DevSecOps 환경을 위한 "Open-Source Governance 자동화 플랫폼"

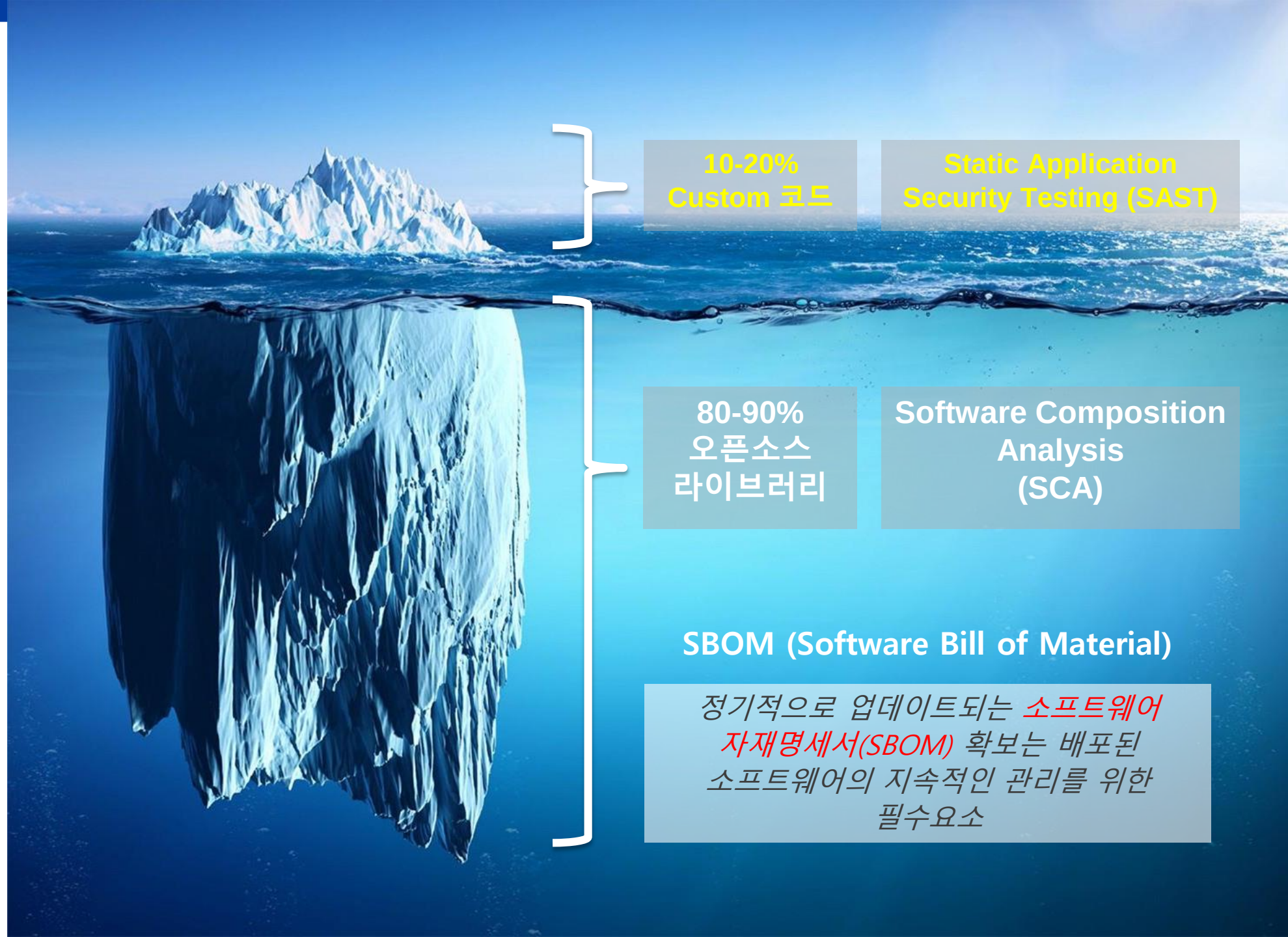
Sonatype Platform

July 2023

㈜오에스씨코리아
www.osckorea.com

Why Sonatype?

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



OSC sonatype

SBOM (Software Bill of Material)

- 소프트웨어 자재명세서

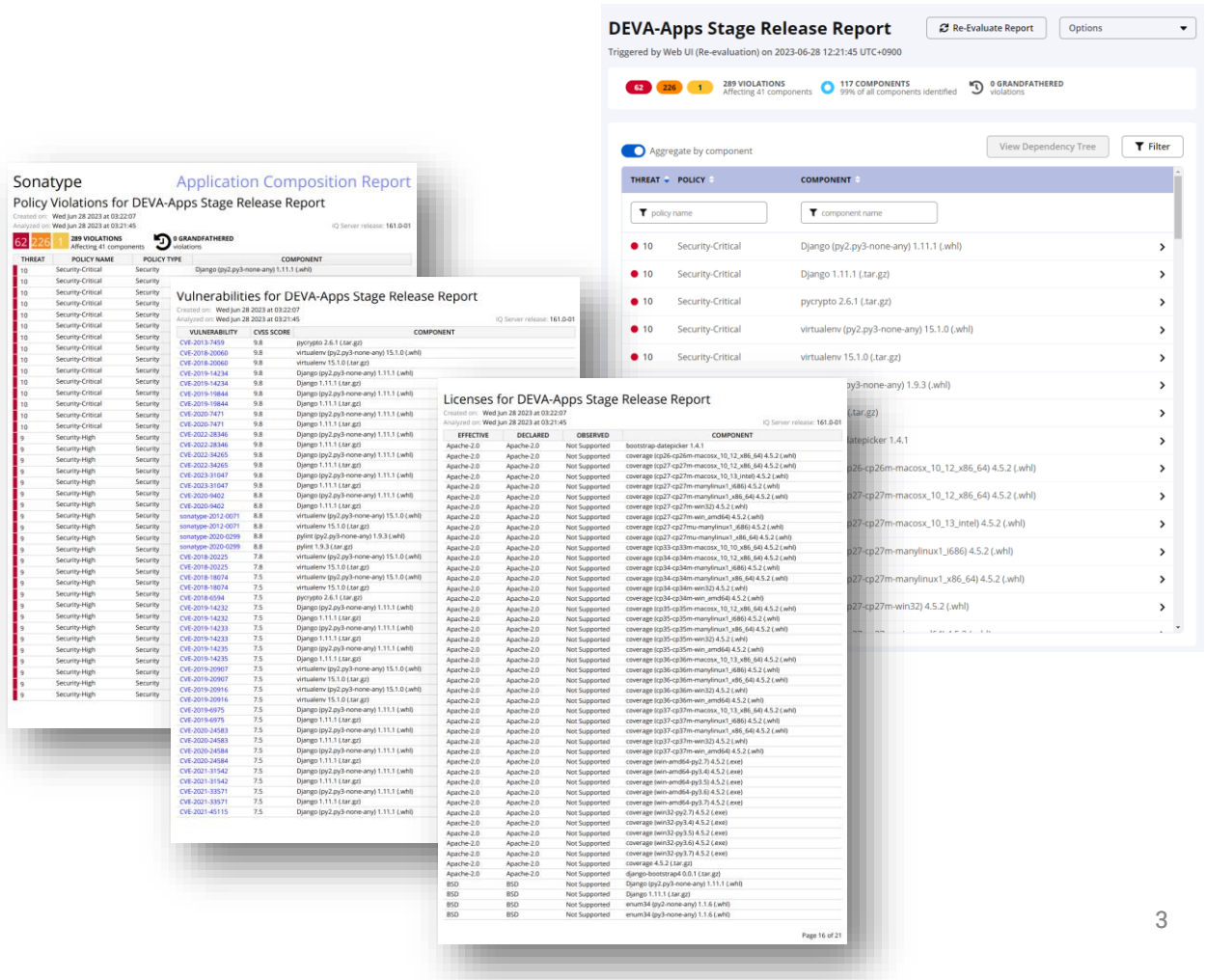
Hardware BOM

Filename: TIDA-00771 E2 (001)_BO M.xls
Variant: 001
Generated: 3/24/2016 3:48:26 PM

TIDA-00771 REV E2 Bill of Materials

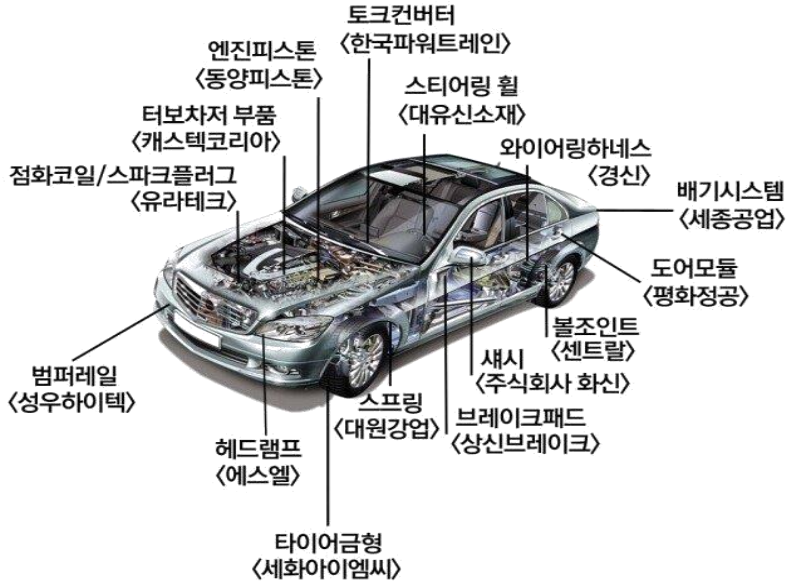
Item #	Designator	Quantity	Value	PartNumber	Manufacturer	Description	PackageReference
1	C1, C3, C15	3	1uF	C1608X7R1C105K	TDK	CAP, CERM, 1 µF, 16 V, +/- 10%, X7R, 0603	0603
2	C2, C4	2	0.047uF	C1608X7R1E473K	TDK	CAP, CERM, 0.047 µF, 25 V, +/- 10%, X7R, 0603	0603
3	C5	1	4.7uF	GRM31CR71H475KA12L	MuRata	CAP, CERM, 4.7 µF, 50 V, +/- 10%, X7R, 1206	1206
4	C6	1	4.7uF	GRM21BR61C475KA88L	MuRata	CAP, CERM, 4.7 µF, 16 V, +/- 10%, X5R, 0805	0805
5	C7, C8, C9	3	2.2uF	GRM32ER72A225KA35L	MuRata	CAP, CERM, 2.2 µF, 100 V, +/- 10%, X7R, 1210	1210
6	C10, C14, C26, C27, C30	5	1000pF	885012205061	Wurth Elektronik	CAP, CERM, 1000 pF, 50 V, +/- 10%, X7R, 0402	0402
7	C11	1	3300pF	C1005X7R1H332K	TDK	CAP, CERM, 3300 pF, 50 V, +/- 10%, X7R, 0402	0402
8	C12	1	2.2uF	GRM31CR71H225KA88L	MuRata	CAP, CERM, 2.2 µF, 50 V, +/- 10%, X7R, 1206	1206
9	C13, C18, C23, C25, C28, C31	6	0.1uF	885012105016	Wurth Elektronik	CAP, CERM, 0.1 µF, 16 V, +/- 20%, X5R, 0402	0402
10	C16	1	10uF	0805YD106MAT2A	AVX	CAP, CERM, 10uF, 16V, +/-20%, X5R, 0805	0805
11	C17, C29	2	0.1uF	0603YC104JAT2A	AVX	CAP, CERM, 0.1 µF, 16 V, +/- 5%, X7R, 0603	0603
12	C19, C20	2	270uF	EKZN350ELL271MJC5S	United Chemi-Con	CAP ALUM 270UF 20% 35V RADIAL	10x20
13	C21	1	0.1uF	C2012X7R1E104K	TDK	CAP, CERM, 0.1 µF, 25 V, +/- 10%, X7R, 0805	0805
14	C22	1	2200pF	GRM155R71H222KA01D	MuRata	CAP, CERM, 2200 pF, 50 V, +/- 10%, X7R, 0402	0402
15	C24	1	0.01uF	C0603X103K5RACTU	Kemet	CAP, CERM, 0.01 µF, 50 V, +/- 10%, X7R, 0603	0603
16	D1	1	RED	150060RS75000	Wurth Elektronics Inc	LED RED CLEAR 0603 SMD	LED_0603
17	D2	1	30V	SMAJ30CA	Littelfuse	Diode, TVS, Bi, 30 V, 400 W, SMA	SMA
18	D3	1	YELLOW	150060YS75000	Wurth Elektronics Inc	LED YELLOW CLEAR 0603 SMD	LED_0603
19	D4	1	GREEN	150060GS75000	Wurth Elektronics Inc	LED, Green, SMD	LED_0603
20	D5	1	40V	NSR0240V2T1G	ON Semiconductor	Diode, Schottky, 40 V, 0.25 A, SOD-523	SOD-523
21	J1	1	PEC04SAAN	PEC04SAAN	Sullins	Header, Male 4-pin, 100mil spacing,	0.100 inch x 4
22	J2	1		800-10-003-10-001000	Mill-Max	Header, 100mil, 3x1, TH	Header, 3x1, 100mil, TH
23	J3	1		800-10-005-10-001000	Mill-Max	Header, 100mil, 5x1, TH	Header, 5x1, 100mil, TH
24	J4	1		800-10-002-10-001000	Mill-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	CSD17576Q5B	Texas Instruments	MOSFET, N-CH, 30 V, 100 A, SON 5x6mm	SON 5x6mm
27	R1, R3	2	10k	CRCW0603310K0JNEA	Vishay-Dale	RES, 10 k, 5%, 0.1 W, 0603	0603
28	R2	1	100	CRCW0603100RJNEA	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, 3.30 k, 0.1%, 0.1 W, 0603	0603
30	R5, R18	2	0.001	CRE2512-FZ-R001E-3	Bourns Inc.	RES SMD 0.001 OHM 1% 3W 2512	2512
31	R6, R7, R22, R27, R28, R39, R42, R43, R44	9	100	ERJ-2RKF1000X	Panasonic	RES, 100, 1%, 0.1 W, 0402	0402
32	R8	1	5.11	RC0603FR-075R11L	Yageo America	RES, 5.11, 1%, 0.1 W, 0603	0603
33	R9	1	47.5k	CRCW0402475KFKED	Vishay-Dale	RES, 47.5 k, 1%, 0.063 W, 0402	0402
34	R10	1	2M	RC0603FR-072ML	Yageo	RES SMD 2M OHM 1% 1/10W 0603	0603
35	R11	1	3.3	CRCW06033R30JNEA	Vishay-Dale	RES, 3.3, 5%, 0.1 W, 0603	0603
36	R12	1	499k	RC0402FR-07499KL	Yageo	RES SMD 499K OHM 1% 1/16W 0402	0402
37	R13, R14, R15	3	3.3k	CRCW04023K30JNED	Vishay-Dale	RES, 3.3 k, 5%, 0.063 W, 0402	0402
38	R19, R21, R32, R36, R37, R38	6	10.0k	ERJ-2RKF1002X	Panasonic	RES, 10.0 k, 1%, 0.1 W, 0402	0402
39	R20	1	0	ERJ-2GE0R00X	Panasonic	RES, 0, 5%, 0.063 W, 0402	0402
40	R23	1	51.1k	CRCW0402511KFKED	Vishay-Dale	RES, 51.1 k, 1%, 0.063 W, 0402	0402
41	R24	1	78.7k	CRCW040278K7FKED	Vishay-Dale	RES, 78.7 k, 1%, 0.063 W, 0402	0402
42	R25	1	100k	CRCW0402651KFKED	Yageo	RES SMD 100K OHM 1% 1/16W 0402	0402
43	R26	1	100	CRCW0402100RFKED	Vishay-Dale	RES, 100, 1%, 0.063 W, 0402	0402
44	R40, R45	2	1.00Meg	ERJ-2RKF1004X	Panasonic	RES, 1.00 M, 1%, 0.1 W, 0402	0402
45	U1	1		DRV83053PHPR	Texas Instruments	Three Phase Gate Driver With Current Shunt Amplifiers and Voltage Regulator, PHP0048G	PHP0048G
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 (PW), Green (RoHS & no Sb/Br)	PW0028A
47	U3	1		LMT87QDCKRQ1	Texas Instruments	SC70 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 to +125 degC, 2-pin X2SON (DPY)	DPY0002A
49	U9	1		SN74LVC126APWR	Texas Instruments	Quadruple Bus Buffer Gate with 3-State Outputs, PW0014A	PW0014A
50	R41	0	0	ERJ-2GE0R00X	Panasonic	RES, 0, 5%, 0.063 W, 0402	0402

SBOM (Software BOM)



Supply Chain & SDLC (Software Development Lifecycle)

- 공급망 & 자재저장소



600여 1/2차 협력사 공급망

Warehouse

Assembly

Repository

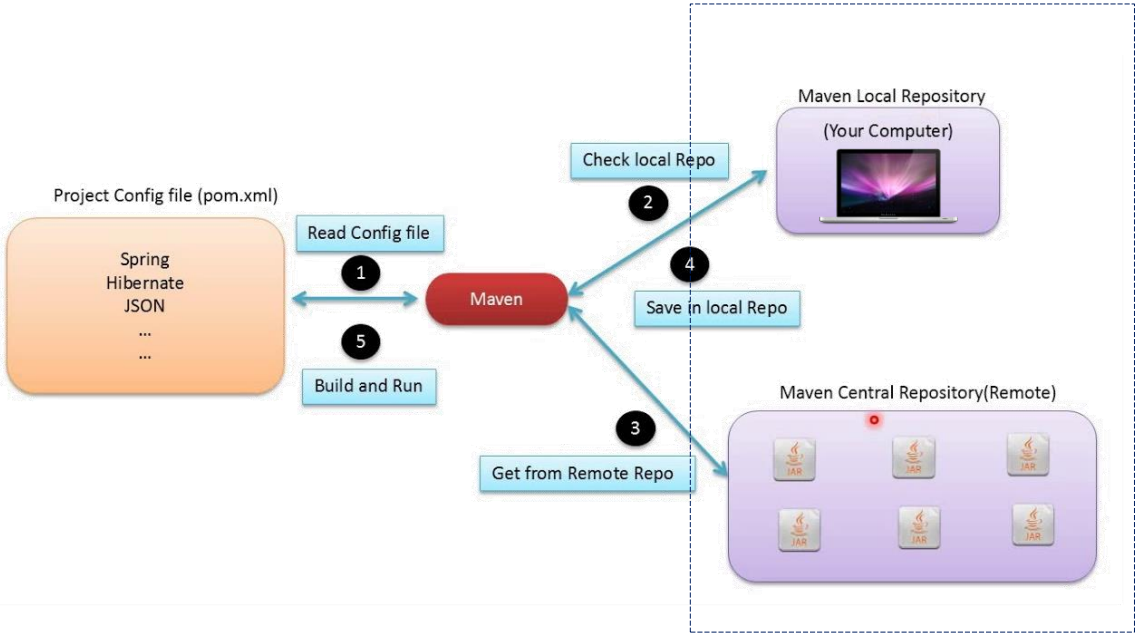
Build(CI/CD)

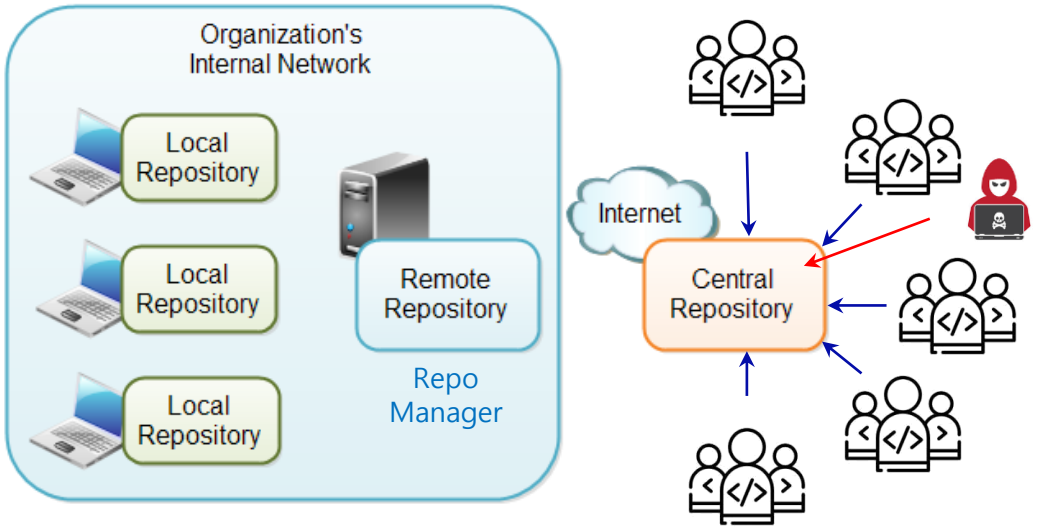
Release Candidate

Ready to ship

Public Repository

Public Repository & Remote Repository (Repo Manager)



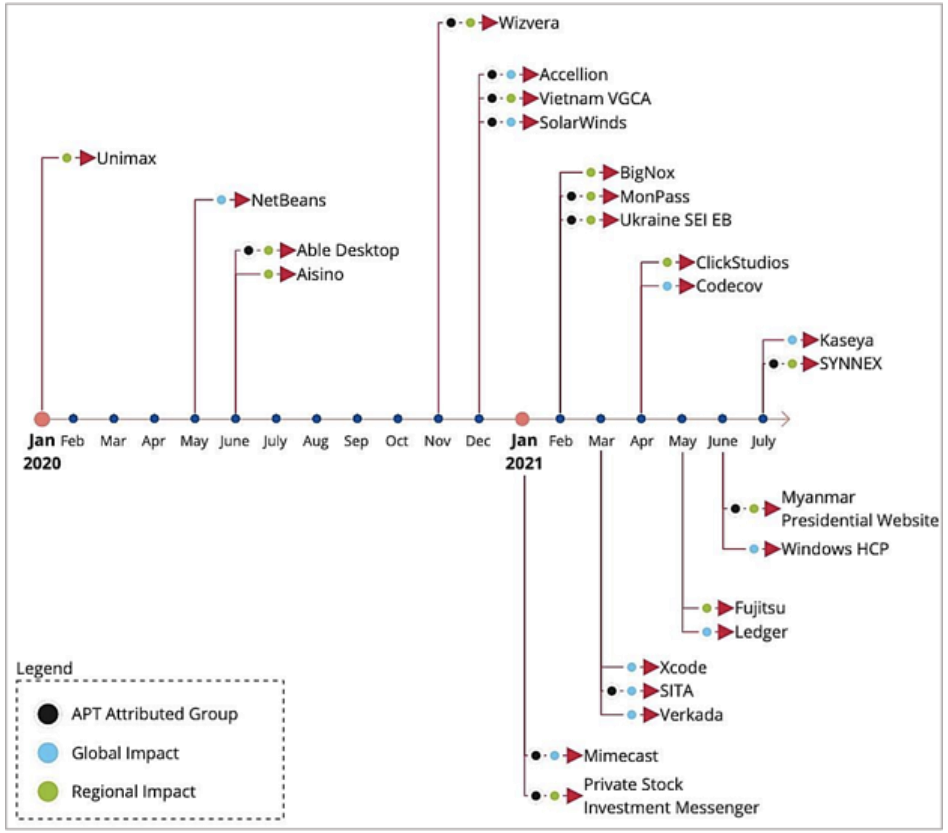


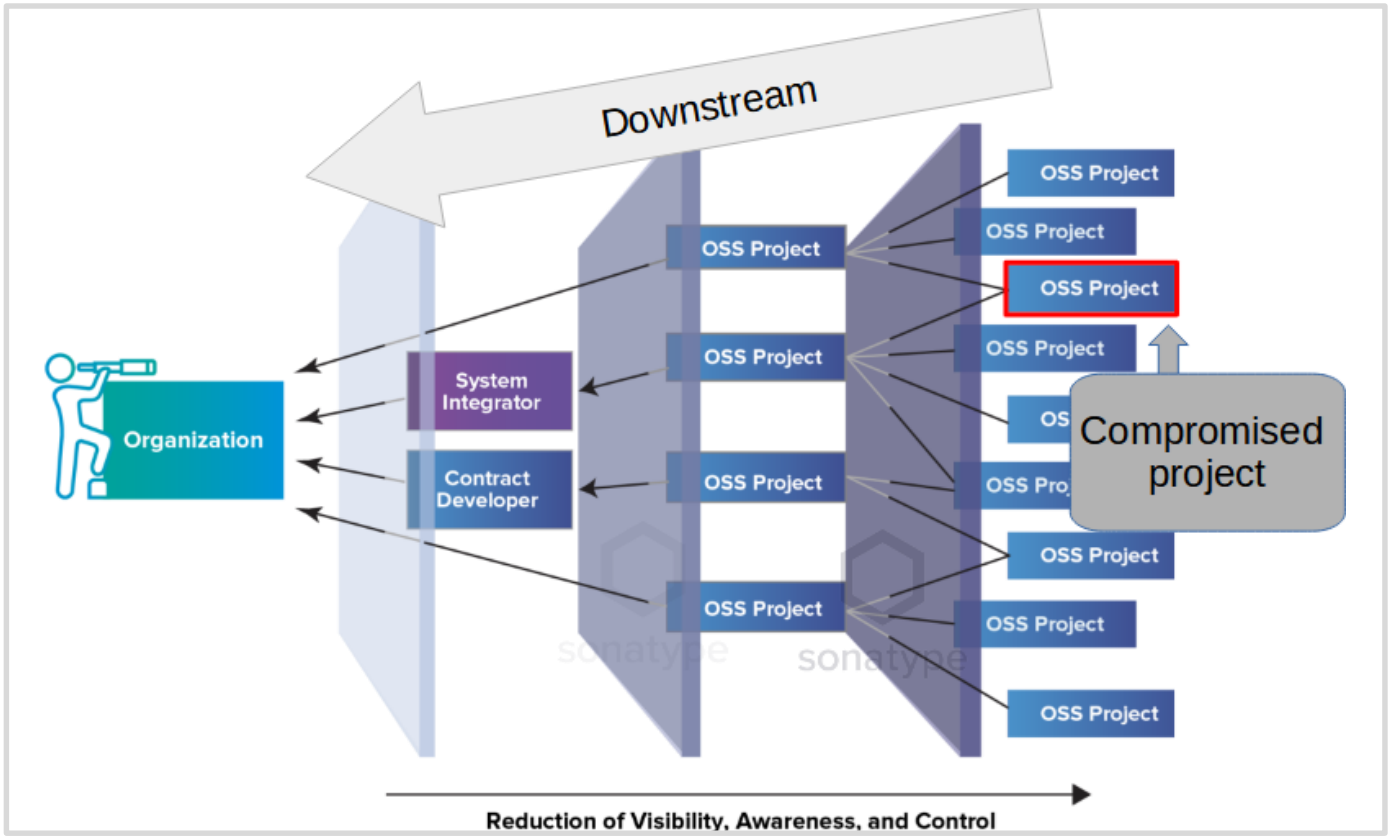
❖ Repository Manager가 필요한 이유

- 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

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

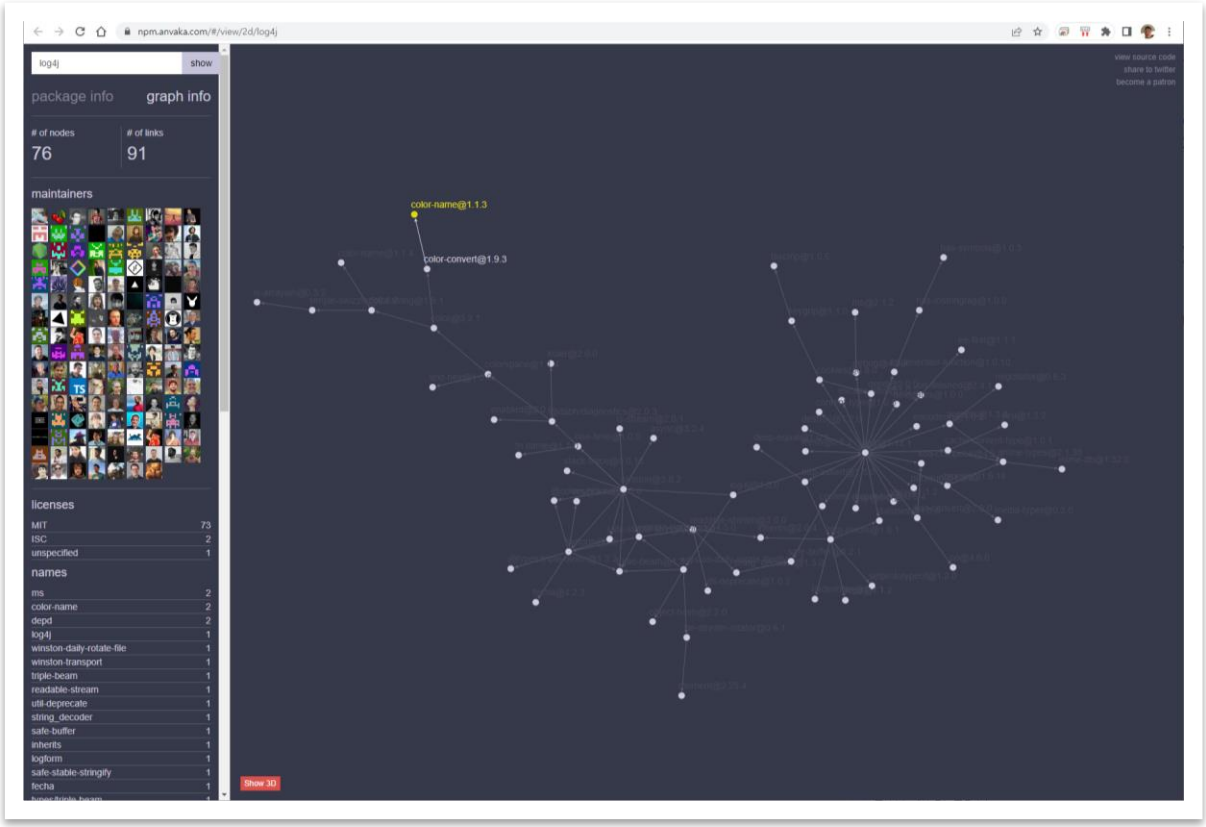
❖ 식별방식

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

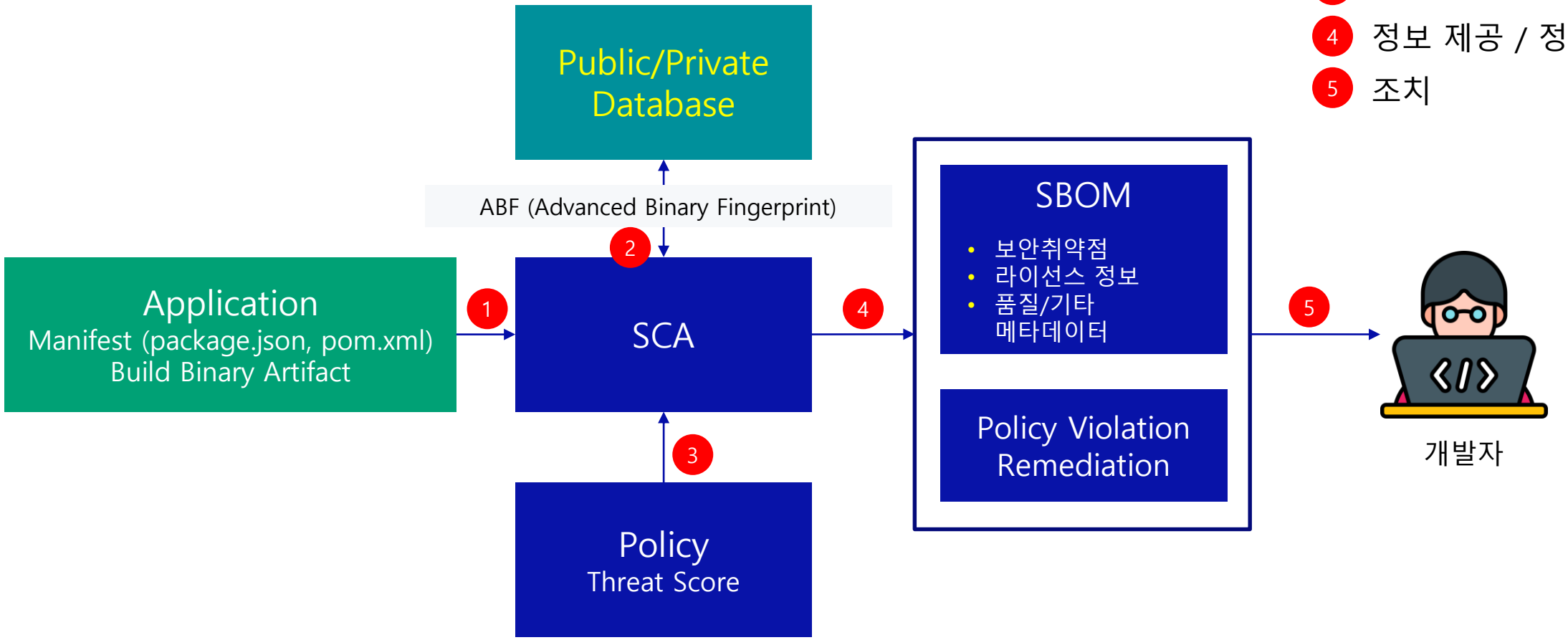


http://npm.anvaka.com/#/view/2d/log4j

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

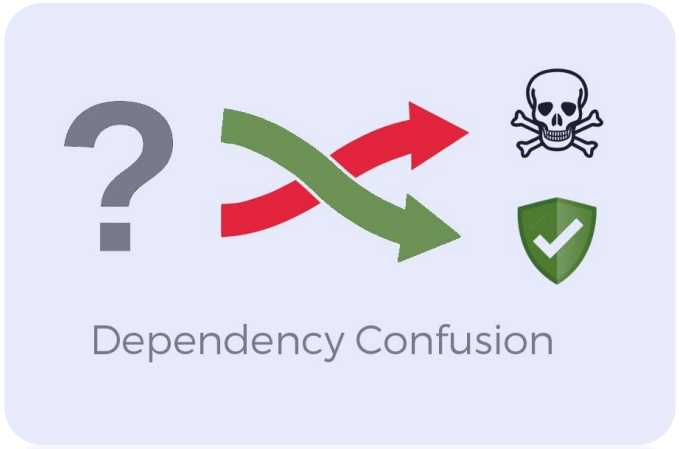


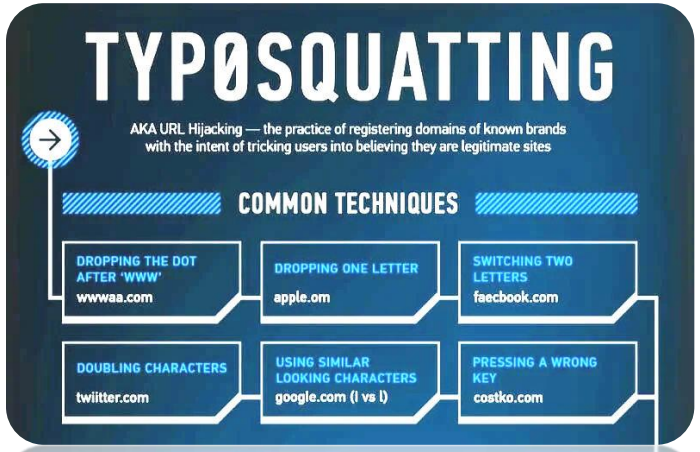
CVE 한계 및 공급망 공격의 고도화

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

Common Vulnerabilities and Exposures





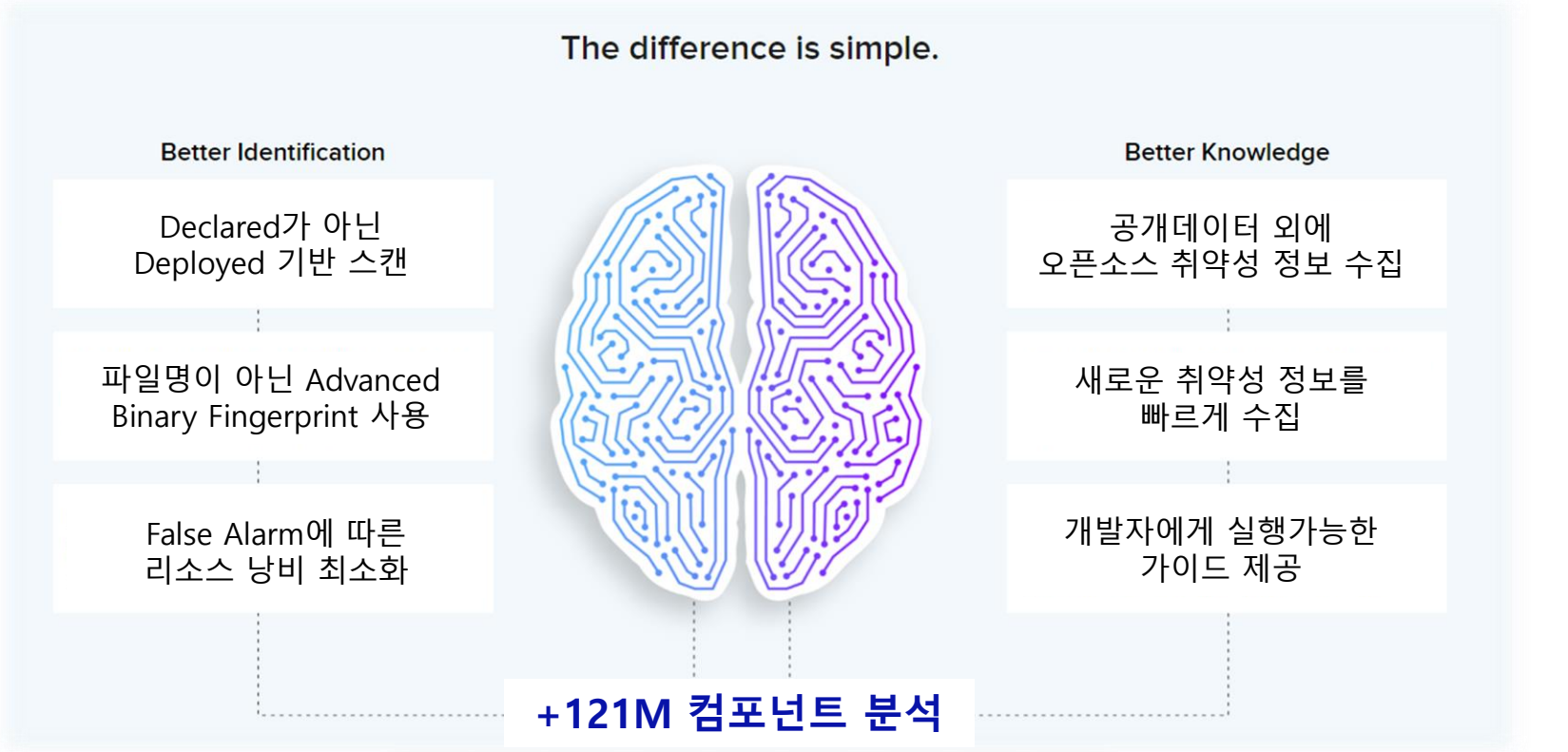
Nexus Intelligence

Nexus Platform은 글로벌 최대 데이터베이스를 기반으로 가장 정확한 정보를 빠르게 제공합니다

경쟁사 대비
70% 많은 취약성 DB

NVD 대비
10배 빠른 속도

65명의 글로벌
보안 전문연구원



Central Repository
Sonatype Research
National Vulnerability Database
GitHub
OSS Index
Nexus Repository
Google Search Alerts
Security Advisories

Nexus Intelligence

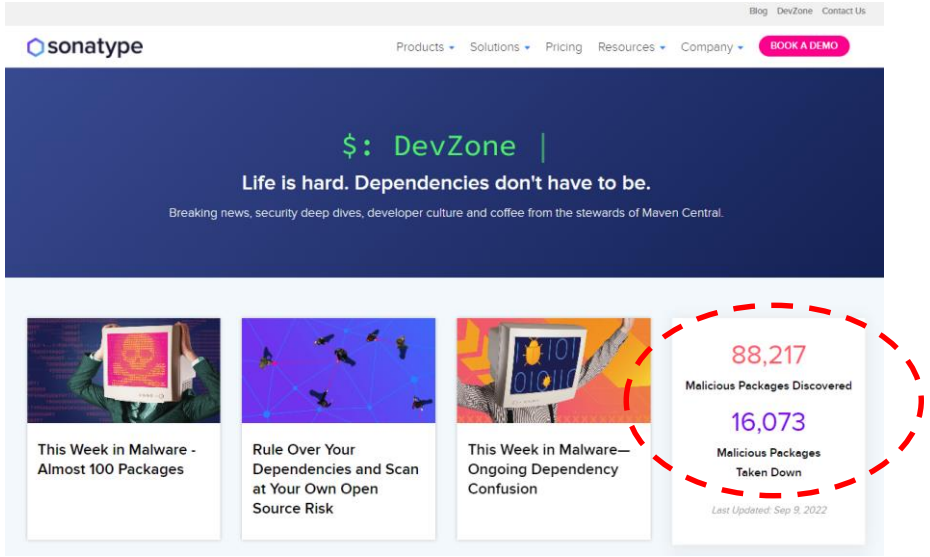
경쟁사 대비
70% 많은 취약성 DB

NVD 대비
10배 빠른 속도

65명의 글로벌
보안 전문연구원

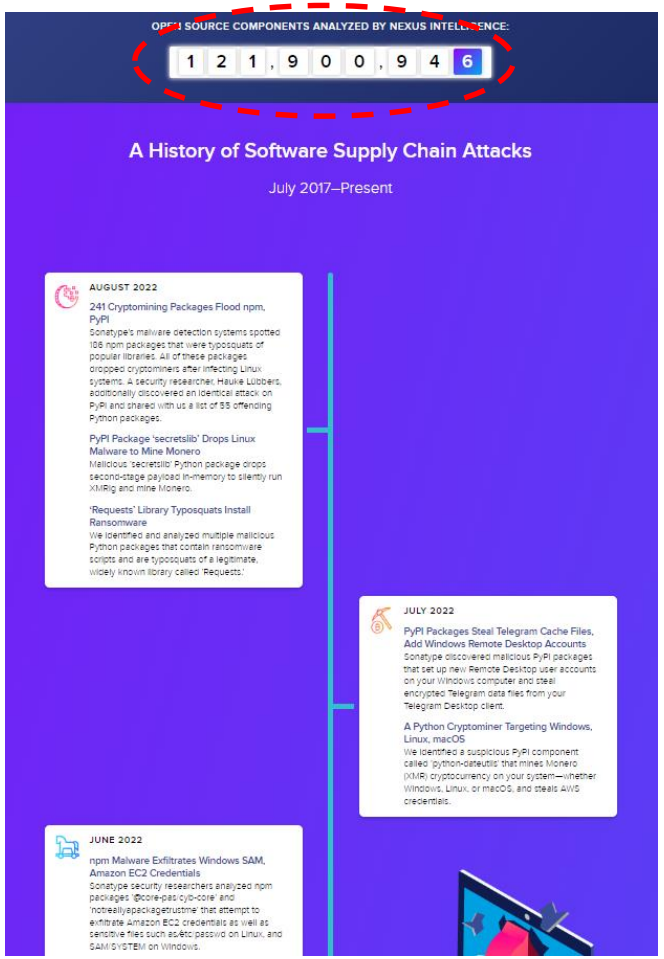
Nexus Platform은 글로벌 최대 데이터베이스를 기반으로 가장 정확한 정보를 빠르게 제공합니다

https://dev.sonatype.com/

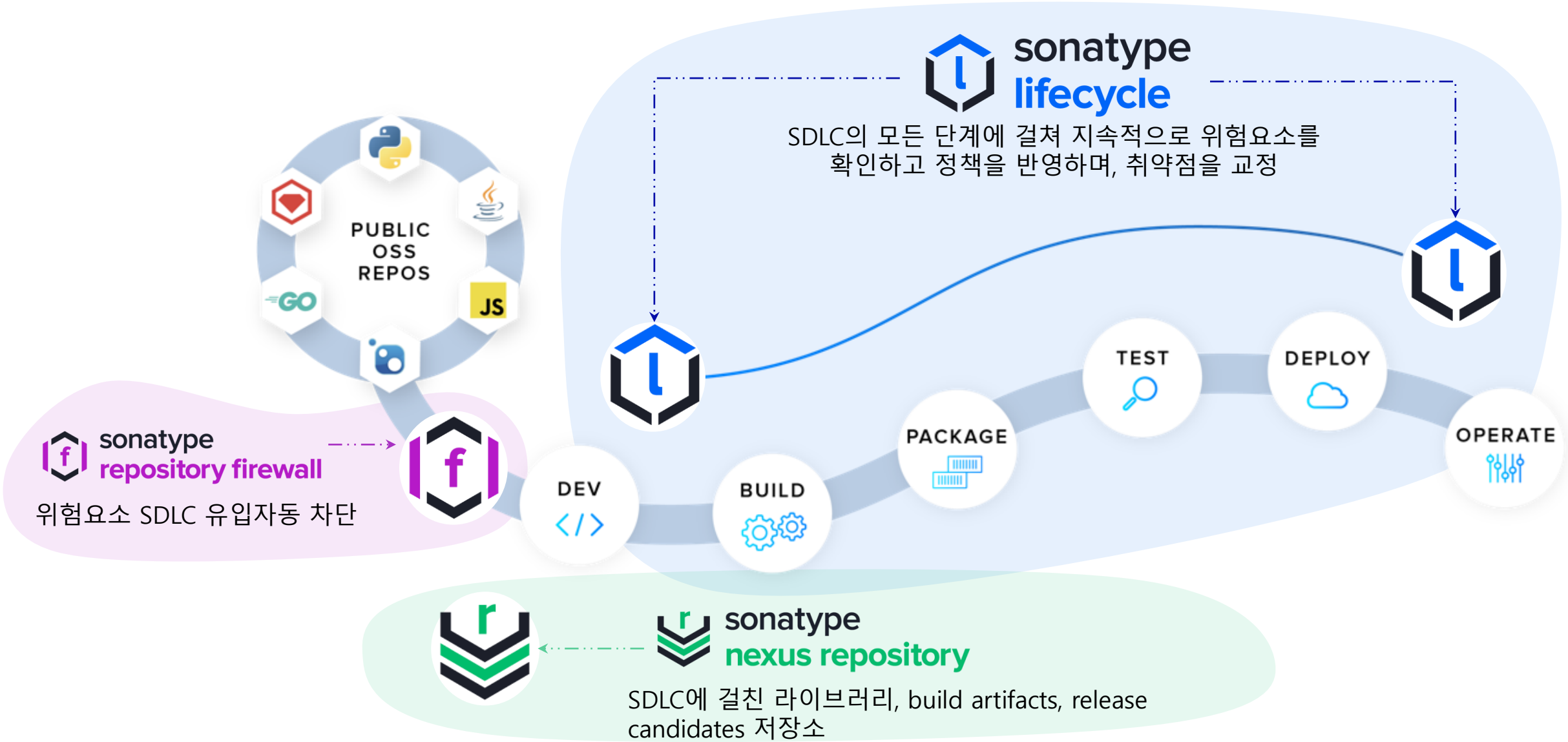


- Advisory 출처 : Sonatype 또는 NVD
- 이슈 심각도 : CVSS 스코어, 출처 및 버전
- CWE (Common Weakness Enumeration)
- Advisory 의 Risk에 대한 세부 추가 설명
- 취약 여부 판단방법
- 수정 및 우회 안(Workaround)에 대한 권고
- 근본 원인 (root cause) : 코드내 취약한 버전 및 클래스
- 공개된 공격요소 및 취약점에 대한 추가 정보

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



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

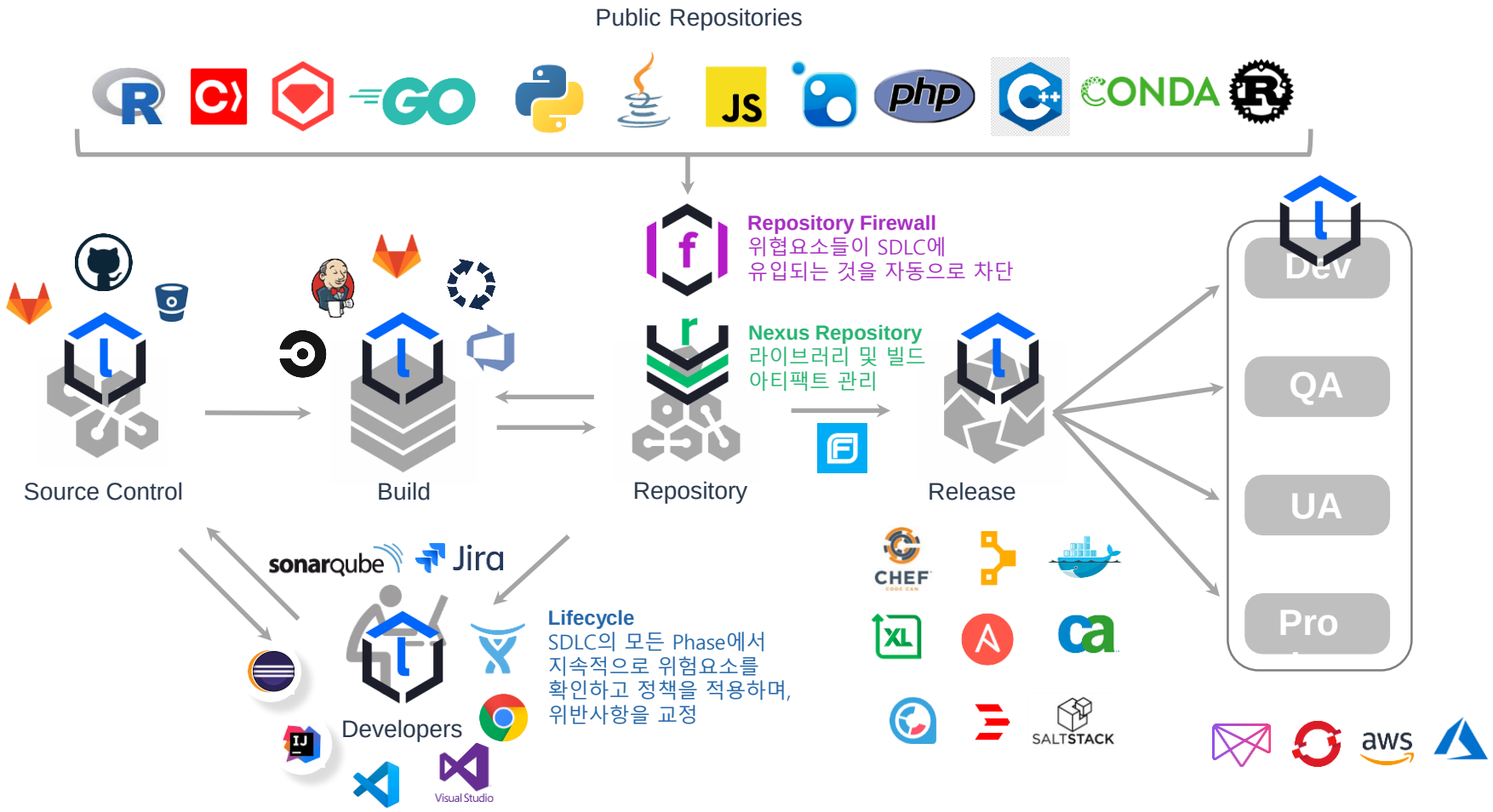
- 바이너리 리포지토리(저장소)를 통해 안정적인 빌드 제공
- Production/Legacy 어플리케이션을 위한 SBOM 생성
- 새로운 위험요소에 대해 지속적인 모니터링

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

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

사전 정합

현업에서 사용하는
대부분의 툴을
Out-of-Box로 지원



https://www.sonatype.com/products/language-and-package-support https://www.sonatype.com/products/integratio

지원 언어 및 패키지

다양한 언어 및 패키지 지원

https://www.sonatype.com/products/language-and-package-support

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)	●	● (EPEL)	

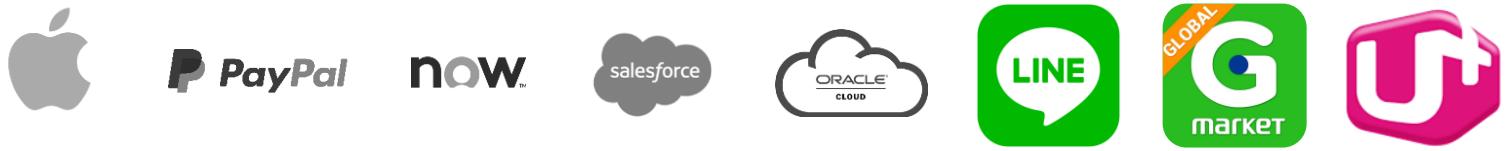
PACKAGE	sonatype nexus repository	sonatype repository firewall	sonatype lifecycle
APK (Alpine)	● via Community	●	●
APT (Debian)	●	●	●
Bower	●	●	
Cargo		●	●
CocoaPods	●	●	●
Composer	● via Community	●	●
CONAN	●	●	●
Conda	●	●	●
CPAN	● via Community		
Docker	●		●
Drupal		●	●
ELPA	● via Community		
Go Modules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

주요 고객사

2,000여 고객사(1,500만 개발자)를 통해 검증된 솔루션

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

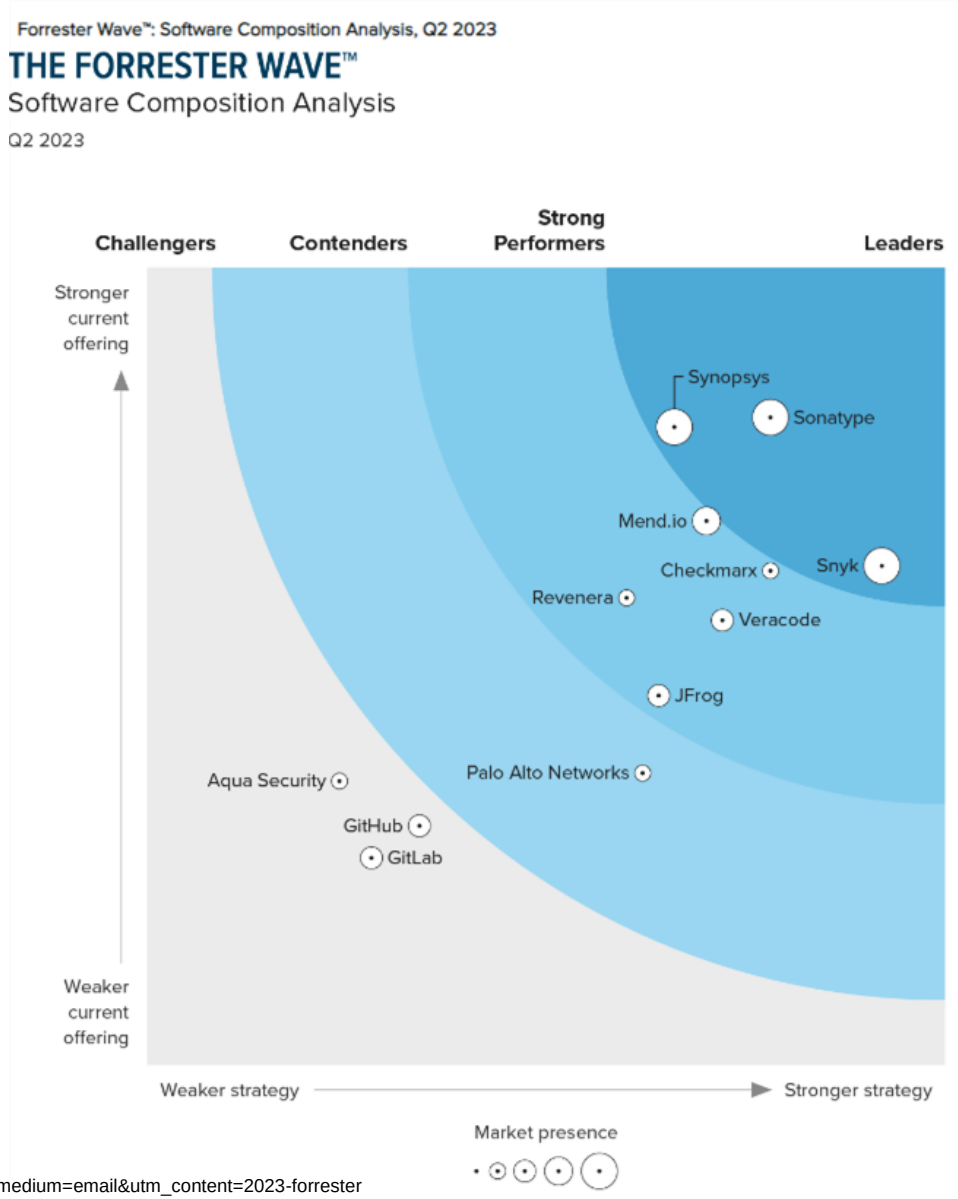
7 of Top 10 US Tech Firms | 4 of 5 US Armed Forces

Fin Serv	
Technology	
Media	
Manufacturing	
Energy	

Software Composition Analysis (SCA)

Forrester Report Q2 2023

	Forrester's weighting	Aqua Security	Checkmarx	GitHub	GitLab	JFrog	Mend	Palo Alto Networks	Revenera	Snyk	Sonatype	Synopsys	Veracode
Current offering	50%	1.78	3.10	1.50	1.30	2.32	3.41	1.83	2.93	3.13	4.06	4.00	2.79
Vulnerability identification	15%	1.60	3.00	1.60	1.60	3.00	3.00	1.00	3.00	1.60	5.00	3.60	3.60
License risk management	10%	0.70	2.10	0.70	1.00	1.00	3.00	0.70	5.00	1.00	5.00	4.40	1.00
SBOM management	10%	3.00	2.40	1.00	0.80	2.40	3.40	2.40	5.00	2.60	3.00	5.00	2.60
Development, security, and operations	10%	1.90	3.30	1.20	1.60	2.30	3.00	2.40	1.50	3.70	3.90	3.30	2.00
Software supply chain security	10%	2.40	2.60	2.60	0.20	3.00	2.60	0.90	0.70	3.40	5.00	3.60	0.70
Policy management	5%	1.00	3.00	1.00	1.00	3.00	3.00	1.00	3.00	3.00	5.00	5.00	3.00
Remediation	30%	1.80	3.80	1.50	1.50	2.50	4.30	2.70	2.50	4.60	3.70	4.00	3.60
Reporting and analytics	5%	1.00	3.00	1.00	1.00	1.00	3.00	1.00	5.00	3.00	3.00	3.00	5.00
Breadth of coverage	5%	2.00	3.40	3.20	3.00	1.00	3.40	2.60	2.20	2.80	2.20	4.60	2.80
Strategy	50%	1.20	3.90	1.70	1.40	3.20	3.50	3.10	3.00	4.60	3.90	3.30	3.60
Vision	25%	1.00	3.00	1.00	1.00	3.00	5.00	3.00	3.00	5.00	5.00	3.00	5.00
Execution roadmap	20%	1.00	5.00	3.00	1.00	5.00	3.00	3.00	3.00	3.00	3.00	3.00	1.00
Planned enhancements	20%	1.00	3.00	1.00	3.00	3.00	3.00	5.00	3.00	5.00	3.00	3.00	3.00
Innovation	10%	3.00	5.00	1.00	1.00	3.00	3.00	3.00	3.00	5.00	5.00	3.00	5.00
Supporting services and offerings	15%	1.00	5.00	3.00	1.00	3.00	3.00	1.00	3.00	5.00	3.00	5.00	5.00
Pricing flexibility and transparency	10%	1.00	3.00	1.00	1.00	1.00	3.00	3.00	3.00	5.00	5.00	3.00	3.00
Market presence	0%	2.00	2.00	3.00	3.00	3.00	3.20	1.20	1.80	4.60	4.60	4.60	2.80
Revenue	60%	2.00	2.00	3.00	3.00	3.00	3.00	1.00	2.00	5.00	5.00	5.00	3.00
Number of customers	20%	1.00	2.00	4.00	5.00	5.00	2.00	1.00	1.00	5.00	4.00	3.00	4.00
Average deal size	20%	3.00	2.00	2.00	1.00	1.00	5.00	2.00	2.00	3.00	4.00	5.00	1.00

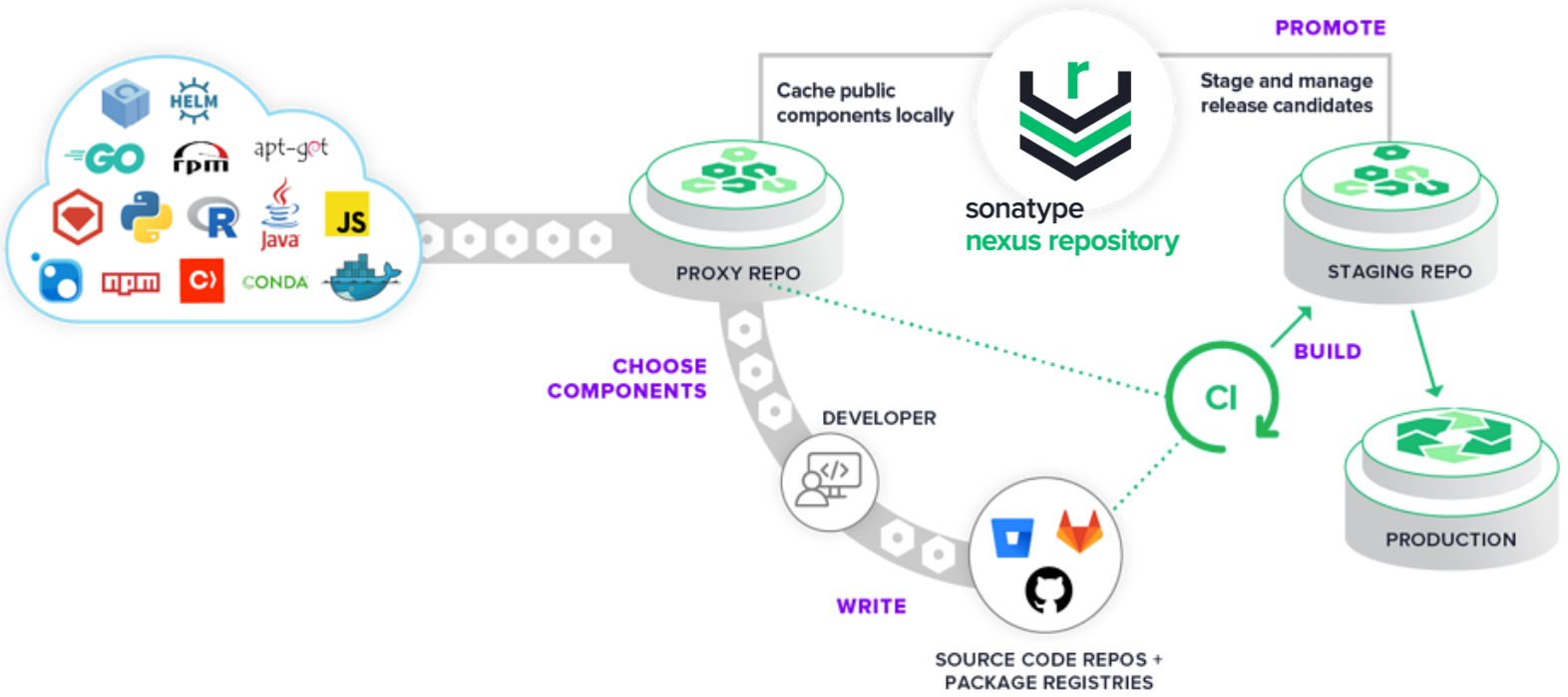


https://reprints2.forrester.com/#/assets/2/425/RES178483/report?utm_campaign=q2%202023%20na%20forrester-sca-wave&utm_source=sales-email&utm_medium=email&utm_content=2023-forrester

sonatype
nexus repository pro

World #1 Repository Manager

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



다양한 개발자 도구 및 에코시스템 지원

sonatype nexus repository pro

World #1 Repository Manager

주요 기능 (Nexus Repository OSS 대비)

Import/ Export
- Repository간 컴포넌트 이동
- Disconnected 망 환경 지원

고급 Blob Store 관리
- 복수의 Blob Store (Group Blob Stores)를 단일 Blob Store로 활용
- Dynamic Storage

User Token
- Username/Password 대신 토큰을 사용하여 빌드 시스템 접근 지원
- LDAP등 SSO 솔루션에 활용

Tagging
- 컴포넌트의 조합을 논리적으로 묶어 관리 – CI Build ID, Release Train 등

Group Deployment
- Pull/Push 컨텐츠에 단일 URL 사용

기술 지원
- Standard/Extended 기술지원
- 장애 대응 및 자문/코칭 서비스

외부 Database
- 내장 DB(OrientDB)외에 외부 PostgreSQL 지원
- 성능 및 안정성, 관리기능 향상

Staging & Build Promotion
- Staging Repository 구분을 통해 DEV/UAT/PRD등 접근제어

SAML SSO
- SAML IdP 연동을 통해 인증/인가 통합 지원

Health Check
- 오픈소스 보안 취약점 및 라이선스 정보 제공

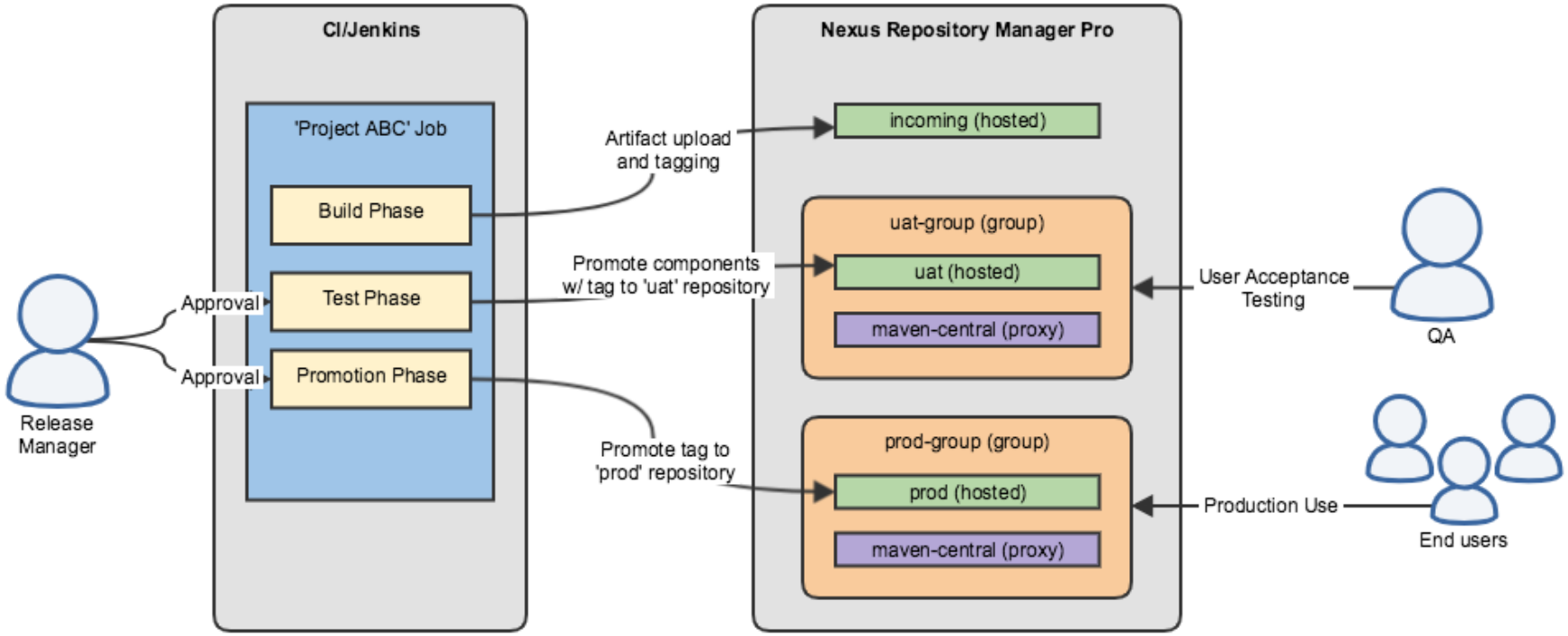
HA & Backup
- HA, 백업/복구 등 Resilient 아키텍처 구성 지원

Crowd SSO 인증
- Atlassian Crowd를 통한 SSO 인증 지원

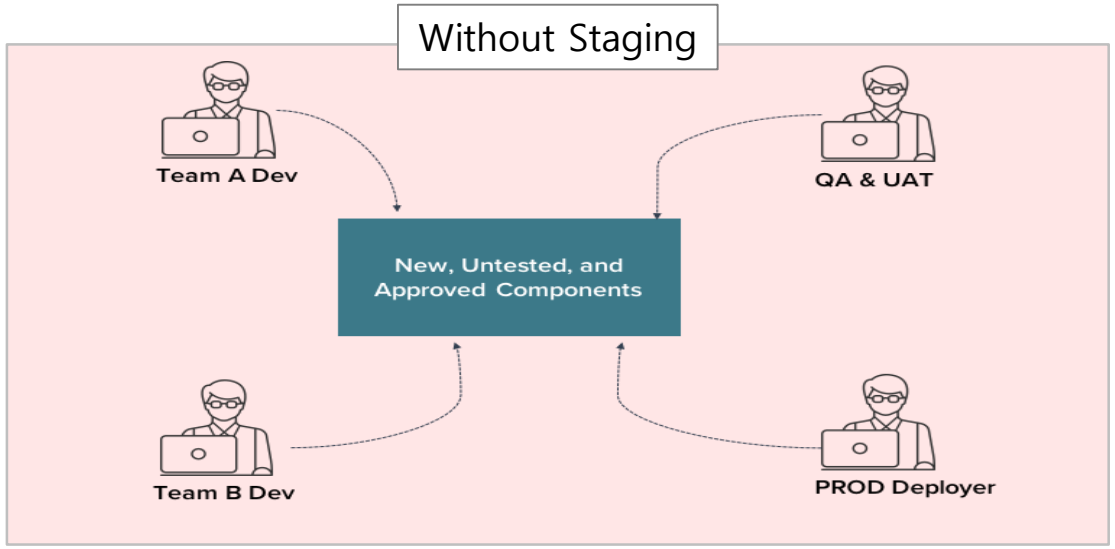
https://help.sonatype.com/repomanager3/repository-manager-pro-features
https://www.sonatype.com/products/repository-oss-vs-pro-features

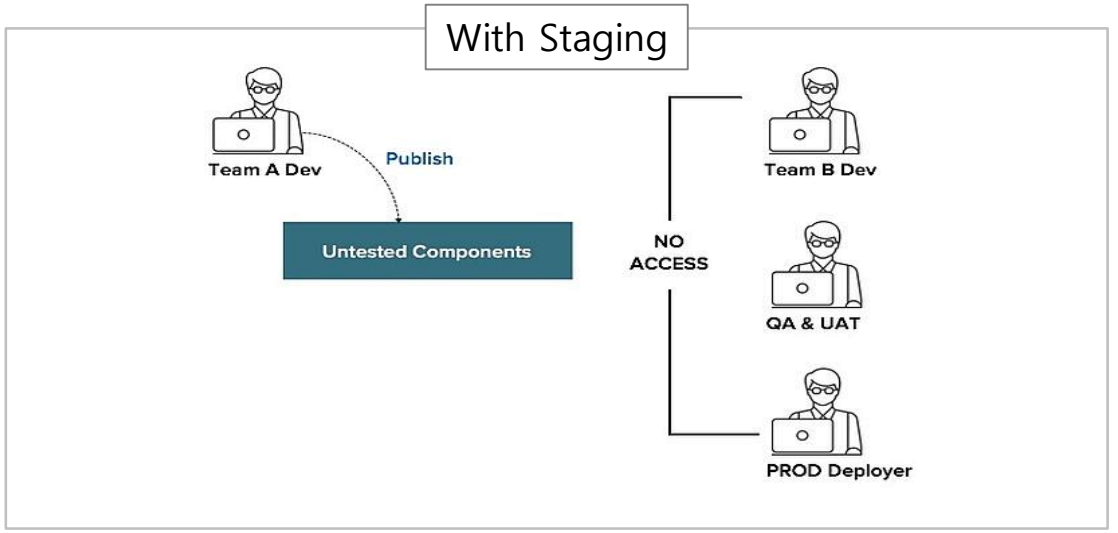
전형적인 Staging Workflow

- 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

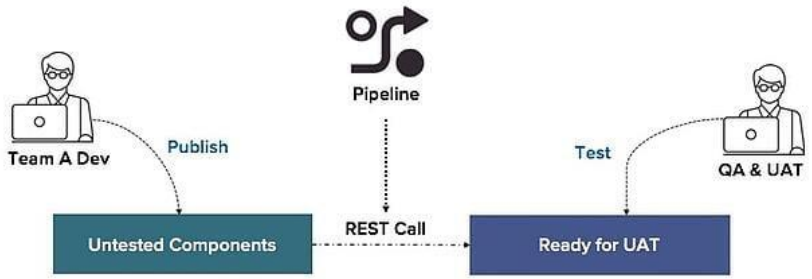


Staged Workflow (Staging and Tagging)

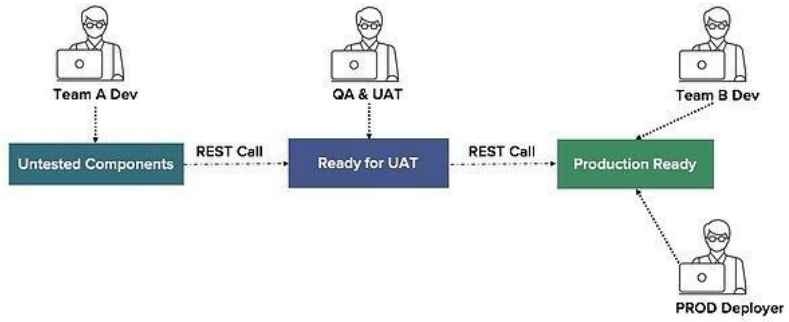




최초 Publish 단계에서 Tagging을 사용하여 Pipeline (e.g. Jenkins)에서 단일 REST Call을 통해 컴포넌트 이동

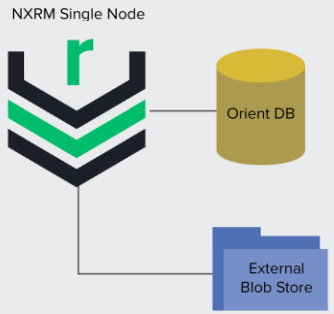


Release Manager는 단계별 승인과정을 통해 Pipeline에 필요한 접근권한을 통제

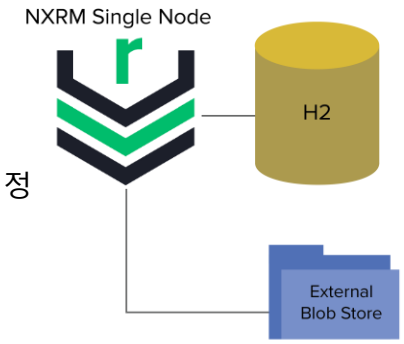


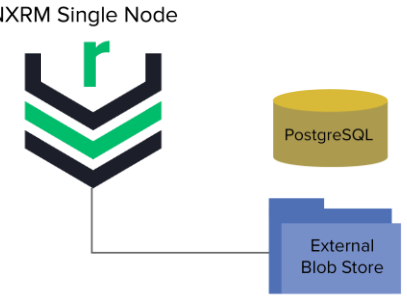
External Database 사용 지원

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



OrientDB는 H2로 대체 예정



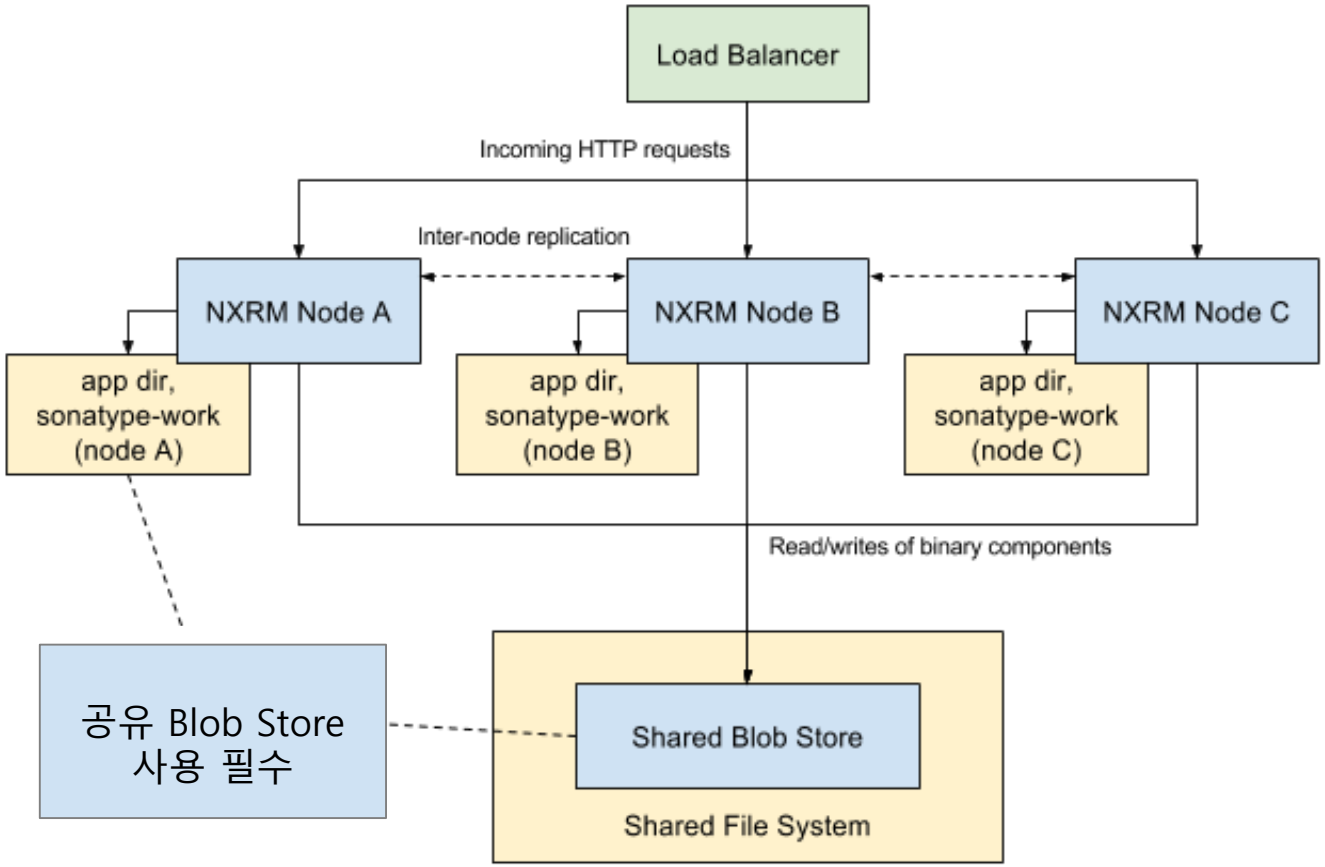


외부 PostgreSQL 대체 사용

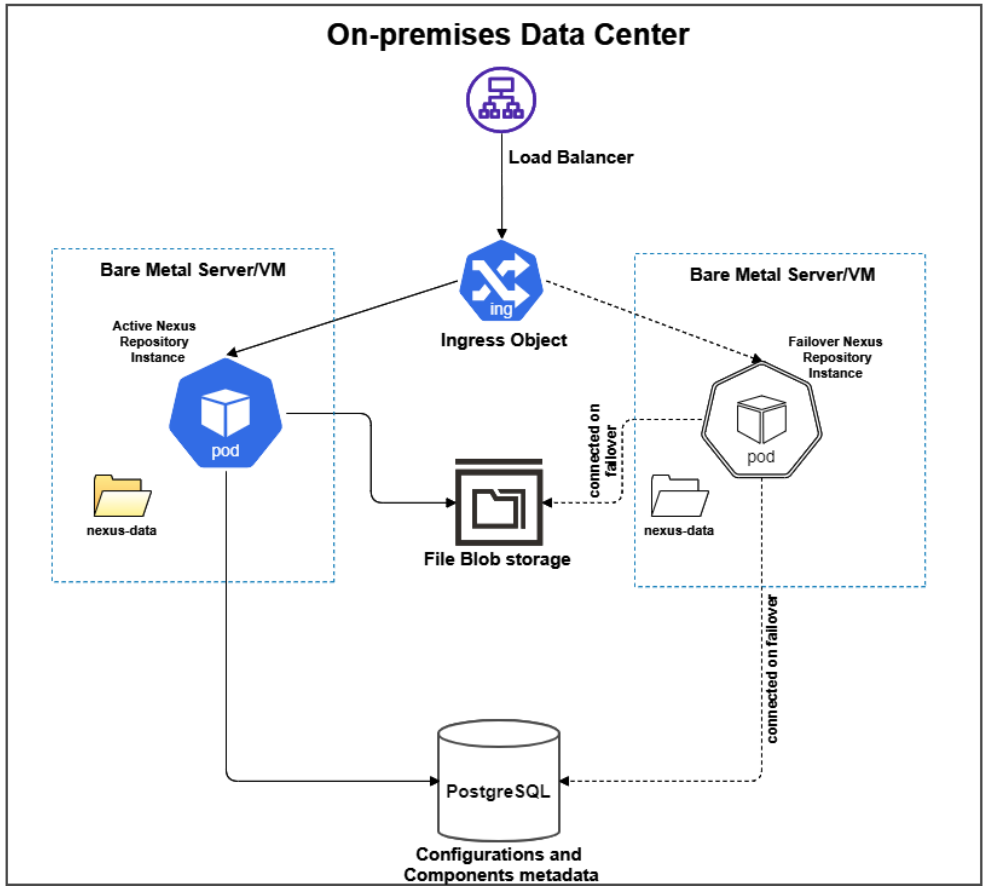
- 성능 및 확장성 향상
- AWS Aurora, RDS 및 Azure Database 등 관리형 데이터베이스 사용 가능
- K8s/Rancher/OpenShift등 컨테이너 오케스트레이션 도구 호환성 향상
- 백업과정의 가용성 지원
- 다중 가용영역 (Availability Zone) 환경의 결함 허용(Fault-tolerant) 향상
- DR 프로세스 단순화

https://help.sonatype.com/repomanager3/new-database-options

Resiliency 및 HA 구성 지원 (Legacy)



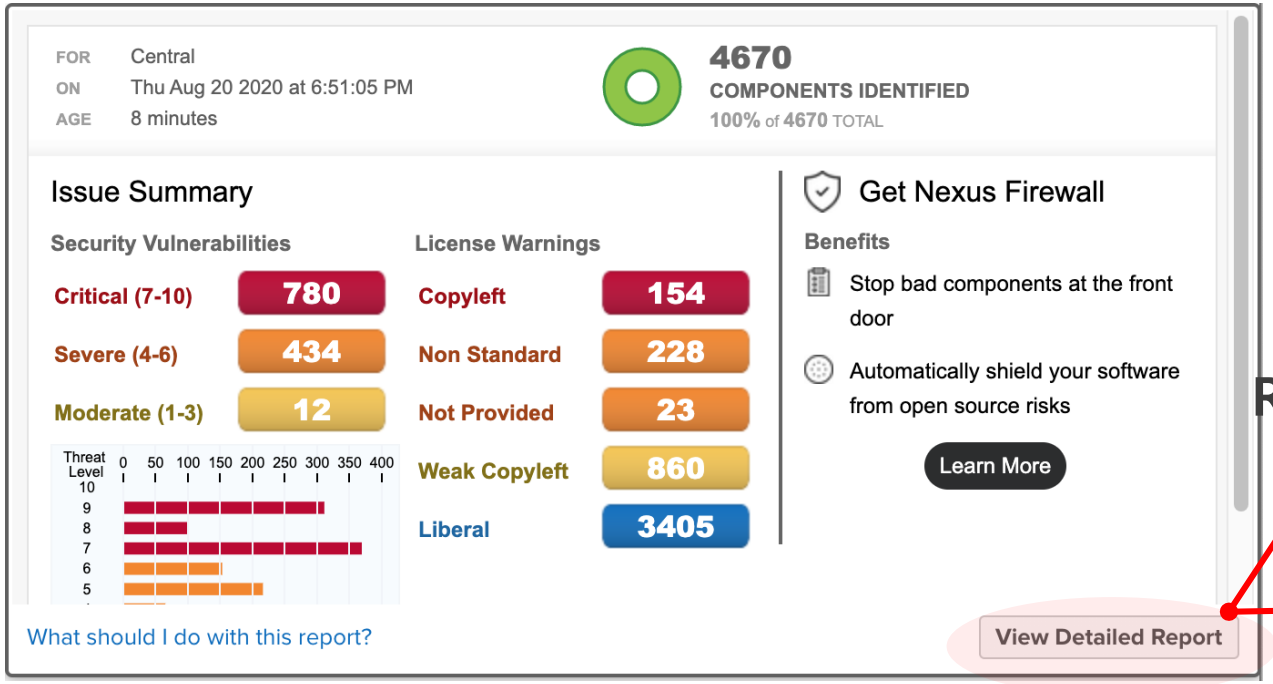
Resiliency 및 HA 구성 지원 (On-Prem using Kubernetes)



sonatype
nexus repository pro

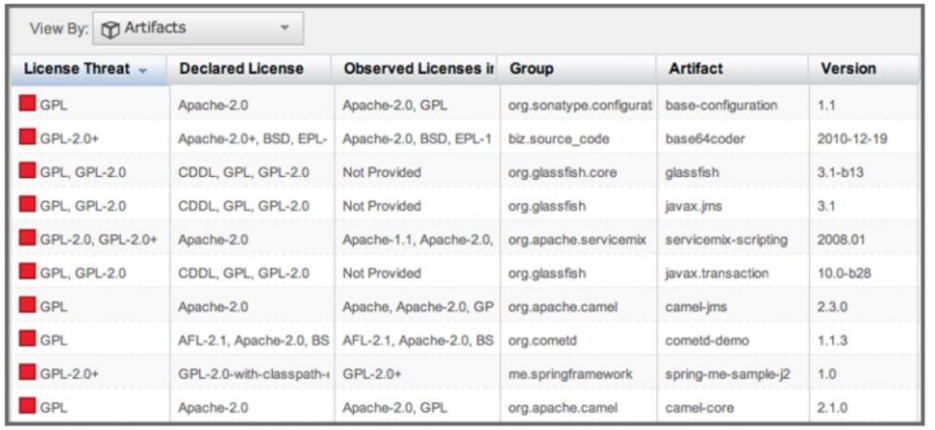
World #1 Repository Manager

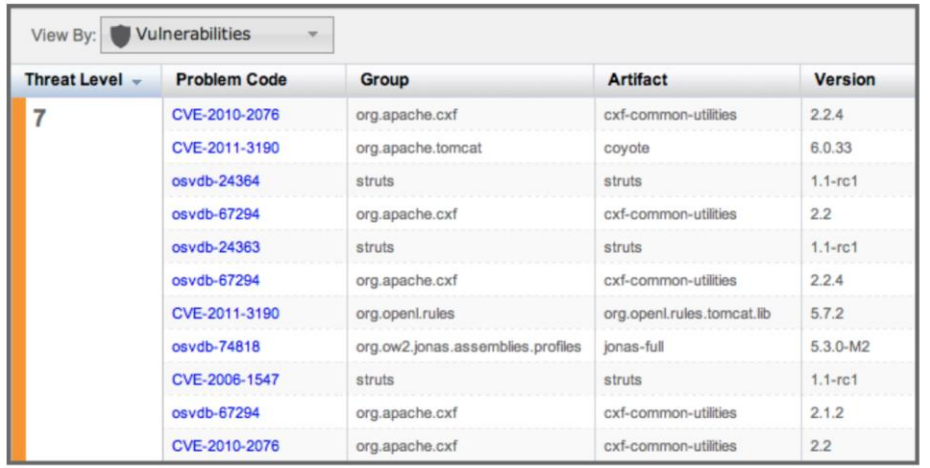
Nexus Repository oss (오픈소스)는 취약점이나 라이선스에 대한
요약정보만 제공하며 Nexus Repository Pro는 세부정보를 추가 제공함



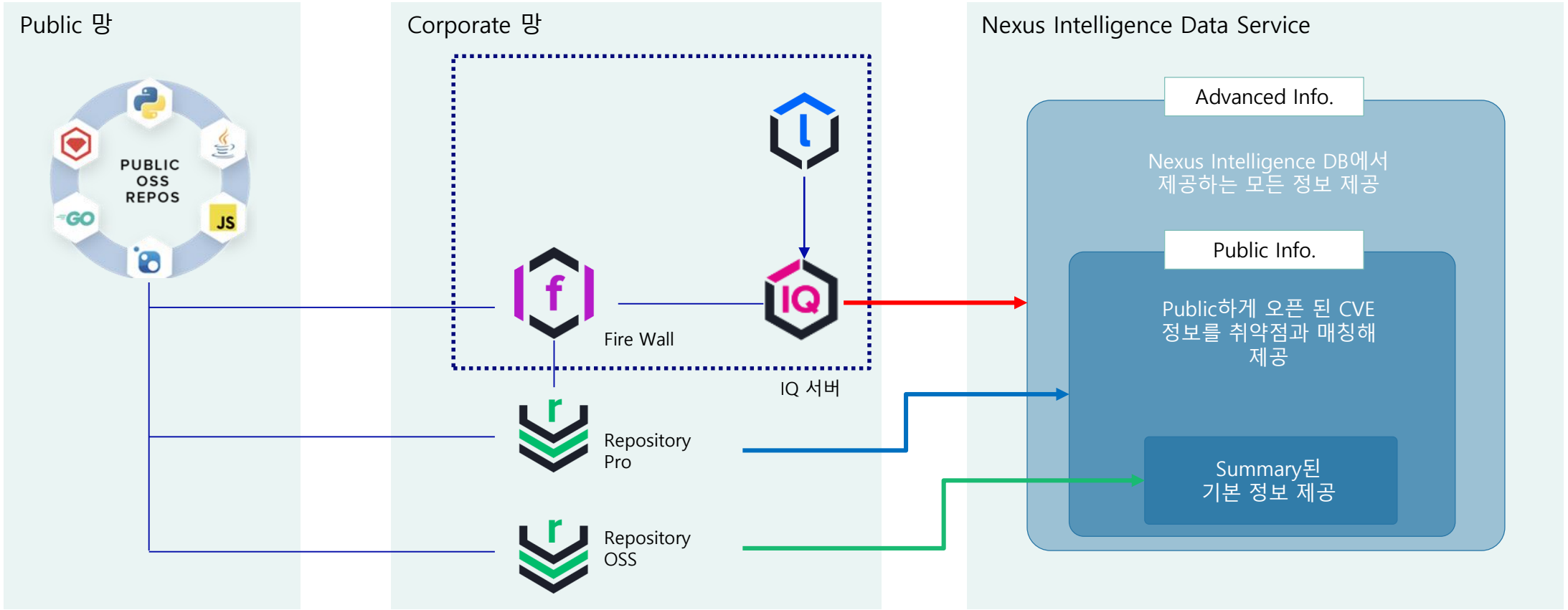
Nexus Repository OSS

Nexus Repository Pro



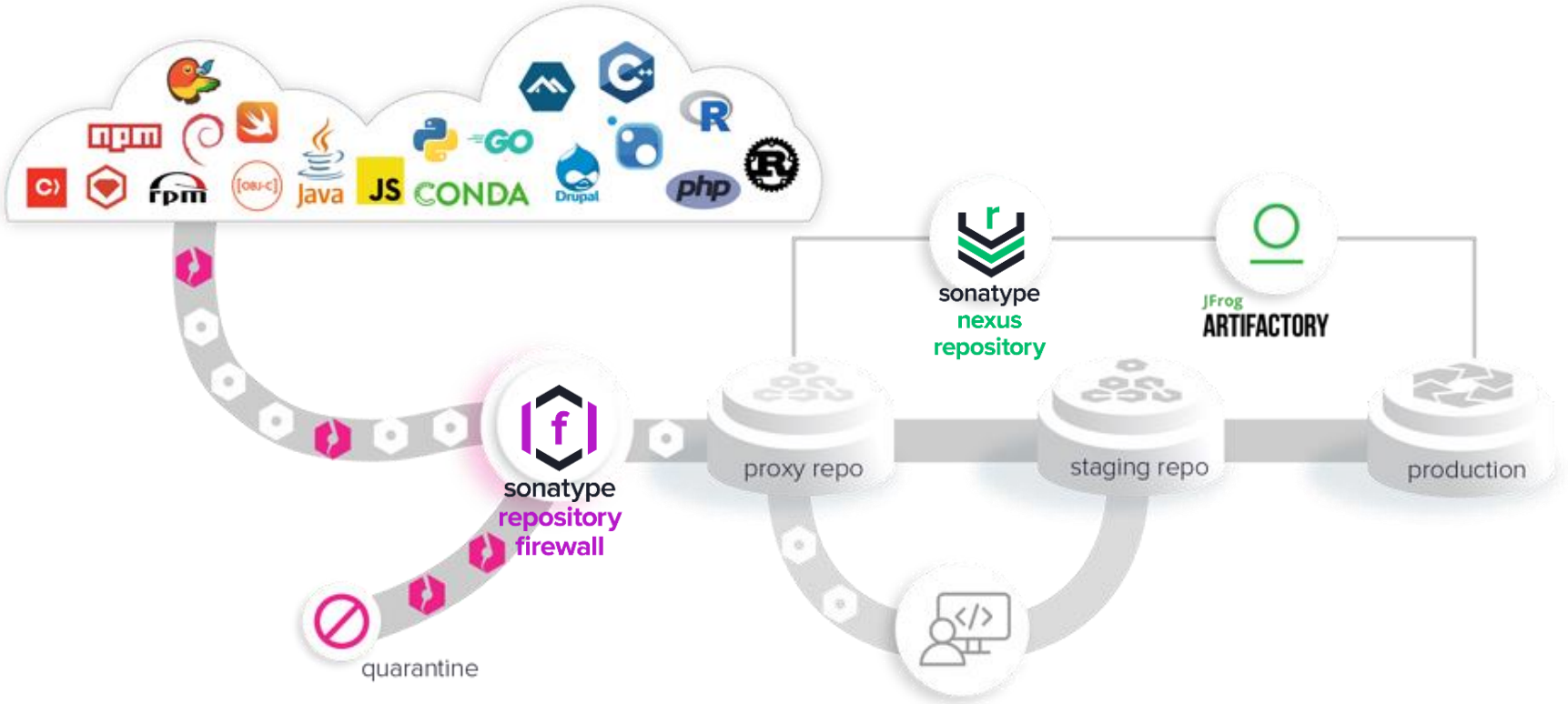


Sonatype 제품의 단계별 취약점 정보 제공



sonatype
repository firewall

Repository Firewall은 취약한 컴포넌트가 SDLC내로 유입되는 것을 차단



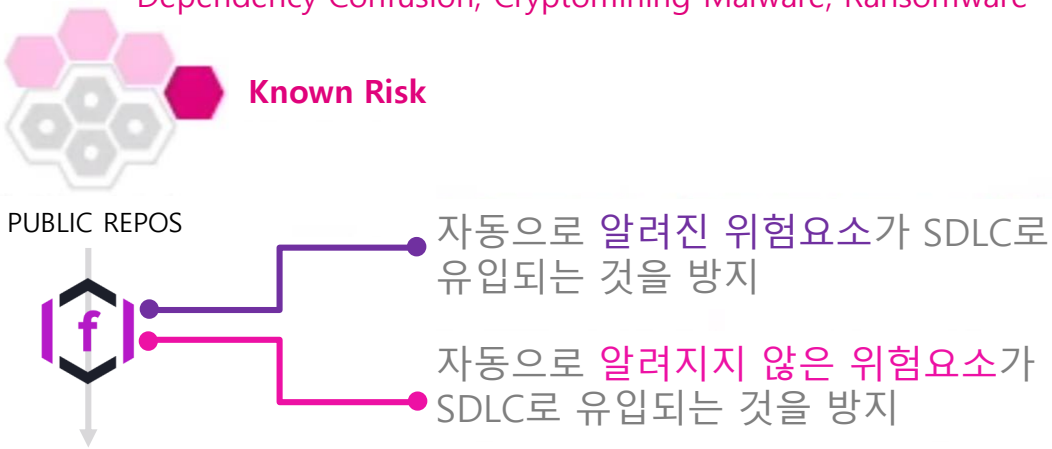
Java, JavaScript, .NET, Python, Go, Ruby, RPM등 다양한 언어 지원

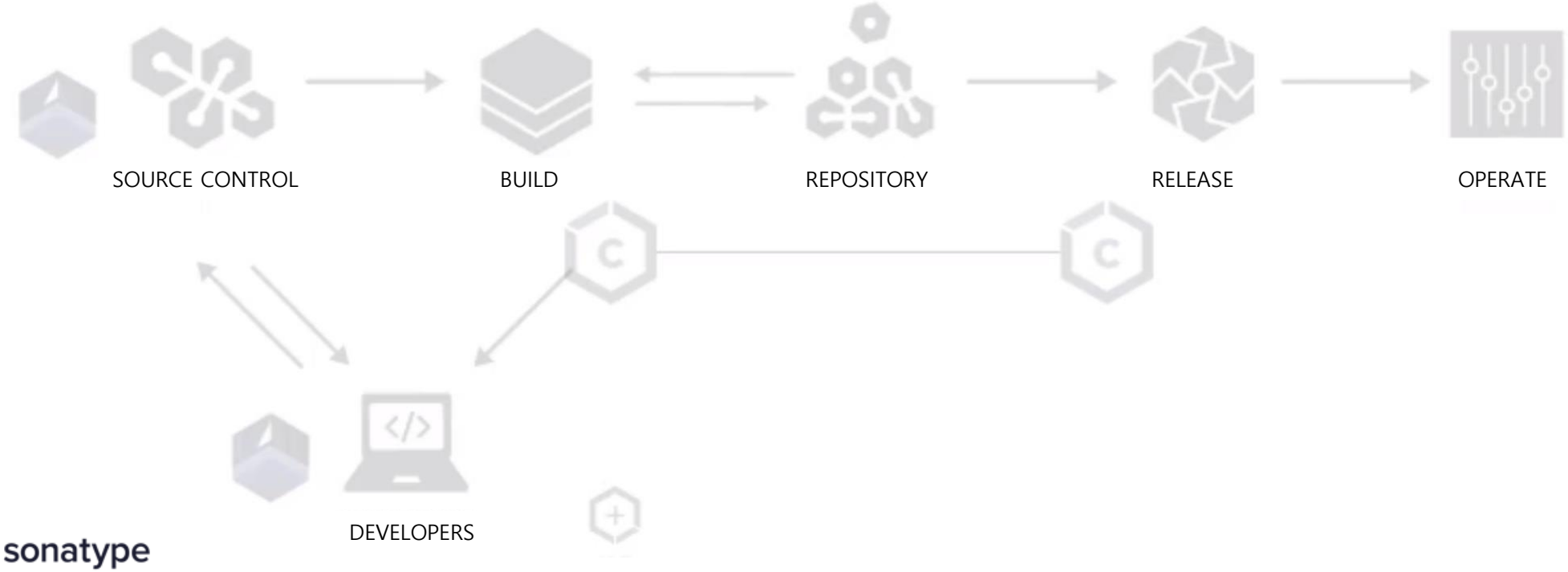
sonatype repository firewall

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

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

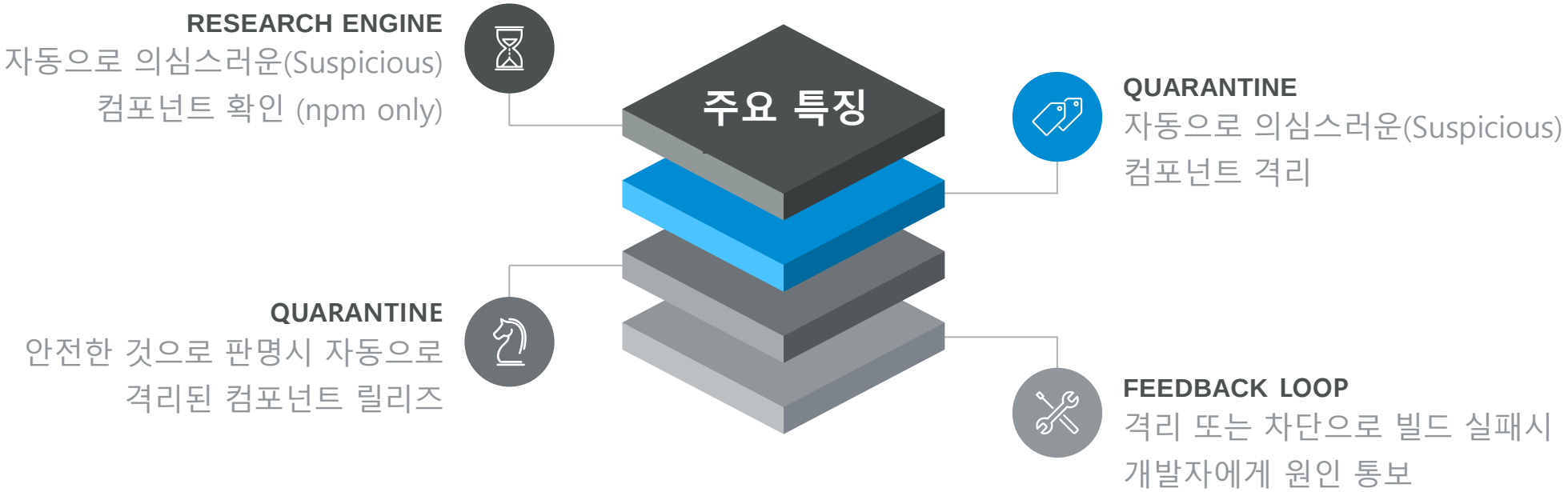
Known Risk





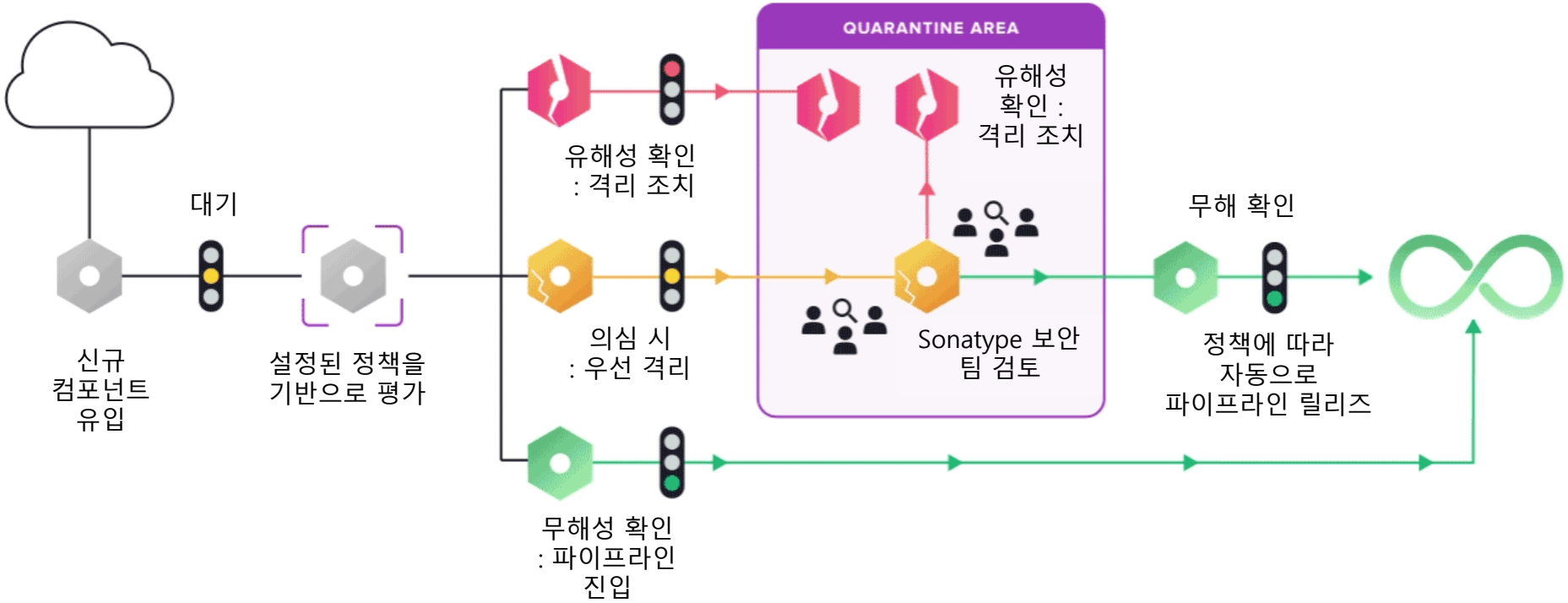
sonatype
repository firewall

알려진 취약점 및 알려지지 않은 취약점까지 선제적으로 방어



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

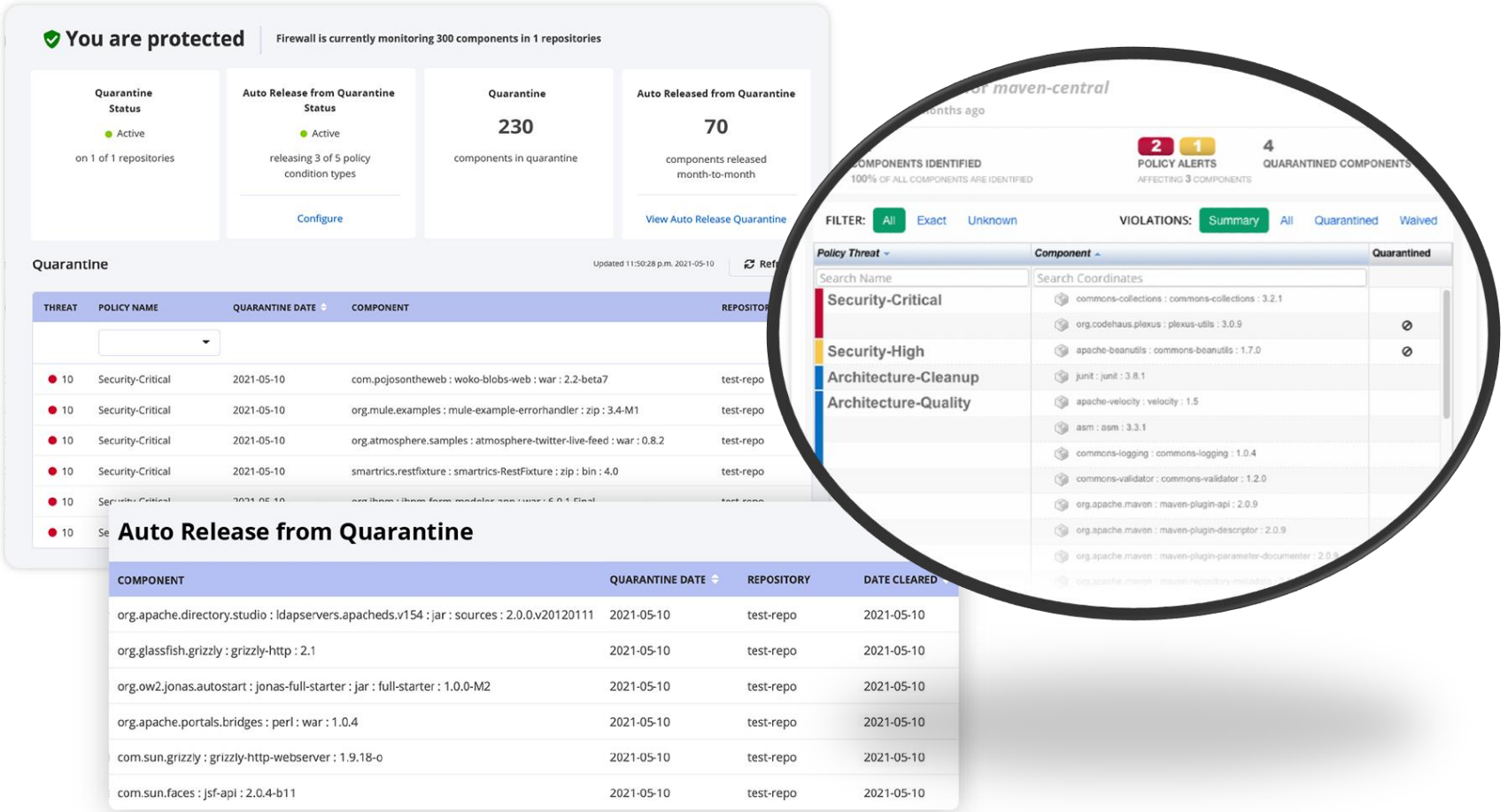
sonatype
repository firewall



- 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

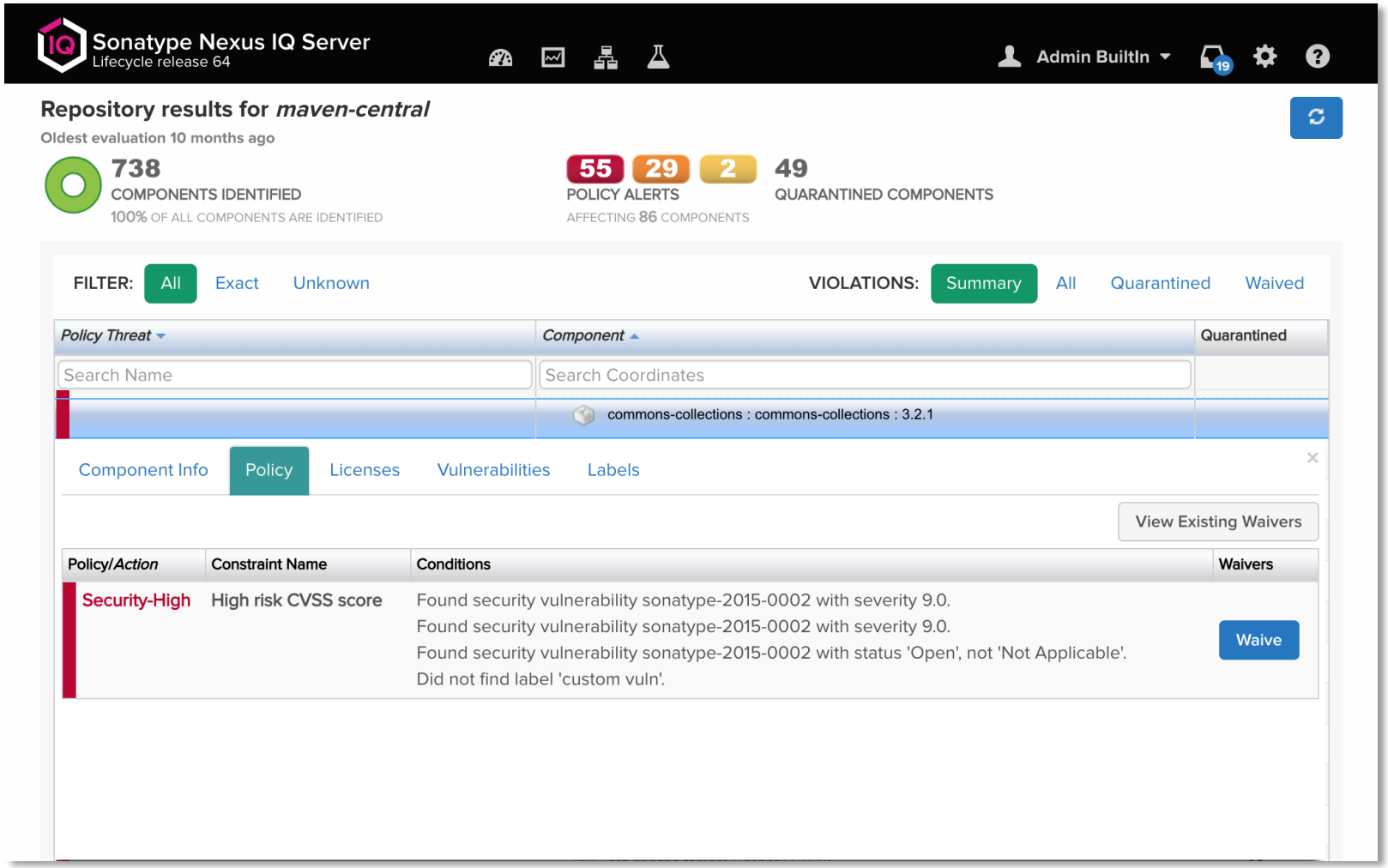
sonatype
repository firewall

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

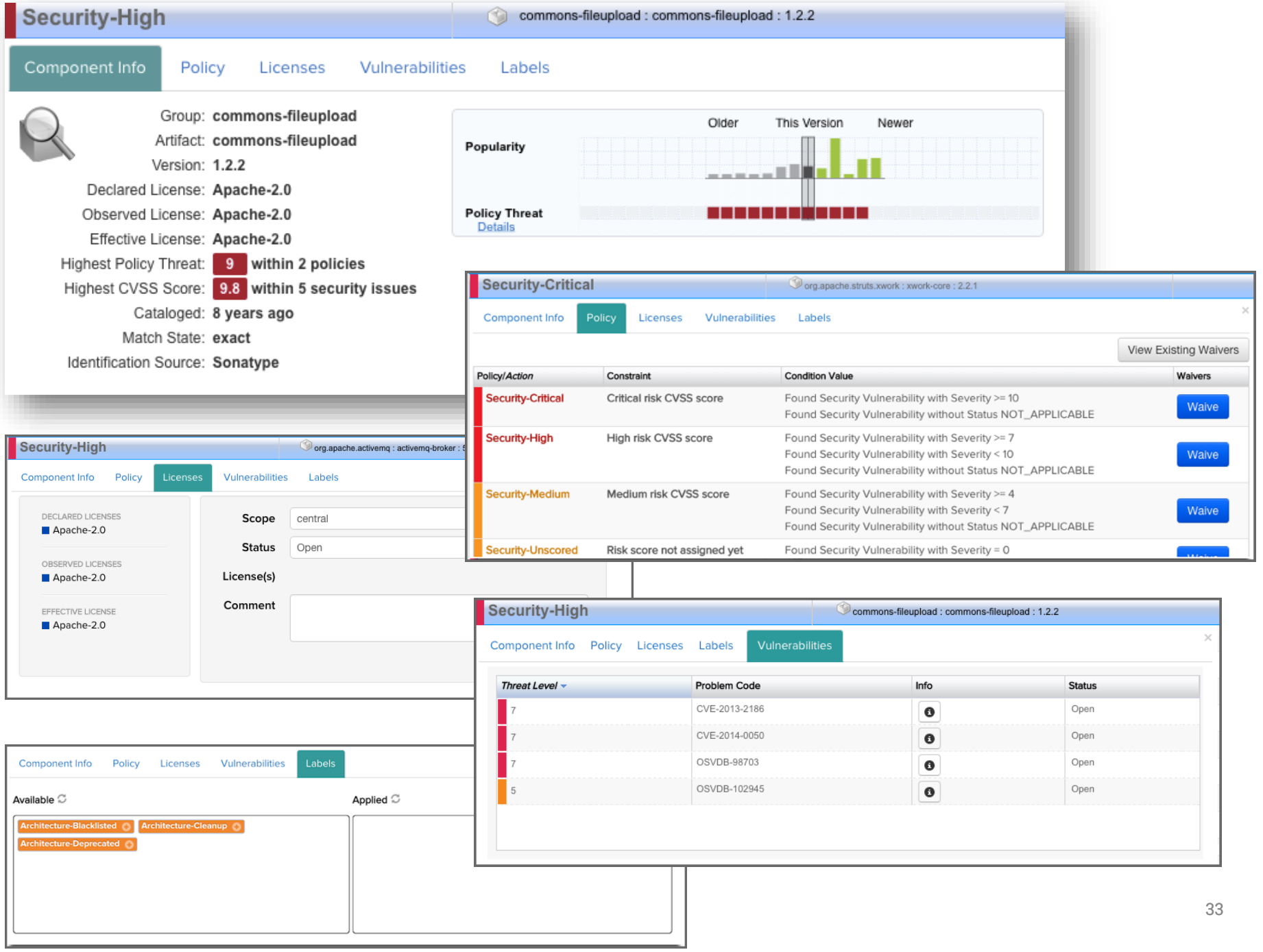


sonatype
repository firewall

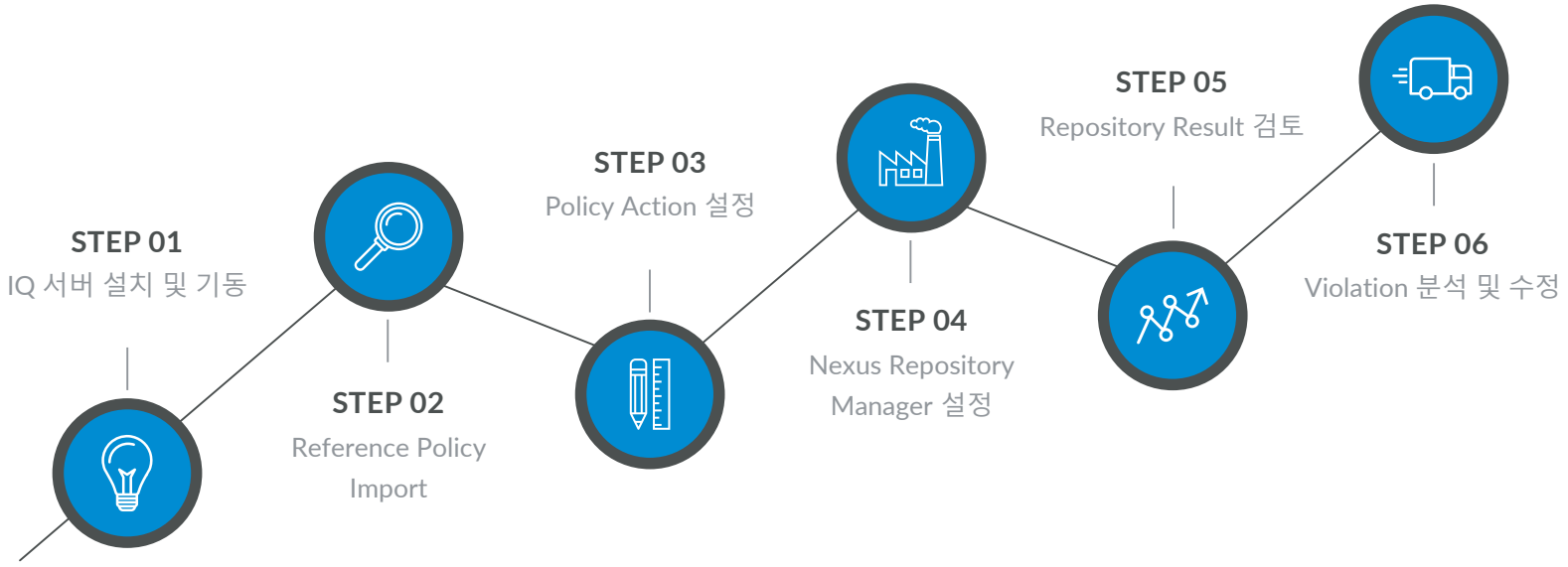
다양한 정책을 반영하여 SDLC 내로 유입되는 컴포넌트를 관리하며 대안 제시



sonatype
repository firewall



Firewall Quick Start

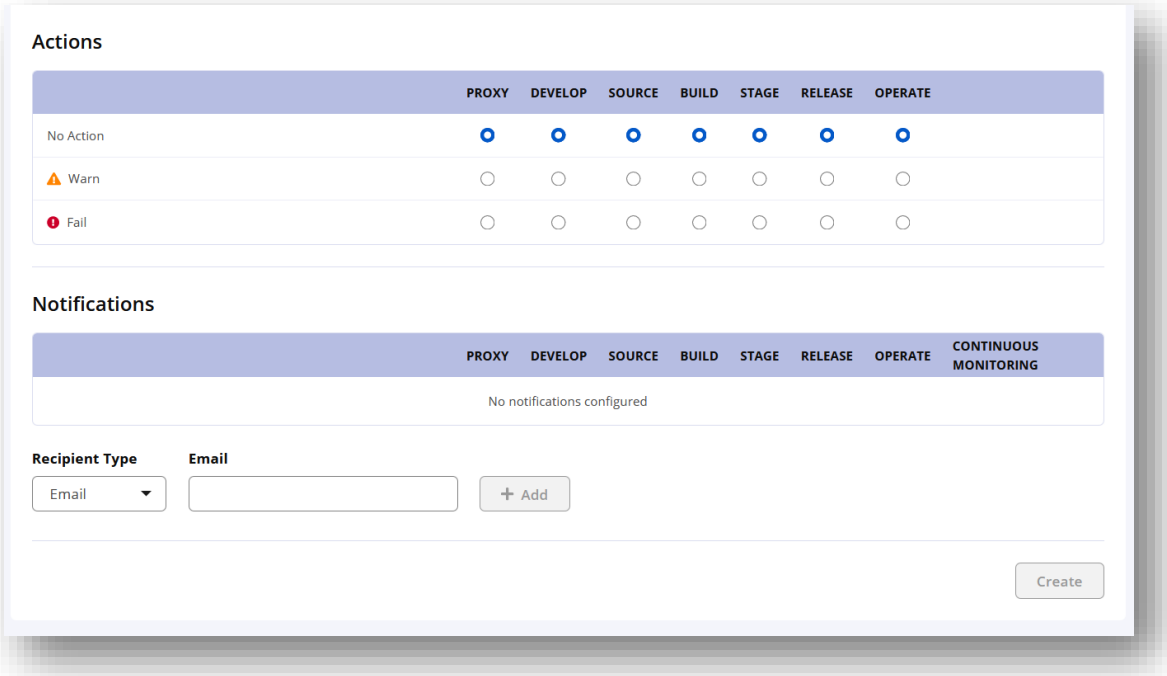


nexus
IQ server

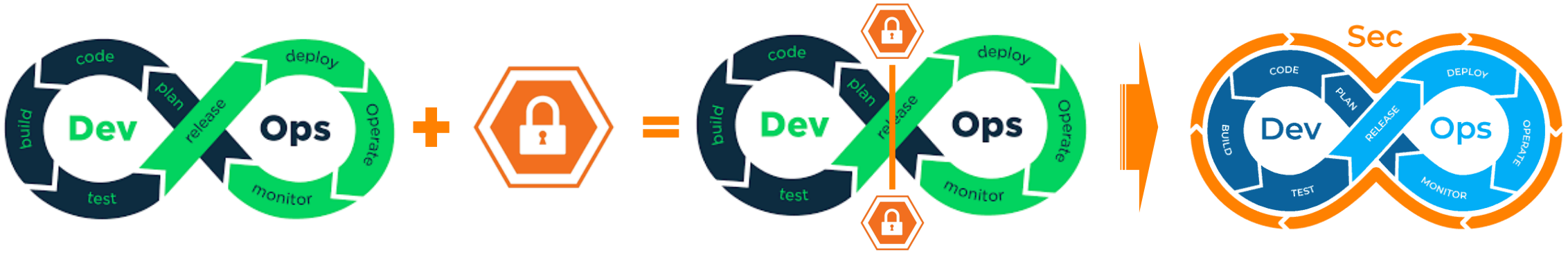
sonatype
nexus
repository
pro

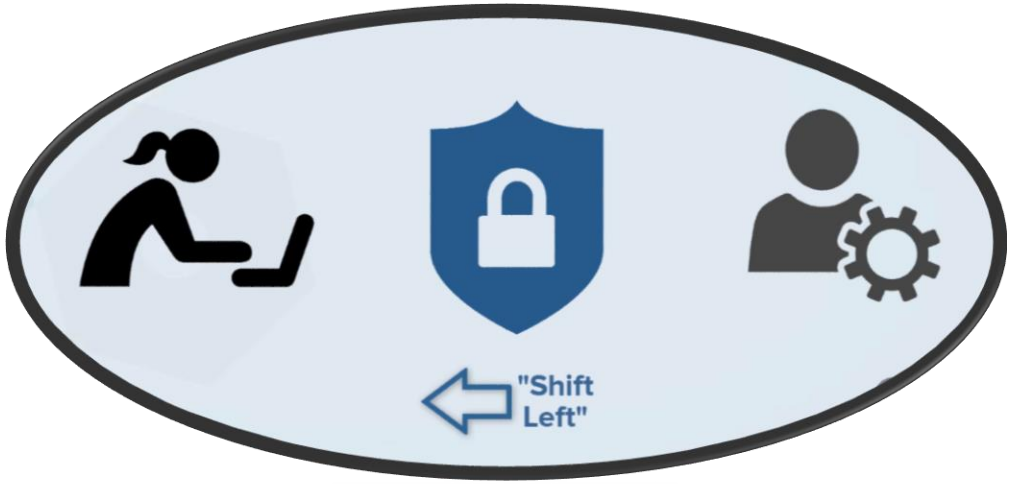
sonatype repository firewall

정책의 적용 (Enforcement)



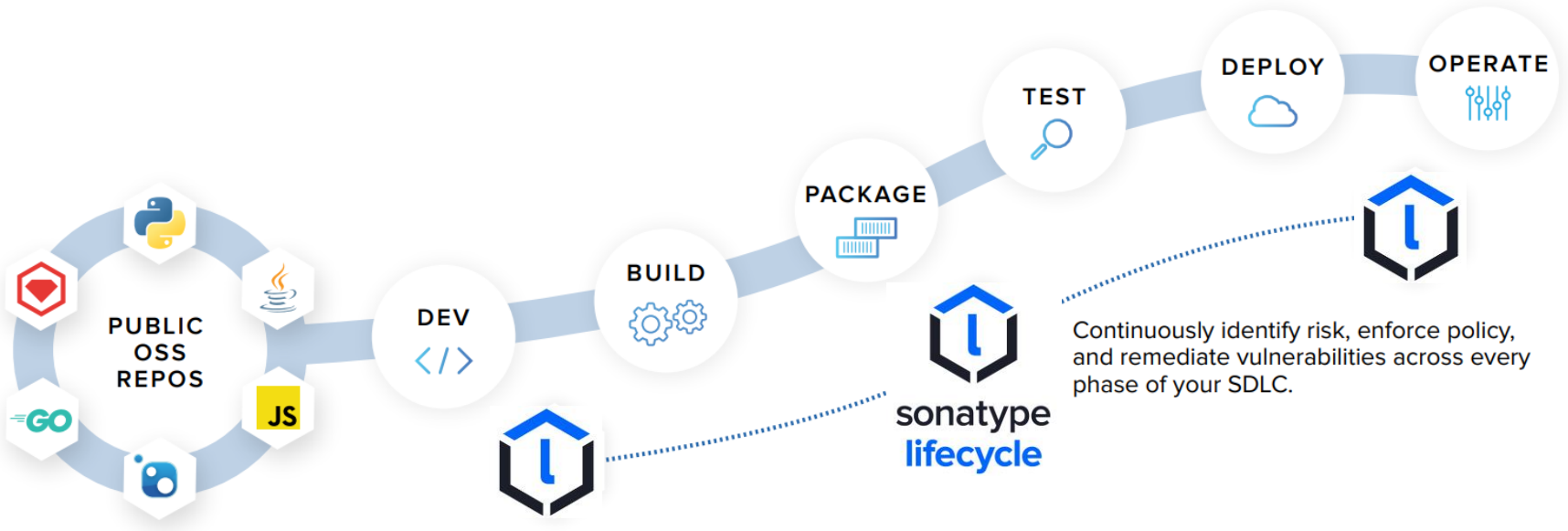
DevOps -> DevSecOps





Shift Left : Put security and compliance into the pipeline before any development begins and verify it in all environments.

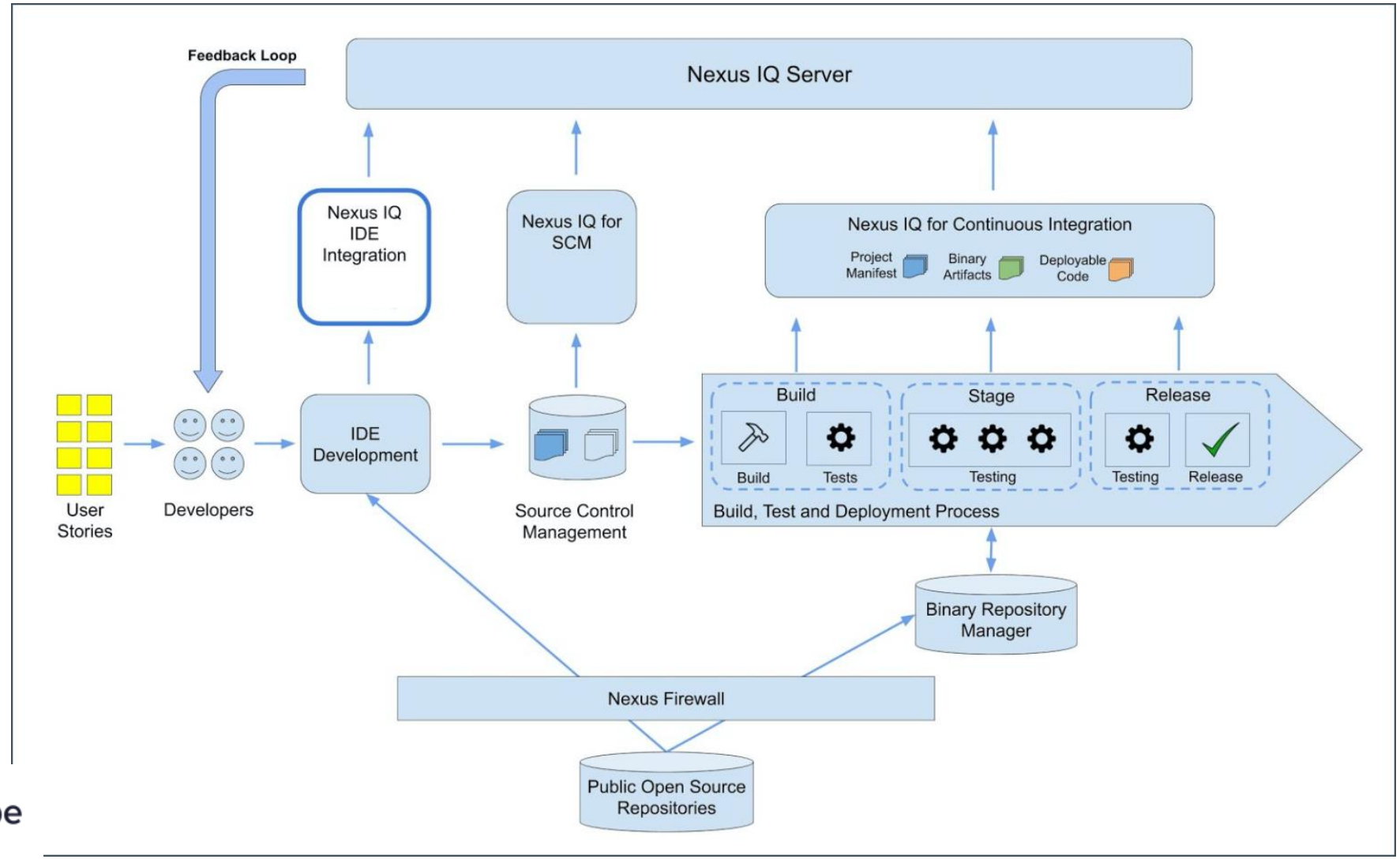
Lifecycle은 개발자 및 보안담당자가 오픈소스를 보다 안전하게 혁신을 추구하도록 합니다.



현업에서 사용하는 주요 Pipeline 툴의 사전 정합

Github, Gitlab, Bitbucket, Azure DevOps, Eclipse, IntelliJ IDEA, VS Code, Jenkins, Bamboo, CircleCI, Github Action, JIRA, Slack, TeamCity

Nexus IQ Server – Big Picture

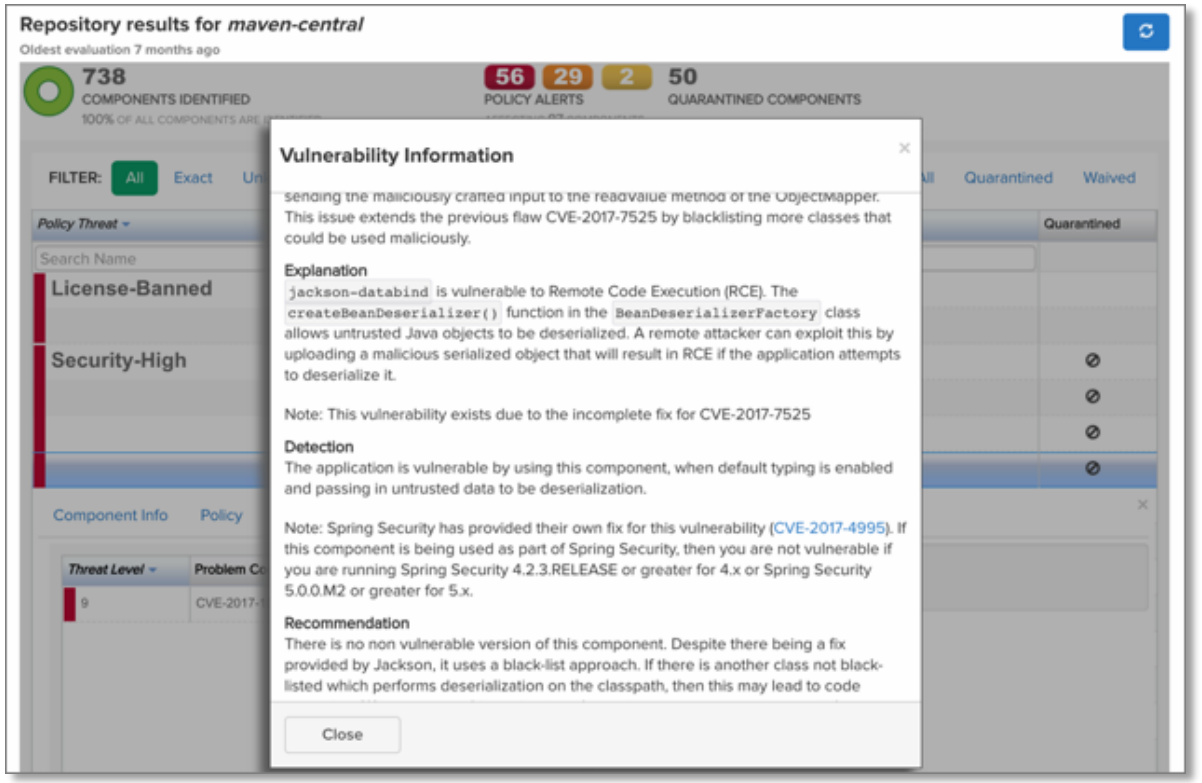


오픈소스 취약점 관리

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

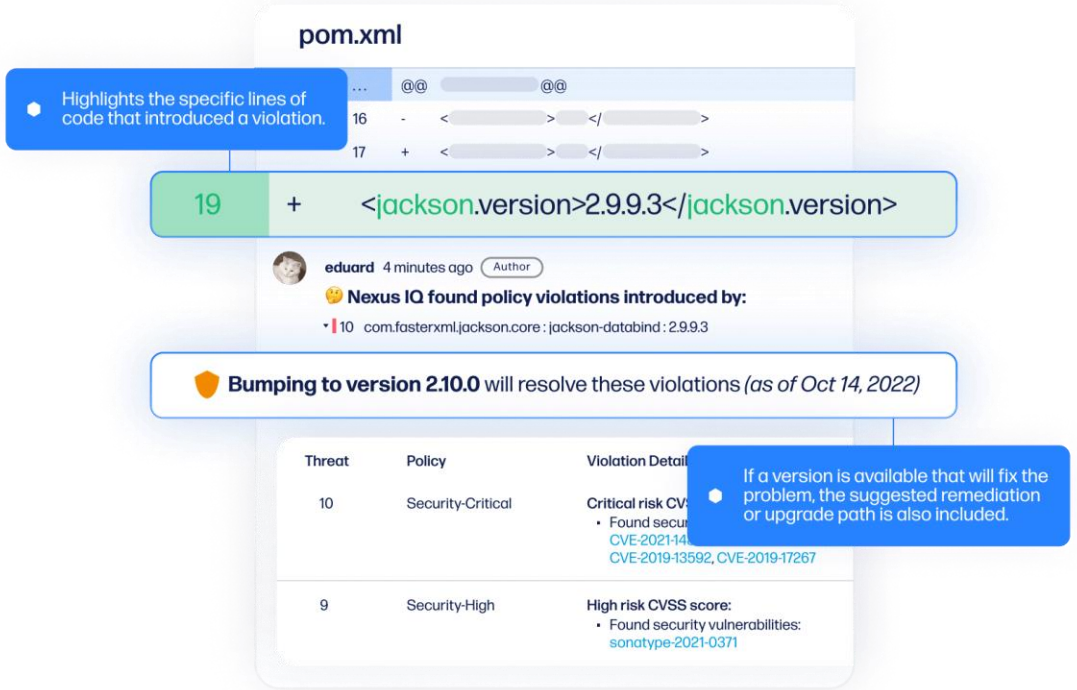
SBOM(Software Bill of Material) 자동 생성

오픈소스 리스크 및 3rd-party 의존성 확인



위험요소에 대한 전문 교정가이드 제공

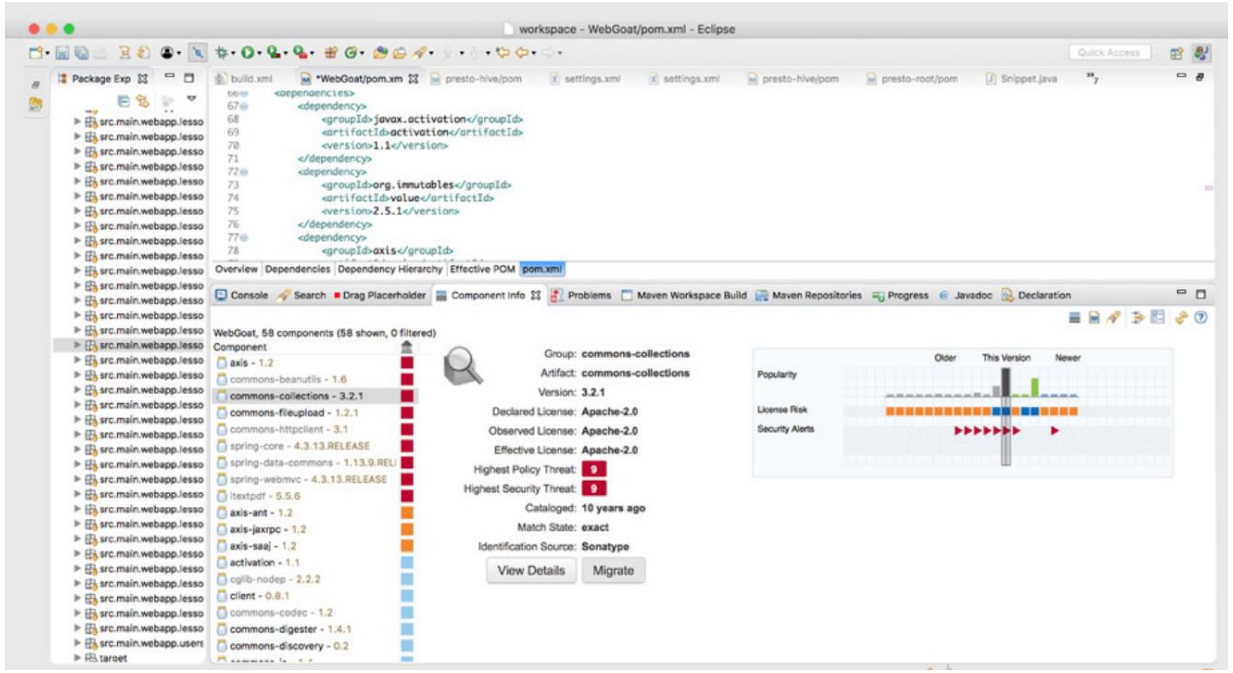
빠르게 고품질 코드 작성



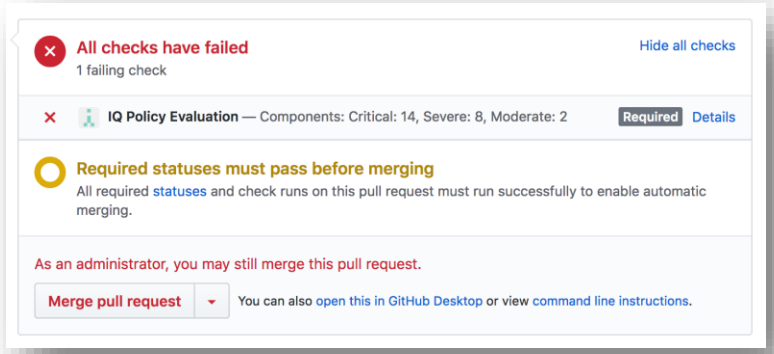
1. 도구 변경없이 Risk 제어
   - IDE, Source Control로부터 직접 개선된 Component 선택
2. 코드 품질 사전 확보
   - 사전에 잠재적인 보안 이슈 및 유지보수 이슈를 탐지하고 조치
3. 취약점을 빠르게 치유
   - 정확한 위치와 의존성을 파악하고 위협요소를 빠르게 수정할 수 있는 정보 확보

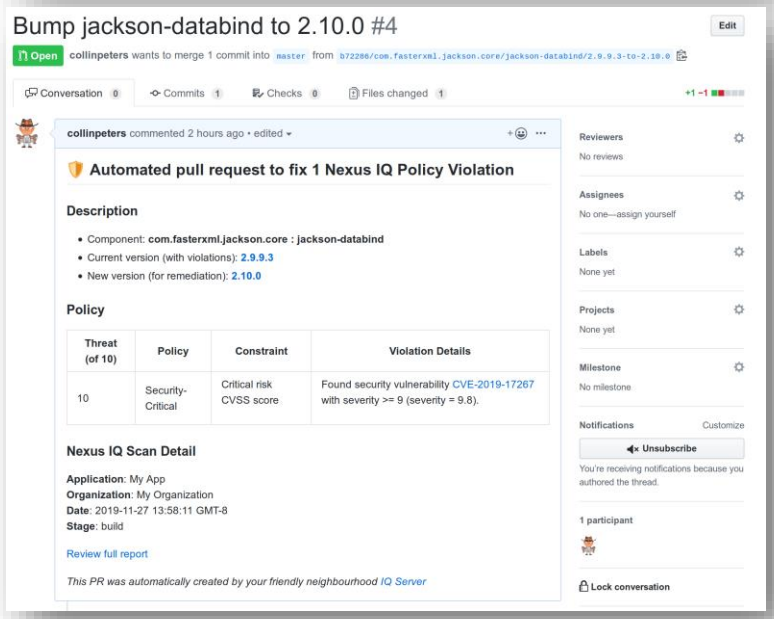
빠르게 고품질 코드 작성

- 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)





Automated Commit Feedback

Commit 또는 Pull Request에 Policy 평가정보를
직접 확인하도록 제공

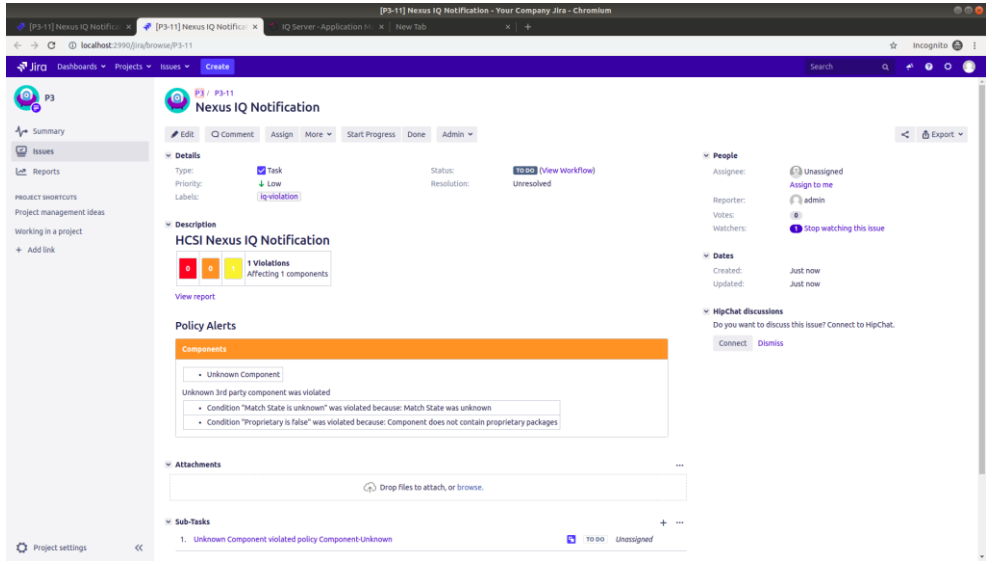
Automated Pull Request

Policy Violation에 대해 수정 버전이 존재하는 경우 자동으로
Pull Request 생성

Pull Request Commenting

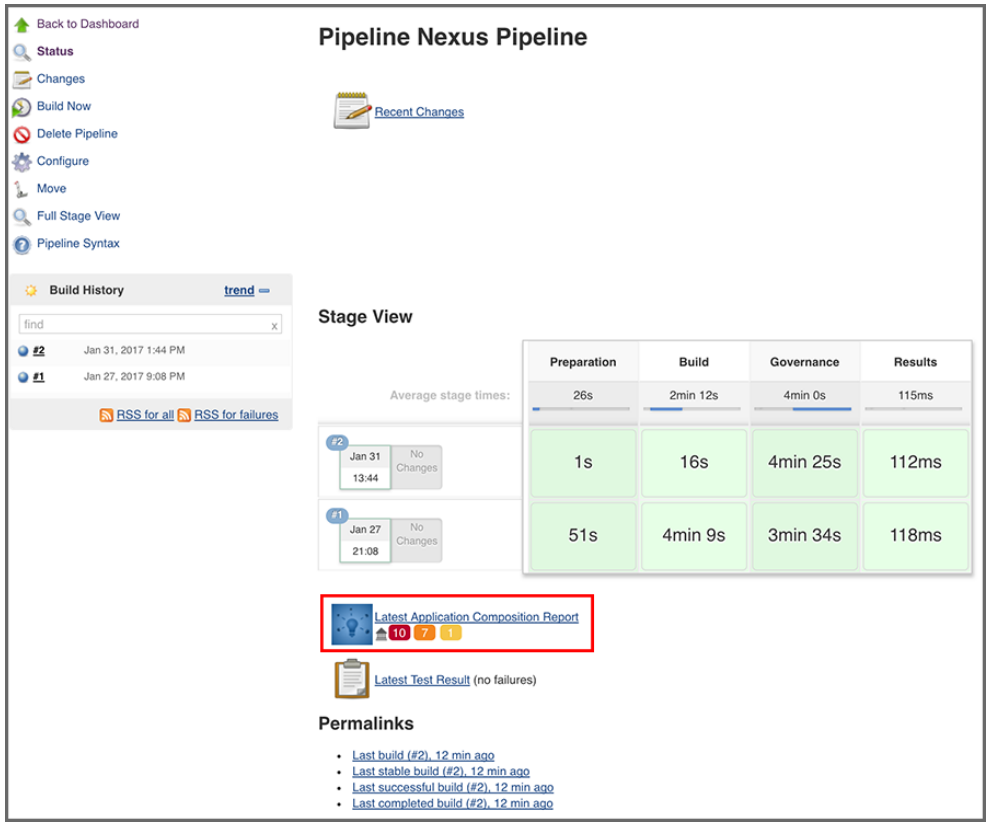
Pull Request가 새로운 Policy Violation을 발생시키는 경우
관련 Comment 추가

JIRA & CI Server 지원



Automated Ticket Creation

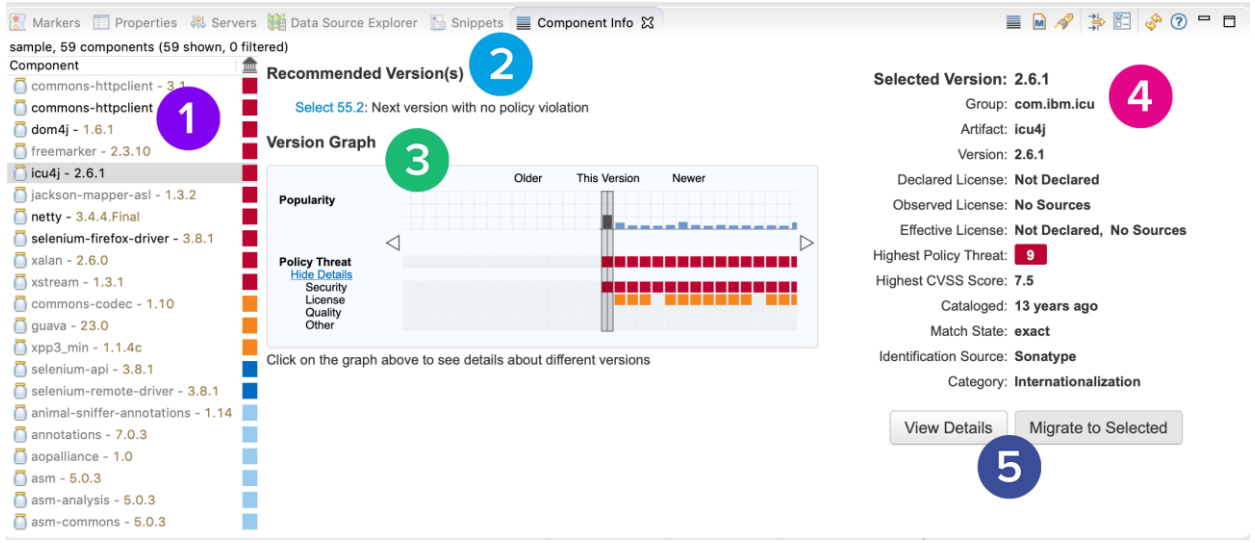
Jira Plugin을 통해 IQ Server Webhook Violation 이벤트를 받아 티켓 자동 생성



Build Scan Result

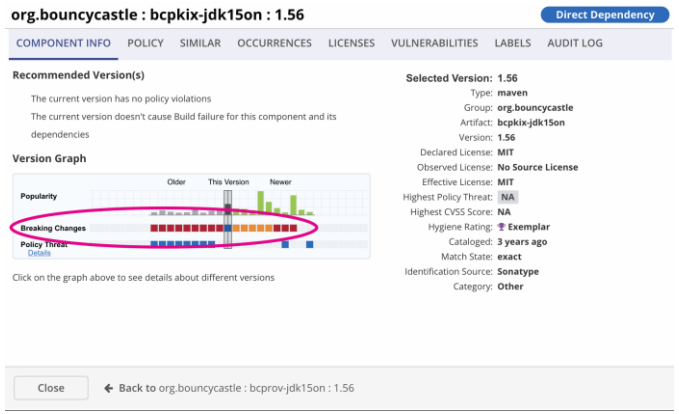
CI Server (Jenkins, Bamboo, Azure DevOps, Gitlab CI등)를 통해 Security & License 분석 결과를 확인

개발자 IDE 환경 지원 (via IQ Integration)



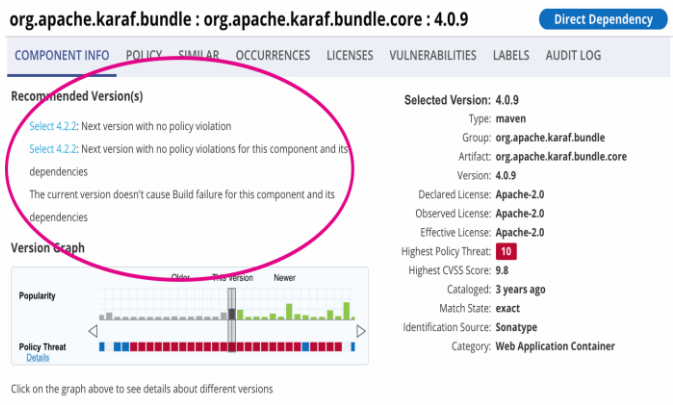
1. Component List : 분석된 Direct Dependency 및 Transitive Dependency 리스트
2. Recommended Versions : 동일 컴포넌트 중 정책에 부합하는 버전 추천
3. Version Graph : 선택된 컴포넌트에 대한 버전 별 Property 확인
4. Version Details : 컴포넌트 세부정보
5. View Details and Migrate Buttons : 관련 정책 및 이슈 세부 확인 및 Migration

Advanced Development Support



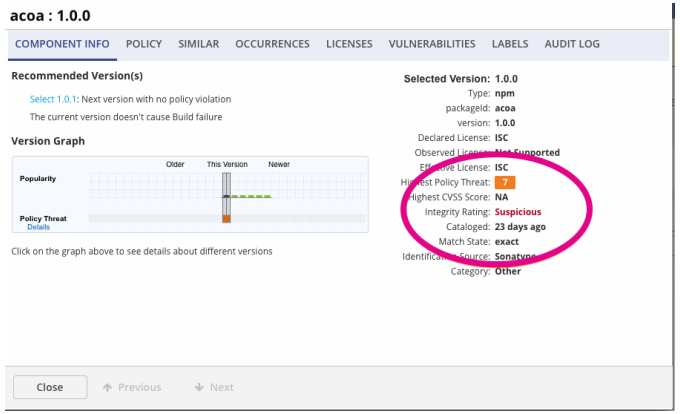
Breaking Changes

Component
업그레이드에 코드변경이 필요한지 여부



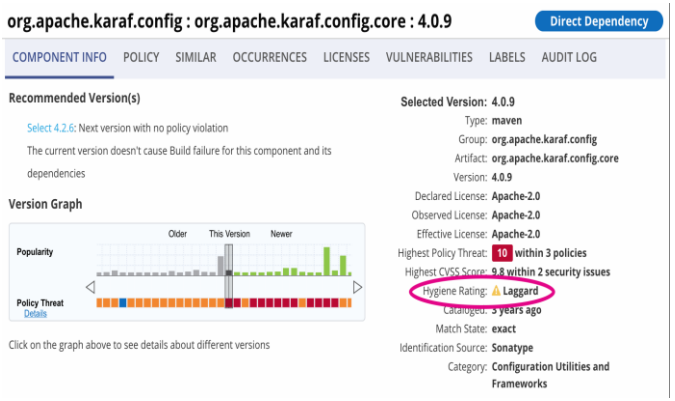
Transitive Solver

정책 및 코드변경 등을 고려한 업그레이드 패스 추천



Release Integrity (ML/AI)

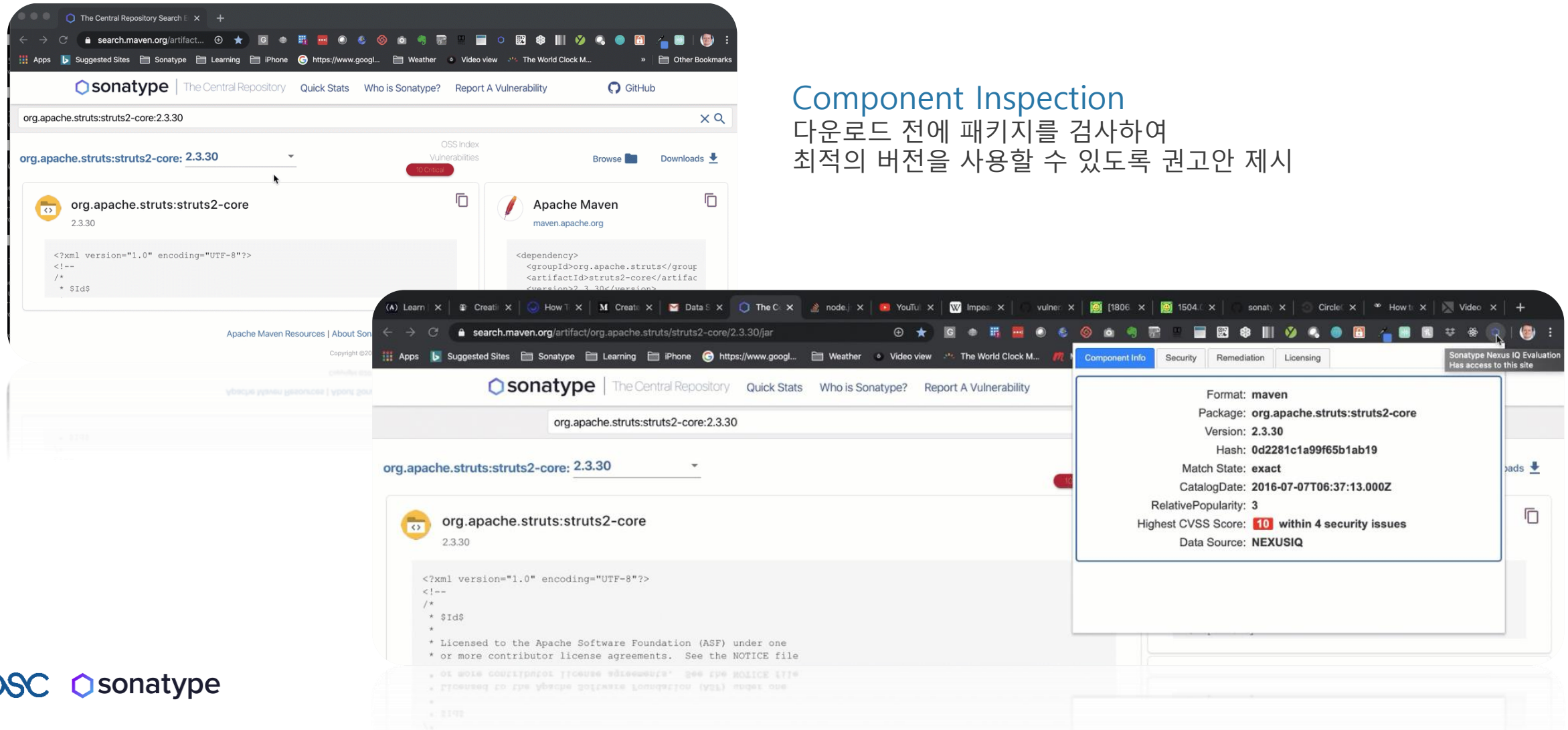
공급망 모니터링을 통해 의심되는 컴포넌트 사전 경고



Hygiene Ratings

Supplier (프로젝트 소스)에 대한 품질 평가 지표

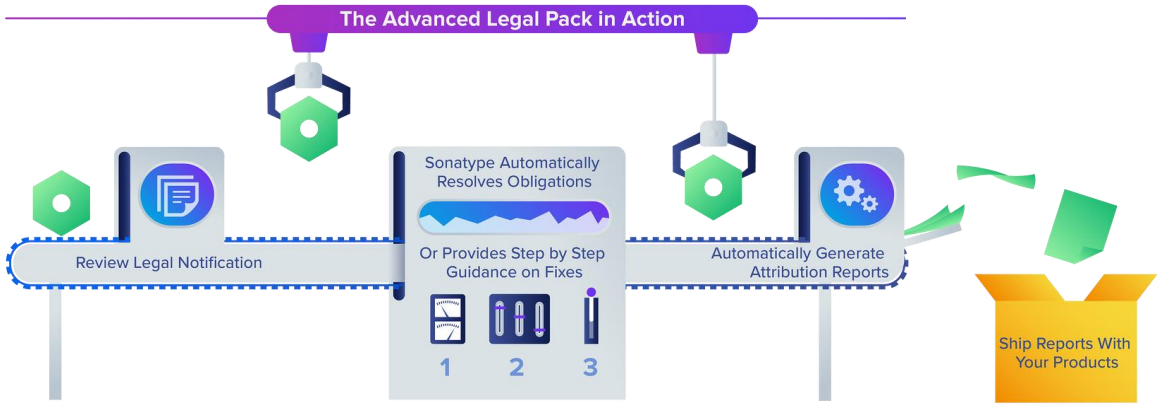
Chrome Extension



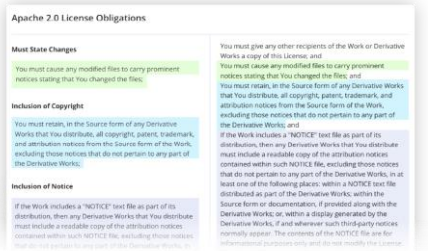
Component Inspection

다운로드 전에 패키지를 검사하여
최적의 버전을 사용할 수 있도록 권고안 제시

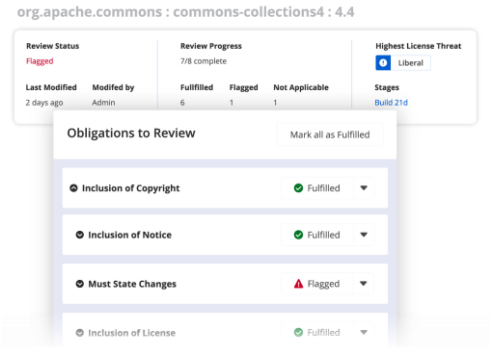
Advanced Legal Pack (Lifecycle Add-On)



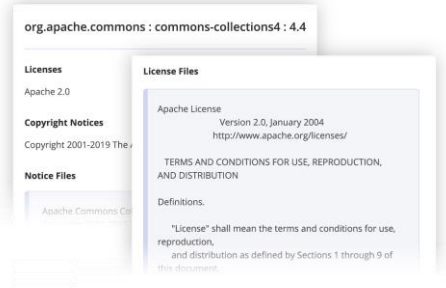
라이선스 의무 검토 도구
License Obligation Review Tool
사용중인 컴포넌트에 대한 모든 라이선스를 쉽게 검토할 수 있는 도구제공



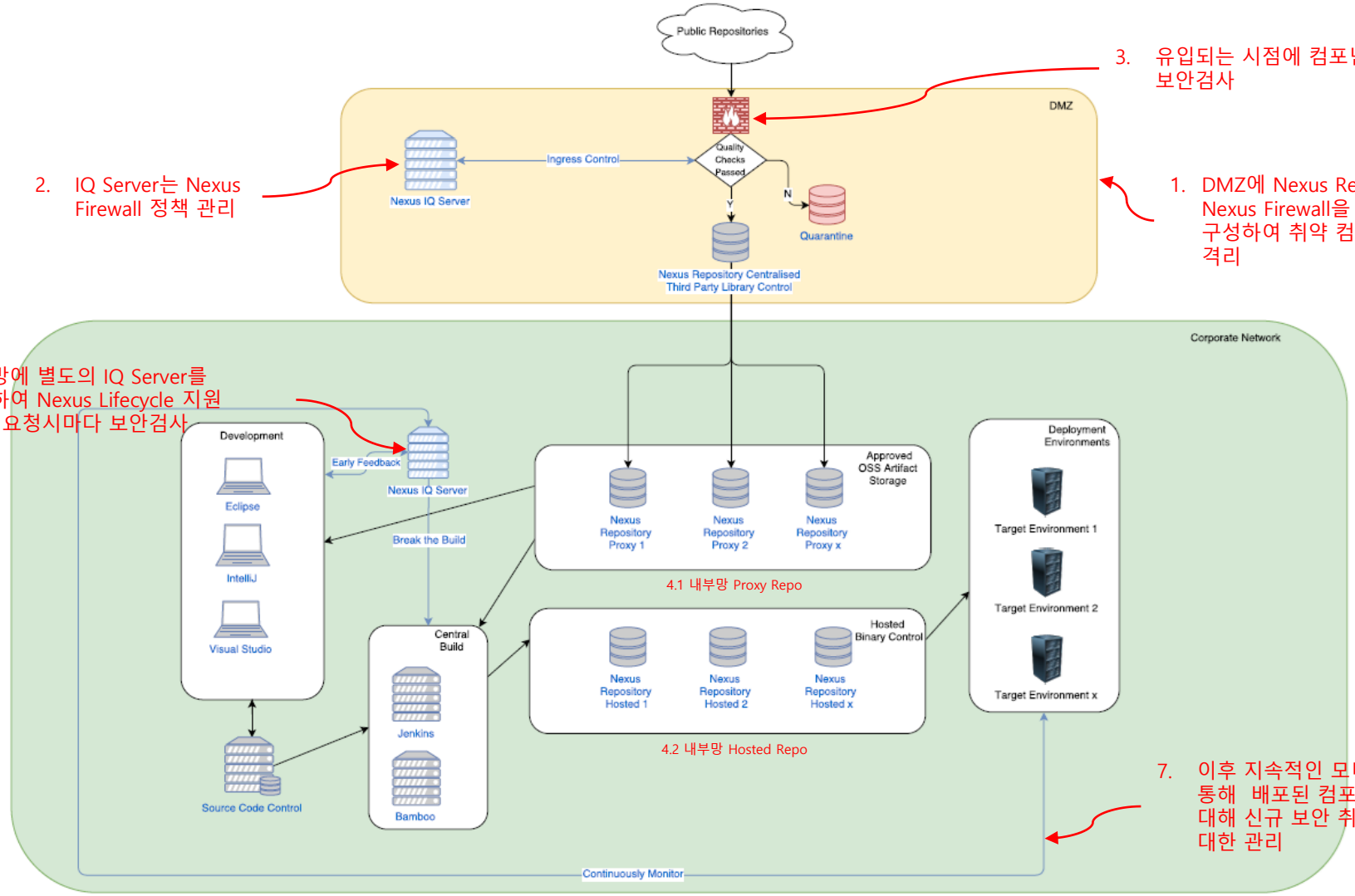
Compliance 워크플로우
의무사항들을 조치할 수 있는 단계별 워크플로우 제공



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



표준 구성



2. IQ Server는 Nexus Firewall 정책 관리

3. 유입되는 시점에 컴포넌트별 보안검사

1. DMZ에 Nexus Repo 및 Nexus Firewall을 구성하여 취약 컴포넌트 격리

5. 내부망에 별도의 IQ Server를 구성하여 Nexus Lifecycle 지원
6. Build 요청시마다 보안검사

7. 이후 지속적인 모니터링을 통해 배포된 컴포넌트에 대해 신규 보안 취약점에 대한 관리

Nexus Firewall 관리/동작 영역

Nexus Lifecycle 관리/동작 영역

Summary – Why Sonatype?

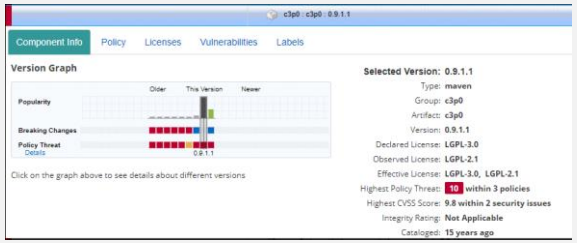
Shift Left
(시프트 레프트)

오픈소스 유입 관문부터 실시간 통제

nexus repository

repository firewall

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

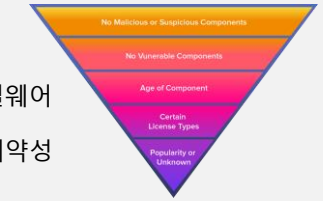
자동화 필수요건

Flexible Policy
(유연한 정책)

다양한 속성을 통한 정책 정의

악성/멀웨어

취약성



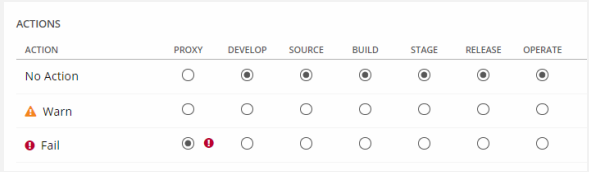
품질

라이선스

인기도

nexus IQ server by sonatype

단계별 차등화 된 정책 적용



Appendix : Sonatype 도입 Roadmap

㈜오에스씨코리아
www.osckorea.com

sales@osckorea.com | 02-539-3690