



오픈소스 소프트웨어 개발 공급망 보안 및 거버넌스 필수 전략



(주)오에스씨코리아
WWW.OSCKOREA.COM



목차

- 소프트웨어 공급망 공격 (Software Supply Chain Attack) 기법 및 현황
- Sonatype Nexus 플랫폼
- Nexus Firewall 구성 및 운영
- Nexus Lifecycle 추가 기능

■ It's All In The Numbers



3년간 SDLC 공격이
742% 증가



매월 12억 개 이상의
취약점이 다운로드



프로젝트 7개 중 6개의 취약점은
전이 취약성에 해당



약 96%의 오픈소스 취약점은
유입단계에서 예방 가능

Source: Sonatype's 8th Annual State Of The Software Supply Chain Report, available at <https://www.sonatype.com/ssc>

- Writing code is out, borrowing code is in



90%

어플리케이션의
오픈소스 구성비율

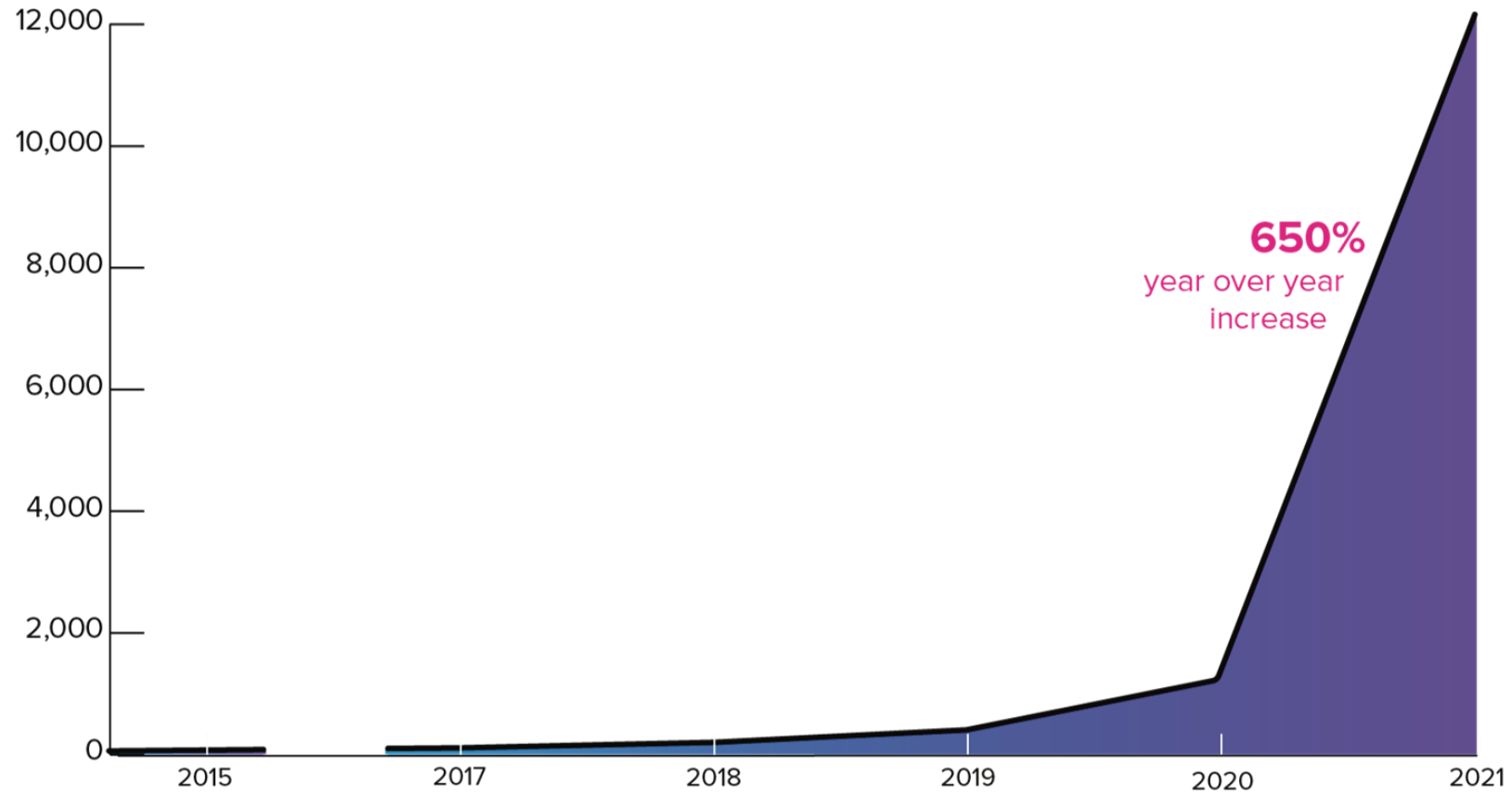


21,000+

이상의 신규 오픈소스 버전이 매일
공급망(또는 프로젝트 매니저)에
릴리스

2020 State of the Software Supply Chain Report, Sonatype

- Novel attacks are on the rise



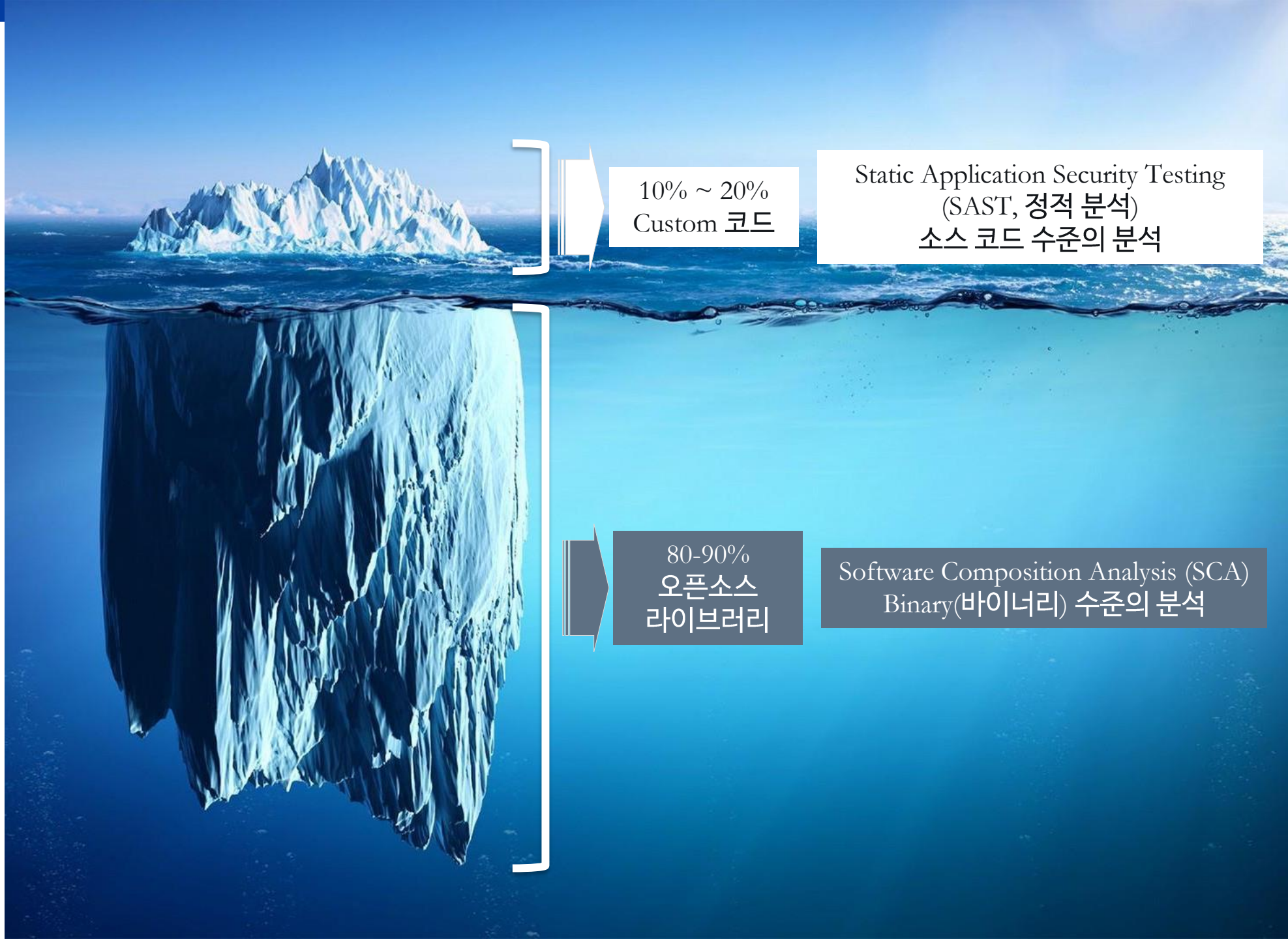
Source: State of the Software Supply Chain Report



sonatype

어플리케이션 보안

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



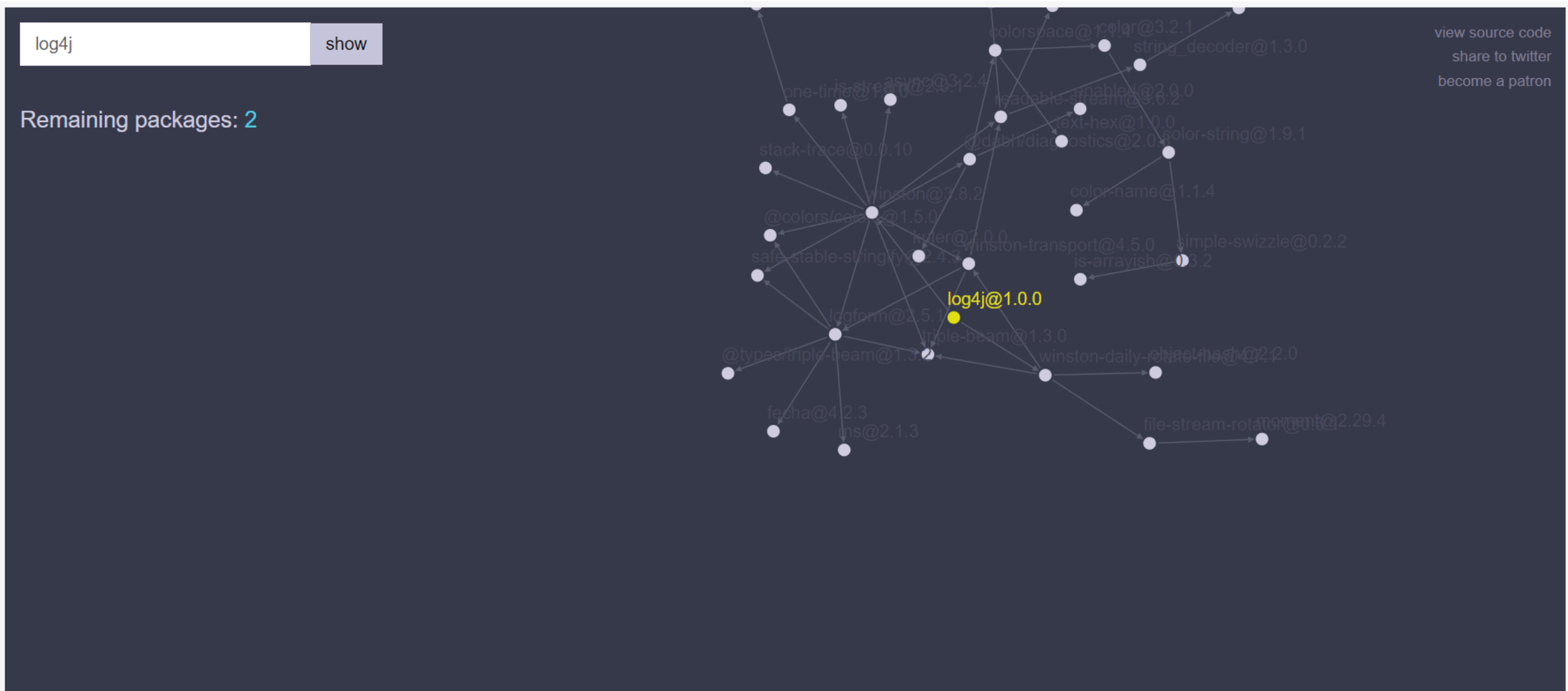
10% ~ 20%
Custom 코드

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

80-90%
오픈소스
라이브러리

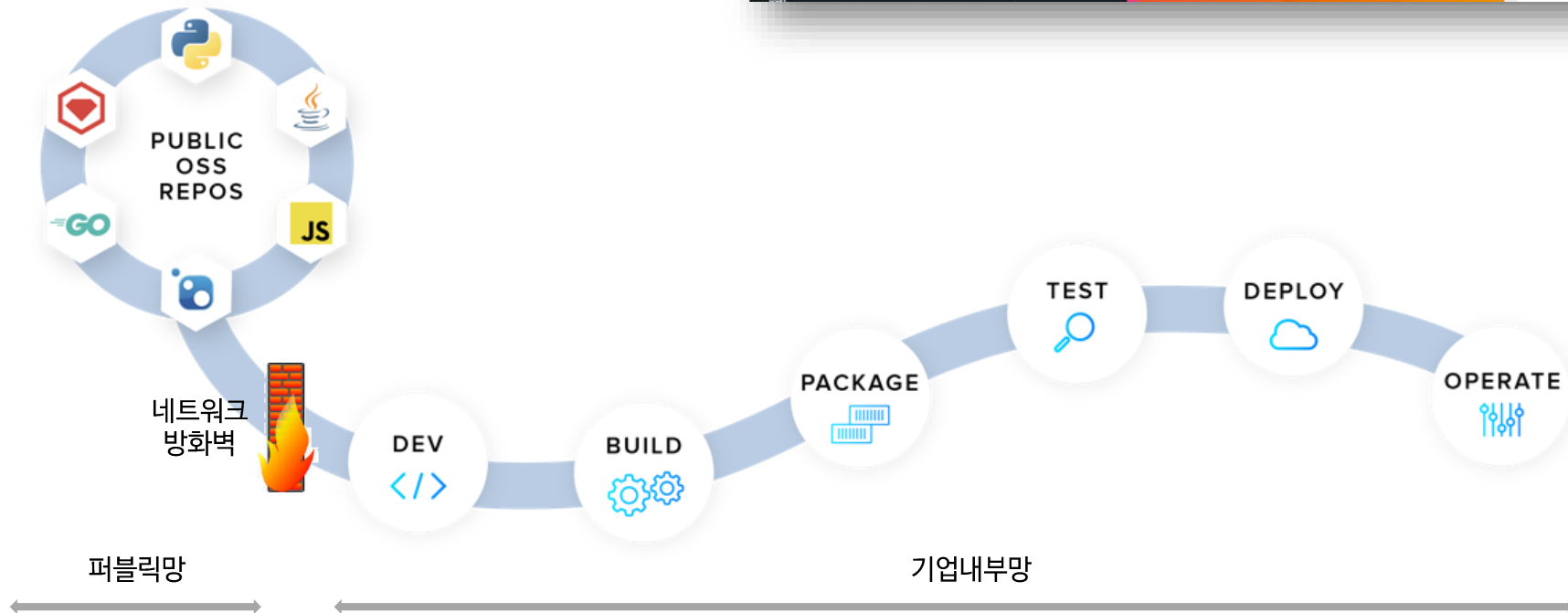
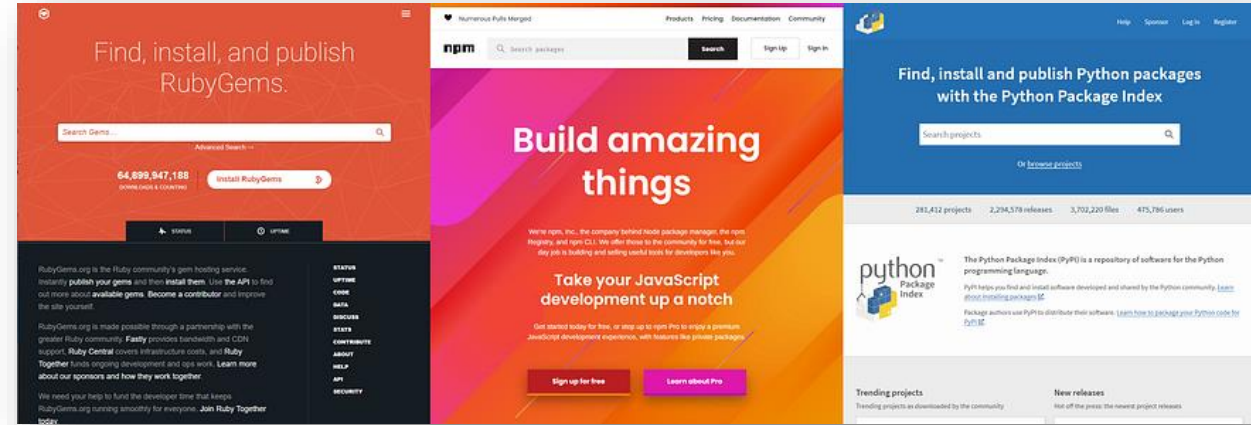
Software Composition Analysis (SCA)
Binary(바이너리) 수준의 분석

■ Dependency & Transitive Dependency



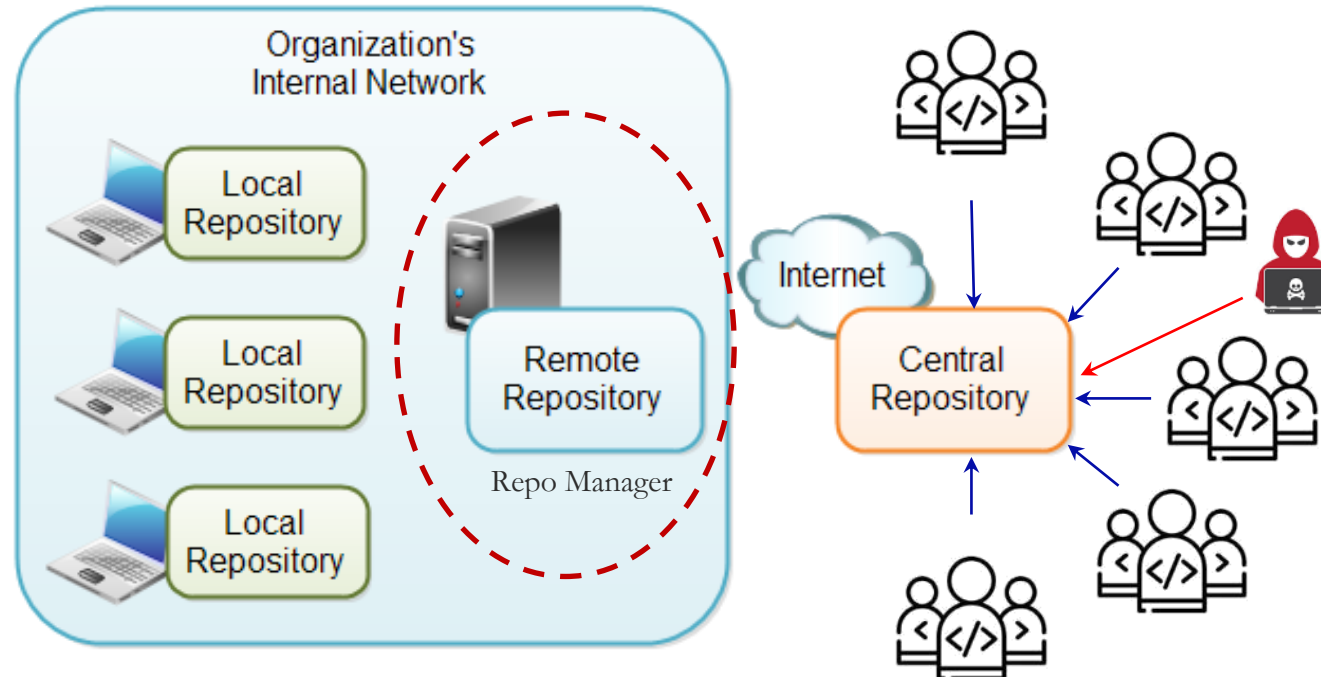
■ 오픈소스 배포 & Public Repository

- Public Repository는 프로그래밍 언어별로 운영
- Binary 패키지 형태로 배포
- Public Repository는 무결성(Malware-Free)을 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 Library를 사용하게 함
- 내부에만 사용되는 공통 Library를 Hosting 하기 위한 저장소 용도



■ Software Supply Chain 공격기법 - Typosquatting (타이포스쿼팅)

- 주요 패키지명의 타이핑 오류를 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 켄(Gem)의 타이포스쿼팅 루비켄(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
```

```
babelcli: 42 babelcli: 20 babelcli: 42
babelcli: 20 babelcli: 42 babelcli: 42 babelcli: 42 babelcli: 42 babelcli: 42 babelcli: 42
babelcli: 42 babelcli: 42 babelcli: 42 babelcli: 42 babelcli: 42 babelcli: 42 babelcli: 42
```



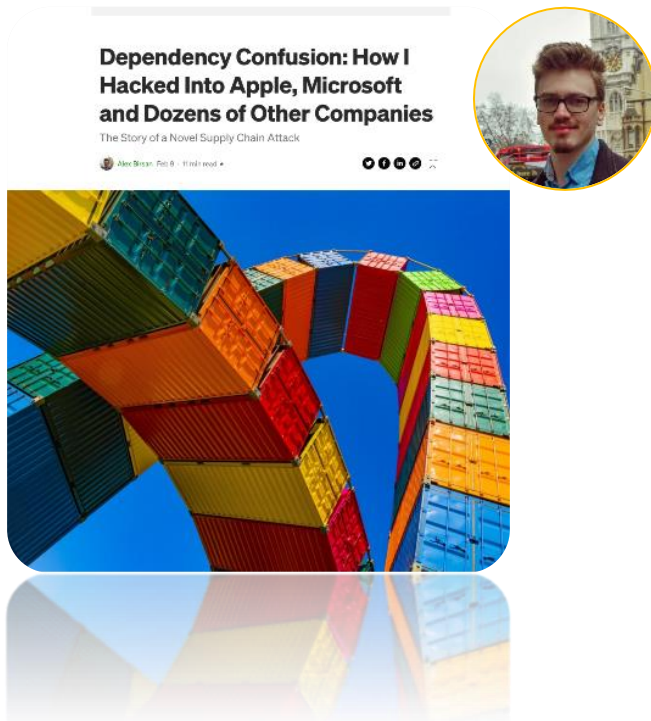
cross-env -> **crossenv**
express -> **exprss**
electron -> **electorn**

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

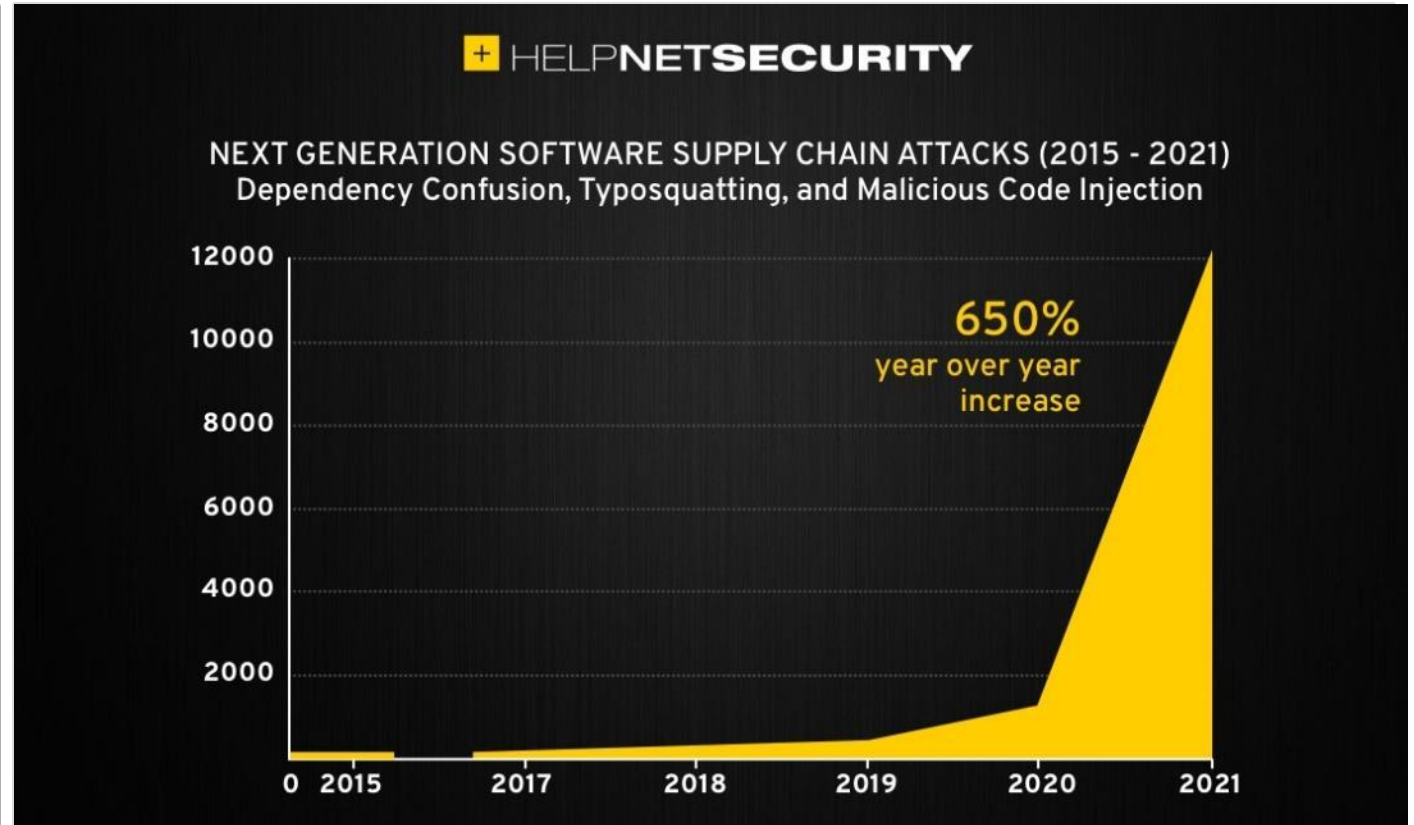
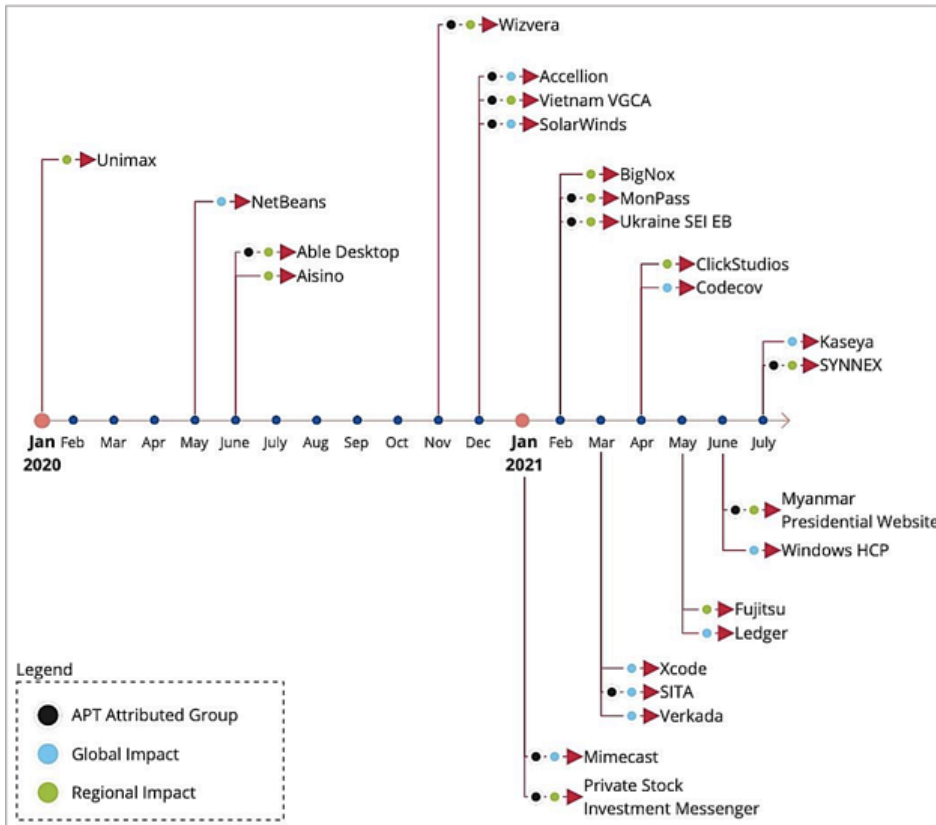
Software Supply Chain 공격기법 - Dependency Confusion (의존성 혼동)

- 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



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.

White House National Cybersecurity Strategy: Landmark Action for a Critical Threat

FIND OUT MORE

[Blog](#) [DevZone](#) [Contact Us](#)



Platform

Solutions

Pricing

Resources

Partners

Company

BOOK A DEMO

OPEN SOURCE COMPONENTS ANALYZED BY NEXUS INTELLIGENCE:

1 2 8 , 6 0 0 , 8 9 9

A History of Software Supply Chain Attacks

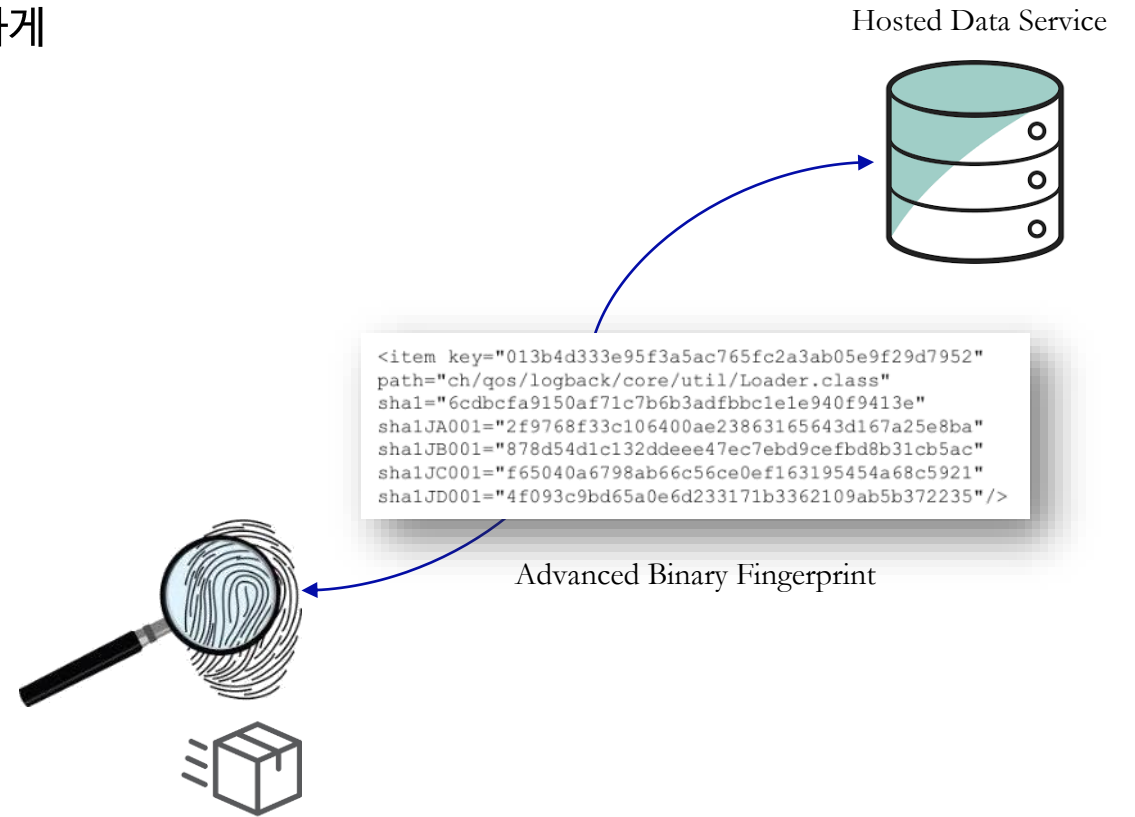
July 2017–Present

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

❖ 식별 방식

- **Manifest Scanning** : Build Manifest 파일을 사용하여 Dependency를 파악 (package.json, pom.xml 등)
- **Binary Scanning** : Binary Fingerprint를 사용하여 Build Artifact를 분석하는 방식으로 Final Build에 포함된 Package만 식별함으로써 False Positive 가능성 감소



Sonatype Nexus Platform은 1) Manifest Scanning과 2) Binary Scanning을 모두 사용하여 보다 정확한 분석결과를 도출함

■ CVE 한계 및 공급망 공격의 고도화

- SCA 도구는 보안 위협을 놓치지 않도록 **False Negative** 가 없어야 하며, **False Positive**를 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 faecbook.com
DOUBLING CHARACTERS twitter.com	USING SIMILAR LOOKING CHARACTERS google.com (l vs i)	PRESSING A WRONG KEY costko.com



sonatype

Nexus Intelligence



경쟁사 대비 70% 많은 취약성 DB

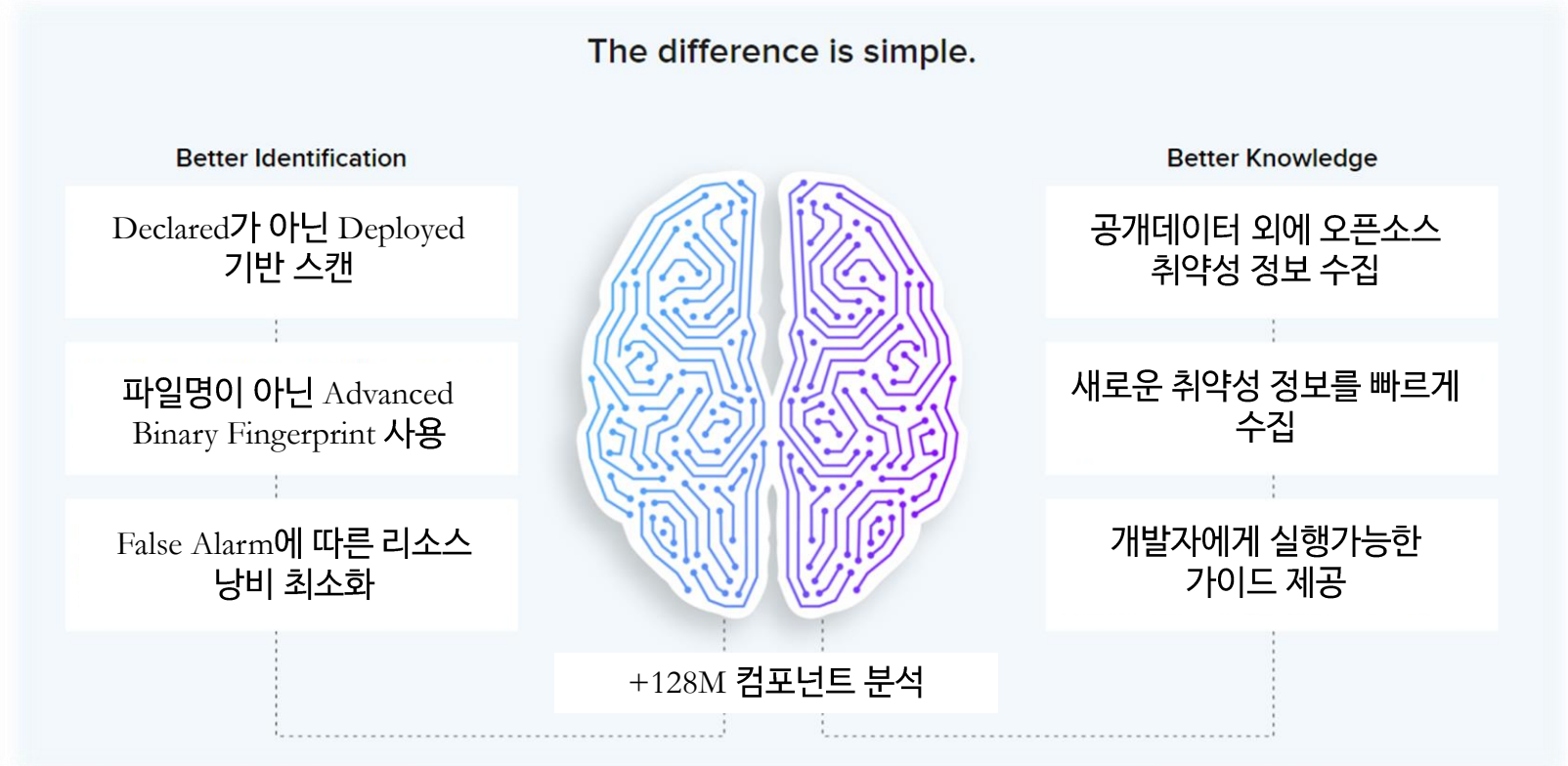


NVD 대비 10배 빠른 속도



65명의 글로벌 보안 전문연구원

Nexus Platform은 **글로벌 최대 데이터베이스를 기반으로** 가장 정확한 정보를 빠르게 제공합니다



Central Repository



Sonatype Research



National Vulnerability Database



GitHub



OSS Index



Nexus Repository



Google Search Alerts



Security Advisories

Sonatype Nexus Platform

Nexus Lifecycle

SDLC의 모든 단계에 걸쳐 지속적으로 위험요소를 확인하고 정책을 반영하며, 취약점 교정



Nexus Firewall

위험요소의 SDLC 유입을 자동으로 차단



DEV



BUILD



PACKAGE



TEST



DEPLOY



OPERATE



Nexus Repository

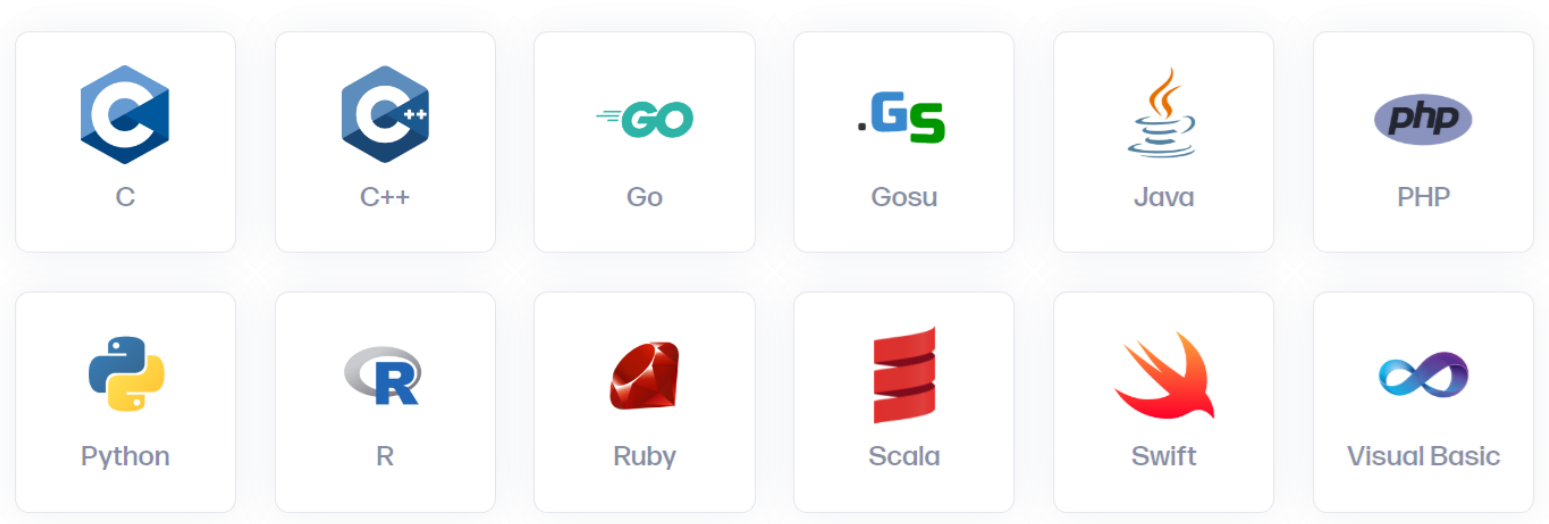
SDLC에 걸친 라이브러리, build artifacts, release candidates



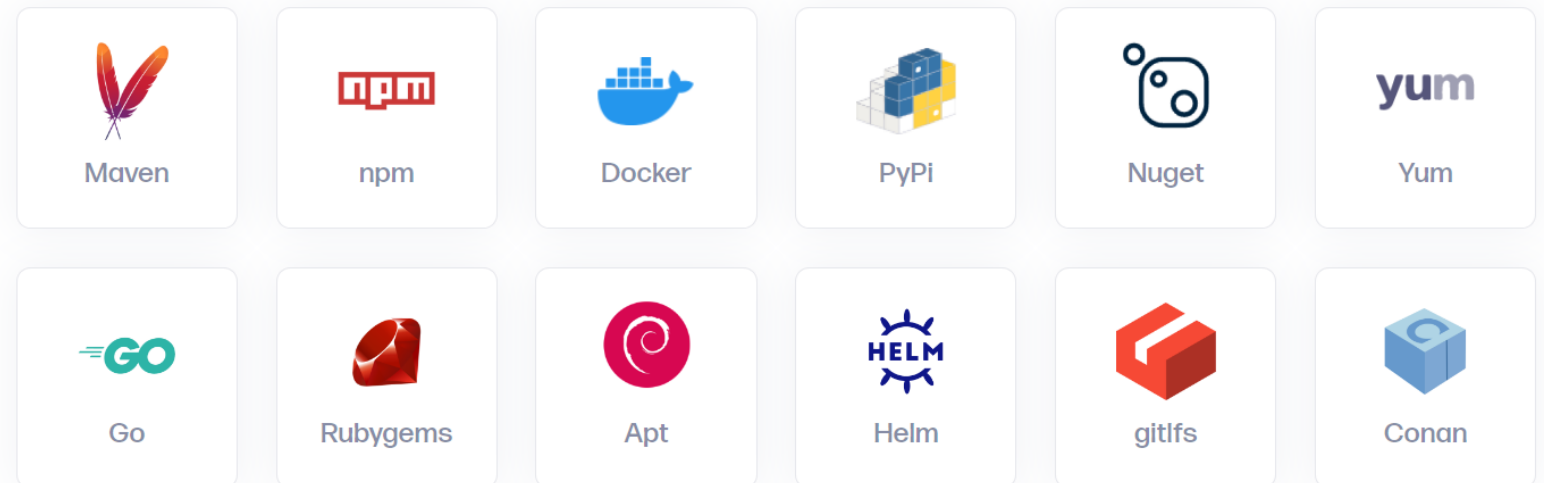
지원 언어 및 패키지

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

Firewall language support



Firewall package support



Nexus Repository OSS(오픈소스)는 취약점이나 라이선스에 대한 요약정보만 제공하며
 Nexus Repository Pro는 세부정보 추가 제공



- World #1 Repository Manager



FOR Central
 ON Thu Aug 20 2020 at 6:51:05 PM
 AGE 8 minutes

4670 COMPONENTS IDENTIFIED
 100% of 4670 TOTAL

Issue Summary

Category	Count
Security Vulnerabilities	
Critical (7-10)	780
Severe (4-6)	434
Moderate (1-3)	12
License Warnings	
Copyleft	154
Non Standard	228
Not Provided	23
Weak Copyleft	860
Liberal	3405

Threat Level 0 50 100 150 200 250 300 350 400

What should I do with this report?

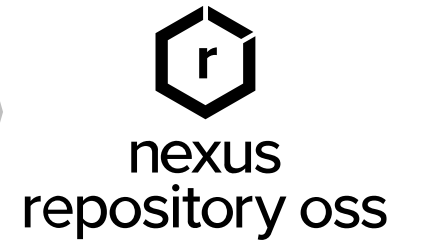
Get Nexus Firewall

Benefits

- Stop bad components at the front door
- Automatically shield your software from open source risks

[Learn More](#)

[View Detailed Report](#)



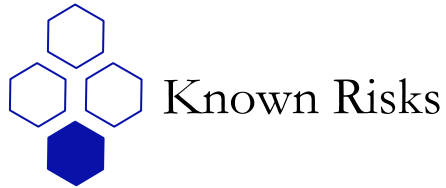
View By: Vulnerabilities

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

- Known vs. Unknown Risk(위협)



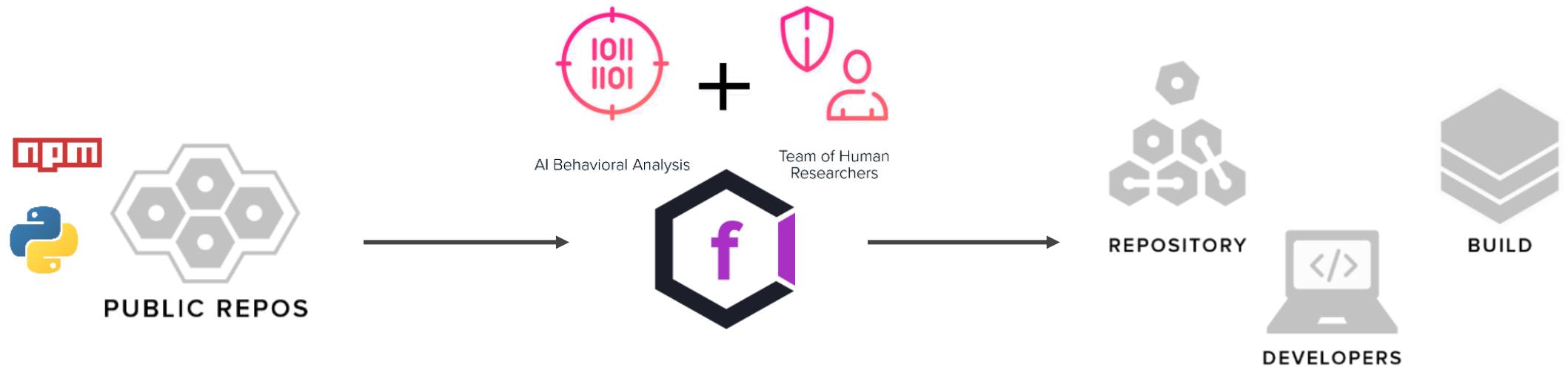
Known Risks

Known Risk에 대한 대응 : 다운로드 차단



Unknown Risks

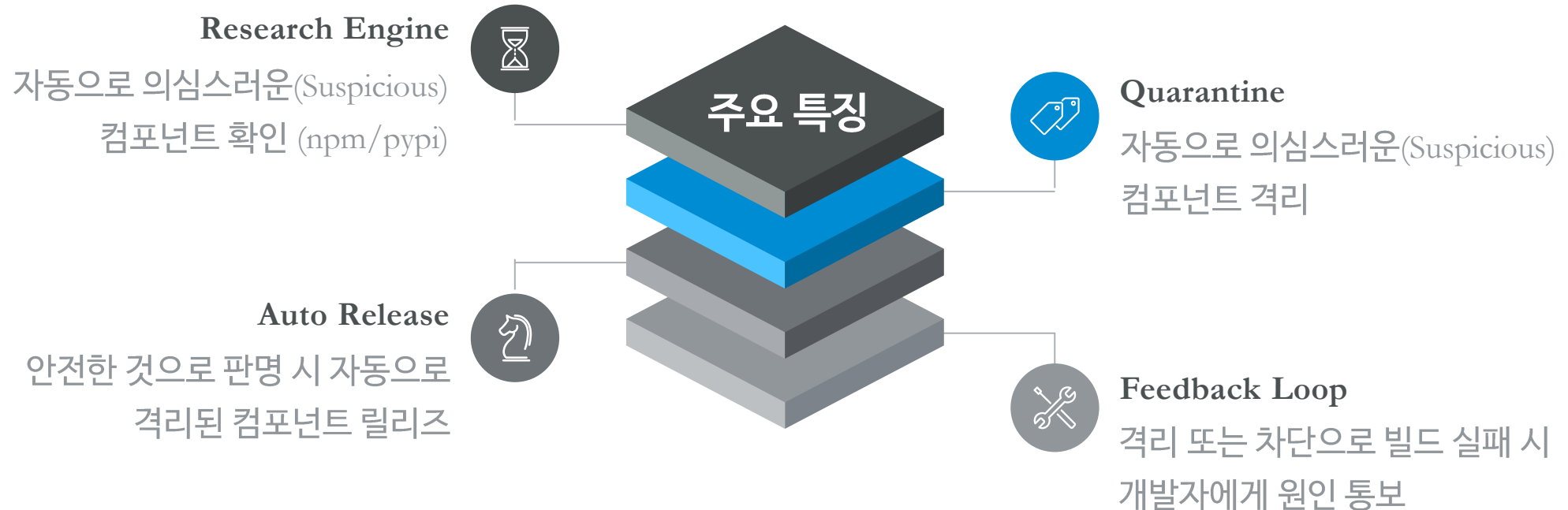
Unknown Risk에 대한 대응 : Nexus Research Engine은 AI/ML 알고리즘을 통해 Ecosystem(npm, pypi) 을 24X7X365 모니터링 하여 선제적으로 대응



nexus firewall

최신 소프트웨어 공급망 공격 방어 최전선

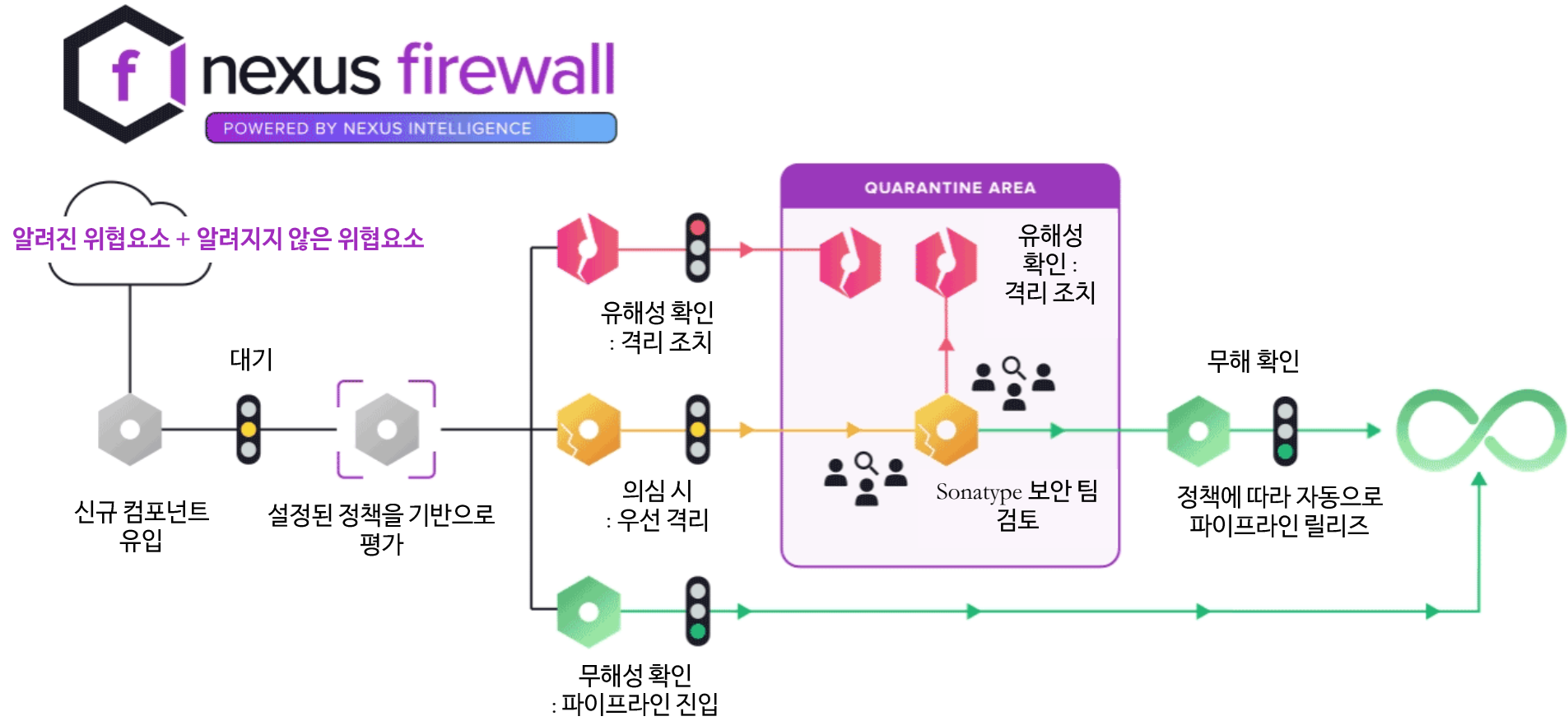
Nexus Firewall 은 알려진 취약점은 물론, 알려지지 않은 취약점까지 **선제적**으로 방어합니다.



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



Shift Security Left



- 인공지능 기반으로 오픈소스를 평가하여 유해한 것으로 판단되는 경우 자동으로 다운로드를 차단하며 오픈소스 유입정책을 수립하여 제어
- Nexus Firewall이 차단하는 주요 공격 : **Dependency Confusion, Cryptomining Malware, Ransomware 등**

Nexus Firewall 주요 기능 – Repository Audit & Quarantine



nexus
firewall

- Powered by IQ Server

IQ Server

Repositories Manage repositories

Create repository

Repo

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

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

Quarantine Status

Active

on 1 of 1 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](#)

Quarantine Updated 11:59:28 p.m. 2021-05-10 [Refresh](#)

THREAT	POLICY NAME	QUARANTINE DATE	COMPONENT	REPOSITORY
10	Security-Critical	2021-05-10	com.pojosontheweb : woko-blobs-web : war : 2.2-beta7	test-repo
10	Security-Critical	2021-05-10	org.mule.examples : mule-example-errorhandler : zip : 3.4-M1	test-repo
10	Security-Critical	2021-05-10	org.atmosphere.samples : atmosphere-twitter-live-feed : war : 0.8.2	test-repo
10	Security-Critical	2021-05-10	smartrics.restfixture : smartrics-RestFixture : zip : bin : 4.0	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-o	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

for maven-central

COMPONENTS IDENTIFIED 100% OF ALL COMPONENTS ARE IDENTIFIED

POLICY ALERTS 2 1 4 AFFECTING 3 COMPONENTS

QUARANTINED COMPONENTS

FILTER: All Exact Unknown VIOLATIONS: Summary All Quarantined Waived

Policy Threat	Component	Quarantined
Security-Critical	commons-collections : commons-collections : 3.2.1	
Security-Critical	org.codehaus.plexus : plexus-utils : 3.0.9	
Security-High	apache-beanutils : commons-beanutils : 1.7.0	
Architecture-Cleanup	junit : junit : 3.8.1	
Architecture-Quality	apache-velocity : velocity : 1.5	
	asm : asm : 3.3.1	
	commons-logging : commons-logging : 1.0.4	
	commons-validator : commons-validator : 1.2.0	
	org.apache.maven : maven-plugin-api : 2.0.9	
	org.apache.maven : maven-plugin-descriptor : 2.0.9	
	org.apache.maven : maven-plugin-parameter-documenter : 2.0.9	
	org.apache.maven : maven-remote-resources-plugin : 2.5	

Nexus Firewall 주요 기능 – Violation Remediation



- Powered by IQ Server

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

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.xwork : xwork-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 with Severity < 10 Found Security Vulnerability without Status NOT_APPLICABLE	Waive
Security-Medium	Medium risk CVSS score	Found Security Vulnerability with Severity >= 4 Found Security Vulnerability with Severity < 7 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
5	OSVDB-102945	?	Open

Developer(개발자) View - Accessing a Report



nexus
firewall

- Shift Security Left

```
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/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 ~ %
```

Developer(개발자) View - Quarantined Component View



nexus
firewall

- Shift Security Left

1 Policy에 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

Component Info Policy Licenses Vulnerabilities Labels

Version Graph

Popularity: Older This Version Newer

Breaking Changes: [Red bars]

Policy Threat: [Red bar] 0.9.1.1

Click on the graph above to see details about different versions

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 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

Policy

SUMMARY

Policy Name: Security-Critical Threat Level: 10

Policy Violation Grandfathering
 Allow this policy to be grandfathered

INHERITANCE

Permits to
 All Applications and Repositories
 Applications of the specified Application Categories in Root Organization

Policy Actions Override
 Allow actions to be overridden by children

CONSTRAINTS

Constraint Name: Critical risk CVSS score

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

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

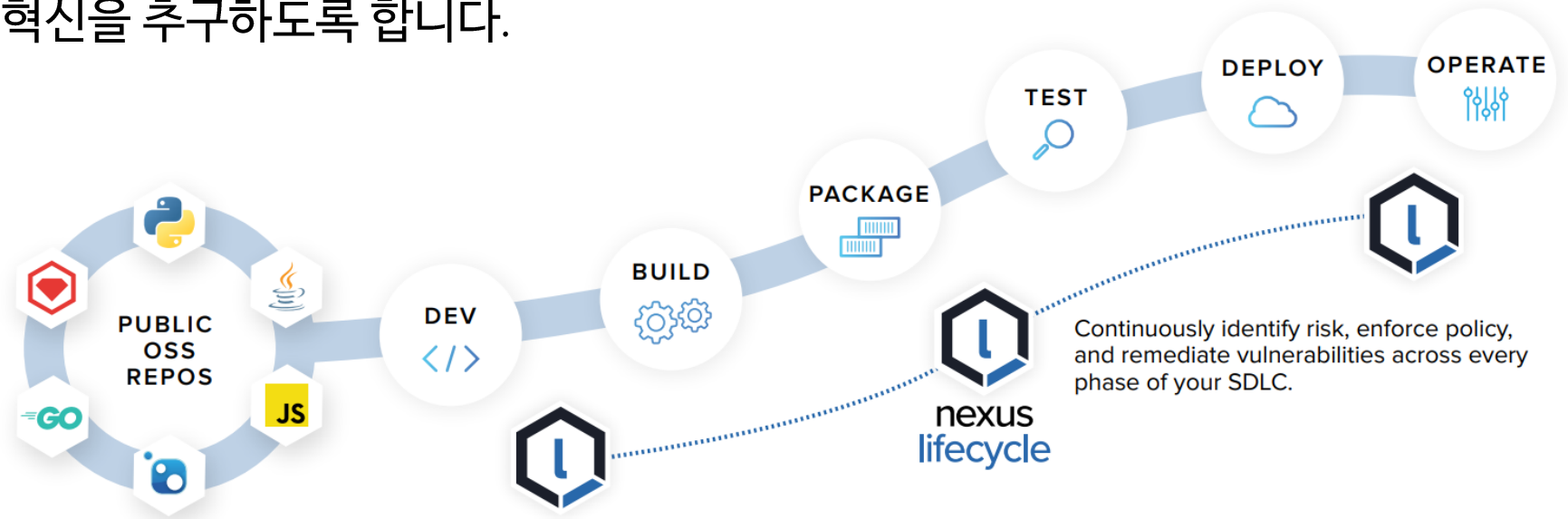
RECIPIENT: PROXY DEVELOP SOURCE BUILD STAGE RELEASE OPERATE CONTINUO... MONITORING

No notifications configured

Notifications

Recipient Type: Email

Nexus Lifecycle은 개발자 및 보안 담당자가 오픈소스를 보다 안전하게 혁신을 추구하도록 합니다.



- World #1 Software Composition Analysis



현업에서 사용하는 주요 Pipeline 툴과 사전 정합 되어 있습니다.



개발자 IDE 환경 지원 (via IQ Server Integration)



- World #1 Software Composition Analysis



The screenshot displays the following components and details:

- Component List (1):** A list of 59 components, with 'icu4j - 2.6.1' selected.
- Recommended Version(s) (2):** Shows '55.2' as the next version with no policy violation.
- Version Graph (3):** A graph comparing 'Older', 'This Version', and 'Newer' versions across 'Popularity' and 'Policy Threat' (Security, License, Quality, Other).
- Selected Version (4):**
 - Group: com.ibm.icu
 - Artifact: icu4j
 - Version: 2.6.1
 - Declared License: Not Declared
 - Observed License: No Sources
 - Effective License: Not Declared, No Sources
 - Highest Policy Threat: 9
 - Highest CVSS Score: 7.5
 - Cataloged: 13 years ago
 - Match State: exact
 - Identification Source: Sonatype
 - Category: Internationalization
- Buttons (5):** 'View Details' and 'Migrate to Selected' buttons.

- 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 Material) 자동 생성



- World #1 Software Composition Analysis



Filter Manage

Results

VIOLATIONS COMPONENTS APPLICATIONS

NAME	AFFECTED APPS	TOTAL RISK	CRITICAL	SEVERE	MODERATE	LOW
commons-httpclient : commons-httpclient : 3.1	11	200	81	113	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	10					
org.apache.struts : struts2-core : 2.3.34	4					
commons-collections : commons-collections : 3.2.1	9					
org.apache.struts.xwork : xwork-core : 2.3.34	4					
org.springframework : spring-context : 2.5.6.SEC03	6					
org.apache.httpcomponents : httpclient : 4.2.5	6					
org.springframework : spring-web : 2.5.6.SEC03	6					
org.apache.jackrabbit : jackrabbit-webdav : 2.5.2	6					
org.springframework : spring-web : 3.0.5.RELEASE	4					
org.apache.struts : struts2-rest-plugin : 2.3.34	4					
commons-fileupload : commons-fileupload : 1.2.1	6					

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

Filter: All Exact Up

Policy Threat -

Search Name

License-Banned

Security-High

Component Info Policy

Threat Level - Problem C

9 CVE-2017-

Explanation

...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.

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.

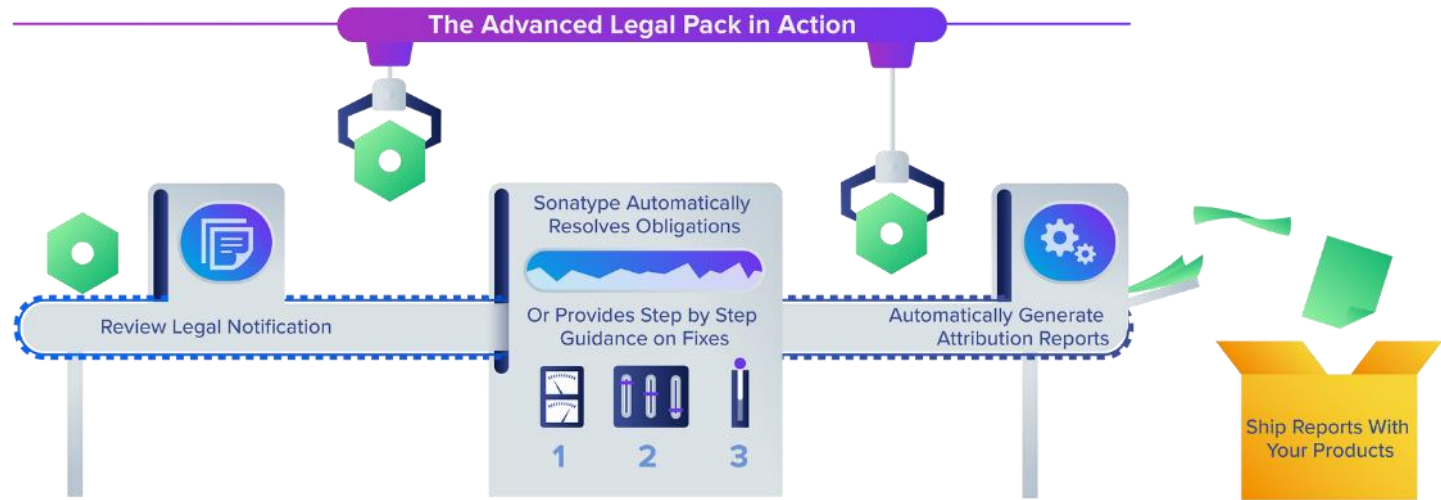
Recommendation

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

Close

위험요소에 대한 전문 교정가이드 제공

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

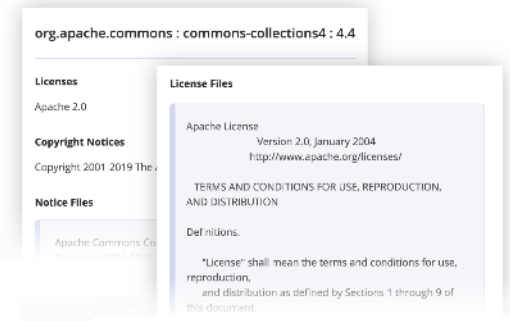
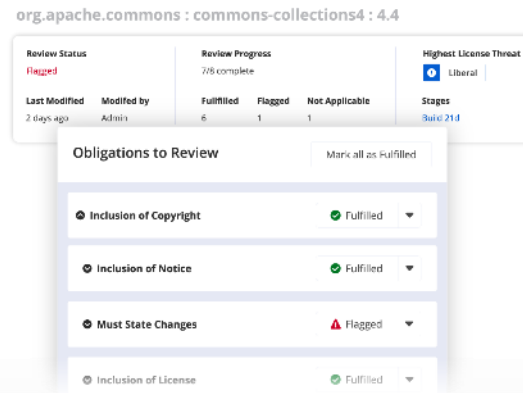
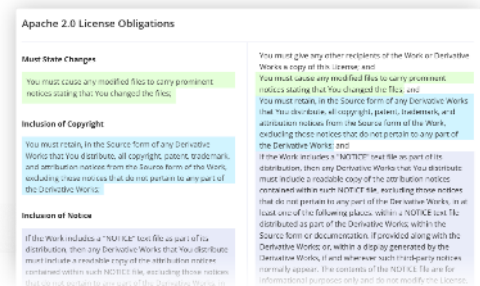


- World #1 Software Composition Analysis

라이선스 의무 검토 도구
License Obligation Review Tool
사용중인 컴포넌트에 대한 모든 라이선스를 쉽게 검토할 수 있는 도구제공

Compliance 워크플로우
의무사항들을 조치할 수 있는 단계별 워크플로우 제공

Attribution 보고서
자동으로 관련정보를 수집하여 Attribution Report (사용내역 고지) 제공



The logo for OSC, consisting of the letters 'O', 'S', and 'C' in a stylized, white, rounded font. The 'O' and 'S' are connected at the bottom, and the 'C' is positioned to the right of the 'S'.

감사합니다

(주)오에스씨코리아
서울 강남구 테헤란로 5길 7, 13층 (KG타워) 06134 | 02.539.3690
sales@osckorea.com | www.osckorea.com