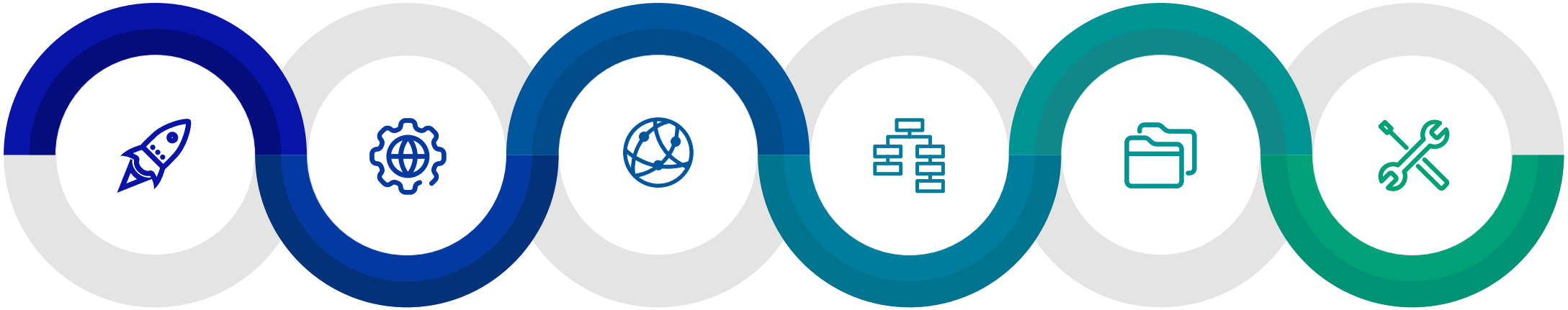

OSC
OpenMSA™
Container 기반의 MSA(Microservice Architecture) 환경 진단 Service
Opensource 기반 DevOps/MSA 전문 기업 – OSC Korea
T : 02-539-3690 ‖ E : sales@osckorea.com
06134 서울 강남구 테헤란로 5길, 7 13층 (KG타워)

Contents

1. OpenMSA™을 이용한 Container 환경 진단 Service 개요

OpenMSA™ 소개



100% OPENSOURCE	검증된 SOLUTION	E2E SOLUTION	MODULE 설계	확장성	DAY 2 기술지원
특정 업체에 종속되지 않는 Opensource 기반 Solution	다수의 구축사례를 통해 검증된 Solution으로 빠른 구축 가능	Container 관리에서 CI/CD, Monitoring, API 관리,인증에 이르기까지 E2E Solution 제공	Module화된 구조로 고객의 수요에 맞게 선택적으로 구축 가능	Service 수요에 따라 유연하게 확장 가능하며 이음새 없이 부가 기능을 수용	표준 기술 지원 Service 및 Enterprise 기술 지원 제공

▪ 100% Opensource 기반의 OpenMSA™ 기대 효과

MSA 운영 환경 확보

MSA 환경을 위해 필수적인 Container 운영환경을 확보하고 이를 유연하게 확장 운영할 수 있는 기틀을 마련할 수 있습니다.

서비스 안정화

서비스 현황을 지속적으로 Monitoring 할 수 있으며 각종 보안 위협이나 잠재적인 취약점을 사전에 격리하여 안정적인 서비스를 유지할 수 있습니다.

Opensource 기반

100% Opensource 기반으로 구성하여 특정 업체에 종속되지 않으며 혁신적인 기술을 발빠르게 도입하여 서비스를 고도화 할 수 있습니다.

DevOps 개발/운영 환경 정착

CI/CD를 포함하여 중단 없는 서비스 개발 / 배포 환경을 확보하여 시장 요구사항에 즉각 부응하고 서비스 고도화를 지속적으로 도모할 수 있습니다.

장애 대응력 향상

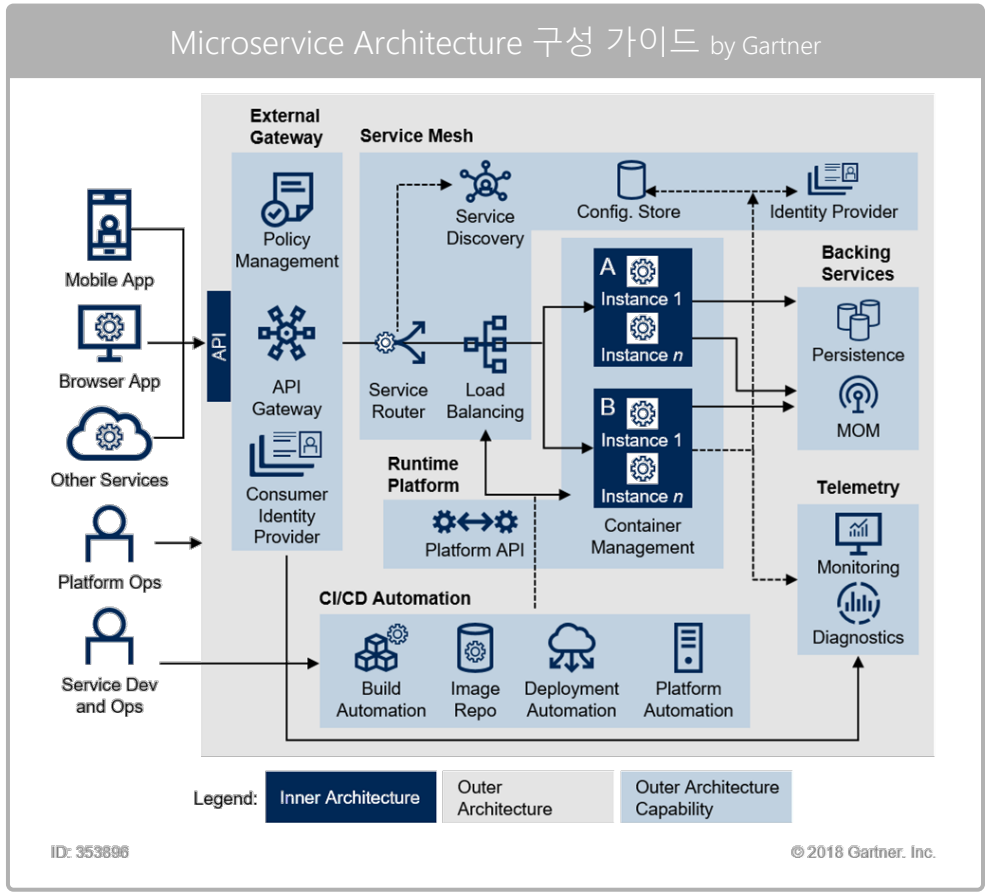
사전에 잠재적인 문제가능성을 파악하여 선 조치 할 수 있으며 장애 발생시 즉각 대응할 수 있도록 각종 지표와 Log 및 Trace 정보를 분석합니다.

고도화 Road-map 확보

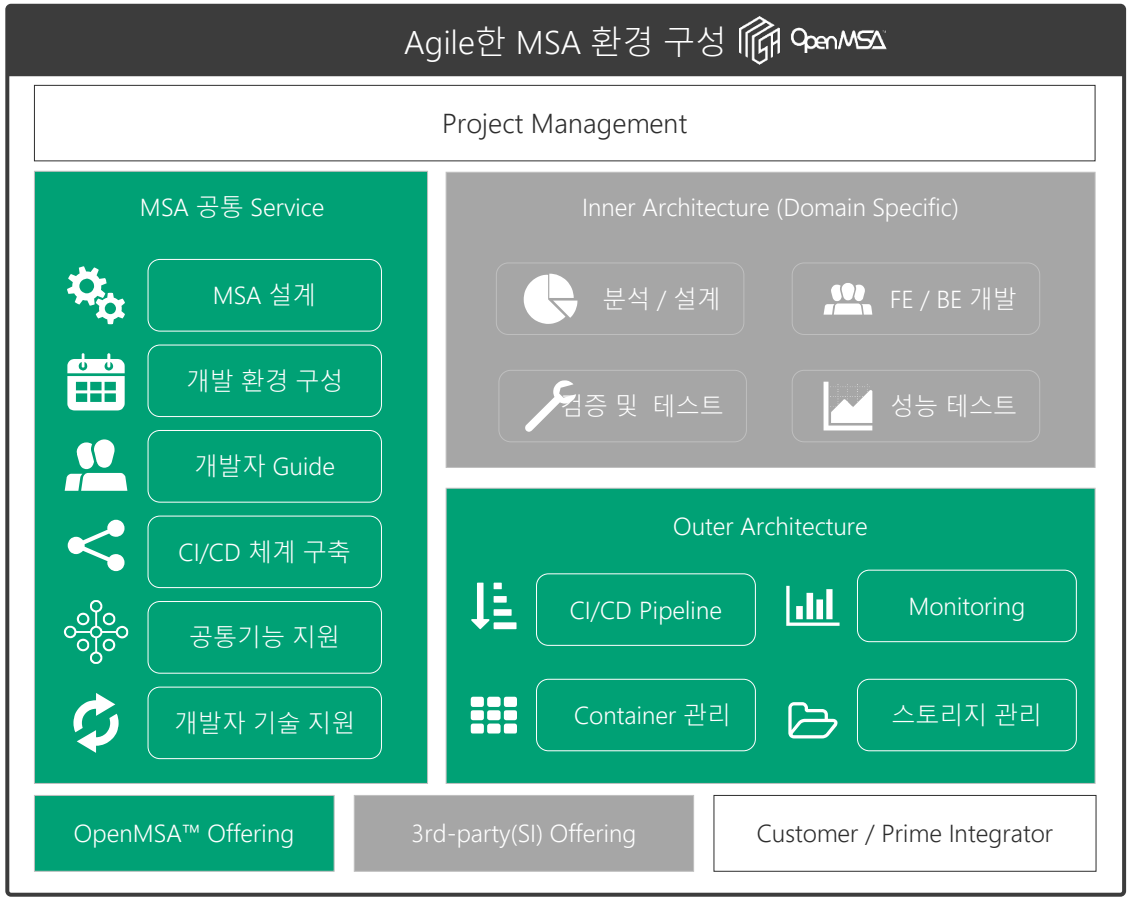
서비스 요구사항에 따라 보다 수준 높은 기능과 SLA를 보장하는 Enterprise 급 서비스와 쉽게 접목할 수 있습니다.

100% Opensource 기반의 OpenMSA™ 구성 개요

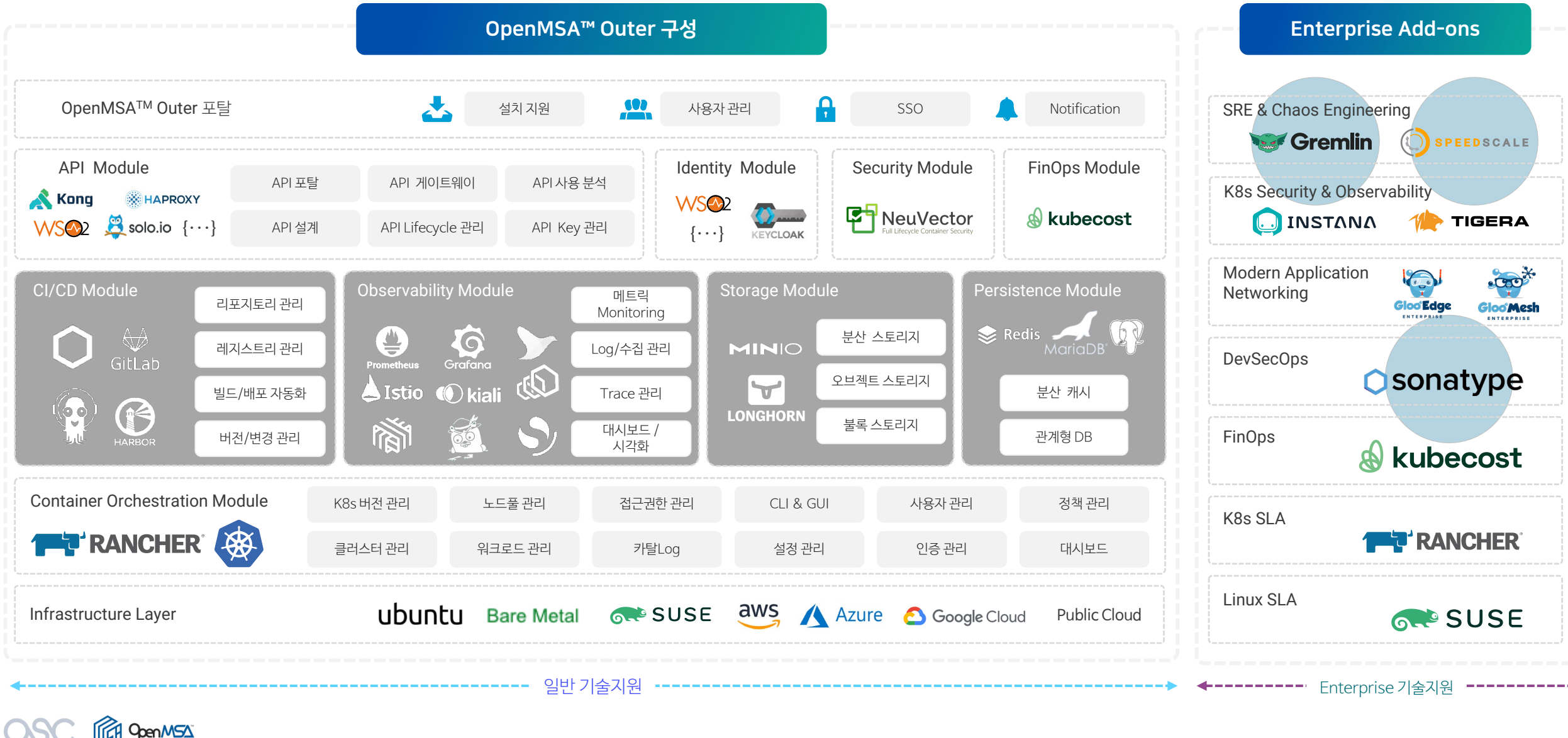
- OpenMSA™는 MSA 공통 서비스와 Outer Architecture(DevOps, GitOps, FinOps 등)에 대해 안정적인 Opensource로 구성한 표준 MSA Framework로, 산업별/Domain별 최적의 MSA 환경 제공



100% Opensource 기반으로 구체화한 서비스 Framework



▪ 100% Opensource 기반의 OpenMSA™ 구성 상세 - MSA Outer



OpenMSA™ 기반의 진단 서비스 개요

장애 진단

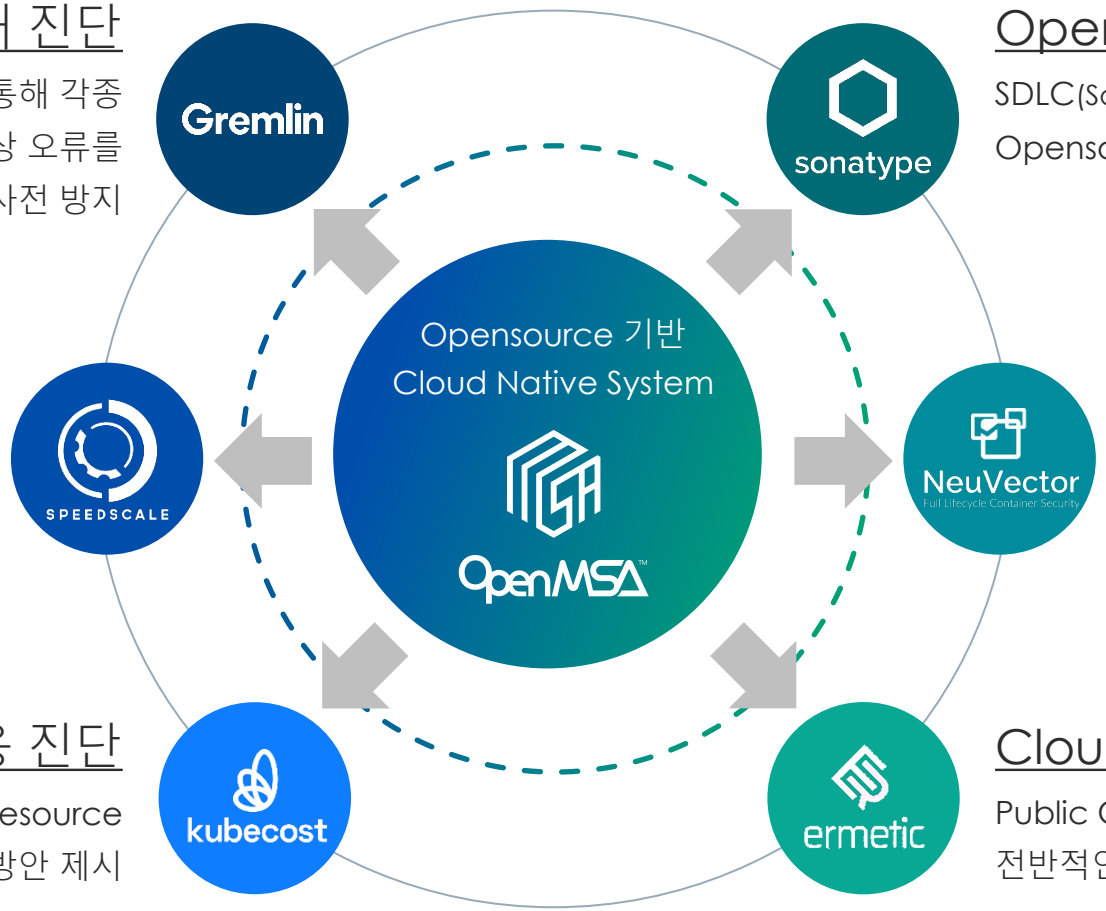
Chaos Engineering 기법을 통해 각종 Resource 장애를 유도하여 구성상 오류를 점검하여 대규모 장애요소 사전 방지

성능 진단

Production 환경 수준의 부하를 자동으로 생성하여 성능 Issue를 사전에 점검

비용 진단

불필요한 Resource나 과도한 Resource 사용을 진단하고 최적화 방안 제시



Opensource 보안 진단

SDLC(Software Development Lifecycle)에 걸쳐 유입되는 Opensource Library에 대한 취약성 점검

Container 보안 진단

Pipeline 및 Runtime 상의 Container 보안 취약점 점검

Cloud Compliance 진단

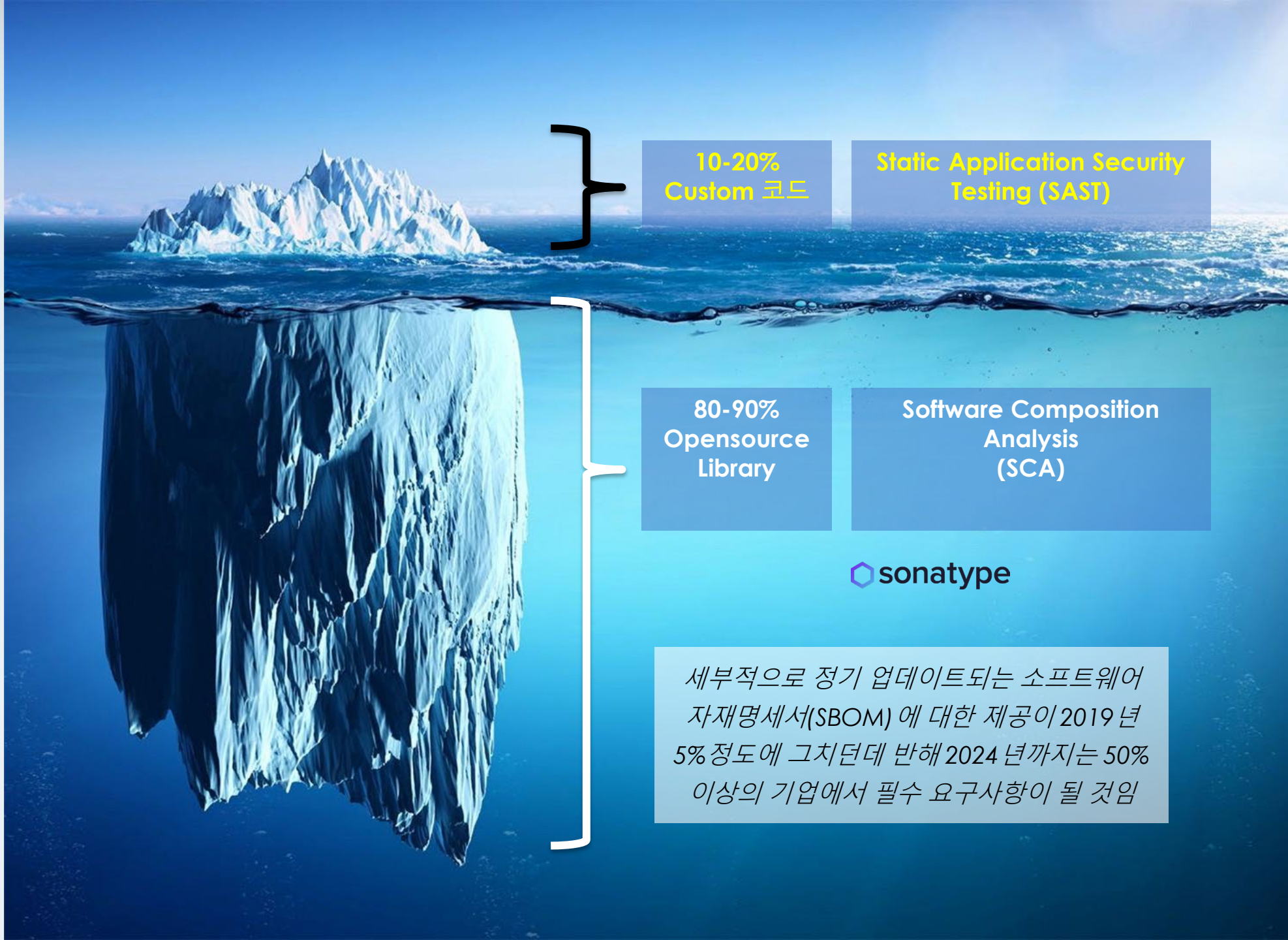
Public Cloud 전반에 걸쳐 Identity를 포함한 전반적인 Compliance 관련한 취약점 점검

2. SDLC환경의 Opensource 보안 진단 - SonaType

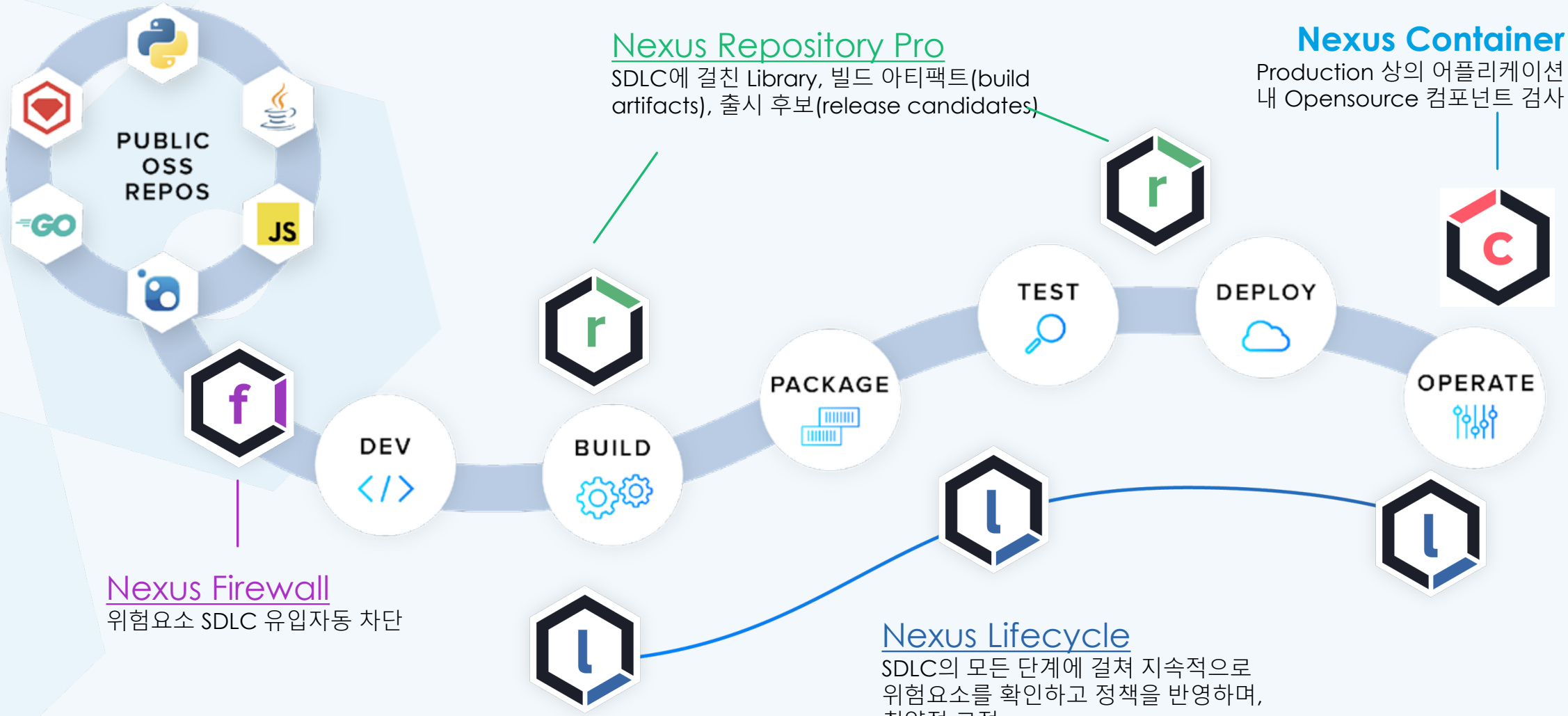
Why Sonatype?

어플리케이션 보안은 복잡하고 다양한 측면을 가진 문제이며 Custom 코드에 대한 테스트 및 Opensource Library에 대한 취약점 분석이 필요함

sonatype



The Nexus Platform



Nexus Repository Pro

SDLC에 걸친 Library, 빌드 아티팩트(build artifacts), 출시 후보(release candidates)

Nexus Container

Production 상의 어플리케이션 내 Opensource 컴포넌트 검사

Nexus Firewall

위험요소 SDLC 유입자동 차단

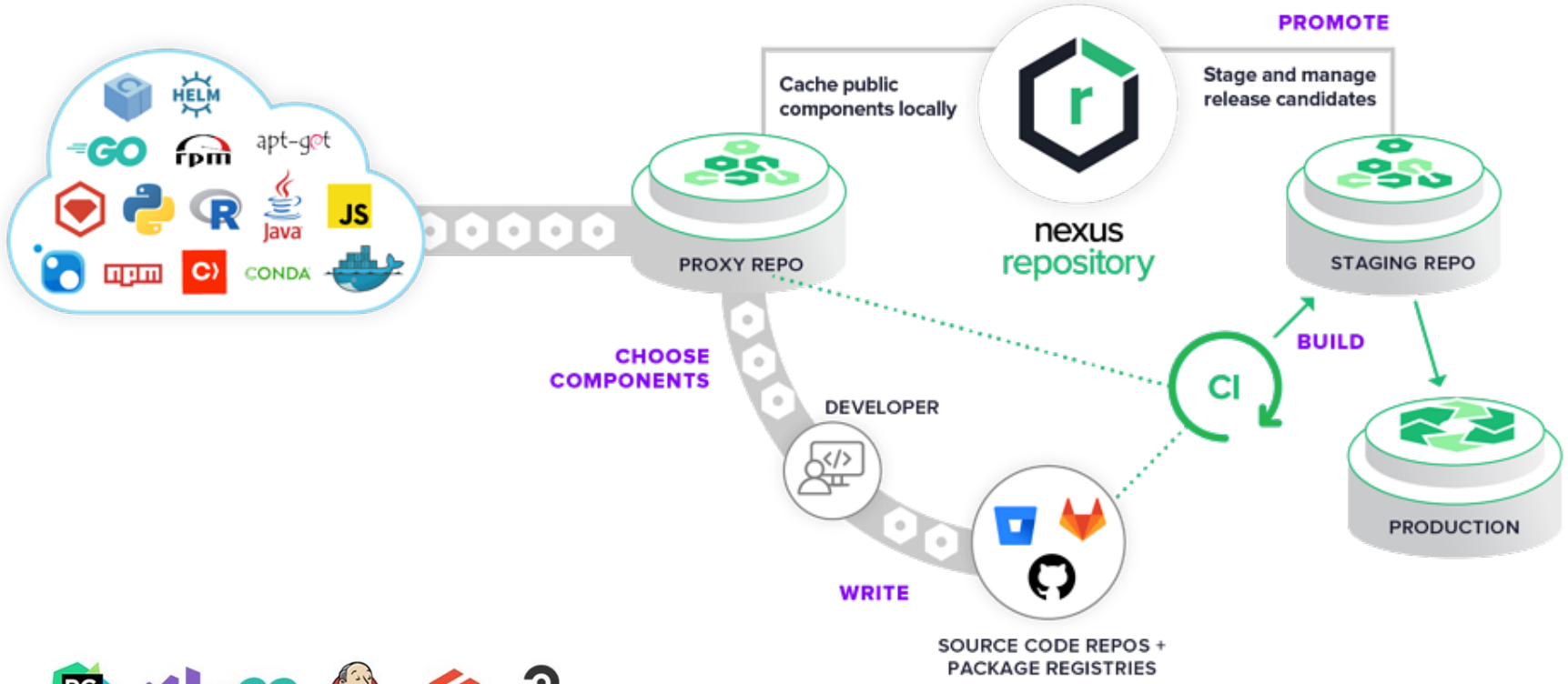
Nexus Lifecycle

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

Nexus Repository Pro

World #1 Repository Manager

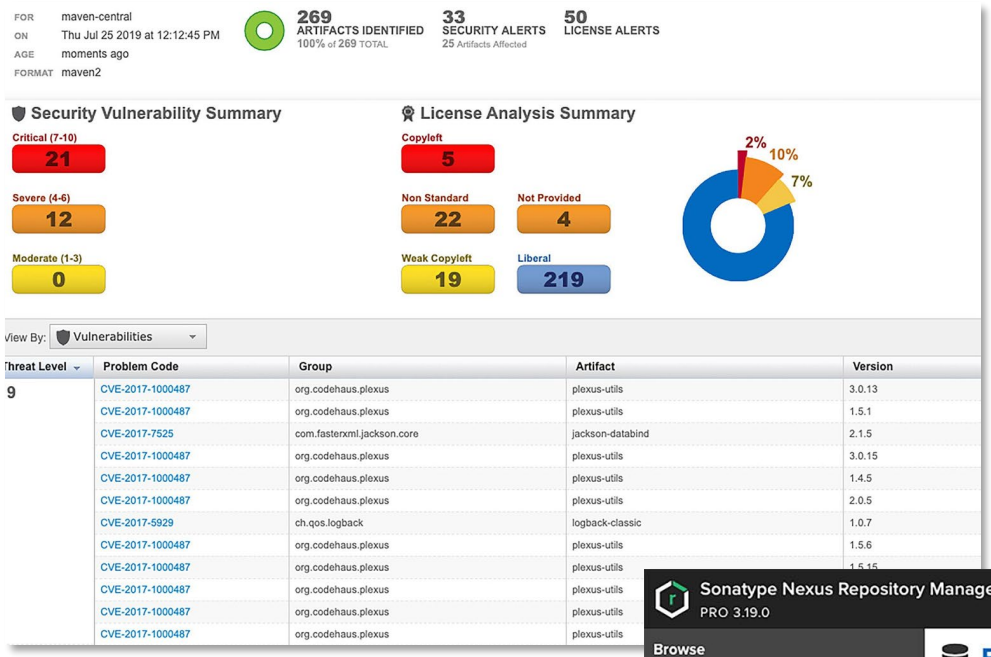
전세계 100,000개 조직에서 사용중인 사설 리포지토리(저장소)로 컴포넌트, Library, 바이너리, 빌드 아티팩트 등을 관리 (HA, SAML/SSO)



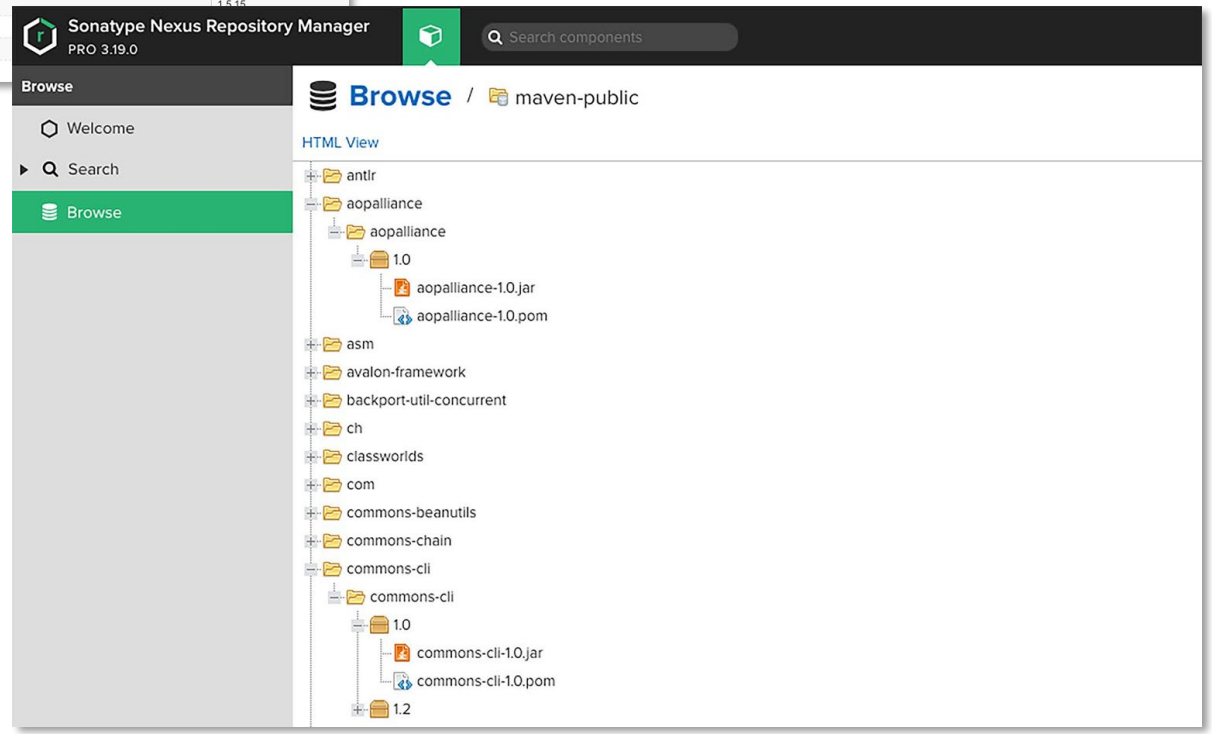
다양한 개발자 도구 및 에코시스템 지원

Nexus Repository Pro

World #1 Repository Manager



Software Supply Chain 의 취약점, 라이선스 Issue 등 Health 확인



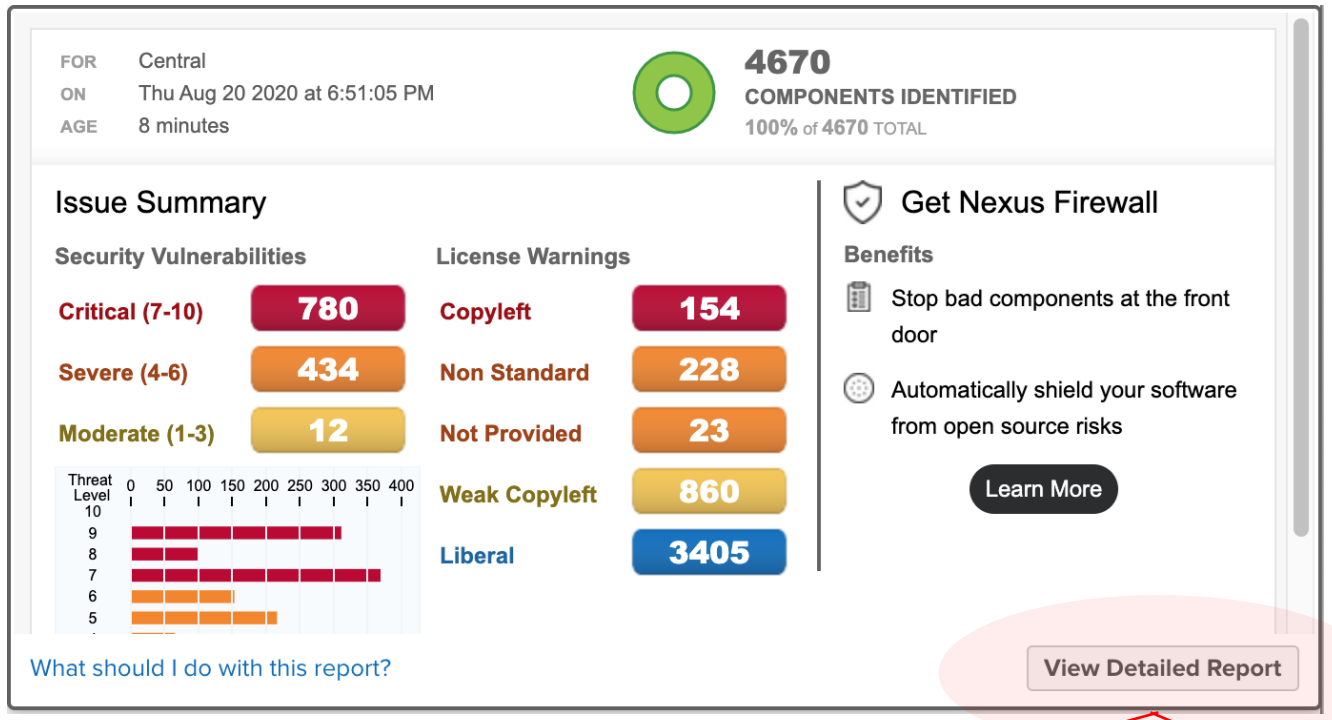
진보된 Staging으로 출시 후보 (Release Candidates) 워크플로우 관리

SONATYPE NEXUS REPOSITORY
#1 RANKED
REPOSITORY MANAGERS
IT Central Station

Nexus Repository Pro

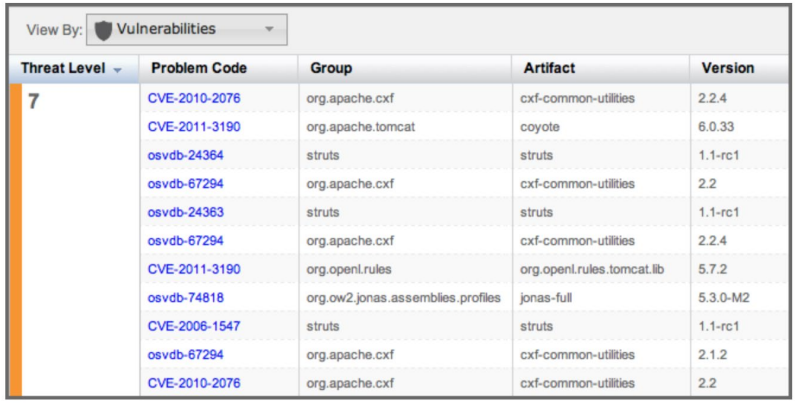
World #1 Repository Manager

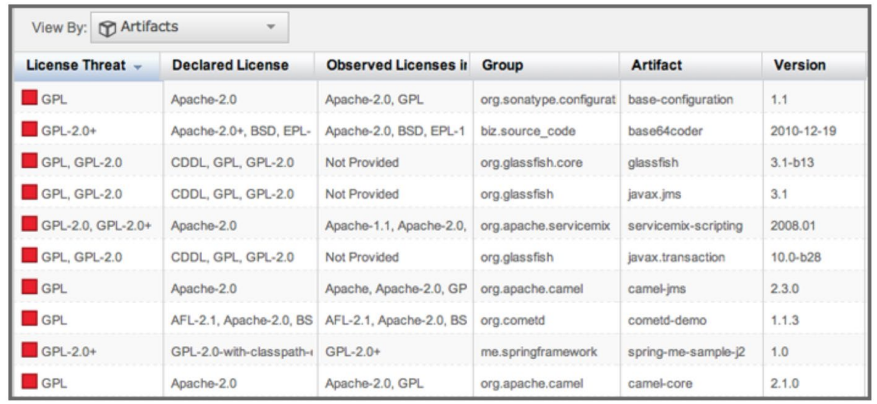
Nexus Repository OSS(Opensource)는 취약점이나 라이선스에 대한 요약정보만 제공하며 Nexus Repository Pro는 세부정보를 추가 제공함



Nexus Repository OSS

Nexus Repository Pro

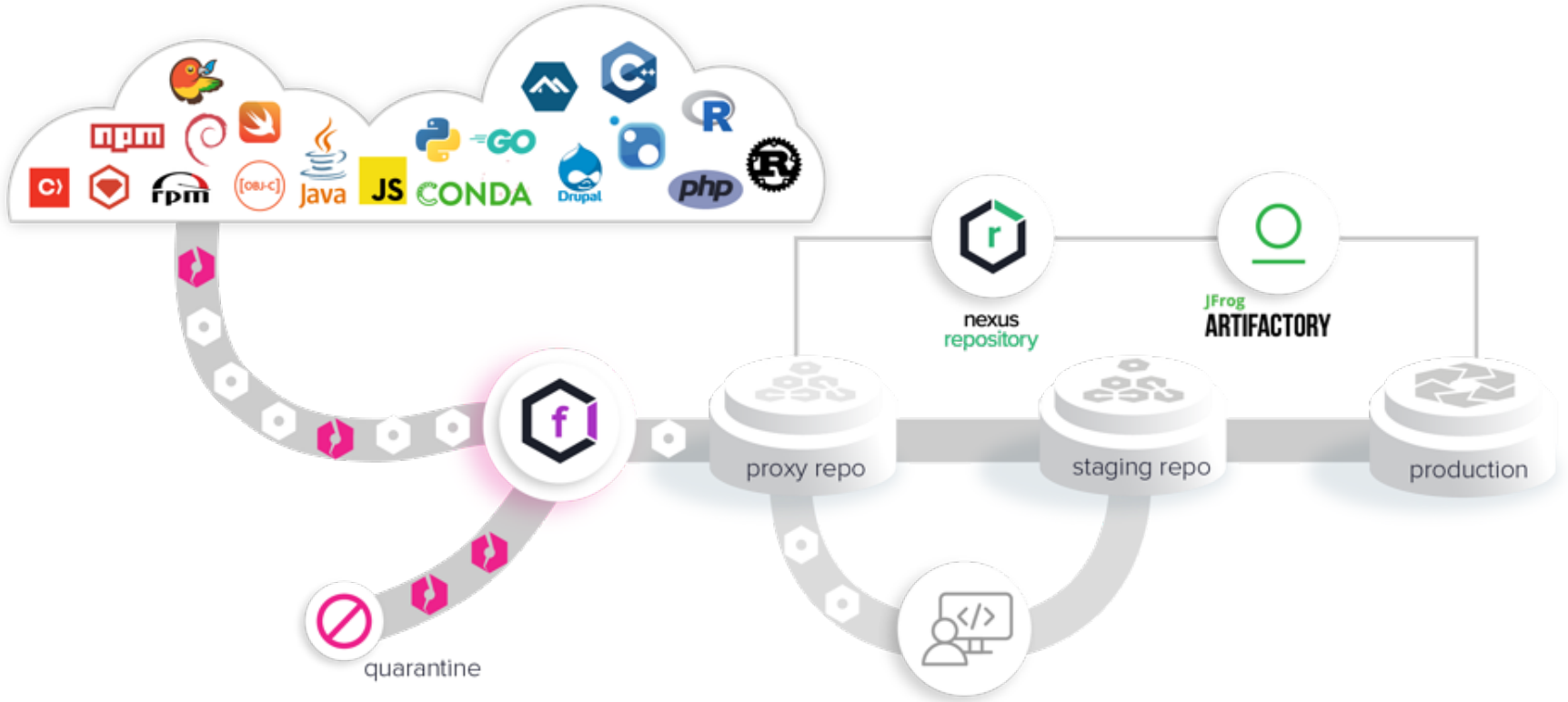




Nexus Firewall

Shift Security Left

Nexus Firewall은 취약한 컴포넌트가 SDLC내로 유입되는 것을 차단

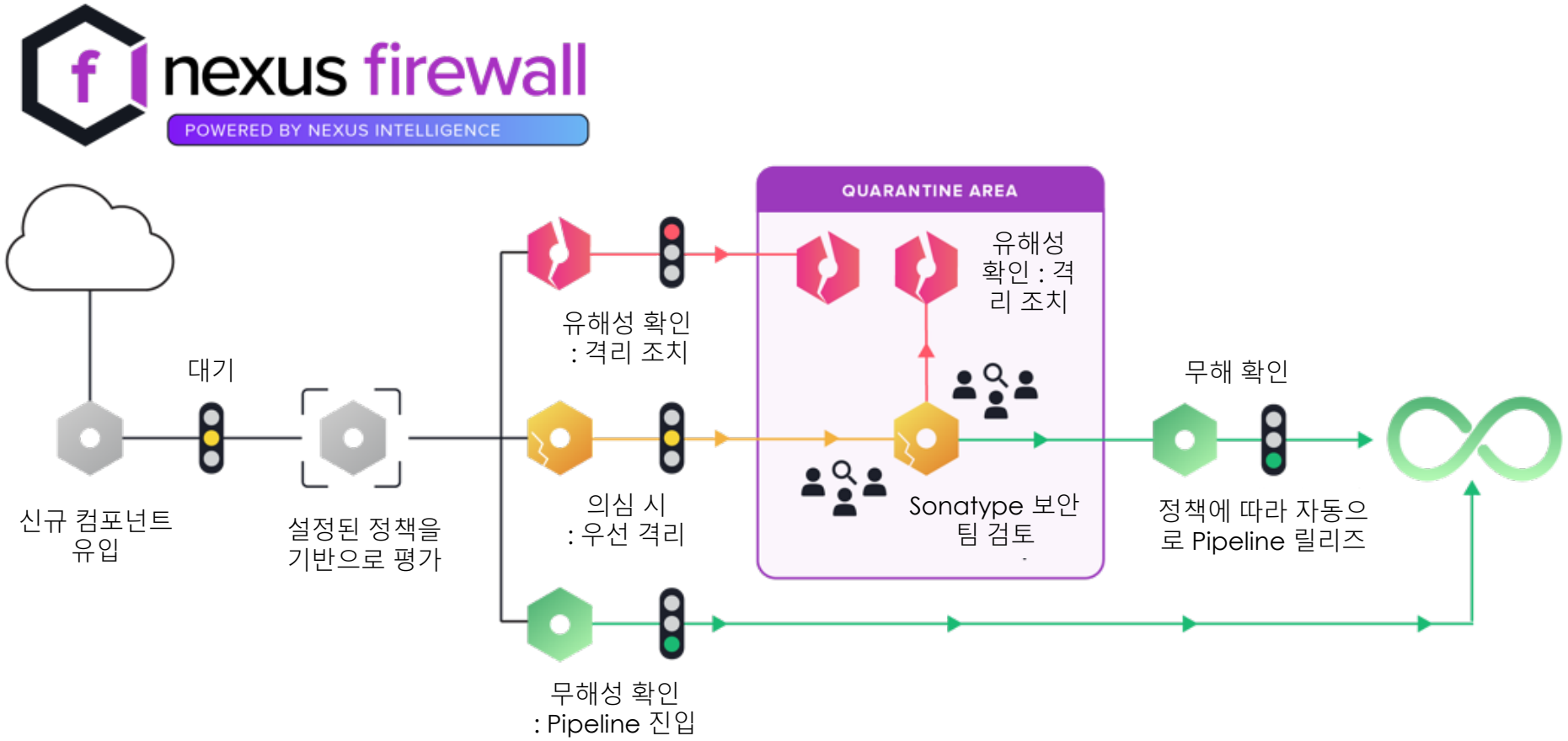


Java, JavaScript, .NET, Python,
Go, Ruby, RPM 등 다양한 언어 지원

sonatype

Nexus Firewall

Shift Security Left



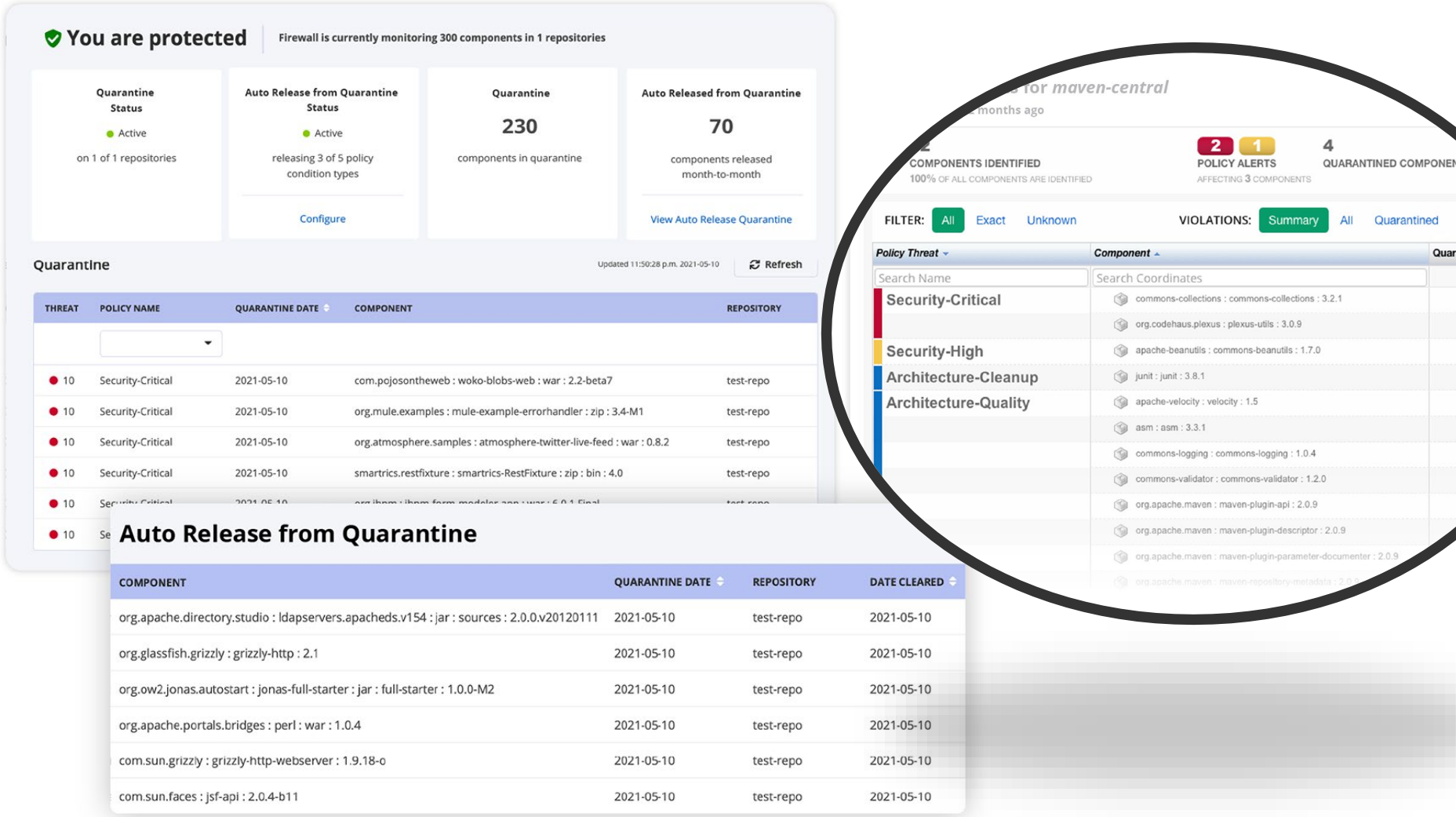
인공지능 기반으로 Opensource를 평가하여 유해한 것으로 판단되는 경우, 자동으로 다운로드를 차단하며 Opensource 유입 정책을 수립하여 제어

sonatype

Nexus Firewall

Shift Security Left

Sonatype AI 엔진은 Opensource에 대한 위험요소를 자동으로 판단하여 정책을 기반으로 유입을 차단하거나 안전이 확인될 때까지 격리합니다.

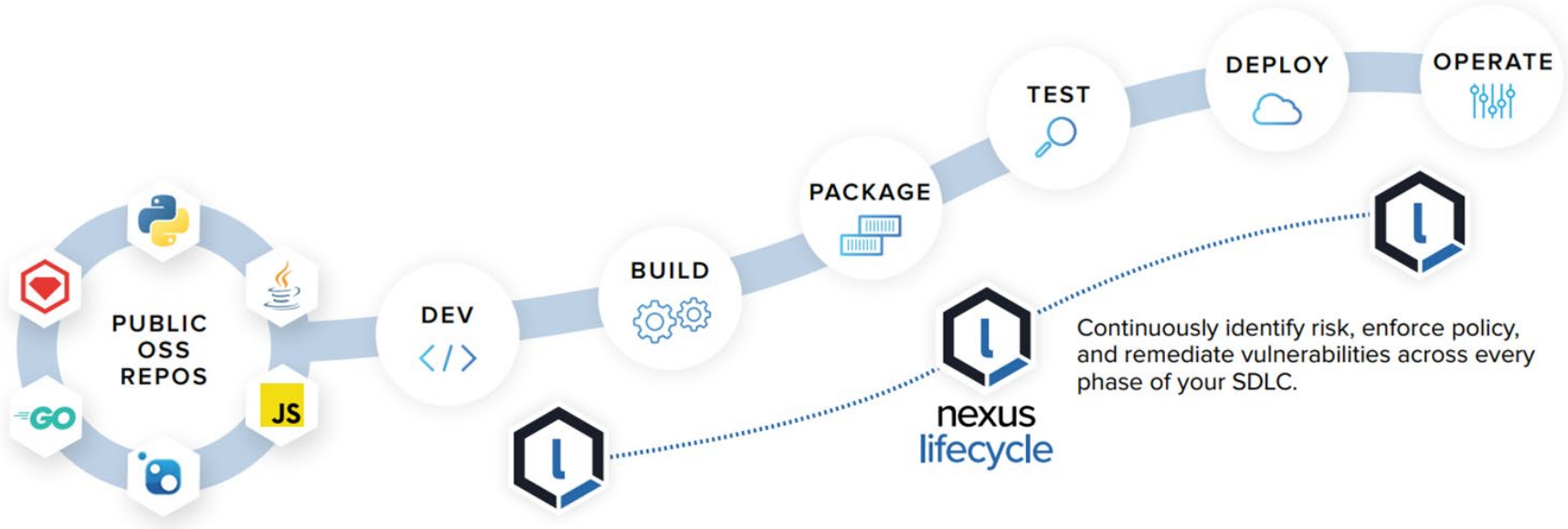


sonatype

Nexus Lifecycle

World #1 Software Composition Analysis

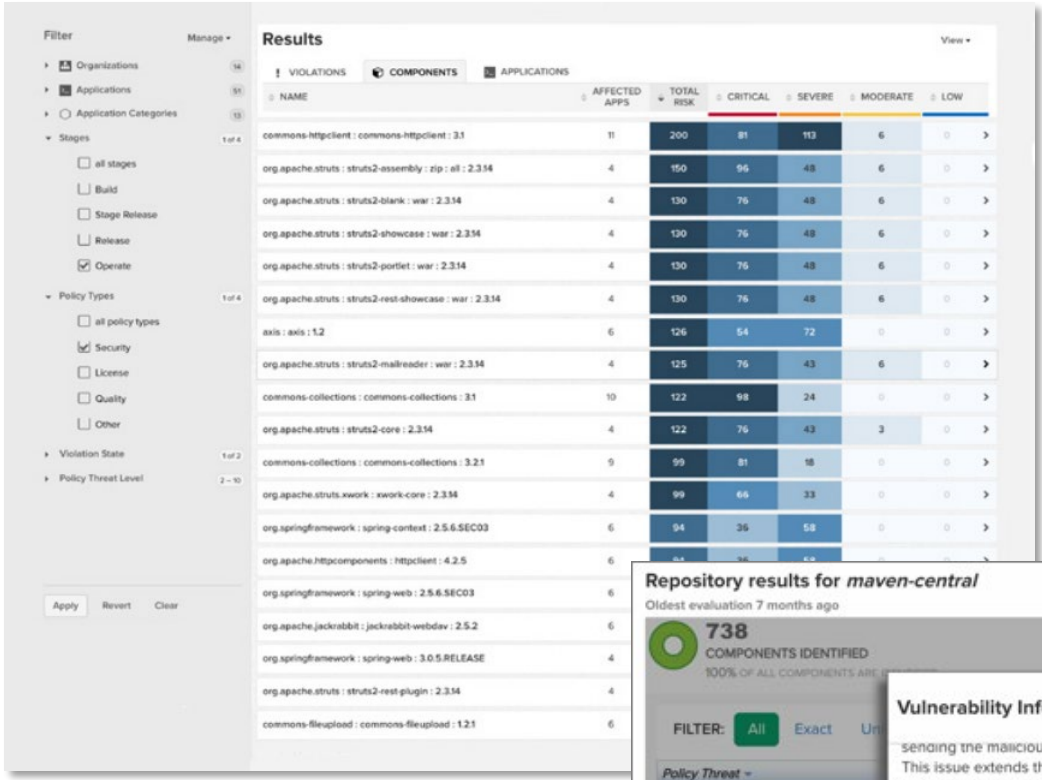
Nexus Lifecycle은 개발자 및 보안 담당자가 Opensource를 보다 안전하게 사용하면서 혁신 추구



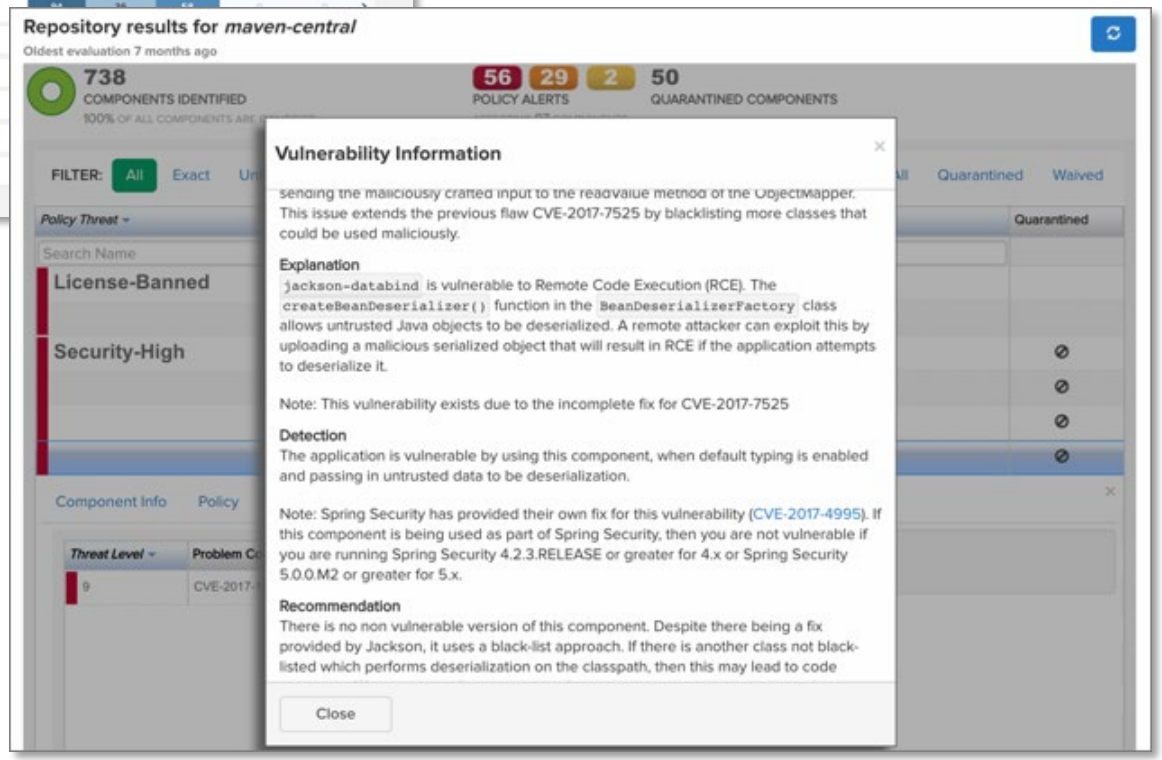
현업에서 사용하는 Pipeline 툴과 사전 정합 되어 있습니다.

Nexus Lifecycle

World #1 Software Composition Analysis



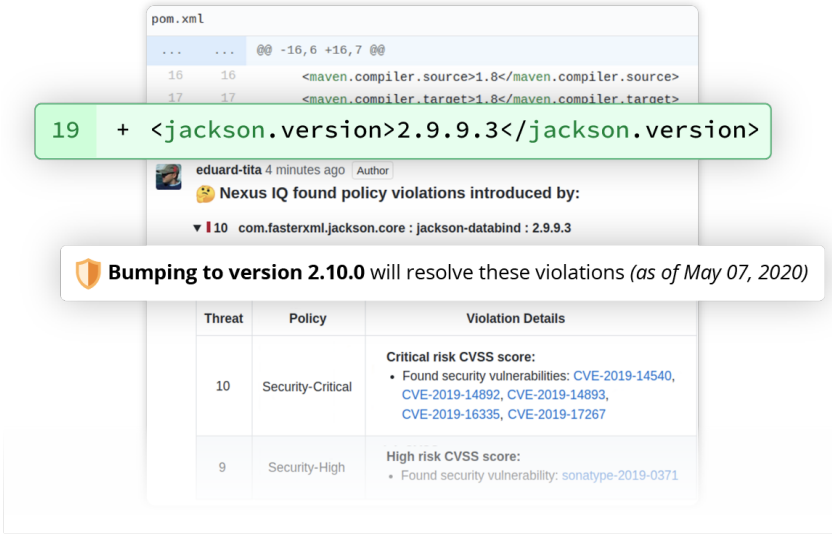
SBOM(Software Bill of Material) 자동 생성 : Opensource 리스크 및 3rd-party 의존성 확인



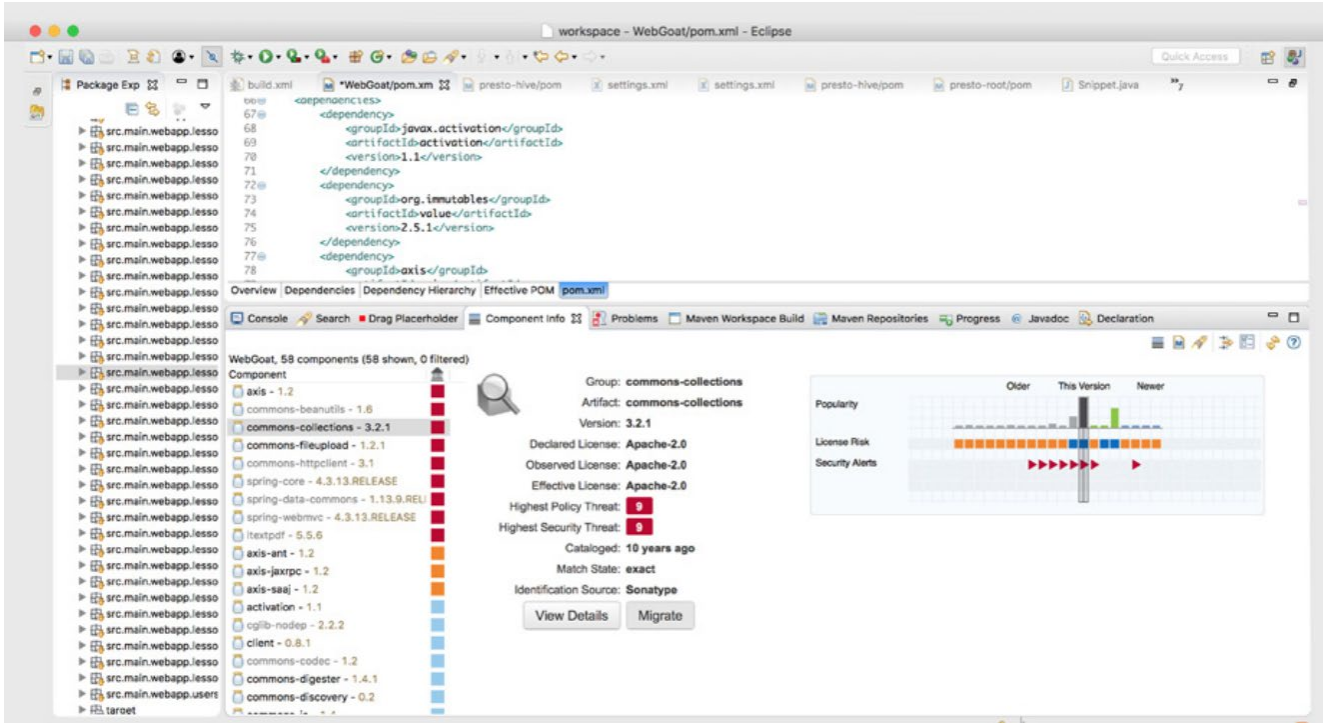
위험요소에 대한 전문 교정가이드 제공

Nexus Lifecycle

World #1 Software Composition Analysis



GitHub, GitLab, BitBucket, Eclipse, IntelliJ, 및 Visual Studio 등 정합을 통해 실시간 정보를 참조하여 한번의 클릭으로 최적의 컴포넌트를 선택

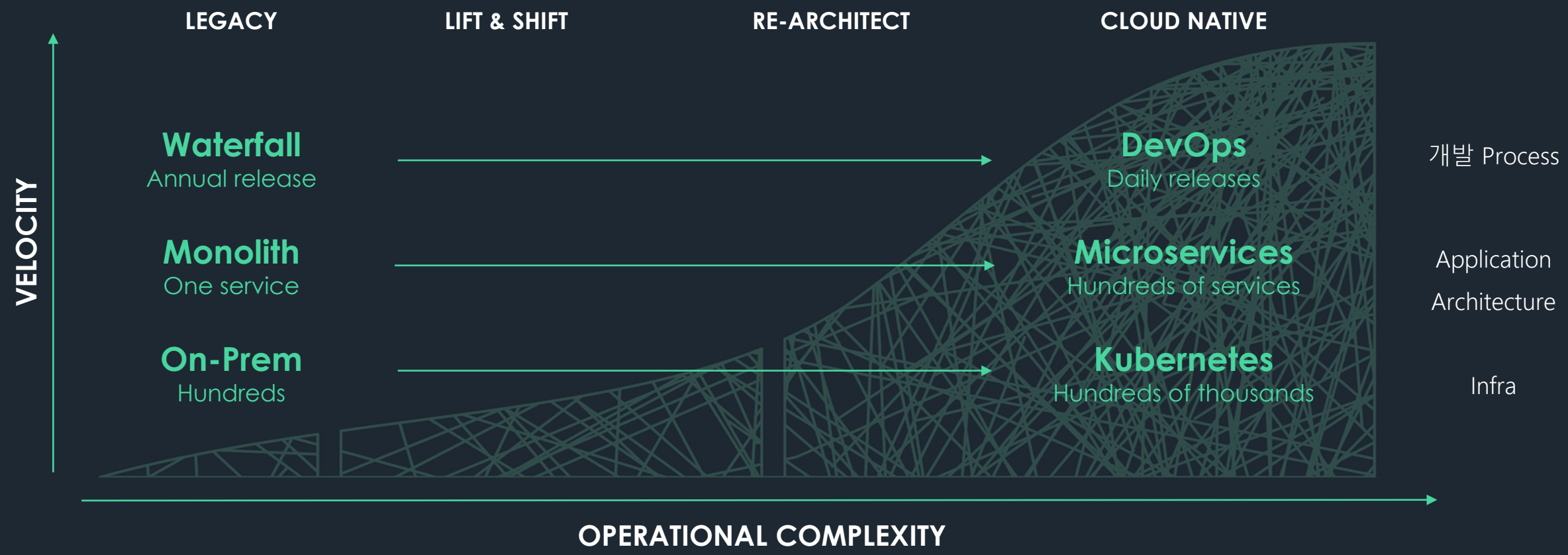


3. SRE (장애 진단) - Gremlin

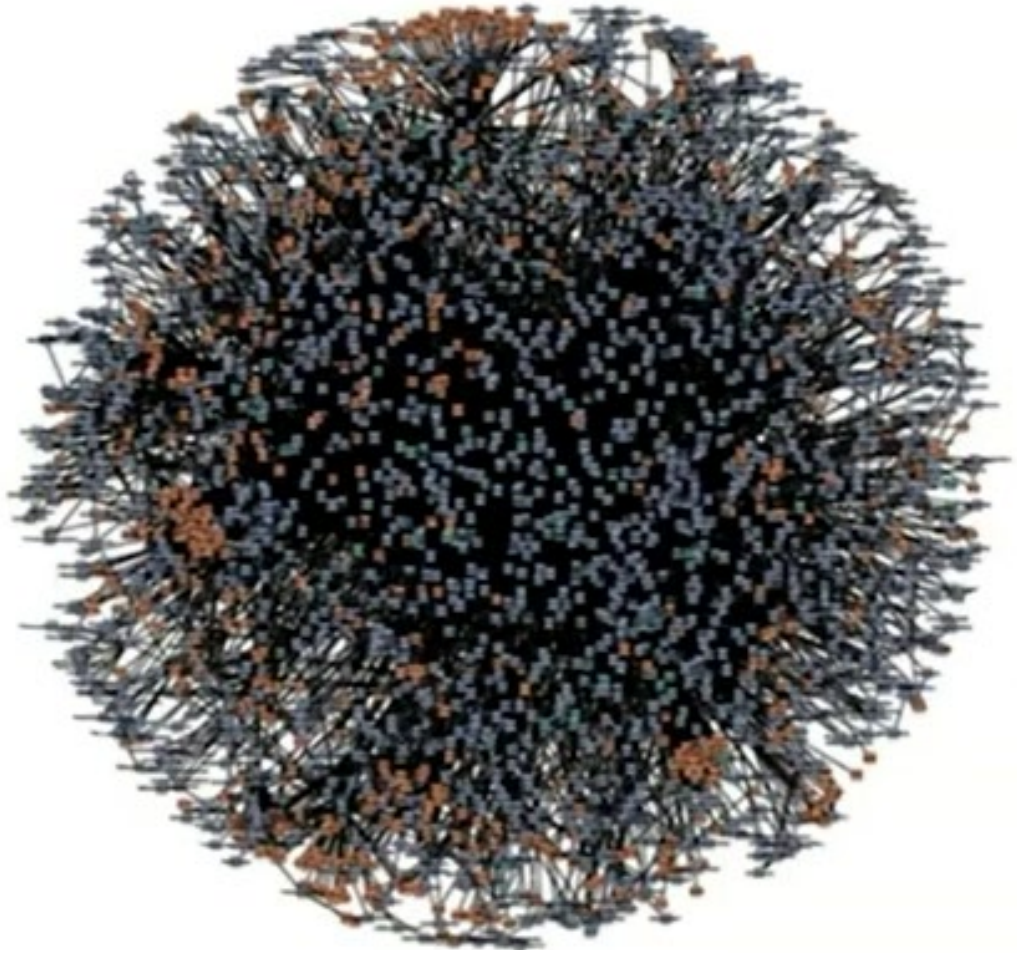
속도는 상응하는 대가를 요구함

Velocity Comes at a Price

Application/Service는 급격한 속도로 복잡해지고 있음 : 운영 난이도 증가

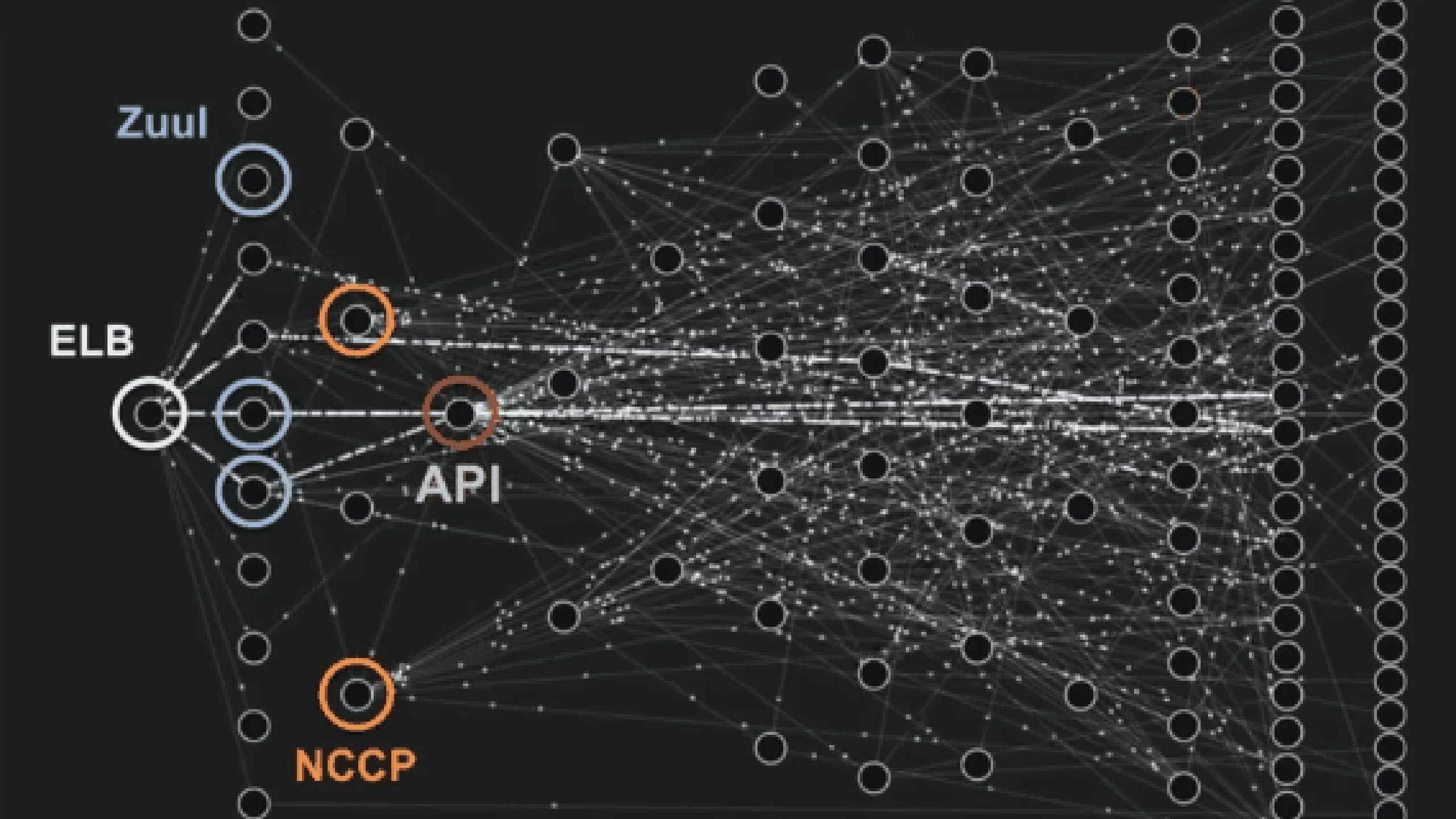


Container기반의 Service를 제공하는 Global 기업 예제

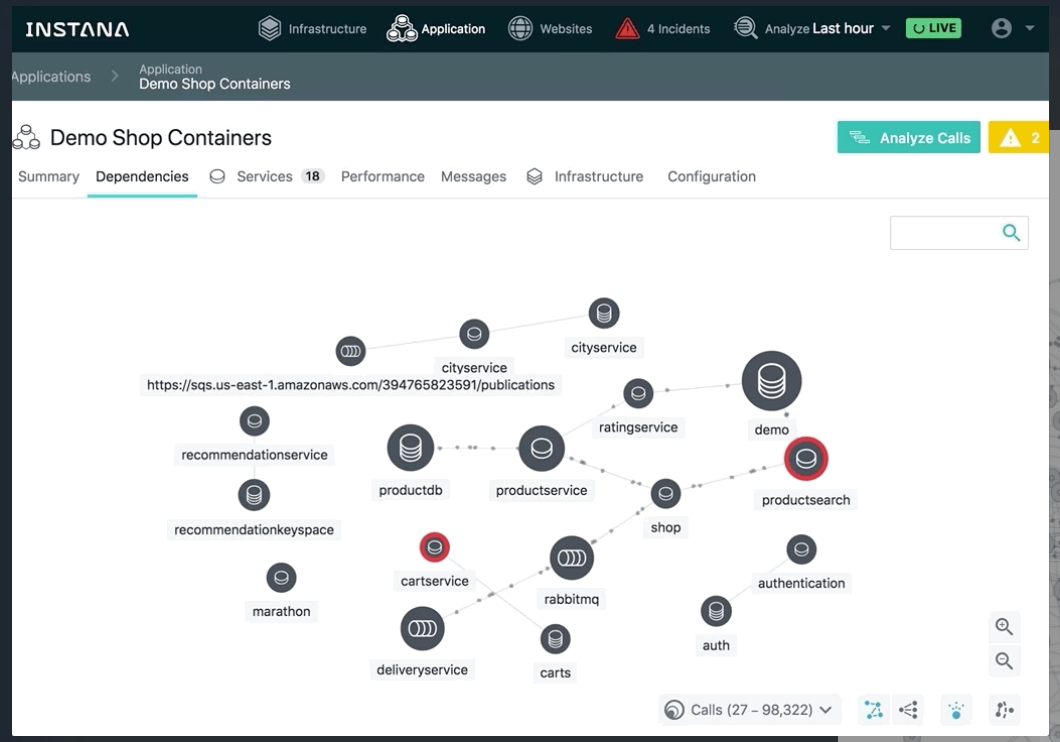


amazon

NETFLIX

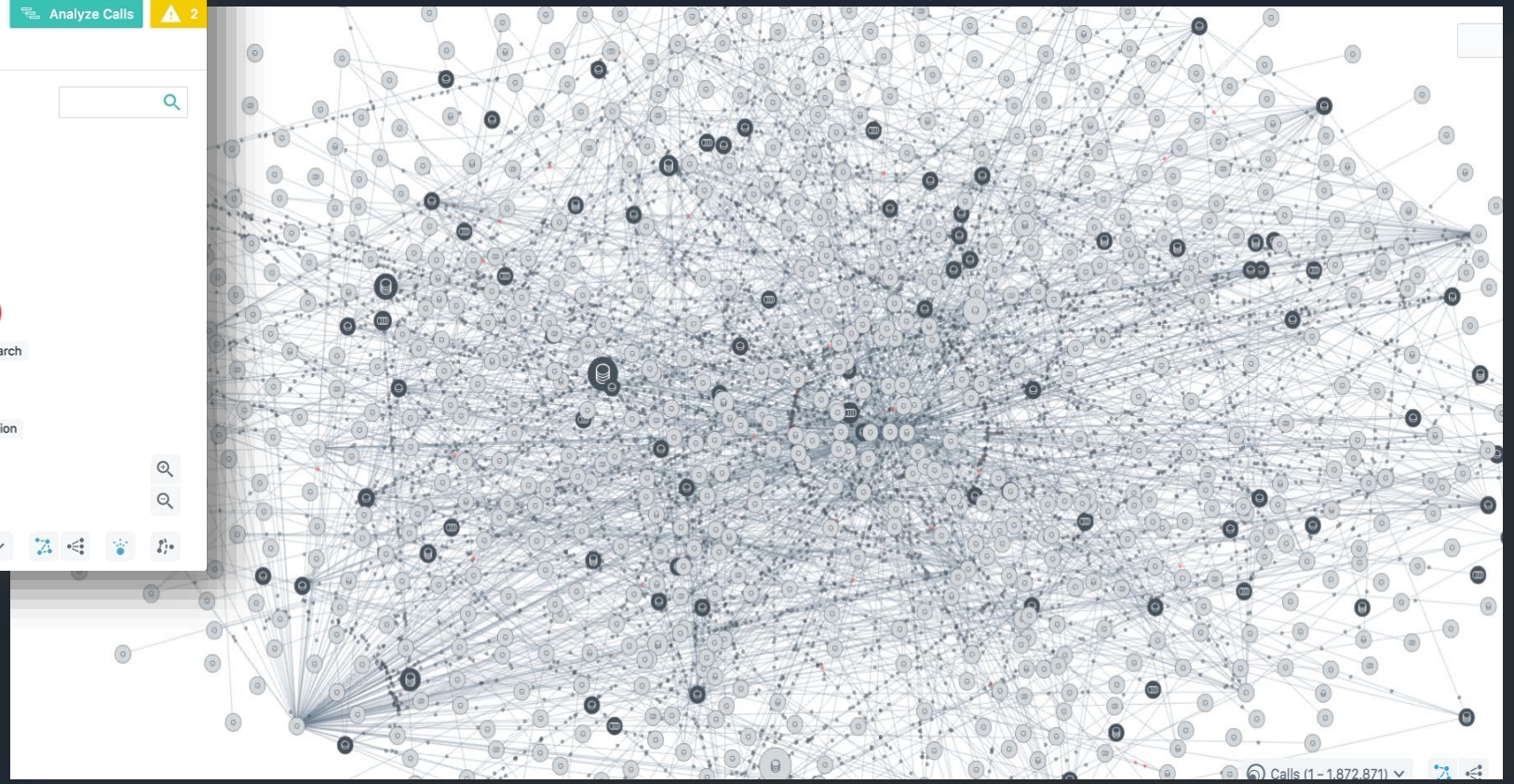

Zuul
ELB
API
NCCP

Dependency Map - Instana View



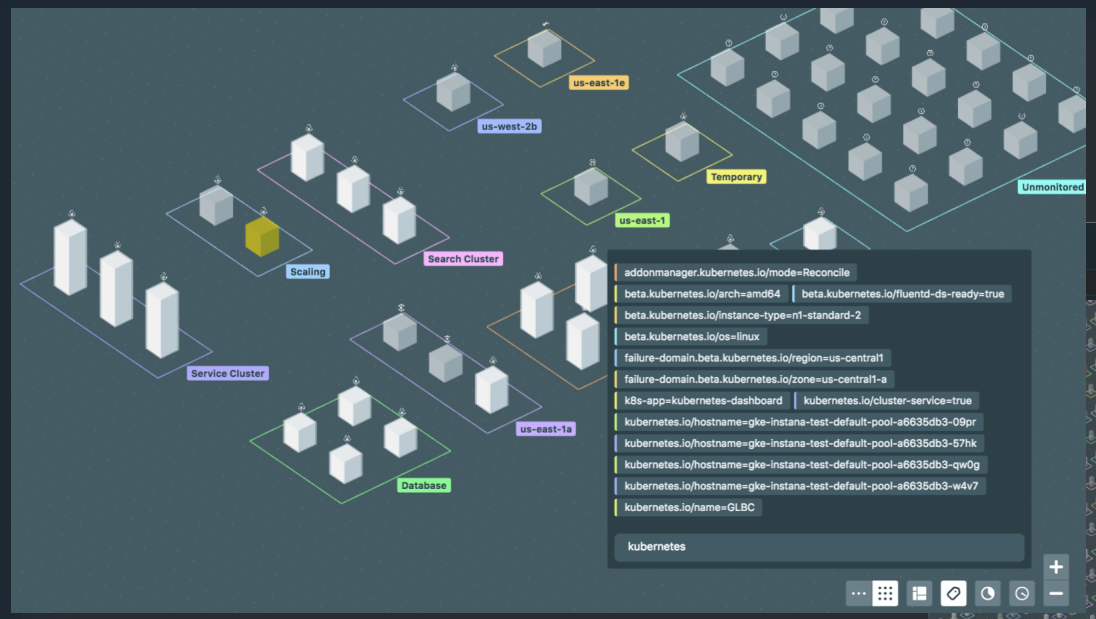
SIT / QA 환경

STG / PRD 환경



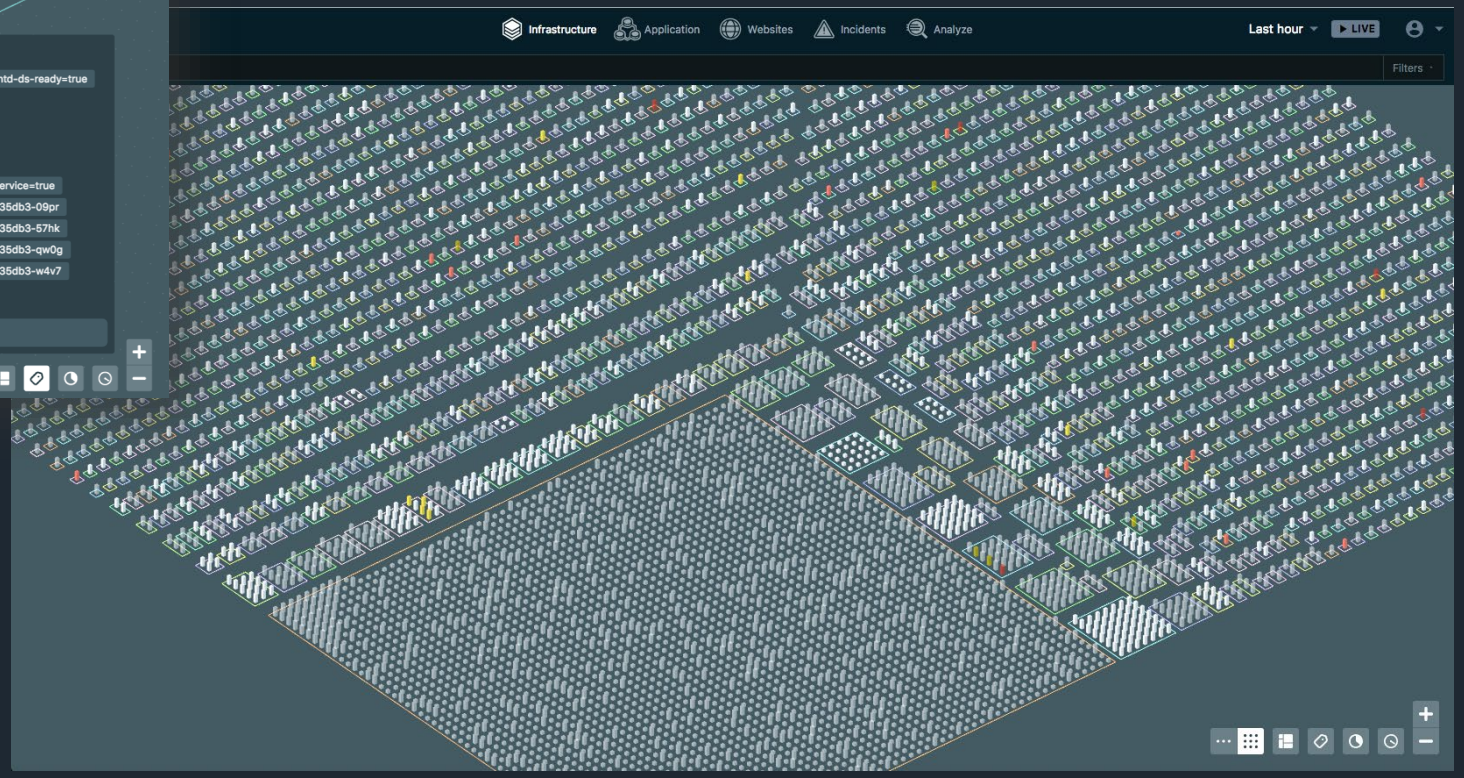
Infrastructure Map - Instana View

INSTANA



SIT / QA 환경

STG / PRD 환경



빠른 혁신의 이면 - 장애사례 3가지

Black Friday 장애

Forbes

기술 Issue로 인해 수조원대 손실이 발생한 유통업체

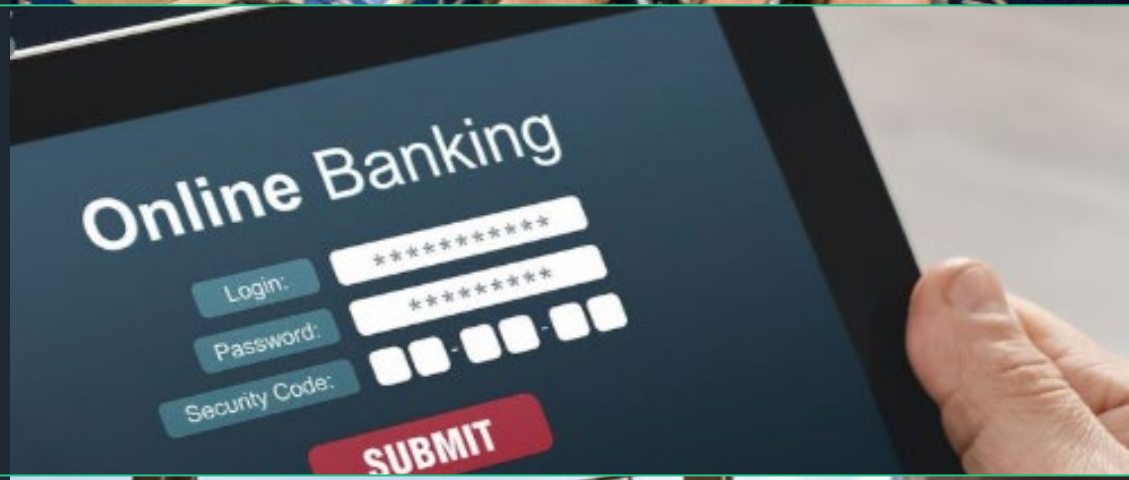
12.01.16

금융 장애

Newsweek

City Bank Web-site, Mobile Service 장애

2.28.19



항공사 장애

npr

System 장애로 인한 항공일정 지연

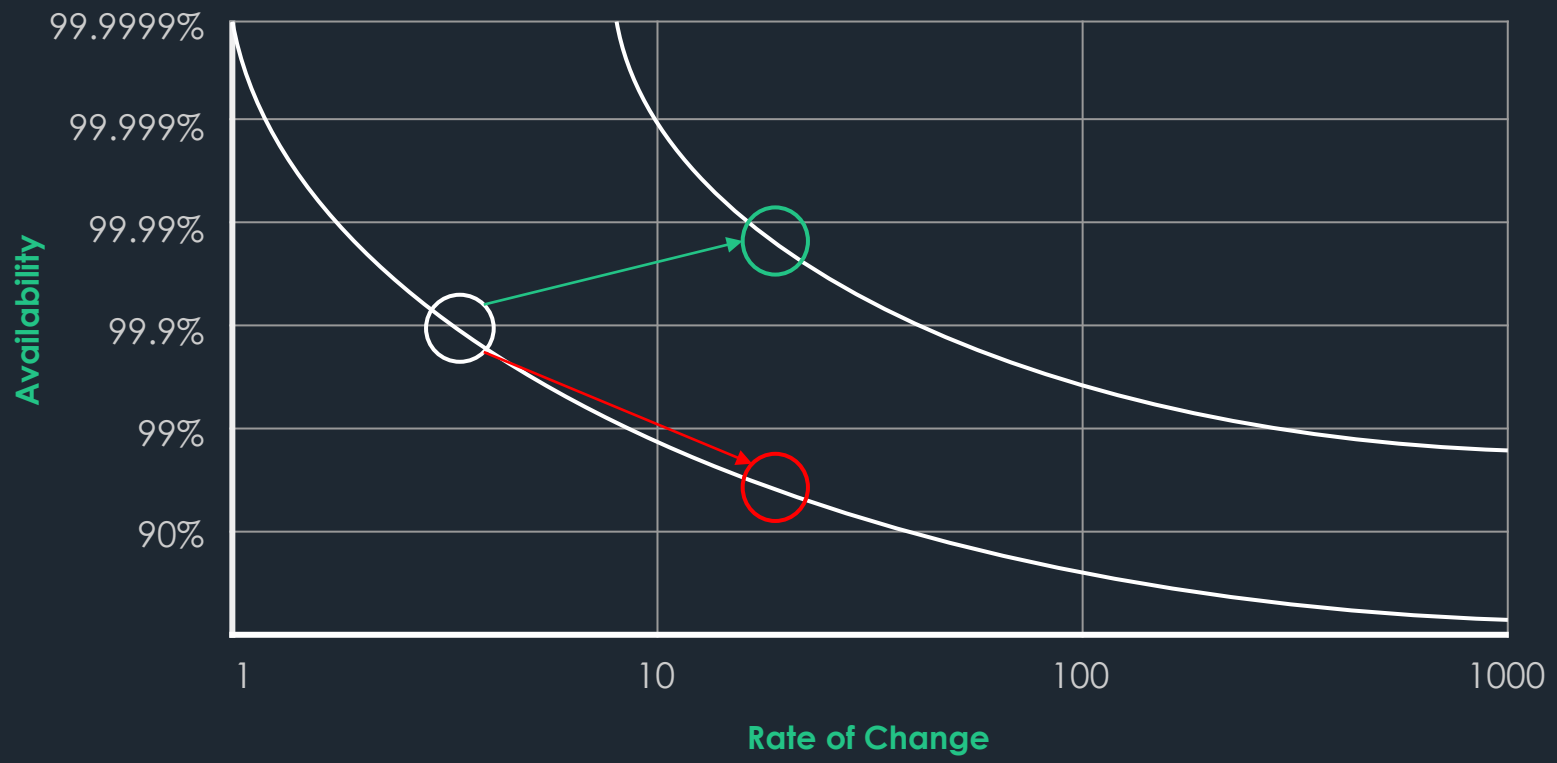
4.1.19

Gremlin

The Reliability Gap

"잦은 배포에도 품질수준을 유지하기 위한 방안 필요"

가용성 vs. 변경 속도

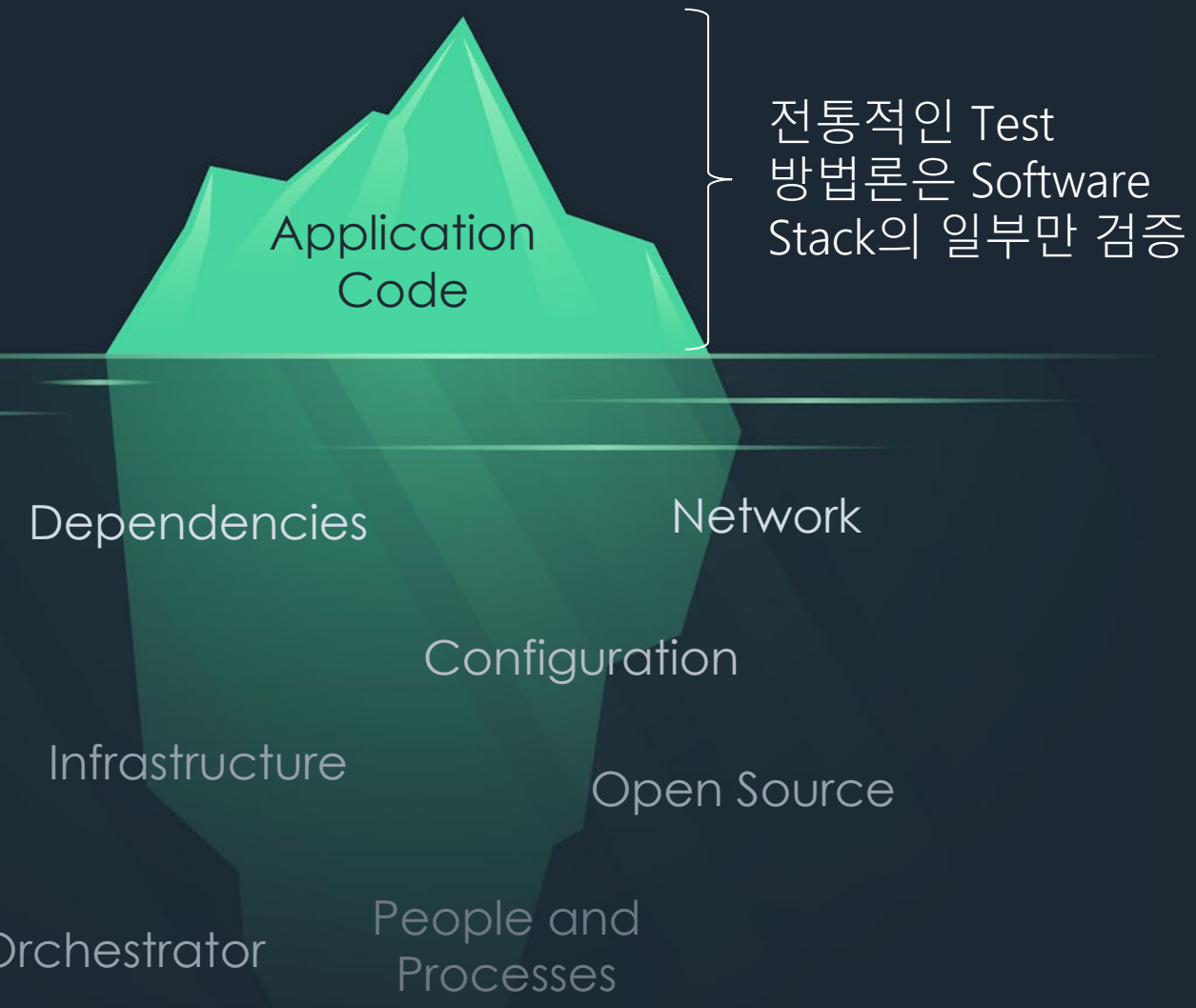


Change introduces new forms of failure that are difficult to see before the fact....

– Richard Cook, How Complex Systems Fail

전통적인 Test 방법론의 한계

Traditional Testing
is not enough
anymore.

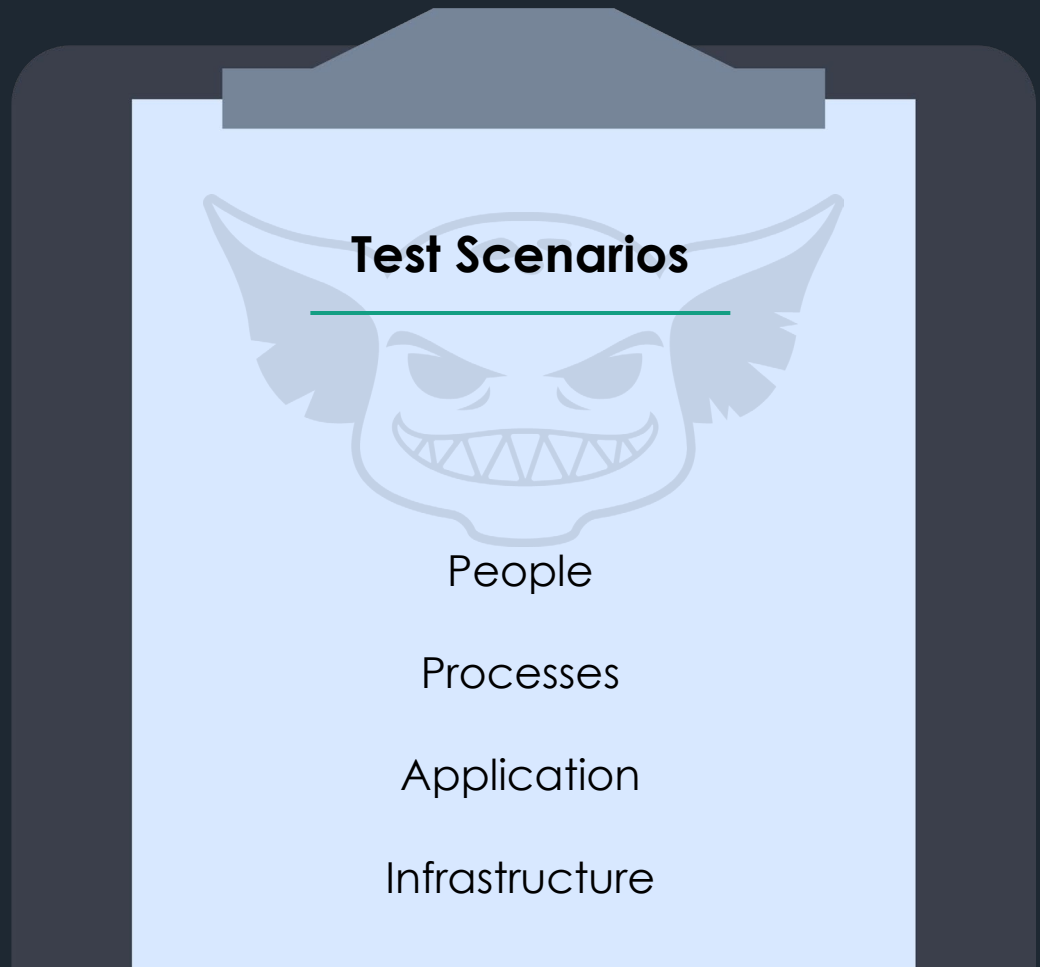


Chaos Engineering의 가치 – System의 취약점을 실험을 통해 확인

> Chaos Engineering은 System이 어떻게 반응하는지 확인하기 위해 제어 가능한 수준의 장애를 인위적으로 발생시켜 System의 취약점을 찾아내는 것

Chaos Engineering

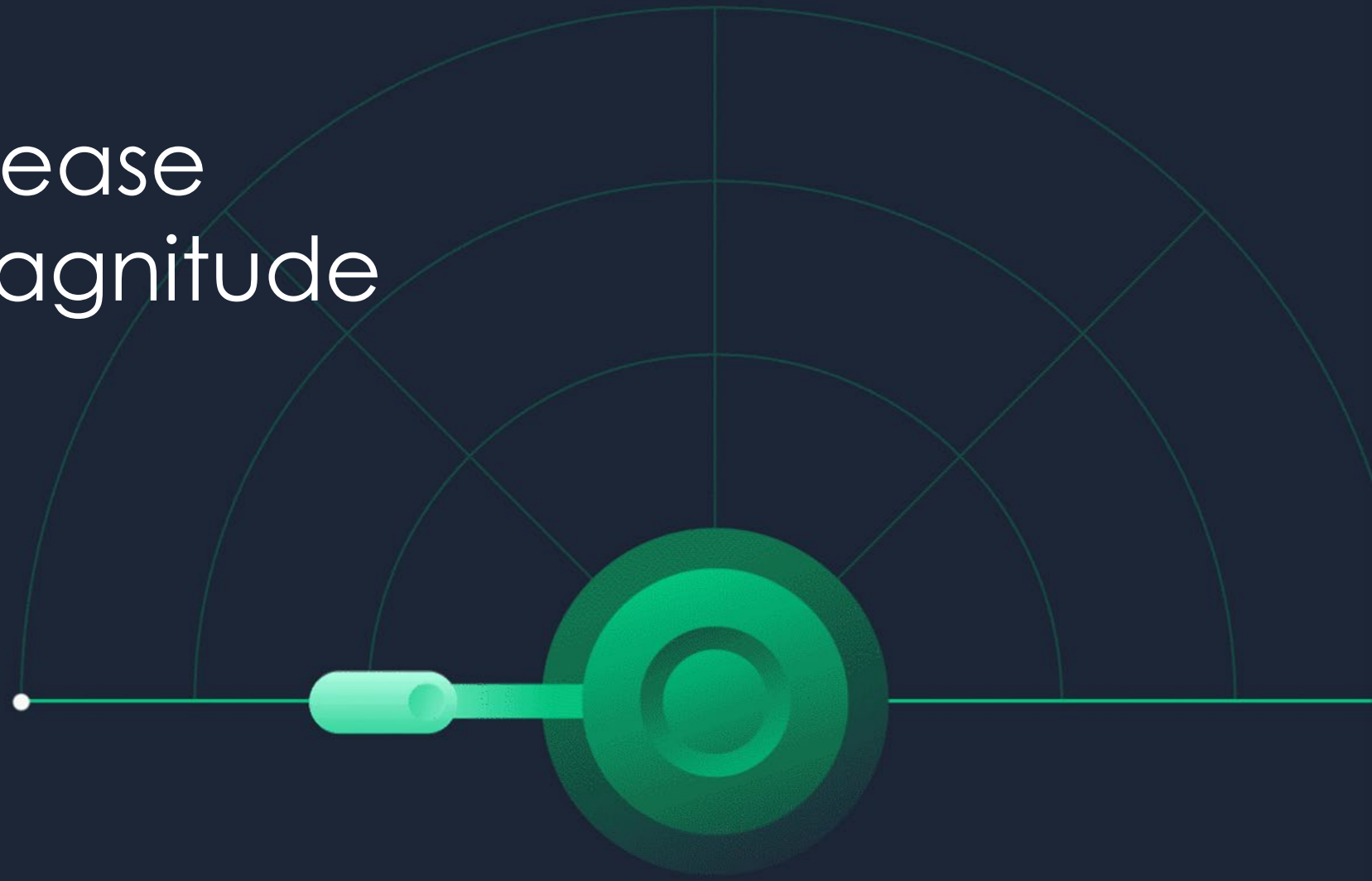
Thoughtful, controlled experiments designed to reveal the weakness in our systems.



OSC

Progressively test
your system to
isolate problems
and mitigate risk

Gradually increase experiment magnitude



Chaos Engineering은 선도적으로 Issue를 찾아내며, System의 취약점을 사전에 확인하여 장애 대응력을 향상시킴

기대효과

장애 요소 선제적 조치

Engineers **proactively** test to find and fix issues and limit the impact of failures

장애 대응력 향상

And are more effective when they work **reactively** during an incident

운영환경의 Monitoring & Detection 방식을 세부적으로 튜닝하여 위험요소 감소

> *Chaos Engineering changes the exercise from one of guessing, to one of staging and observing. It helps mitigate risk from emergent failure paths that we literally have no other way to discover.*

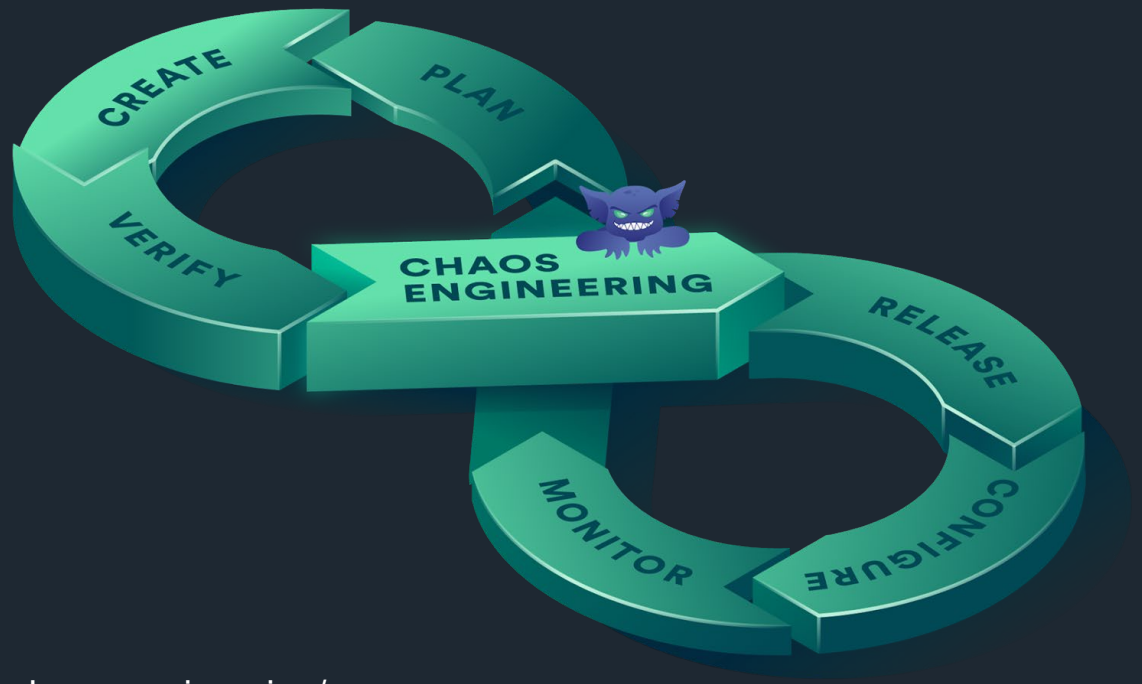
Workiva

Matt Simons
Sr. Engineering Manager

Chaos Engineering completes DevOps

" 분산System을 안정적으로 운영하는 유일한 방법은 Chaos Engineering을 도입하는 것 "
- Gartner

> *By 2023, 40% of organizations will implement chaos engineering practices as part of DevOps initiatives,* ***reducing unplanned downtime by 20%.***
>
> –Gartner

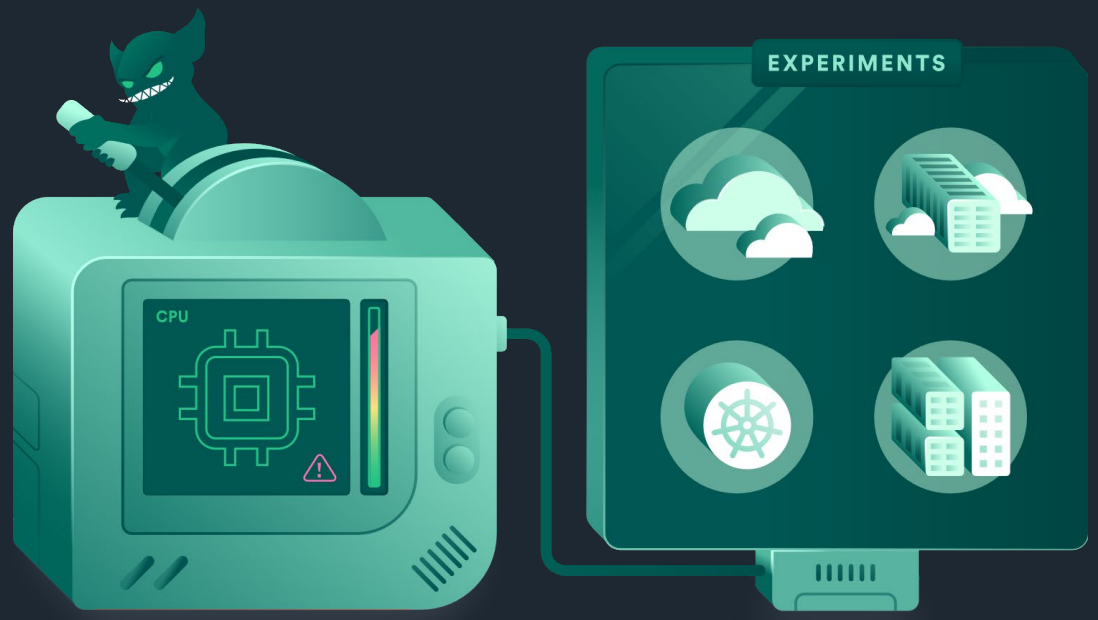


"2023년까지 40%의 조직이 Chaos Engineering을 DevOps의 일환으로 도입하여 Downtime을 20% 감소시킬 것" - Gartner

https://www.gartner.com/smarterwithgartner/the-io-leaders-guide-to-chaos-engineering/

Chaos Engineering Platform

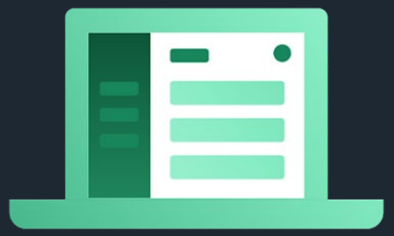
Gremlin



Why Gremlin?

"Failure as a Service"

복잡한 System의 장애요소를 찾아내는 경험과 전문성에 기반한 Solution



Simple

단순한 Interface와 정리된 API 문서 제공

Safe

안전한 장애 유발 및 해소, Roll Back 지원

Secure

SOC II 인증
RBAC, MFA, SSO

Comprehensive

다양한 Stack Layer에 대한 Attack 지원

Gremlin Architecture & Use Cases

Expedia® | TARGET | UNDER ARMOUR | NIKE | Workiva | qualtrics.

Cloud 전환 | Team 교육 | Cloud Native 전환 | Monitoring/Tool 검증 | 의존성/상관관계 검증 | DR 검증

Gremlin

Simple Interface
UI | CLI | API

Orchestration
Schedule | Scenarios

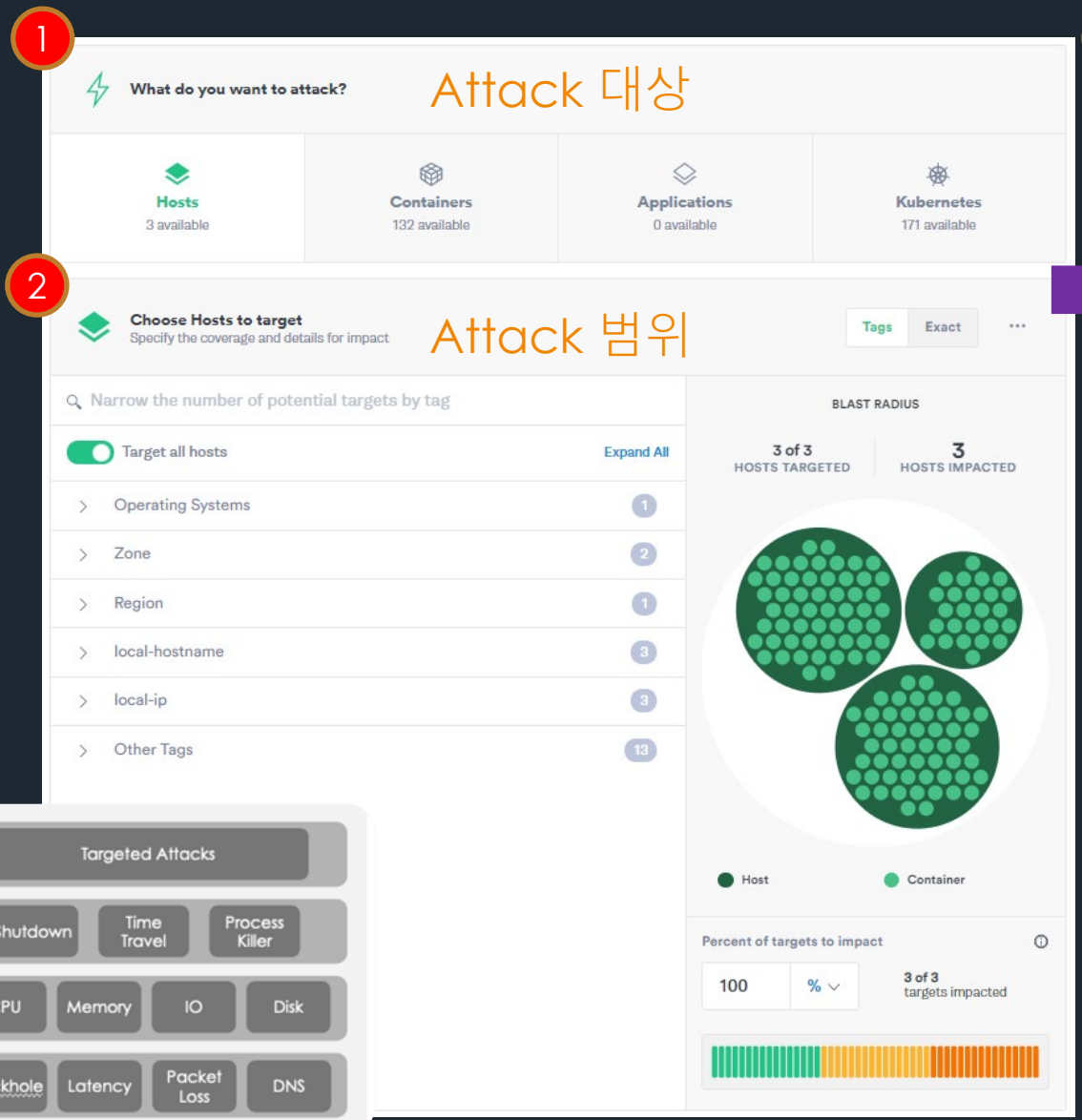
Safety
Magnitude | Blast Radius | Halt Button

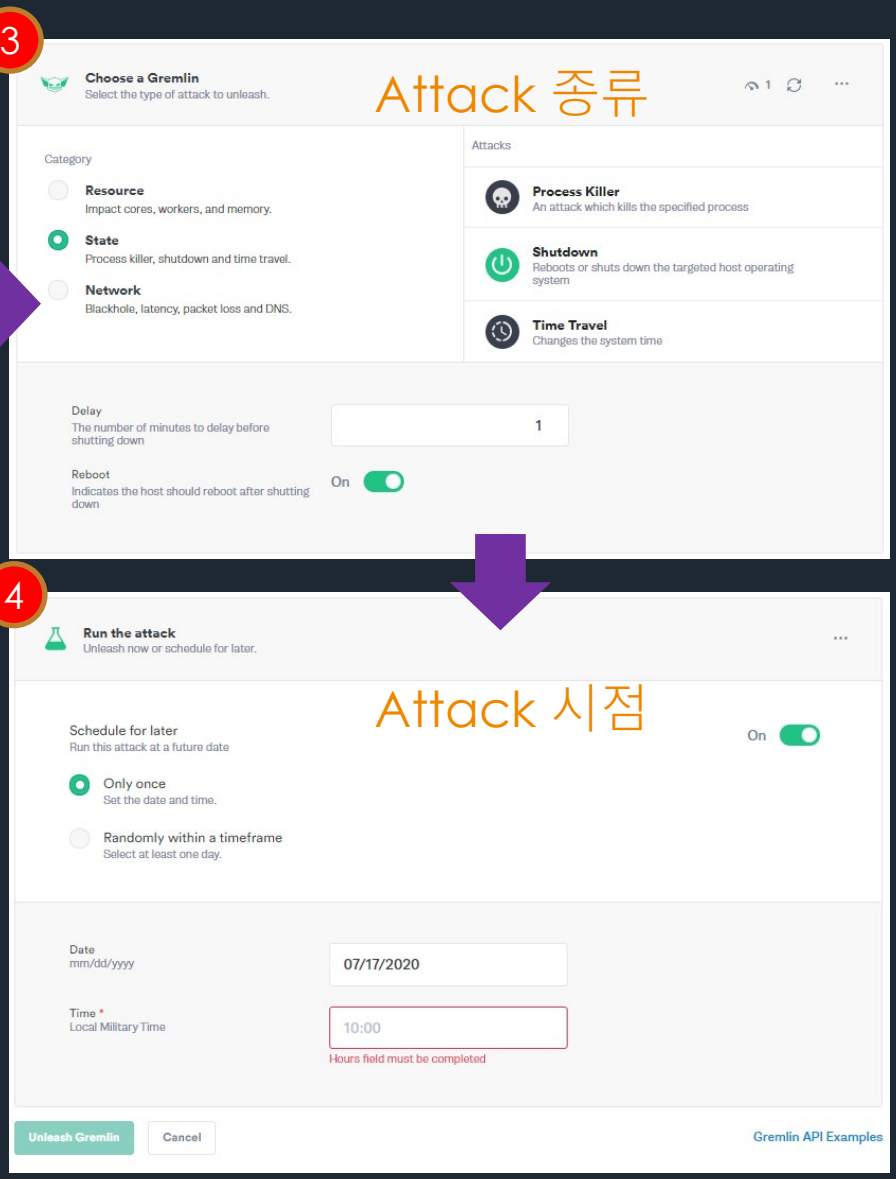
Security
MFA | SAML | Google SSO | RBAC | Access Logs

Attacks
Network | Resources | State

VMware | AWS | Azure | Google | Docker | K8S | Linux | Windows | Serverless

Attack Setup 절차

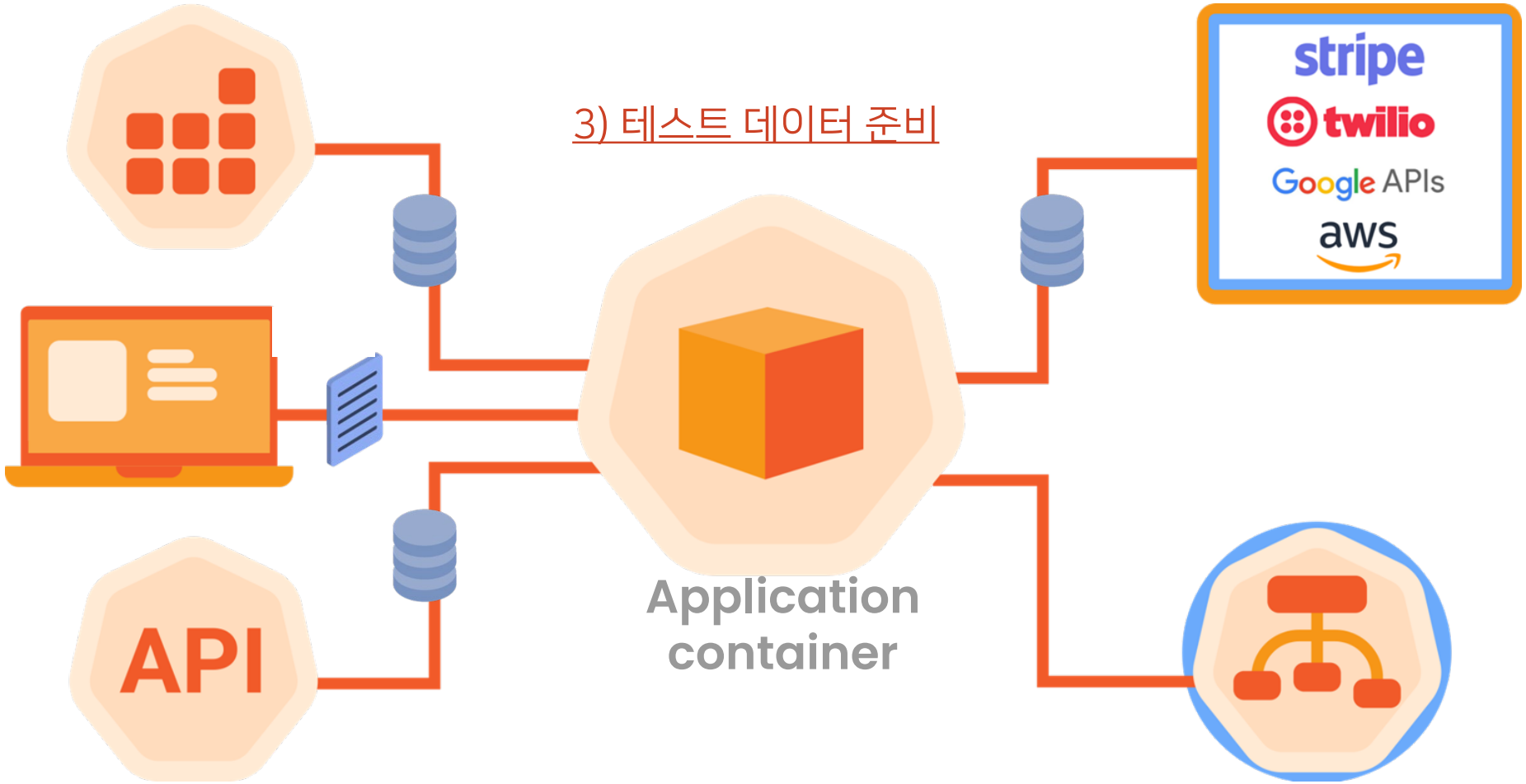




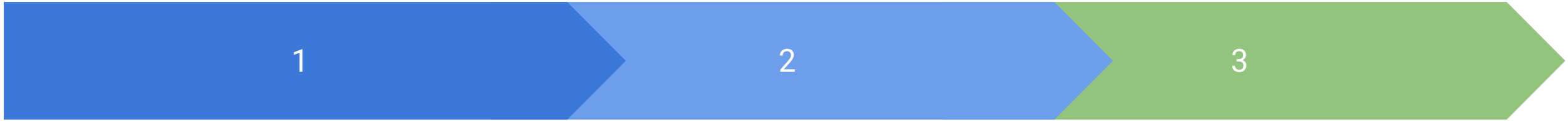
Gremlin

4. SRE (성능 진단) - Speedscale

API 테스트의 해결과제



이상적인 API 테스트 방법론



Identify

: 테스트 대상 확인

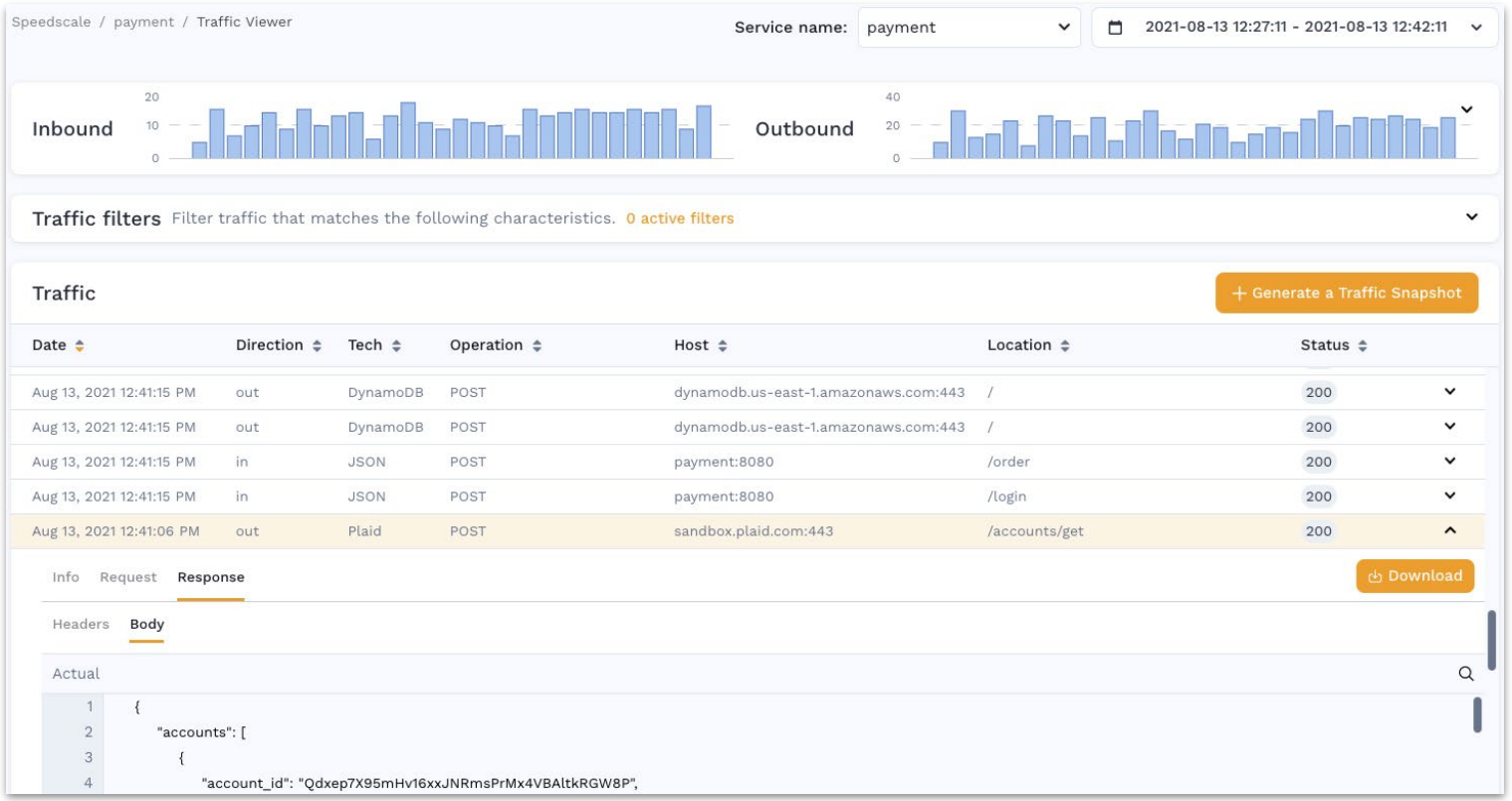
Generate

: 자동 테스트 생성

Run

: 안정된 테스트 환경 확보

Identify : 테스트 대상 확인



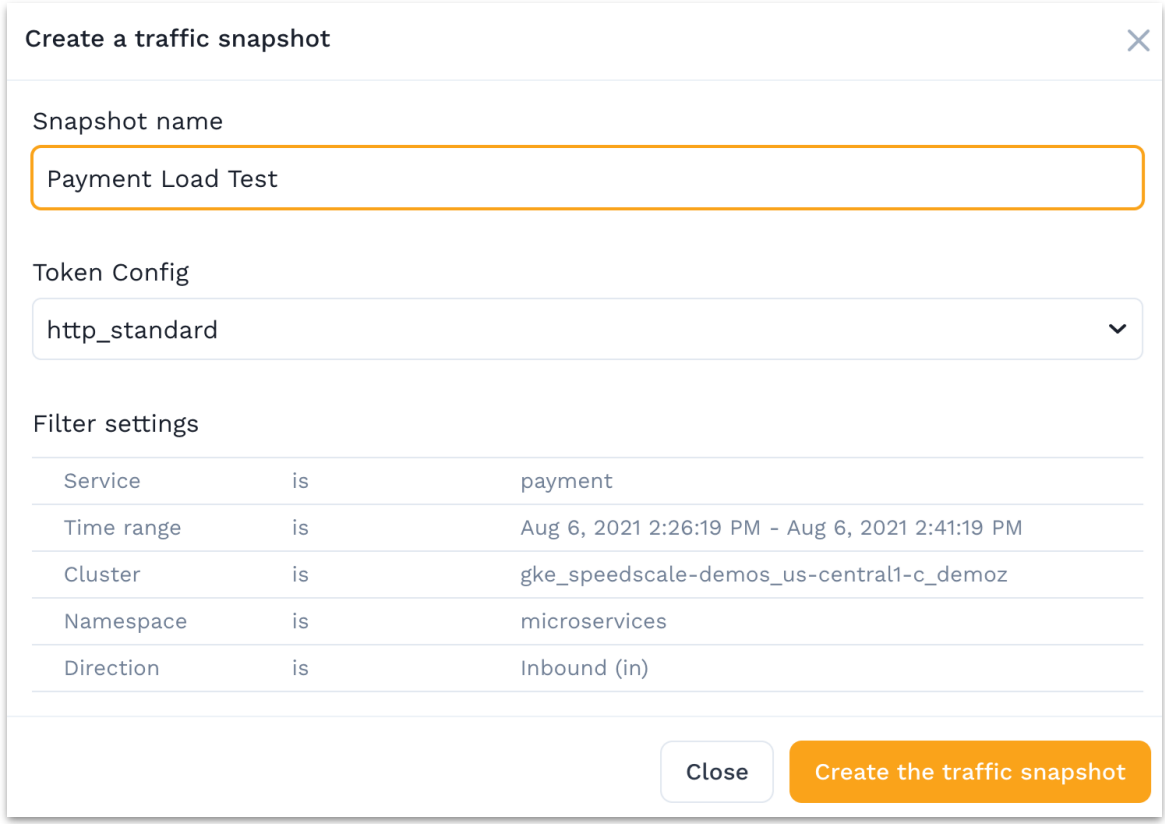
- API Call 확인
- 관련 기술 확인
- 세부 사항 확인

Generate : 자동 테스트 생성

1 2 3

- API 트래픽을 테스트 케이스로 변환
- 보안 토큰, 파라미터, Timestamp 등 업데이트
- 모든 Call 에 대해 응답 확인

"스크립트 작성 등 수작업 없이 테스트 케이스를 자동 생성하며 Replay가 정상적으로 동작하도록 트랜잭션내 주요 데이터를 자동으로 변경 "

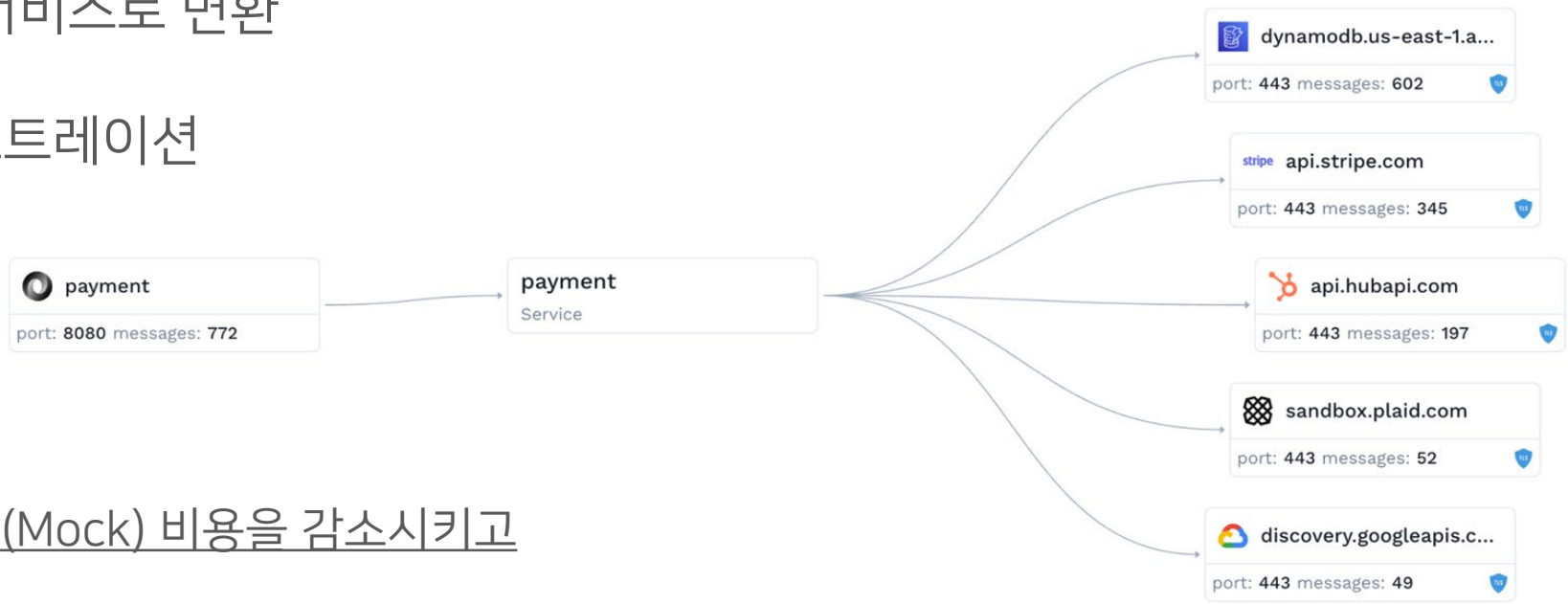


SPEEDSCALE

Run : 안정된 테스트 환경확보

1 2 3

- 마이크로 서비스 의존성 탐지
- API 트래픽을 Mock 서비스로 변환
- 데이터 및 환경 오케스트레이션

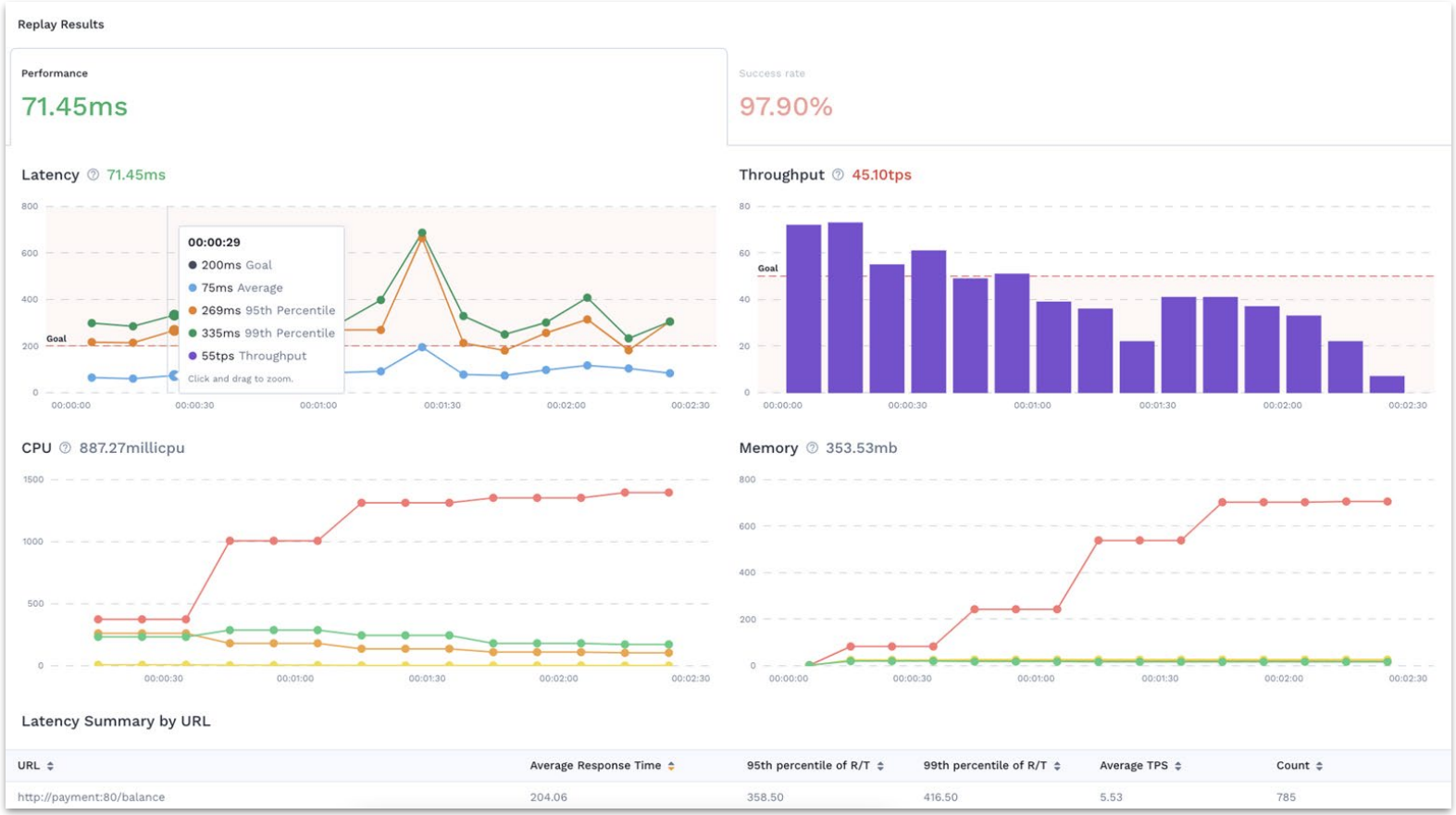


"외부서비스를 대신 응답하여 (Mock) 비용을 감소시키고

테스트를 위해 충분히 안정된 환경을 확보 "

SPEEDSCALE

Use Case : SRE팀의 성능검증



SRE 골든 시그널(Golden Signals)

- Latency
- Throughput or Traffic
- Success Rate or Error
- Saturation

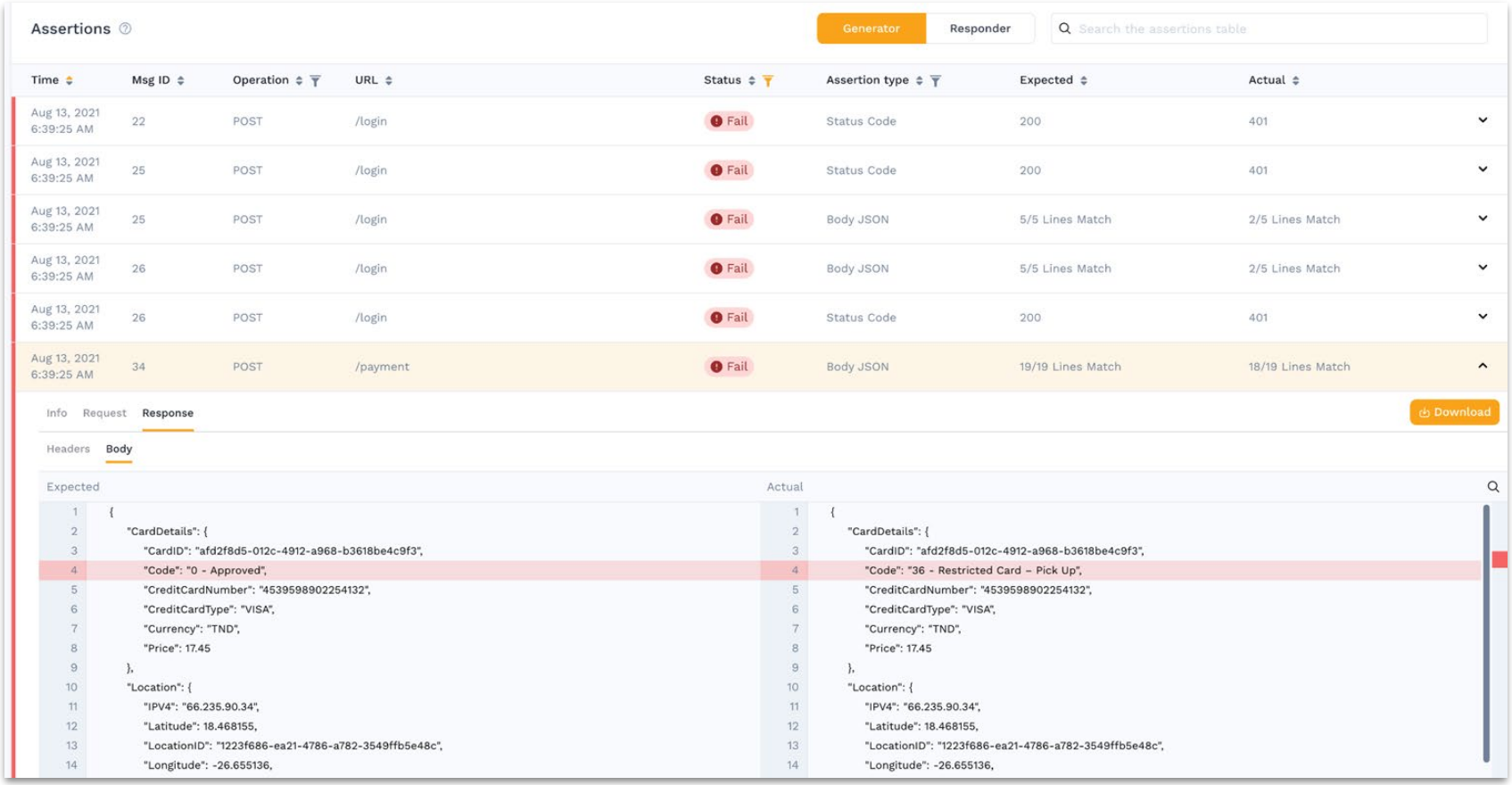
 www.speedscale.com

SPEEDSCALE

Use Case : 소프트웨어 개발 엔지니어 기능 테스트

Call 검증

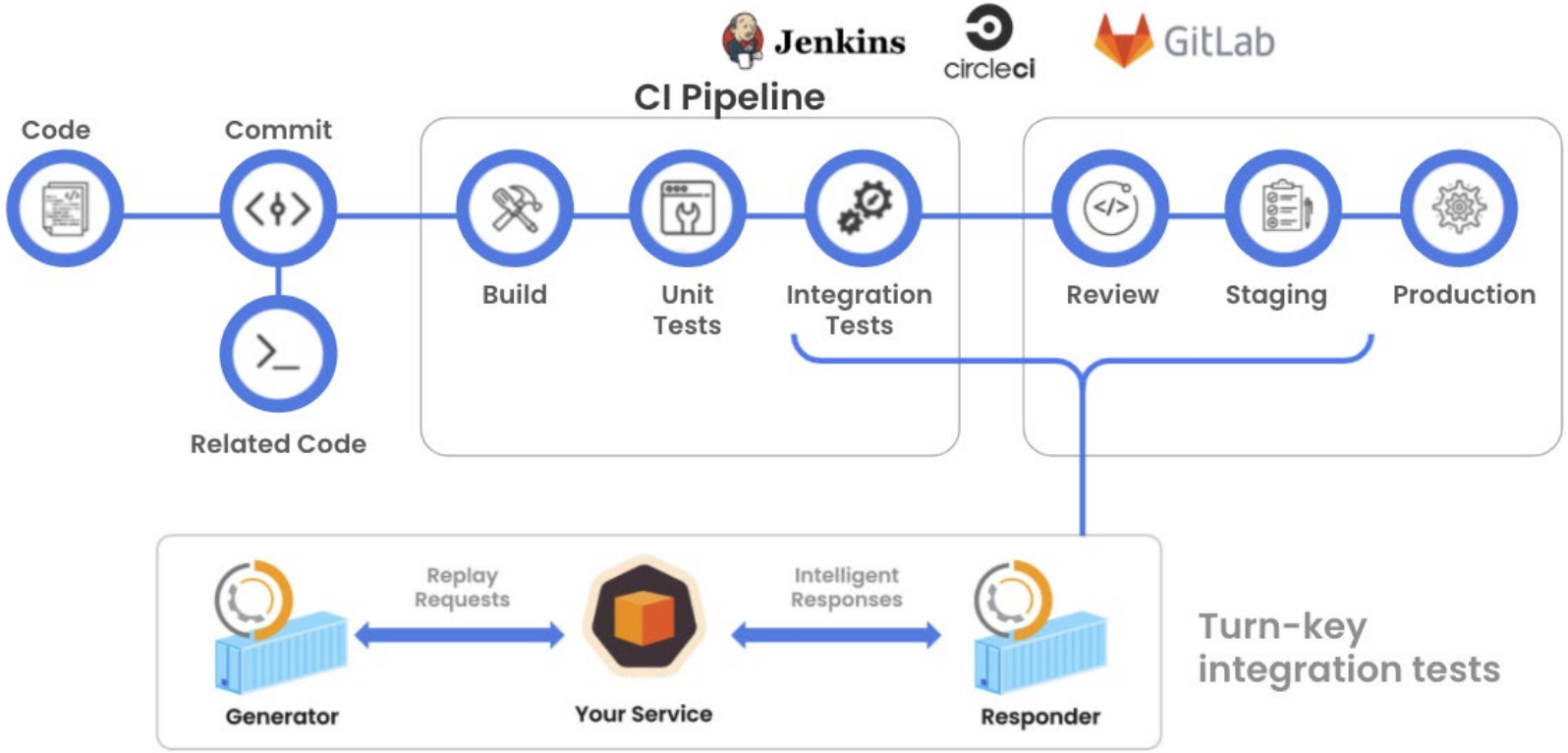
- 비교
- 차이점 분석
- CI 정합



CI Integration

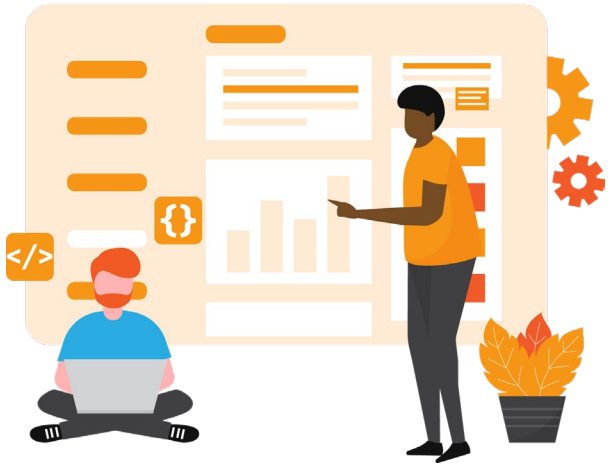
Continuous Resiliency for Kubernetes

CI Integration을 통해 새로운 빌드에 대해서 즉각적인 검증 수행



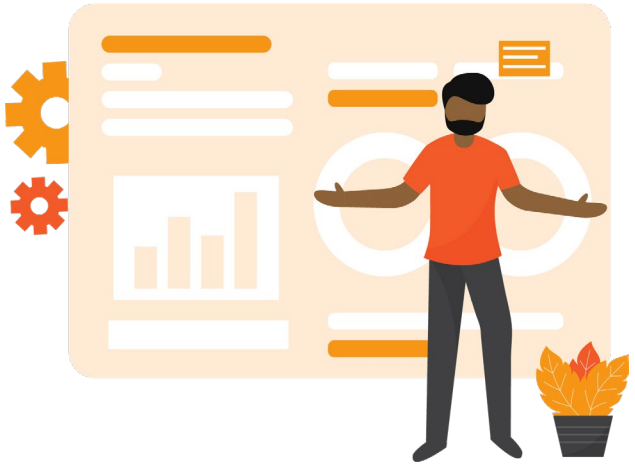
Speedscale 가치

Engineers



- 테스트 생성 자동화
- 실제 환경 상시 구현

SRE / DevOps Pros



- E2E 테스트 환경 쉽게 확보
- 자동화된 SLO 구현
- Production 장애 예방

Executives

- 안전한 구축 환경 확보
- Cloud 비용 감소

5. OSC Korea 소개

OSC Korea 소개

- Opensource(O), Security(S), Content_Delivery(C) 기반을 Motto로 아태지역 중심의 ICT Business Platform Group
- 오픈소스 기반의 전문 Knowledge Service 및 신기술 컨설팅, 설계, 구축, 개발, 운영, 자문 서비스
  - Linux 한국 재단(비영리) 활동을 통해, Opensource 기반의 다양한 기술 Trend, 전문성 및 생태계 Partner 보유
  - 다양한 신기술 Knowledge/경험과 폭넓은 Global Network을 지속적인 신규 솔루션 및 서비스 확보

OSC Asia Group Limited

- 2008년 설립 in Hong Kong
- 아시아 시장의 ICT 분야 Business Development Platform Group
- 아시아 지사 : 한국, 중국, 싱가포르, 대만, 홍콩

삼양데이터시스템(주)

- 삼양데이타시스템㈜, 지주회사인 ㈜삼양홀딩스가 전략적 투자
- Public Cloud 사업 확장, 고도화를 위해, Opensource 기반의 전략적인 WIN-WIN 구조로 사업의 Synergy 기대

samyang 삼양홀딩스

samyang 삼양데이타시스템

Linux 한국 재단 - 비영리 재단

- Global 최대의 Opensource Technology Projects 운영 및 생태계 Governing 재단
- Linux 재단 산하 주요 Project들에 대해 국내 활성화를 위한 다양한 활동 i.e., CNCF(Cloud Native Computing Foundation), Hyperledger, LF Edge, LF AI, OpenChain, 등

THE LINUX FOUNDATION

CLOUD NATIVE COMPUTING FOUNDATION

▪ OSC 사업 영역

- Opensource 기반 DevOps, MSA 전문 기업 & 신기술 Solution Incubation 전문 기업의 시장 선도

Opensource 기반의 MSA(Microservice) 전문 기업

- Opensource 기술(Kubernetes, Rancher, Kafka, AI/ML, NoSQL/SQL, BlockChain, Edge, 5G 등) 이용한 설계, 구축, 개발, 컨설팅 및 공인 교육 서비스
- Opensource 와 Cloud Native 기술로, Vendor Lock-in 과 특정 Cloud Provider(AWS, Azure, etc)의 Lock-in 방지 및 Agile 한 CI/CD, DevOps, MSA 설계, 개발, 구축, 유지보수, 자문
- 다양한 MSA 방법론(DDD, Event-Driven, Event-Sourcing with CQRS, etc)에 대한 기술 서비스

kafka RANCHER K3S WSO2
kubecost SUSE Gremlin AxonIQ
krakenD sonatype TIGERA CALICO GitLab

Global Solution Incubation 전문 기업

- Opensource를 포함한 최신의 Trend 및 다양한 신기술에 대한 경험 Insight를 통해, O(Opensource), S(Security), C(Content Delivery)기반의 다양한 글로벌 신기술 Solution 및 서비스 국내 선점
- Opensource 기반의 신기술 Solution(SaaS, PaaS, etc)에 대한 한국 지사 대행, 총판, 전략적 Partnership 체결
- 신기술 기반의 다양한 IT 분야 전문 Global Partner (Vendor)들과 함께, 한국을 포함한 Asia 시장 개척 주도

axual imply SPEEDSCALE INSTANA
solo.io TIGERA evergent Edgio
CONVIVA OCEANBLUE CLOUD DB VISIT LUMEN

OSC 사업 영역 - 계속

- Cloud & Cloud Native MSP(Managed Service Provider) 및 Opensource 공인 교육 사업

Cloud Native & Cloud MSP 기업

- 기업의 Cloud Infra와 Kubernetes, Cloud Native기반의 System을 운영 및 관리하는 IT 운영 서비스
- Cloud에 최적화된 기술 지원을 통해 반복되는 IT 서비스를 자동화하고, Issue/장애 발생 시 신속하게 처리
- Cloud & Cloud Native 전문 운영 인력 24 x 7 지원 체계와 폭 넓은 지원 범위를 기반으로 고객의 Cloud 내 computing, 보안, Network, Backup, Application 등 다양한 영역을 안정적으로 운영

aws
NAVER CLOUD PLATFORM
kubernetes
Microsoft Azure
RANCHER

Opensource 전문 공인 교육 기업

- Opensource, Cloud Native 중심의 실무자 교육 제공
- Linux 재단 공인 교육 Partner : Kubernetes 중심의 Admin, 개발자 On/Off site 교육 제공
- 국내 유일의 SUSE Gold 교육 Partner : Rancher 중심의 실무자 이론 및 실습 교육 제공
- 공인 강사 양성 및 기업 맞춤형 Curriculum 제공

THE LINUX FOUNDATION
AUTHORIZED TRAINING PARTNER
SUSE
Gold Partner
TRAIN
RANCHER

감사합니다.

We are your trusted Digital Transformation Partner

www.osckorea.com