

OSC



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

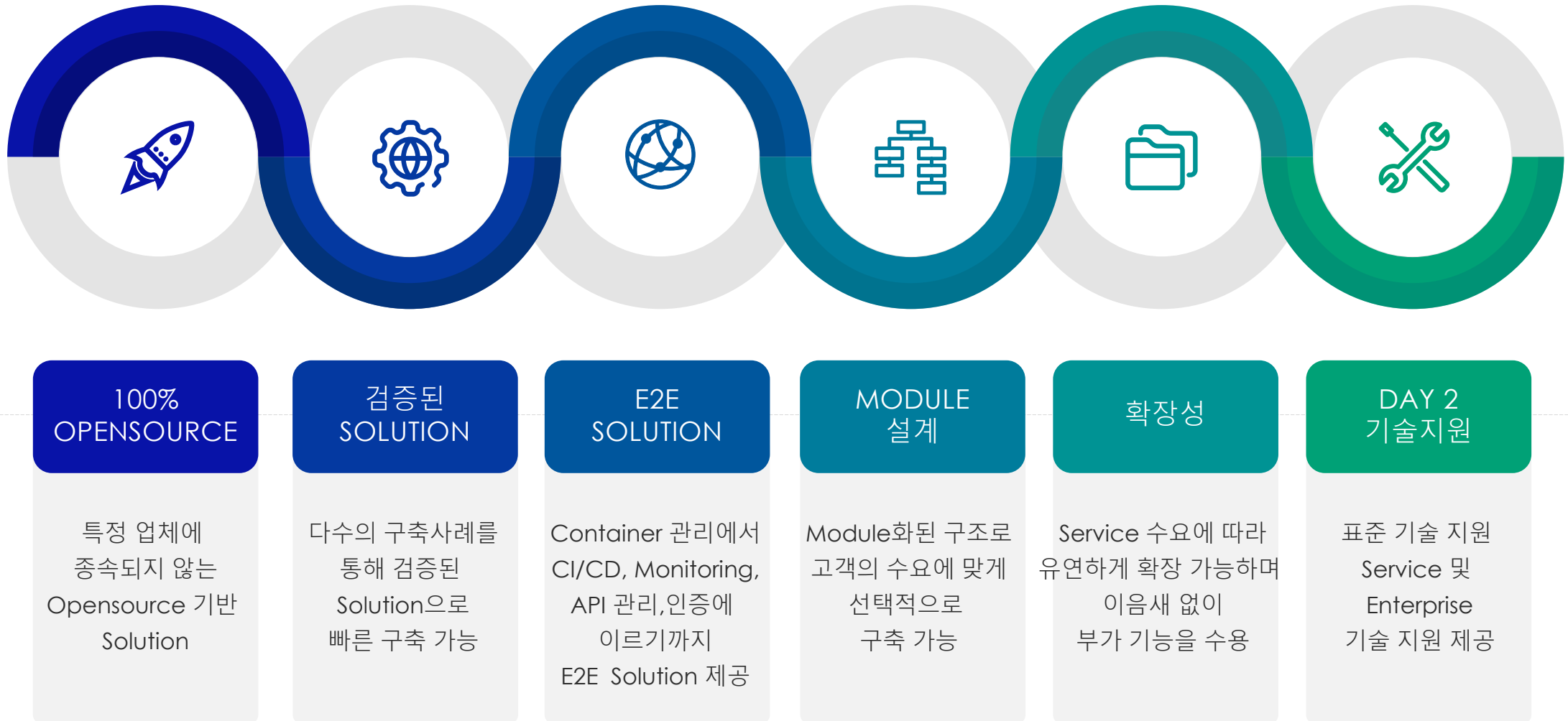


1. OpenMSA™을 이용한 Container 환경 진단 Service 개요
2. SDLC환경의 [OpenSource 보안 진단](#) - Sonatype
3. [SRE \(장애 진단\)](#) - Gremlin
4. [SRE \(성능 진단\)](#) - Speedscale
5. OSC Korea 소개

1. OpenMSA™을 이용한 Container 환경 진단 Service 개요

OSC

■ OpenMSA™ 소개



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.



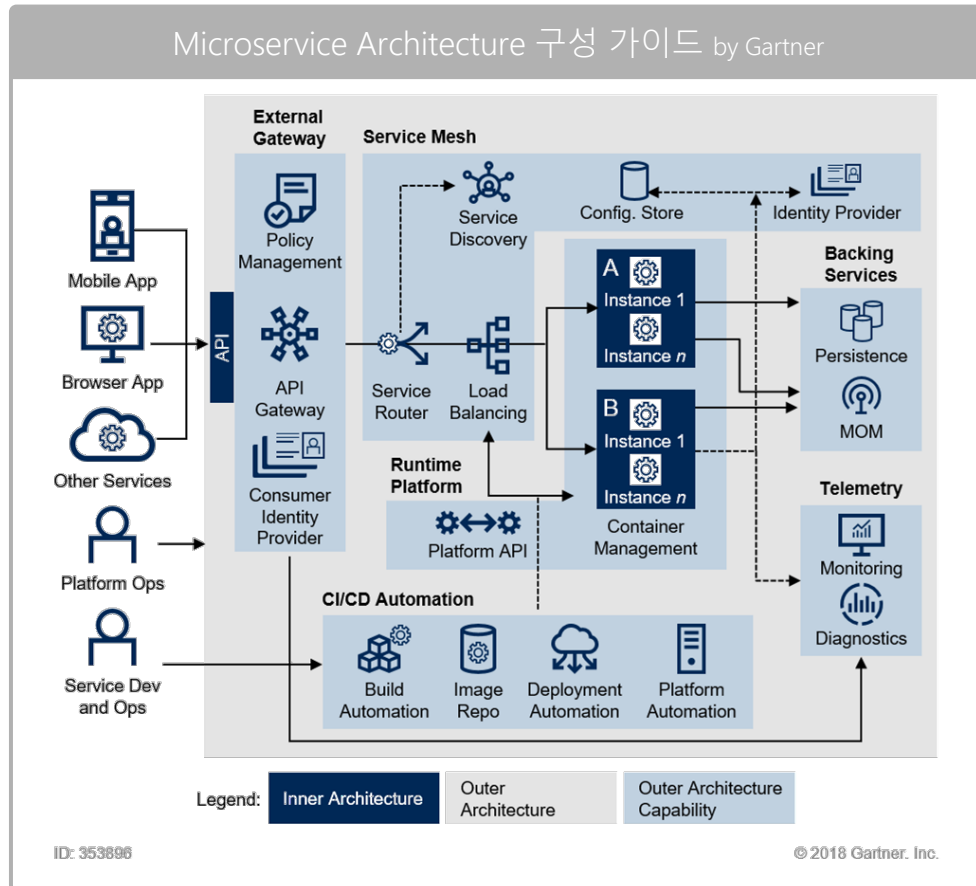
고도화 Road-map 확보

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

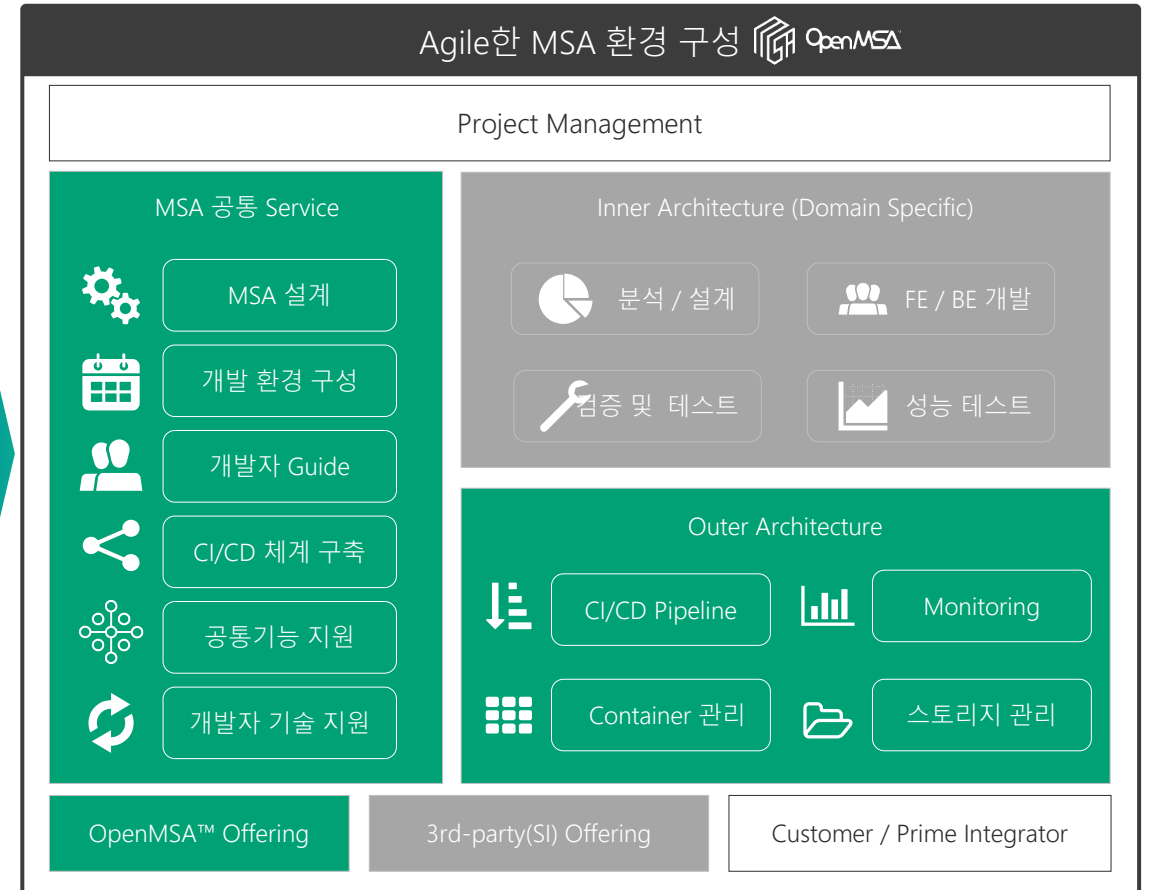


100% Opensource 기반의 OpenMSA™ 구성 개요

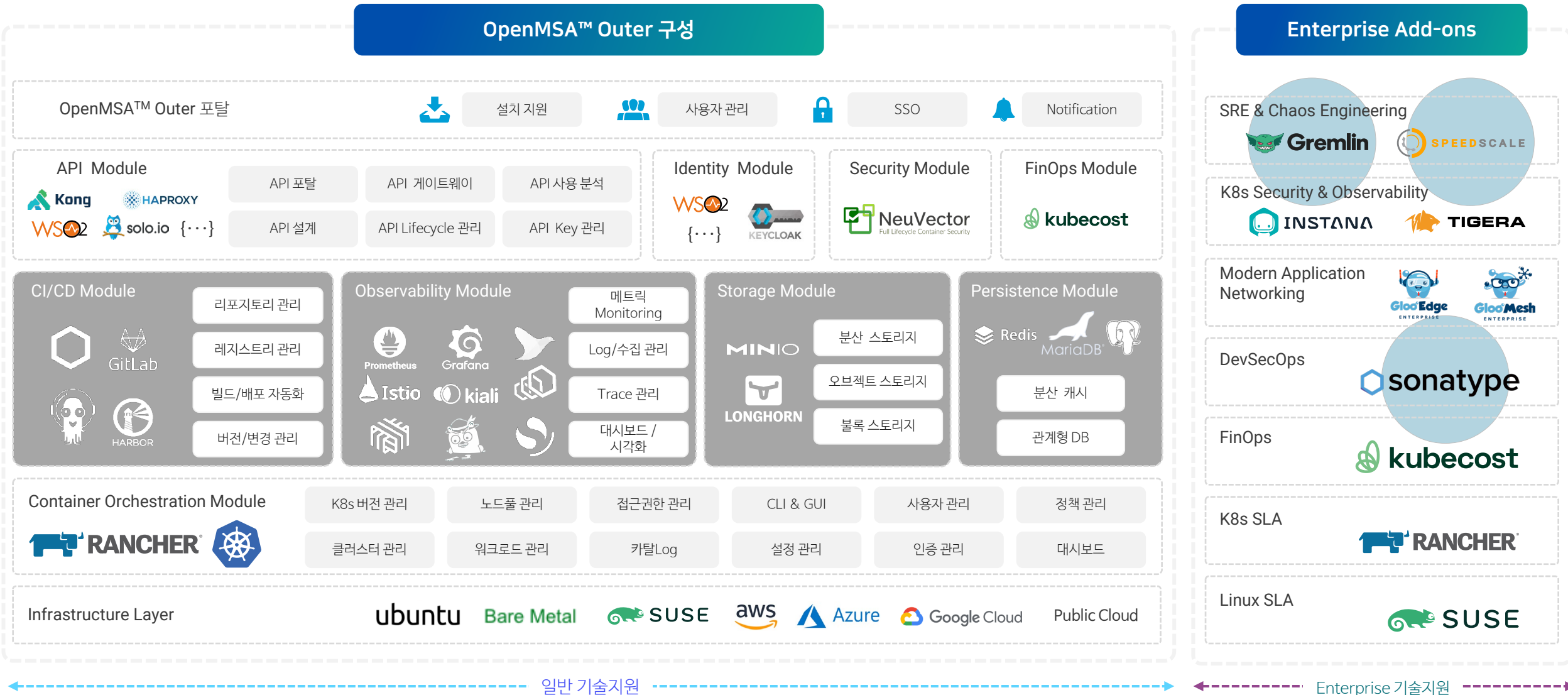
- OpenMSA™는 MSA 공통 서비스와 Outer Architecture(DevOps, GitOps, FinOps 등)에 대해 안정적인 Opensource로 구성한 표준 MSA Framework로, 산업별/Domain별 최적의 MSA 환경 제공



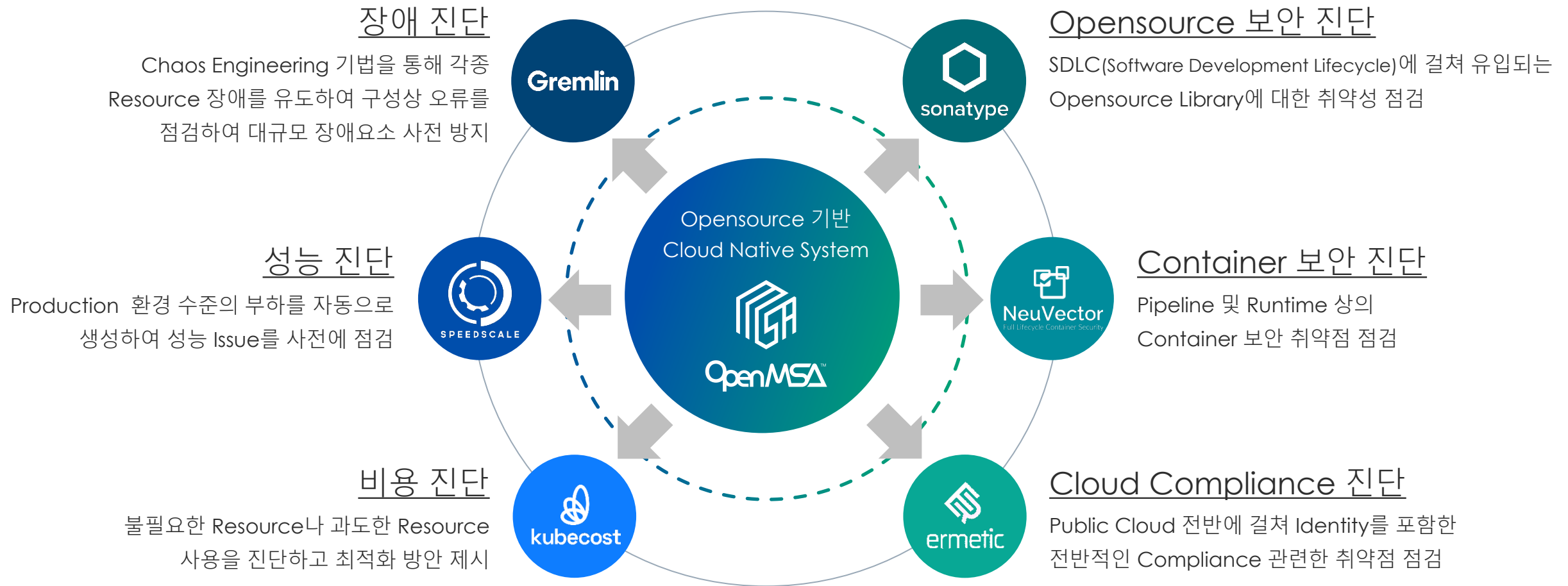
100% Opensource 기반으로 구체화한 서비스 Framework



100% Opensource 기반의 OpenMSA™ 구성 상세 - MSA Outer



OpenMSA™ 기반의 진단 서비스 개요

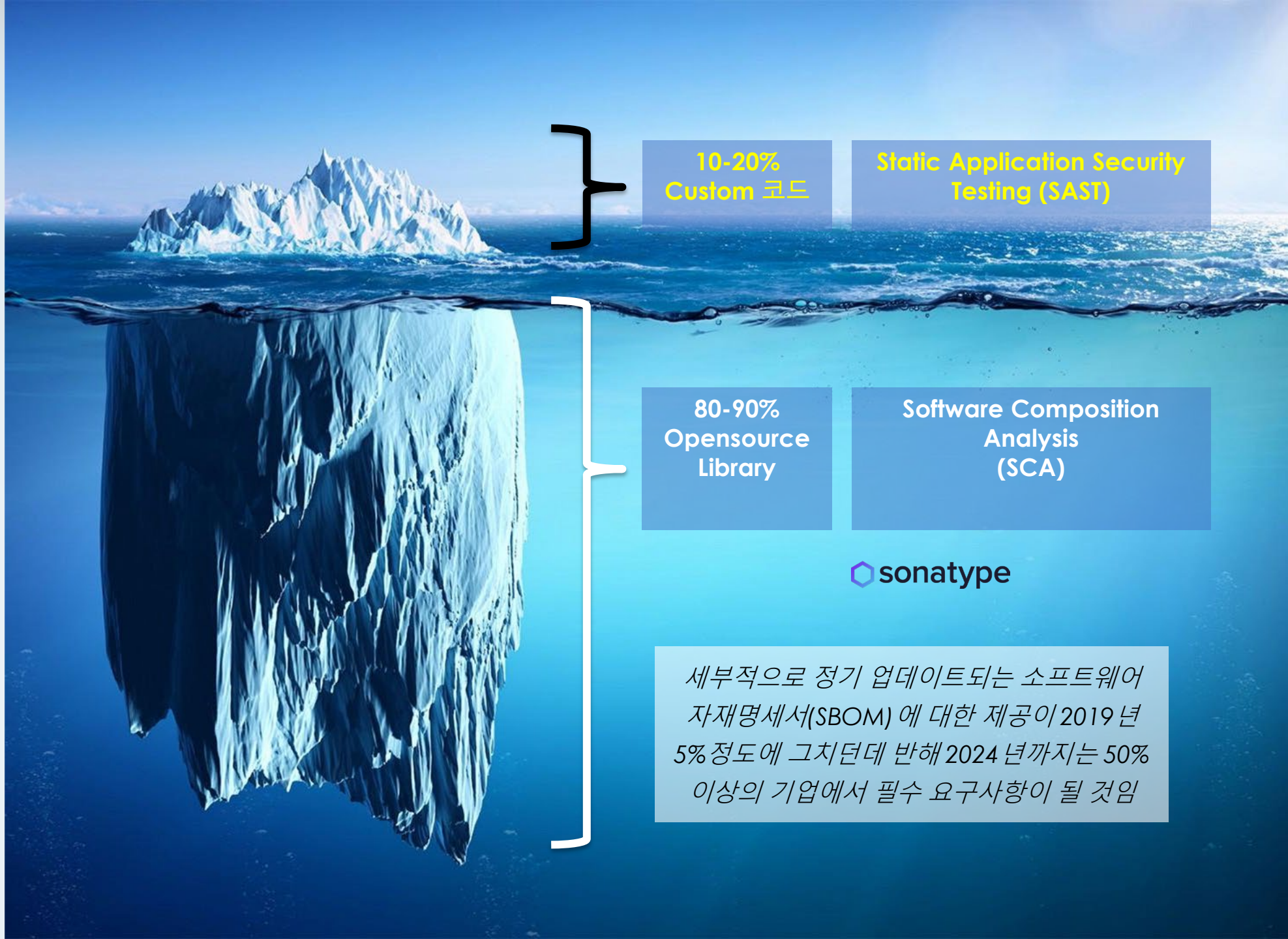


2. SDLC환경의 Opensource 보안 진단 - Sonatype

OSC

Why Sonatype?

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



10-20%
Custom 코드

Static Application Security
Testing (SAST)

80-90%
Opensource
Library

Software Composition
Analysis
(SCA)



세부적으로 정기 업데이트되는 소프트웨어 자재명세서(SBOM)에 대한 제공이 2019년 5% 정도에 그치던데 반해 2024년까지는 50% 이상의 기업에서 필수 요구사항이 될 것임

The Nexus Platform



PUBLIC
OSS
REPOS



Nexus Firewall
위험요소 SDLC 유입자동 차단



DEV
</>



BUILD

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



PACKAGE



TEST



DEPLOY



Nexus Container
Production 상의 어플리케이션 내 Opensource 컴포넌트 검사



OPERATE

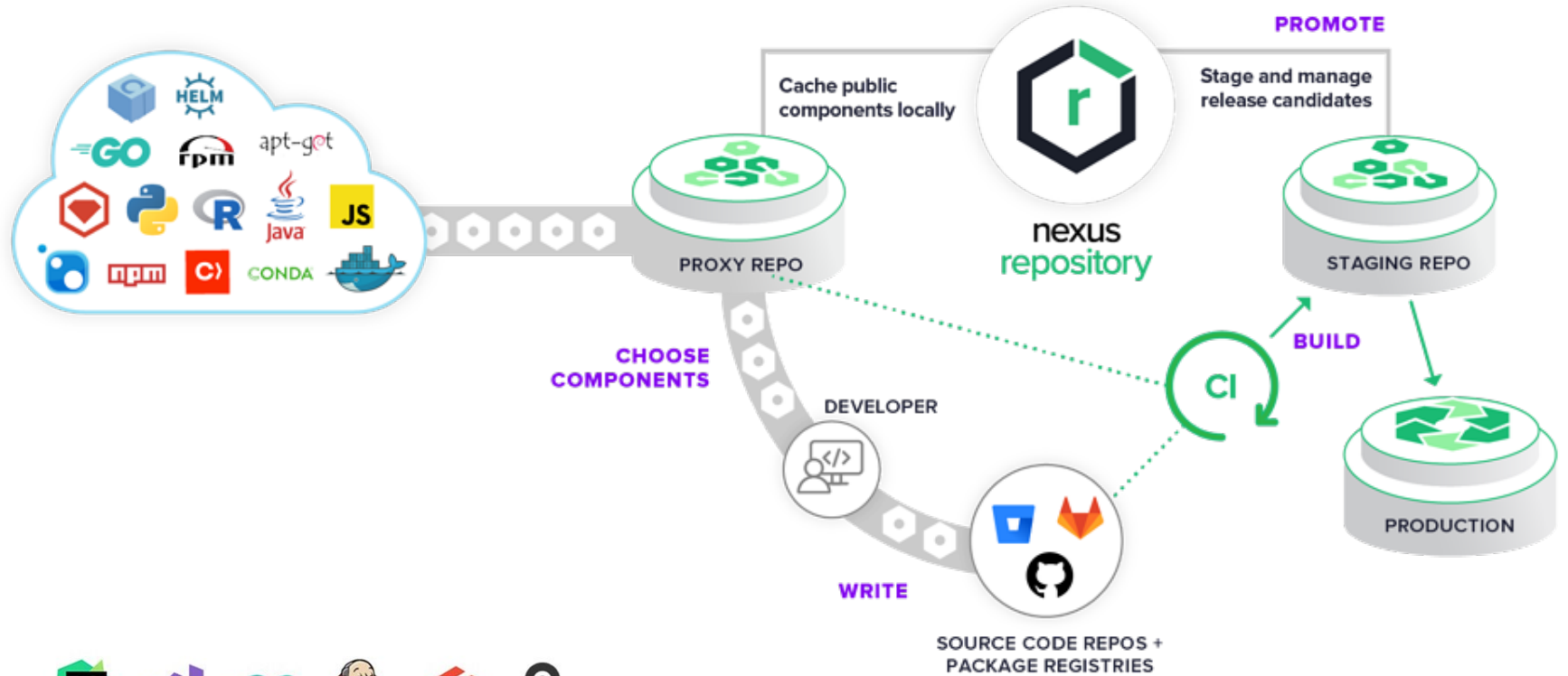


Nexus Lifecycle
SDLC의 모든 단계에 걸쳐 지속적으로 위험요소를 확인하고 정책을 반영하며, 취약점 교정

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

Nexus Repository Pro

World #1 Repository Manager

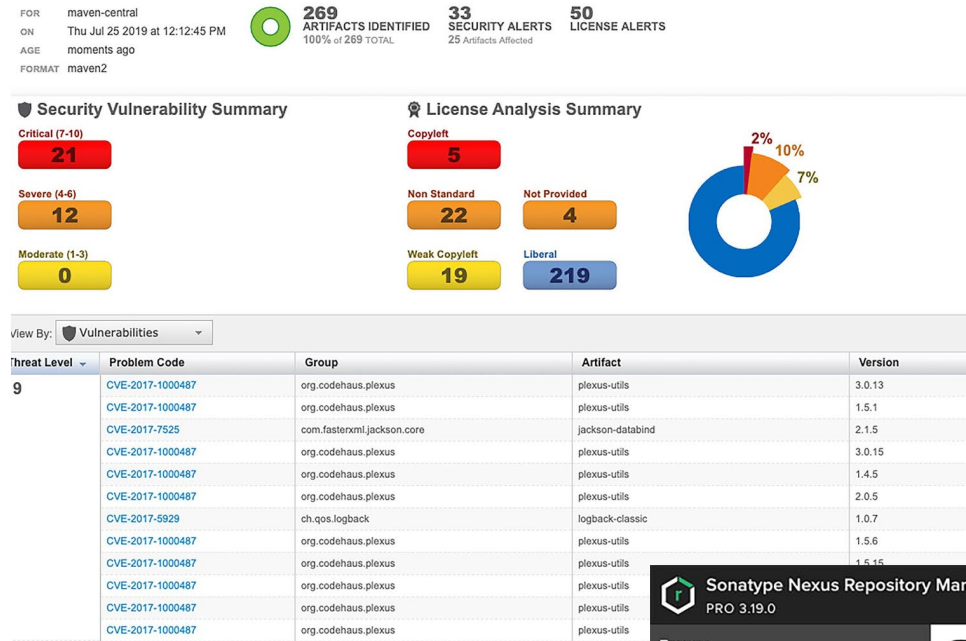


다양한 개발자 도구 및 에코시스템 지원



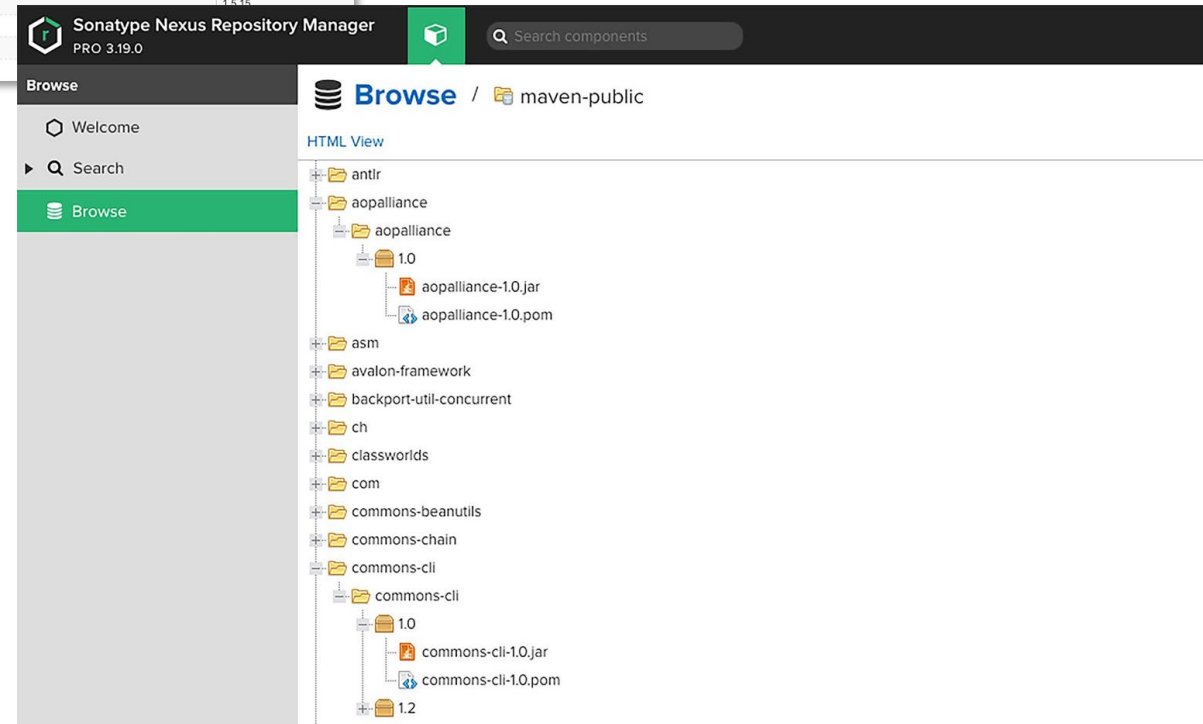
Nexus Repository Pro

World #1 Repository Manager



Software Supply Chain 의 취약점, 라이선스 Issue 등 Health 확인

진보된 Staging으로 출시 후보 (Release Candidates) 워크플로우 관리



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

Nexus Repository Pro

World #1 Repository Manager



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

4670 COMPONENTS IDENTIFIED
100% of 4670 TOTAL

Issue Summary

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

Threat Level 0 50 100 150 200 250 300 350 400

What should I do with this report?

[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

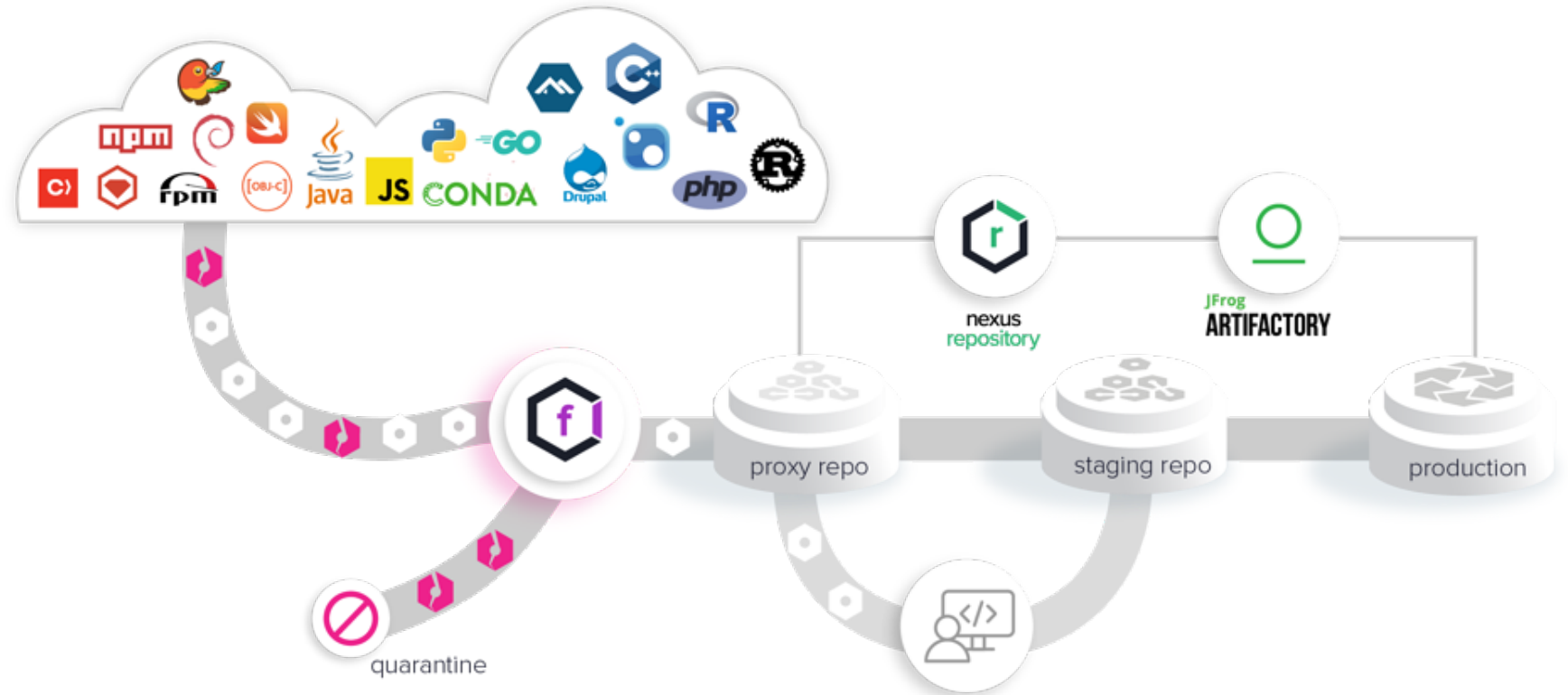
View By: Vulnerabilities

Threat Level	Problem Code	Group	Artifact	Version
7	CVE-2010-2076	org.apache.cxf	cxf-common-utilities	2.2.4
	CVE-2011-3190	org.apache.tomcat	coyote	6.0.33
	osvdb-24364	struts	struts	1.1-rc1
	osvdb-67294	org.apache.cxf	cxf-common-utilities	2.2
	osvdb-24363	struts	struts	1.1-rc1
	osvdb-67294	org.apache.cxf	cxf-common-utilities	2.2.4
	CVE-2011-3190	org.openl.rules	org.openl.rules.tomcat.lib	5.7.2
	osvdb-74818	org.ow2.jonas.assemblies.profiles	jonas-full	5.3.0-M2
	CVE-2006-1547	struts	struts	1.1-rc1
	osvdb-67294	org.apache.cxf	cxf-common-utilities	2.1.2
	CVE-2010-2076	org.apache.cxf	cxf-common-utilities	2.2

View By: Artifacts

License Threat	Declared License	Observed Licenses	Group	Artifact	Version
GPL	Apache-2.0	Apache-2.0, GPL	org.sonatype.configurat	base-configuration	1.1
GPL-2.0+	Apache-2.0+, BSD, EPL-	Apache-2.0, BSD, EPL-1	biz.source_code	base64coder	2010-12-19
GPL, GPL-2.0	CDDL, GPL, GPL-2.0	Not Provided	org.glassfish.core	glassfish	3.1-b13
GPL, GPL-2.0	CDDL, GPL, GPL-2.0	Not Provided	org.glassfish	javax.jms	3.1
GPL-2.0, GPL-2.0+	Apache-2.0	Apache-1.1, Apache-2.0,	org.apache.servicemix	servicemix-scripting	2008.01
GPL, GPL-2.0	CDDL, GPL, GPL-2.0	Not Provided	org.glassfish	javax.transaction	10.0-b28
GPL	Apache-2.0	Apache, Apache-2.0, GP	org.apache.camel	camel-jms	2.3.0
GPL	AFL-2.1, Apache-2.0, BS	AFL-2.1, Apache-2.0, BS	org.cometd	cometd-demo	1.1.3
GPL-2.0+	GPL-2.0-with-classpath+	GPL-2.0+	me.springframework	spring-me-sample-j2	1.0
GPL	Apache-2.0	Apache-2.0, GPL	org.apache.camel	camel-core	2.1.0

Nexus Firewall은 취약한 컴포넌트가 SDLC내로 유입되는 것을 차단



Nexus Firewall

Shift Security Left

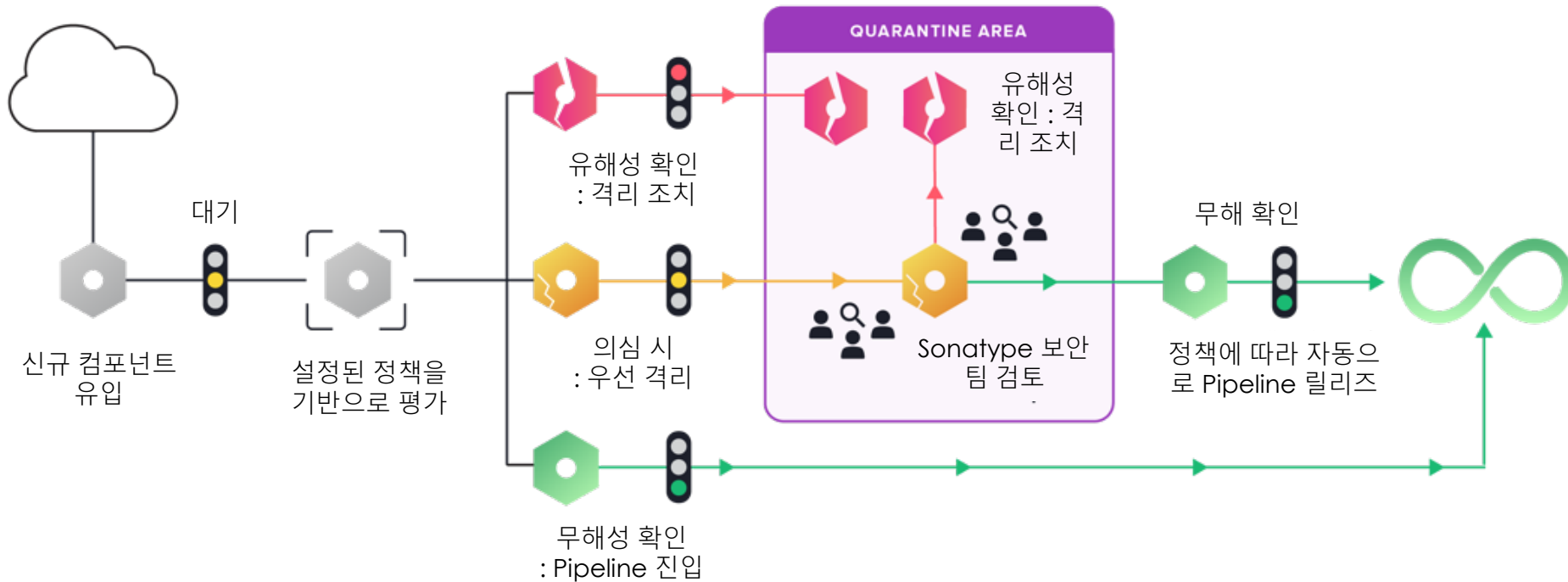
Java, JavaScript, .NET, Python, Go, Ruby, RPM 등 다양한 언어 지원





Nexus Firewall

Shift Security Left



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

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



Nexus Firewall

Shift Security Left

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

Quarantine Status ● Active on 1 of 1 repositories	Auto Release from Quarantine Status ● Active releasing 3 of 5 policy condition types Configure	Quarantine 230 components in quarantine	Auto Released from Quarantine 70 components released month-to-month View Auto Release Quarantine
--	--	--	--

Quarantine Updated 11:50:28 p.m. 2021-05-10 [Refresh](#)

THREAT	POLICY NAME	QUARANTINE DATE	COMPONENT	REPOSITORY
● 10	Security-Critical	2021-05-10	com.pojosontheweb : woko-blobs-web : war : 2.2-beta7	test-repo
● 10	Security-Critical	2021-05-10	org.mule.examples : mule-example-errorhandler : zip : 3.4-M1	test-repo
● 10	Security-Critical	2021-05-10	org.atmosphere.samples : atmosphere-twitter-live-feed : war : 0.8.2	test-repo
● 10	Security-Critical	2021-05-10	smartrics.restfixture : smartrics-RestFixture : zip : bin : 4.0	test-repo
● 10	Security-Critical	2021-05-10	org.apache.maven.plugins : maven-assembly-plugin : jar : 3.0.0-M1	test-repo
● 10	Security-Critical	2021-05-10	org.apache.maven.plugins : maven-compiler-plugin : jar : 3.8.1	test-repo

Auto Release from Quarantine

COMPONENT	QUARANTINE DATE	REPOSITORY	DATE CLEARED
org.apache.directory.studio : ldapservers.apacheds.v154 : jar : sources : 2.0.0.v20120111	2021-05-10	test-repo	2021-05-10
org.glassfish.grizzly : grizzly-http : 2.1	2021-05-10	test-repo	2021-05-10
org.ow2.jonas.autostart : jonas-full-starter : jar : full-starter : 1.0.0-M2	2021-05-10	test-repo	2021-05-10
org.apache.portals.bridges : perl : war : 1.0.4	2021-05-10	test-repo	2021-05-10
com.sun.grizzly : grizzly-http-webserver : 1.9.18-o	2021-05-10	test-repo	2021-05-10
com.sun.faces : jsf-api : 2.0.4-b11	2021-05-10	test-repo	2021-05-10

Policy Threat for maven-central

COMPONENTS IDENTIFIED: 100% OF ALL COMPONENTS ARE IDENTIFIED

POLICY ALERTS: 2 (AFFECTING 3 COMPONENTS)

QUARANTINED COMPONENTS: 4

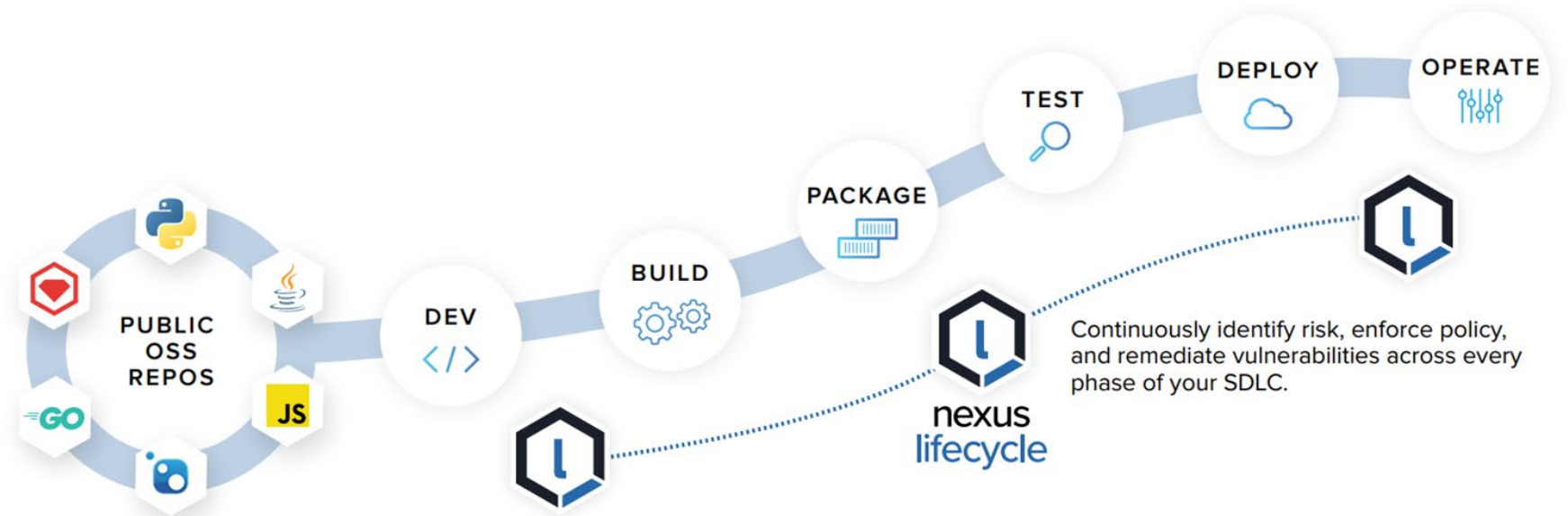
FILTER: All Exact Unknown VIOLATIONS: Summary All Quarantined

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

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

Nexus Lifecycle

World #1 Software Composition Analysis



현업에서 사용하는 Pipeline 툴과 사전 정합 되어 있습니다.



Nexus Lifecycle

World #1 Software Composition Analysis



Filter Manage

Results

VIOLATIONS COMPONENTS APPLICATIONS

NAME	AFFECTED APPS	TOTAL RISK	CRITICAL	SEVERE	MODERATE	LOW
commons-httpclient : commons-httpclient : 3.1	11	200	81	113	6	0
org.apache.struts : struts2-assembly : zip : all : 2.3.14	4	150	96	48	6	0
org.apache.struts : struts2-blank : war : 2.3.14	4	130	76	48	6	0
org.apache.struts : struts2-showcase : war : 2.3.14	4	130	76	48	6	0
org.apache.struts : struts2-portlet : war : 2.3.14	4	130	76	48	6	0
org.apache.struts : struts2-rest-showcase : war : 2.3.14	4	130	76	48	6	0
axis : axis : 1.2	6	126	54	72	0	0
org.apache.struts : struts2-mailreader : war : 2.3.14	4	125	76	43	6	0
commons-collections : commons-collections : 3.1	10	122	98	24	0	0
org.apache.struts : struts2-core : 2.3.14	4	122	76	43	3	0
commons-collections : commons-collections : 3.2.1	9	99	81	18	0	0
org.apache.struts.xwork : xwork-core : 2.3.14	4	99	66	33	0	0
org.springframework : spring-context : 2.5.6.SEC03	6	94	36	58	0	0
org.apache.httpcomponents : httpclient : 4.2.5	6	84	36	48	0	0
org.springframework : spring-web : 2.5.6.SEC03	6	84	36	48	0	0
org.apache.jackrabbit : jackrabbit-webdav : 2.5.2	6	84	36	48	0	0
org.springframework : spring-web : 3.0.5.RELEASE	4	84	36	48	0	0
org.apache.struts : struts2-rest-plugin : 2.3.14	4	84	36	48	0	0
commons-fileupload : commons-fileupload : 1.2.1	6	84	36	48	0	0

Apply Revert Clear

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

위험요소에 대한 전문
교정가이드 제공

Repository results for maven-central

Oldest evaluation 7 months ago

738 COMPONENTS IDENTIFIED
100% OF ALL COMPONENTS ARE

56 POLICY ALERTS
29 2 50 QUARANTINED COMPONENTS

Vulnerability Information

Filter: All Exact Up

Policy Threat -

Search Name

License-Banned

Security-High

Component Info Policy

Threat Level - Problem C

9 CVE-2017-

Explanation
sending the maliciously crafted input to the readValue method of the ObjectMapper.
This issue extends the previous flaw CVE-2017-7525 by blacklisting more classes that could be used maliciously.

Note: This vulnerability exists due to the incomplete fix for CVE-2017-7525

Detection
The application is vulnerable by using this component, when default typing is enabled and passing in untrusted data to be deserialization.

Note: Spring Security has provided their own fix for this vulnerability (CVE-2017-4995). If this component is being used as part of Spring Security, then you are not vulnerable if you are running Spring Security 4.2.3.RELEASE or greater for 4.x or Spring Security 5.0.0.M2 or greater for 5.x.

Recommendation
There is no non vulnerable version of this component. Despite there being a fix provided by Jackson, it uses a black-list approach. If there is another class not black-listed which performs deserialization on the classpath, then this may lead to code

Close

Nexus Lifecycle

World #1 Software Composition Analysis



```
pom.xml
...
16 <maven.compiler.source>1.8</maven.compiler.source>
17 <maven.compiler.target>1.8</maven.compiler.target>

```

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

eduard-tita 4 minutes ago Author
👤
😬 Nexus IQ found policy violations introduced by:
▼ 10 com.fasterxml.jackson.core : jackson-databind : 2.9.9.3

🛡️ **Bumping to version 2.10.0** will resolve these violations (as of May 07, 2020)

Threat	Policy	Violation Details
10	Security-Critical	Critical risk CVSS score: <ul style="list-style-type: none">Found security vulnerabilities: CVE-2019-14540, CVE-2019-14892, CVE-2019-14893, CVE-2019-16335, CVE-2019-17267
9	Security-High	High risk CVSS score: <ul style="list-style-type: none">Found security vulnerability: sonatype-2019-0371

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

workspace - WebGoat/pom.xml - Eclipse

Package Exp | build.xml | *WebGoat/pom.xml | presto-hive/pom | settings.xml | settings.xml | presto-hive/pom | presto-root/pom | Snippet.java

```
<dependencies>
  <dependency>
    <groupId>javax.activation</groupId>
    <artifactId>activation</artifactId>
    <version>1.1</version>
  </dependency>
  <dependency>
    <groupId>org.immutables</groupId>
    <artifactId>value</artifactId>
    <version>2.5.1</version>
  </dependency>
  <dependency>
    <groupId>axis</groupId>

```

Overview | Dependencies | Dependency Hierarchy | Effective POM | pom.xml

Console | Search | Drag Placeholder | Component Info | Problems | Maven Workspace Build | Maven Repositories | Progress | Javadoc | Declaration

WebGoat, 58 components (58 shown, 0 filtered)

Component	Group	Artifact	Version
axis - 1.2	commons-collections	commons-collections	3.2.1
commons-beanutils - 1.6			
commons-collections - 3.2.1			
commons-fileupload - 1.2.1			
commons-httpclient - 3.1			
spring-core - 4.3.13.RELEASE			
spring-data-commons - 1.13.9.RELEASE			
spring-webmvc - 4.3.13.RELEASE			
itextpdf - 5.5.6			
axis-ant - 1.2			
axis-jaxrpc - 1.2			
axis-saaj - 1.2			
activation - 1.1			
cglib-nodep - 2.2.2			
client - 0.8.1			
commons-codec - 1.2			
commons-digester - 1.4.1			
commons-discovery - 0.2			

Group: commons-collections
Artifact: commons-collections
Version: 3.2.1
Declared License: Apache-2.0
Observed License: Apache-2.0
Effective License: Apache-2.0
Highest Policy Threat: 9
Highest Security Threat: 9
Cataloged: 10 years ago
Match State: exact
Identification Source: Sonatype
View Details | Migrate

Popularity | Older | This Version | Newer
License Risk
Security Alerts

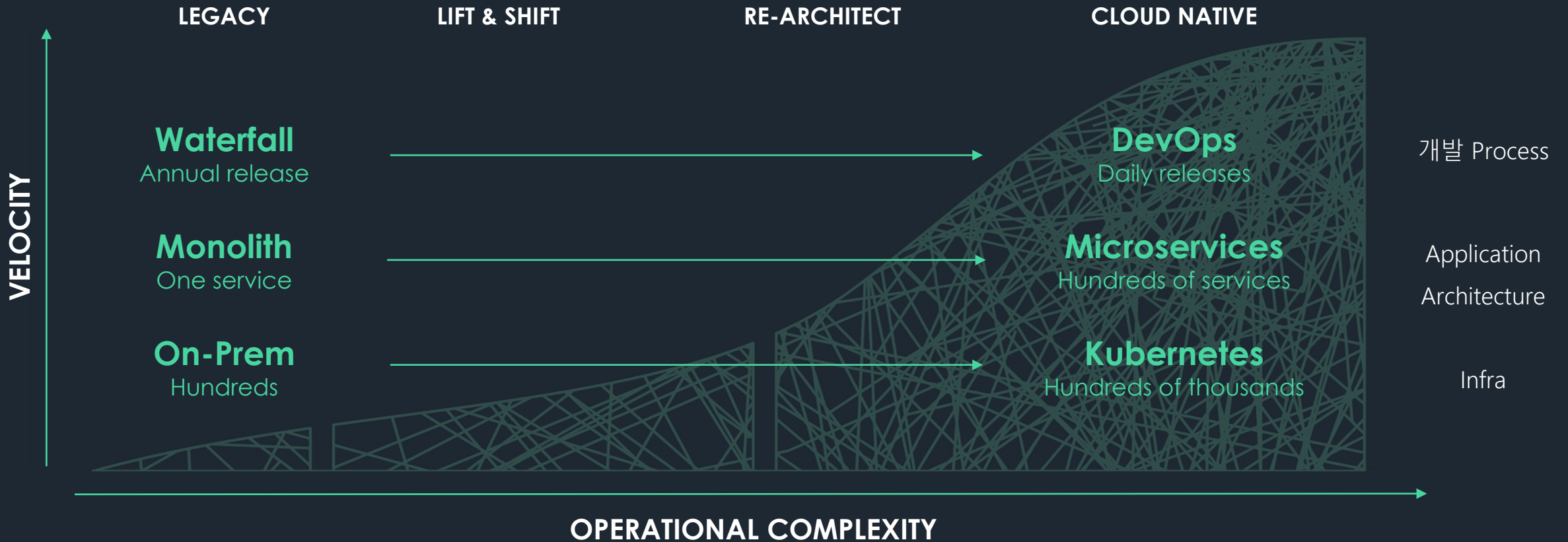


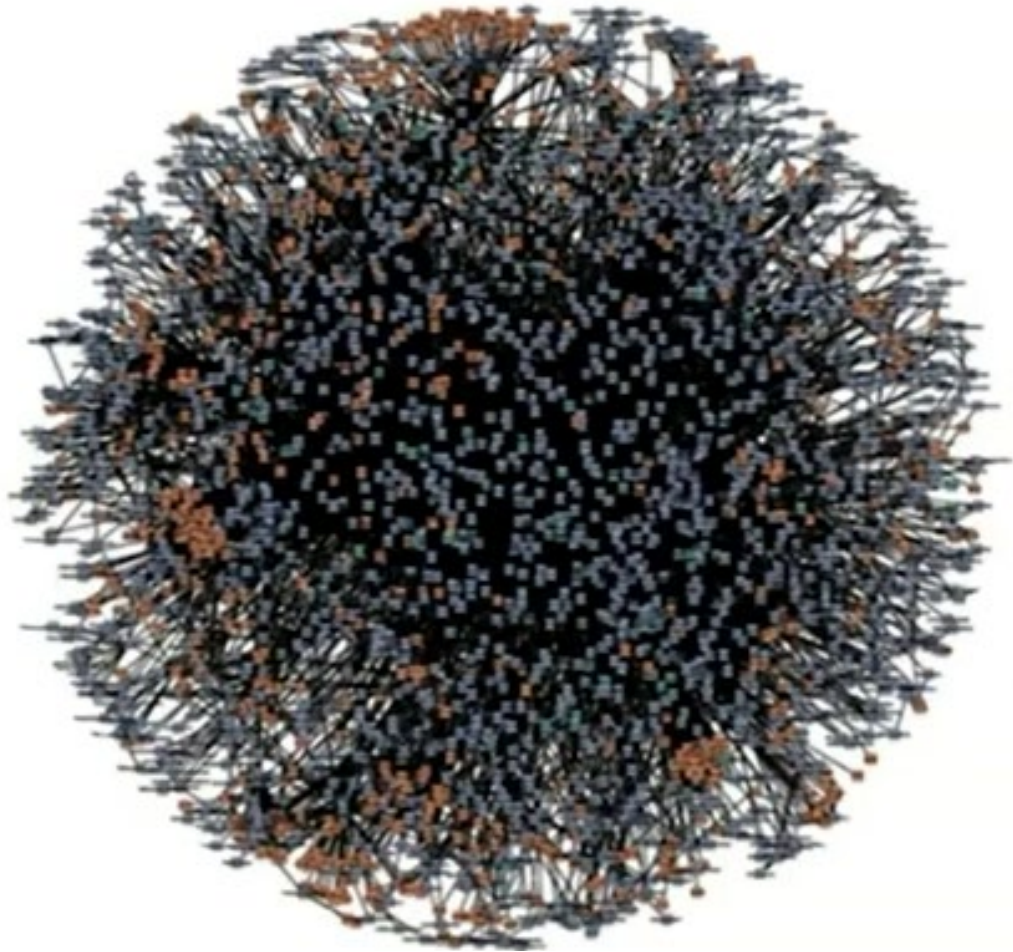
3. SRE (장애 진단) - Gremlin

OSC

Velocity Comes at a Price

Application/Service는 급격한 속도로 복잡해지고 있음 : 운영 난이도 증가

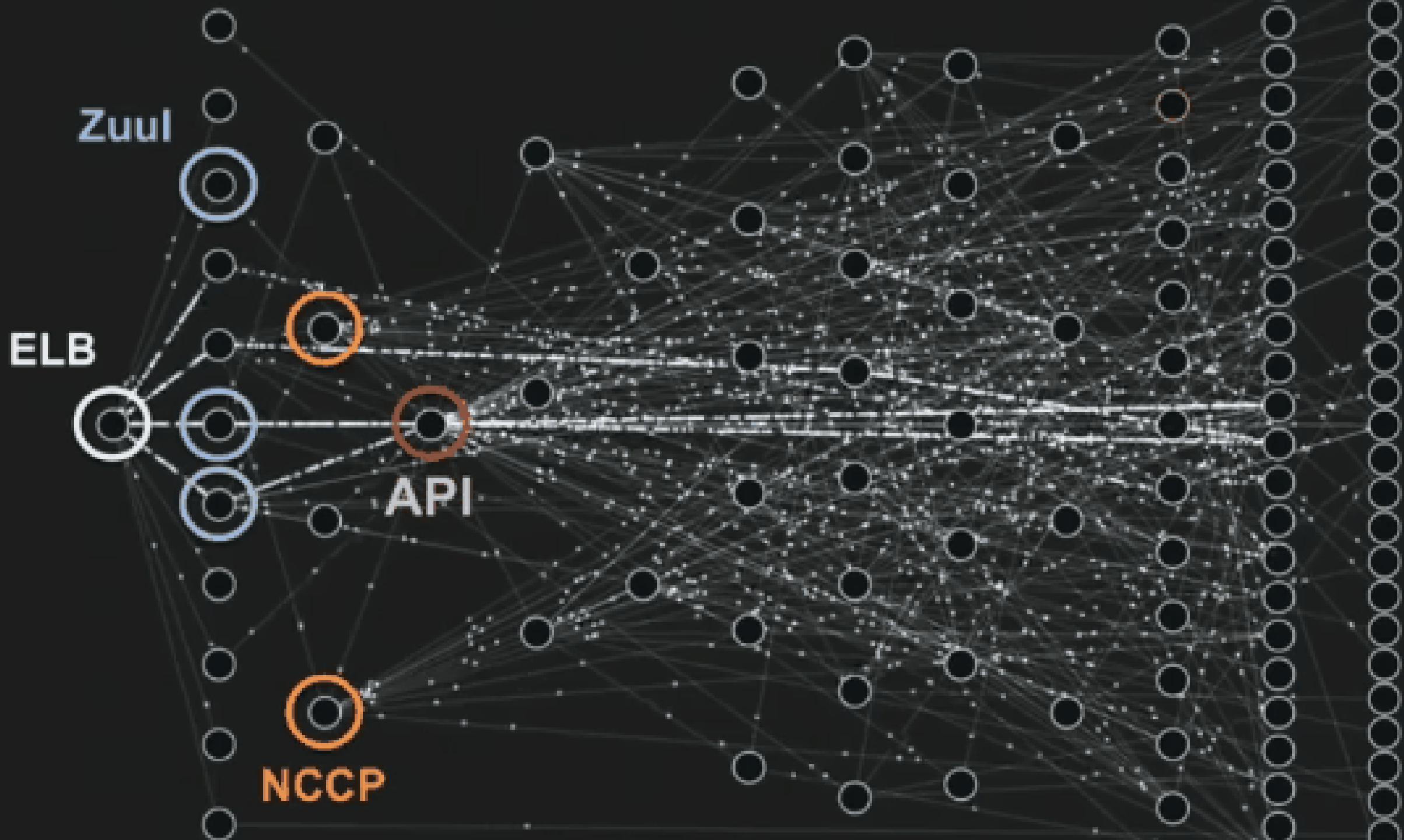




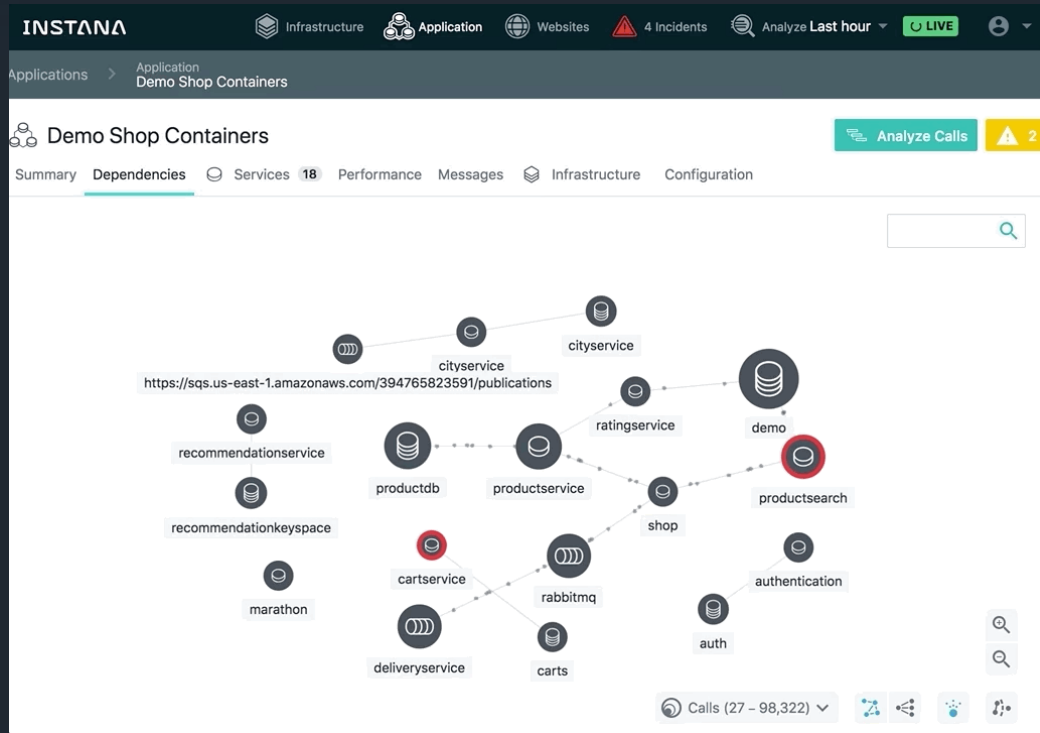
amazon



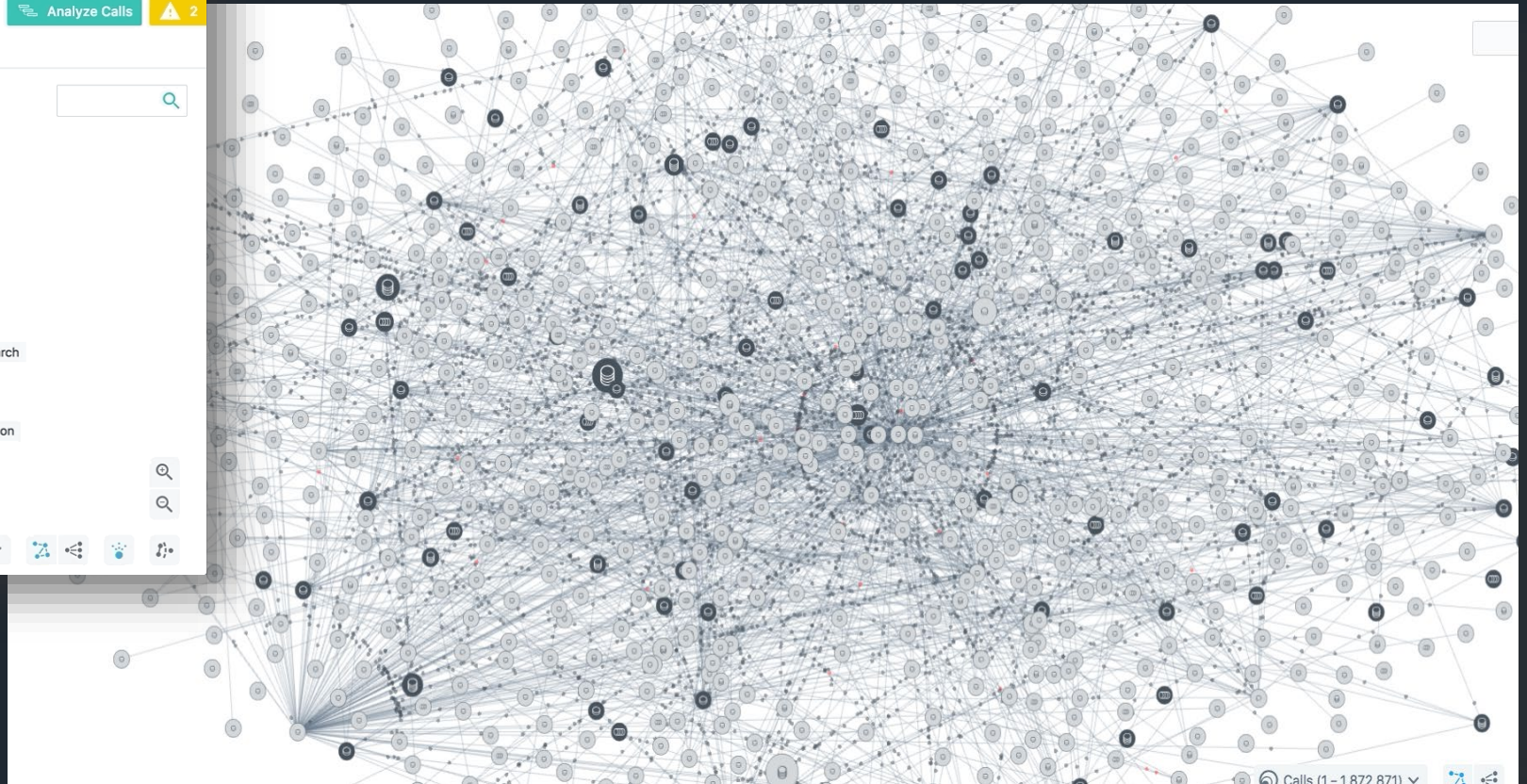
NETFLIX



Dependency Map - Instana View



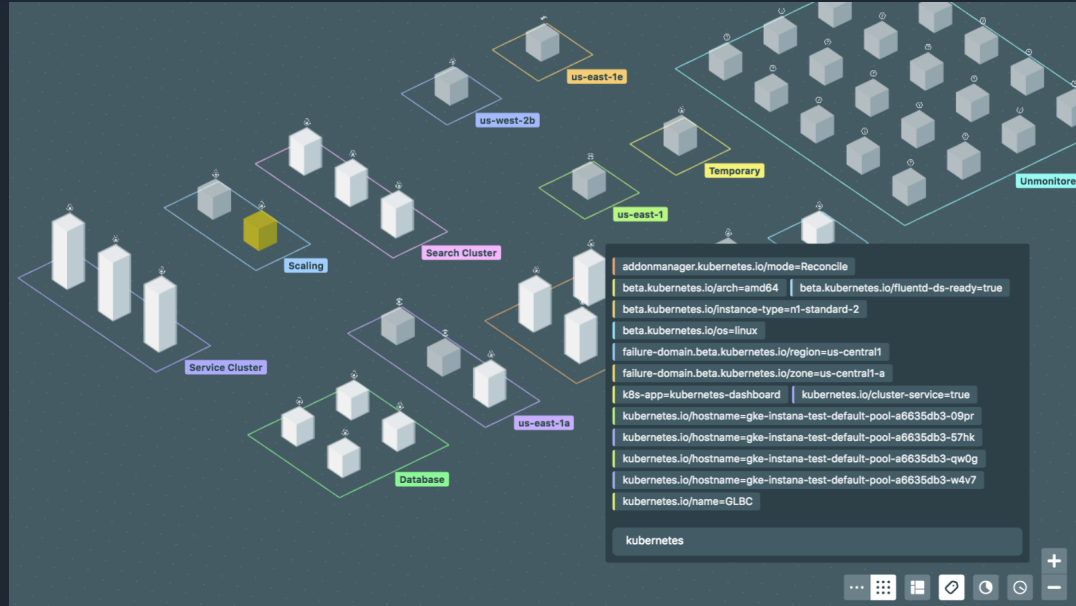
STG / PRD 환경



SIT / QA 환경

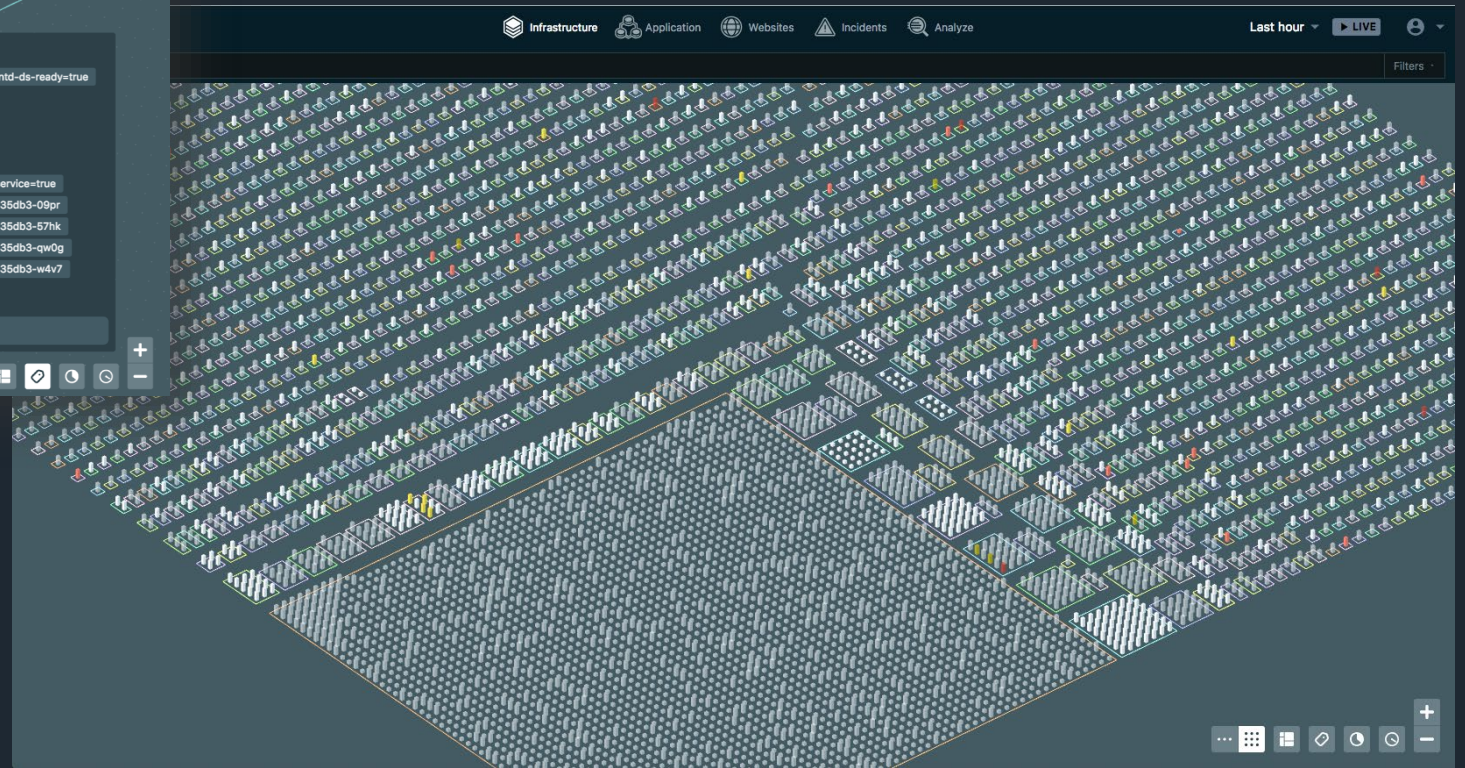
Infrastructure Map - Instana View

INSTANA



SIT / QA 환경

STG / PRD 환경



Black Friday 장애



기술 Issue로 인해 수조원대 손실이 발생한 유통업체
12.01.16



금융 장애



City Bank Web-site, Mobile Service 장애
2.28.19



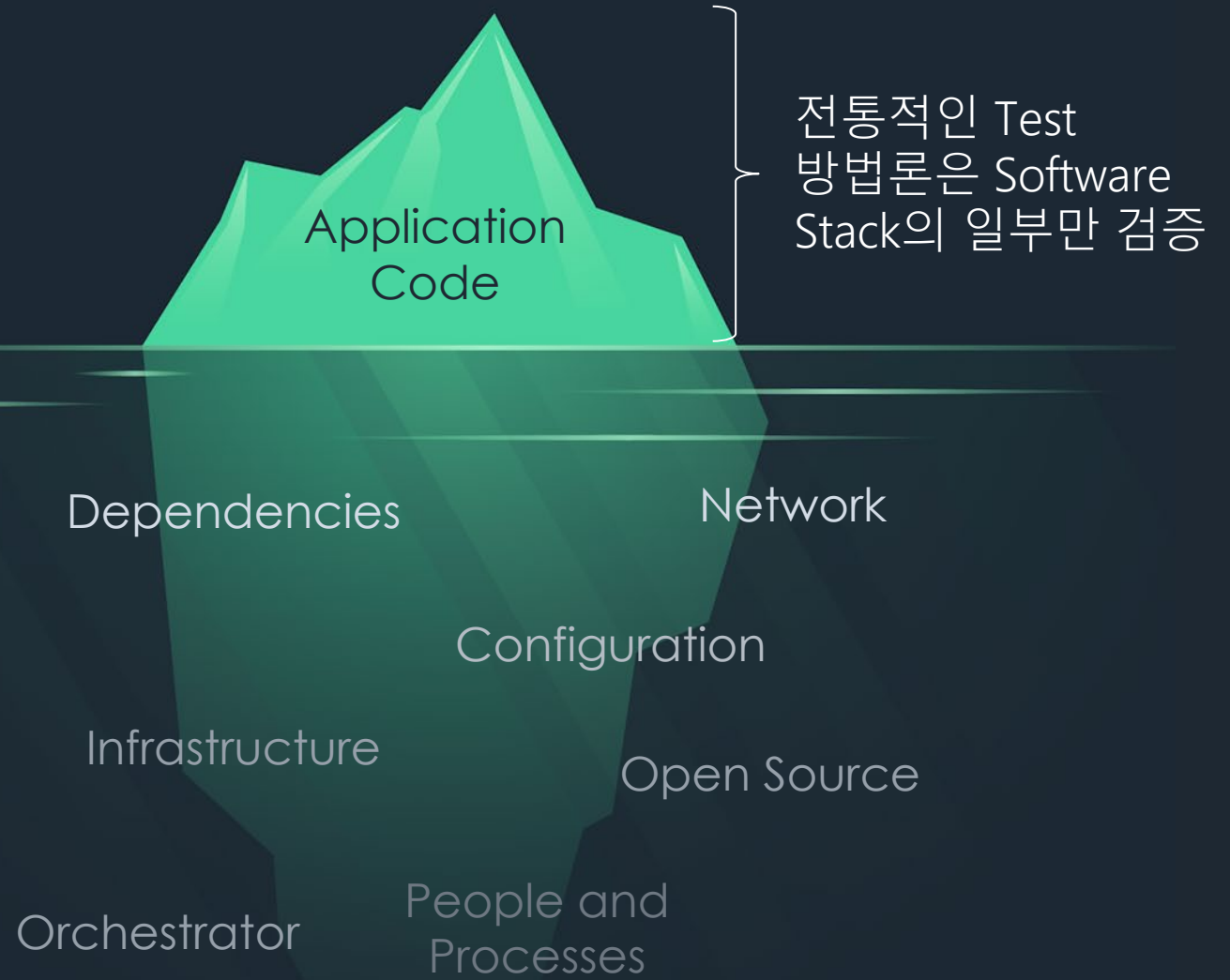
항공사 장애



System 장애로 인한 항공일정 지연
4.1.19



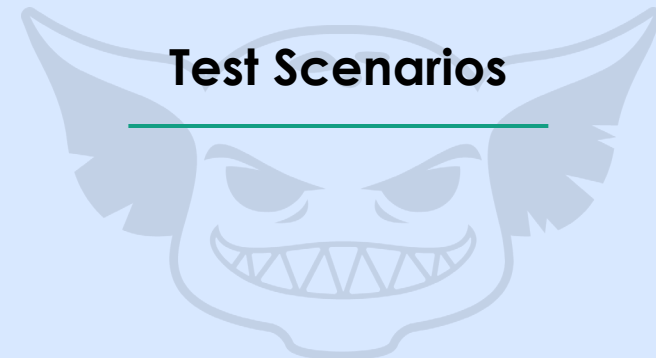
Traditional Testing
is not enough
anymore.



“ 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.



Test Scenarios

People

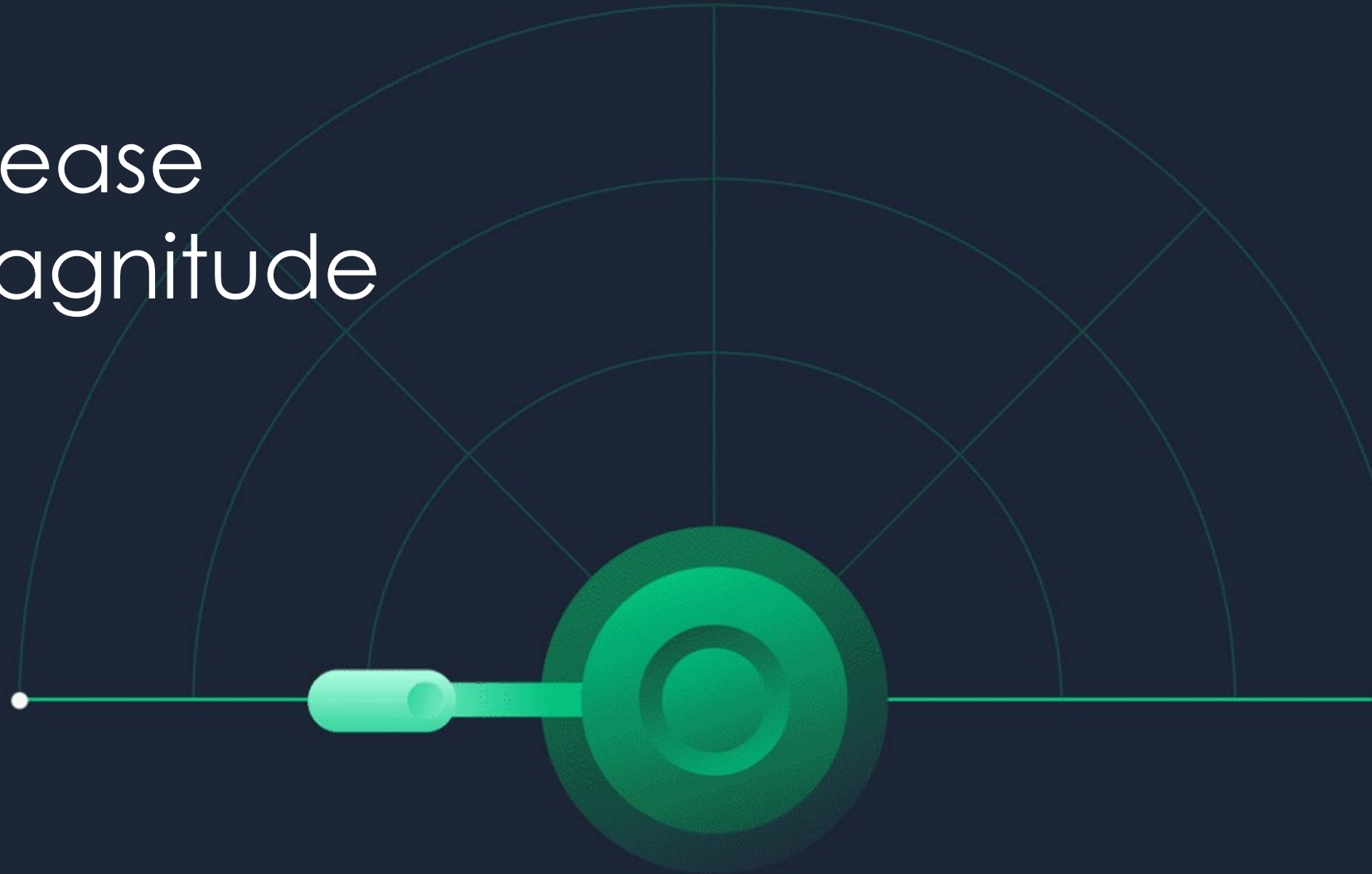
Processes

Application

Infrastructure

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 ”

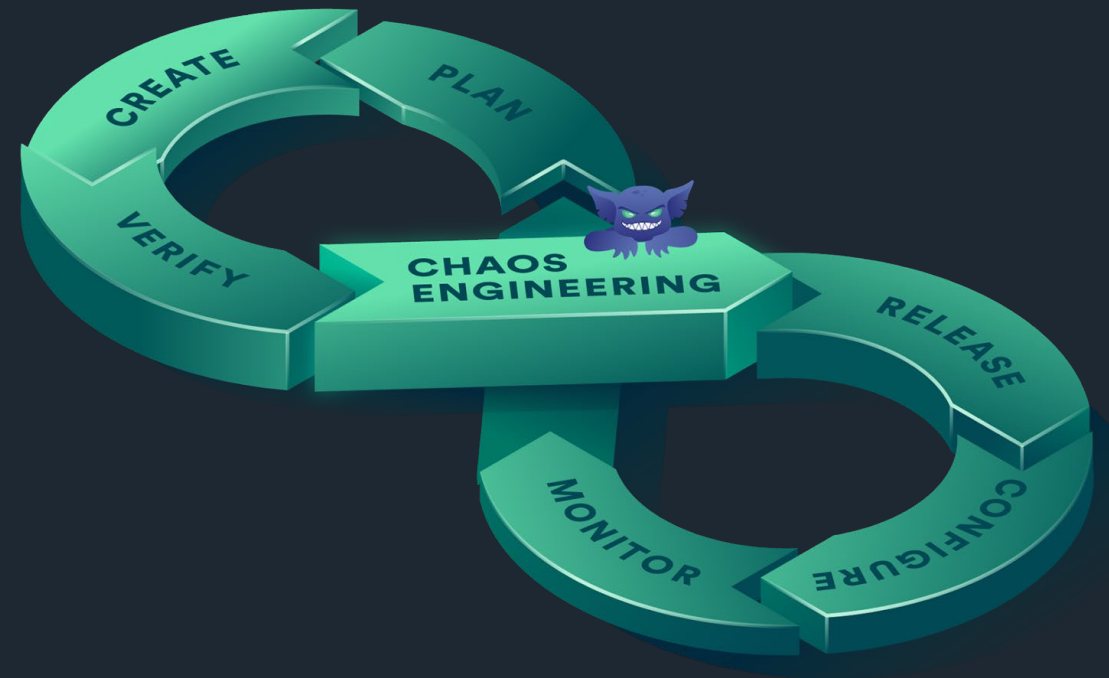
- Gartner

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

-Gartner

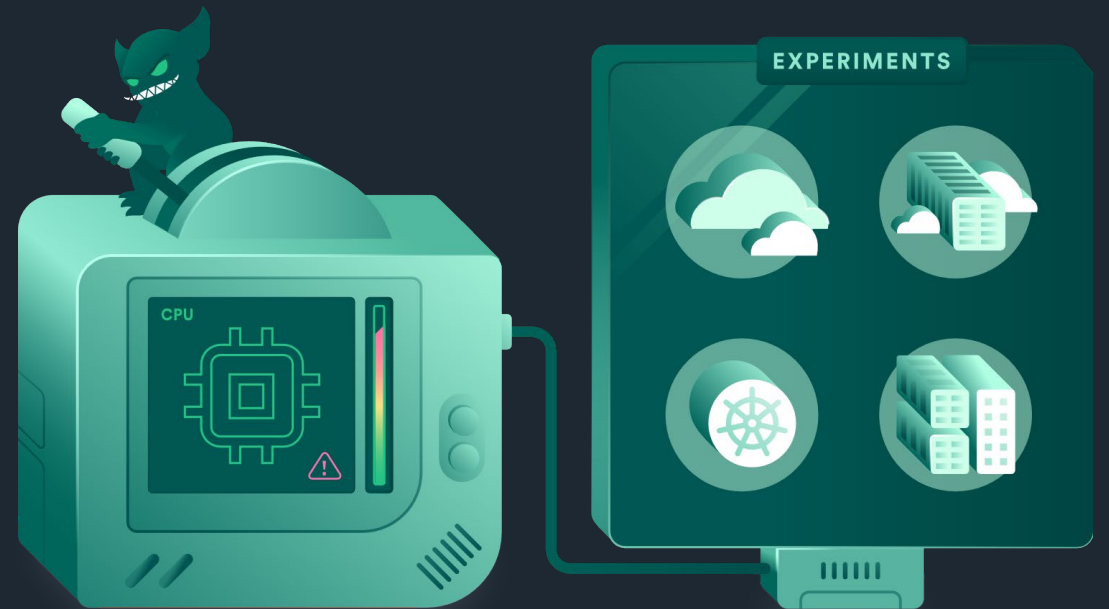
“2023년까지 40%의 조직이 Chaos Engineering을 DevOps의 일환으로 도입하여 Downtime을 20% 감소시킬 것” - Gartner

<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

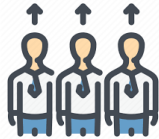


Comprehensive

다양한 Stack Layer에 대한 Attack 지원



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



Gremlin VMware



AWS



Azure



Google



Docker



K8S



Linux



Windows



Serverless

1 What do you want to attack? **Attack 대상**

Hosts (3 available) Containers (132 available) Applications (0 available) Kubernetes (171 available)

2 Choose Hosts to target **Attack 범위**

Specify the coverage and details for impact

Tags Exact ...

Narrow the number of potential targets by tag

Target all hosts [Expand All](#)

- Operating Systems (1)
- Zone (2)
- Region (1)
- local-hostname (3)
- local-ip (3)
- Other Tags (13)

BLAST RADIUS

3 of 3 HOSTS TARGETED | 3 HOSTS IMPACTED

Host Container

Percent of targets to impact

100 % 3 of 3 targets impacted

3 Choose a Gremlin **Attack 종류**

Select the type of attack to unleash.

Category

- Resource: Impact cores, workers, and memory.
- State: Process killer, shutdown and time travel.
- Network: Blackhole, latency, packet loss and DNS.

Attacks

- Process Killer: An attack which kills the specified process.
- Shutdown: Reboots or shuts down the targeted host operating system.
- Time Travel: Changes the system time.

Delay: The number of minutes to delay before shutting down.

Reboot: Indicates the host should reboot after shutting down.

4 Run the attack **Attack 시점**

Unleash now or schedule for later.

Schedule for later: Run this attack at a future date.

- Only once: Set the date and time.
- Randomly within a timeframe: Select at least one day.

Date mm/dd/yyyy:

Time * Local Military Time:

Hours field must be completed

Gremlin API Examples

Application Targeted Attacks

State Shutdown Time Travel Process Killer

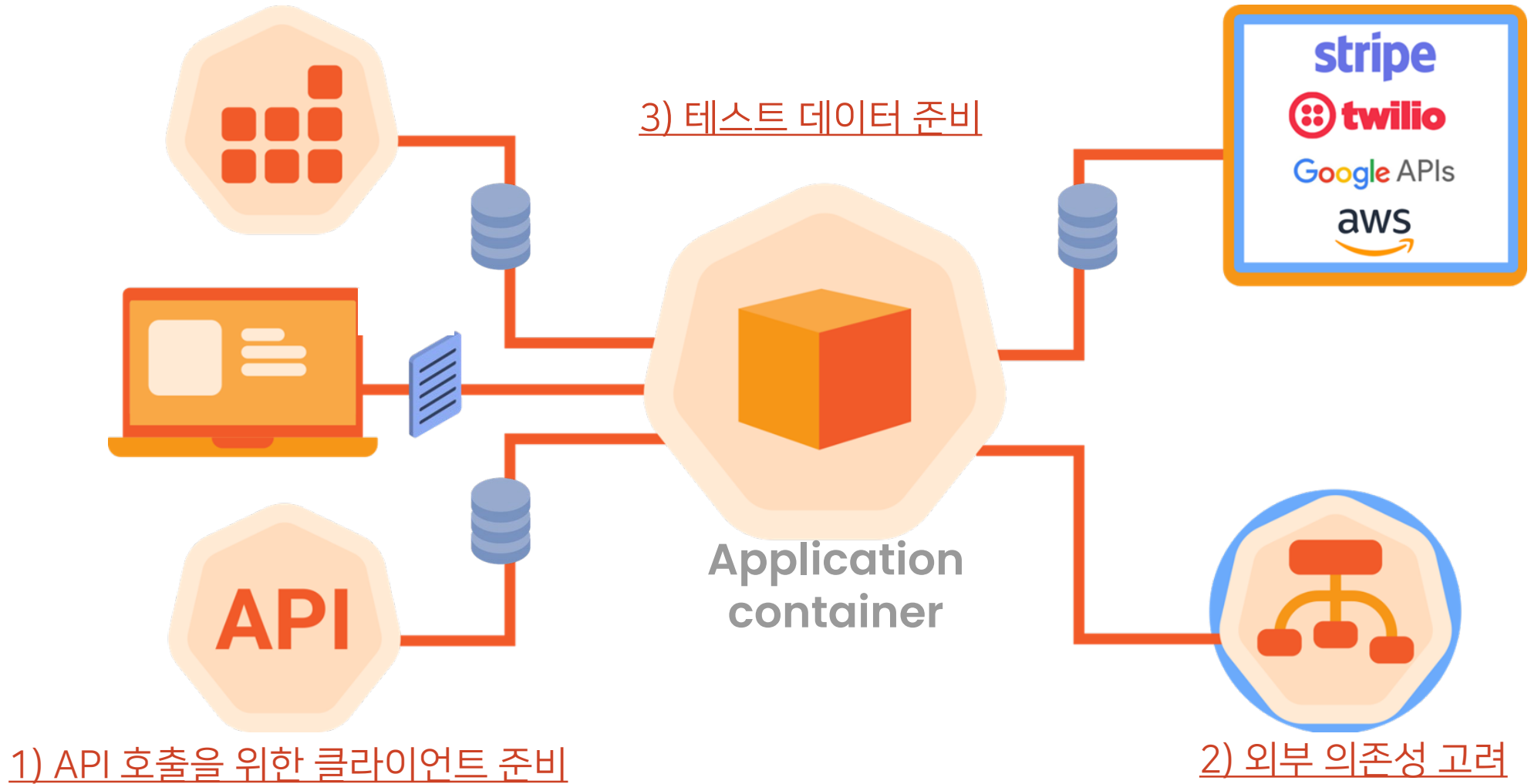
Resource CPU Memory IO Disk

Network Blackhole Latency Packet Loss DNS

4. SRE (성능 진단) - Speedscale

OSC

API 테스트의 해결과제



이상적인 API 테스트 방법론

1

2

3

Identify

: 테스트 대상 확인

Generate

: 자동 테스트 생성

Run



: 안정된 테스트 환경 확보

Identify : 테스트 대상 확인



Speedscale / payment / Traffic Viewer

Service name: 2021-08-13 12:27:11 - 2021-08-13 12:42:11

Inbound  Outbound 

Traffic filters Filter traffic that matches the following characteristics. 0 active filters

Traffic [+ Generate a Traffic Snapshot](#)

Date	Direction	Tech	Operation	Host	Location	Status
Aug 13, 2021 12:41:15 PM	out	DynamoDB	POST	dynamodb.us-east-1.amazonaws.com:443	/	200
Aug 13, 2021 12:41:15 PM	out	DynamoDB	POST	dynamodb.us-east-1.amazonaws.com:443	/	200
Aug 13, 2021 12:41:15 PM	in	JSON	POST	payment:8080	/order	200
Aug 13, 2021 12:41:15 PM	in	JSON	POST	payment:8080	/login	200
Aug 13, 2021 12:41:06 PM	out	Plaid	POST	sandbox.plaid.com:443	/accounts/get	200

Info Request **Response** [Download](#)

Headers **Body**

Actual

```
1 {
2   "accounts": [
3     {
4       "account_id": "Qdkep7X95mHv16xxJNRmsPrMx4VBAItkRGW8P",
```

- API Call 확인
- 관련 기술 확인
- 세부 사항 확인

Generate : 자동 테스트 생성



- 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 "

Create a traffic snapshot

Snapshot name
Payment Load Test

Token Config
http_standard

Filter settings

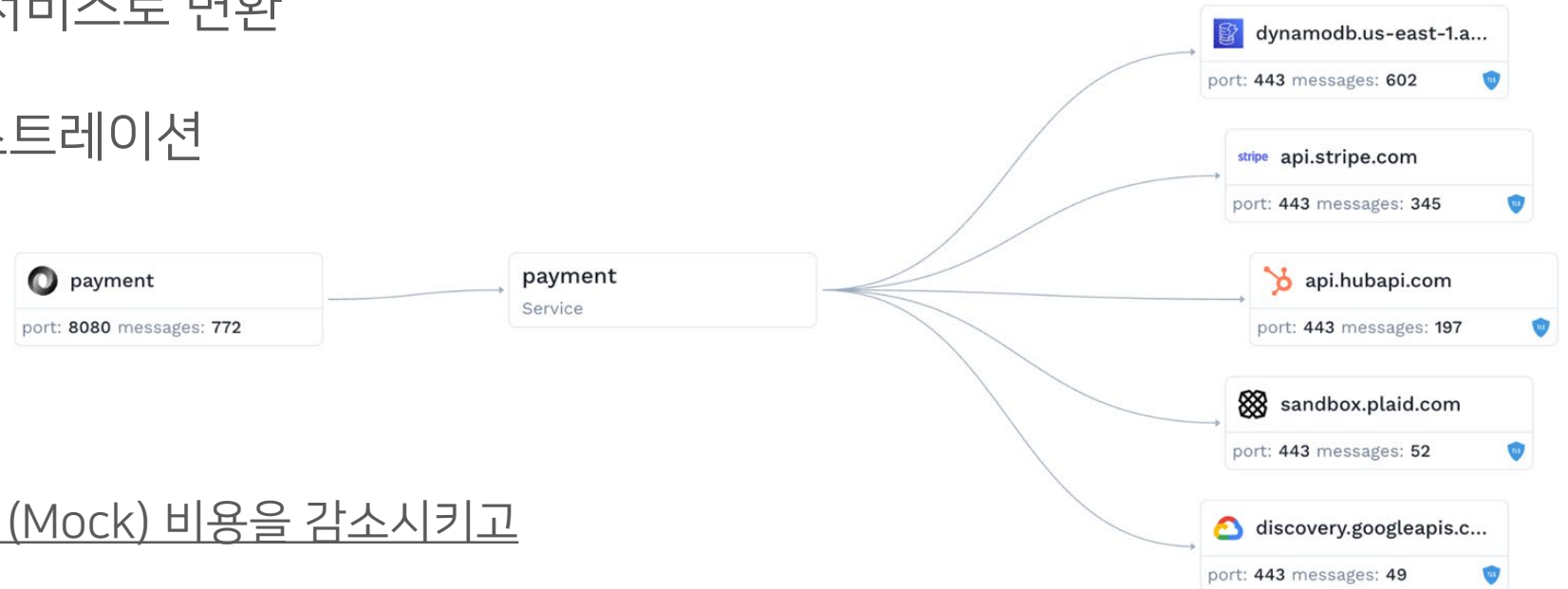
Service	is	payment
Time range	is	Aug 6, 2021 2:26:19 PM - Aug 6, 2021 2:41:19 PM
Cluster	is	gke_speedscale-demos_us-central1-c_demoz
Namespace	is	microservices
Direction	is	Inbound (in)

Close Create the traffic snapshot

Run : 안정된 테스트 환경 확보



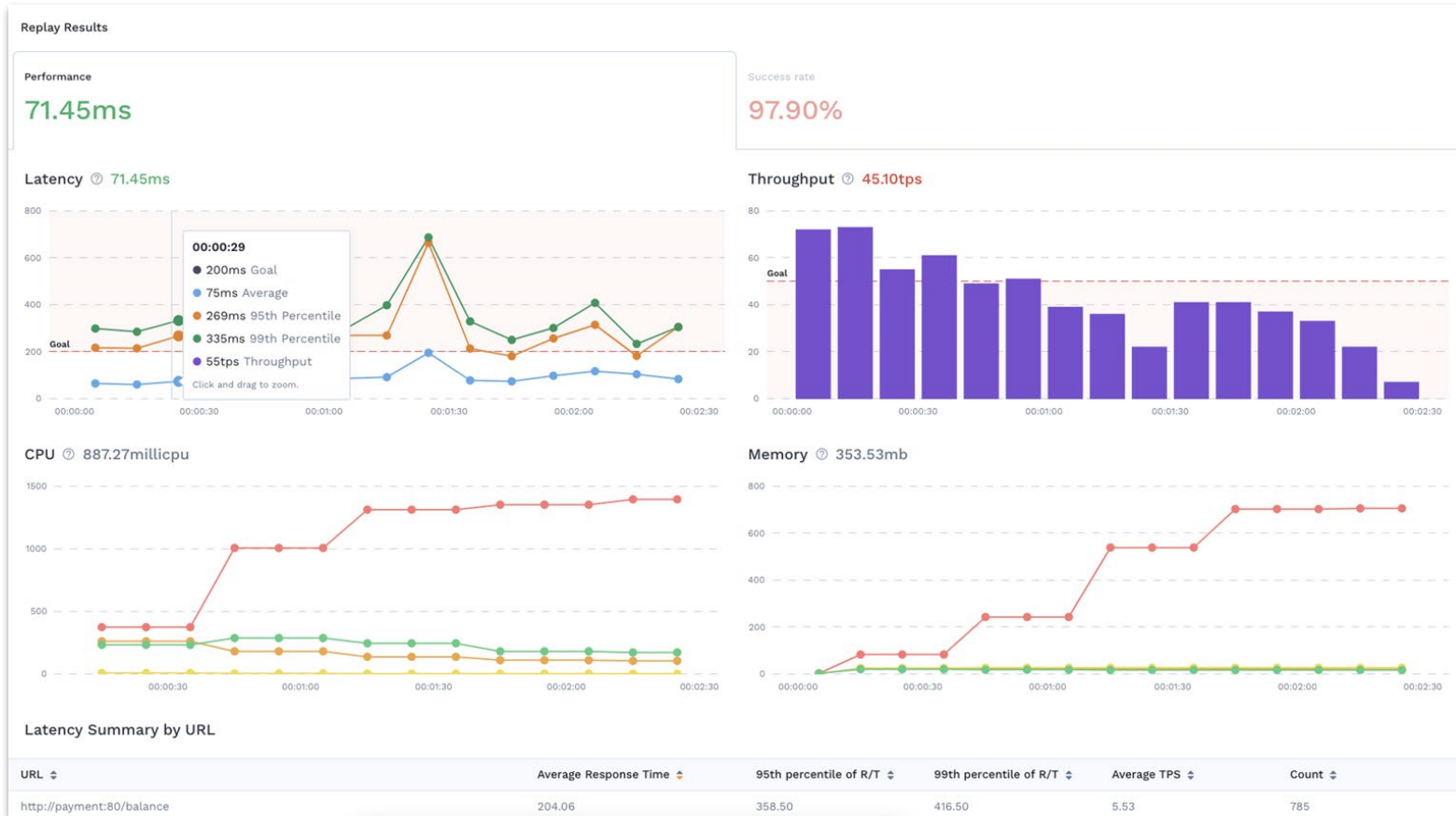
- 마이크로 서비스 의존성 탐지
- API 트래픽을 Mock 서비스로 변환
- 데이터 및 환경 오케스트레이션



"외부서비스를 대신 응답하여 (Mock) 비용을 감소시키고

테스트를 위해 충분히 안정된 환경을 확보 "

Use Case : SRE팀의 성능검증



SRE 골든 시그널(Golden Signals)

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

Use Case : 소프트웨어 개발 엔지니어 기능 테스트

Call 검증

- 비교
- 차이점 분석
- CI 정합

The screenshot displays a test results interface with a table of assertions and a detailed comparison of expected and actual JSON responses.

Time	Msg ID	Operation	URL	Status	Assertion type	Expected	Actual
Aug 13, 2021 6:39:25 AM	22	POST	/login	Fail	Status Code	200	401
Aug 13, 2021 6:39:25 AM	25	POST	/login	Fail	Status Code	200	401
Aug 13, 2021 6:39:25 AM	25	POST	/login	Fail	Body JSON	5/5 Lines Match	2/5 Lines Match
Aug 13, 2021 6:39:25 AM	26	POST	/login	Fail	Body JSON	5/5 Lines Match	2/5 Lines Match
Aug 13, 2021 6:39:25 AM	26	POST	/login	Fail	Status Code	200	401
Aug 13, 2021 6:39:25 AM	34	POST	/payment	Fail	Body JSON	19/19 Lines Match	18/19 Lines Match

Below the table, the 'Response' section shows a comparison of 'Expected' and 'Actual' JSON bodies. The 'Actual' response shows a discrepancy in the 'Code' field.

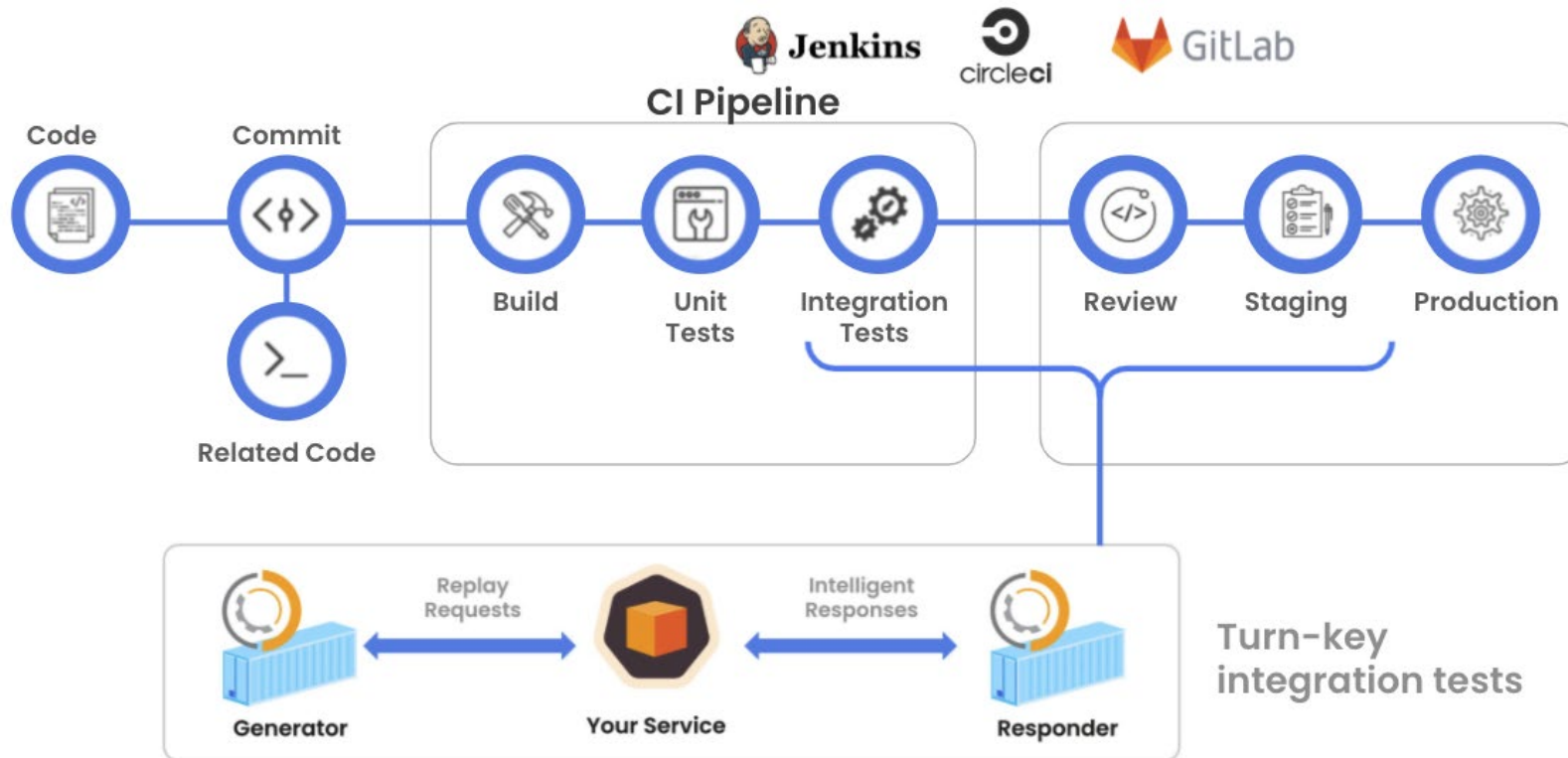
```
Expected: {
  "CardDetails": {
    "CardID": "afd2f8d5-012c-4912-a968-b3618be4c9f3",
    "Code": "0 - Approved",
    "CreditCardNumber": "4539598902254132",
    "CreditCardType": "VISA",
    "Currency": "TND",
    "Price": 17.45
  },
  "Location": {
    "IPV4": "66.235.90.34",
    "Latitude": 18.468155,
    "LocationID": "1223f686-aa21-4786-a782-3549ffb5e48c",
    "Longitude": -26.655136
  }
}

Actual: {
  "CardDetails": {
    "CardID": "afd2f8d5-012c-4912-a968-b3618be4c9f3",
    "Code": "36 - Restricted Card - Pick Up",
    "CreditCardNumber": "4539598902254132",
    "CreditCardType": "VISA",
    "Currency": "TND",
    "Price": 17.45
  },
  "Location": {
    "IPV4": "66.235.90.34",
    "Latitude": 18.468155,
    "LocationID": "1223f686-aa21-4786-a782-3549ffb5e48c",
    "Longitude": -26.655136
  }
}
```

CI Integration

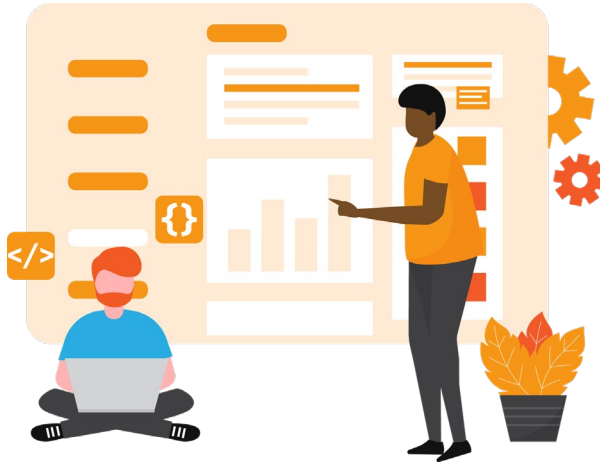
Continuous Resiliency for Kubernetes

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

■ 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

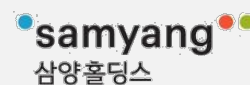
OSC Asia Group Limited

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



삼양데이터시스템(주)

- 삼양데이터시스템(주), 지주회사인 (주)삼양홀딩스가 전략적 투자
- Public Cloud 사업 확장, 고도화를 위해, Opensource 기반의 전략적인 WIN-WIN 구조로 사업의 Synergy 기대



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



■ 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



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



■ 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



NAVER
CLOUD
PLATFORM



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



Gold
Partner
TRAIN



감사합니다.

We are your trusted Digital Transformation Partner

www.osckorea.com