

Gremlin OSC

# OSC Korea & Demo

김대성 과장, DevOps Engineer, OSC Korea

Break Things On Purpose



Inject something harmful to  
**build an immunity.**

# Gremlin

항체 주입을 통해 면역체계 형성





Microservices

“경쟁 우위 확보를 위해 빠른 혁신 불가피“

Speed of innovation is a competitive advantage



DevOps

*“The time has come for IT to face the actual complexity required to really drive its own transformation”*

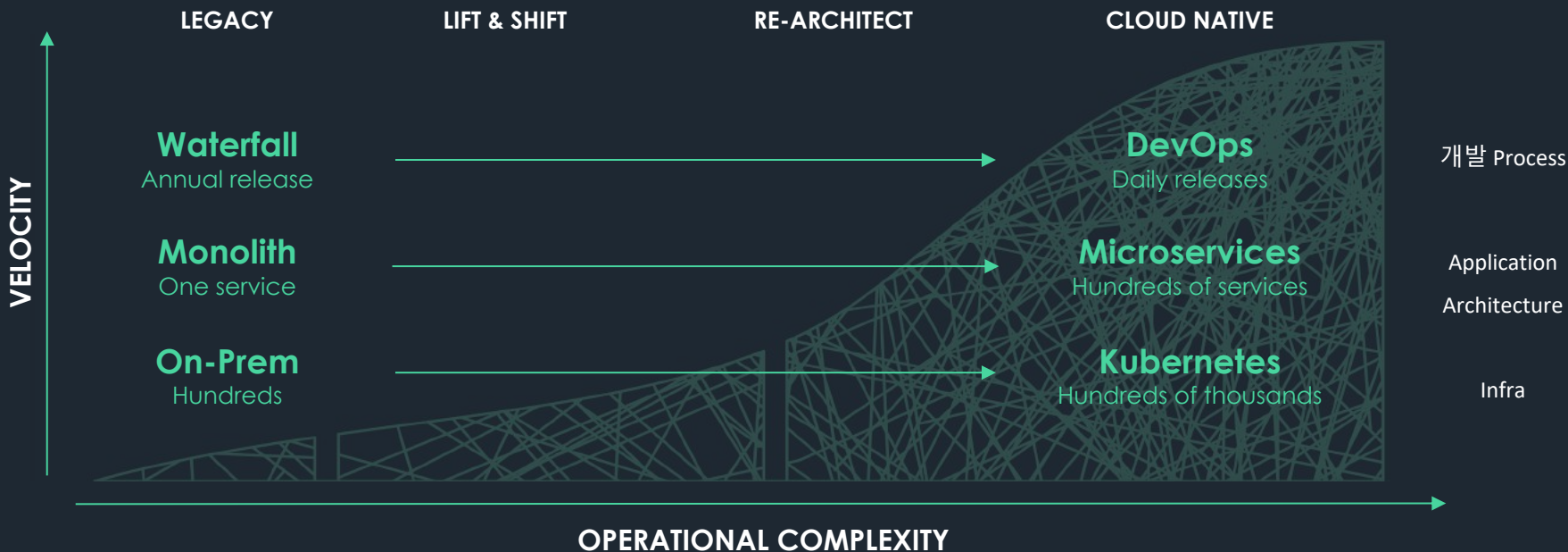
– McKinsey

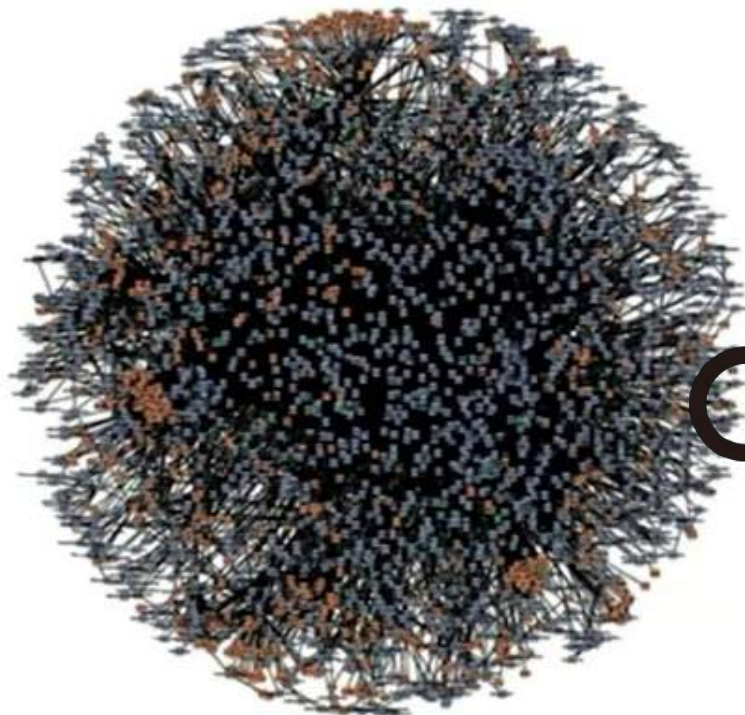


Cloud

# Velocity Comes at a Price

Application/Service는 급격한 속도로 복잡해지고 있음 : 운영 난이도 증가



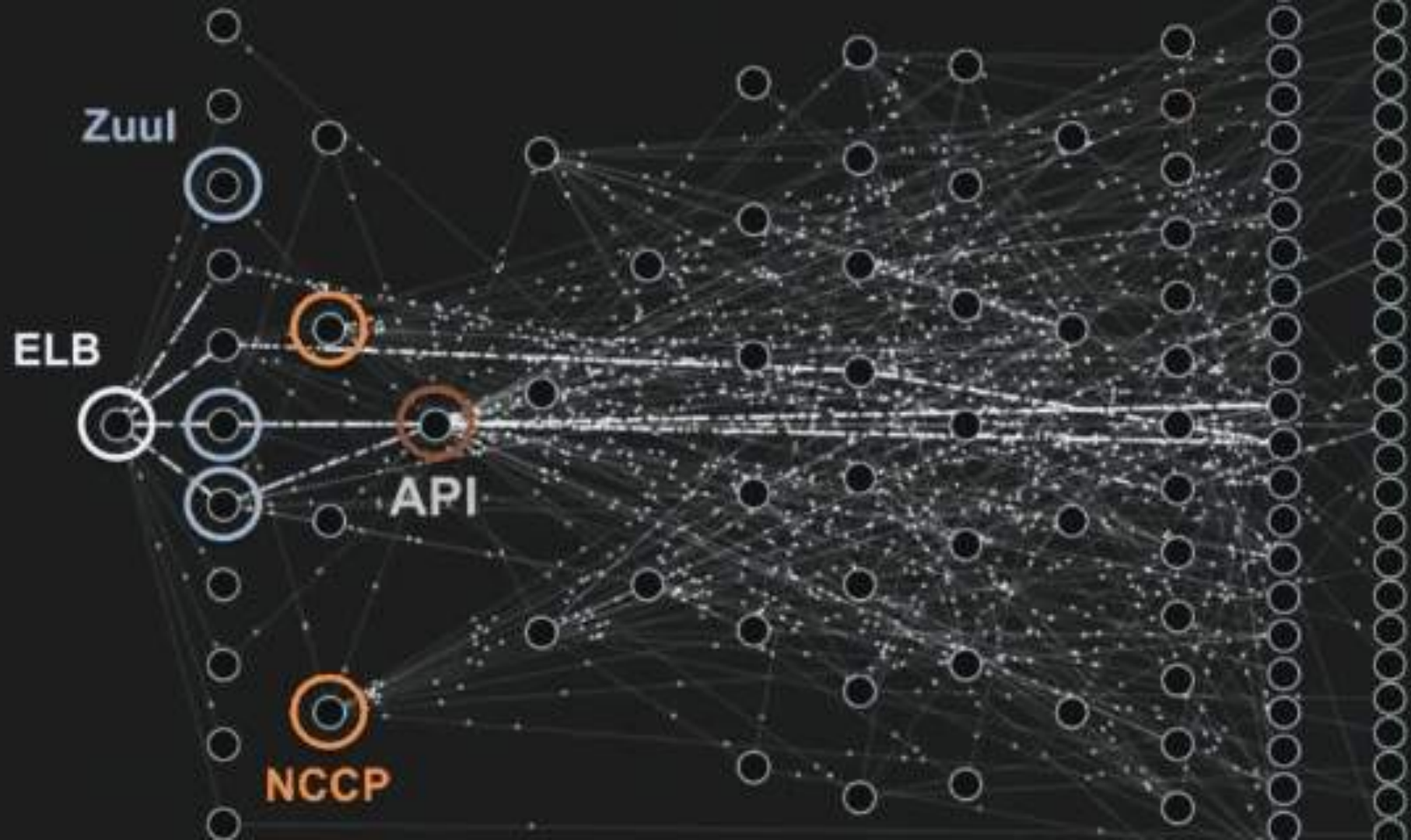


amazon

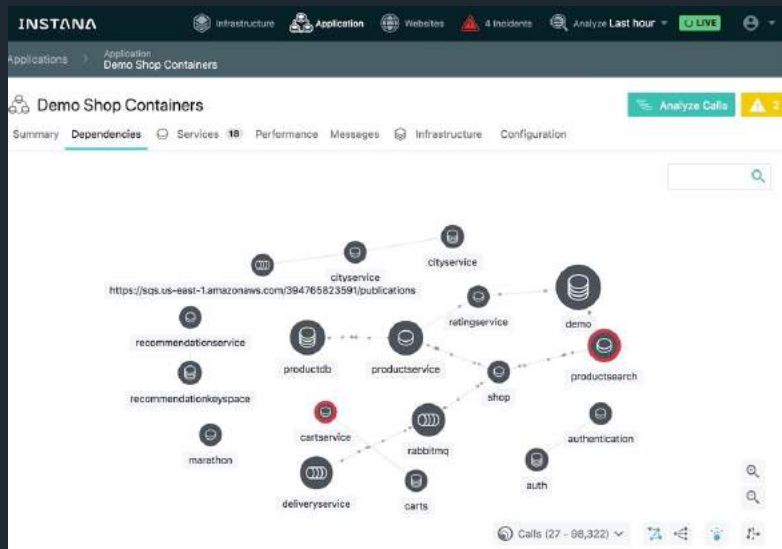
OSC



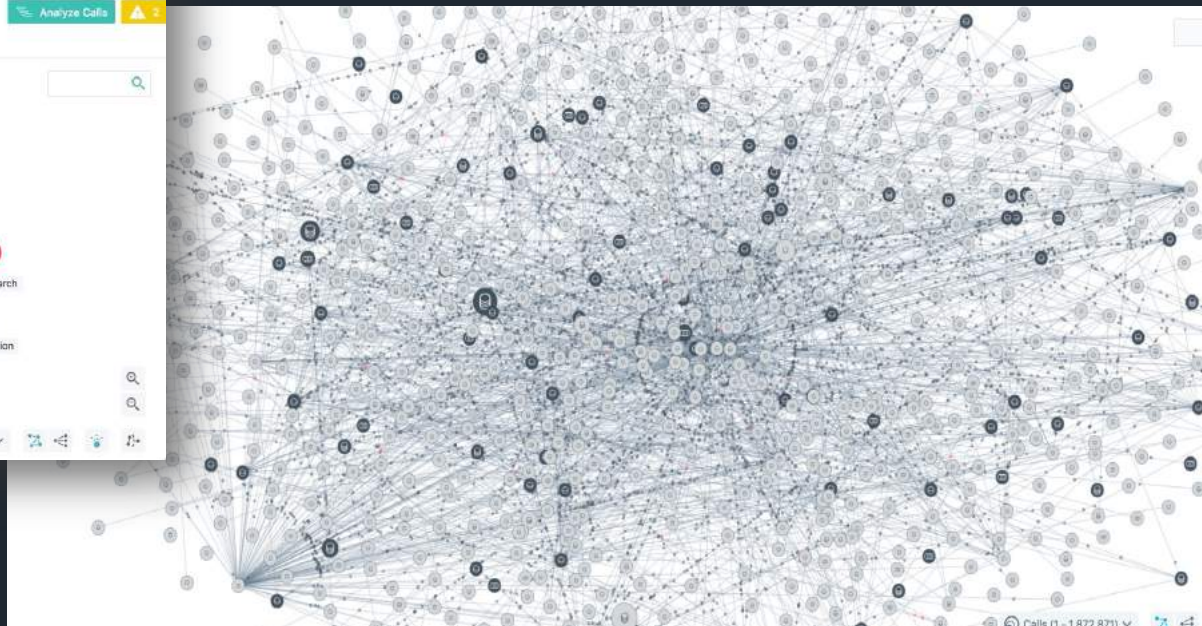
NETFLIX



# Dependency Map - Instana View

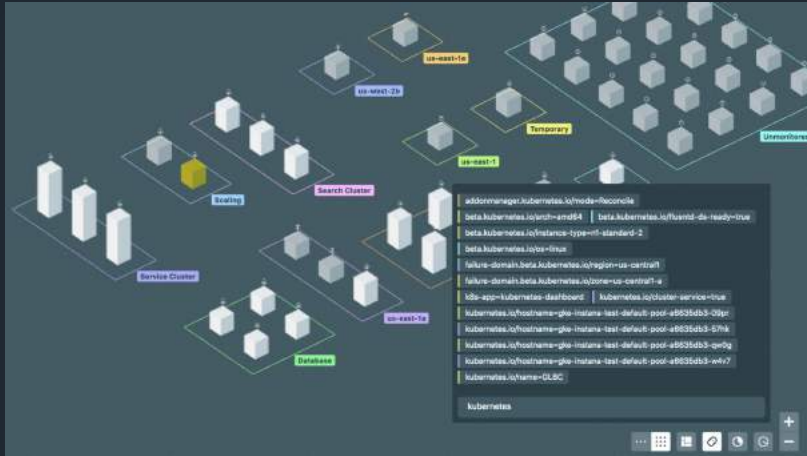


STG / PRD 환경



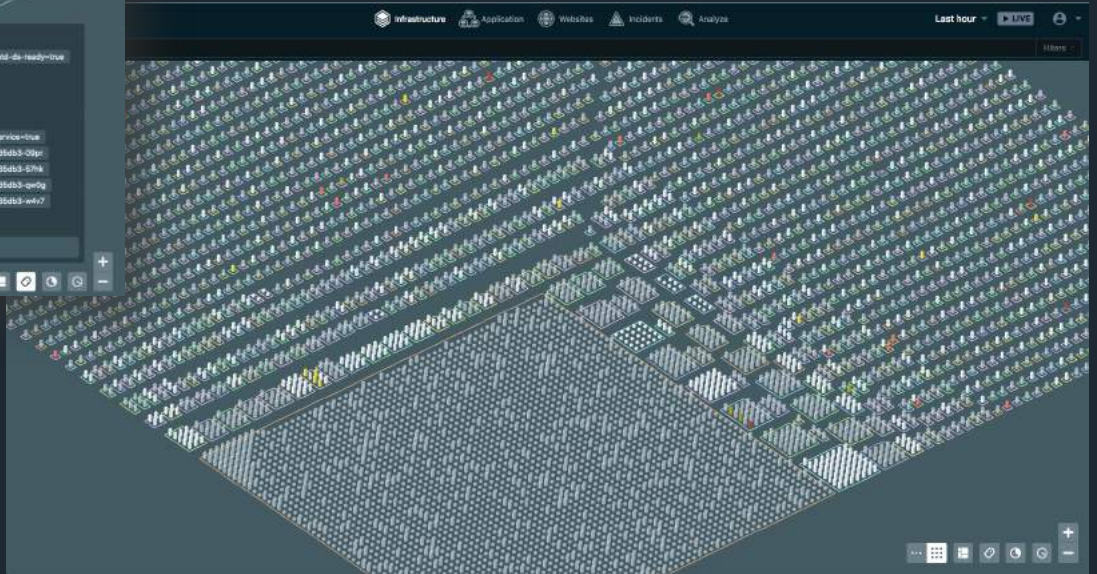
SIT / QA 환경

# Infrastructure Map - Instana View



SIT / QA 환경

STG / PRD 환경



## 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

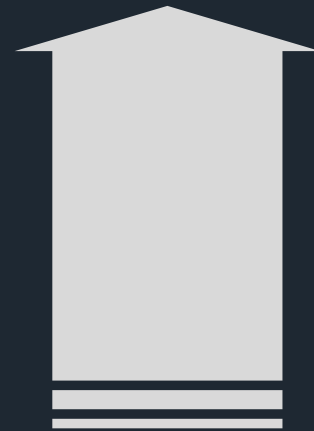
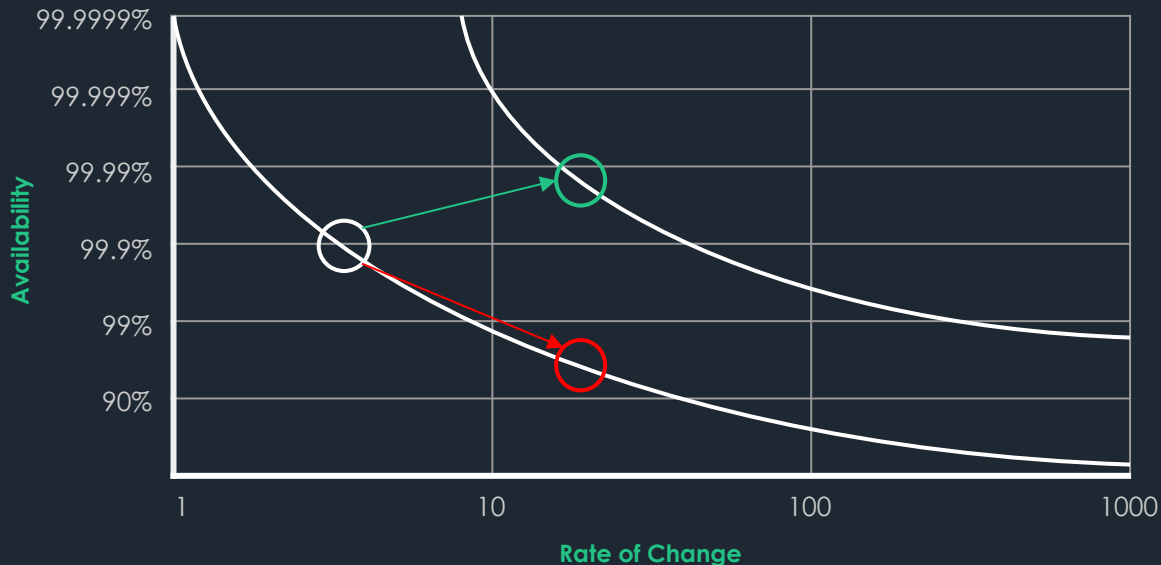
4.1.19



# The Reliability Gap

“ 작은 배포에도 품질수준을 유지하기 위한 방안 필요 ”

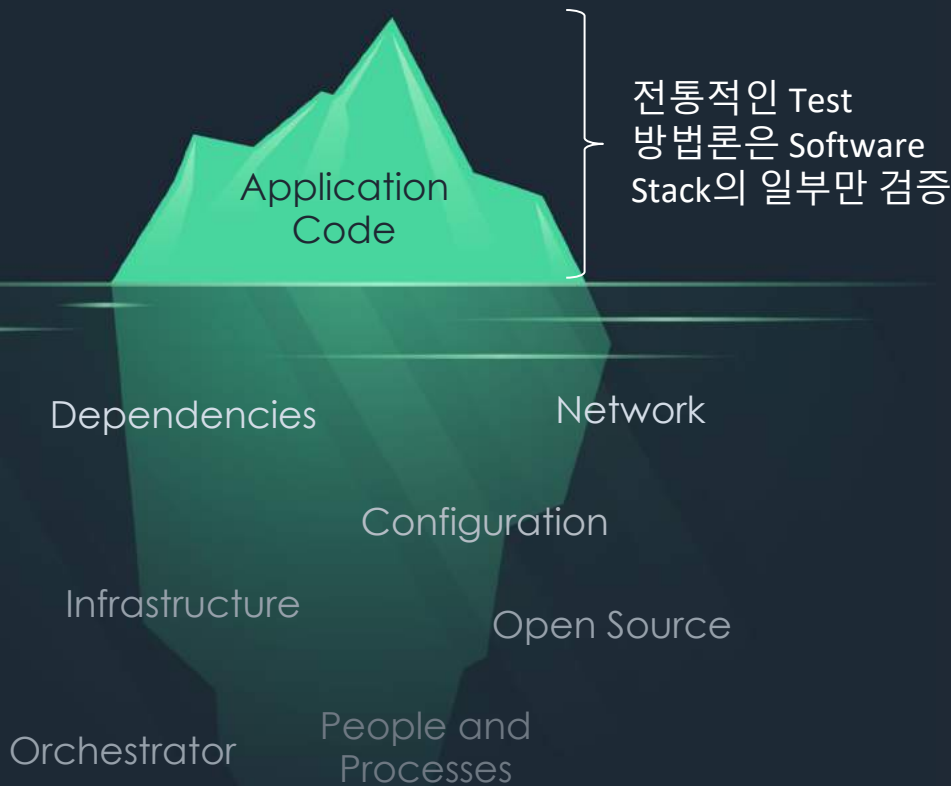
가용성 vs. 변경 속도



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

- Richard Cook, How Complex Systems Fail

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

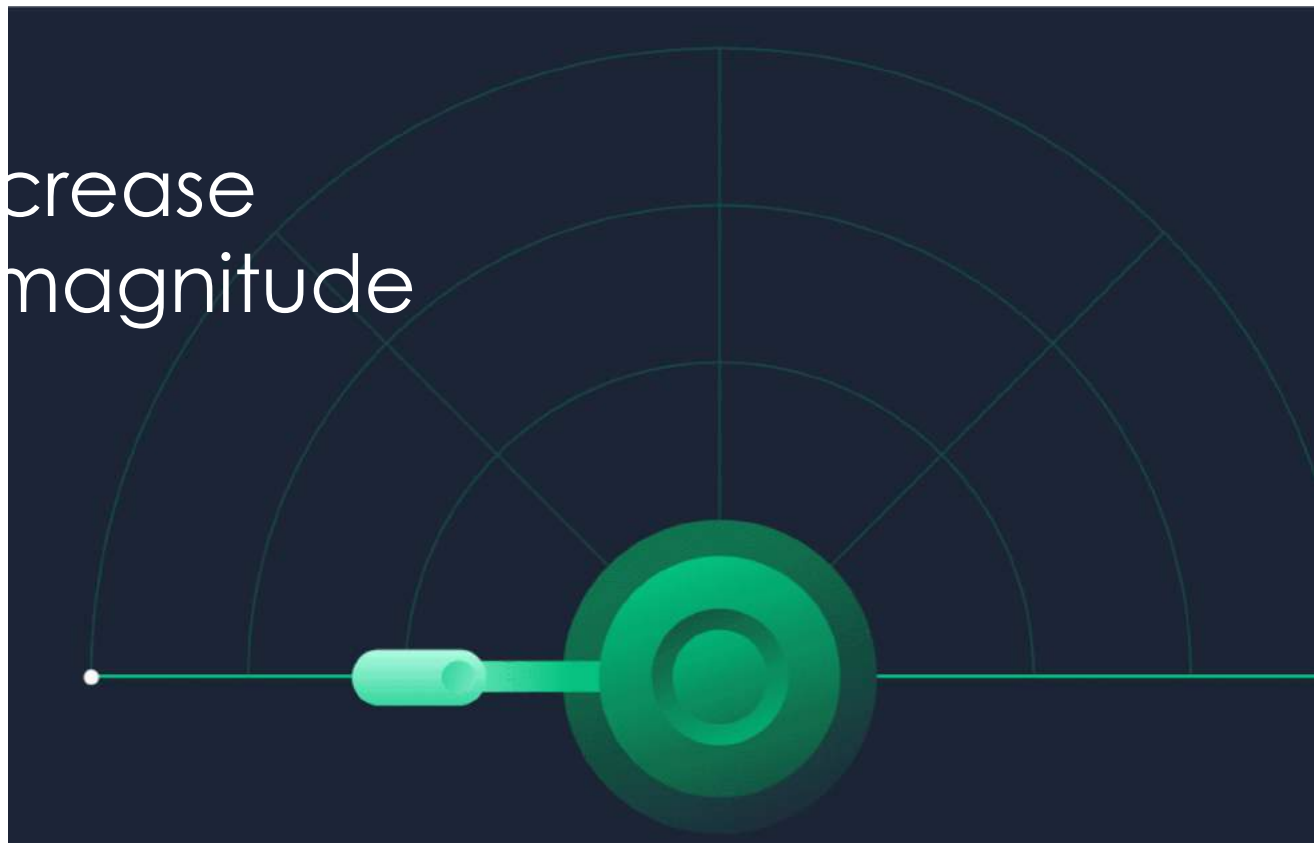
Processes

Application

Infrastructure

Progressively test  
your system to  
isolate problems  
and mitigate risk

Increase  
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

# Benefits of Chaos Engineering

장애감소



장애 10배 감소



장애 해결시간 감소



MTTD (Mean Time to Detect)  
수시간에서 5분으로 감소



빠른 배포



4배 빠른 K8S Migration



성공적인 런치



GameDay 한번으로 35개의 High  
Priority 버그를 발견하여 수정



# Chaos Engineering completes DevOps

“분산System을 안정적으로 운영하는 유일한 방법은 Chaos Engineering을 도입하는 것”

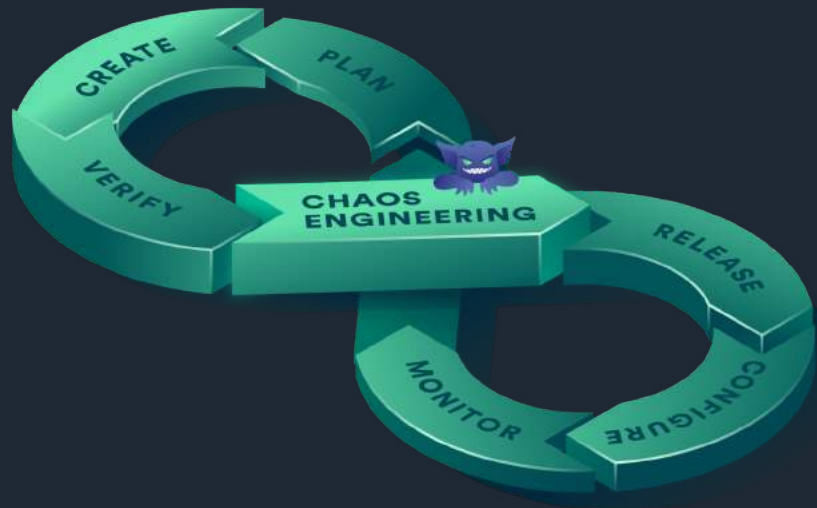
- Gartner

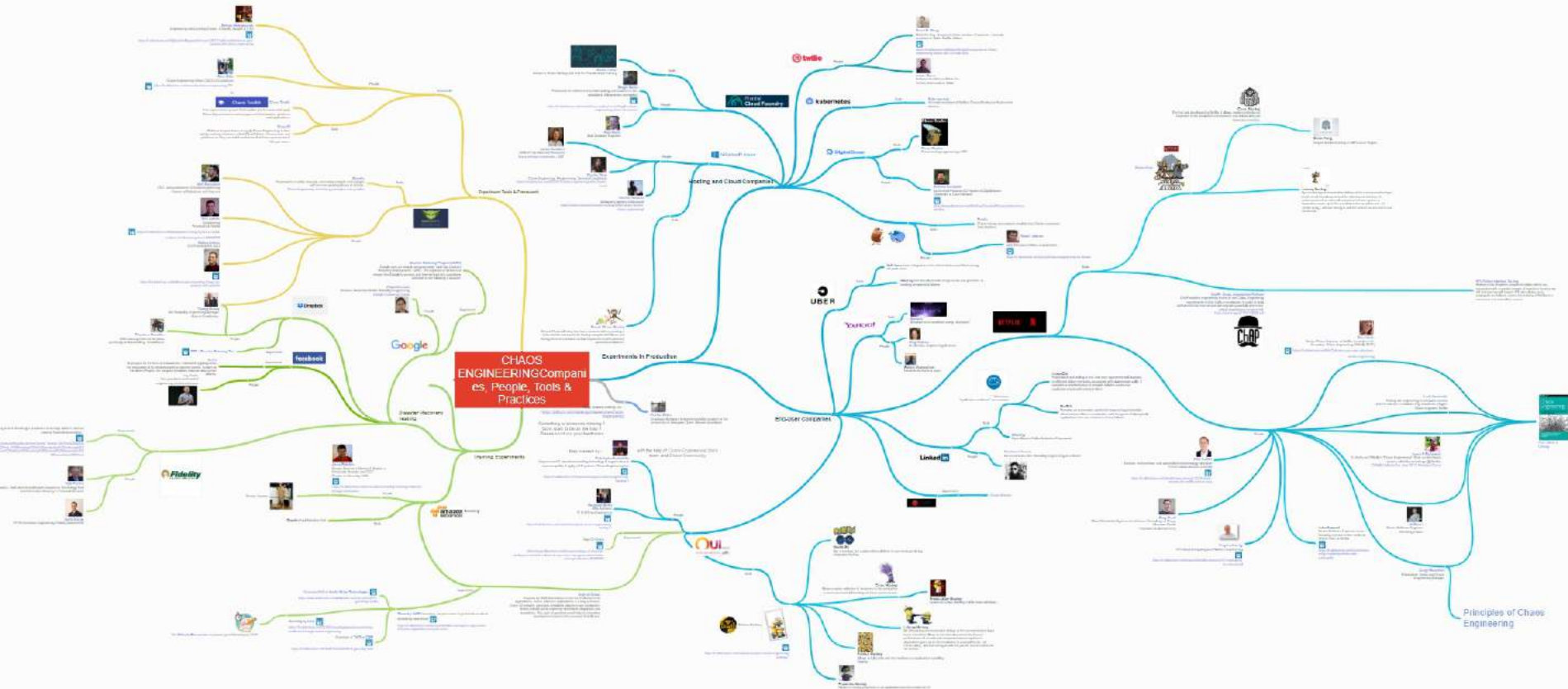
“By 2023, 40% of organizations will implement chaos engineering practices as part of DevOps initiatives, **reducing unplanned downtime by 20%**.”

-Gartner

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

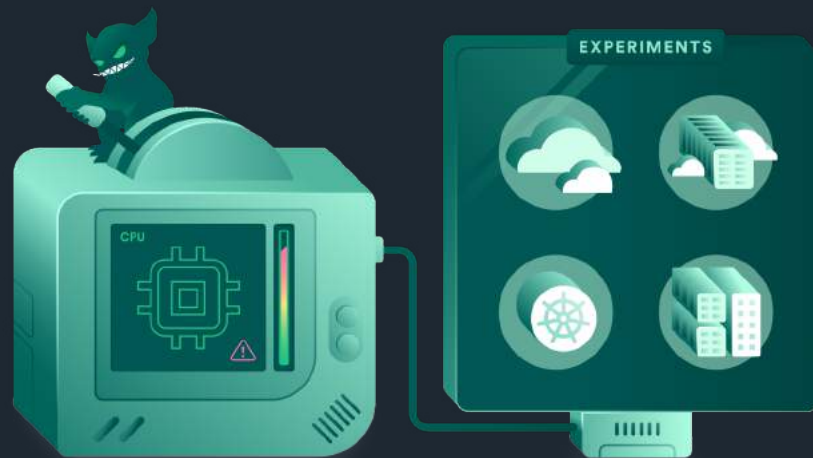
<https://www.gartner.com/smarterwithgartner/the-io-leaders-guide-to-chaos-engineering/>





# Chaos Engineering Platform

  
**Gremlin**





**Kolton Andrus**  
**CO-FOUNDER &**  
**CEO**

Chaos Engineer & Call Leader  
Netflix & Amazon



**Matthew Fornaciari**  
**CO-FOUNDER & CTO**

Senior Platform Engineer  
Salesforce & Amazon

---

**We've done this before.**

---

**NETFLIX**

**amazon**

**salesforce**

# Trusted By Teams Worldwide

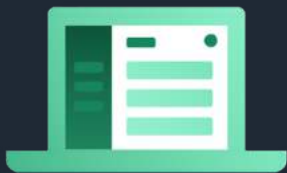
Across Retail, Financial Services, High Tech, Media, Healthcare, and more



# 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 | Application



Gremlin VMware



AWS



Azure



Google



Docker



K8S



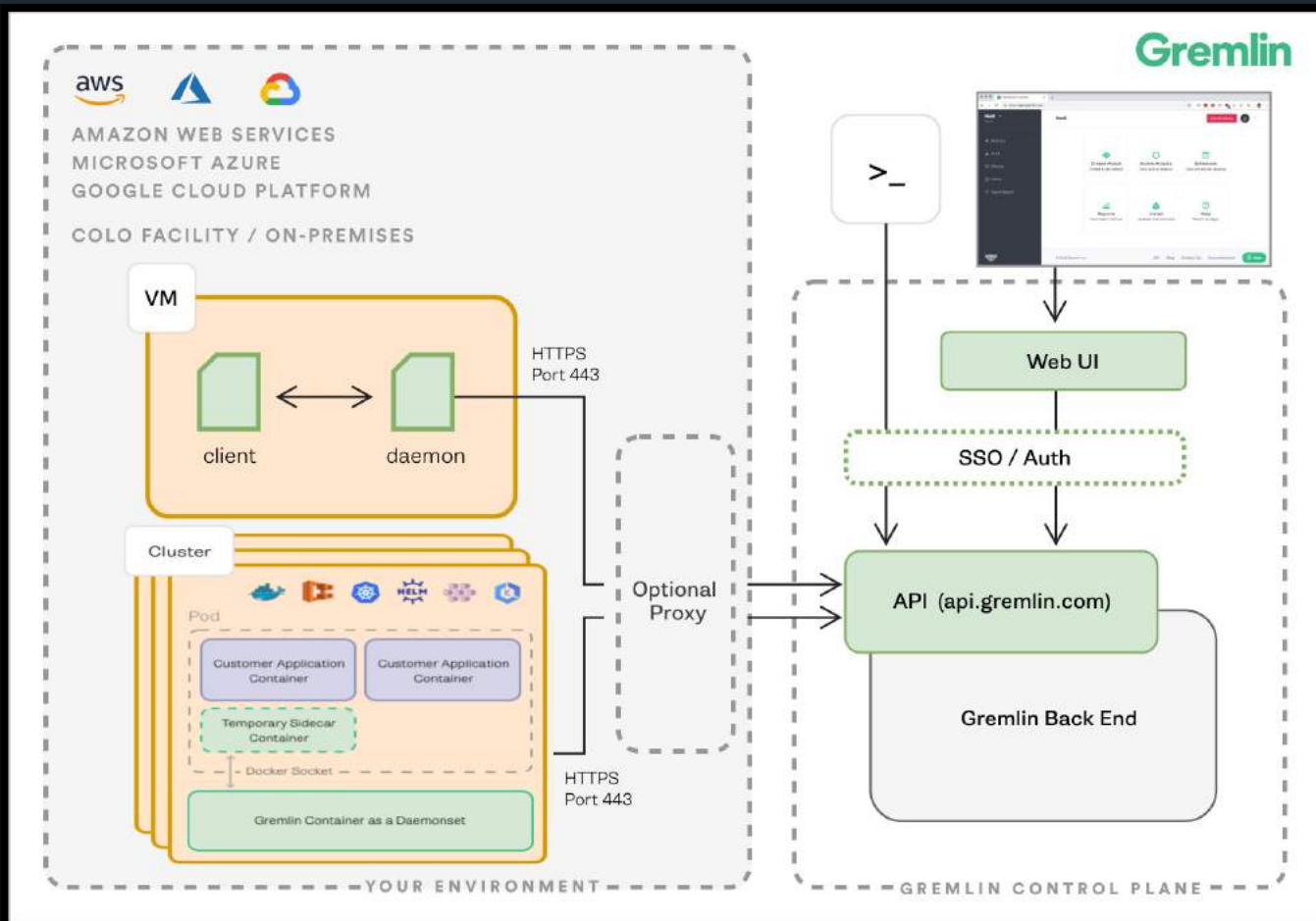
Linux



Windows



Serverless



Scenarios

Attack

Schedule

Client

보고서

문서

API



Scenarios

Attacks

Schedules

Clients

Reports

Docs

<> API



Halt All Attacks

**ENTERPRISE** Client Version: 2.15.2 - 2.15.3

### Welcome back, Thomas!

SE



+ Invite your team members

Link your attacks together

Create Scenario

Want to recreate a failure?

View Recommended Scenarios

Quickly run an attack

Create Attack

#### Targets

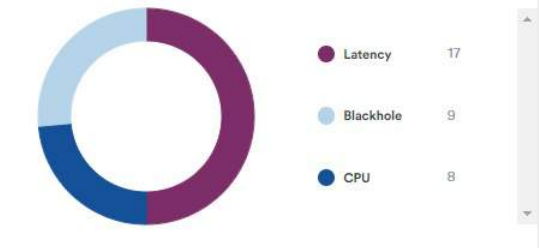
Provisioned: 50/day

View All

<b>ACTIVE</b>	2.compute.internal Last Attacked: 5 hours ago ip-172-31-61-227.ap-northeast-1.compute.amazonaws.com	Attack
<b>REVOKED</b>	172.31.10.86 Last Attacked: 5 hours ago	
<b>REVOKED</b>	172.31.13.165	
<b>REVOKED</b>	172.31.13.165	

#### Total Attacks Run

This week

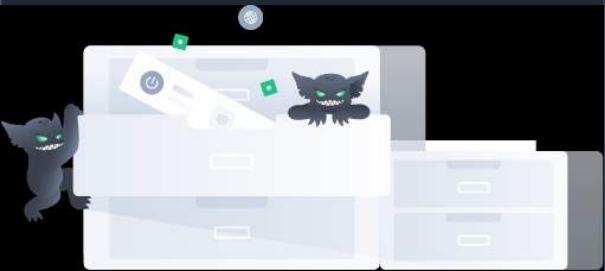


#### Recent Scenarios

<b>Latency</b> Last run: 7/16/2020		>
<b>CPU</b> Last run: 6/22/2020		>
<b>Memory</b> Last run: 6/22/2020		>
<b>Latency</b> Last run: 6/4/2020		>

#### Recent Attacks

<b>Latency</b> 7/17/2020 1:28 pm	<b>SUCCESSFUL</b>	>
<b>Latency</b> 7/17/2020 1:25 pm	<b>SUCCESSFUL</b>	>
<b>CPU</b> 7/17/2020 11:19 am	<b>SUCCESSFUL</b>	>
<b>CPU</b> 7/17/2020 11:16 am	<b>SUCCESSFUL</b>	>



1

### What do you want to attack? Attack 대상

Hosts 0 available   Containers 122 available   Applications 0 available   Kubernetes 171 available

2

### Choose Hosts to target Attack 범위

Specify the coverage and details for impact

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 2
- 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

Application Targeted Attacks

State Shutdown Time Travel Process Killer

Resource CPU Memory IO Disk

Network Blackhole Latency Packet Loss DNS

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 Blockade, 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 Change the system time.

Delay The number of minutes to delay before shutting down: 1

Reboot Indicate the host should reboot after shutting down:

4

### Run the attack Attack 시점

Unleash now or schedule for later

Schedule for later Run the 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 07/17/2020

Time \* Local Military Time 10:00

Hours field must be completed

Unleash Gremlin Cancel Gremlin API Example

## Gremlin

### Uh-oh, a status check failed and halted this Scenario

Scenario	Validate Auto-Scaling
Author	koltzn@gremlin.com
Team	Status Checks
Status Check	Pagerduty endpoint
Scenario Start	2020-06-16 17:48:35
Scenario Halted	2020-06-16 17:48:36

OPEN SCENARIO

#### Can't click the link?

Copy and paste this URL into your browser: <https://app.staging.gremlin.com/scenarios/detail/7679b10d-4332-44cb-b9b1-0d4332e4cb3a/runs/1>



© 2020 Gremlin Inc.

55 S. Market Street, Suite 1205, San Jose, CA 95113

## Configure Scenario

Specify the steps to run.

## Status Check

Configure Scenario

- What's my system's steady state?** app.datadoghq.com... Status Code: 200 Timeout: 500 ✓  
Delay: 5 s
- Is my system ready? Should I halt the Scenario?** api.pagerduty.com... Status Code: 200 Timeout: 500 ✓  
Delay: 5 s
- Latency** 1 minute 50% of 23 MS: 500 ...  
Delay: 5 s
- Did my system return to normal? Should I continue the Scenario?** api.newrelic.com... Status Code: 200 Timeout: 500 ✓  
Delay: 5 s
- Latency** 1 minute 100% of 23 MS: 1000 ...  
Delay: 5 s
- Was my Scenario successful?** app.datadoghq.com... Status Code: 200 Timeout: 500 ✓  
Delay: 5 s

NEW

**Add a Status Check**  
Ensure your system stability.

**Add a Completed Attack**  
Find an attack to use.

**Add a New Attack**  
Create a new attack.

# Application Level Fault Injection (ALFI)

Request 기반 Metadata 활용

Customer ID, Device ID, Country 등을 이용해 **Attack Radius**를 제어

System 접근이 어려운 경우

AWS Lambda 등 **Serverless** 환경에서 Application에 장애 삽입 메커니즘 구현 (e.g. Run in the JVM)

## 응용 사례

Id

특정 Customer ID에 대한 적용되는 Attack을 생성하여 Monitoring 하여 다른 사용자는 영향을 주지 않도록 구성



일부 특정 Endpoint에 만 장애를 유발하고 나머지 Endpoint는 정상인 환경 구성



Always-on 장애 환경을 관리하여 있는 특정 Device에 대해서만 구성하여 정기적으로 장애영향 분석

# Application 수준의 장애 주입 설정

4

**Choose a Gremlin**  
Select the type of attack to unleash.

## Attack 종류

Latency\*  
The amount of latency in ms to apply.

Throw Exception\*  
Simulate an exception with this impact.  Off

5

**Run the attack**  
Unleash now or schedule for later.

## Attack 수행

**Now**  
Immediately run the attack.

Duration\*  
The duration of the attack.

**Unleash Gremlin** Cancel



⚡ What do you want to attack?

## 1 Application Attack

**Hosts**  
2 available

**Containers**  
80 available

**Applications**  
0 available

**Kubernetes**  
101 available

**Choose application coordinates to attack**  
Specify the coverage and details for impact.

2

Application Query

- AWS Lambda Function**  
Target your AWS Lambda functions.
- AWS EC2 Application**  
Target your AWS EC2 applications.
- Custom Application Type**  
Create a custom application type.

Region (required)

Availability Zone (required)

Instance ID (required)

Custom Value

Key	Value
	<input type="text"/>

## Application Query

3

Traffic Query

- Outbound HTTP Traffic**  
Impact an HTTP client in your applications.
- Dynamo DB Traffic**  
Impact an AWS Dynamo DB client in your applications.
- Custom Traffic Type**  
Create a custom traffic type.

Verb (required)

Client Name (required)

Percent to Impact

%

Custom Value

Key	Value
	<input type="text"/>

## Traffic Query

## FREE

### FOR GETTING STARTED

Familiarize yourself with Chaos Engineering by safely experimenting with a limited Blast Radius.

- ✓ 1 Team
- ✓ 1 Installed Agent
- ✓ Unlimited Attacks per Target
- ✓ 2 Attacked Targets per month
- ✓ [Community support](#)

## STARTER

### FOR SINGLE APPLICATIONS

First time users running GameDays on a single application. Unlocks all experiment types for one Team.

- ✓ 1 Team
- ✓ 5 Installed Agents
- ✓ Unlimited Attacks per Target
- ✓ 5 Attacked Targets per month
- ✓ [Community support](#)

## PRO

### FOR SMALL ORGANIZATIONS

For small organizations with a limited number of Teams and applications. Adds security controls and compliance.

- ✓ 3 Teams
- ✓ Unlimited Agents
- ✓ Unlimited Attacks per Target
- ✓ 30 Attacked Targets per week
- ✓ [Basic 8-8, M-F support](#)

## ENTERPRISE

### FOR MID-LARGE ORGANIZATIONS

Mid and large organizations with multiple Teams running and automating experiments. Includes security controls and production support.

- ✓ 5 Teams
- ✓ Unlimited Agents
- ✓ Unlimited Attacks per Target
- ✓ 50 Attacked Targets per day
- ✓ 2 Large scale experiments
- ✓ [Dedicated 24/7 support](#)

## Add-on packages

### STARTER

- ✓ 5 additional Attacked Targets per month
- ✓ 1 Add-on maximum

### PRO

- ✓ 1 additional Team
- ✓ 10 additional Attacked Targets per week

### ENTERPRISE

- ✓ 1 additional Team
- ✓ 10 additional Attacked Targets per day

# Feature Comparison

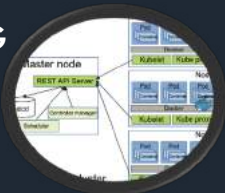
	FREE	STARTER	PRO	ENTERPRISE
Linux/Windows	✓	✓	✓	✓
Containers	✓	✓	✓	✓
Kubernetes	✓	✓	✓	✓
Application/Serverless	✗	✗	✓	✓
State Attack	1	3	3	3
Resource Attack	1	4	4	4
Network Attack	1	4	4	4
Large Scale Exp.	✗	✗	✗	2
SAML	✗	✗	✓	✓
RBAC	✗	✗	✓	✓
Audit Trail	✗	✗	✓	✓

### Service A

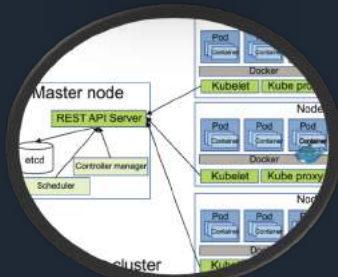


**STARTER**

DEV/STG



PRD



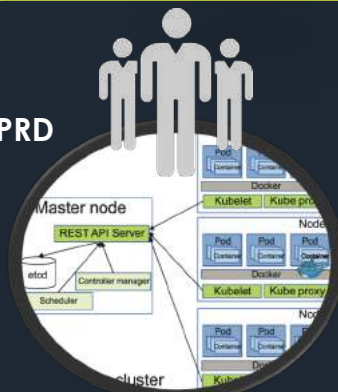
### Service B



DEV/STG



PRD



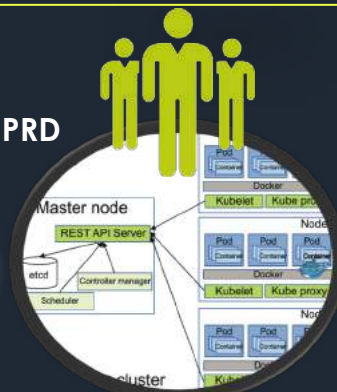
### Service C



DEV/STG



PRD



**PRO**

**ENTERPRISE**

- License 정책 : 최소 계약기간 12개월
- Plan 변경 : Upgrade 가능
- Team별 최대 사용자 : 제한 없음
- Target 당 Attack 수 제한 : Attack 횟수 및 Attack Type 에 대한 제한 없음
- Attacked Target 산정 : 첫번째 Attack이 Target에 대해 이루어지면 Attacked Target으로 기록됨
- Attacked Target 수 제한 : Plan에 따라 월별/주별/일별 Unique한 Target 수 한정
- Team간 Attacked Target 수 조정 : 계약기간내 변경 불가 (Enterprise Plan만 분기별 재조정 가능)
- ALFI 산정 : Query 하나당 하나의 Attacked Target으로 산정 (Query내 Traffic Query는 산정 하지 않음)

***“ The best way to avoid failure is to fail constantly ”***

***“ Chaos doesn't cause problems. It reveals them ”***

# OSC Korea Demo

# OSC Korea는 디지털 트랜스포메이션 전문기업입니다.

고객에게 혁신적이고 이상적인  
모던 아키텍처와 최적화된 기술을  
제공합니다.

## 한국 리눅스 재단 운영

- 국내 오픈소스 생태계 활성화 지원
- CNCF, Cloud Foundry, Hyperledger, LFEEdge, LFAI, LFPH 등 후원



## MSA(Microservice) 전문기업

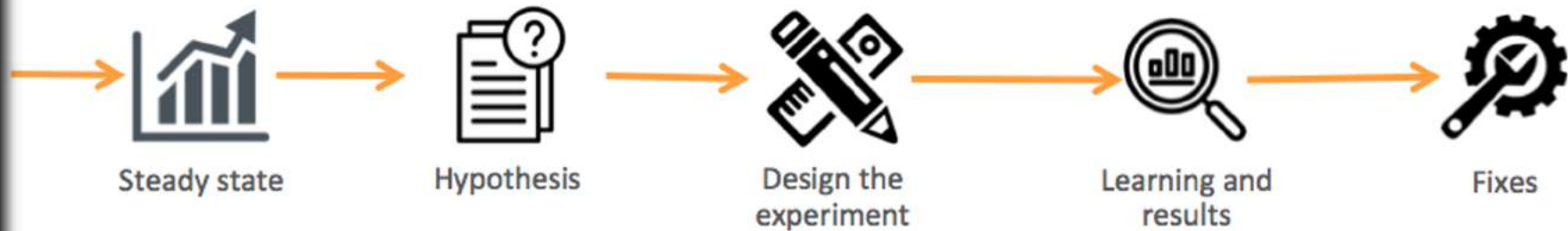
- 오픈소스 기반 아키텍처 컨설팅 및 구축
- 다양한 MSA 방법론에 기반한 Modern Architecture 설계 지원












## 글로벌 솔루션 공급

- 디지털 트랜스포메이션에 필요한 글로벌 솔루션 발굴
- 고객 요구사항 및 시장 환경에 부합하는 최적의 솔루션 통합 제공





- 
-  Services
-  Scenarios
-  Attacks
-  Schedules
-  Clients
-  Reports
-  Docs
-  API

## Attacks > New

 What do you want to attack?

Services Infrastructure Applications BETA

 **Hosts**  
4 available

 **Containers**  
52 available

 **Kubernetes**  
55 available

 **Choose Hosts to target**  
Specify the coverage and details for impact

Tags Exact

Q Narrow the number of potential targets by tag

Target all hosts

Expand All

> Operating Systems

1

> Zone

2

> Region

1

> local-hostname

4

> local-ip

4

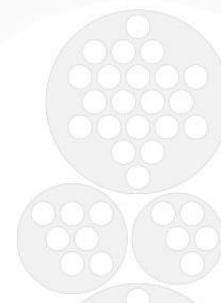
> Other Tags

17

BLAST RADIUS

0 of 4  
HOSTS TARGETED

0  
HOSTS IMPACTED



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

Hosts (0 available) Containers (122 available) Applications (0 available) Kubernetes (171 available)

**2** **Choose Hosts to target** **Attack 범위**  
Specify the coverage and details for impact

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 (2)
- Other Tags (13)

**ELAST RADIUS**

3 of 3 HOSTS TARGETED | 3 HOSTS IMPACTED

Host (green dot) Container (light green dot)

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, State, Network

Attacks: Process Killer, Shutdown, Time Travel

Delay: 1 (The number of minutes to delay before shutting down)

Reboot: On (Indicate the host should reboot after shutting down)

**4** **Run the attack** **Attack 시점**  
Unleash now or schedule for later

Schedule for later:  Only once (Set the date and time) |  Randomly within a timeframe (Select at least one day)

Date: 07/17/2020

Time: 10:00 (Local Military Time)

Hour field must be completed

Unleash Gremlin | Cancel | Gremlin API Example

리소스

**Choose a Gremlin**  
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

- CPU**  
Consumes CPU resources
- Disk**  
Consumes disk space
- IO**  
Consumes targeted file system device resources
- Memory**  
Consumes memory

상태

**Choose a Gremlin**  
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

네트워크

**Choose a Gremlin**  
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

- Blackhole**  
Drops all outgoing network traffic
- DNS**  
Blocks access to DNS servers
- Latency**  
Adds latency to all matching egress network traffic
- Packet Loss**  
Introduces packet loss to all matching egress network traffic

**Length**  
The length of the attack (seconds)

60

**CPU Capacity**  
The percentage of CPU to consume on each core  
Percent utilization is subject to active processes and will not exceed the requested amount

**Cores**

1

The number of CPU cores to hog

**Length**  
The length of the attack (seconds)

60

**IP Addresses**  
Only impact traffic to these IP addresses  
Exclude an IP address from impact with a leading "-" Add spaces or commas (,) after each log

**Device**  
Impact traffic over this network interface  
Default is the first device found (e.g. eth0)

**Hostnames**  
Only impact traffic to these hostnames  
Exclude a host from impact with a leading "-" Add spaces or commas (,) after each log

[api.gremlin.com](http://api.gremlin.com)

**Remote Ports**  
Impact outgoing and incoming traffic to and from these remote ports  
Range work like "1000-2000"

^53

**Local Ports**  
Impact outgoing and incoming traffic to and from these local ports  
Range work like "1000-2000"

**Providers**  
External service providers to affect

Service Providers

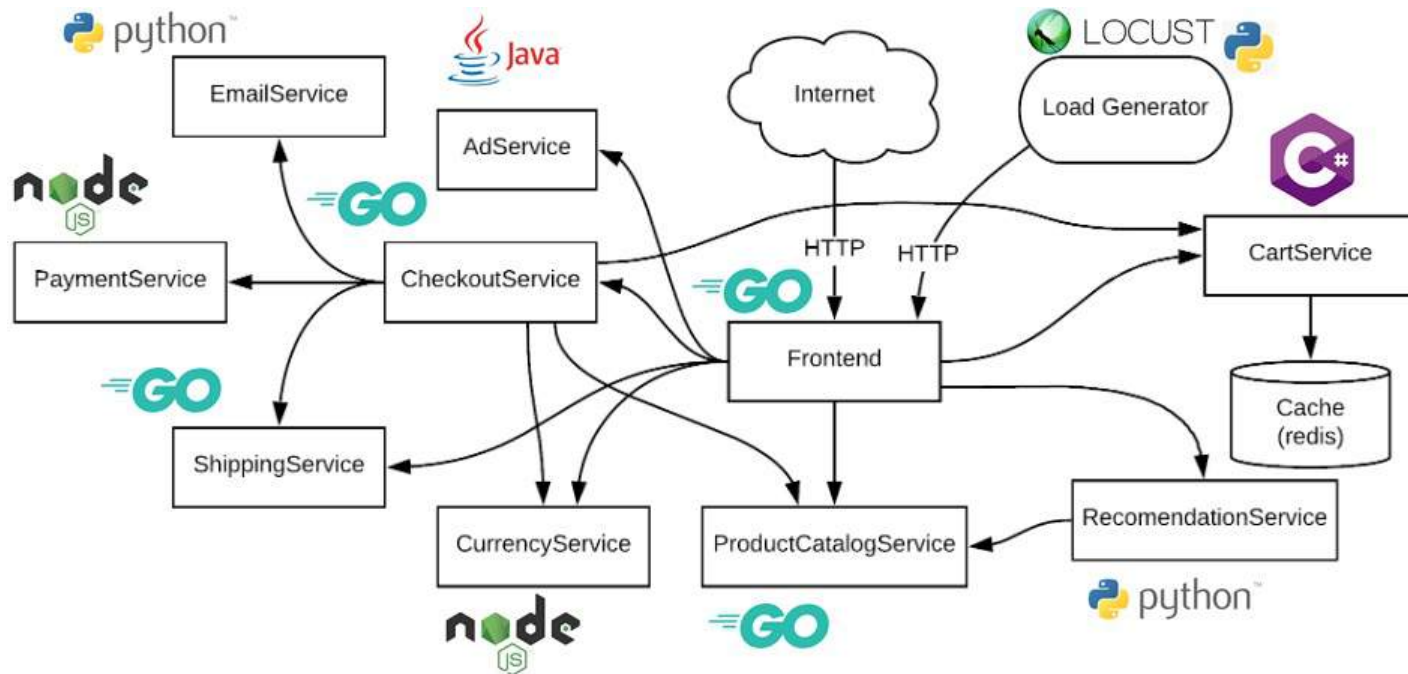
**Tags**  
Only impact traffic to hosts running Gremlin clients associated with these tags

Host Tags

HIDE ADVANCED OPTIONS

**Protocol**  
Impact traffic only for this protocol  
Default is all protocols

# Hipster Shop Anatomy (Online Boutique)



<https://github.com/GoogleCloudPlatform/microservices-demo>

감사합니다.