

DevSecOps 환경을 위한 "Open-Source Governance 자동화 플랫폼"

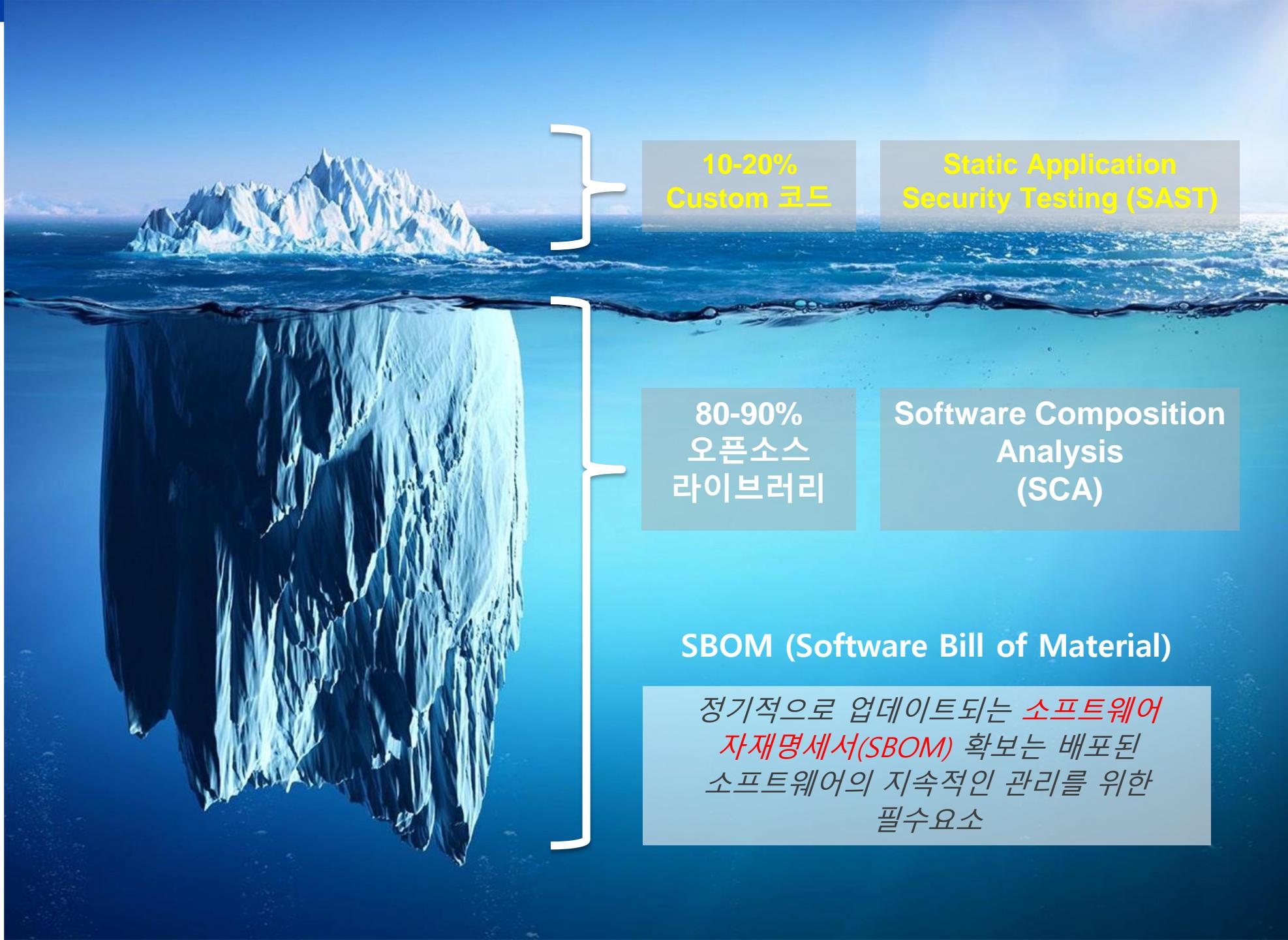
Sonatype Platform

July 2023

(주)오에스씨코리아
www.osckorea.com

Why Sonatype?

어플리케이션 보안은 복잡하고 다양한 측면을 가진 문제이며 Custom 코드에 대한 테스트 및 오픈소스 라이브러리에 대한 취약점분석이 필요함



10-20%
Custom 코드

Static Application
Security Testing (SAST)

80-90%
오픈소스
라이브러리

Software Composition
Analysis
(SCA)

SBOM (Software Bill of Material)

정기적으로 업데이트되는 **소프트웨어 자재명세서(SBOM)** 확보는 배포된 소프트웨어의 지속적인 관리를 위한 필수요소

SBOM (Software Bill of Material)

- #### ▪ 소프트웨어 자재명세서

Hardware BOM

TIDA-00771 REV E2 Bill of Materials									
Item #	Designator	Quantity	Value	PartNumber	Manufacturer	Description			PackageReference
1	C1, C3, C15	3	1uF	C1608XTRIC105K	TDK	CAP, CERM, 1 μ F, 16 V, +/- 10%, XTR_0603			0603
2	C2, C4	2	0.047uF	C1608XTRIE473K	TDK	CAP, CERM, 0.047 μ F, 25 V, +/- 10%, XTR_0603			0603
3	C5	1	4.7uF	GRM31CR71E475KA13L	MuRata	CAP, CERM, 4.7 μ F, 50 V, +/- 10%, XTR_1206			1206
4	C6	1	4.7uF	GRM21B81C474KAB8L	MuRata	CAP, CERM, 4.7 μ F, 16 V, +/- 10%, XSR_0805			0805
5	C7, C8, C9	3	2.2uF	GRM32ER27A225KA35L	MuRata	CAP, CERM, 2.2 μ F, 100 V, +/- 10%, XTR_1210			1210
6	C10, C14, C26, C27, C30	5	1000pF	885012205061	Wurth Elektronik	CAP, CERM, 1000 pF, 50 V, +/- 10%, XTR_0402			0402
7	C11	1	3300pF	C1005XTR1H332K	TDK	CAP, CERM, 3300 pF, 50 V, +/- 10%, XTR_0402			0402
8	C12	1	2.2uF	GRM31CR71E225KA8L	MuRata	CAP, CERM, 2.2 μ F, 50 V, +/- 10%, XTR_1206			1206
9	C13, C18, C23, C28, C31	6	0.1uF	885012050516	Wurth Elektronik	CAP, CERM, 0.1 μ F, 16 V, +/- 10%, XSR_0402			0402
10	C16	1	10uF	0805YD106M07A2	AVX	CAP, CERM, 10uF, 16V, +/-20%, XSR_0805			0805
11	C17, C29	2	0.1uF	0603YC104JAT2A	AVX	CAP, CERM, 0.1 μ F, 16V, +/- 5%, XTR_0603			0603
12	C19, C20	2	270uF	EKN23N30E0L271MCC5S	United Chemi-Con	CAP, ALUM 270uF 20% 55°C RADIAL			10x20
13	C21	1	0.1uF	C2012XTR1E104K	TDK	CAP, CERM, 0.1 μ F, 25 V, +/- 10%, XTR_0805			0805
14	C22	1	2200pF	GRM55R71H222KA01D	MuRata	CAP, CERM, 2200 pF, 50 V, +/- 10%, XTR_0402			0402
15	C24	1	0.01uF	O0603X103K5RACTU	Kemel	CAP, CERM, 0.01 μ F, 50 V, +/- 10%, XTR_0603			0603
16	D1	1	RED	15000605R57000	Wurth Electronics Inc	LED, RED CLEAR 15000605R57000 SMD	LED_0603		
17	D2	1	30V	SM3A03CA	Littelfuse	Diode, Schottky, 30V, 0.3A, DO-214AC	DO214AC-30V-0.3A		DO214AC
18	D3	1	10ULLCW	10ULLCW	Wurth Electronics Inc	LED, YELLOW, CLEAR 10ULLCW SMD	LED_0603		
19	D4	1	GREEN	1500606GS75000	Wurth Electronics Inc	LED, Green, SMD	LED_0603		
20	D5	1	40V	NSR0240V21TG	ON Semiconductor	Diode, Schottky, 40 V, 0.25 A, SOD-523	SOD-523		
21	J1	1	PEC045AA	PEC045AAN	Sullins	Header, Male 4-pin, 100mil spacing.			0.100 inch x 4
22	J2	1	800-10-003-10-001000	Mil-Max	Header, 100mil, 3x1, TH				Header, 3x1, 100mil, TH
23	J3	1	800-10-005-10-001000	Mil-Max	Header, 100mil, 5x1, TH				Header, 5x1, 100mil, TH
24	J4	1	800-10-002-10-001000	Mil-Max	Header, 100mil, 2x1, TH				Header, 2x1, 100mil, TH
25	LBL1	1	TIDA-00771	Any	Printed Circuit Board				
26	Q1, Q2, Q3, Q4, Q5, Q6	6	30V	CSD17576Q5	Texas Instruments	MOSFET, N-CH, 30 V, 100 A, SON 5x6mm	SON 5x6mm		
27	R1, R3	2	10k	CRCW060310K0JN1EA	Vishay-Dale	RES, 10 k, 1%, 0.1 W, 0603			0603
28	R2	1	100	CRCW060310R0JN1EA	Vishay-Dale	RES, 100, 5%, 0.1 W, 0603			0603
29	R4, R16, R17	3	3.30k	RG1608P-332-B-T5	Susumu Co Ltd	RES, 3.3 k, 0.1%, 0.1 W, 0603			0603
30	R5, R18	2	0.001	CRE2512-F2-R001E-3	Bourns Inc	RES SMD 0.001 OHM CH 3W 2512	2512		
31	R6, R7, R22, R27, R28, R39, R42, R43, R44	9	100	ERJ-2RFK100X	Panasonic	RES, 100, 1%, 0.1 W, 0402			0402
32	R8	1	5.11	RC060307-075R11L	Yageo America	RES, 5.11, 1%, 0.1 W, 0603			0603
33	R9	1	47.5k	CRCW14047K7KFKED	Vishay-Dale	RES, 47.5 k, 1%, 0.063 W, 0402			0402
34	R10	1	2M	RC060307-072ML	Yageo	RES SMD 2M OHM CH 1% 1/10W 0603			0603
35	R11	1	3.3	CRCW060303K0JN1EA	Vishay-Dale	RES, 3.3, 5%, 0.1 W, 0603			0603
36	R12	1	496k	RC0402P-07496KL	Yageo	RES SMD 496K OHM CH 1% 1/16W 0402			0402
37	R13, R14, R15	3	3.3k	CRCW0402K30JUNED	Vishay-Dale	RES, 3.3 k, 5%, 0.063 W, 0402			0402
38	R16, R21, R32, R36, R37, R38	6	10.0k	ERJ-2RFK100X2	Panasonic	RES, 10.0 k, 1%, 0.1 W, 0402			0402
39	R39	1	0	ERJ-2GE0R00X	Panasonic	RES, 5.0, 0.5%, 0.063 W, 0402			0402
40	R42	1	51.1k	CRCW140251K1FKED	Vishay-Dale	RES, 51.1 k, 1%, 0.063 W, 0402			0402
41	R24	1	78.7k	CRCW140278K7KFKED	Vishay-Dale	RES, 78.7 k, 1%, 0.063 W, 0402			0402
42	R25	1	100k	CRCW140251K1FKED	Yageo	RES SMD 100K OHM CH 1% 1/16W 0402			0402
43	R26	1	100	CRCW1402100RPFKED	Vishay-Dale	RES, 100, 1%, 0.063 W, 0402			0402
44	R40, R45	2	1.00Meg	ERJ-2RFK100X4	Panasonic	RES, 1.0 M, 1%, 0.1 W, 0402			0402
45	U1	1	DRV8305SPSHPR	Texas Instruments	Three Phase Gate Driver With Current Shunt Amplifiers and Voltage Regulator, PH0408G				PH0408G
46	U2	1	MSP430G2553IPW28	Texas Instruments	16 MHz Mixed Signal Microcontroller with 16 KB Flash, 512 B SRAM and 24 GPIOs, -40 to 85 degC, 28-pin SOP (TQFP), Green (RoHS and no SnBr)				PW0028A
47	U3	1	LMT870DKCR01	Texas Instruments	SC710 Analog Temperature Sensor with Class AB Output, DCK0005A				DCK0005A
48	U4, U6, U7, U8	4	TPD1E10B06DPYT	Texas Instruments	ESD Protection in 0402 Package with 10 pF Capacitance and 6 V Breakdown, 1 Channel, 40 V to +125 degC, 2-pin X2SOJ (DPY)				DPY0002A
49	U9	1	SN74LVC126APW	Texas Instruments	Quadbuffer Bus Buffer Gate with 3-State Outputs, PW0014A				PW0014A
50	R41	0	0	ERJ-2GE0R00X	Panasonic	RES, 5.0, 0.5%, 0.063 W, 0402			0402

SBOM (Software BOM)

DEVA-Apps Stage Release Report

Triggered by Web UI (Re-evaluation) on 2023-06-28 12:21:45 UTC+0900

62 **226** **1** **289 VIOLATIONS** Affecting 41 Components **117 COMPONENTS** 99% of all components identified **0 GRANDFATHERED** violations

Aggregate by component View Dependency Tree Filter

THREAT	POLICY	COMPONENT	LAST CHECKED
●	policy name	component name	py3-none-any 1.9.3 (.whl)
● 10	Security-Critical	Django (py2.py3-none-any 1.11.1 (.whl))	>
● 10	Security-Critical	Django 1.11.1 (.tar.gz)	>
● 10	Security-Critical	pycrypto 2.6.1 (.tar.gz)	>
● 10	Security-Critical	virtualenv (py2.py3-none-any 15.1.0 (.whl))	>
● 10	Security-Critical	virtualenv 15.1.0 (.tar.gz)	>

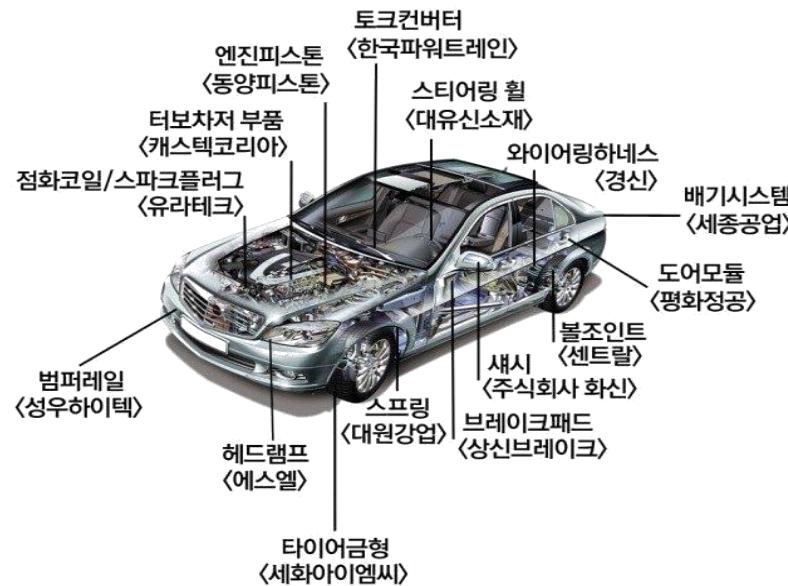
Page Release Report

iQ Server release: 161.0-01

INDEX	COMPONENT	LAST CHECKED
0	bootstrap-datepicker 1.4.1	datepicker 1.4.1
1	coverage (cp26-cp26-macosx_10_12_x86_64 4.5.2 (.whl))	cp26-cp26m-macosx_10_12_x86_64 4.5.2 (.whl)
2	coverage (cp27-cp27-macosx_10_12_x86_64 4.5.2 (.whl))	cp27-cp27m-macosx_10_12_x86_64 4.5.2 (.whl)
3	coverage (cp27-cp27-win32 4.5.2 (.whl))	cp27-cp27m-win32 4.5.2 (.whl)
4	coverage (cp27-cp27-manylinux1_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
5	coverage (cp27-cp27-manylinux1_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
6	coverage (cp27-cp27-manylinux1_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
7	coverage (cp27-cp27-manylinux1_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
8	coverage (cp33-cp33-macosx_10_12_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
9	coverage (cp34-cp34-macosx_10_12_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
10	coverage (cp34-cp34-macosx_10_12_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
11	coverage (cp34-cp34-manylinux1_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
12	coverage (cp34-cp34-win32 4.5.2 (.whl))	cp27-cp27m-win32 4.5.2 (.whl)
13	coverage (cp34-cp34-win32 4.5.2 (.whl))	cp27-cp27m-win32 4.5.2 (.whl)
14	coverage (cp35-cp35-manylinux1_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
15	coverage (cp35-cp35-win32 4.5.2 (.whl))	cp27-cp27m-win32 4.5.2 (.whl)
16	coverage (cp36-cp36-manylinux1_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
17	coverage (cp36-cp36-manylinux1_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
18	coverage (cp36-cp36-manylinux1_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
19	coverage (cp36-cp36-manylinux1_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
20	coverage (cp37-cp37-macosx_10_13_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
21	coverage (cp37-cp37-manylinux1_x86_64 4.5.2 (.whl))	cp27-cp27m-manylinux1_x86_64 4.5.2 (.whl)
22	coverage (cp37-cp37-win32 4.5.2 (.whl))	cp27-cp27m-win32 4.5.2 (.whl)
23	coverage (cp37-cp37-win32 4.5.2 (.whl))	cp27-cp27m-win32 4.5.2 (.whl)
24	coverage (win-amd64-py2 7.4.5.2 (.exe))	cp27-cp27m-win32 4.5.2 (.whl)
25	coverage (win-amd64-py2 7.4.5.2 (.exe))	cp27-cp27m-win32 4.5.2 (.whl)
26	coverage (win-amd64-py3 4.5.2 (.exe))	cp27-cp27m-win32 4.5.2 (.whl)
27	coverage (win-amd64-py3 4.5.2 (.exe))	cp27-cp27m-win32 4.5.2 (.whl)
28	coverage (win32-py2 7.4.5.2 (.exe))	cp27-cp27m-win32 4.5.2 (.whl)
29	coverage (win32-py3 4.5.2 (.exe))	cp27-cp27m-win32 4.5.2 (.whl)
30	coverage (win32-py3 4.5.2 (.exe))	cp27-cp27m-win32 4.5.2 (.whl)
31	coverage (win32-py3 7.4.5.2 (.exe))	cp27-cp27m-win32 4.5.2 (.whl)
32	coverage (win32-py3 7.4.5.2 (.exe))	cp27-cp27m-win32 4.5.2 (.whl)
33	django-constance 0.0.1 (.tar.gz)	cp27-cp27m-win32 4.5.2 (.whl)
34	Django (py2.py3-none-any 1.11.1 (.whl))	cp27-cp27m-win32 4.5.2 (.whl)
35	Django 1.11.1 (.tar.gz)	cp27-cp27m-win32 4.5.2 (.whl)
36	enum34 (py3-none-any 1.6.6 (.whl))	cp27-cp27m-win32 4.5.2 (.whl)
37	enum34 (py3-none-any 1.6.6 (.whl))	cp27-cp27m-win32 4.5.2 (.whl)

Supply Chain & SDLC (Software Development Lifecycle)

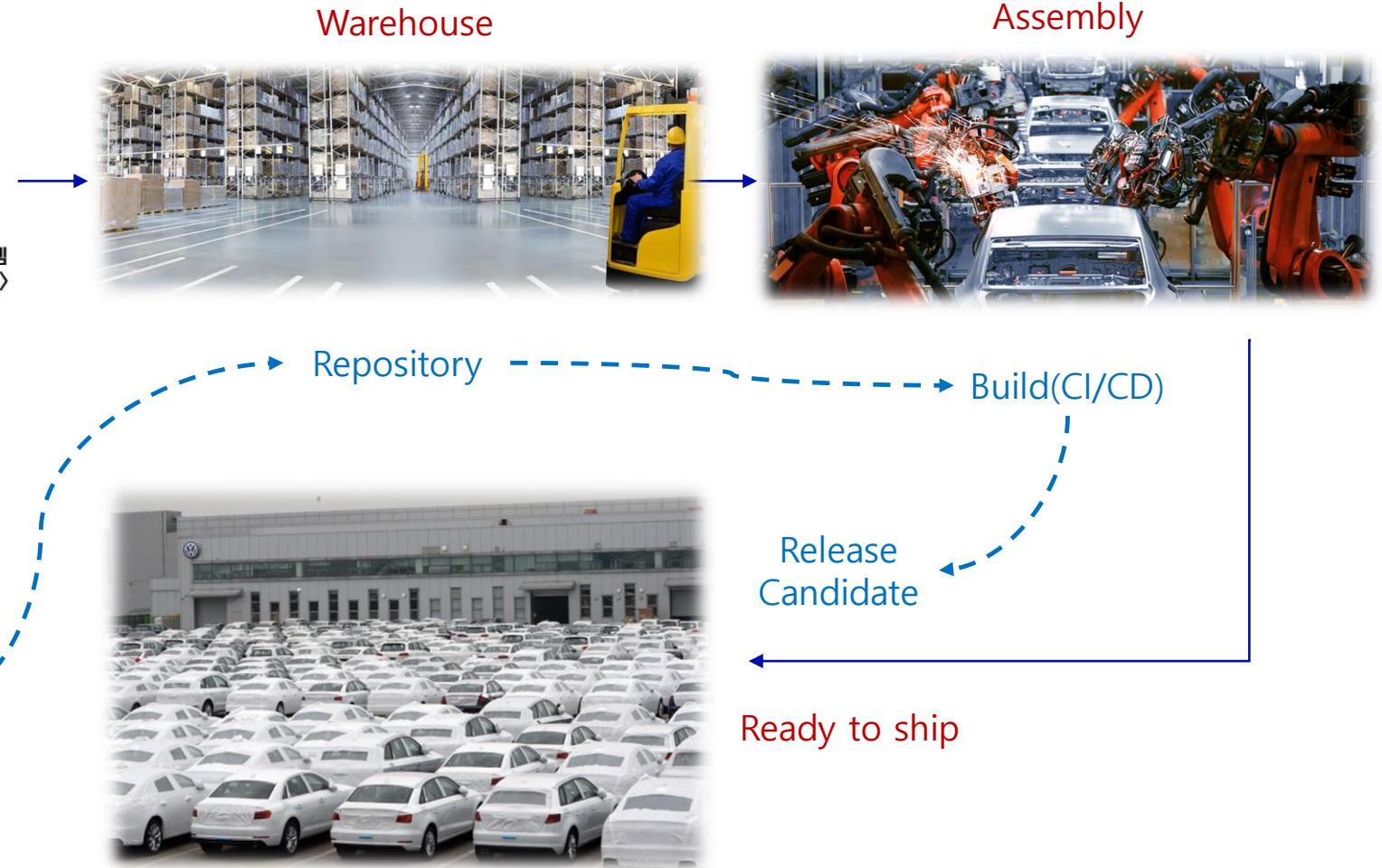
- 공급망 & 자재저장소



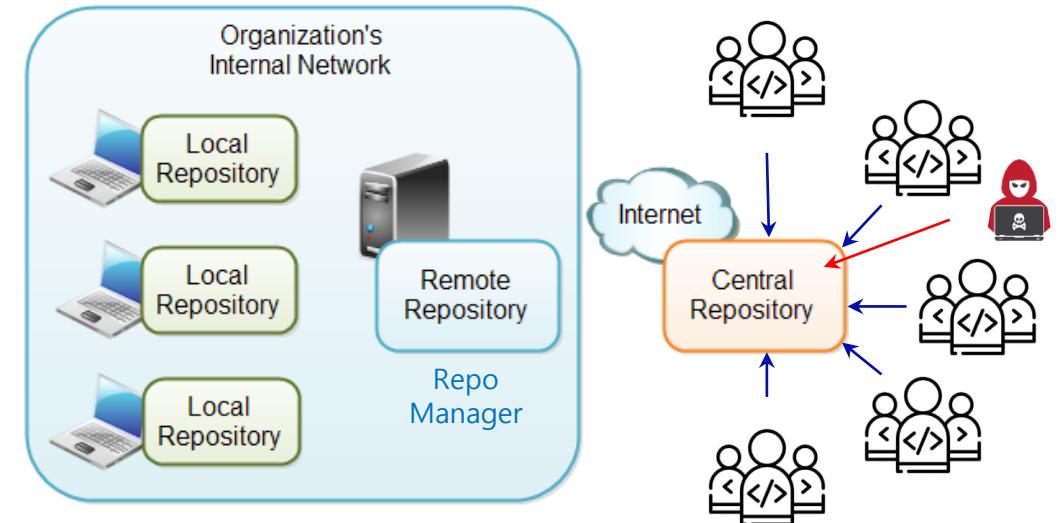
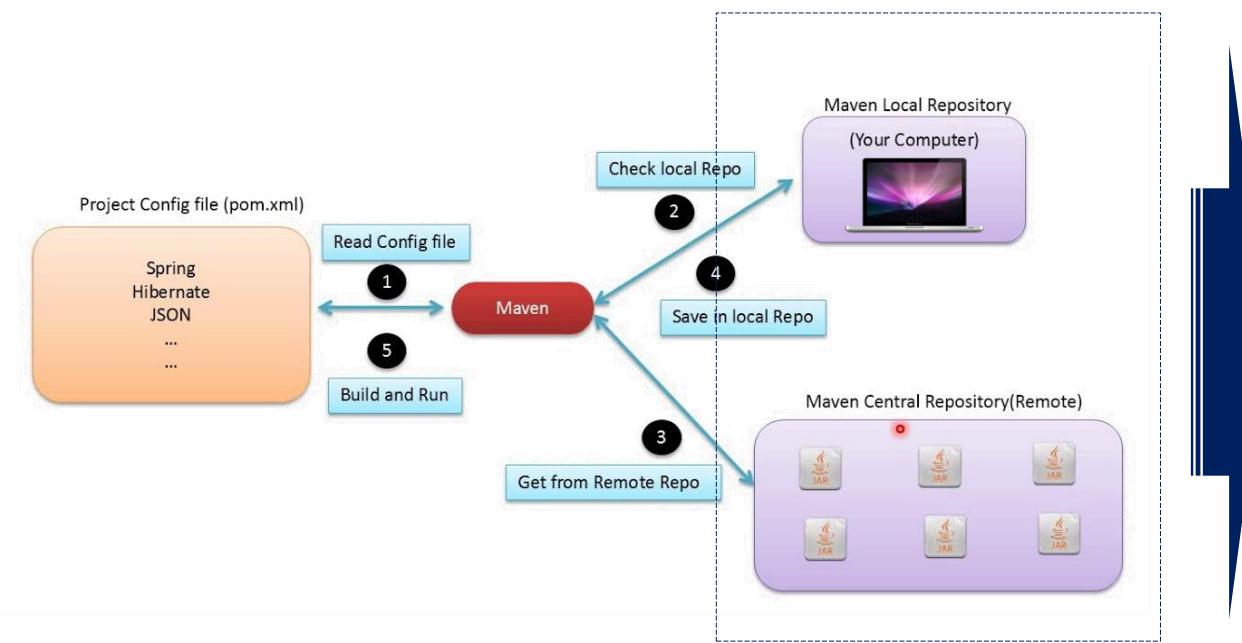
600여 1/2차 협력사
공급망



Public
Repository



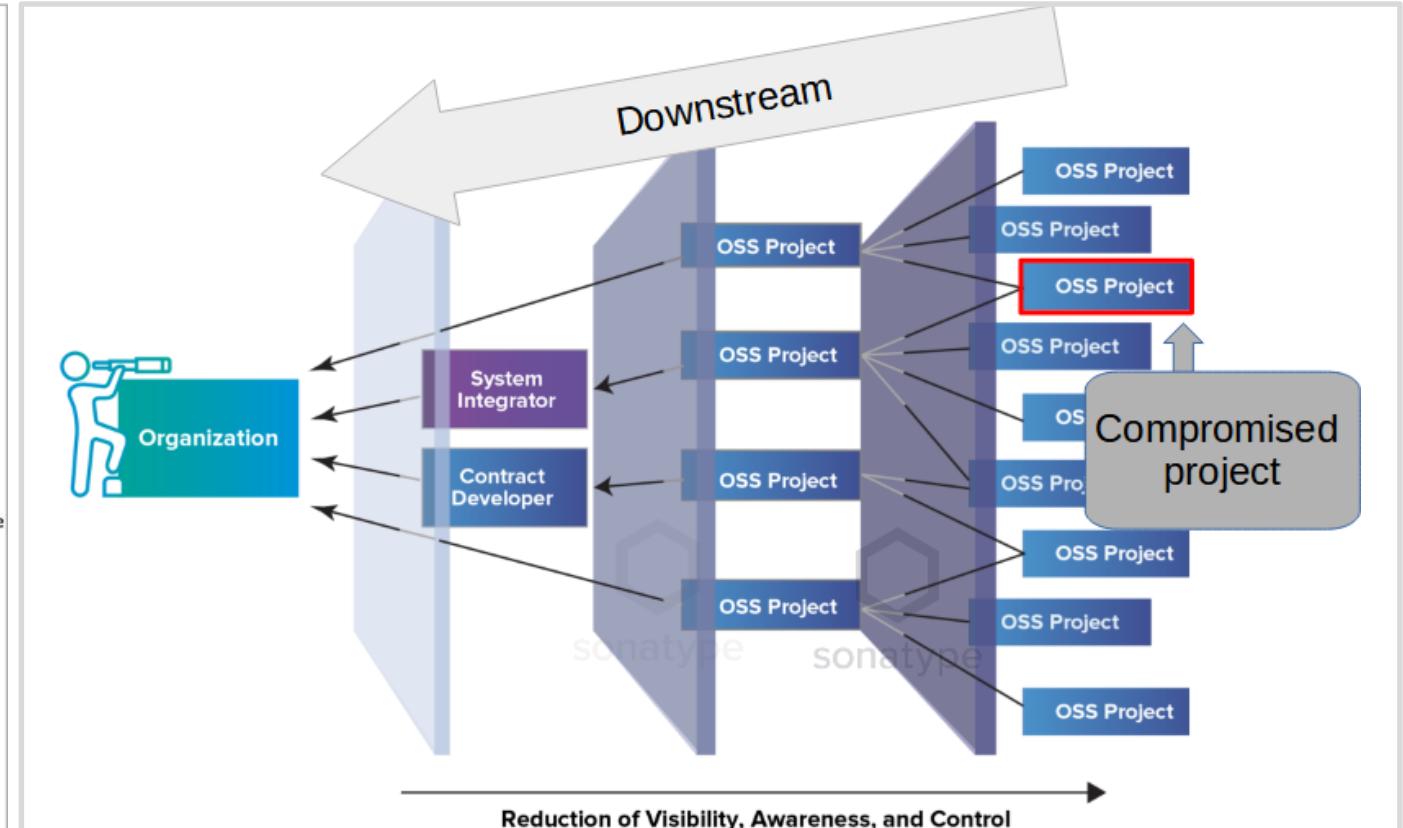
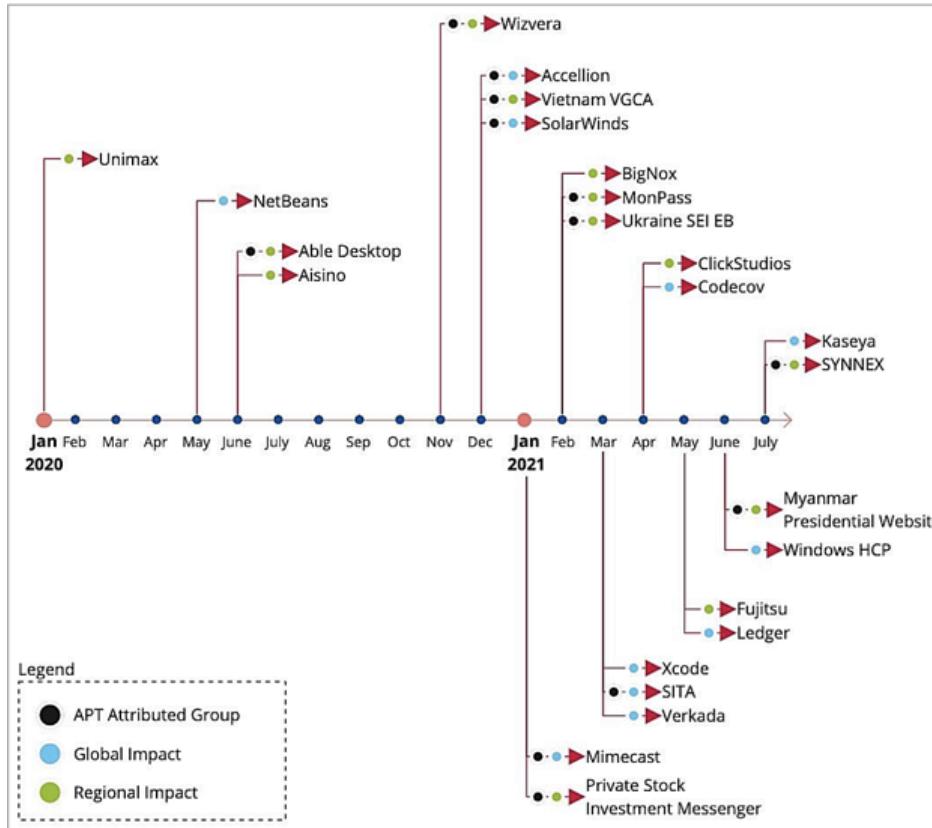
Public Repository & Remote Repository (Repo Manager)



- ❖ Repository Manager가 필요한 이유
 - 외부 저장소에 (Public Repository) 대한 Proxy/Cache 용도
 - 보안상의 이유로 개발자가 외부 네트워크에 접속하지 못하는 경우에도 필요한 Library를 사용하게 함
 - 내부에만 사용되는 공통 Library를 Hosting 하기 위한 저장소 용도

Supply Chain Attack

ENISA Report



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

SCA (Software Composition Analysis)

어플리케이션을 구성하는 오픈소스 구성요소(Component)를 자동으로 식별하고 SBOM(Software BOM)을 구성하여 잠재적인 위협요소(취약점, 라이선스, 품질 등)를 파악하는 절차로, Dependency 및 Transitive Dependency를 정확하게 추적해야 함

❖ 식별방식

- **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 Platform은

Manifest Scanning과 Binary Scanning을 모두 사용하여
보다 정확한 분석결과를 도출함

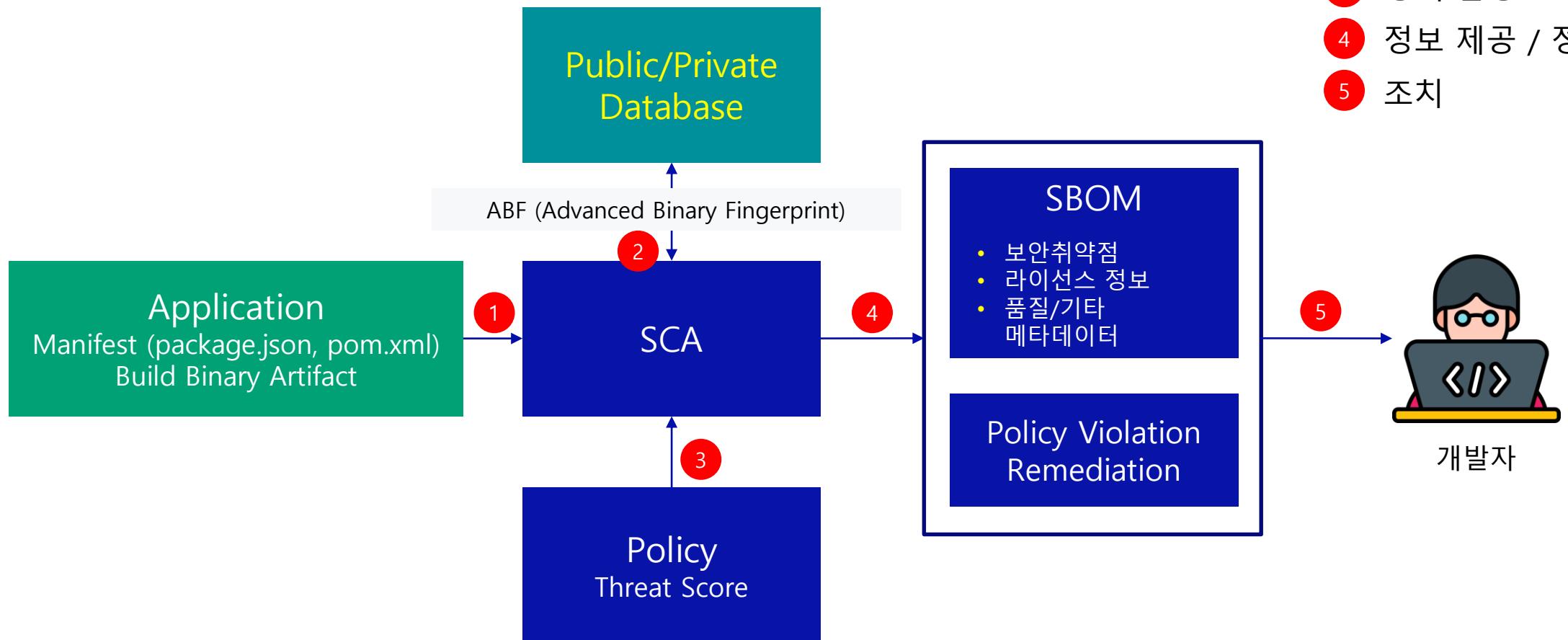


<http://npm.anvaka.com/#/view/2d/log4j>

How SCA Works

Manifest 파일과 Binary Artifact 분석을 통해 식별된 구성요소(Component)에 대한
Binary Fingerprint는 데이터베이스로 전달되어 관련된 보안정보, 라이선스 정보를 확인합니다.

- 1 Component 식별
- 2 Database 비교
- 3 정책 반영
- 4 정보 제공 / 정책 적용
- 5 조치



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

Icons of a laptop with a skull, a worm, and a virus are visible on the right side of the slide.

Dependency Confusion

A diagram illustrating dependency confusion. It features a large question mark on the left, followed by two crossed arrows (one red, one green) pointing towards a skull-and-crossbones icon on the right. Below the arrows, the text "Dependency Confusion" is written in a serif font.

TYPOSQUATTING

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
facebook.com
- DOUBLING CHARACTERS
twiitter.com
- USING SIMILAR LOOKING CHARACTERS
google.com (i vs l)
costko.com
- PRESSING A WRONG KEY
costko.com

Icons of a browser and a smartphone are at the bottom of the slide.

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

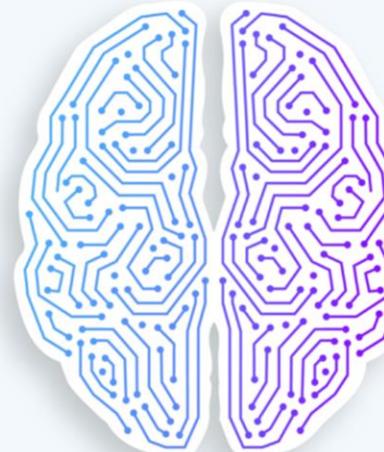
The difference is simple.

Better Identification

Declared가 아닌
Deployed 기반 스캔

파일명이 아닌 Advanced
Binary Fingerprint 사용

False Alarm에 따른
리소스 낭비 최소화



Better Knowledge

공개데이터 외에
오픈소스 취약성 정보 수집

새로운 취약성 정보를
빠르게 수집

개발자에게 실행 가능한
가이드 제공

+121M 컴포넌트 분석



Central
Repository



Sonatype
Research



National
Vulnerability
Database



Github



OSS
Index



Nexus
Repository



Google
Search Alerts



Security
Advisories

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

<https://dev.sonatype.com/>

The screenshot shows the Sonatype DevZone homepage. It features a dark blue header with the Sonatype logo and navigation links for Products, Solutions, Pricing, Resources, Company, and a pink 'BOOK A DEMO' button. Below the header is a teal banner with the text '\$: DevZone | Life is hard. Dependencies don't have to be.' and a subtext 'Breaking news, security deep dives, developer culture and coffee from the stewards of Maven Central.' The main content area has three cards: 'This Week in Malware - Almost 100 Packages' (image of a person holding a tablet with a skull icon), 'Rule Over Your Dependencies and Scan at Your Own Open Source Risk' (image of a network graph with nodes), and 'This Week in Malware—Ongoing Dependency Confusion' (image of a computer monitor with a skull icon). To the right, there's a summary box with the text '88,217 Malicious Packages Discovered' and '16,073 Malicious Packages Taken Down', both with small subtext 'Last Updated: Sep 9, 2022'. A red dashed circle highlights these statistics.

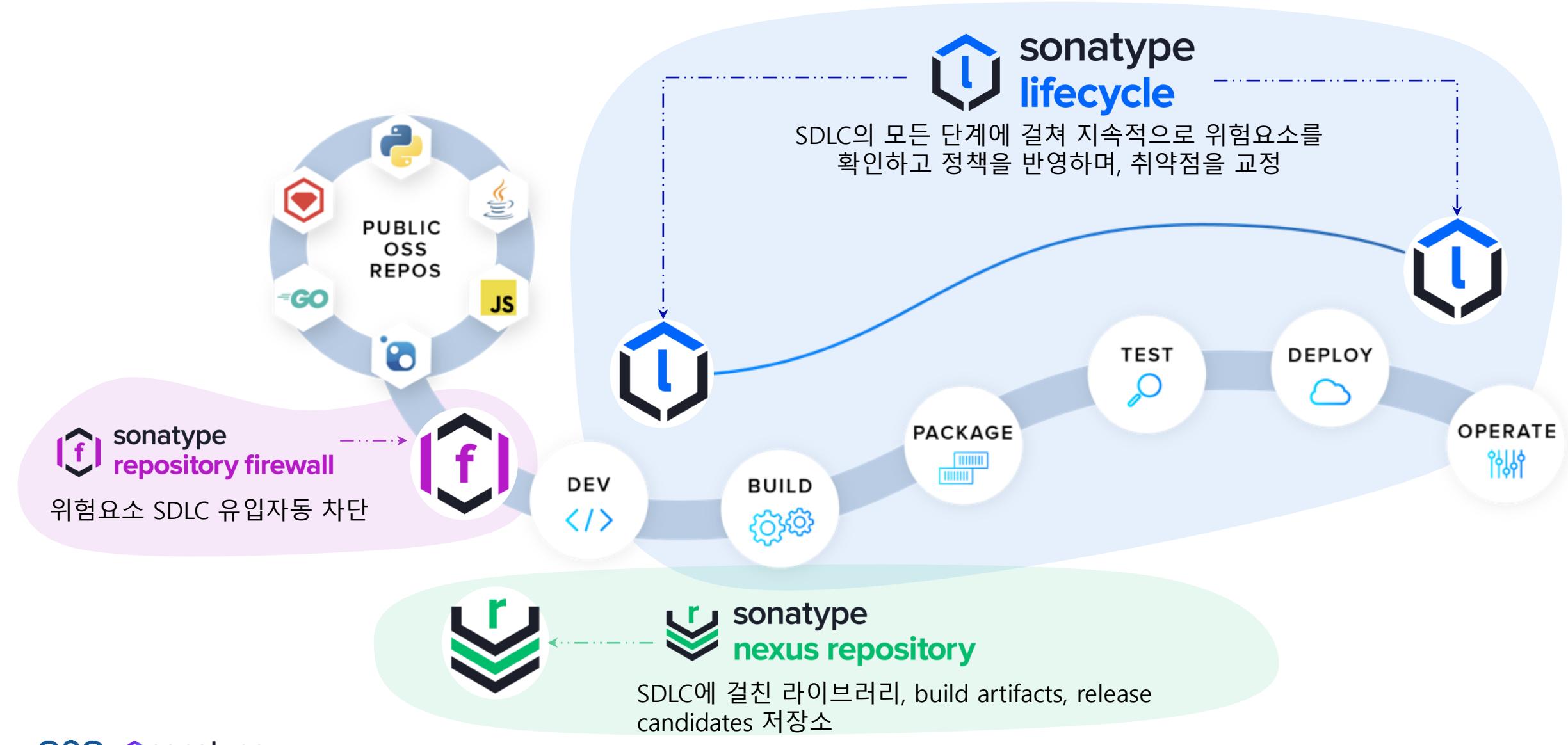
- Advisory 출처 : Sonatype 또는 NVD
- 이슈 심각도 : CVSS 스코어, 출처 및 버전
- CWE (Common Weakness Enumeration)
- Advisory 의 Risk에 대한 세부 추가 설명
- 취약 여부 판단방법
- 수정 및 우회 안(Workaround)에 대한 권고
- 근본 원인 (root cause) : 코드내 취약한 버전 및 클래스
- 공개된 공격요소 및 취약점에 대한 추가 정보

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

The screenshot shows the Sonatype vulnerability timeline page. At the top, it says 'OPEN SOURCE COMPONENTS ANALYZED BY NEXUS INTELLIGENCE:' with a grid of numbers: 1, 2, 1, 9, 0, 0, 9, 4, 6. Below this is a section titled 'A History of Software Supply Chain Attacks' with the subtitle 'July 2017–Present'. The page is divided into three main sections by month:

- AUGUST 2022:** PyPI Package 'secretst0f' Drops Linux Malware to Mine Monero. Malicious secretst0f Python package drops second-stage payload in-memory to silently run XMRig and mine Monero. 'Requests' Library Typosquats Install Requests. We identified and analyzed multiple malicious Python packages that contain ransomware scripts and are typosquats of a legitimate, widely known library called 'Requests'.
- JULY 2022:** PyPI Packages Steal Telegram Cache Files, Add Windows Remote Desktop Accounts. Sonatype discovered malicious PyPI packages that set up new Remote Desktop user accounts on your Windows computer and steal encrypted Telegram cache files from your Telegram Desktop client. A Python Cryptominer Targeting Windows, Linux, macOS. We identified a suspicious PyPI component called 'python-cryptominer' that mines Monero (XMR) cryptocurrency on your system—whether Windows, Linux, or macOS, and steals AWS credentials.
- JUNE 2022:** npm Malware Exfiltrates Windows SAM, Amazon EC2 Credentials. Sonatype security researchers analyzed npm packages '@core-plus/cyo-core' and 'nodejs-eapkg@0.1.0' that attempt to exfiltrate Amazon EC2 credentials as well as sensitive files such as /etc/passwd on Linux, and SAM SYSTEM on Windows.

Sonatype Platform





sonatype platform

단일 플랫폼을 통해
어플리케이션을
시장에 빠르게 출시



- 빠르게 최고의 컴포넌트를 찾아내 재작업 시간을 단축하여 기술부채 감소
- 기사용중인 툴(IDEs and SCM)에서 정확한 인텔리전스를 통해 오픈소스 정책 위반사항을 교정
- 의존성 관리 자동화

- 기업환경을 위한 유연한 정책엔진
- 유해 컴포넌트 차단을 위한 오픈소스 방화벽
- 악성 행위 탐지를 위한 리스크 스코어 (Risk score)
- 세부적인 보안 리서치 : 65 연구원, 96M 컴포넌트, 14M 취약점, 수 백여개 데이터 소스, AI/ML

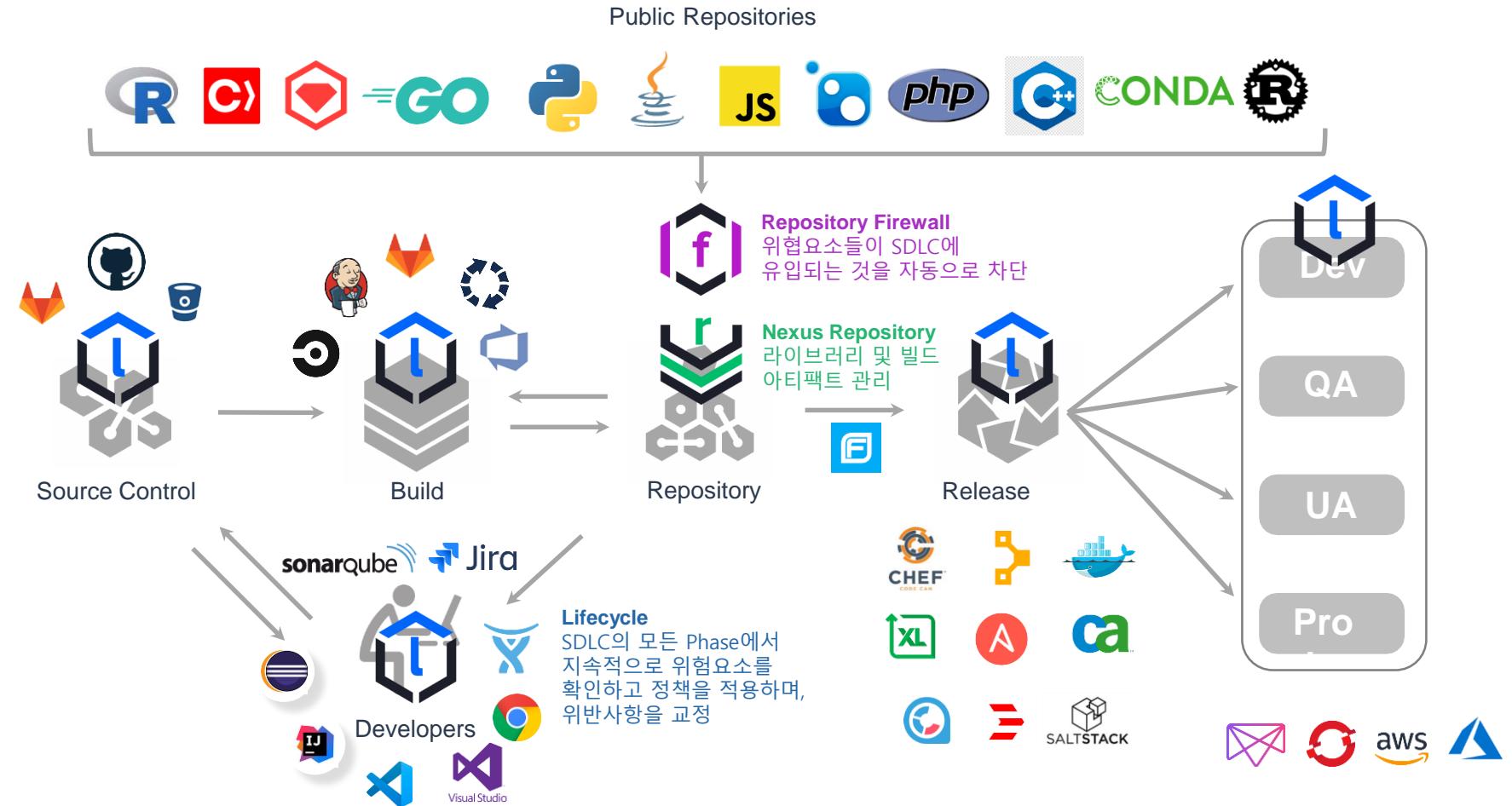
- 바이너리 리포지토리(저장소)를 통해 안정적인 빌드 제공
- Production/Legacy 어플리케이션을 위한 SBOM 생성
- 새로운 위협요소에 대해 지속적인 모니터링

- 라이선스 의무사항(Obligation) 및 권리귀속(Attribution)에 대한 명확한 시각 제공
- 라이선스 검토 자동화를 위한 법적 워크플로우

사전 정합

현업에서 사용하는
대부분의 툴을
Out-of-Box로 지원

Nexus Platform은 현업에서 사용하는 DevOps 툴에 사전 통합되어
별도의 정합작업 없이 즉시 사용할 수 있습니다.



자원 언어 및 패키지

다양한 언어 및
패키지 지원

LANGUAGE	sonatype repository firewall	sonatype lifecycle	sonatypelift
C, C++	●	(Conan)	●
C#	●	●	
Clojure	●	●	
CoffeeScript	●	●	
F#	●	●	
GO	●	●	●
Gosu	●	●	
Groovy	●	●	
Haskell			●
Java	●	●	●
JavaScript	●	●	●
Kotlin	●	●	●
Markdown			●
PHP	●	●	
Python	●	●	●
ObjectiveC	●	●	
R	●	●	
Ruby	●	●	●
Rust	●	●	●
Scala	●	●	
Scala.js	●	●	
Swift	●	(CocoaPods)	
Visual Basic	●	●	
Yum (RPM)	●	(SPEL)	

PACKAGE	sonatype nexus repository	sonatype repository firewall	sonatype lifecycle
APK (Alpine)	via Community	●	●
apt-gpg APT (Debian)	●	●	●
Bower	●	●	
Cargo		●	●
CocoaPods	●	●	●
Composer	via Community	●	●
CONAN	●	●	●
Conda	●	●	●
CPAN CPAN	via Community	●	
Docker	●		●
Drupal		●	●
ELPA	via Community	●	
Go Modules	●	●	●
Gradle	●	●	via Community
HELM Helm Charts	●		
Maven	(Maven2)	●	●
npm	●	●	●
NuGet	●	●	●
OBR	●		
P2	●		
PyPI	●	●	●
RubyGems	●	●	●
R	●	●	●
yum Yum (RPM)	●	●	●

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

주요 고객사

2,000여 고객사(1,500
만 개발자)를 통해
검증된 솔루션

Fin Serv



Technology



Media



Manufacturing



Energy



Software Composition Analysis (SCA)

Forrester Report Q2 2023

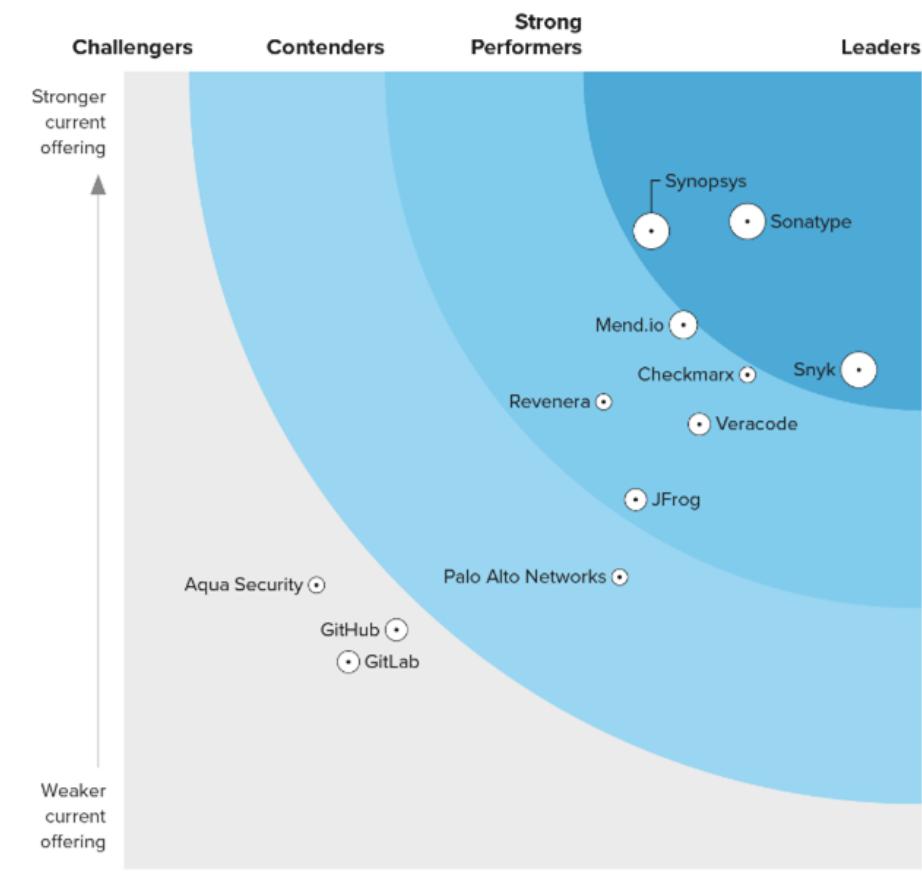
	Forrester's weighting	Aqua Security	Checkmarx	Github	GitLab	JFrog	Mend	Palo Alto Networks	Reverena	Snyk	Sonatype	Synopsys	Veracode
Current offering	50%	1.78	3.10	1.50	1.30	2.32	3.41	1.83	2.93	3.13	4.06	4.00	2.79
Vulnerability identification	15%	1.60	3.00	1.60	1.60	3.00	3.00	1.00	3.00	1.60	5.00	3.60	3.60
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

Forrester Wave™: Software Composition Analysis, Q2 2023

THE FORRESTER WAVE™

Software Composition Analysis

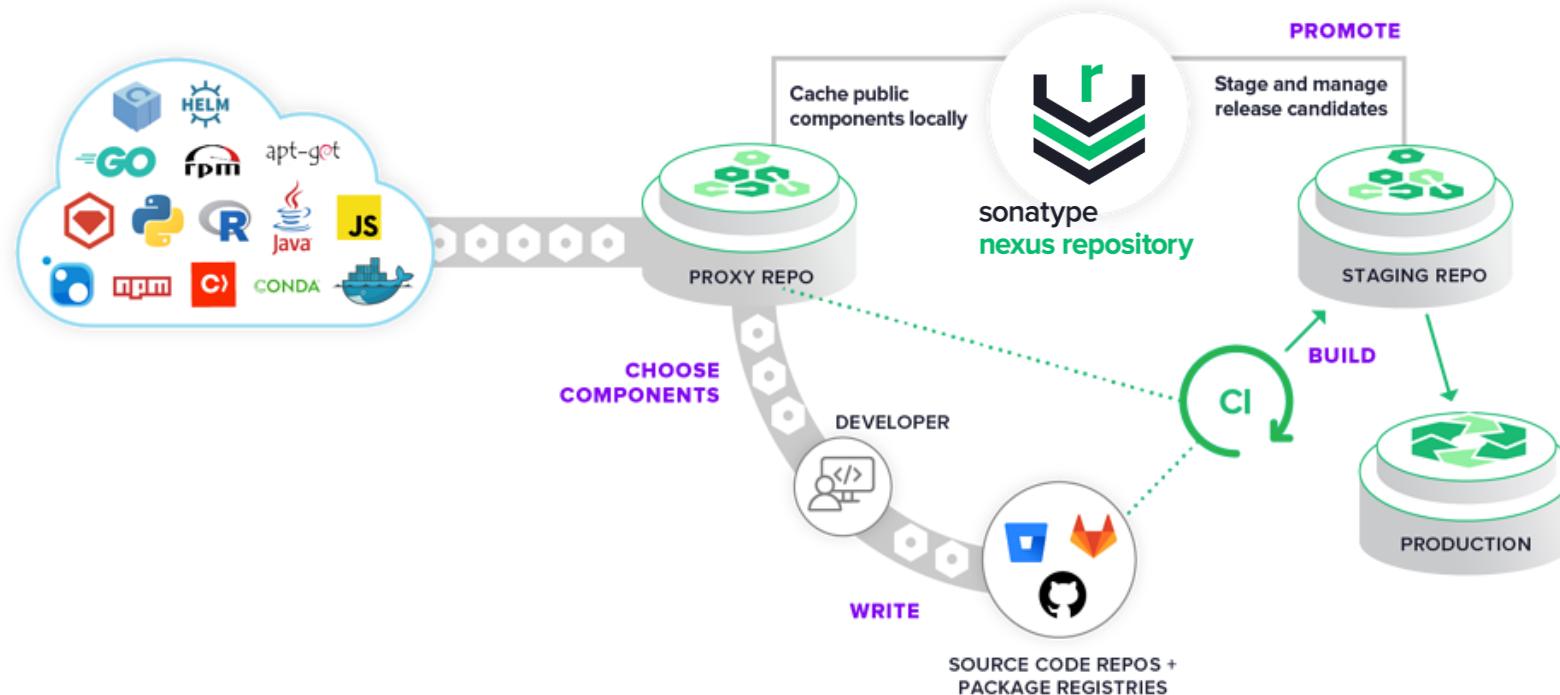
Q2 2023



Market presence
• ○ ○ ●



전 세계 100,000개 조직에서 사용중인 사설 리포지토리(저장소)로
컴포넌트, 라이브러리, 바이너리, 빌드 아티팩트 등을 관리



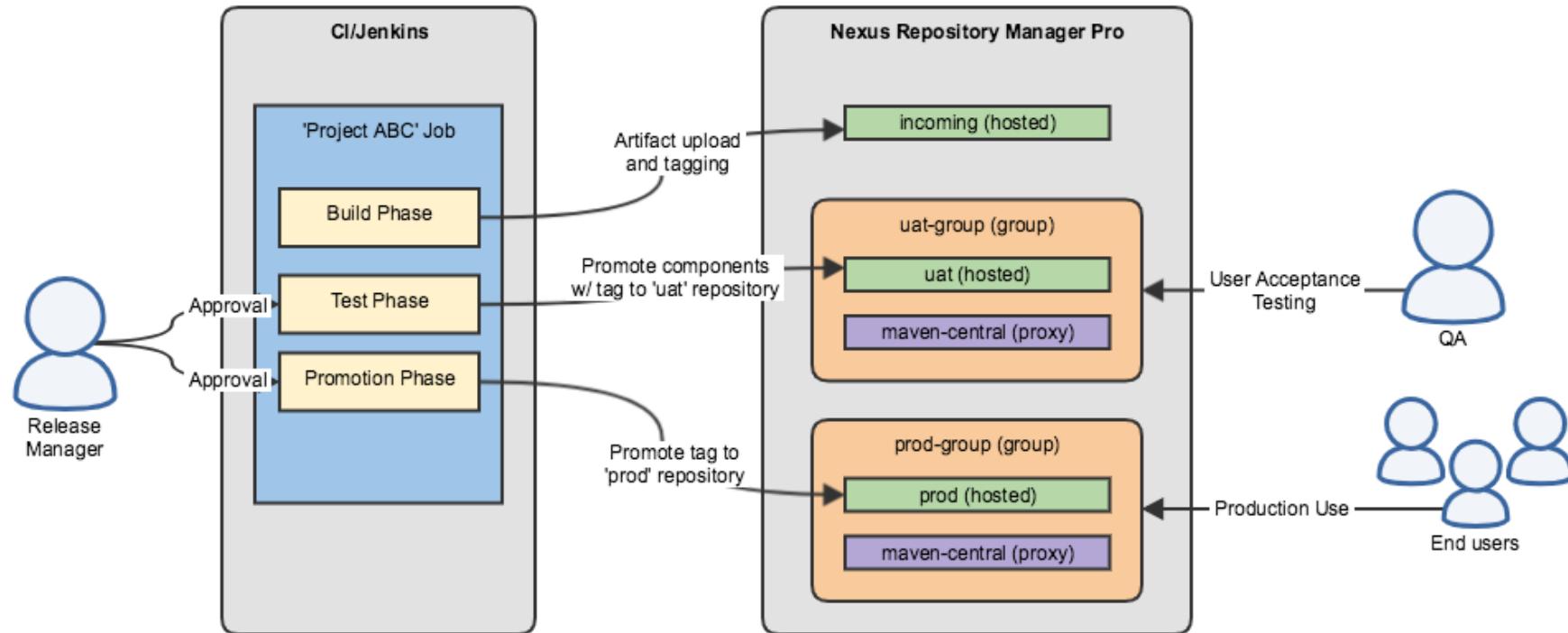


주요 기능 (Nexus Repository OSS 대비)

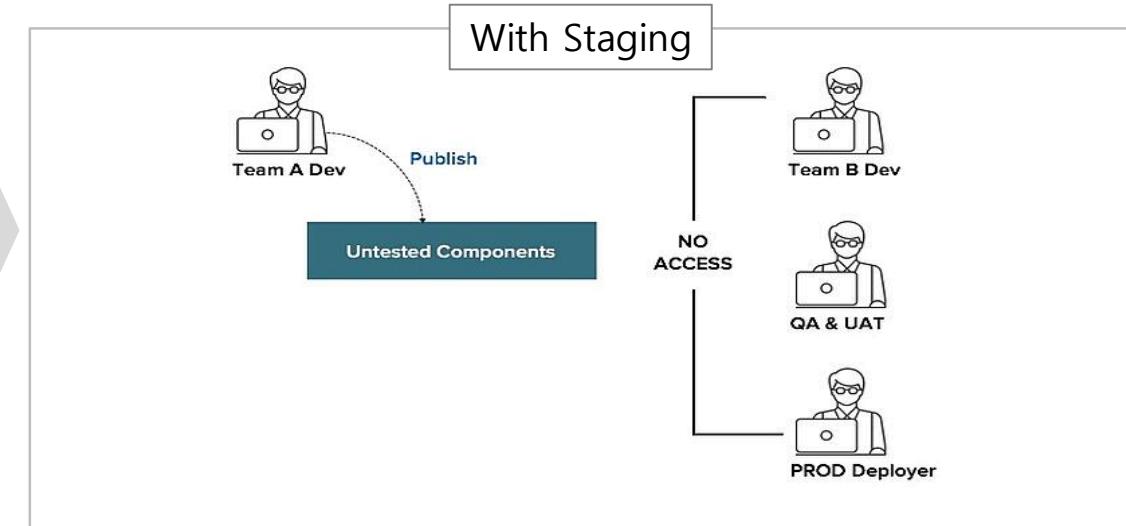
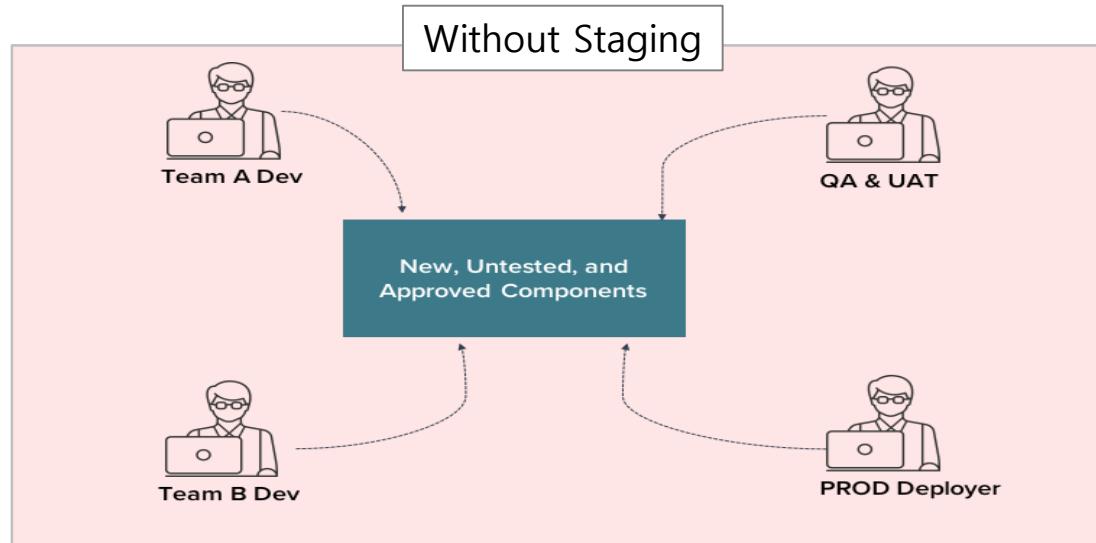
 Import/ Export	<ul style="list-style-type: none"> Repository간 컴포넌트 이동 Disconnected 망 환경 지원 	 고급 Blob Store 관리	<ul style="list-style-type: none"> 복수의 Blob Store (Group Blob Stores)를 단일 Blob Store로 활용 Dynamic Storage 	 User Token	<ul style="list-style-type: none"> Username/Password 대신 토큰을 사용하여 빌드 시스템 접근 지원 LDAP등 SSO 솔루션에 활용
 Tagging	<ul style="list-style-type: none"> 컴포넌트의 조합을 논리적으로 묶어 관리 – CI Build ID, Release Train 등 	 Group Deployment	<ul style="list-style-type: none"> Pull/Push 컨텐츠에 단일 URL 사용 	 기술 지원	<ul style="list-style-type: none"> Standard/Extended 기술지원 장애 대응 및 자문/코칭 서비스
 외부 Database	<ul style="list-style-type: none"> 내장 DB(OrientDB)외에 외부 PostgreSQL 지원 성능 및 안정성, 관리기능 향상 	 Staging & Build Promotion	<ul style="list-style-type: none"> Staging Repository 구분을 통해 DEV/UAT/PRD등 접근제어 	 SAML SSO	<ul style="list-style-type: none"> SAML IdP 연동을 통해 인증/인가 통합 지원
 Health Check	<ul style="list-style-type: none"> 오픈소스 보안 취약점 및 라이선스 정보 제공 	 HA & Backup	<ul style="list-style-type: none"> HA, 백업/복구 등 Resilient 아키텍처 구성 지원 	 Crowd SSO 인증	<ul style="list-style-type: none"> Atlassian Crowd를 통한 SSO 인증 지원

전형적인 Staging Workflow

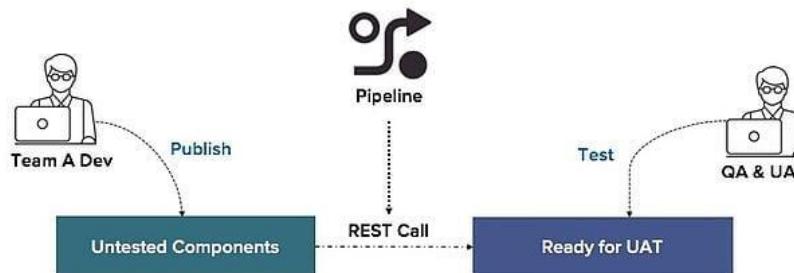
- Nexus Repository Pro의 Staging 기능은 소프트웨어 개발 라이프사이클 단계에 맞도록 소프트웨어 컴포넌트에 대한 프로모션을 지원
- 격리된 Release Candidates를 생성하여 기준에 따라 컴포넌트에 대한 단계를 격상하거나 개발단으로 되돌릴 수 있음



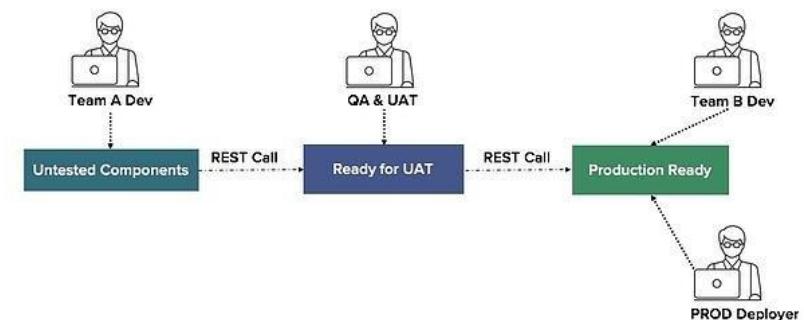
Staged Workflow (Staging and Tagging)



최초 Publish 단계에서 Tagging을 사용하여 Pipeline (e.g. Jenkins)에서 단일 REST Call을 통해 컴포넌트 이동

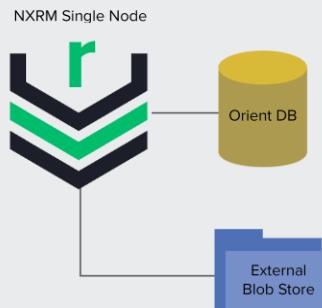


Release Manager는 단계별 승인과정을 통해 Pipeline에 필요한 접근권한을 통제

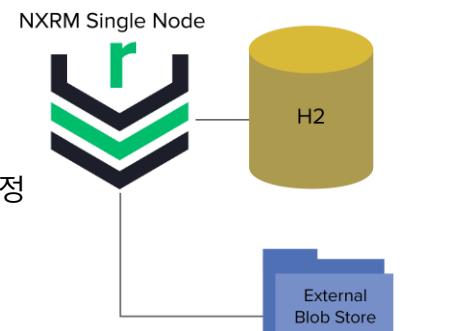


External Database 사용 지원

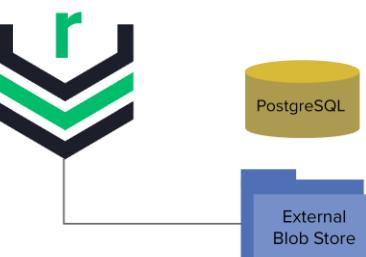
기본 구성 : 내장 DB(OrientDB)에 컴포넌트
메타데이터 및 Configuration 저장



OrientDB는 H2로 대체 예정



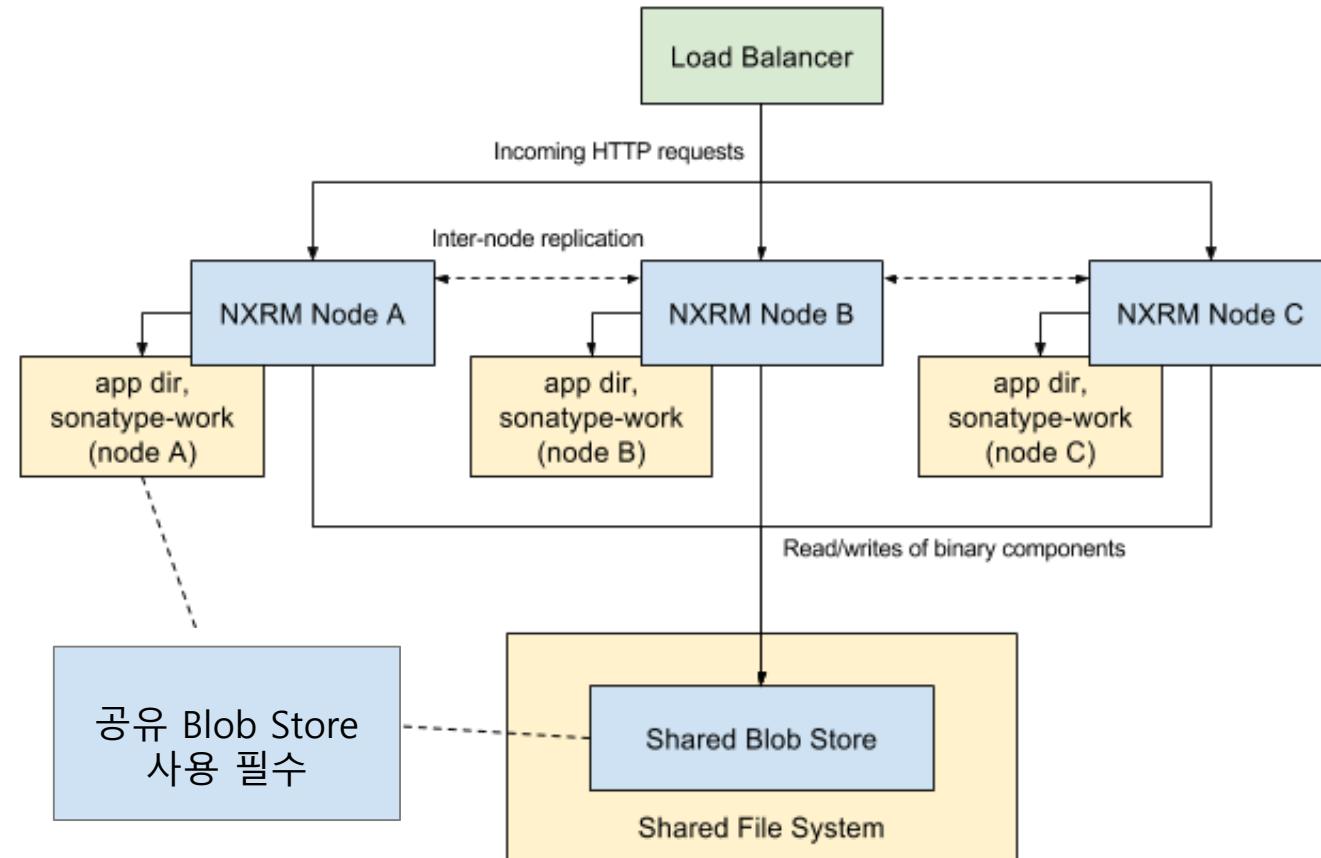
NXRM Single Node



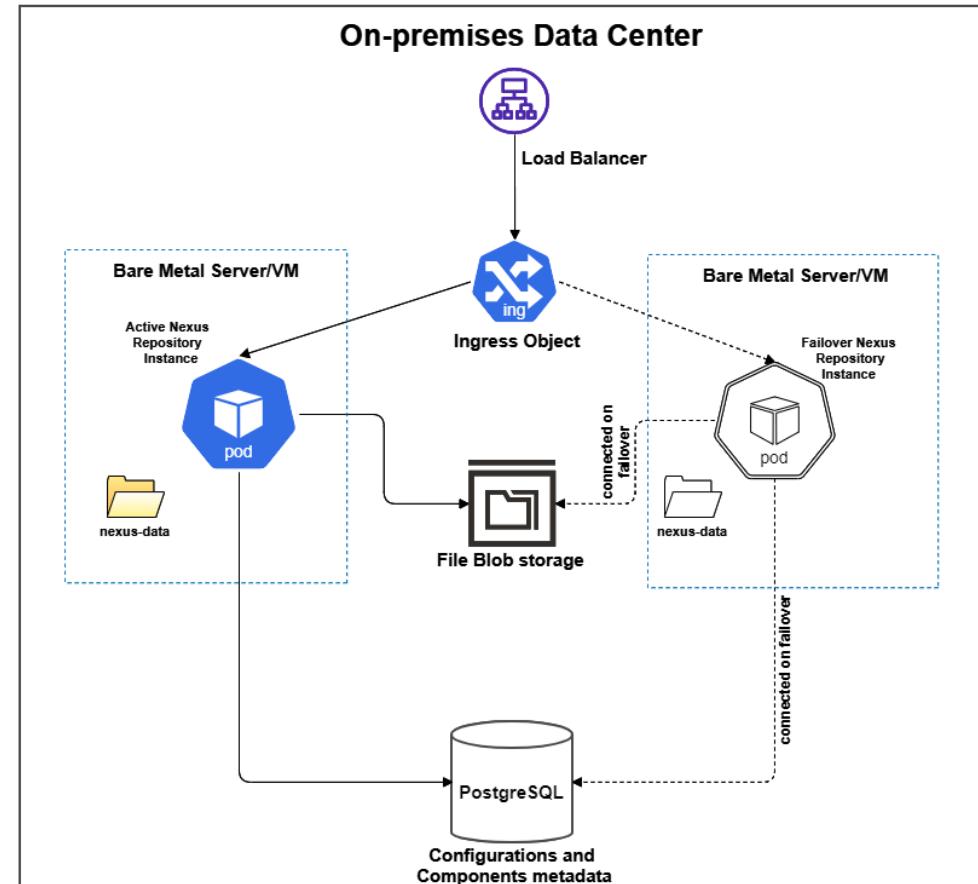
외부 PostgreSQL 대체 사용

- 성능 및 확장성 향상
- AWS Aurora, RDS 및 Azure Database 등 관리형 데이터베이스 사용 가능
- K8s/Rancher/OpenShift등 컨테이너 오케스트레이션 도구 호환성 향상
- 백업과정의 가용성 지원
- 다중 가용영역 (Availability Zone) 환경의 결합 허용(Fault-tolerant) 향상
- DR 프로세스 단순화

Resiliency 및 HA 구성 지원 (Legacy)



Resiliency 및 HA 구성 지원 (On-Prem using Kubernetes)



Nexus Repository oss (오픈소스)는 취약점이나 라이선스에 대한
요약정보만 제공하며 Nexus Repository Pro는 세부정보를 추가 제공함

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	License Warnings
Critical (7-10) 780	Copyleft 154
Severe (4-6) 434	Non Standard 228
Moderate (1-3) 12	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?

[View Detailed Report](#)

Get Nexus Firewall

Benefits

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

[Learn More](#)

Nexus Repository OSS

Nexus
Repository
Pro

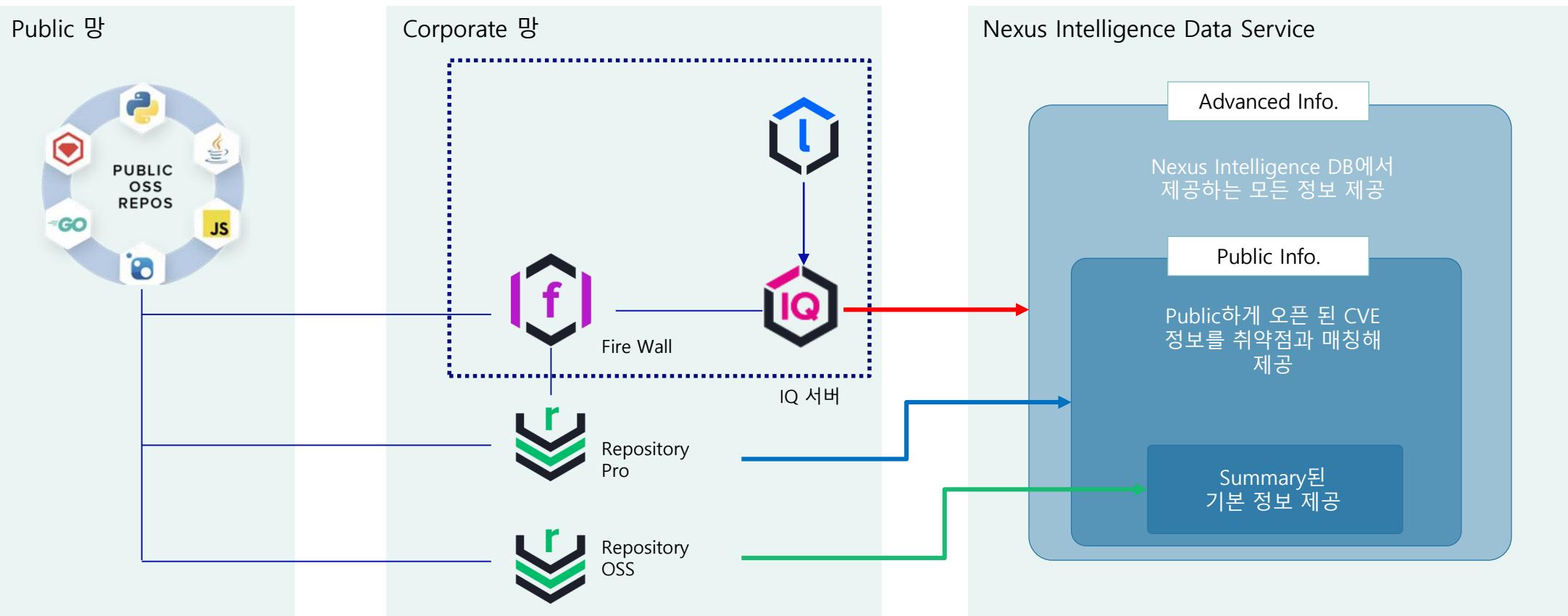
View By: Artifacts

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	jaxws.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	jaxws.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-i	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

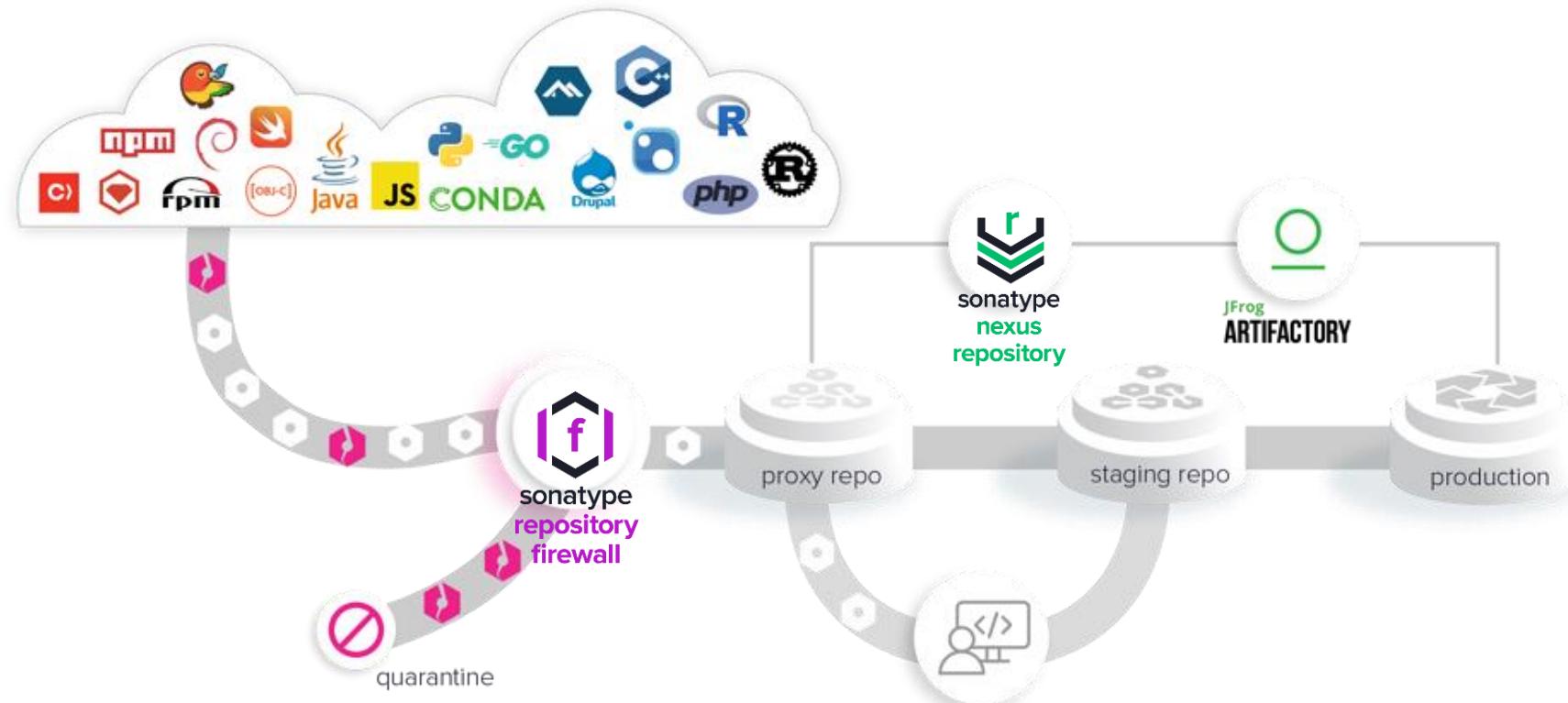
View By: Vulnerabilities

Threat Level	Problem Code	Group	Artifact	Version
7	CVE-2010-2076	org.apache.cxf	cxfr-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	cxfr-common-utilities	2.2
	osvdb-24363	struts	struts	1.1-rc1
	osvdb-67294	org.apache.cxf	cxfr-common-utilities	2.2.4
	CVE-2011-3190	org.open.rules	org.open.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	cxfr-common-utilities	2.1.2
	CVE-2010-2076	org.apache.cxf	cxfr-common-utilities	2.2

Sonatype 제품의 단계별 취약점 정보 제공



Repository Firewall은 취약한 컴포넌트가 SDLC내로 유입되는 것을 차단

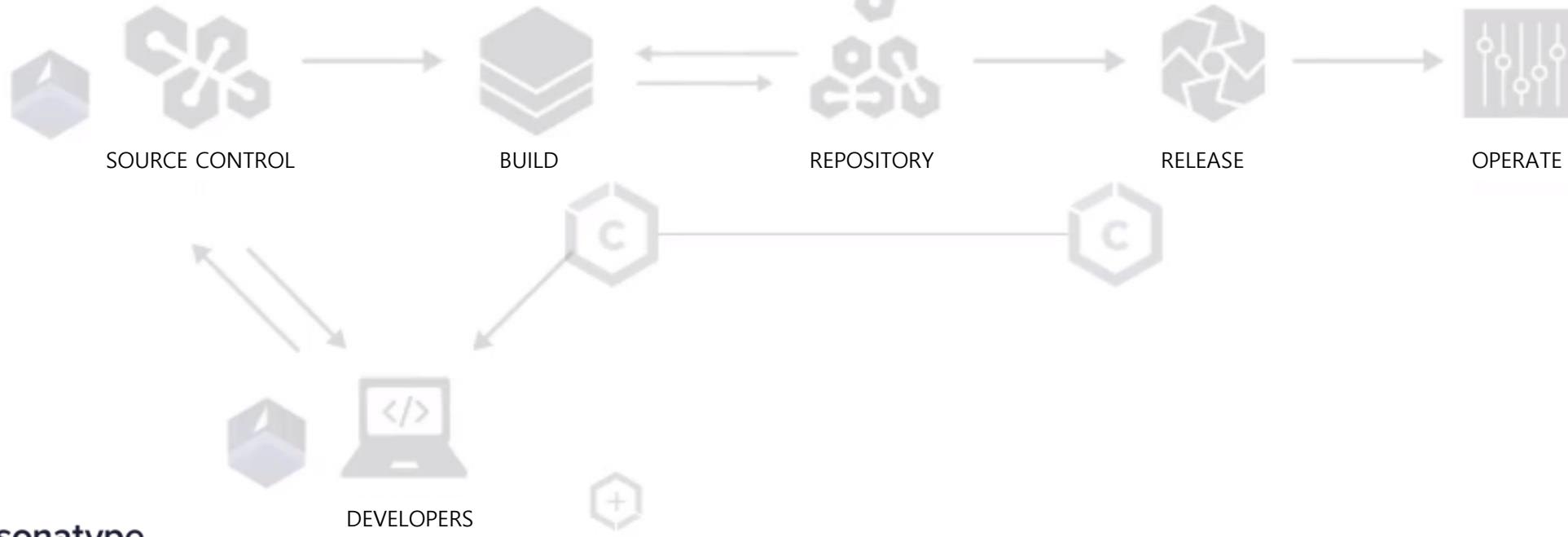
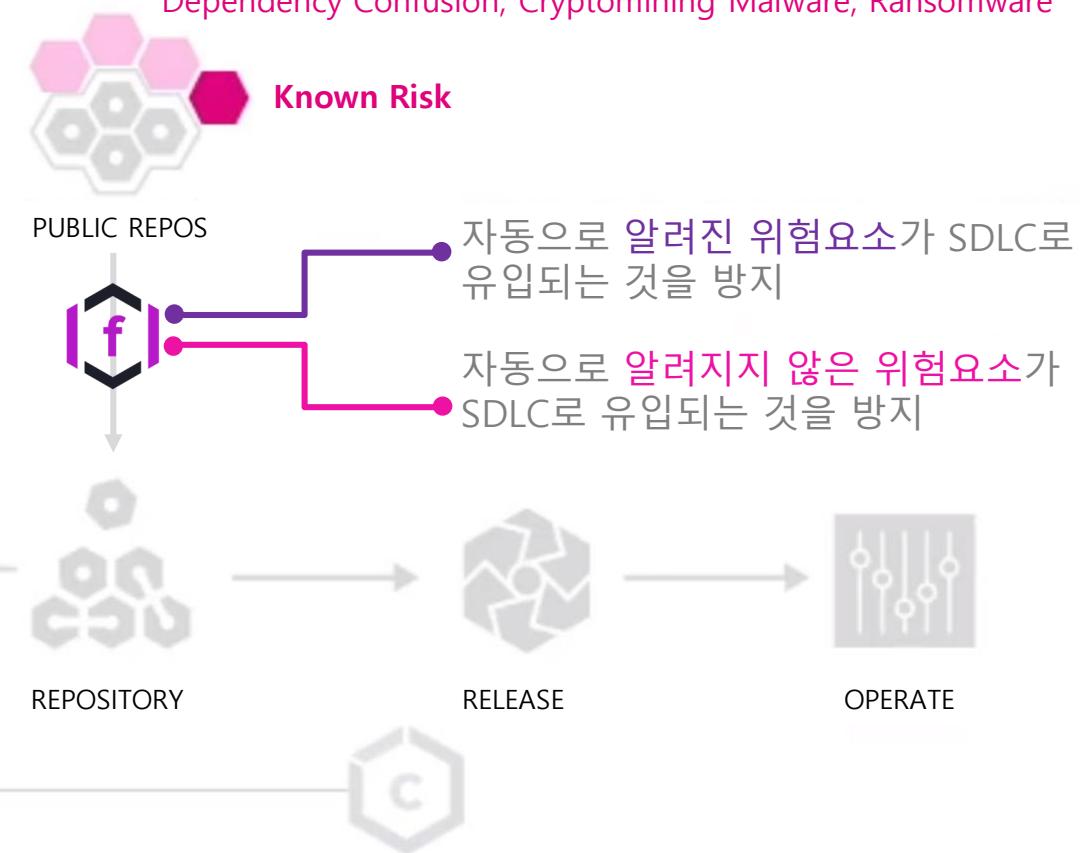


Java, JavaScript, .NET, Python, Go, Ruby, RPM등 다양한 언어 지원

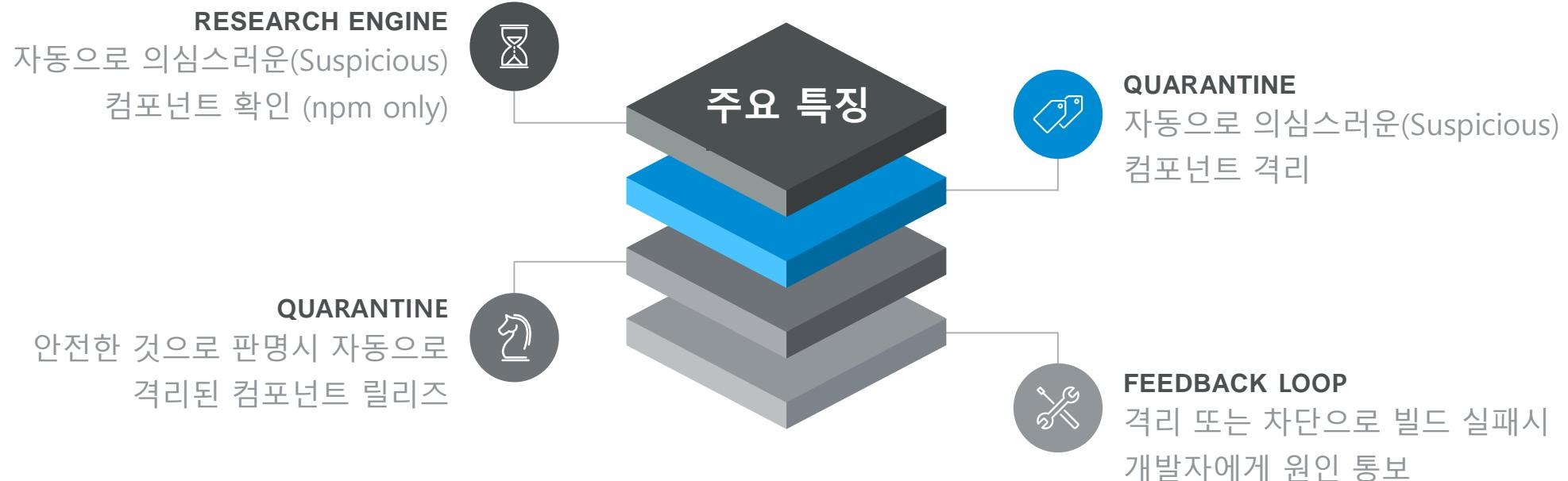
sonatype repository firewall

- 개발자는 수많은 OSS/3rd-Party 라이브러리를 사용
- 일부 OSS는 알려진 취약점을 가지고 있음
- Public Repo를 견디는 다양한 사이버공격의 일환으로 다수의 컴포넌트가 알려지지 않은 취약점을 포함
- Repository Firewall을 통해 알려진 취약점으로부터 보호
- 알려지지 않은 취약점으로부터 Software Supply Chain 보호 필요

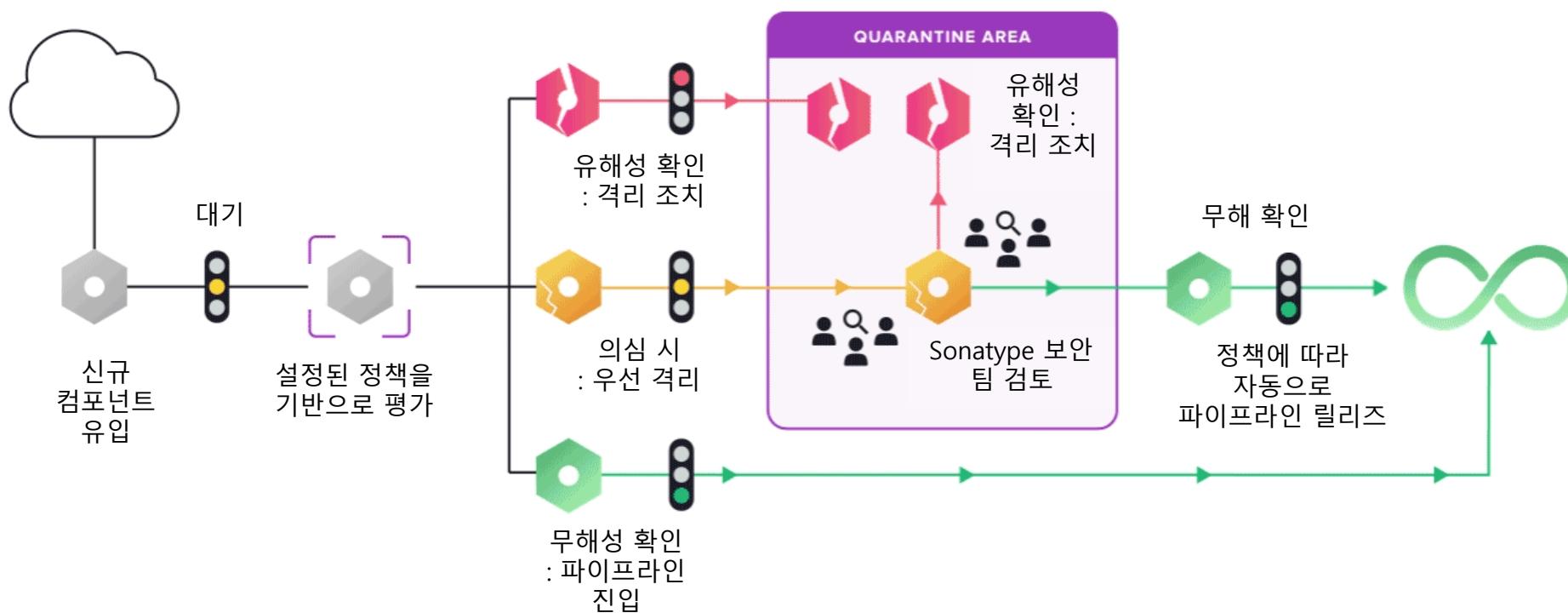
Unknown Risk – Malware Injection, Type Squatting, Namespace Confusion, Dependency Confusion, Cryptomining Malware, Ransomware



알려진 취약점 및 알려지지 않은 취약점까지 선제적으로 방어

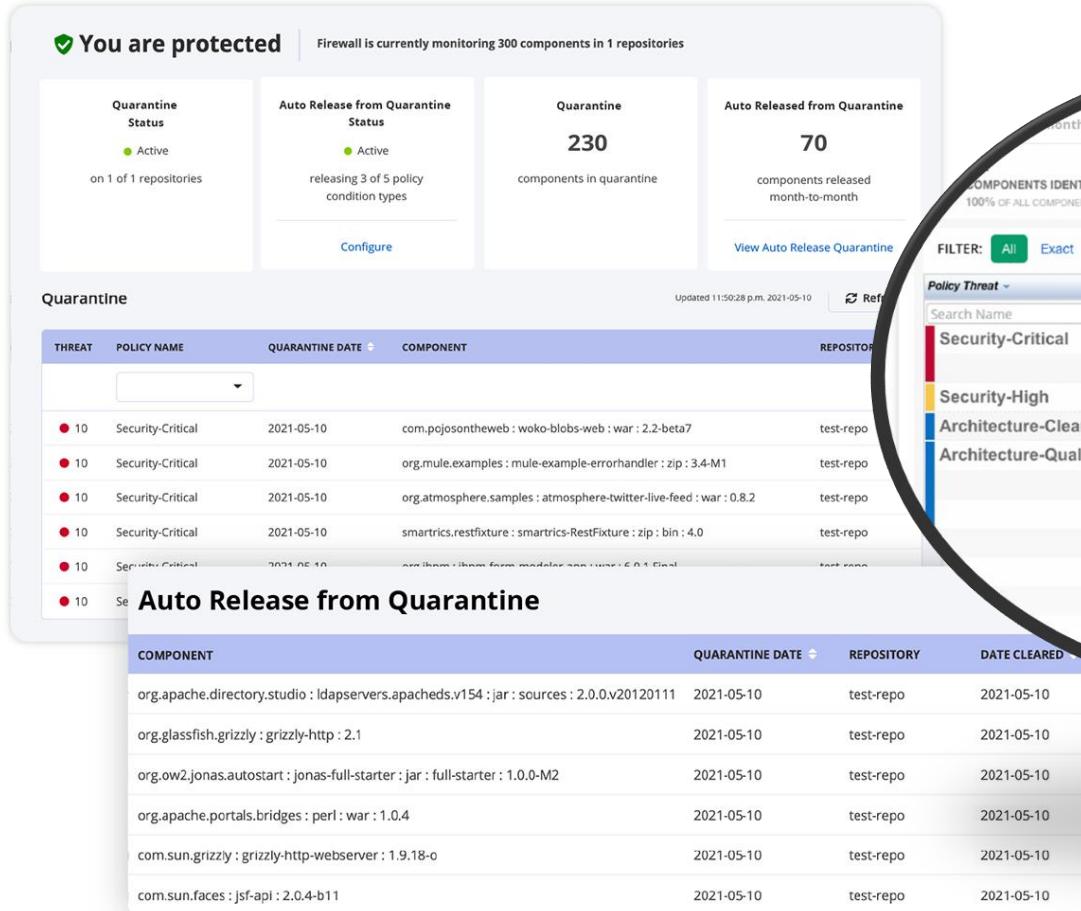


Nexus Intelligence의 Research Engine은 AI/ML 알고리즘을 사용하여 npm ecosystem을 상시 (24x7x365) 감시



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

Sonatype AI 엔진은 오픈소스에 대한 위협요소를 자동으로 판단하여
정책을 기반으로 유입을 차단하거나 안전이 확인 될 때까지 격리



The dashboard displays the following information:

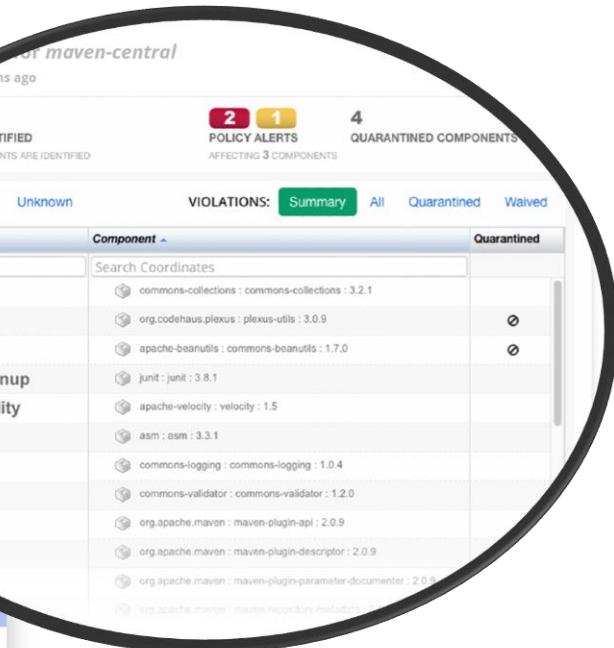
- You are protected**: Firewall is currently monitoring 300 components in 1 repositories.
- Quarantine Status**: Active on 1 of 1 repositories.
- Auto Release from Quarantine Status**: Active, releasing 3 of 5 policy condition types.
- Quarantine**: 230 components in quarantine.
- Auto Released from Quarantine**: 70 components released month-to-month.

Below these are two tables:

- Quarantine** table (highlighted by a large black circle):

THREAT	POLICY NAME	QUARANTINE DATE	COMPONENT	REPOSITORY
● 10	Security-Critical	2021-05-10	com.pojoontheweb : 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
● 10	Security-Critical	2021-05-10	com.ibm.libvirt : libvirt-farm-modeler : jar : war : 6.0.1.Final	test-repo
● 10	Security-Critical	2021-05-10	com.ibm.libvirt : libvirt-farm-modeler : jar : war : 6.0.1.Final	test-repo
- Auto Release from Quarantine** table:

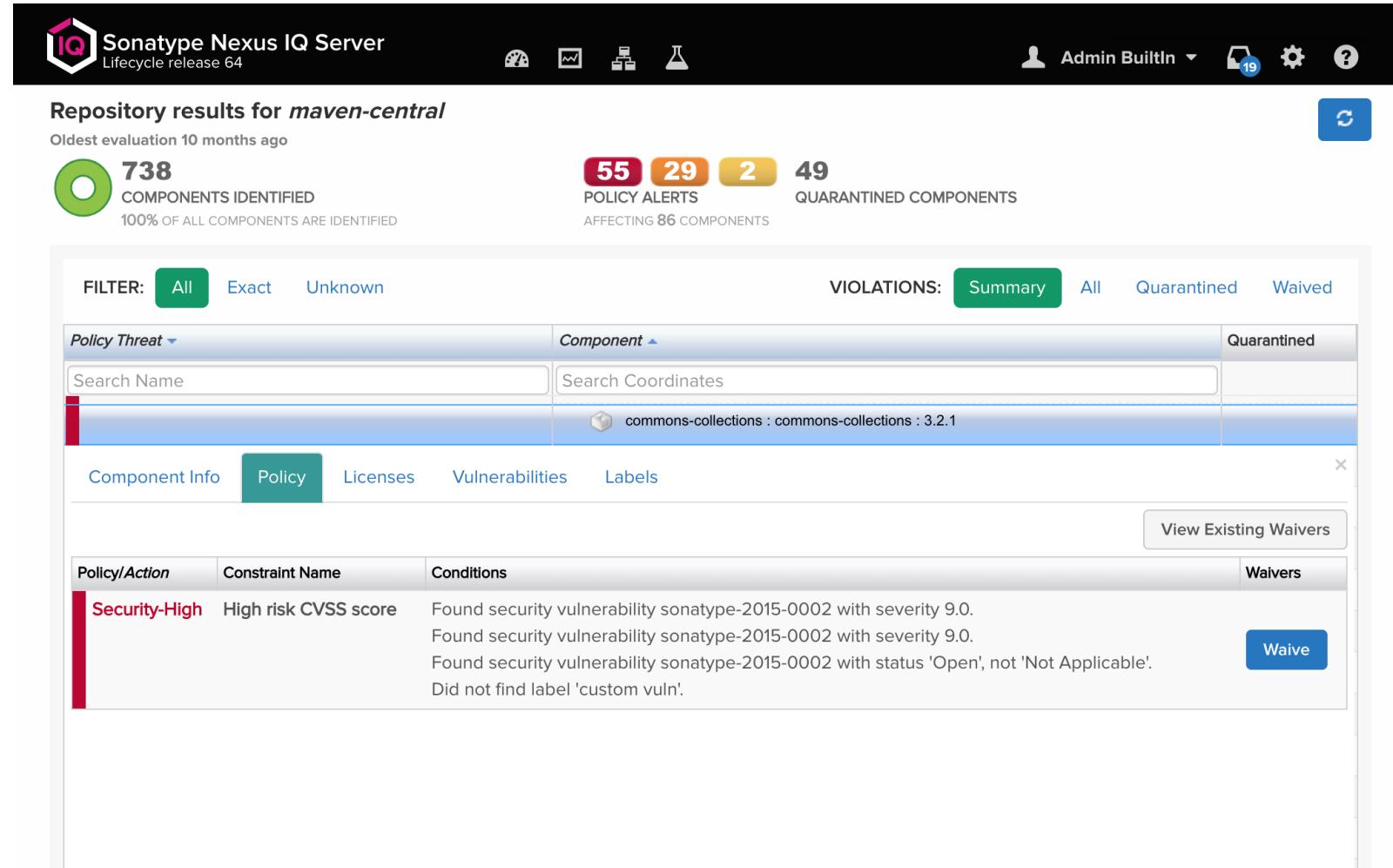
COMPONENT	QUARANTINE DATE	REPOSITORY	DATE CLEARED
org.apache.directory.studio : ldapservers.apacheds.v154 : jar : sources : 2.0.0.v20120111	2021-05-10	test-repo	2021-05-10
org.glassfish.grizzly : grizzly-http : 2.1	2021-05-10	test-repo	2021-05-10
org.ow2.jonas.autostart : jonas-full-starter : jar : full-starter : 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



This detailed view shows the following information:

- Alert for maven-central** (published 1 month ago)
- COMPONENTS IDENTIFIED**: 100% of all components are identified.
- POLICY ALERTS**: 2 Critical, 1 High, 4 Quarantined Components.
- VIOLATIONS**: Summary, All, Quarantined, Waived.
- Policy Threat** dropdown: Security-Critical, Security-High, Architecture-Cleanup, Architecture-Quality.
- Component** dropdown: Search Name (Security-Critical), Search Coordinates (commons-beanutils : commons-beanutils : 1.7.0).

다양한 정책을 반영하여 SDLC 내로 유입되는 컴포넌트를 관리하며 대안 제시



Sonatype Nexus IQ Server
Lifecycle release 64

Repository results for *maven-central*
Oldest evaluation 10 months ago

738 COMPONENTS IDENTIFIED
100% OF ALL COMPONENTS ARE IDENTIFIED

55 POLICY ALERTS
29 AFFECTING 86 COMPONENTS

2 QUARANTINED COMPONENTS
AFFECTING 86 COMPONENTS

FILTER: All Exact Unknown VIOLATIONS: Summary All Quarantined Waived

Policy Threat	Component	Quarantined
	commons-collections : commons-collections : 3.2.1	

Component Info Policy Licenses Vulnerabilities Labels View Existing Waivers

Policy/Action	Constraint Name	Conditions	Waivers
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 'Not Applicable'. Did not find label 'custom vuln'.	<button>Waive</button>

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	 Policy Threat Details		

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

Component Info	Policy	Licenses	Vulnerabilities	Labels
				View Existing Waivers
				Waive

Security-High org.apache.activemq : activemq-broker : 5.10.0

Component Info	Policy	Licenses	Vulnerabilities	Labels
DECLARED LICENSES  Apache-2.0	Scope central Status Open	License(s) Comment		

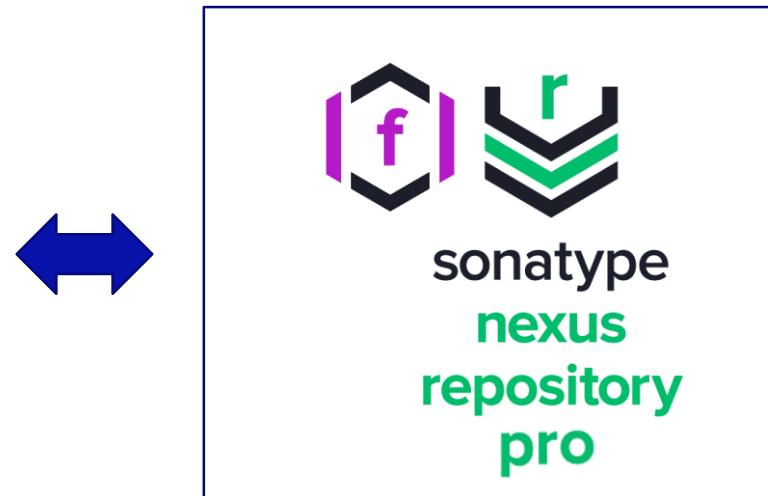
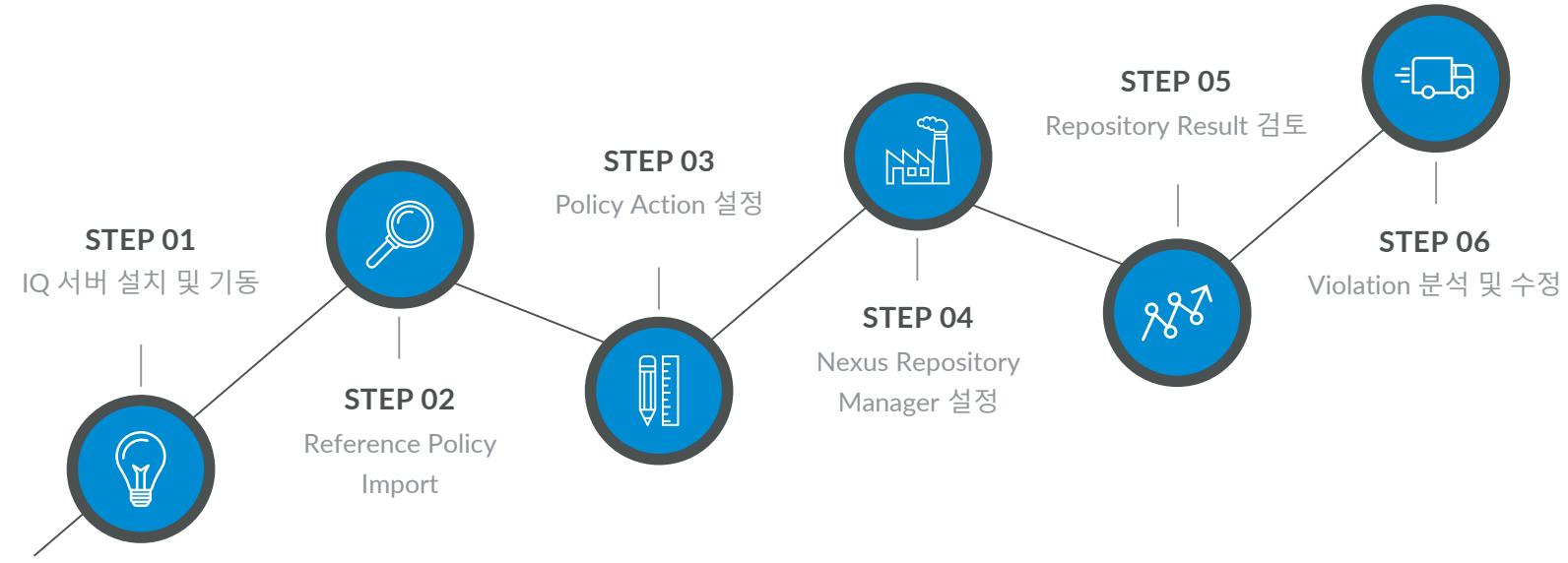
Security-High commons-fileupload : commons-fileupload : 1.2.2

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

Available  **Applied** 

Available	Applied
 Architecture-Blacklisted   Architecture-Cleanup   Architecture-Deprecated 	

Firewall Quick Start



정책의 적용 (Enforcement)

Actions

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

Notifications

	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE	CONTINUOUS MONITORING
No notifications configured								

Recipient Type Email

Email

ACTIONS

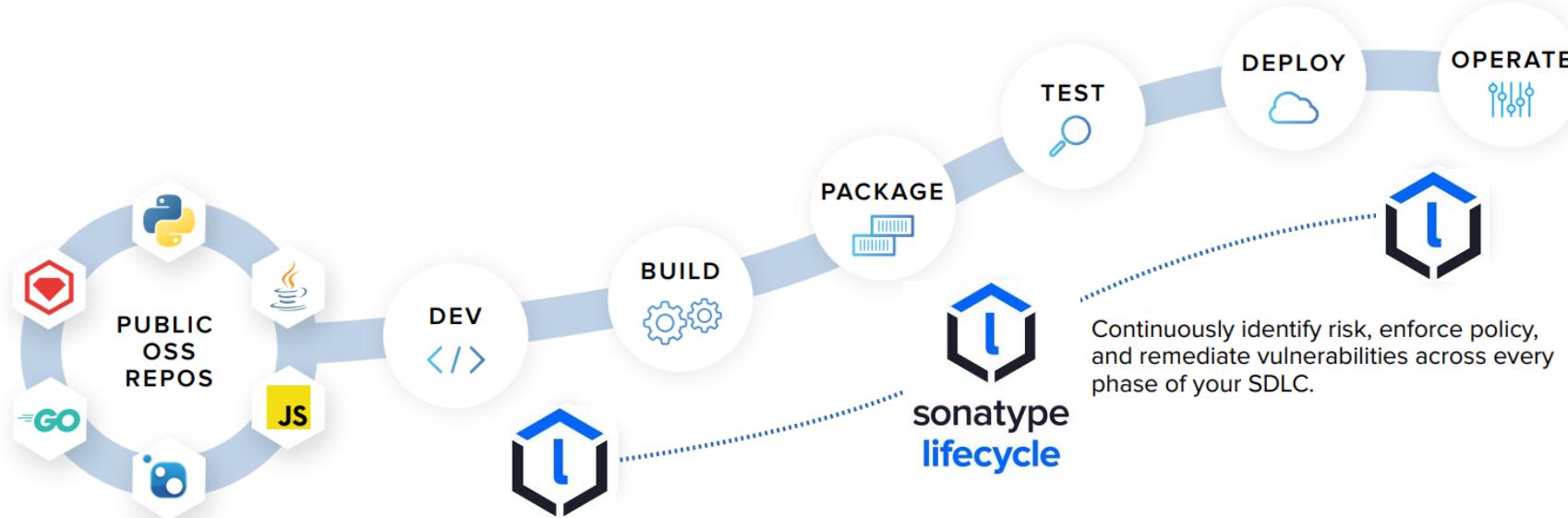
ACTION	PROXY	DEVELOP	BUILD	STAGE	RELEASE	OPERATE
No Action	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
⚠ Warn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>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

DevOps -> DevSecOps





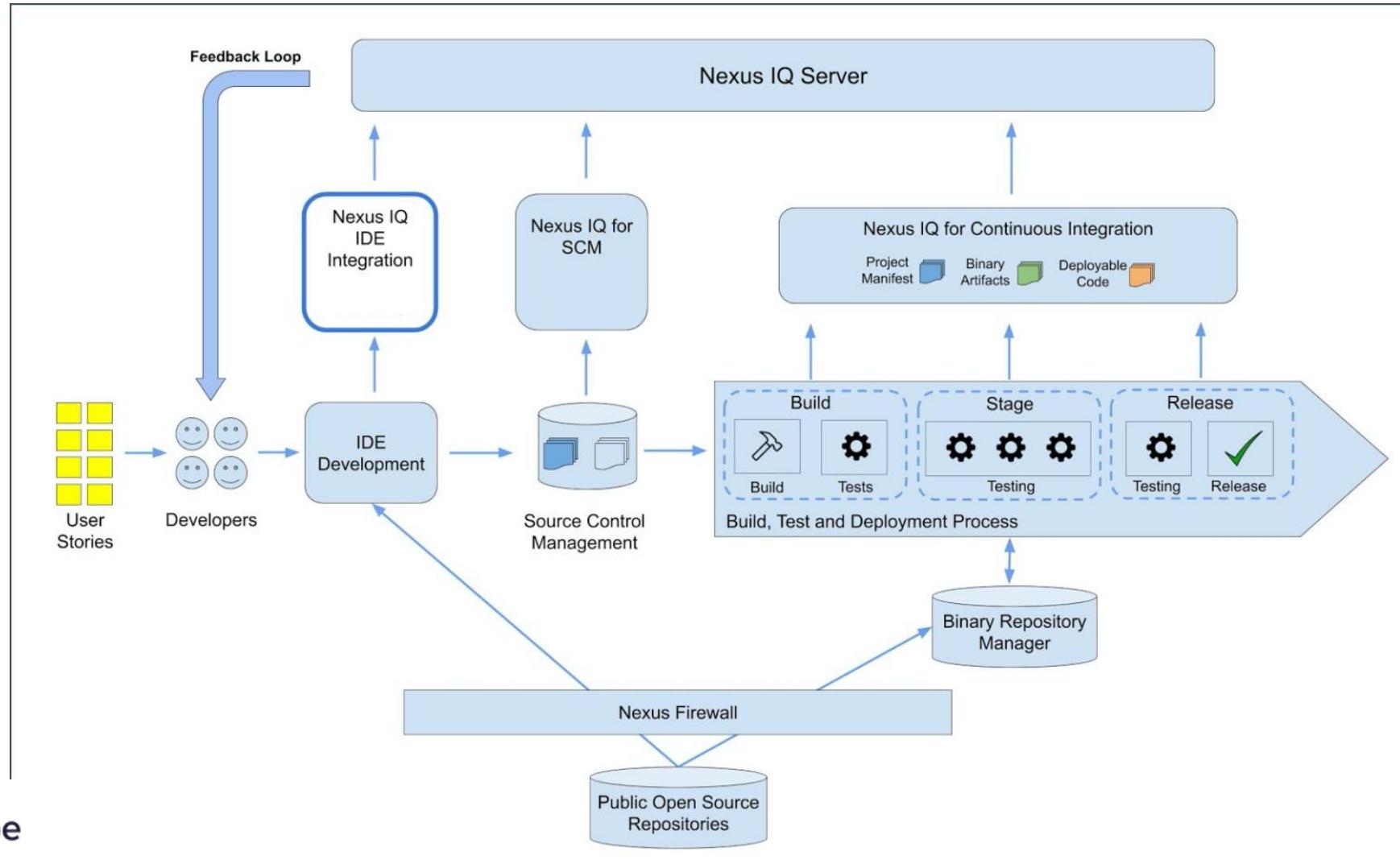
Lifecycle은 개발자 및 보안담당자가 오픈소스를 보다 안전하게 혁신을 추구하도록 합니다.



현업에서 사용하는 주요 Pipeline 툴의 사전 정합

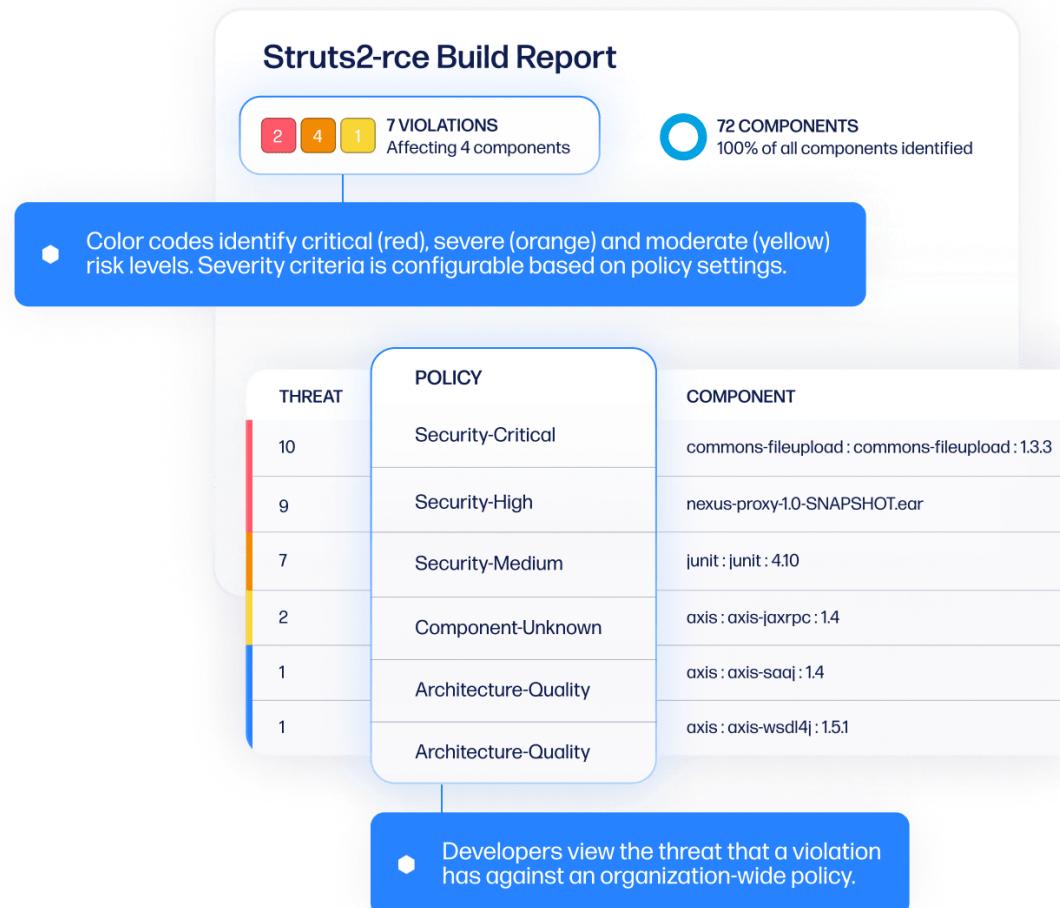


Nexus IQ Server – Big Picture





오픈소스 취약점 관리



1. 오픈소스 리스크 모니터링

- 구성요소, 리스크 수준, 및 어플리케이션 별로 취약점에 대한 지속적인 모니터링 및 경고

2. 정책 자동 적용

- 특정 Compliance 목표 달성을 위해 정책을 Customize 하며 다양한 개발도구를 통해 속도 감소 없이 정책 적용

3. SBOM 생성

- 어플리케이션 별로 수분내에 전반적인 가시성을 확보하고 빠르게 조치 방안을 확인



SBOM(Software Bill of Material) 자동 생성

The screenshot shows the Sonatype Lifecycle interface with the 'Components' tab selected in the 'Results' section. The table displays various software components along with their affected apps, total risk, and critical, severe, moderate, and low severity counts. The interface includes a detailed sidebar for filtering by organizations, applications, stages, policy types (Security checked), violation state, and policy threat level.

오픈소스 리스크 및 3rd-party 의존성 확인

The screenshot shows the Sonatype interface for the 'maven-central' repository. It highlights a 'License-Banned' component with a 'Security-High' threat level. A detailed modal window provides 'Vulnerability Information' about jackson-databind being vulnerable to Remote Code Execution (RCE). It notes that the 'createBeanDeserializer()' function in the BeanDeserializerFactory class allows untrusted Java objects to be deserialized, and that a remote attacker can exploit this by uploading a malicious serialized object. It also mentions a note about an incomplete fix for CVE-2017-7525 and a detection note about Spring Security's fix for CVE-2017-4995.

위험요소에 대한 전문 교정가이드 제공



빠르게 고품질 코드 작성

pom.xml

Highlights the specific lines of code that introduced a violation.

```

16 - < />
17 + < />
  
```

19 + <jackson.version>2.9.9.3</jackson.version>

eduard 4 minutes ago (Author)

Nexus IQ found policy violations introduced by:

- com.fasterxml.jackson.core:jackson-databind:2.9.9.3

Bumping to version 2.10.0 will resolve these violations (as of Oct 14, 2022)

Threat	Policy	Violation Details
10	Security-Critical	Critical risk CVSS score: • Found security vulnerabilities: CVE-2021-1474, CVE-2019-13592, CVE-2019-17267
9	Security-High	High risk CVSS score: • Found security vulnerabilities: sonatype-2021-0371

If a version is available that will fix the problem, the suggested remediation or upgrade path is also included.

1. 도구 변경없이 Risk 제어

- IDE, Source Control로부터 직접 개선된 Component 선택

2. 코드 품질 사전 확보

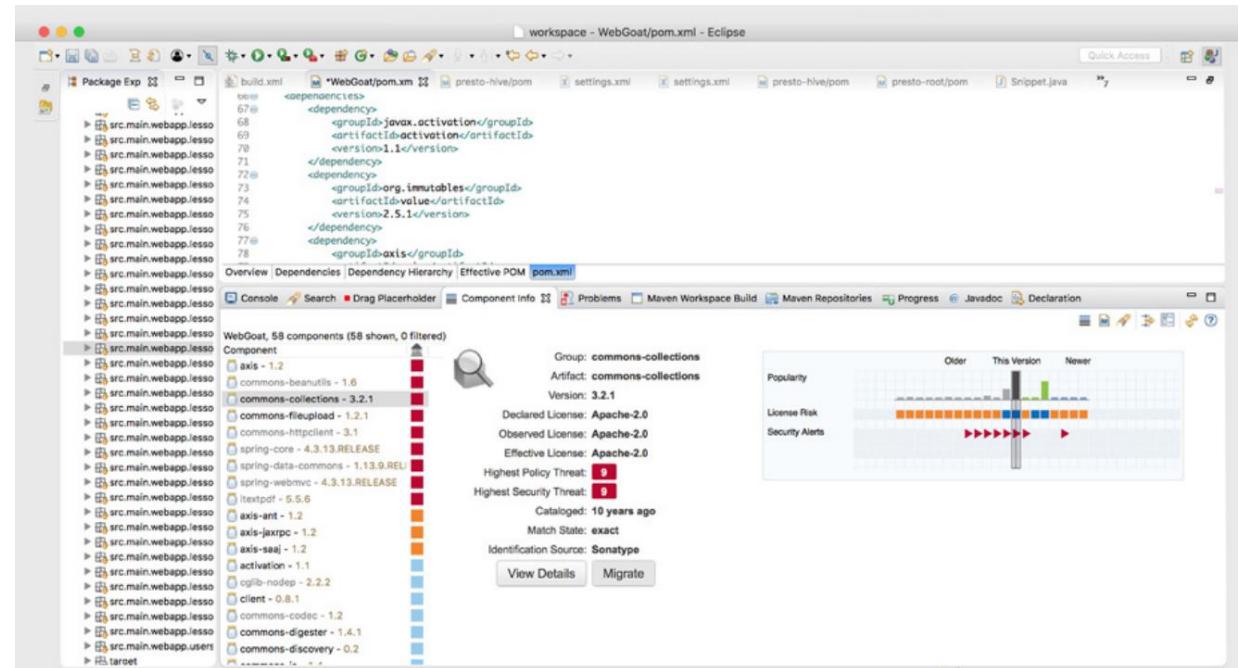
- 사전에 잠재적인 보안 이슈 및 유지보수 이슈를 탐지하고 조치

3. 취약점을 빠르게 치유

- 정확한 위치와 의존성을 파악하고 위협요소를 빠르게 수정할 수 있는 정보 확보

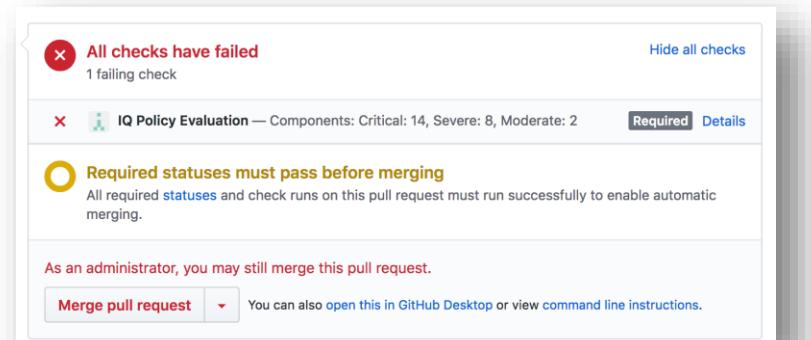
빠르게 고품질 코드 작성

- GitHub, GitLab, BitBucket등과 통합되어 정책을 위반한 구성요소에 대해 자동으로 Pull 리퀘스트 생성
- 모든 활성브랜치의 차이점을 비교하여 악성 구성요소나 취약성이 Pull/Merge 리퀘스트에 포함되어 있는 경우 코드라인에 수정방안 제시
- Eclipse, IntelliJ, 및 Visual Studio등 정합을 통해 실시간 정보를 참조하여 한번의 클릭으로 최적의 컴포넌트를 선택





IQ for SCM (Source Control Management)



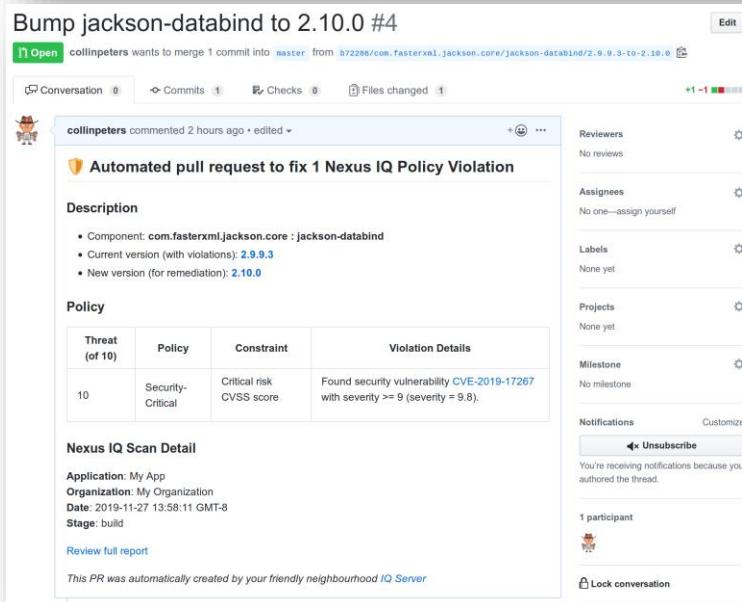
All checks have failed
1 failing check

IQ Policy Evaluation — Components: Critical: 14, Severe: 8, Moderate: 2

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.



Bump jackson-databind to 2.10.0 #4

Open collinpeters wants to merge 1 commit into master from b7228e/com.fasterxml.jackson.core:jackson-databind/2.9.9.3-to-2.10.0

Conversation Commits Checks Files changed

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

Automated Commit Feedback

Commit 또는 Pull Request에 Policy 평가정보를
직접 확인하도록 제공

Automated Pull Request

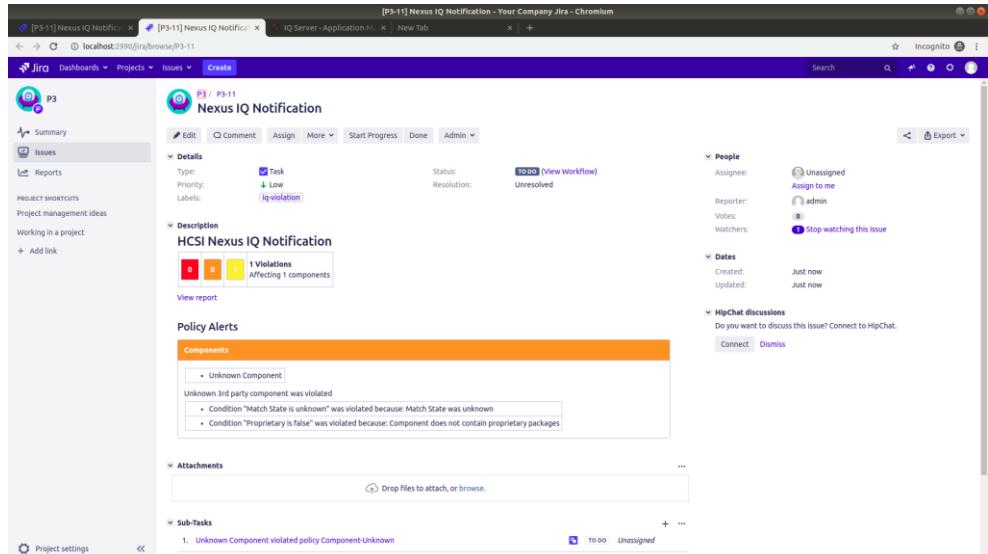
Policy Violation에 대해 수정 버전이 존재하는 경우 자동으로
Pull Request 생성

Pull Request Commenting

Pull Request가 새로운 Policy Violation을 발생시키는 경우
관련 Comment 추가

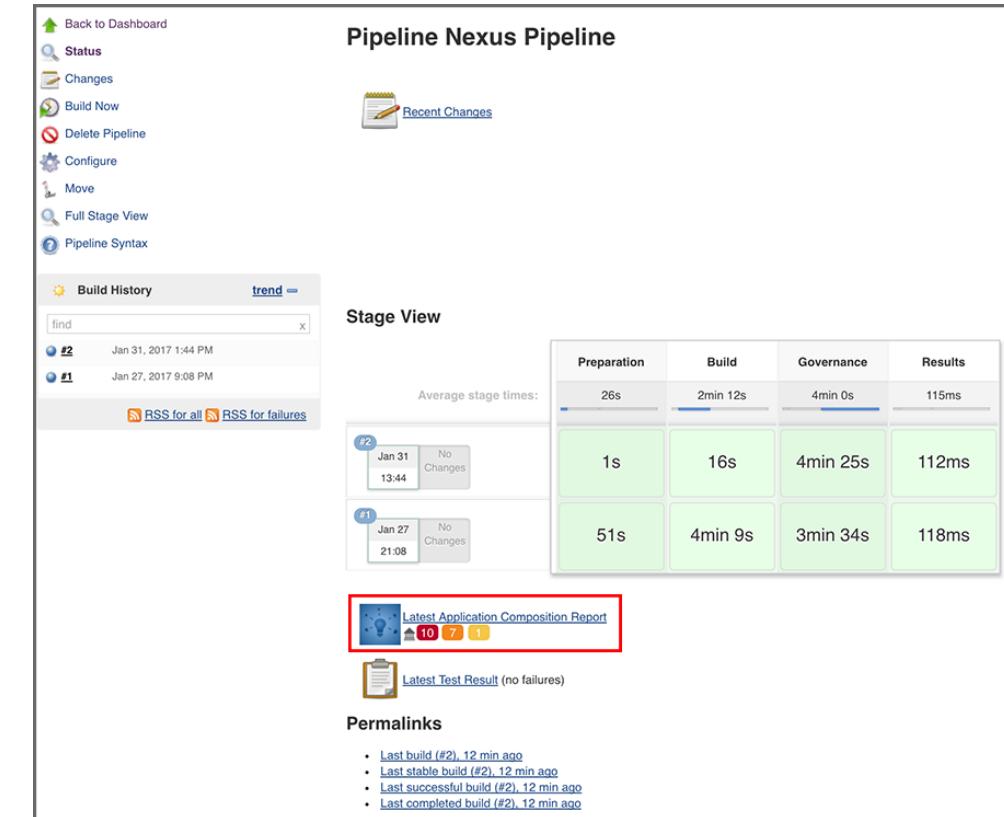


JIRA & CI Server 지원




Automated Ticket Creation

Jira Plugin을 통해 IQ Server Webhook Violation 이벤트를 받아 티켓 자동 생성

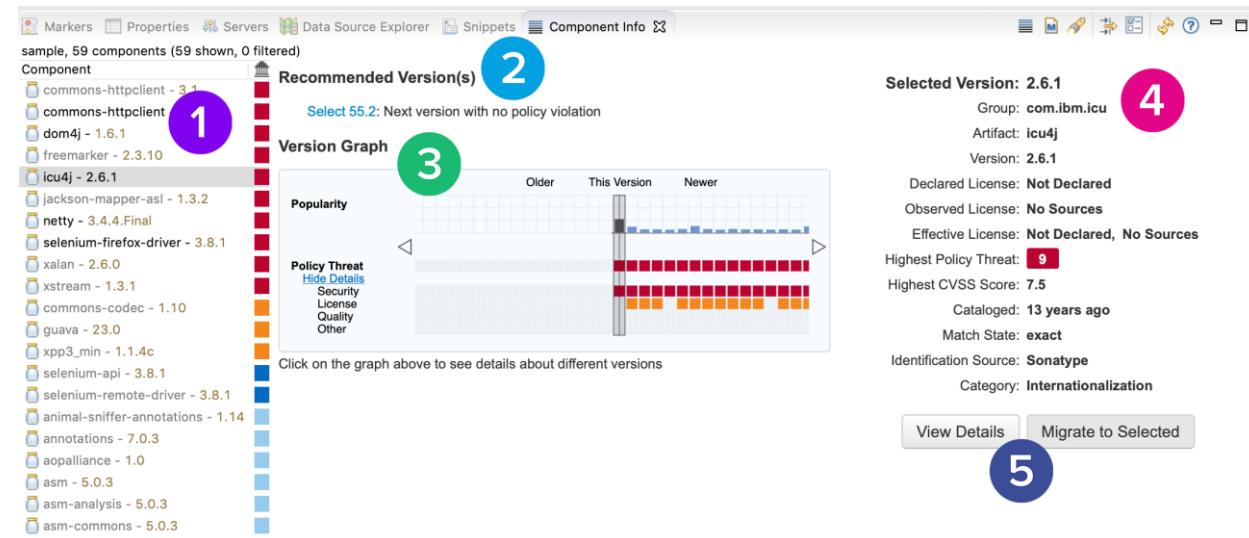


Build Scan Result

CI Server (Jenkins, Bamboo, Azure DevOps, Gitlab CI등)를 통해 Security & License 분석 결과를 확인



개발자 IDE 환경 지원 (via IQ Integration)



- 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



Advanced Development Support

Breaking Changes

Component
업그레이드에 코드변경이
필요한지 여부

org.bouncycastle : bcprov-jdk15on : 1.56

Direct Dependency

COMPONENT INFO	POLICY	SIMILAR	OCCURRENCES	LICENSES	VULNERABILITIES	LABELS	AUDIT LOG						
Recommended Version(s)													
The current version has no policy violations.													
The current version doesn't cause Build failure for this component and its dependencies.													
Version Graph													
Click on the graph above to see details about different versions													
Selected Version: 1.56	Type: maven	Group: org.bouncycastle	Artifact: bcprov-jdk15on	Version: 1.56	Declared License: MIT	Observed License: No Source License	Effective License: MIT	Highest CVSS Score: NA	Hygiene Rating: Exemplar	Cataloged: 3 years ago	Match State: exact	Identification Source: Sonatype	Category: Other

Close [Back to org.bouncycastle : bcprov-jdk15on : 1.56](#)

org.apache.karaf.bundle : org.apache.karaf.bundle.core : 4.0.9

Direct Dependency

COMPONENT INFO	POLICY	SIMILAR	OCCURRENCES	LICENSES	VULNERABILITIES	LABELS	AUDIT LOG					
Recommended Version(s)												
Select 4.2.2: Next version with no policy violation												
Select 4.2.2: Next version with no policy violations for this component and its dependencies												
The current version doesn't cause Build failure for this component and its dependencies.												
Version Graph												
Click on the graph above to see details about different versions												
Selected Version: 4.0.9	Type: maven	Group: org.apache.karaf.bundle	Artifact: org.apache.karaf.bundle.core	Version: 4.0.9	Declared License: Apache-2.0	Observed License: Apache-2.0	Effective License: Apache-2.0	Highest CVSS Score: 9.8	Cataloged: 3 years ago	Match State: exact	Identification Source: Sonatype	Category: Web Application Container

Transitive Solver

정책 및 코드변경 등을
고려한 업그레이드 패스
추천

Release Integrity (ML/AI)

공급망 모니터링을 통해
의심되는 컴포넌트 사전
경고

aoco : 1.0.0

COMPONENT INFO **POLICY** **SIMILAR** **OCCURRENCES** **LICENSES** **VULNERABILITIES** **LABELS** **AUDIT LOG**

Recommended Version(s)													
Select 1.0.1: Next version with no policy violation													
The current version doesn't cause Build failure.													
Version Graph													
Click on the graph above to see details about different versions													
Selected Version: 1.0.0	Type: npm	packaged: aoco	version: 1.0.0	Declared License: ISC	Observed License: Not Supported	Effective License: ISC	Highest CVSS Score: 7.2	Hygiene Rating: NA	Integrity Rating: Suspicious	Cataloged: 23 days ago	Match State: exact	Identification Source: Sonatype	Category: Other

Close [Previous](#) [Next](#)

org.apache.karaf.config : org.apache.karaf.config.core : 4.0.9

Direct Dependency

COMPONENT INFO	POLICY	SIMILAR	OCCURRENCES	LICENSES	VULNERABILITIES	LABELS	AUDIT LOG						
Recommended Version(s)													
Select 4.2.6: Next version with no policy violation													
The current version doesn't cause Build failure for this component and its dependencies.													
Version Graph													
Click on the graph above to see details about different versions													
Selected Version: 4.0.9	Type: maven	Group: org.apache.karaf.config	Artifact: org.apache.karaf.config.core	Version: 4.0.9	Declared License: Apache-2.0	Observed License: Apache-2.0	Effective License: Apache-2.0	Highest CVSS Score: 9.8 within 3 policies	Hygiene Rating: Laggard	Cataloged: 3 years ago	Match State: exact	Identification Source: Sonatype	Category: Configuration Utilities and Frameworks

Hygiene Ratings

Supplier (프로젝트
소스)에 대한 품질 평가
지표

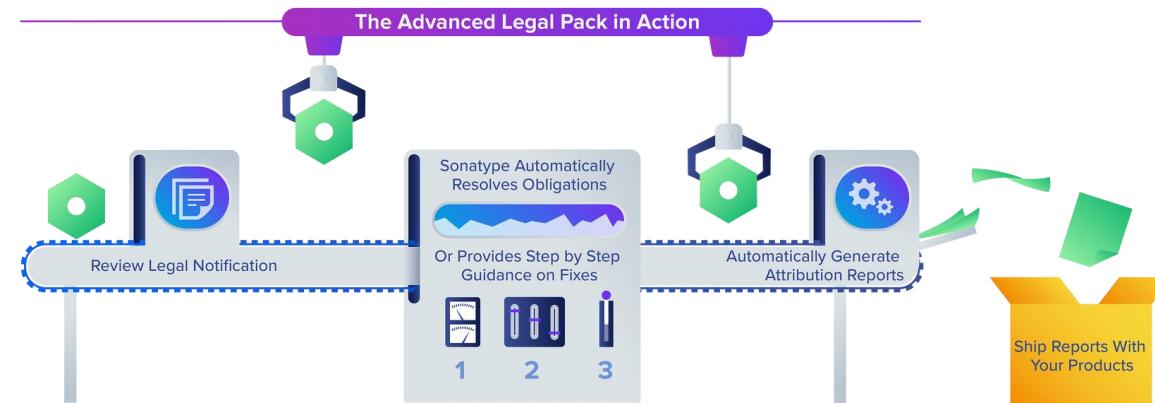


Chrome Extension

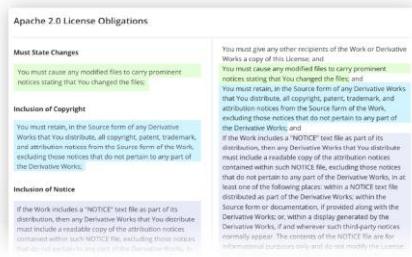
The image shows two screenshots of a web browser demonstrating the Sonatype Chrome Extension. The top screenshot shows the extension's interface over a search.maven.org page for org.apache.struts:struts2-core:2.3.30. It displays component details like version 2.3.30, a dependency XML snippet, and a link to Apache Maven Resources. The bottom screenshot shows the extension's interface over the same search results page, highlighting a detailed component info box. This box contains information such as Format: maven, Package: org.apache.struts:struts2-core, Version: 2.3.30, Hash: 0d2281c1a99f65b1ab19, Match State: exact, CatalogDate: 2016-07-07T06:37:13.000Z, RelativePopularity: 3, Highest CVSS Score: 10 within 4 security issues, and Data Source: NEXUSIQ.



Advanced Legal Pack (Lifecycle Add-On)



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

org.apache.commons : commons-collections4 : 4.4

Review Status	Review Progress	Highest License Threat
Flagged	7/8 complete	Liberal
Last Modified	Modified by	Stages
2 days ago	Admin	Build 21d

Obligations to Review

- Inclusion of Copyright (Fulfilled)
- Inclusion of Notice (Fulfilled)
- Must State Changes (Flagged)
- Inclusion of License (Fulfilled)

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

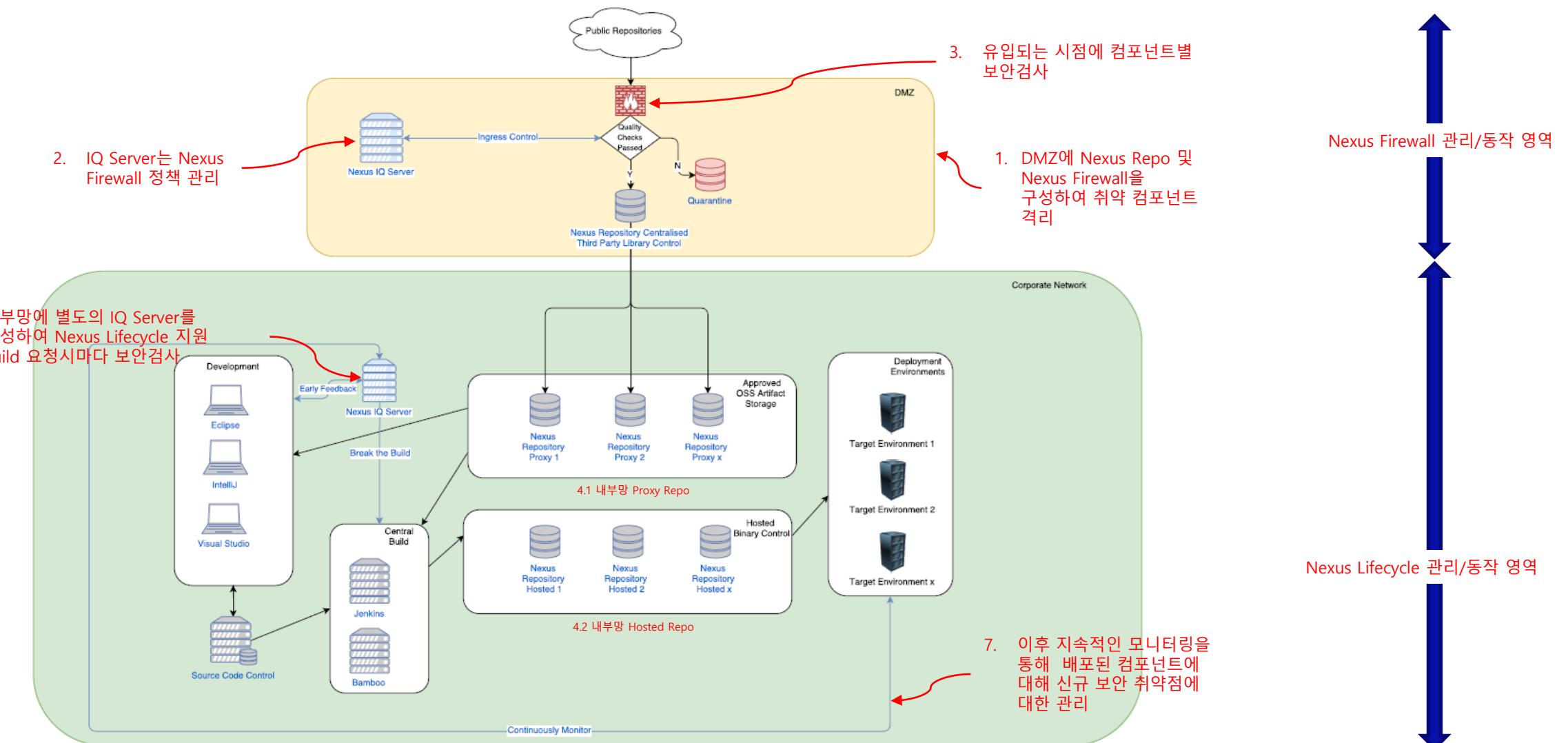
org.apache.commons : commons-collections4 : 4.4

Licenses	Copyright Notices	Notice Files
Apache 2.0	Copyright 2001-2019 The Apache Software Foundation	Apache Commons Collection

Definitions:

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

표준 구성



Summary – Why Sonatype?

Shift Left (시프트 레프트)

오픈소스 유입 관문부터 실시간 통제



개발자 스스로 최적의 컴포넌트 선택



Accuracy (정확성)

글로벌 최대 데이터베이스 운영

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



Advanced Binary Fingerprint 식별 기술



자동화 필수요건

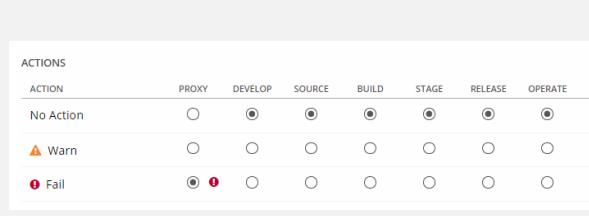
Flexible Policy (유연한 정책)

다양한 속성을 통한 정책 정의



액성/맬웨어
취약성

품질
라이선스
인기도



단계별 차등화 된 정책 적용

Appendix : Sonatype 도입 Roadmap





(주)오에스씨코리아
www.osckorea.com

sales@osckorea.com | 02-539-3690