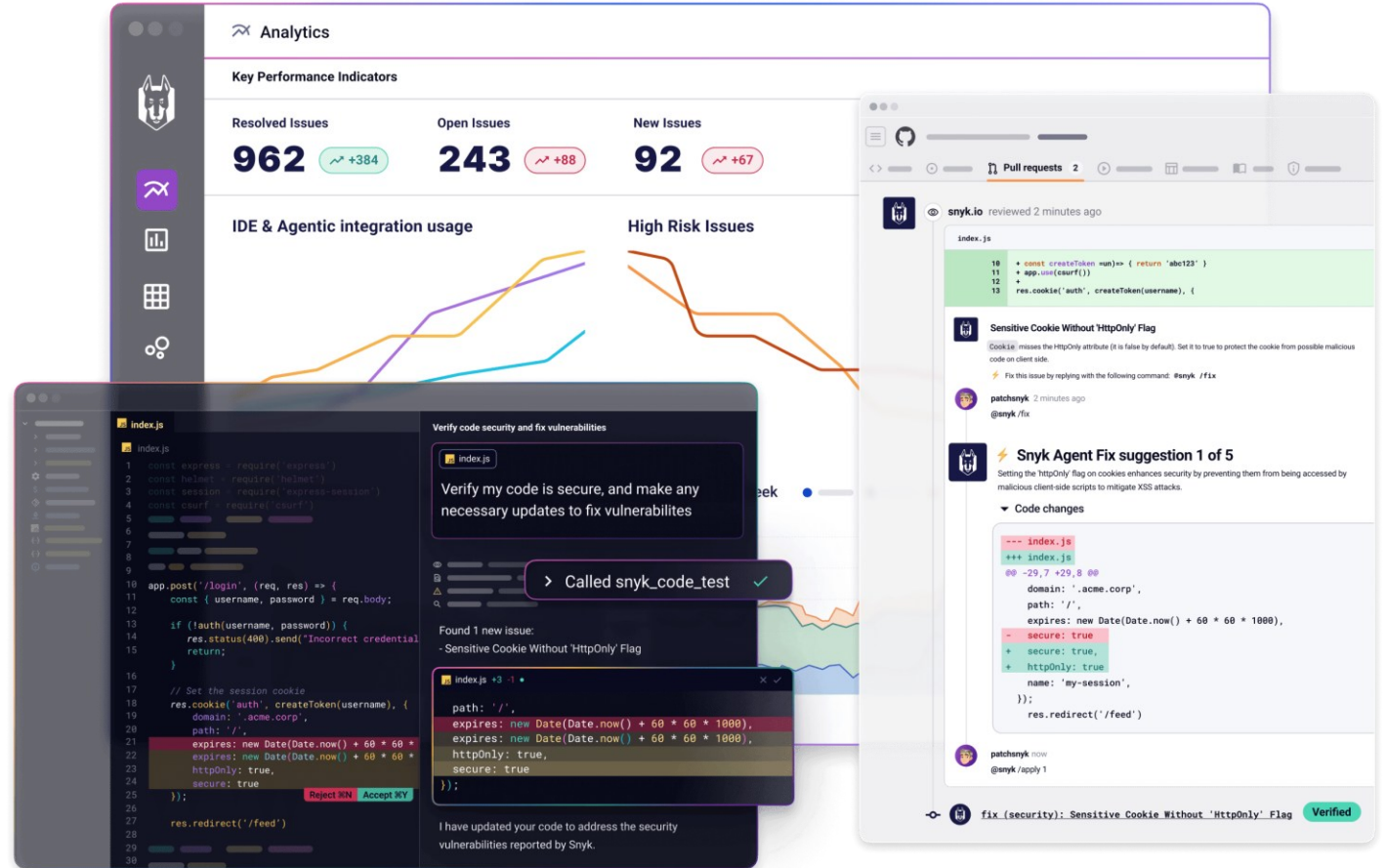
제품명	주요 특징	주요 사용자	운영방식	비고
AI기반 DevSecOps 보안플랫폼 Snyk 	IDE, CI/CD, 배포/운영 등 개발 전 주기 맞춤형 다양한 연 동 체계 지원, DevSecOps 적용 및 자동화 강점 AI 코딩 어시스턴트 통합(MCP) 제공	오픈소스 담당자 개발자, 보안담당자	SaaS	
공급망 관리 특화 SCA Insignary Clarity 	강력한 바이너리 분석 기능 지원, 공급망 관리 및 다양한 개발 및 운영 환경 대응	오픈소스 담당자 개발자, QA, 법무 등	하이브리드 온프레미스 SaaS	
스니펫 단위 정밀 분석 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	

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

Gartner 2025년
매직퀵드렌트 – 애플리케이션
보안 테스트툴(AST) 리더



Gartner Peer Insights
Customers' Choice
선정(2022)



Forrester Wave
2024년 SCA 도구 리더 선정

개발 전체 라이프사이클을 안전하게 보호하는 Snyk

모든 개발자

모든 유형의 코드

기존에 사용하는 다양한 워크플로우 도구들까지

상위 위험 우선순위 지정 및 수정

앱 개발자

플랫폼 개발자

Code

Open Source Dependencies

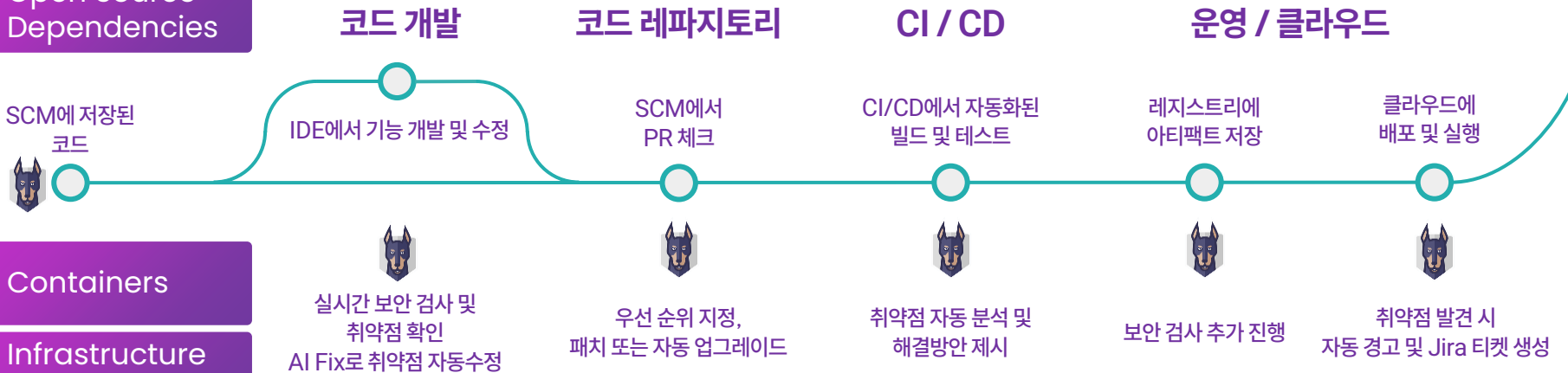
Containers

Infrastructure as Code

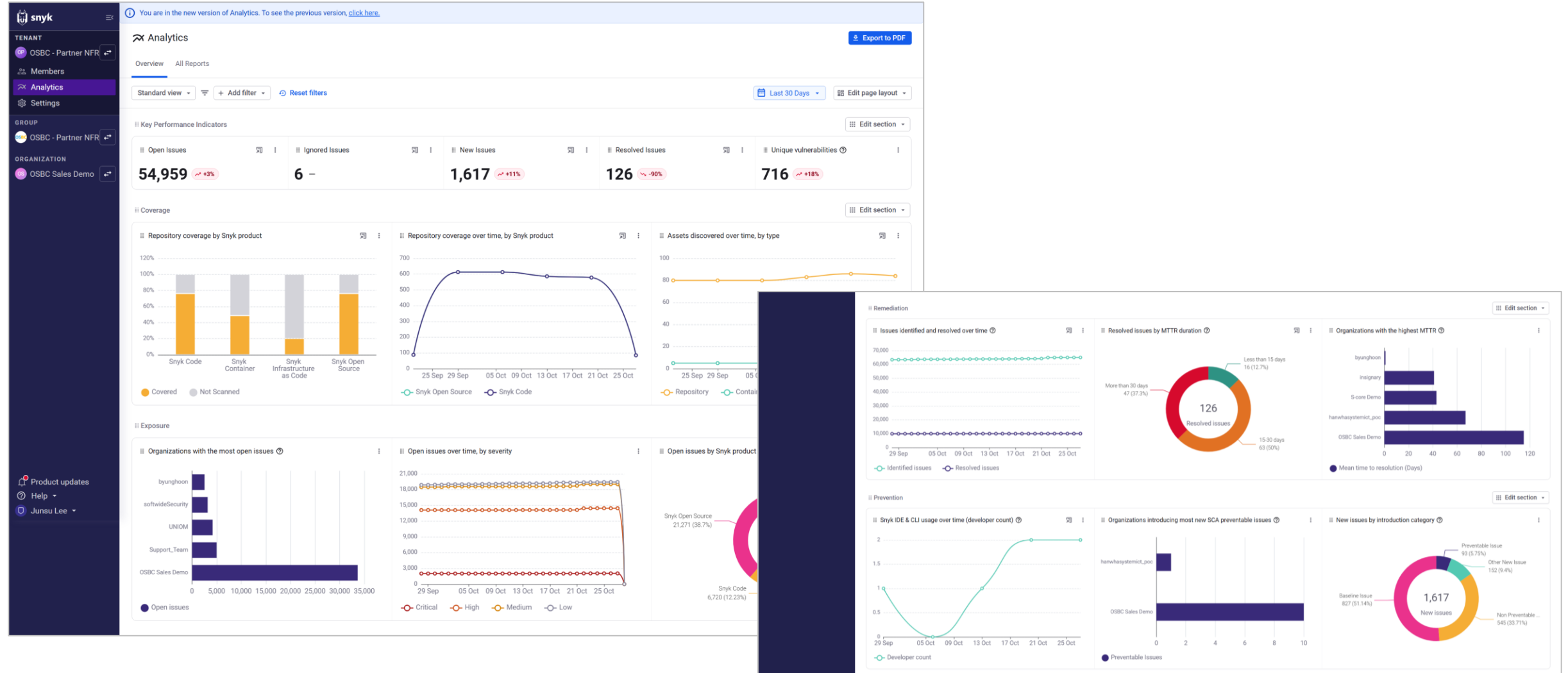
애플리케이션 인텔리전스

보안 교육 제공

보안 인텔리전스



Snyk Analytics, 최상위 레벨 통합 대시보드

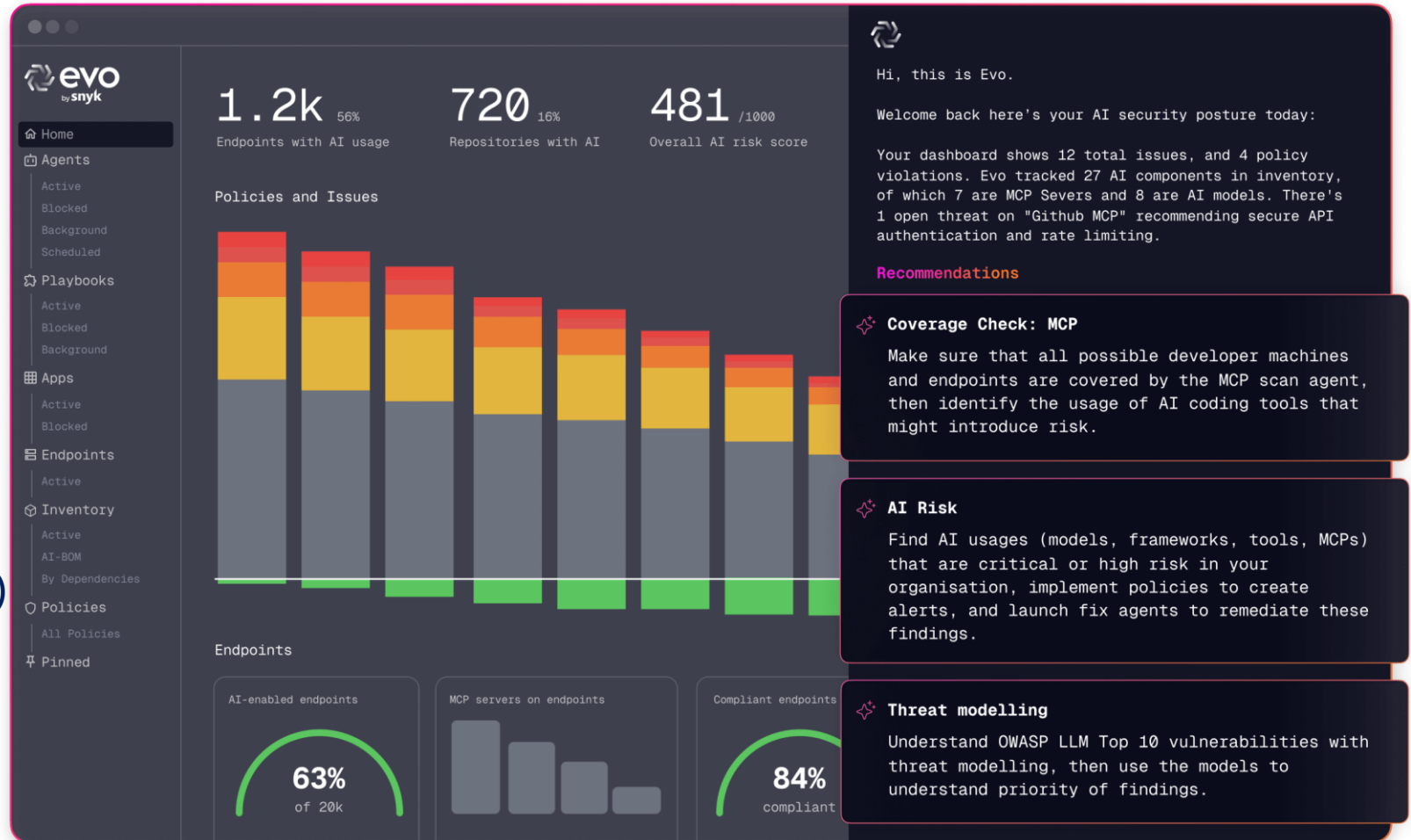


Evo by Snyk - 에이전틱 보안 오케스트레이션의 시작

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 작동하는 AI 보안 오케스트레이션 시스템입니다.

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



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

바이너리·소스코드 기반, SBOM·공급망 관리 특화 SCA 도구



01

소스코드 및 바이너리 모두 지원하는
정확한 오픈소스 식별

02

Deep Fingerprinting 기반의 정확한 분석
(특히 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

AI 생성 코드 대응, 스니펫 단위 오픈소스 정밀 식별 플랫폼

FossID Workbench 오픈소스 검증 프로세스

프로젝트 생성

프로젝트 기본 정보 입력

소스코드 분석

파일 업로드 또는 Git 지정

오픈소스 검증 진행

코드 비교 및 출처 식별작업 진행

오픈소스 내역(SBOM) 산출

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

자체 개발 코드와 일치하는 오픈소스 목록

Component	Version	License	Match Status	Matched Lines	Matched Lines Count
partial systemd	198	systemd	LGPL-2.1-only	src/boot/boot-loader.c	73 (32.3%)
partial systemd-stable	198	systemd	LGPL-2.1-only	src/boot/boot-loader.c	73 (32.3%)
partial systemd	f7ab...	linuxmint	LGPL-2.1-only	src/boot/boot-loader.c	73 (32.3%)
partial kernel	2.6.34.1	linux	GPL-2.0-only	src/boot/a20.c	67 (29.65%)
partial linux_kernel	2.6.34.1	linux	GPL-2.0-WIT	src/boot/a20.c	67 (29.65%)

자체 개발 코드

```

90 return count;
91 }
92
93
94
95 #include "boot.h"
96 #define MAX_BK42_LOOPS 100000
97 #define MAX_BK42_FF 32
98 static int empty_BK42(void)
99 {
100     u8 status;
101     int loops = MAX_BK42_LOOPS;
102     int ffs = MAX_BK42_FF;
  
```

오픈소스 코드

```

13 * Enable A2B gate (return -1 on failure)
14 *
15
16 #include "boot.h"
17
18 #define MAX_BK42_LOOPS 100000
19 #define MAX_BK42_FF 32
20
21 static int empty_BK42(void)
22 {
23     u8 status;
24     int loops = MAX_BK42_LOOPS;
25     int ffs = MAX_BK42_FF;
  
```


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 언제든지 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.

```

Evaluate Gates; Fail on Issues 36s
75 Resolving scan for gate evaluation...
76 Successfully found the 'develop' scan in the 'fossid-ab/fossid-e2e-demo' project!
77 Verifying scan completion...
78 Ensuring the Scan finished...
79 KB Scan is in progress. Waiting for completion...
80 KB Scan status: RUNNING (SCANNING) - File 16/16 (100%) -
81 KB Scan completed successfully (Completed in 17s).
82 KB Scan has completed successfully.
83 Ensuring Dependency Analysis finished...
84 Dependency Analysis has completed successfully.
85 Checking for pending files...
86 X Gate Failed: Found 2 pending files that require identi
87 Checking for policy warnings...
88 No policy warnings found.
89 Checking for vulnerabilities...
90 Warning: Found 149 vulnerabilities. Bv CVSS Score:
91 - CRITICAL: 24
92 - HIGH: 54
93 - MEDIUM: 70
94 - LOW: 1
95 Note: Gate is not
96 =====
97 Gate Evaluation Si
98 =====
99 Pending Files Ga
100 Policy Warnings G

X Check failure on line 1 in chaos.go
GitHub Actions / Run FossID D
FossID Detected License Issue
Snippet with 'Apache-2.0' file
Location: https://github.com/Ne
Component: pkg:github/netflix/cl
Download: https://github.com/Ne

Run VSF
failed now in 22s
> Checkout code
Run VSF
1 Run fossid \
11
12 ** VSF issue found in file: inflate.c:
13 CVE: CVE-2023-20966
14 CVE-URL: https://nvd.nist.gov/vuln/detail/CVE-2023-20966
15 [736] if (copy > have) copy = have;
16 [737] if (copy) {
17 [738] if (state->head != Z_NULL &&
18 [739] state->head->extra != Z_NULL) {
19 [740] len = state->head->extra_len - state->length;
20 [741] memcpy(state->head->extra + len, next,
21 [742] len + copy > state->head->extra_max ?
22 [743] state->head->extra_max - len : copy);
23 Error: CVE: CVE-2023-20966
24 CVE URL: https://nvd.nist.gov/vuln/detail/CVE-2023-20966
25
26
27 ** VSF issue found in file: inflate.c:
28 CVE: CVE-2023-21100
29 CVE-URL: https://nvd.nist.gov/vuln/detail/CVE-2023-21100
30 [736] if (copy > have) copy = have;
31 [737] if (copy) {
32 [738] if (state->head != Z_NULL &&
33 [739] state->head->extra != Z_NULL) {
34 [740] len = state->head->extra_len - state->length;
35 [741] memcpy(state->head->extra + len, next,

```


OSiMS (CSC)

SBOM 통합관리 플랫폼



TOP 5 컴포넌트/라이선스 현황

컴포넌트 라이선스

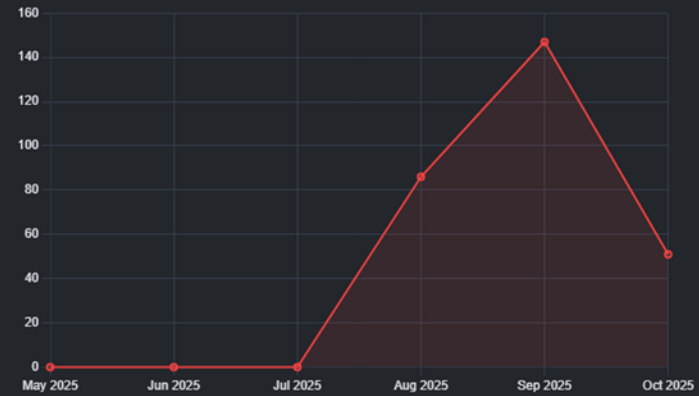


컴포넌트 사용 횟수

openssl	53
itextsharp	37
samba	37
libibatis-java	24
mybatis	24

문제가 감지된 컴포넌트

최근 6개월



취약점 현황

취약점 등급

등급 S	39
등급 A	4
등급 B	0
등급 C	4

의무 유형 현황

1	20
2	88
3	114
4	25
5	0

충돌 현황

정책 충돌	55
라이선스 충돌	38

감사합니다.

이준수

jslee@osbc.co.kr

jslee@opensource.or.kr

OSBC