

WATCHA와 함께 하는

슬기로운
DevSecOps 생활



DATADOG

Speakers



정영석 부장

세일즈 엔지니어
DATADOG



김재훈

인프라 클라우드팀 팀장
WATCHA



이승규

커머셜 세일즈 리드
DATADOG



김동현

보안 엔지니어
WATCHA

VISION & MISSION

다양한 사람과 다양한 콘텐츠를 연결하여 세상을 더 다양하게

개인화 기술과 데이터를 이용해
다양한 취향의 사람들이
다양한 관점의 콘텐츠를 발견하고 소비할 수 있도록 연결한다

SERVICE

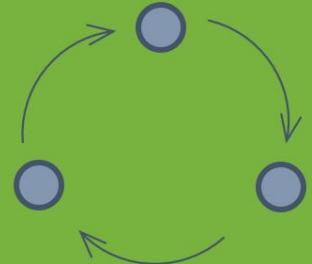


왓챠피디아
콘텐츠 평가 / 추천 서비스



왓챠
온라인 동영상 스트리밍 서비스

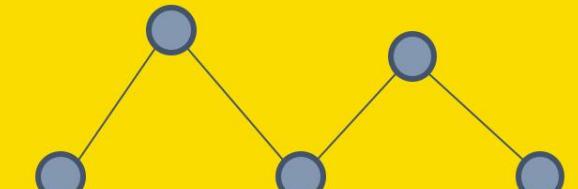
CI/CD



DevOps



Cloud
Native

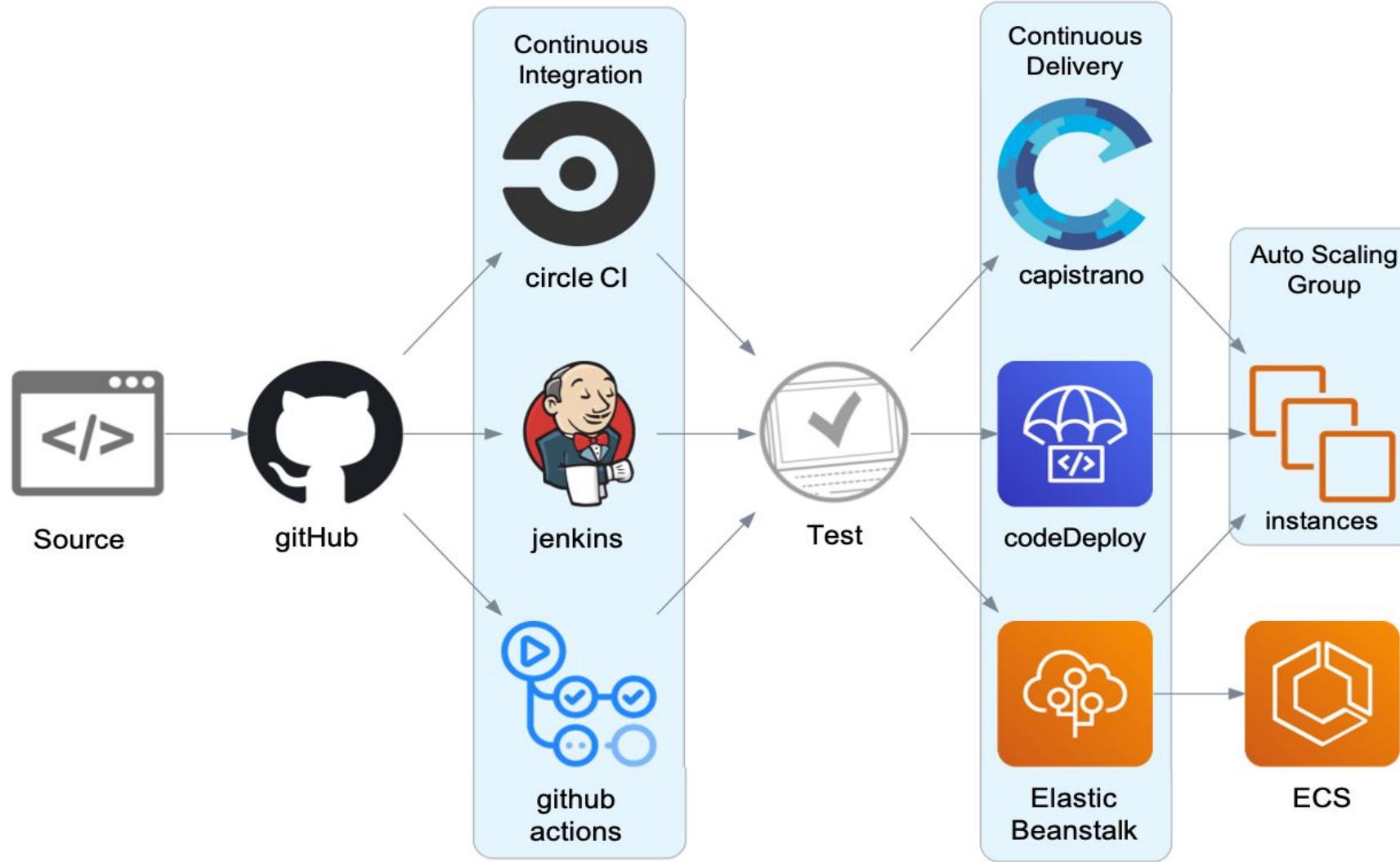


Microservices

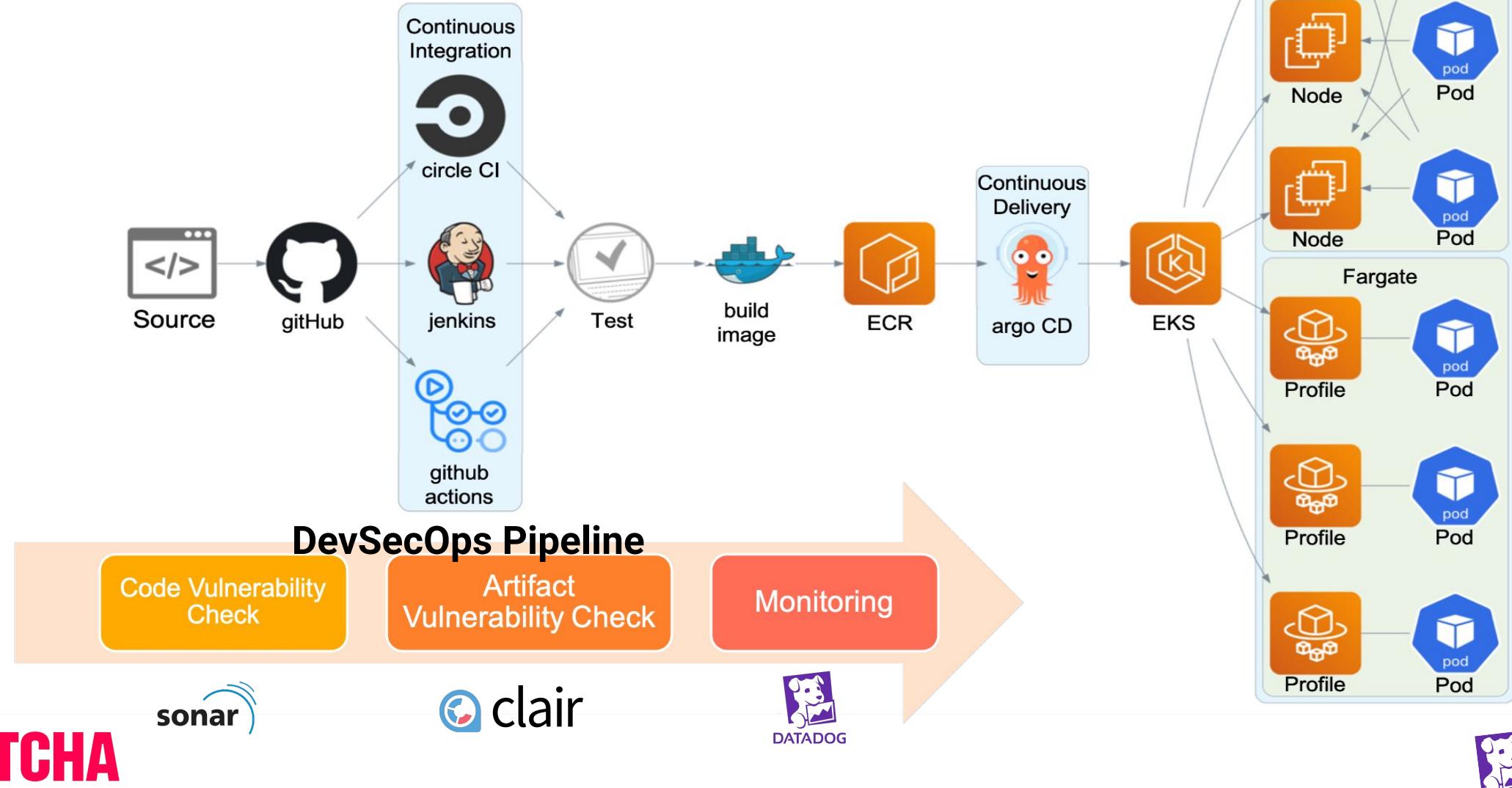


Containers

Before DevSecOps



After DevSecOps





Services

Traces

Profiles

+ New Service

Service Map 54 Services

1h Past 1 Hour



List



Search services

env:prod



Web



DB



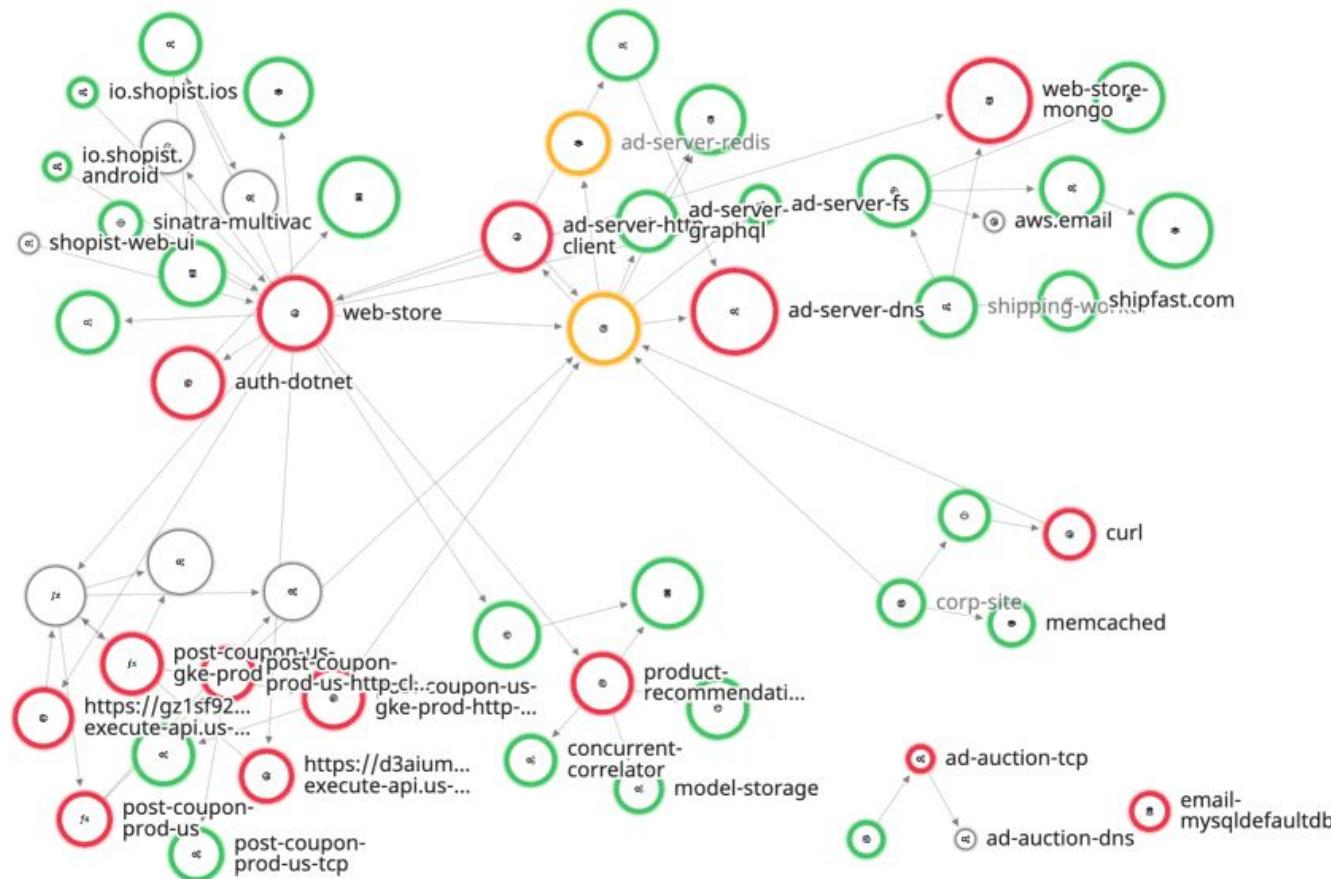
Cache



Function



Custom



Node Size | Requests (req/s)



Min < 0.01

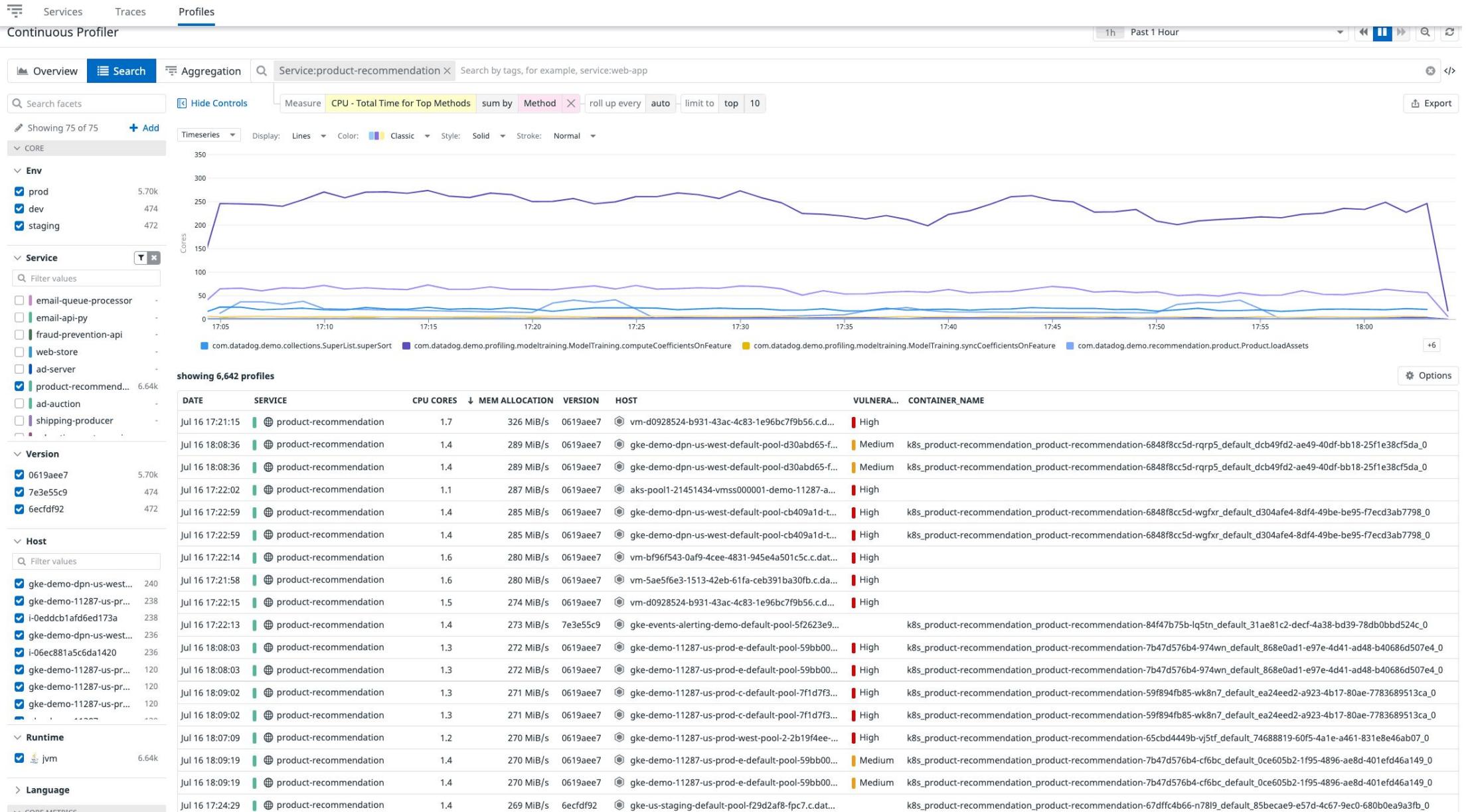


Max 2.48k



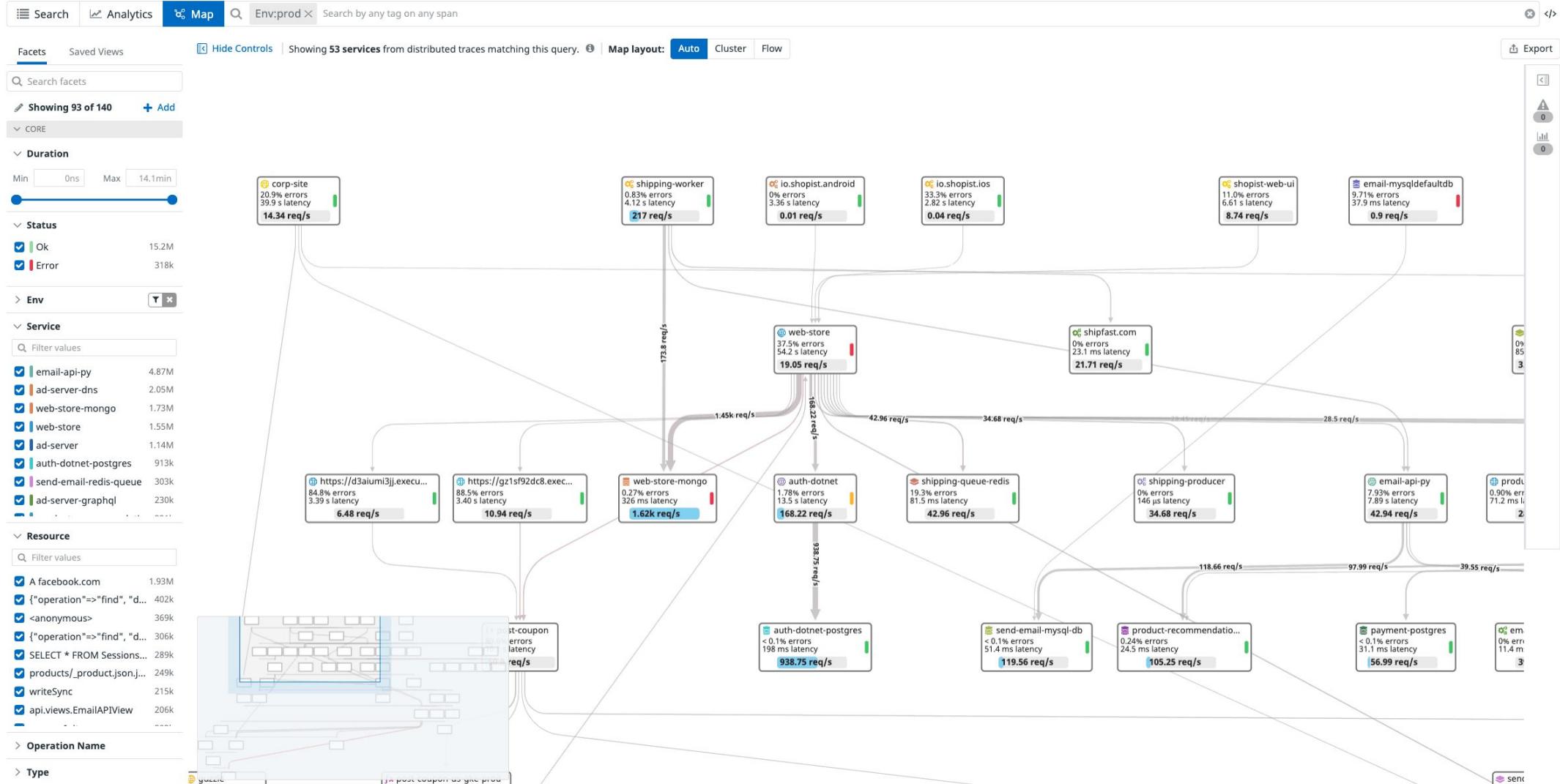
WATCHA DATADOG

WATCHA

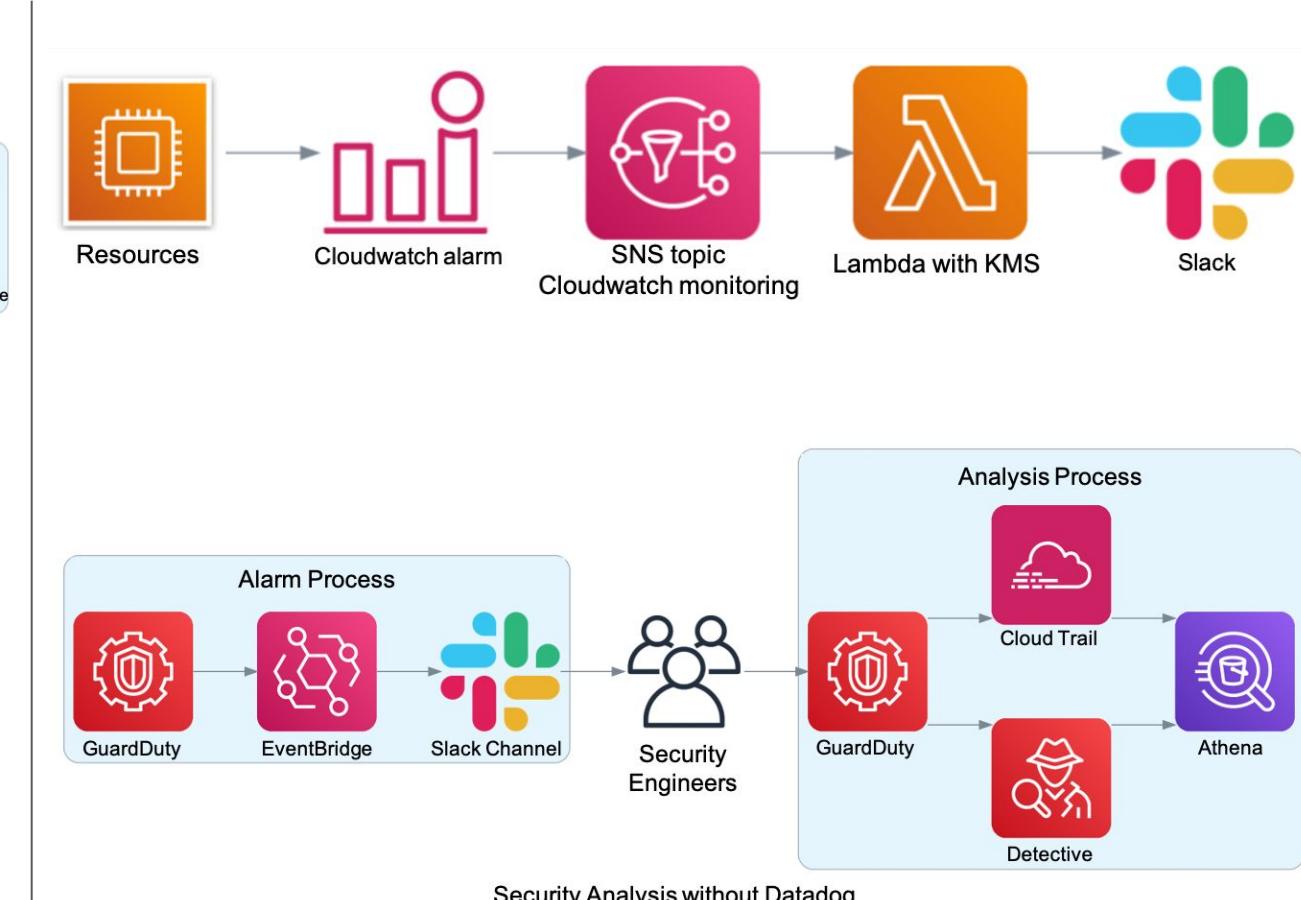
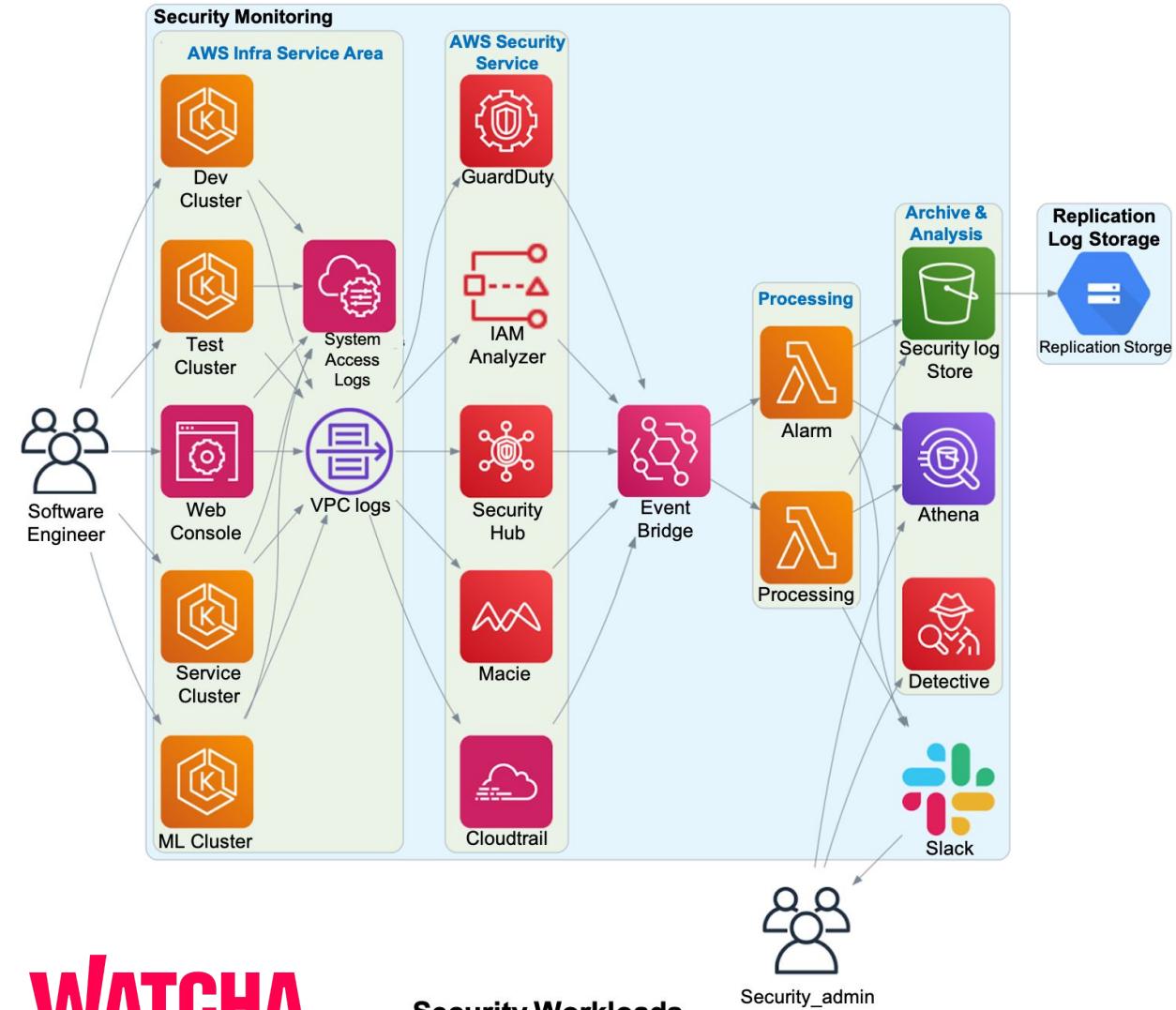


WATCHA


DATADOG



Security 분석 아키텍쳐 before Datadog



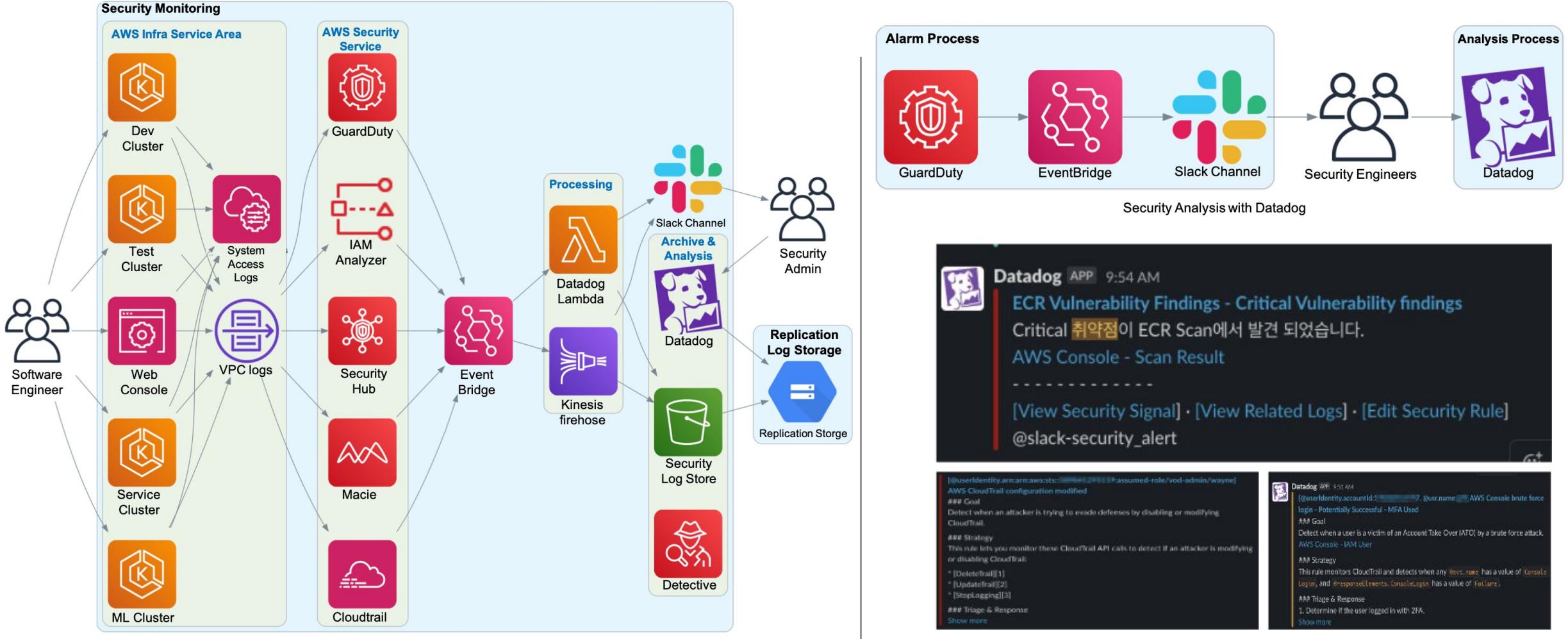
WATCHA

Security Workloads

Security_admin

 **DATADOG**

Security 분석 아키텍쳐 after Datadog



WATCHA

DATADOG

Datadog Security Signal

The screenshot shows the Datadog Security Signals interface. At the top, there are tabs for Views, Security Signals (selected), Save, Explore, and Dashboard. Below the tabs is a search bar with filters: Security:attack and Source:(2 terms). A timeline chart shows event counts from Mon 19 to 09:00, with a peak around 03:00.

Event Details:

HIGH Jul 19, 2021 at 23:08:42.998 (38 minutes ago)

AWS RDS Cluster deleted

attack > TA0040-impact > T1485-data-destruction

First seen: Jul 19, 2021 at 23:08:43.000 | Last seen: Jul 19, 2021 at 23:08:43.000 | Triggered on: 1 log

Type: Log Detection | **Source:** cloudtrail

User ARN: arn:aws:iam::172597598159:use... | **Client IP:** 231.240.191.220 | **Event Name:** DeleteDBCluster

User ID: Bruce.Brown | **User Name:** Bruce.Brown

All Tags: account:172597598159 demo:true purpose:sec-demo scope:rds

Message: Event Attributes Samples (1) Related Issues (4)

Goal:
Detect when an attacker is destroying a RDS Cluster.

Strategy:
This rule lets you monitor this CloudTrail API call to detect if an attacker is deleting a RDS cluster:

- DeleteDBCluster

Triage & Response:

1. Determine which user in your organization owns the API key that made this API call.
2. Contact the user to see if they intended to make this API call.
3. If the user did not make the API call:
 - Rotate the credentials.
 - Investigate if the same credentials made other unauthorized API calls.

Cloud Security Posture Management

Posture Management Home Findings

Security posture score

85%
of all weighted findings passed [?](#)

-0.10% vs. 30 days ago

[Explore all resources](#)

Posture score per account

473437055159 (160 resources)	79%	-8% ↘
291fba3f-e0a5-47bc-a299-3bdbab2a50a05 (153	90%	
363525035937 (134 resources)	88%	+3% ↗
363525035921 (14 resources)	83%	-3% ↘

[Manage accounts](#)

Top 5 high-severity rule failures

6,413	PIDs cgroup limit is used
376	Host's network namespace is not shared
294	Docker socket is not mounted inside any containers
31	S3 bucket employs default encryption at-rest
30	CloudTrail multi-region is enabled

[Explore issues](#)

CIS - AWS

PASS	FAIL
5	6

[Explore rules](#)

Rules evaluation

PASS	FAIL
5	6

[Explore requirements](#)

Top 5 requirements by rule failures

Networking	0	4
Logging	2	1
Storage	1	1
IAM	1	0

Resource types with the most fail findings

aws_s3_bucket	31	31
aws_security_group	178	29
aws_network_acl	0	23
aws_vpc	23	5
aws_account	4	0

[Explore resource types](#)

CIS - Azure BETA

PASS	FAIL
0	26

[Explore rules](#)

Rules evaluation

PASS	FAIL
0	26

[Explore requirements](#)

Top 5 requirements by rule failures

Database-Services	0	16
Other-Security-Considerations	0	4
Networking	0	3
Security-Center	0	3

Resource types with the most fail findings

azure_postgresql_server_configuration	15	25
azure_sql_server_vulnerability_assessm...	65	25
azure_security_contact	75	15
azure_security_group	75	15
azure_sql_server_audit_setting	40	10

[Explore resource types](#)

CIS - Kubernetes BETA

PASS	FAIL
32	6

[Explore rules](#)

Rules evaluation

PASS	FAIL
32	6

[Explore requirements](#)

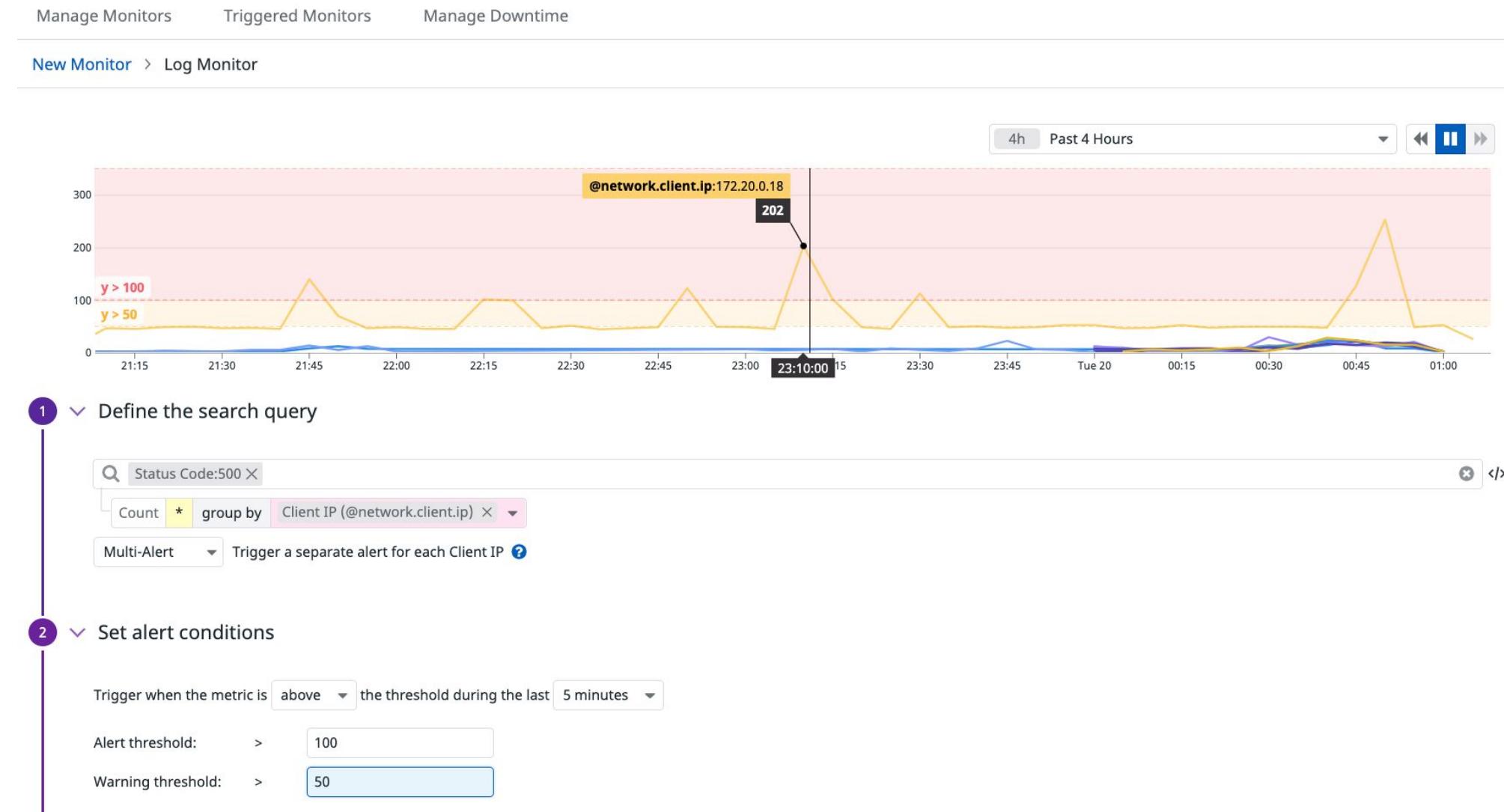
Top 5 requirements by rule failures

Kubelet	4	2
API-Server	12	1
General-Policies	1	0
Worker-Node-Configuration-Files	2	0
etcd	6	0

Resource types with the most fail findings

kubernetes_worker_node	334	368
kubernetesNode	167	8
kubernetesCluster	25	0

특정 Client에서 반복적으로 50X 알람 발생시 알람



IP Threat Intelligence

The screenshot displays the Watcha IP Threat Intelligence interface. On the left, a dashboard shows a bar chart of threat intelligence signals over time (03:00 to 09:00) and a list of rules. The rules include:

- User Logged in From IP on Threat Intelligence
- S3 Object Downloaded from an IP on a Threat Intel List
- Instance Resolved an IP on a Threat Intel List

The right side shows a detailed view of an event: "S3 Object Downloaded from an IP on a Threat Intel List" (Medium, Jul 20, 2021 at 00:00:26.307). The event details are:

- TYPE:** Log Detection
- SOURCE:** clouptrail
- HOST:** i-0cf8a64af62989629
- CLIENT IP:** ! 83.97.20.30
- EVENT NAME:** GetObject

A context menu is open over the client IP field, showing options like "Threat Intel BETA", "Flagged as: Scanner by GreyNoise", "Flagged as: Attack by FireHOL", "View logs with @network.client.ip:83.97.20.30", "Filter by @network.client.ip:83.97.20.30", "Exclude @network.client.ip:83.97.20.30", "Add column for @network.client.ip", "Never trigger signals for @network.client.ip:83.97.20.30", "Copy to clipboard", and "Explore in IP Investigation dashboard".

Datadog Cloud Security Platform

FULL-STACK SECURITY

APPLICATIONS



App Runtime Threat Monitoring



Application Protection

HOSTS & CONTAINER



File Integrity Monitoring & Configuration Audit



eBPF Based Workload Security

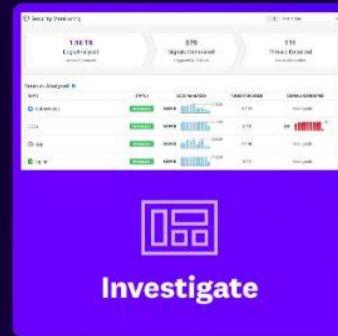
CLOUD AND ON-PREMISE



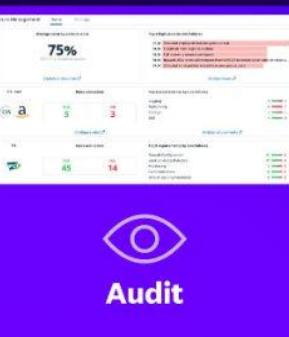
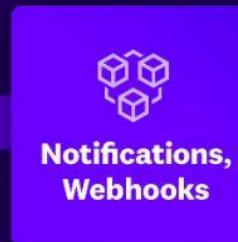
Endpoint, Network, IdP, Platform Logs



Continuous Configuration Audit



Investigate



BROAD-BASED OBSERVABILITY

TRACES

LOGS

CONFIGURATION AUDIT

WORKLOAD EVENTS

450+ OOTB Integrations

Normalization & Enrichment

Stream-Based Rules Engine

Logging without Limits™

Threat Intel Customer Context

Sub-second Threat Detection
OOTB & Custom Rules

MITRE
ATT&CK™

CIS Benchmarks™

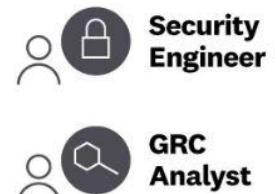


DevOps



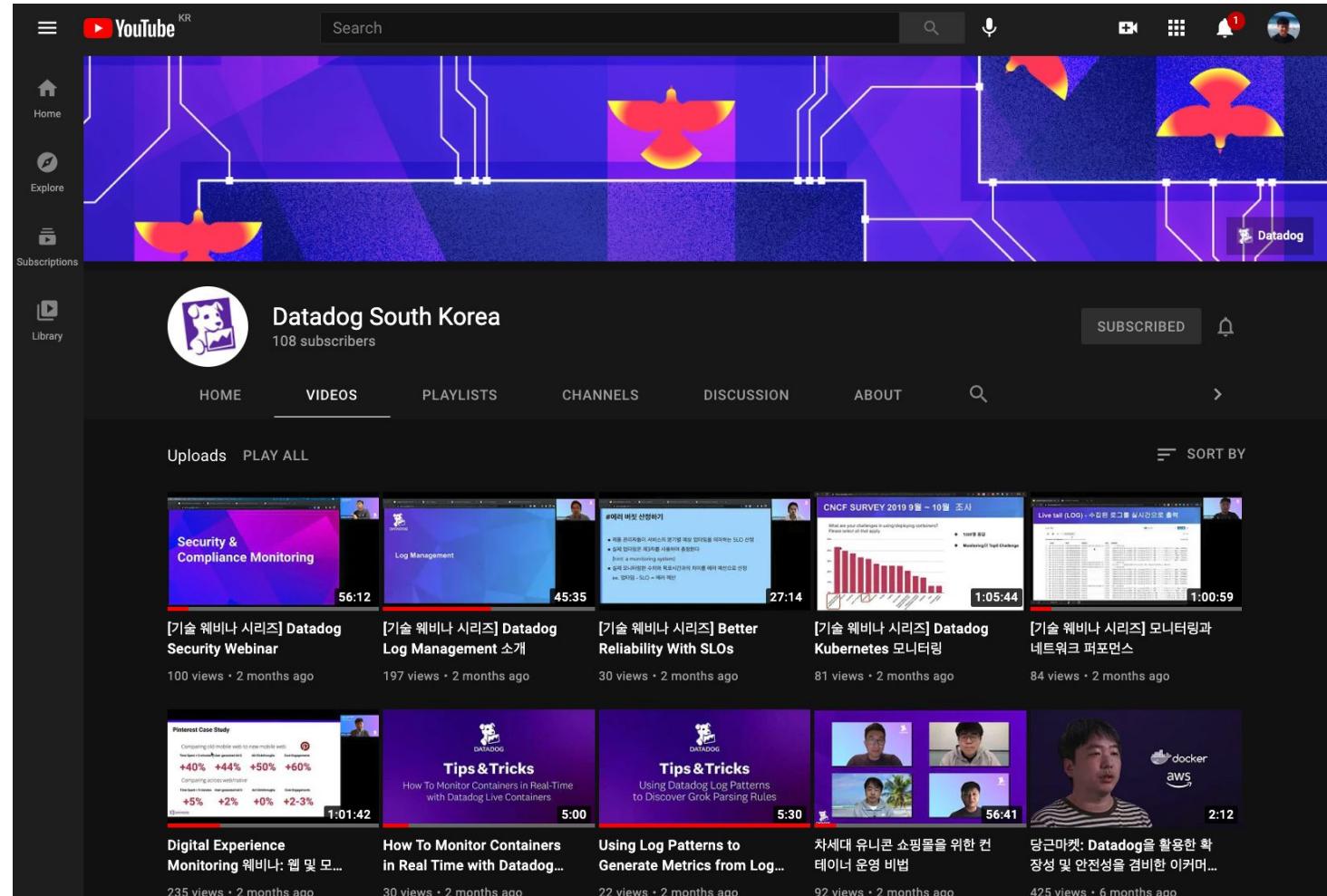
SHARED GOALS

Security



Youtube에 Datadog South Korea 채널을 오픈하였습니다!

- 국내 고객 사례 영상
- 기술 웨비나 영상 (한국어)
- Datadog Tips & Tricks



W
함께 해피[주식회사](#)
감사합니다!

