DemoGo Prime Day

보안 위협 탐지 및 모니터링을 위한 SIEM 구성해보기

DemoGo Prime Team

Kyungshik Shin / Myeongsu Jeon / Yongho Choi / Munkyu Seong

Solutions Architect

AWS

Agenda

- 클라우드에서의 보안 Overview
- SIEM 알아보고 구축해보기
- 보안 로그 통합 및 파이프라인 구축
- 위협 탐지를 위한 대시보드 및 알람 구성
- Summary

클라우드 보안 Overview

온프레미스 보안 vs. 클라우드 보안

온프레미스 보안

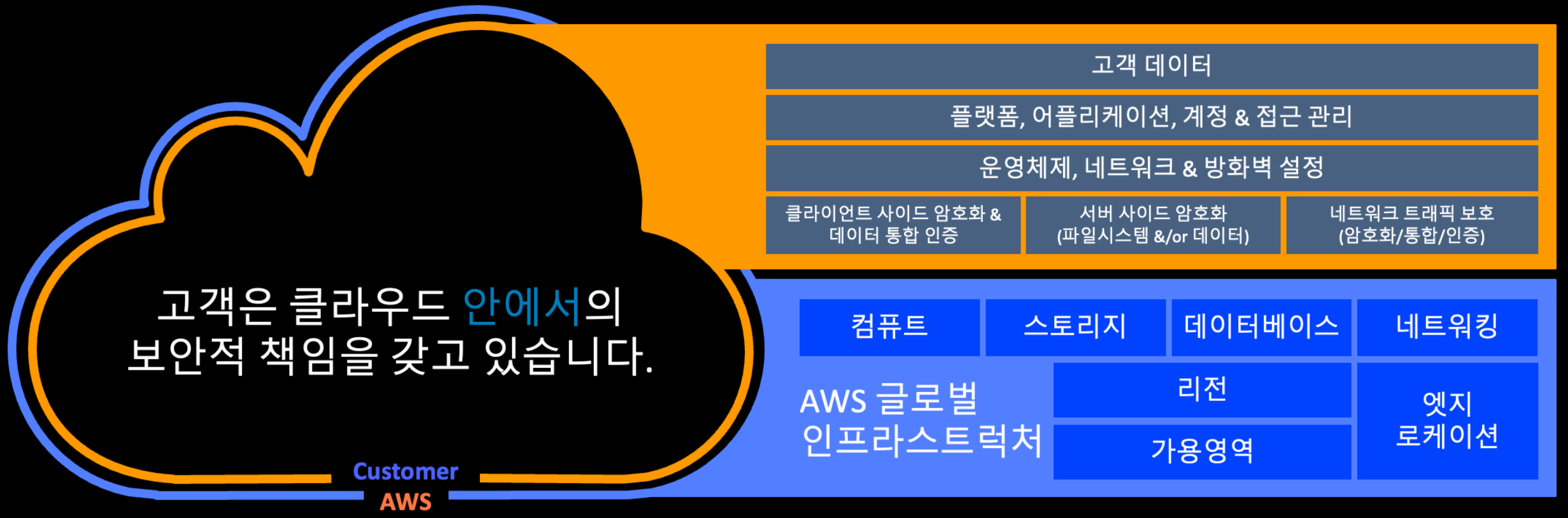
- 성벽형 보안 모델
  - 방화벽을 통한 방어
- 경계 방어 형태
- 단순한 보안 인프라 구성
- 경계 내부에서의 접근은 안전하다고 판단
- 3rd party 솔루션 의존

온프레미스 보안 vs. 클라우드 보안

클라우드 보안

- 인증 및 권한 제어 형태
- 내부/외부 상관없이 철저한 인증 절차 필요
  - 제로 트러스트 보안 모델
  - 최소 권한 부여 원칙
- 필요다양한 AWS 보안 서비스 라인업
- 모든 이벤트 추적 가능하도록 가시성 확보
- 책임 공유 모델

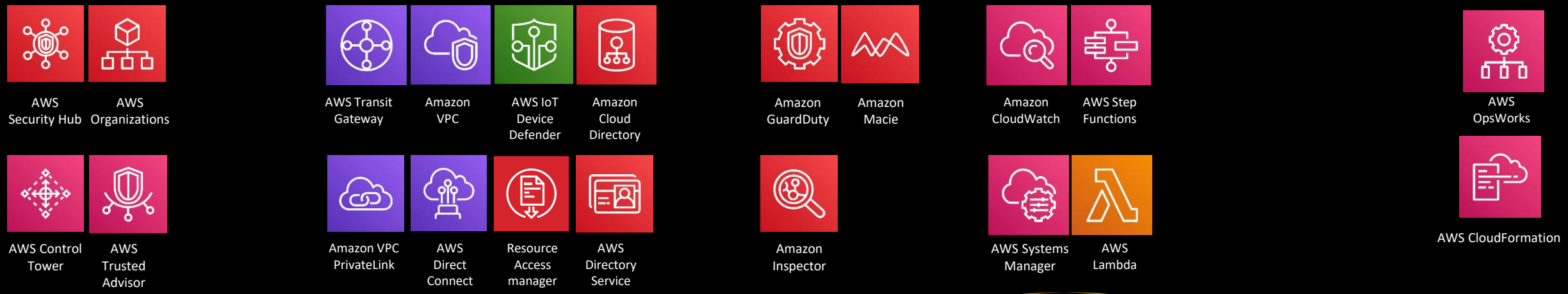
보안 책임 공유 모델



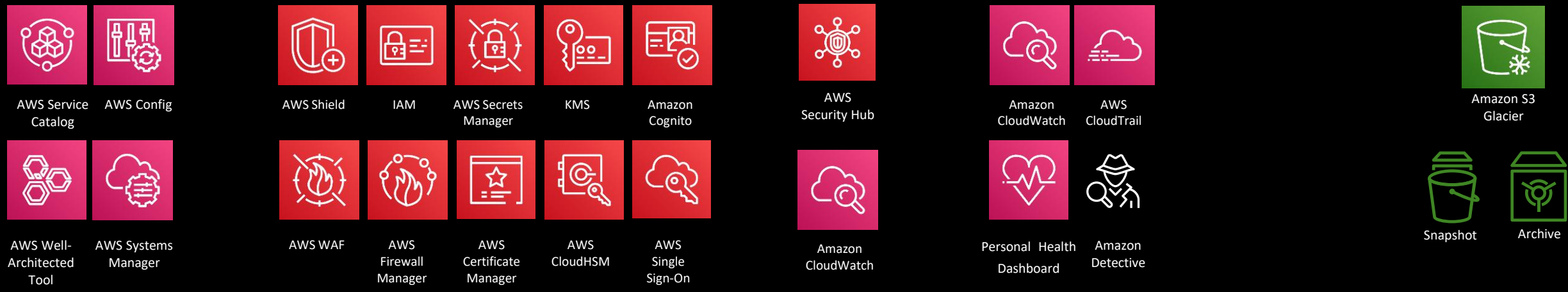
보안 모범 사례 영역

- 클라우드 보안 이해
- 계정 및 접근 권한 관리
- 탐지
- 인프라 보호
- 데이터 보호
- 인시던트 대응

AWS 보안 서비스 라인업



식별 → 보호 → 탐지 ⇄ 자동화 / 분석 → 대응 → 복구



aws

나의 워크로드에 적합한 **AWS** 보안 서비스만 구성하고 활성화하면 되는가?

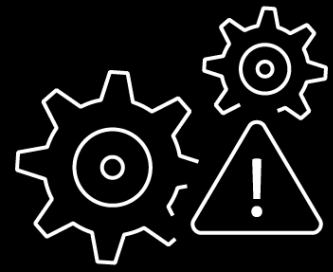
+@가 필요하다

중앙 집중화된 통합 모니터링 구성이 필요하다.

보안 로그 통합

로그 분석

현황 대시보드

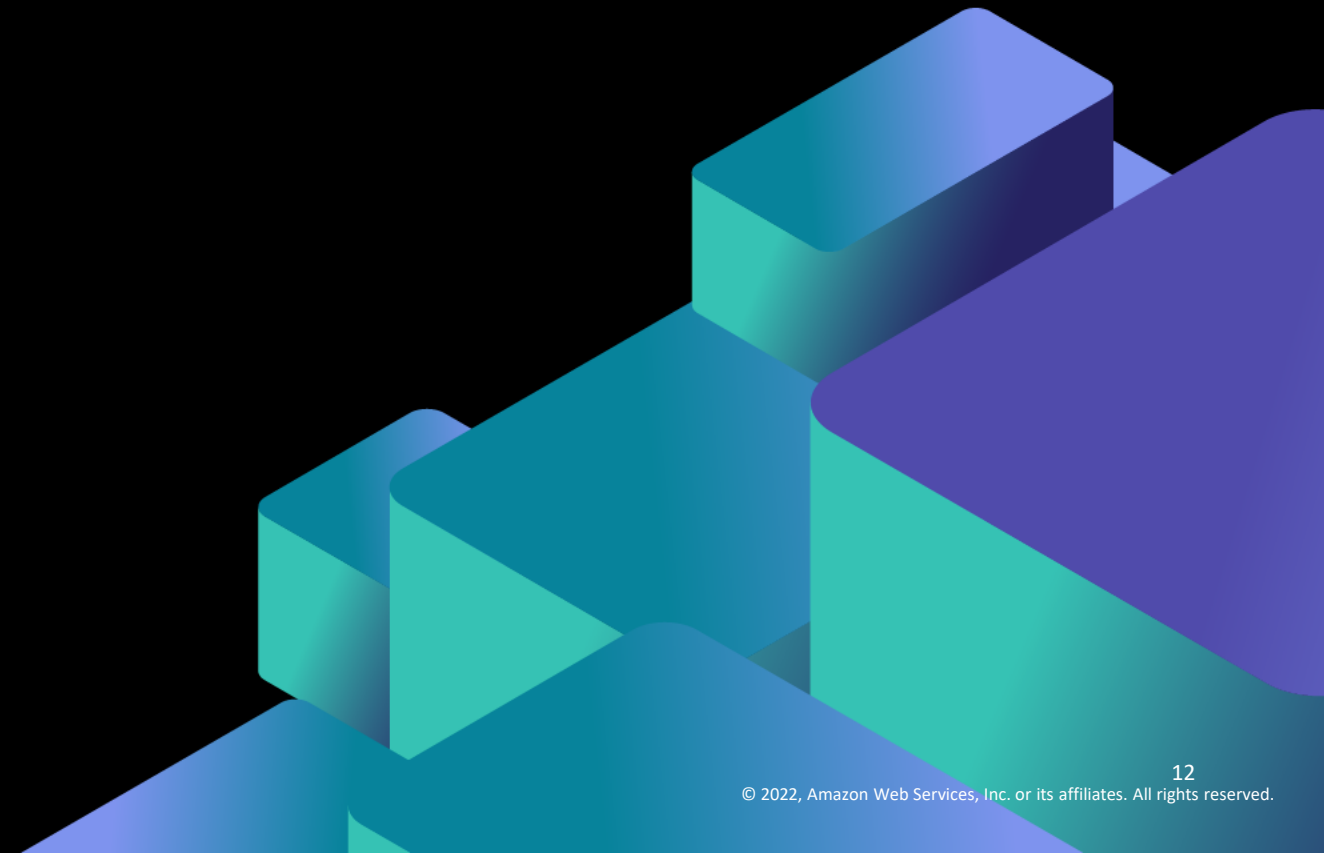


경보 알람

SIEM을 구축하자

SIEM 알아보고 구축해보기

SIEM이란?



SIEM이란?

SIM

Security Information Management

- 수집된 로그 데이터 분석
- 리포트 생성
- 규정준수 여부 확인

SEM

Security Event Management

- 실시간 보안 이벤트 탐지
- 모니터링, 분석, 알람

SIEM이란?

SIM

Security Information Management

- 수집된 로그 데이터 분석
- 리포트 생성
- 규정준수 여부 확인

SEM

Security Event Management

- 실시간 보안 이벤트 탐지
- 모니터링, 분석, 알람

SIEM이란?

SIM

Security Information Management

- 수집된 로그 데이터 분석
- 리포트 생성
- 규정준수 여부 확인

SIEM

Security Information and Event Management

- 중앙 집중형 솔루션
- 로그 수집, 상관관계 분석
- 다양한 소스로부터 수집
- SIM + SEM

SEM

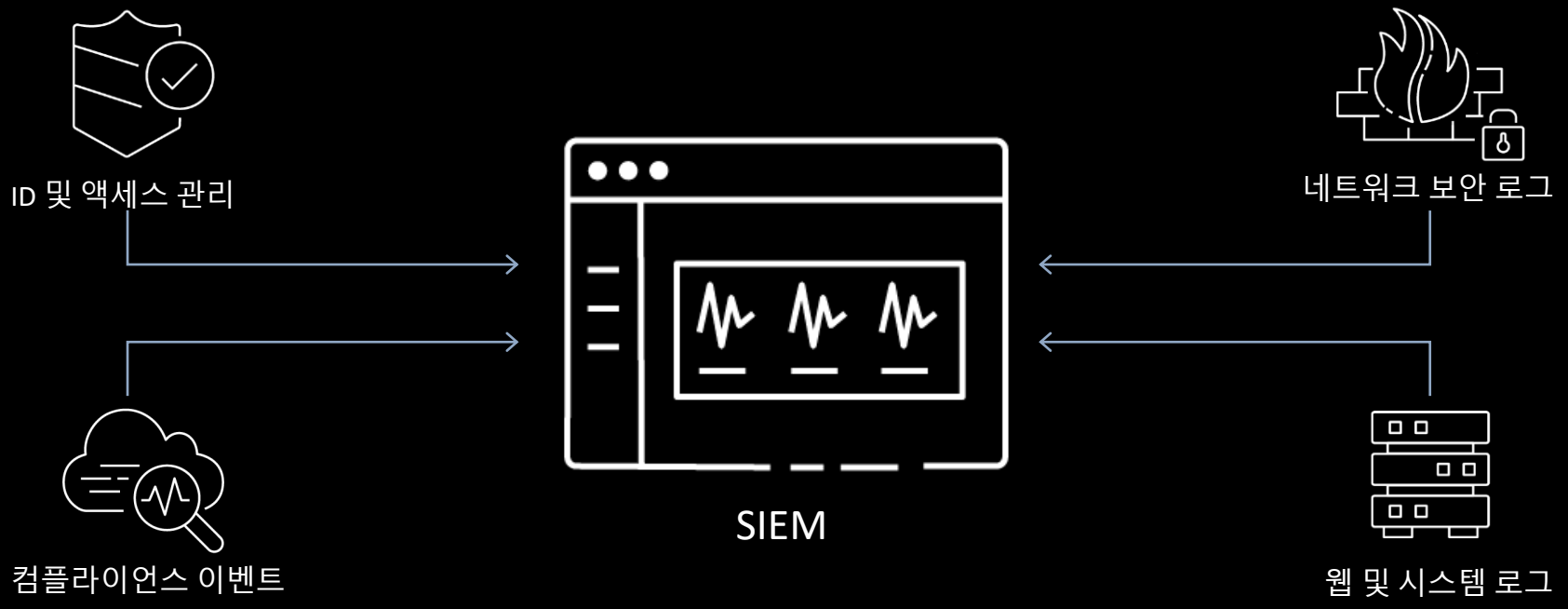
Security Event Management

- 실시간 보안 이벤트 탐지
- 모니터링, 분석, 알람

SIEM이란?

- **S**ecurity **I**nformation and **E**vent **M**anagement

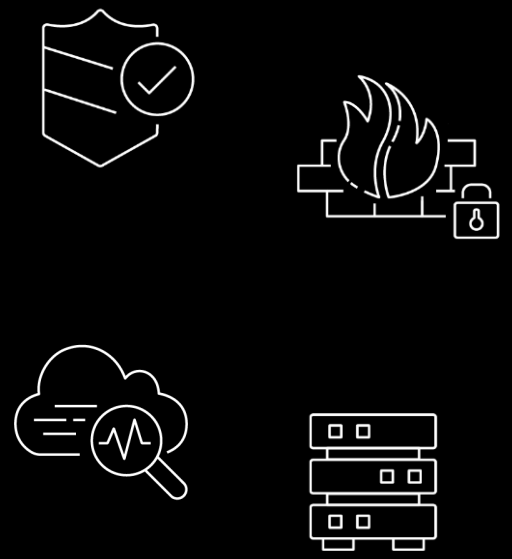
  : 계정 보안, 네트워크 보안, 애플리케이션 보안 등 다양한 보안 시스템 전체에서 발생하는 로그와 이벤트를 수집하여 **보안 현황을 모니터링하고 탐지된 이상징후를 알려주는 솔루션**



대표적인 SIEM 솔루션

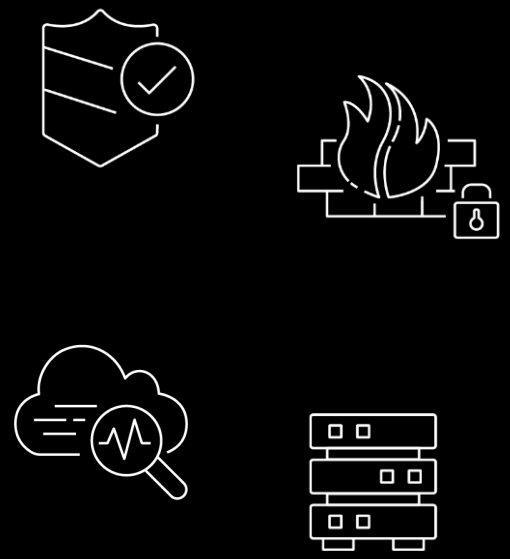
https://www.gartner.com/reviews/market/security-information-event-management

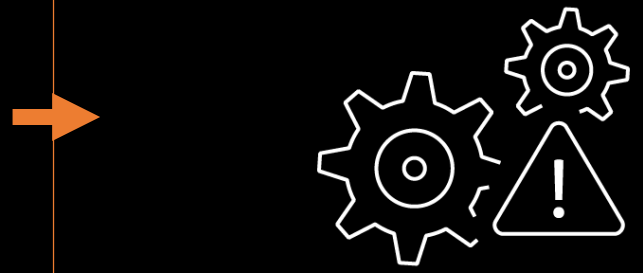
SIEM 구조



- 모든 데이터 수집

SIEM 구조

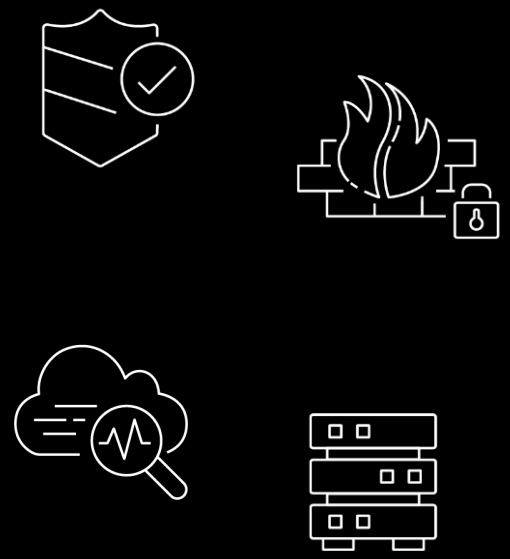


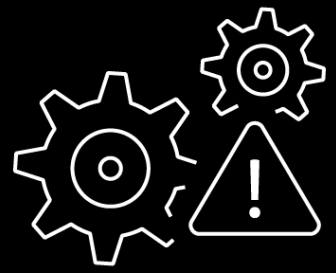


- 모든 데이터 수집

SIEM에서 통합 분석

SIEM 구조





- 모든 데이터 수집

SIEM에서 통합 분석

Dashboard, Alarm, Monitoring

SIEM 구조


AWS WAF


AWS CloudTrail


Amazon GuardDuty


AWS Shield


3rd party Solution


Amazon Macie


Amazon Detective


Amazon OpenSearch Service


AWS Network Firewall


Amazon VPC

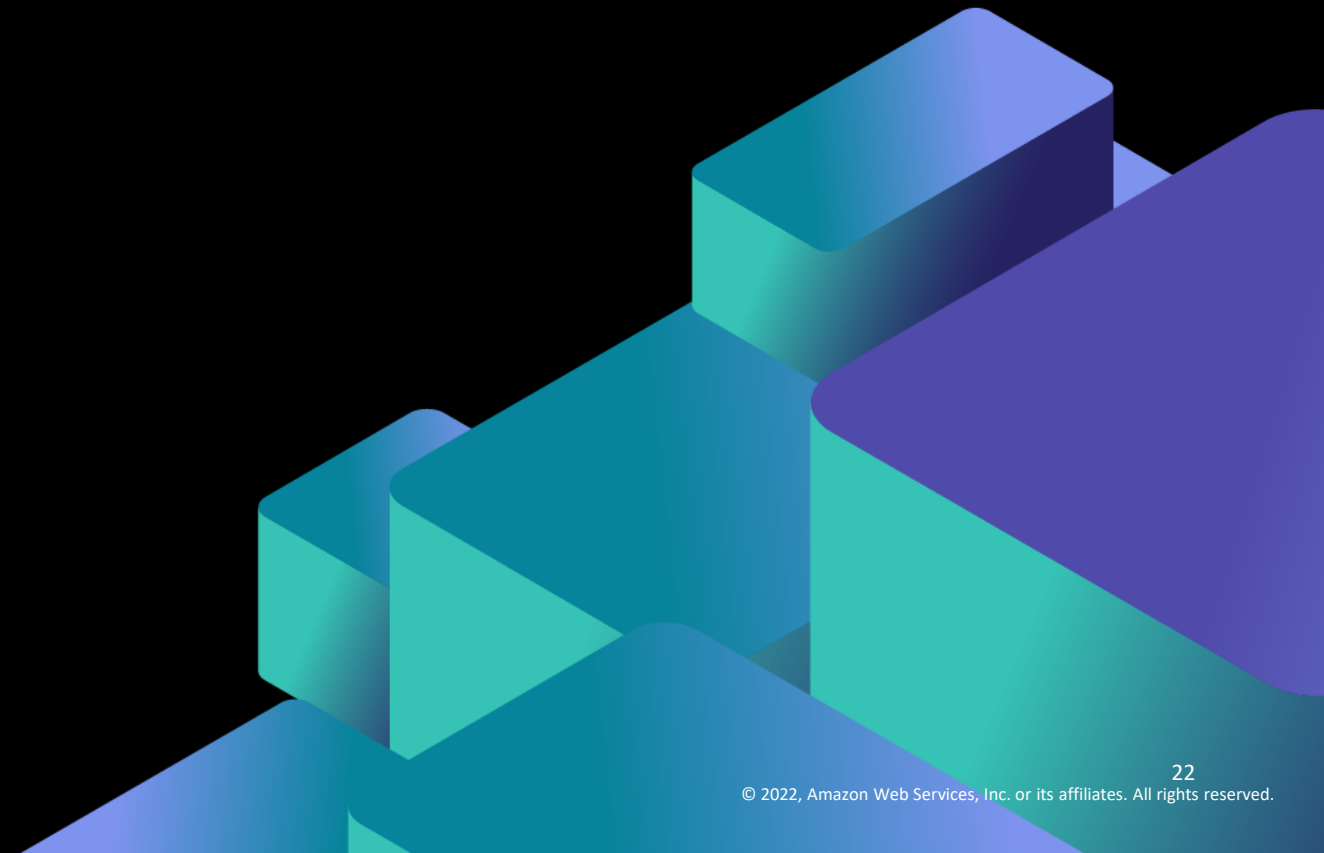

AWS Security Hub

- 모든 데이터 수집

SIEM에서 통합 분석

Dashboard, Alarm, Monitoring

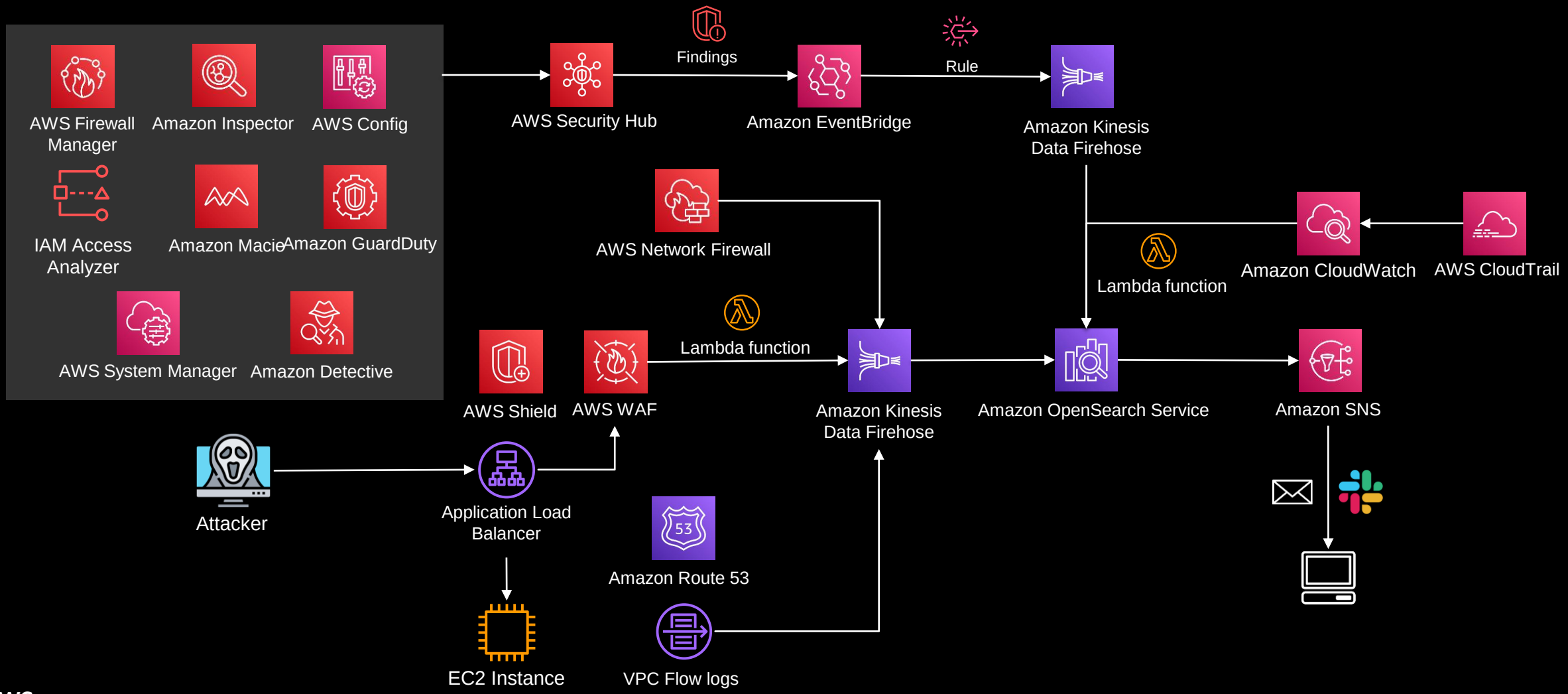
SIEM on AWS



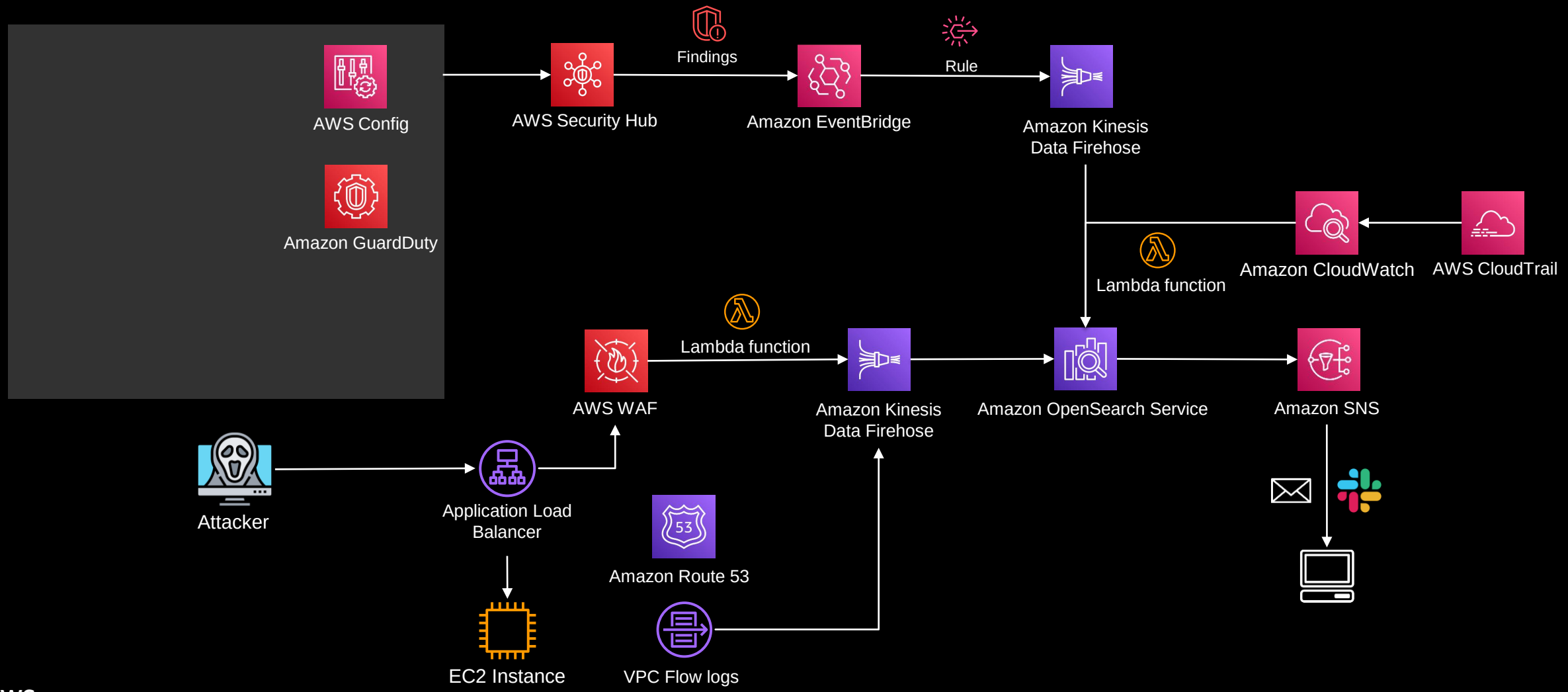
SIEM on AWS의 장점

- ✓ Amazon S3 스토리지로의 데이터 중앙집중화
- ✓ 다양한 3rd-party 솔루션 연동 가능
- ✓ AWS 서비스 연동 용이
- ✓ 손쉬운 Dashboard 솔루션 교체
- ✓ Pay-as-you-go 모델로 인한 비용 효율성
- ✓ CloudFormation을 이용한 손쉬운 구축

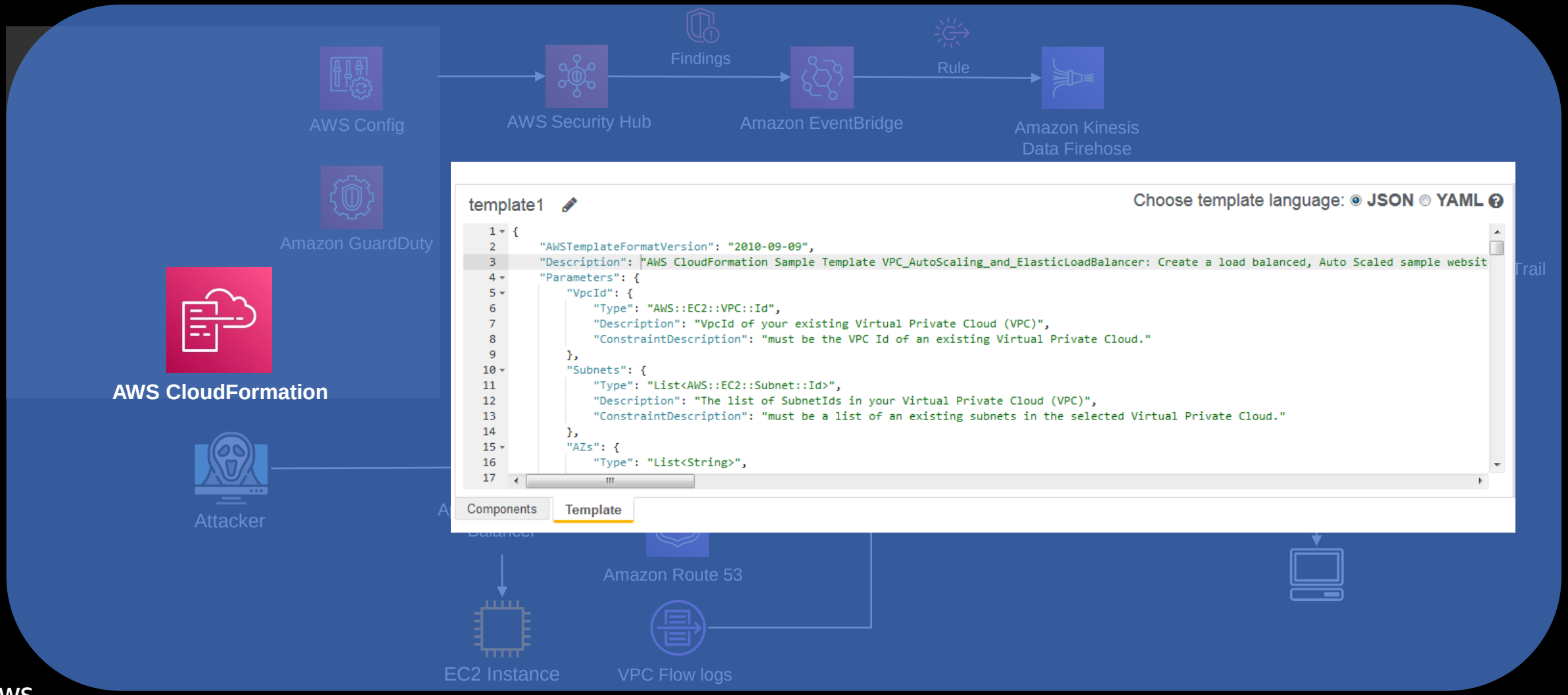
SIEM on AWS



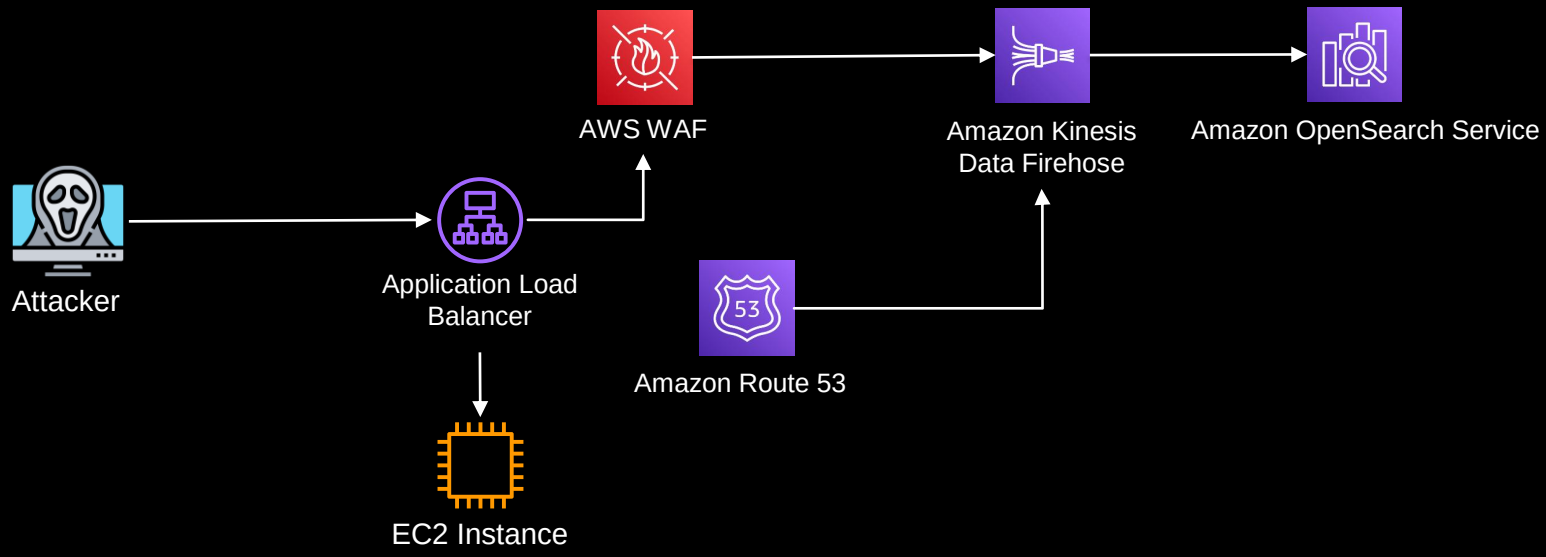
SIEM on AWS



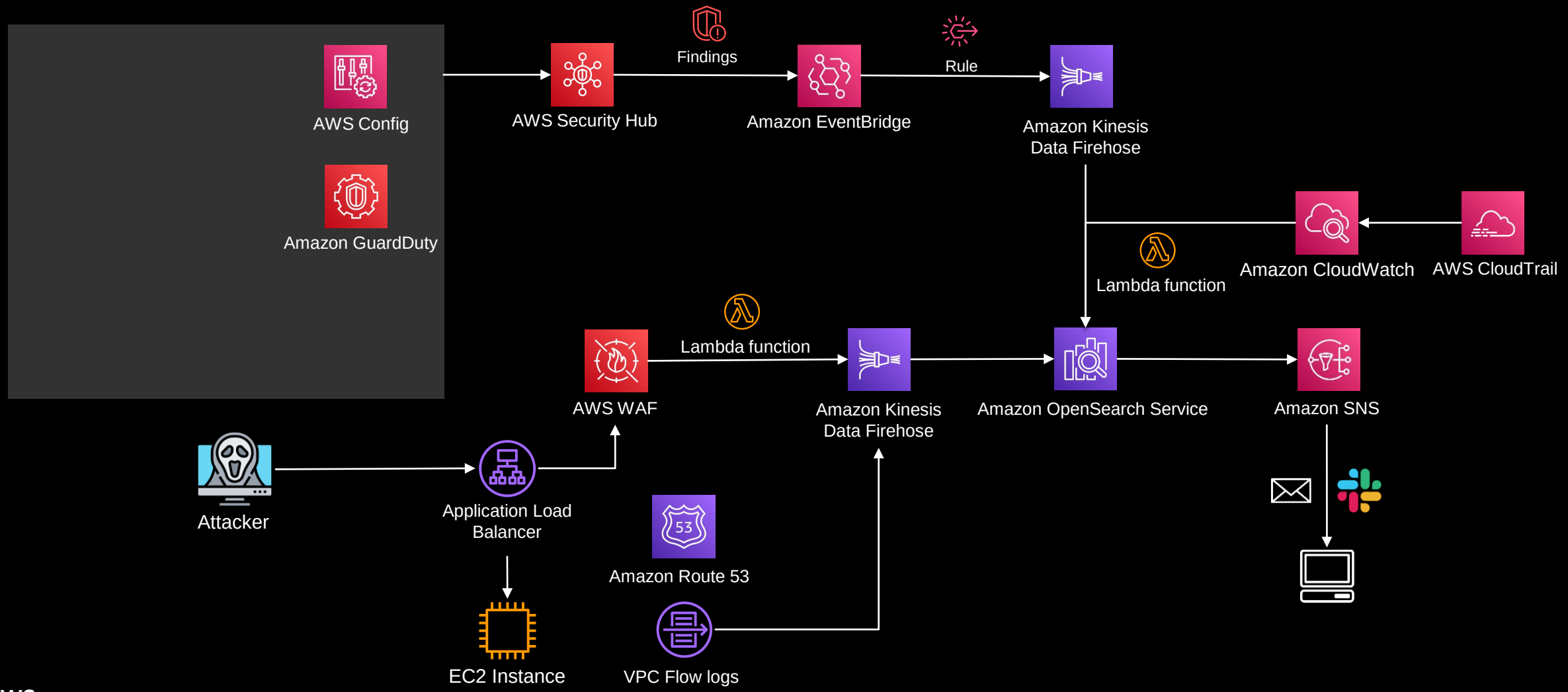
SIEM on AWS



SIEM on AWS



SIEM on AWS



보안 로그 통합 및 파이프라인 구축

Data Pipeline Architecture

Data Pipeline Architecture

Data


EC2


ECS

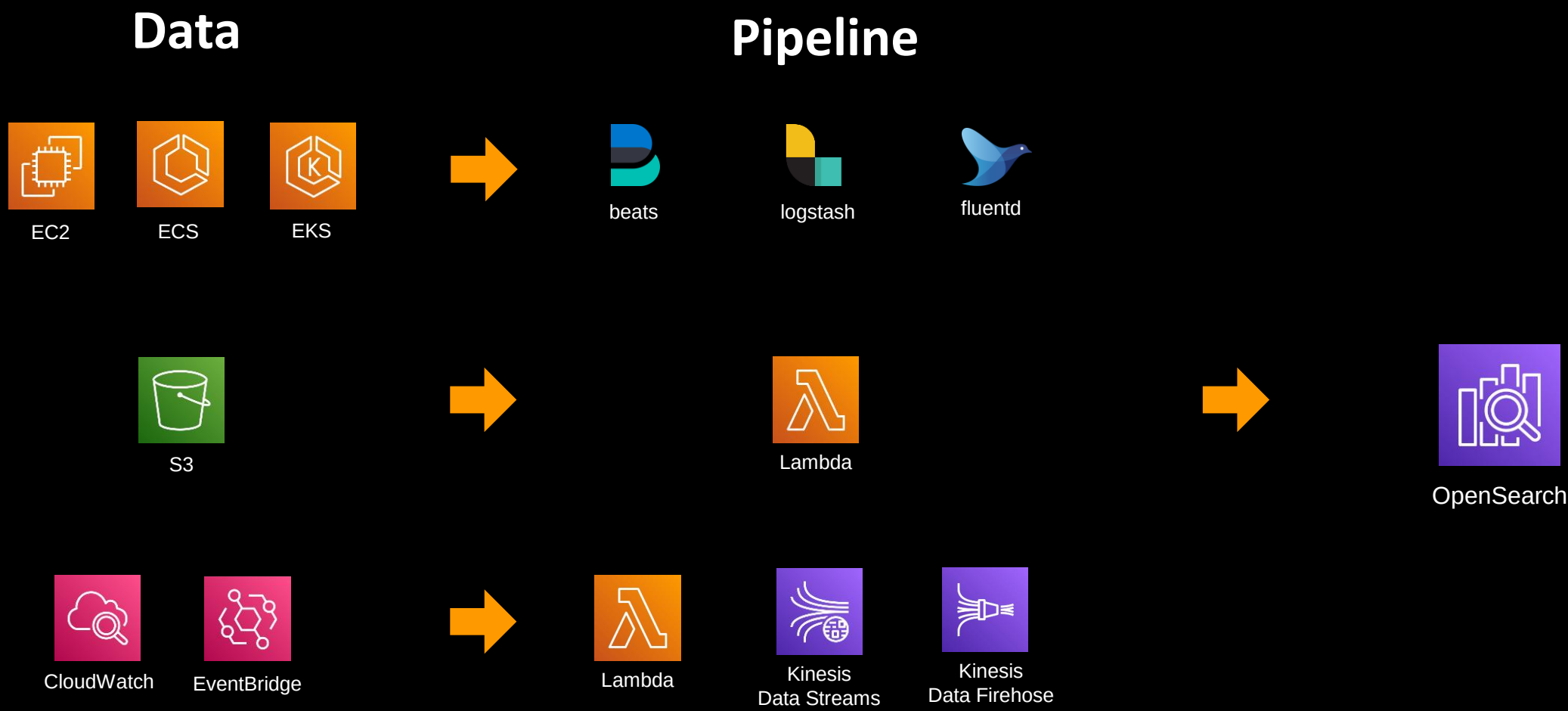

EKS


S3

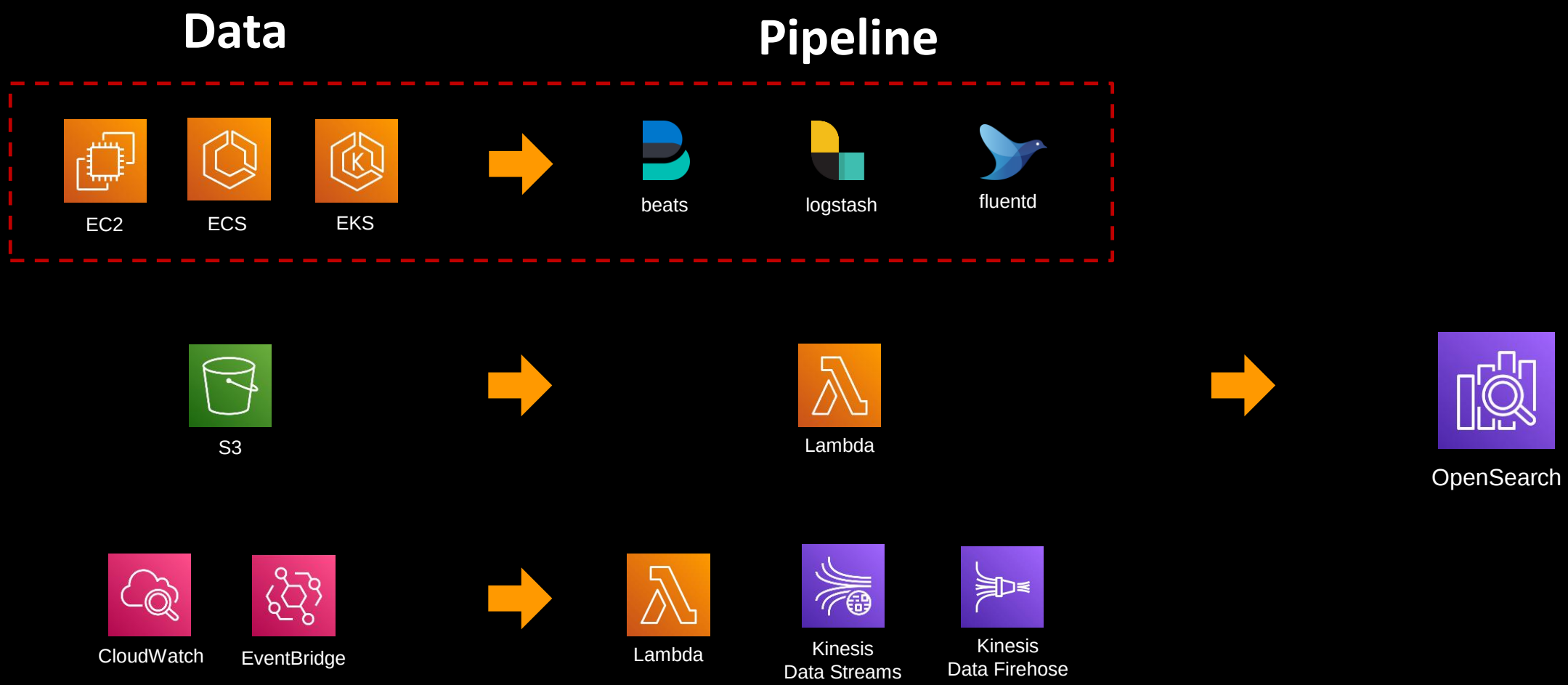

CloudWatch


EventBridge

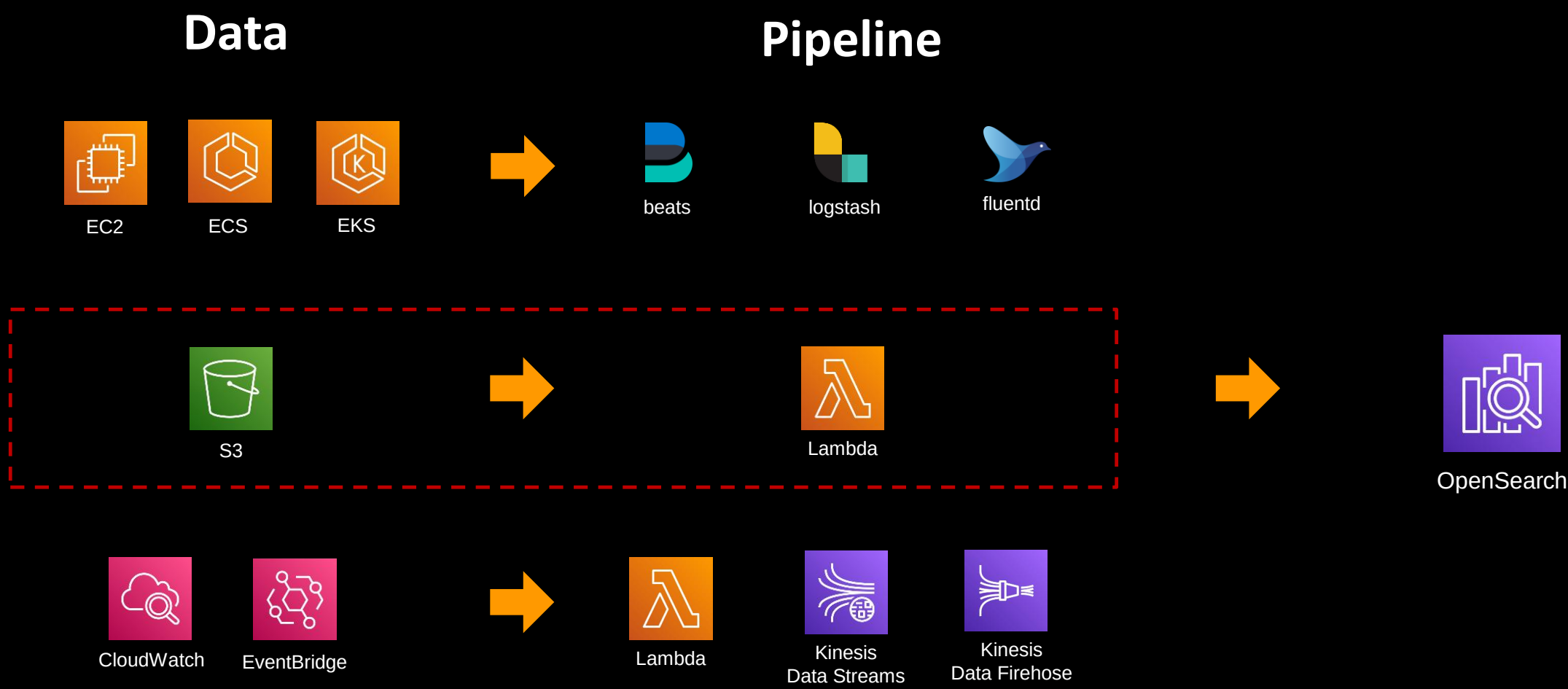
Data Pipeline Architecture



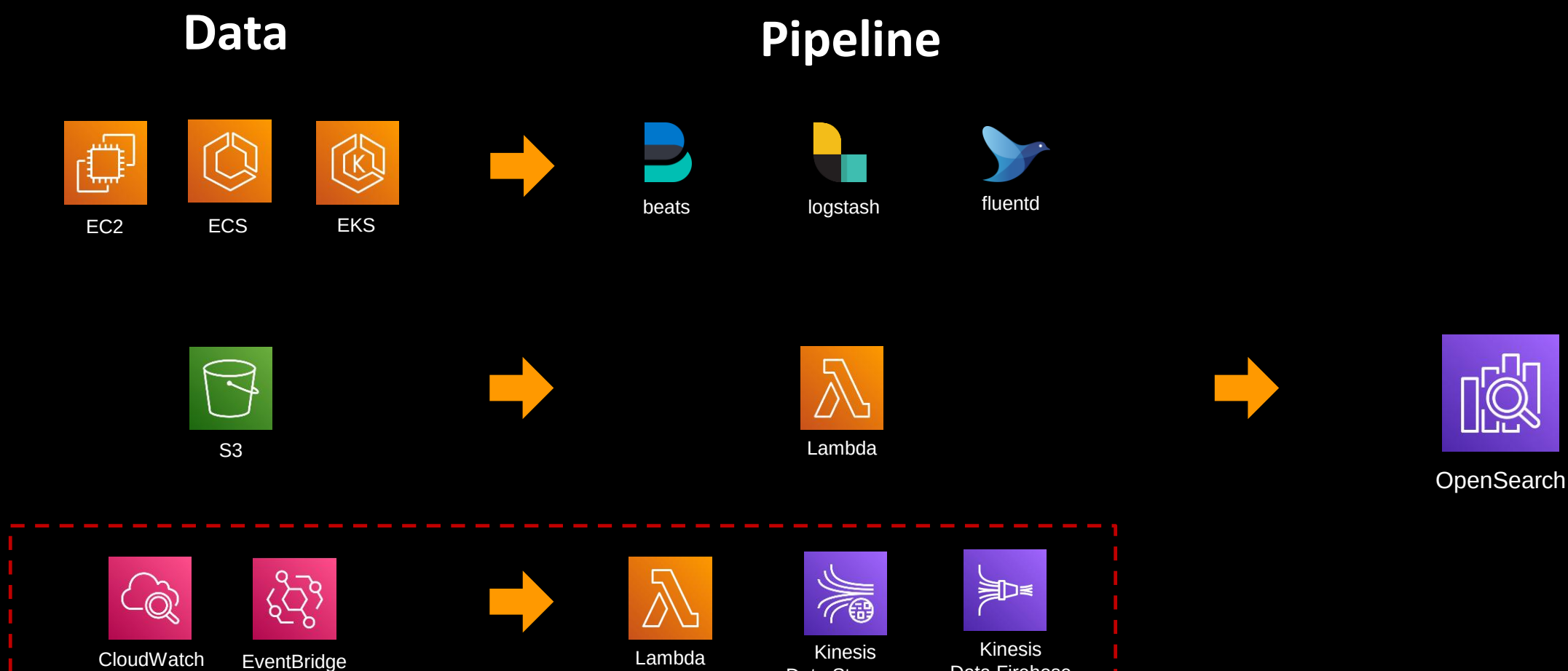
Data Pipeline Architecture



Data Pipeline Architecture



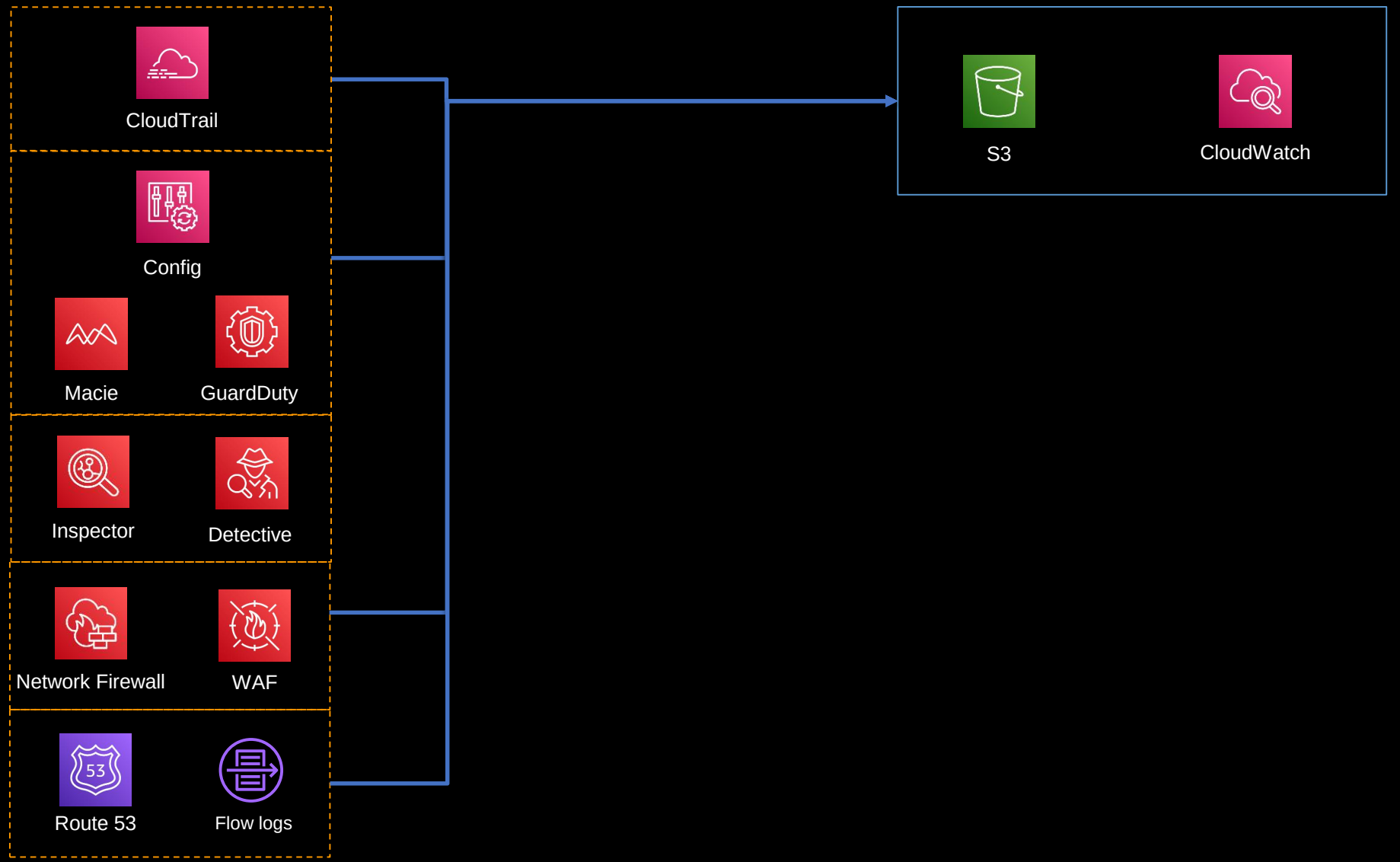
Data Pipeline Architecture



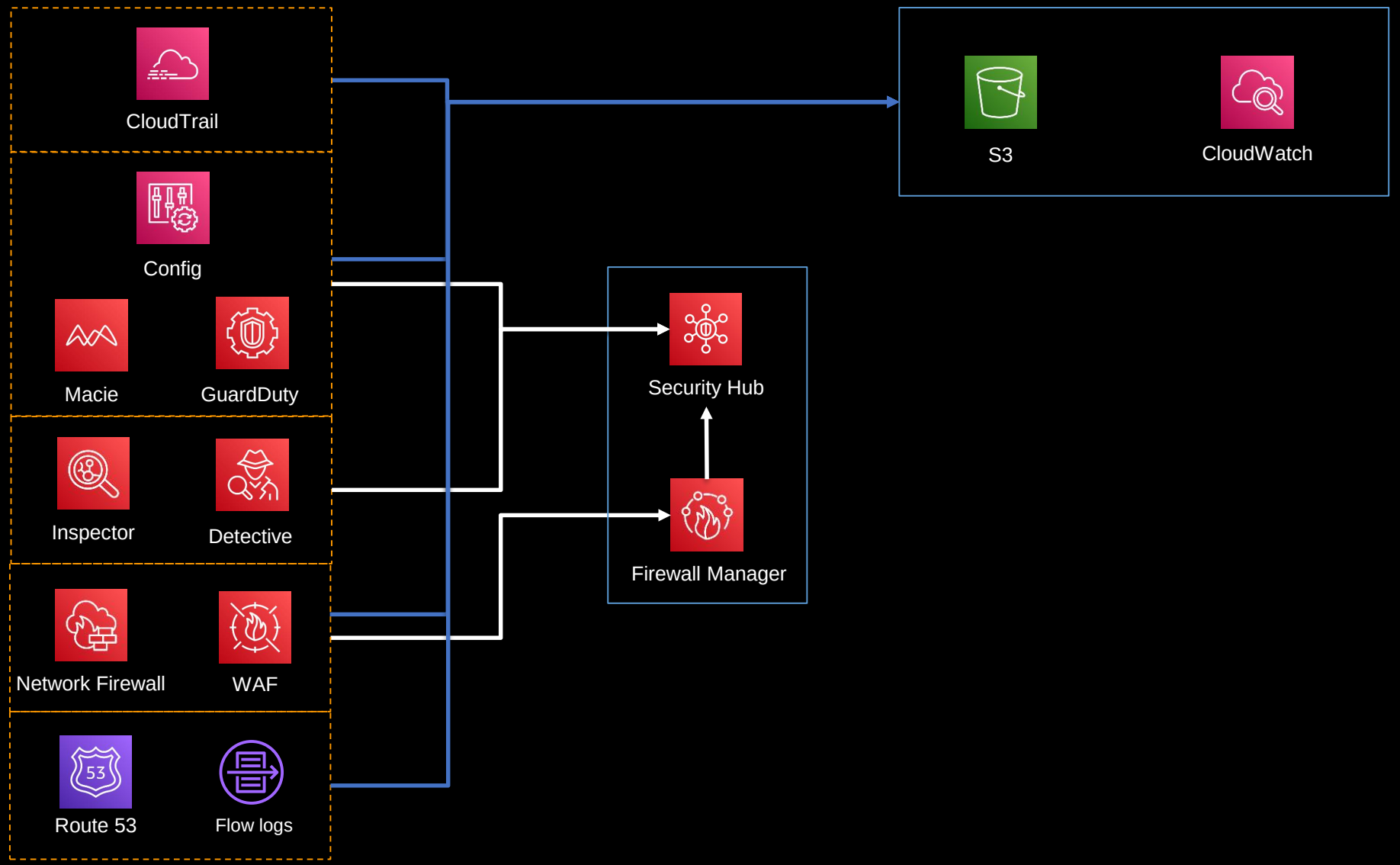
Log Export Path

Log Export Path

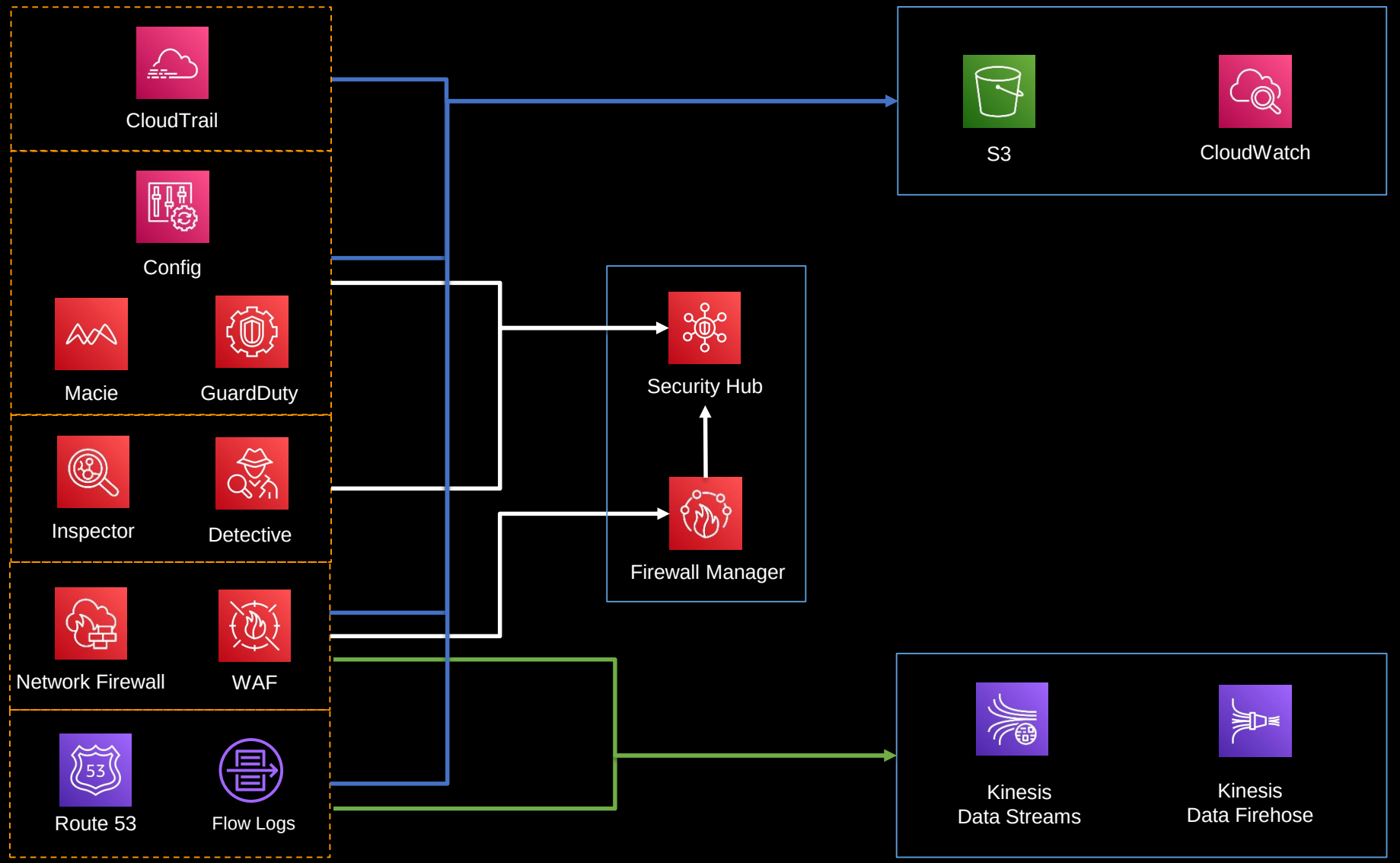
Log Export Path



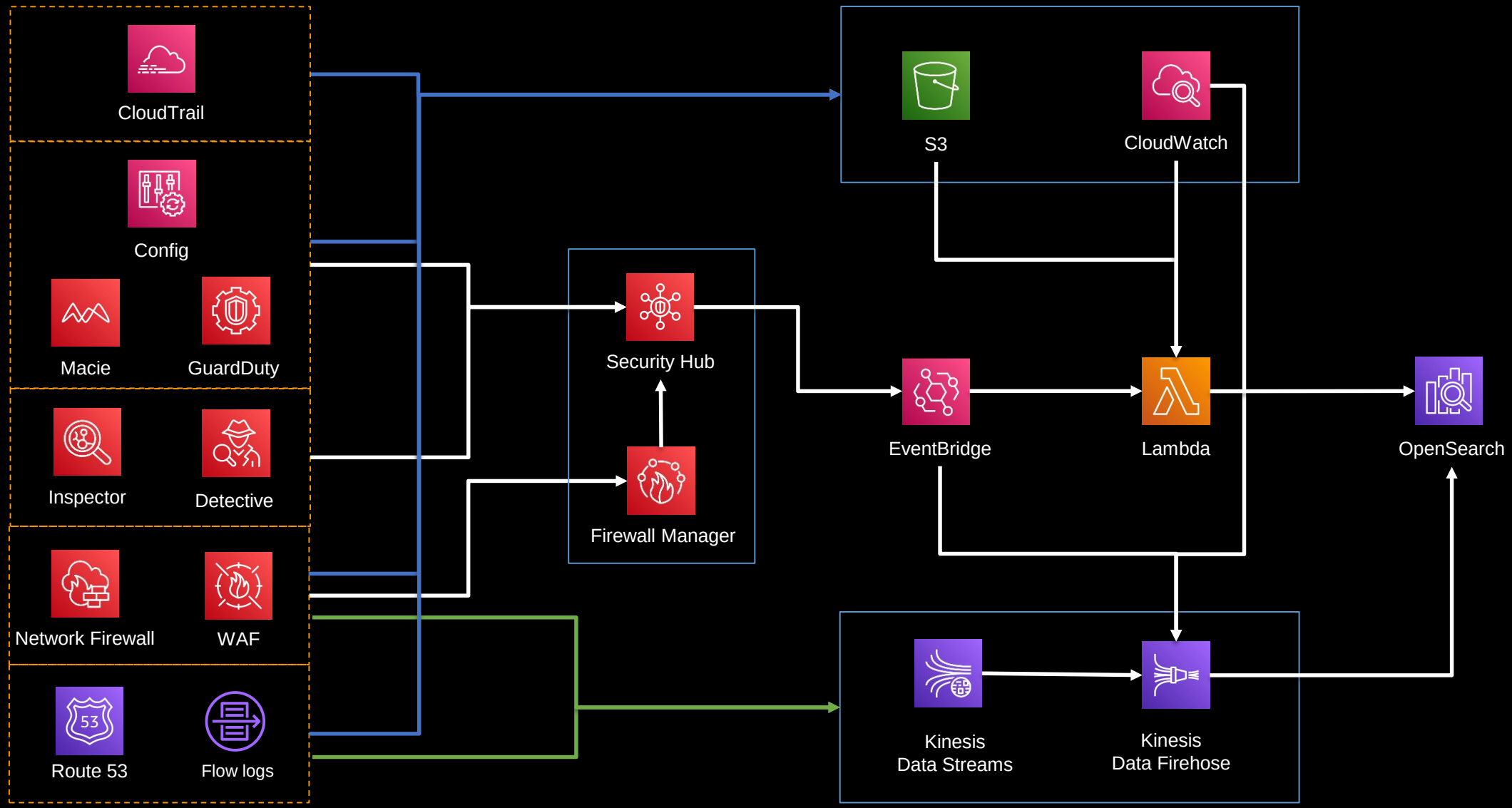
Log Export Path



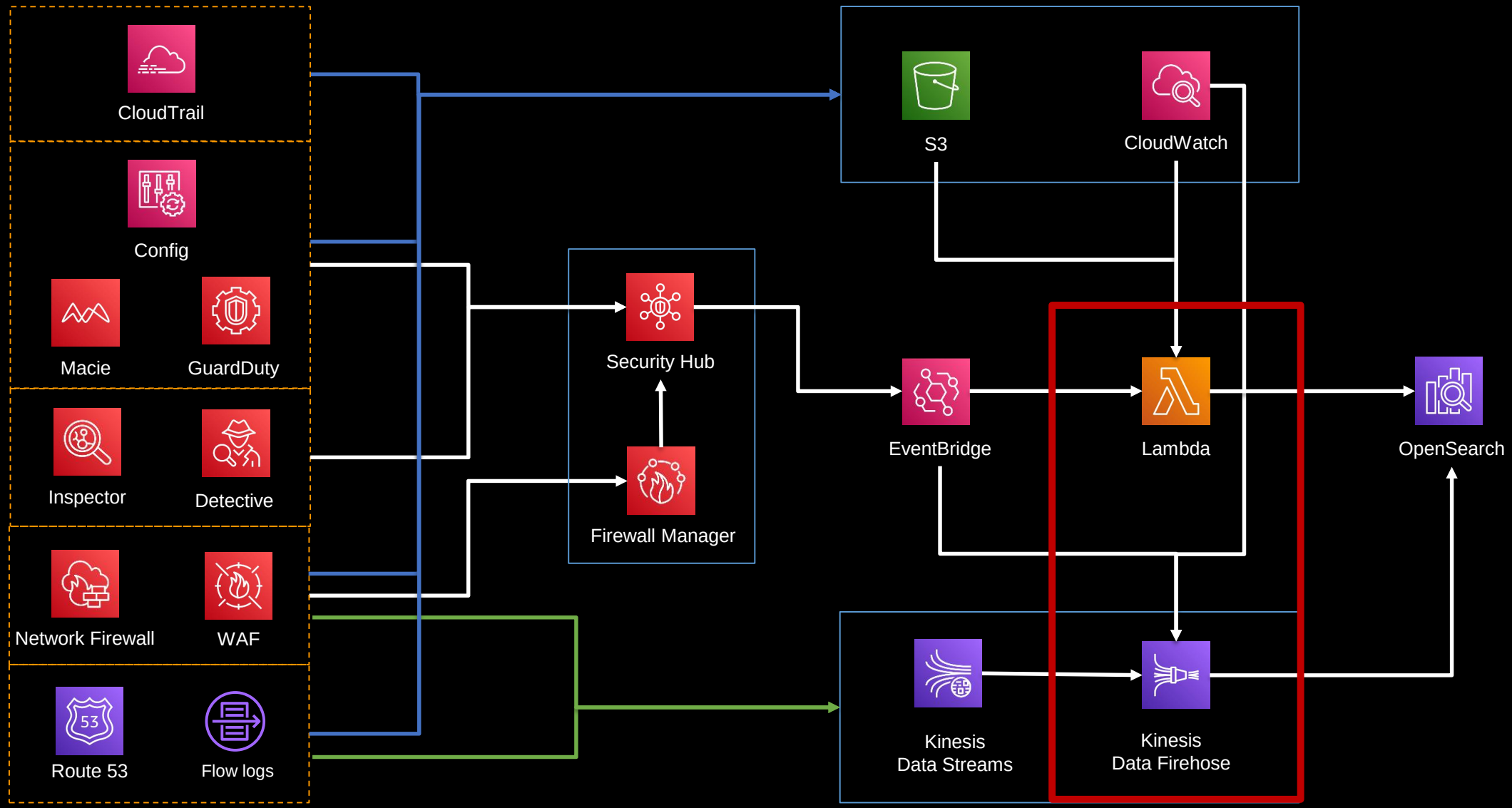
Log Export Path



Log Export Path



Log Export Path



Lambda vs KDF

AWS Lambda

- 저렴한 비용
- 개발이 필요함
- 소형 워크로드에 적합

VS

Kinesis
Data Firehose

- 상대적으로 비용이 비쌈
- 개발 없이 손쉽게 사용
- 대형 워크로드에 적합

Considerations

Considerations

COST-EFFECTIVE

FAST

WORKLOADS

EASY

Too many services...


AWS Config


AWS CloudTrail


Amazon VPC


IAM


AWS WAF


AWS Shield


Amazon Inspector


Amazon CloudWatch


AWS Systems Manager

Amazon Route 53


AWS Secrets Manager


Amazon GuardDuty


AWS Audit Manager


Amazon Macie


AWS Trusted Advisor


AWS Personal Health Dashboard


Amazon CloudFront

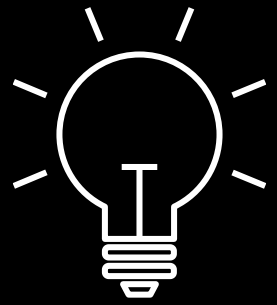

KMS


Amazon Cognito

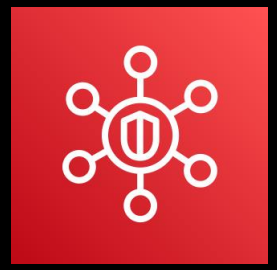

AWS Firewall Manager


Amazon Detective

Security Hub



Innovate Security Hub



What is AWS Security Hub?

Insights 및
규정 준수 확인

- AWS 보안서비스나 3rd Party 보안 서비스에서 탐지한 다양한 보안 탐지 내역을 통합하여 모니터링
- 보안 트렌드에 대한 분석 및 발견된 보안 탐지 내역에 대한 가중치 기준 선별
- 규정 준수 확인 (CIS AWS Foundation v1.2.0, PCI DSS v3.2.1)

AWS Security Hub

Findings

보안 탐지
내역
제공 서비스

Amazon Inspector

Amazon GuardDuty

Amazon Macie

AWS Config

Firewall Manager

IAM Access Analyzer

AWS Systems Manager

파트너 솔루션

추후 추가 예정

AWS Security Finding Format (ASFF)

AWS Security Finding Format (ASFF)

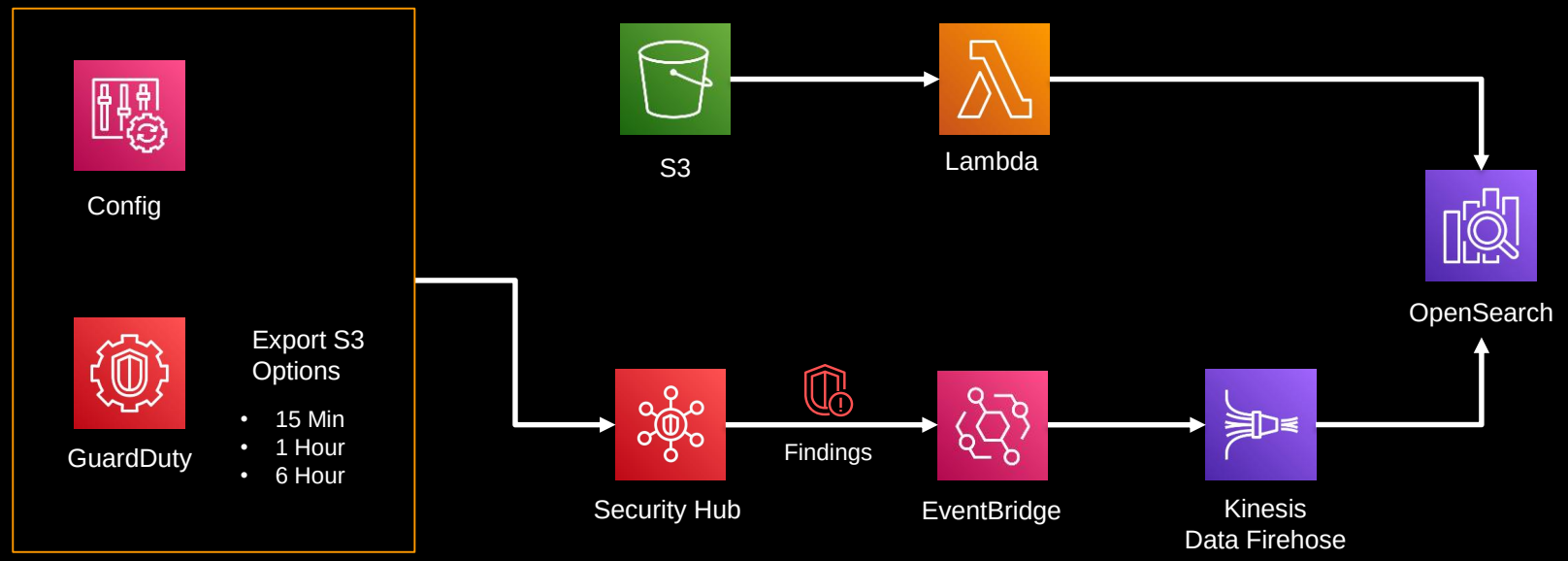
필수속성	설명
AwsAccountId	AWS 계정 ID
CreatedAt	검색 결과로 포착된 잠재적 보안 문제가 언제 생성되었는지를 나타냅니다.
Description	결과에 대한 설명입니다. 이 필드는 일반적인 표준 문안 텍스트이거나 결과의 인스턴스에만 해당하는 세부 정보일 수 있습니다.
GeneratorId	결과를 생성한 솔루션별 구성 요소(로직의 개별 단위)에 대한 식별자입니다.
Id	결과의 제품별 식별자입니다.
ProductArn	제품이 Security Hub에 등록된 후 타사 조사 결과 제품을 고유하게 식별하는 Security Hub에서 생성한 아마존 리소스 이름 (ARN) 입니다.
Resources	리소스 데이터 형식 세트를 제공합니다.
SchemaVersion	결과의 형식을 지정할 스키마 버전입니다. 이 필드의 값은 AWS로 식별되는 공식적으로 게시된 버전 중 하나여야 합니다. 현재 릴리스에서 AWS Security Finding 형식 스키마 버전은 2018-10-08입니다.
Severity	발견된 결과의 중요성을 정의합니다. INFORMATIONAL, LOW, MEDIUM, HIGH, CRITICAL
Types	결과를 분류하는 namespace/category/classifier 형식으로 구성된 하나 이상의 결과 유형입니다
UpdatedAt	결과 레코드를 마지막으로 업데이트한 시점을 나타냅니다.

AWS Security Finding Format (ASFF)

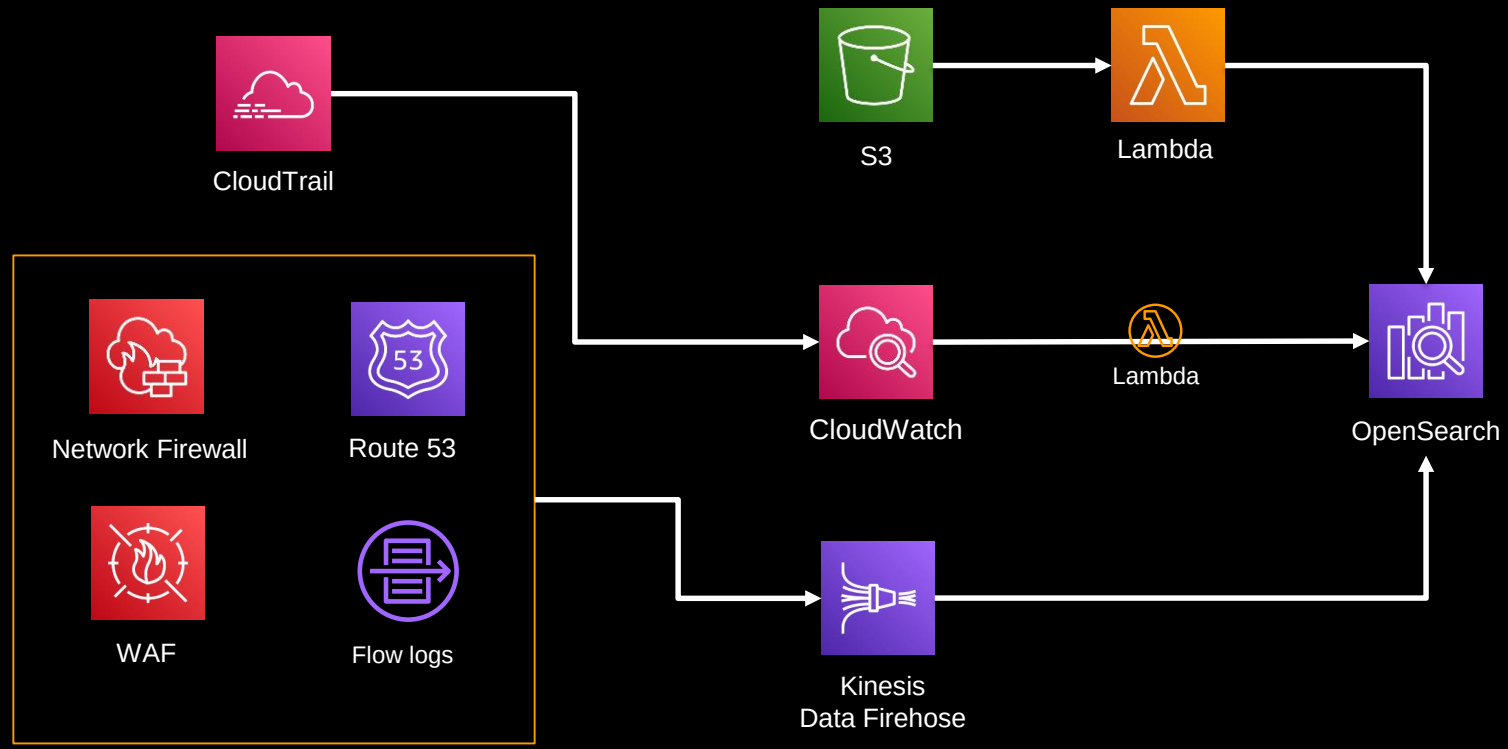
필수속성	설명
AwsAccountId	AWS 계정 ID
CreatedAt	검색 결과로 포착된 잠재적 보안 문제가 언제 생성되었는지를 나타냅니다.
Description	결과에 대한 설명입니다. 이 필드는 일반적인 표준 문안 텍스트이거나 결과의 인스턴스에만 해당하는 세부 정보일 수 있습니다.
GeneratorId	결과를 생성한 솔루션별 구성 요소(로직의 개별 단위)에 대한 식별자입니다.
Id	결과의 제품별 식별자입니다.
ProductArn	제품이 Security Hub에 등록된 후 타사 조사 결과 제품을 고유하게 식별하는 Security Hub에서 생성한 아마존 리소스 이름 (ARN) 입니다.
Resources	리소스 데이터 형식 세트를 제공합니다.
SchemaVersion	결과의 형식을 지정할 스키마 버전입니다. 이 필드의 값은 AWS로 식별되는 공식적으로 게시된 버전 중 하나여야 합니다. 현재 릴리스에서 AWS Security Finding 형식 스키마 버전은 2018-10-08입니다.
Severity	발견된 결과의 중요성을 정의합니다. INFORMATIONAL, LOW, MEDIUM, HIGH, CRITICAL
Types	결과를 분류하는 namespace/category/classifier 형식으로 구성된 하나 이상의 결과 유형입니다
UpdatedAt	결과 레코드를 마지막으로 업데이트한 시점을 나타냅니다.

심각도 등급	범위	타입	기준
Informational	0	Sensitive data identification	기록차원의 정보. Compliance Check을 Pass했거나 민감정보가 식별된 경우에 해당
Low	1 ~ 39	S/W and configuration checks	미래에 침해될 가능성이 발견된 경우. 취약점이나 구성 오류 등을 탐지한 경우에 해당
Medium	40 ~ 69	Threat detection and unusual behavior ~ TTPS(Tactics Techniques and procedures)	침해행위를 적발했지만 공격자의 의도가 달성되었는지 불분명한 경우. 멀웨어 활동, 해킹 시도를 감지했거나 비정상적인 행동을 탐지한 경우에 해당
High	70 ~ 89	Effects	공격자가 공격목적을 달성한 것을 분명히 탐지한 경우. 데이터 유출을 감지했거나 서비스의 중단을 탐지한 경우에 해당
Critical	90 ~ 100		

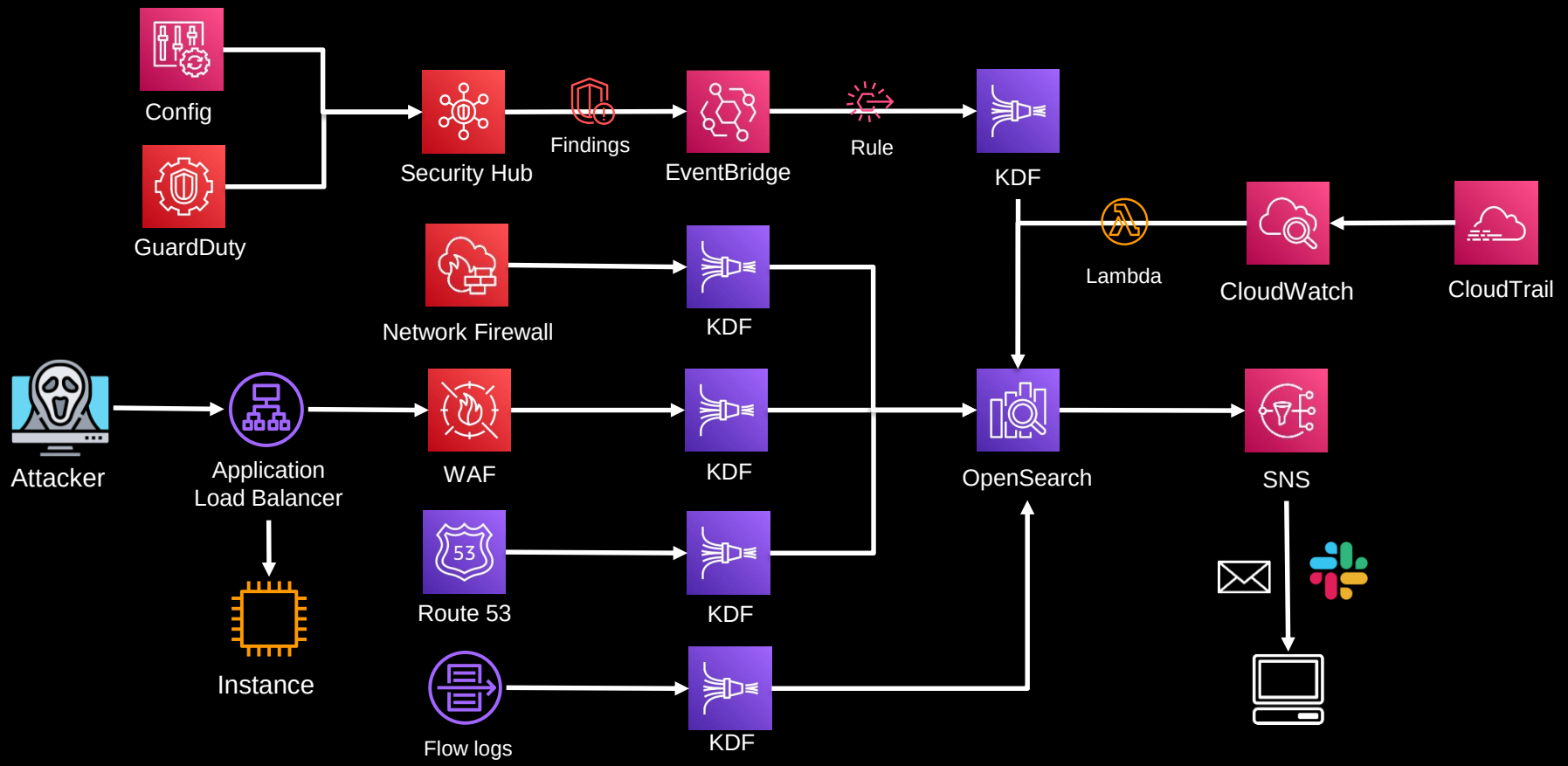
AWS Security Service Log Collect Choice



AWS Security Service Log Collect Choice

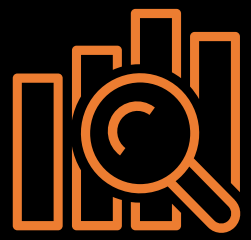


Architecture Pattern



위협 탐지를 위한 대시보드 및 알람 구성

Amazon OpenSearch Service소개



Amazon OpenSearch Service

Amazon OpenSearch Service는 운영 데이터의 실시간 검색, 모니터링 및 분석을 안전하게 제공합니다.

관리형: 많은 유즈케이스가 있는 오픈소스 솔루션을 관리형으로 사용함으로써 운영 우수성 확보

보안성: 견고한 네트워 아키텍처와 내장된 인증도구로 데이터를 감사하고 안전하게 보호

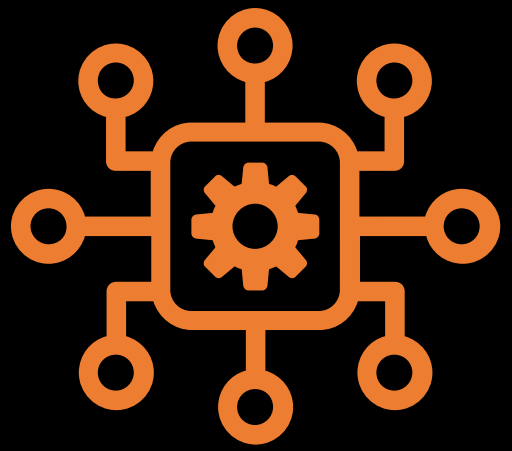
관찰가능성: 머신러닝 기반 탐지 및 경보체계, 시각화 기능을 통해 잠재적 위협을 감지하고 체계적으로 대응 가능

비용 최적화: 시간과 자원 사용 최적화

OpenSearch와 Amazon OpenSearch Service는 어떤 관계인가?

- 커뮤니티 주도의 검색 및 분석 오픈소스 이며, 엘라스틱서치 7.10.2 버전에서 분기됨
- **OpenSearch** 는 Apache Lucene기반의 분산 검색 엔진이며, **OpenSearch Dashboards**는 **데이터 시각화 및 유저인터페이스를 제공**
- 엘라스틱서치 오픈 배포판의 모든 기능을 포함

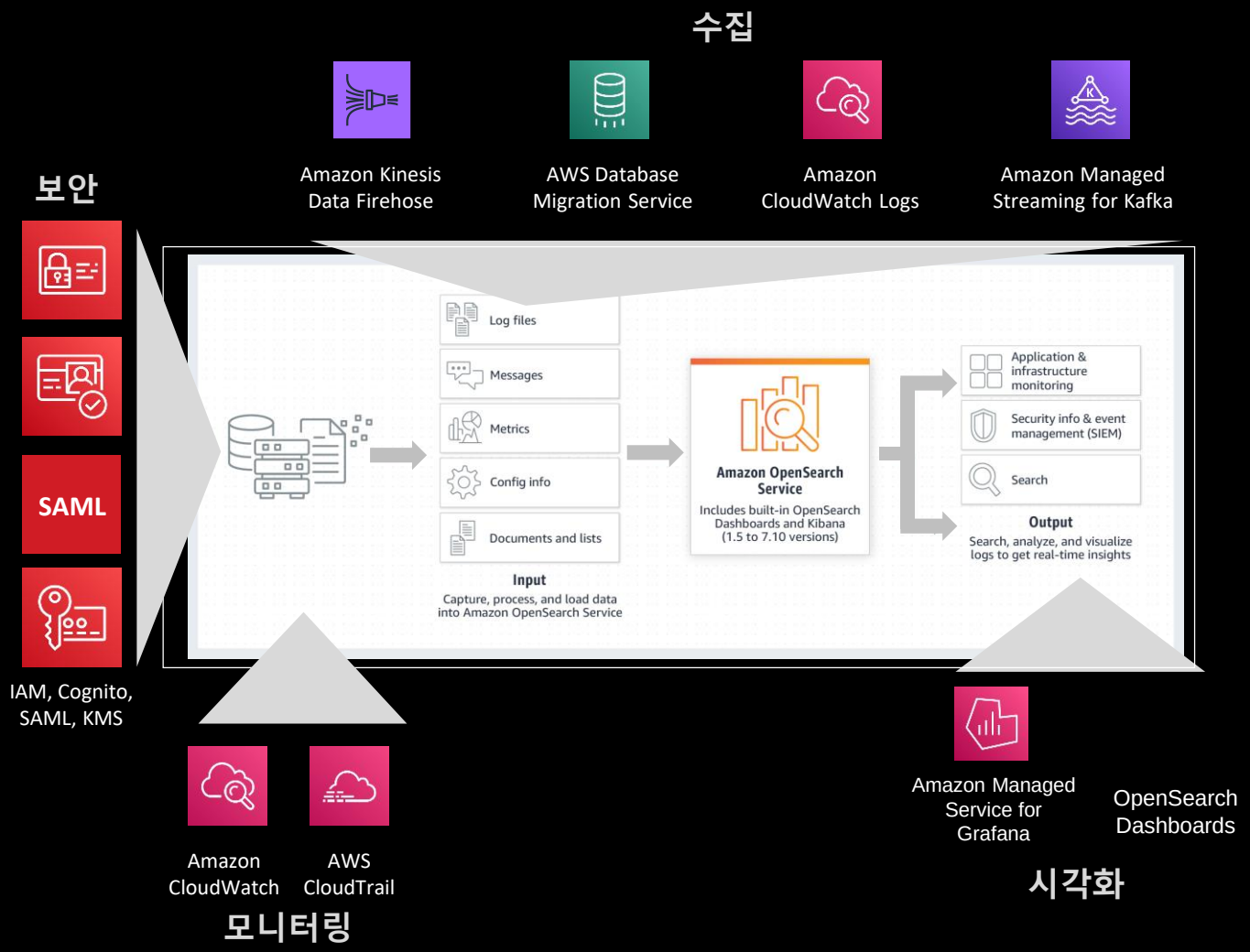
관리형 오픈소스



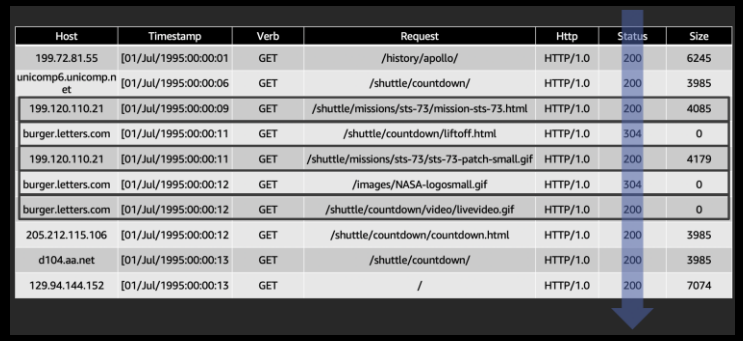
- 자동 조정 및 인덱싱 번호
- 하드웨어 프로비저닝
- AWS 매니지드 소프트웨어 설치 및 패치
- AWS 모니터링 및 문제 해결, 24x7
- AWS 클러스터 확장
- AWS 교차 리전 복제 지원
- 업데이트나 업그레이드 시 다운타임 없음
- 스토리지 티어링

빌트인 통합 제공

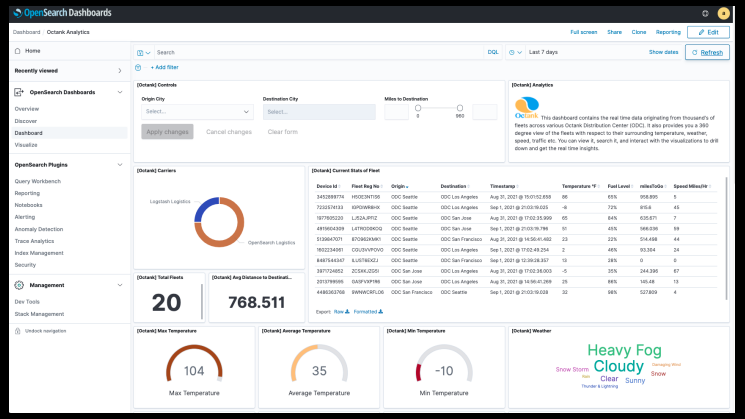
- **수집 통합** : 로그, 추적 및 메트릭 데이터 로드
- **모니터링 통합** : 이상 징후 및 경고 모니터링
- **보안 통합** : 보안 정책 확장
- **시각화 통합** : 차트 생성 및 대시보드 구성



데이터로부터 인사이트 획득



Host	Timestamp	Verb	Request	Http	Status	Size
199.72.81.55	[01/Jul/1995:00:00:01	GET	/history/apollo/	HTTP/1.0	200	6245
unicomp6.unicomp.net	[01/Jul/1995:00:00:06	GET	/shuttle/countdown/	HTTP/1.0	200	3985
199.120.110.21	[01/Jul/1995:00:00:09	GET	/shuttle/missions/sts-73/mission-sts-73.html	HTTP/1.0	200	4085
burger.letters.com	[01/Jul/1995:00:00:11	GET	/shuttle/countdown/liftoff.html	HTTP/1.0	304	0
199.120.110.21	[01/Jul/1995:00:00:11	GET	/shuttle/missions/sts-73/sts-73-patch-small.gif	HTTP/1.0	200	4179
burger.letters.com	[01/Jul/1995:00:00:12	GET	/images/NASA-logosmall.gif	HTTP/1.0	304	0
burger.letters.com	[01/Jul/1995:00:00:12	GET	/shuttle/countdown/video/livevideo.gif	HTTP/1.0	200	0
205.212.115.106	[01/Jul/1995:00:00:12	GET	/shuttle/countdown/countdown.html	HTTP/1.0	200	3985
d104.aa.net	[01/Jul/1995:00:00:13	GET	/shuttle/countdown/	HTTP/1.0	200	3985
129.94.144.152	[01/Jul/1995:00:00:13	GET	/	HTTP/1.0	200	7074

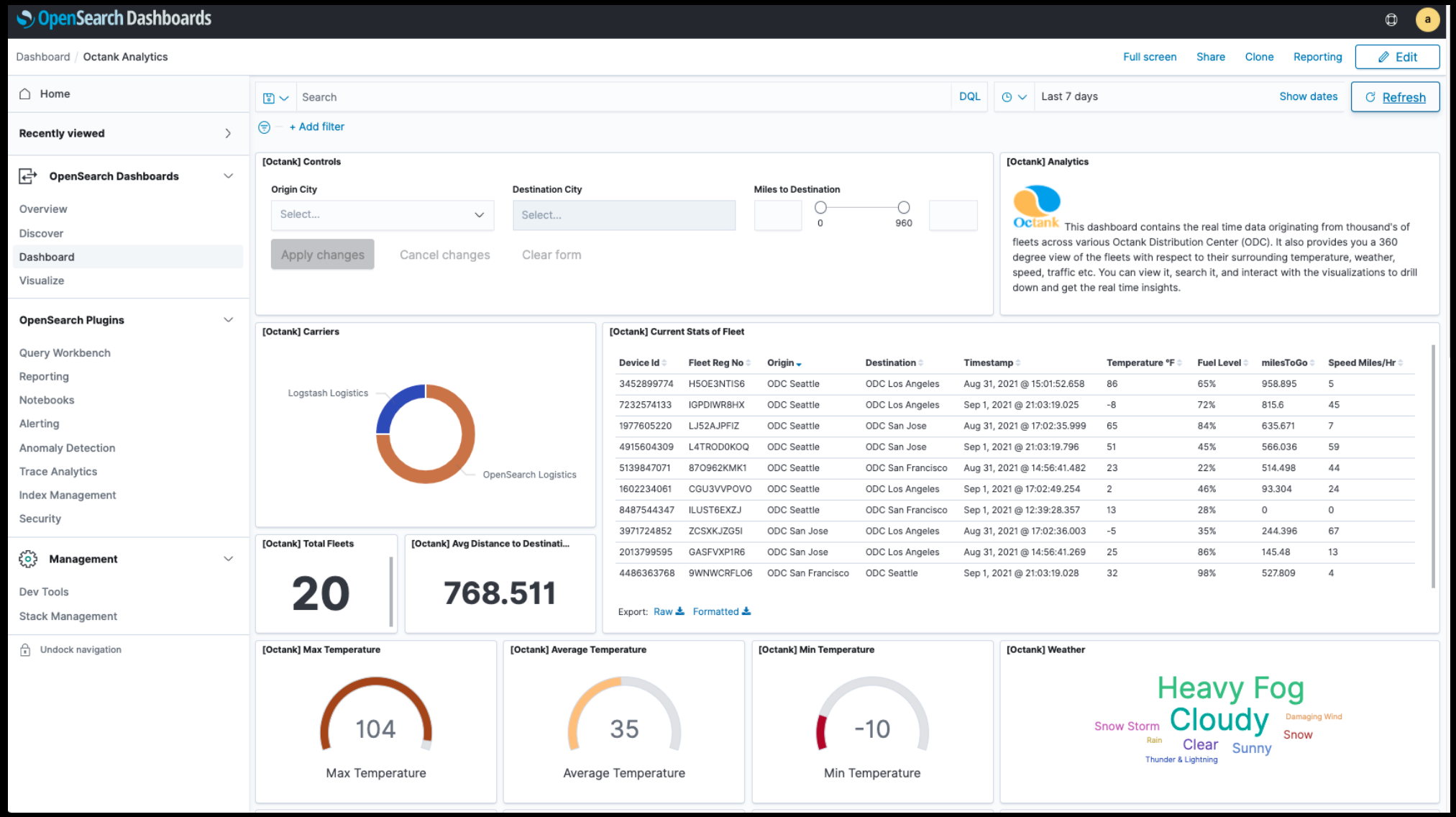


OpenSearch 실시간에 가까운 통찰력을 제공합니다.

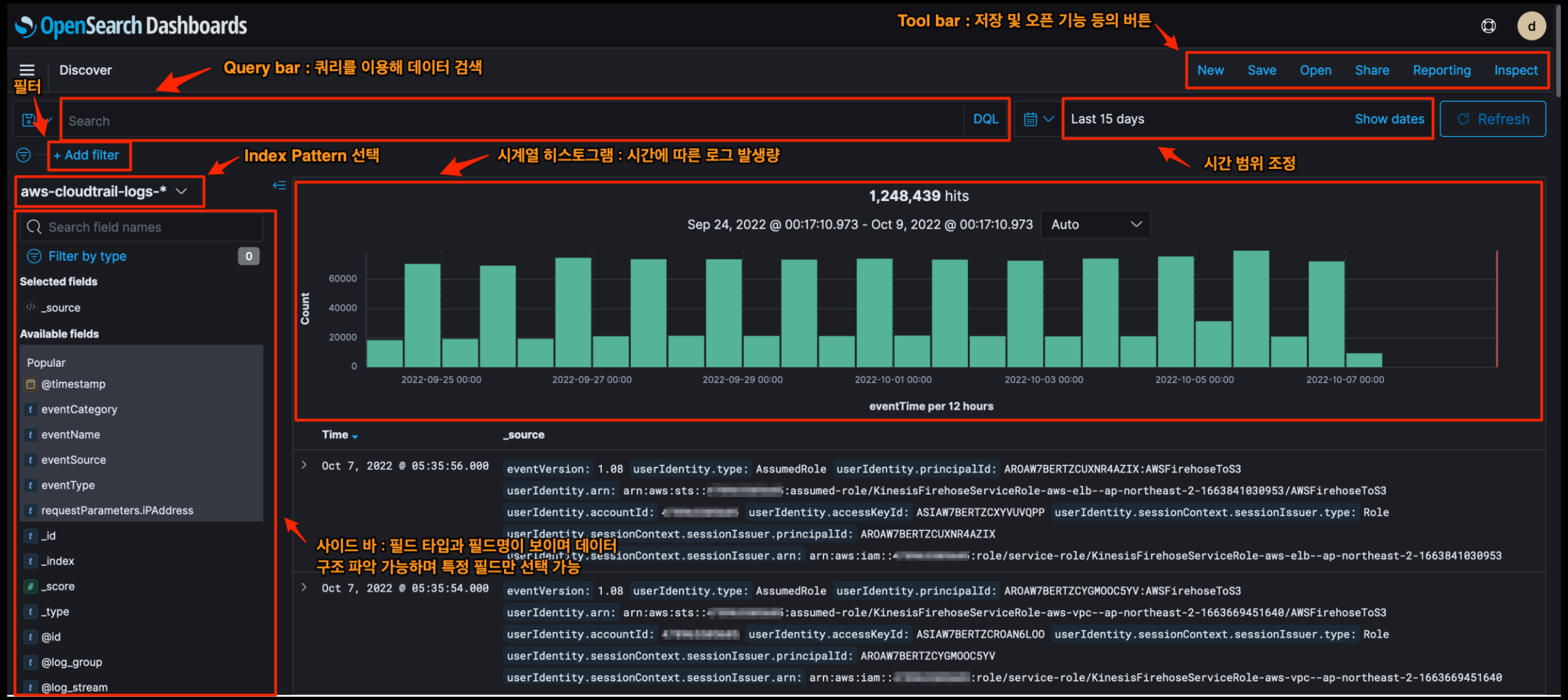
aws

OpenSearch Dashboard 소개

OpenSearch Dashboards - 실시간 시각화 툴

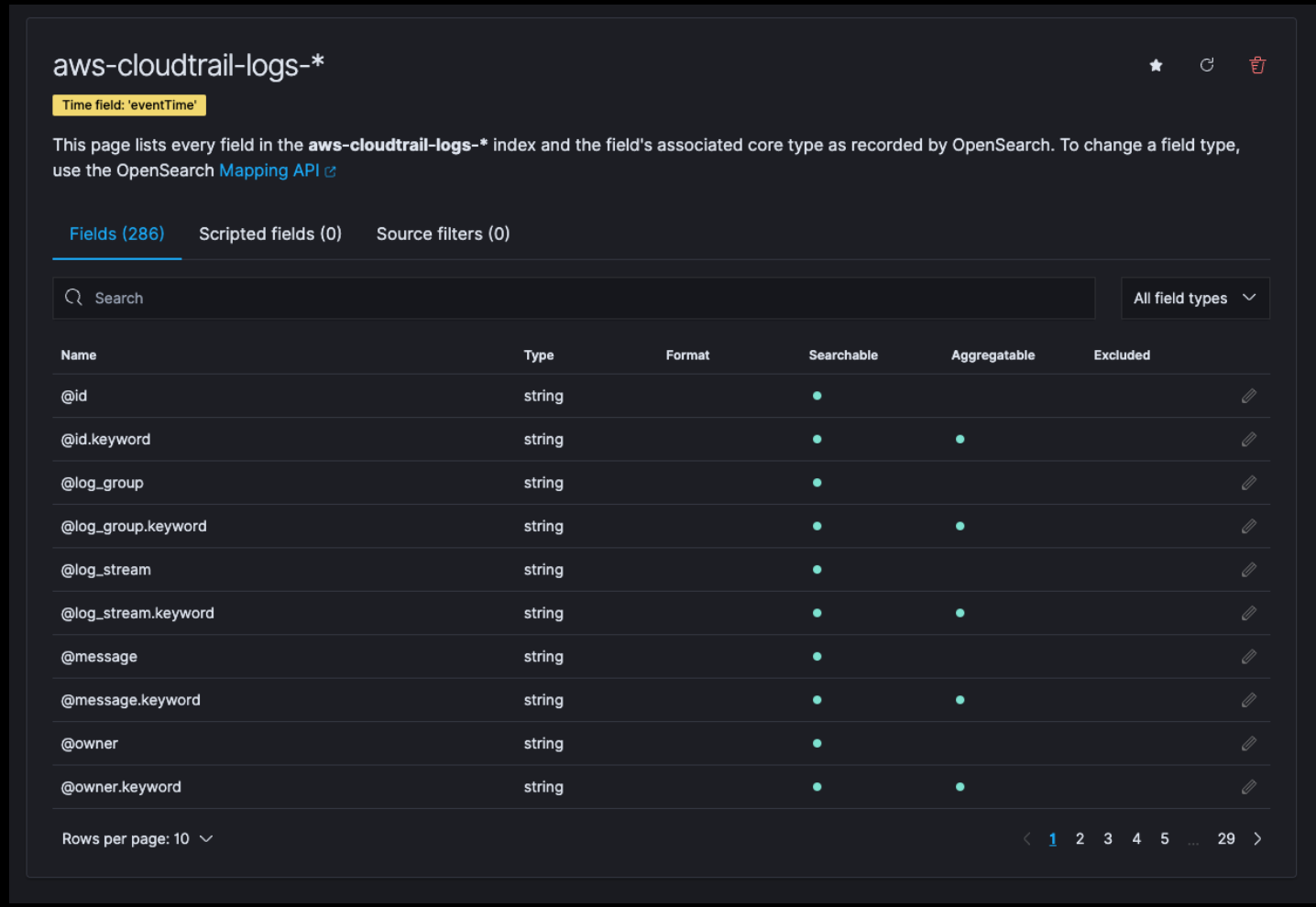


Discover UI



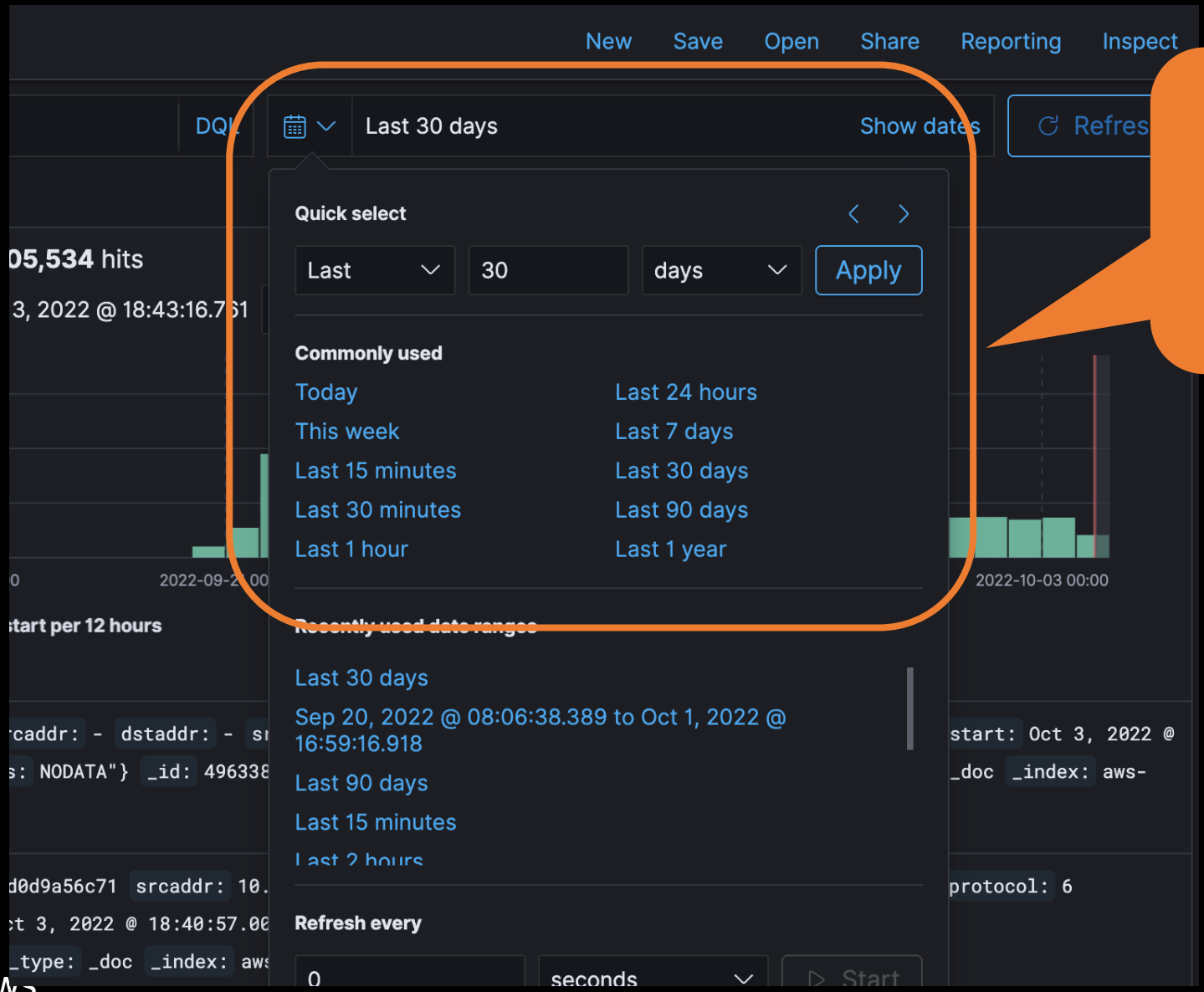
Index Pattern 이란?

- OpenSearch Dashboards의 시각화를 위해서는 반드시 인덱스 패턴 필요
- 인덱스의 각 필드들에 대한 매핑 정보를 기록하여 검색과 시각화에 사용
- OpenSearch에 인덱싱 된 데이터에 대해서만 인덱스 패턴 생성 가능
- Wildcard(*)를 사용하여 Prefix가 동일한 인덱스에 대해 인덱스 패턴 생성 가능



Discover에서 index pattern 지정

Discover 날짜 지정 방법

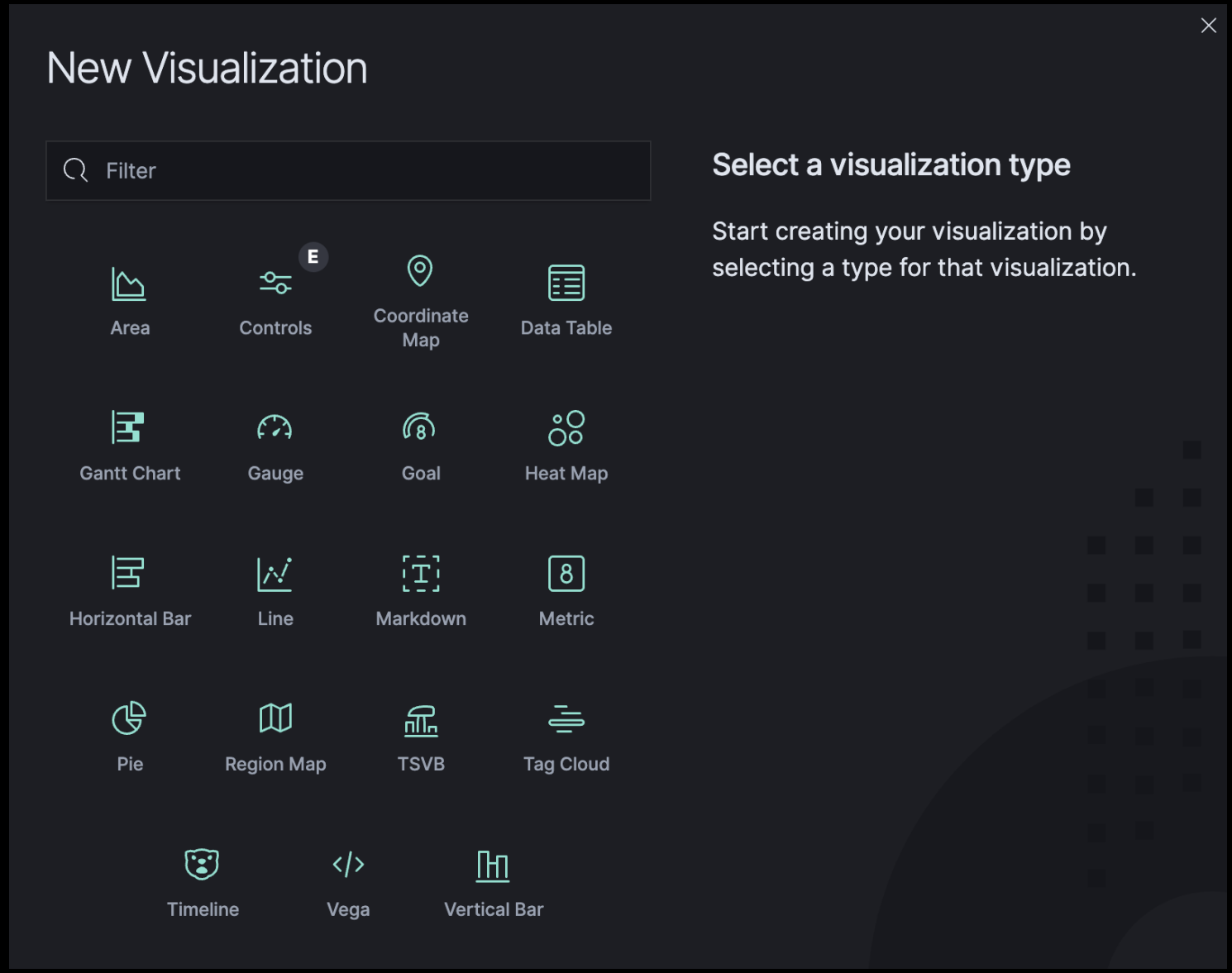


선택한 기간에 해당하는
도큐먼트만 결과에 표시

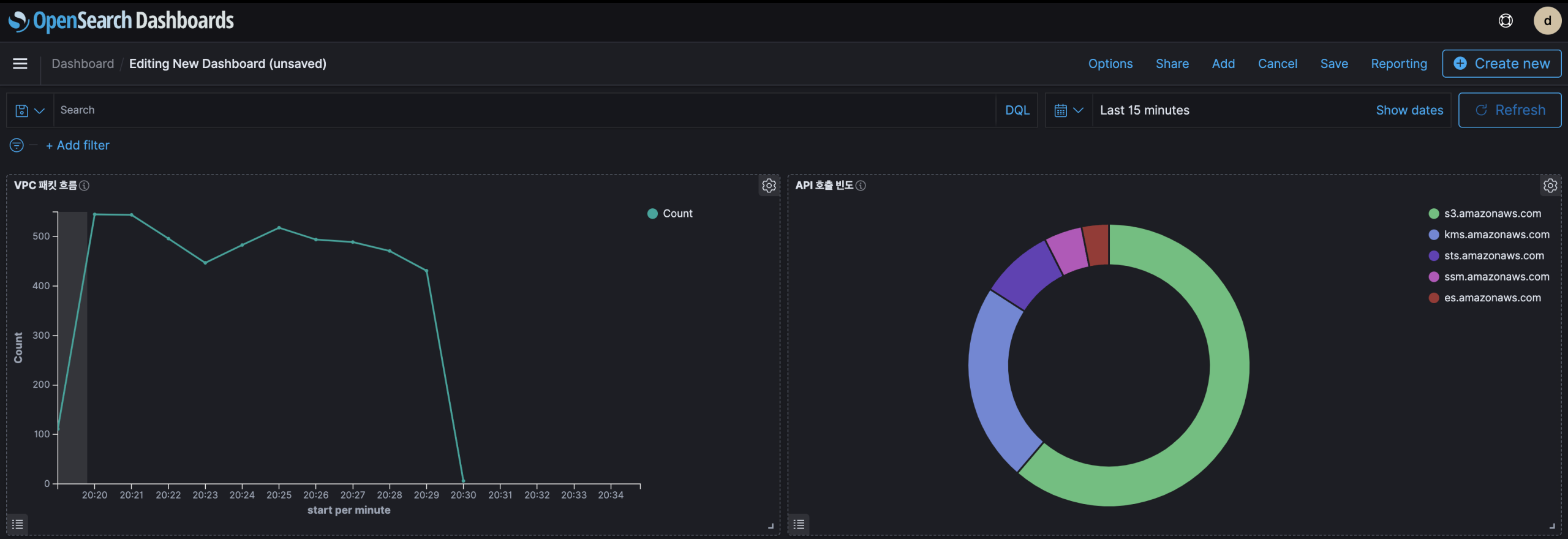
DQL (Dashboards Query Language) 쿼리 유형

- 용어 쿼리 (Term query) : 입력한 용어와 일치하는 도큐먼트 검색
- 부울 쿼리 (Boolean query) : and, or, not을 사용하여 결과가 true 인 도큐먼트 검색
- 날짜 및 범위 쿼리 (Date and range queries)
- 중첩 필드 쿼리 (Nested field query)

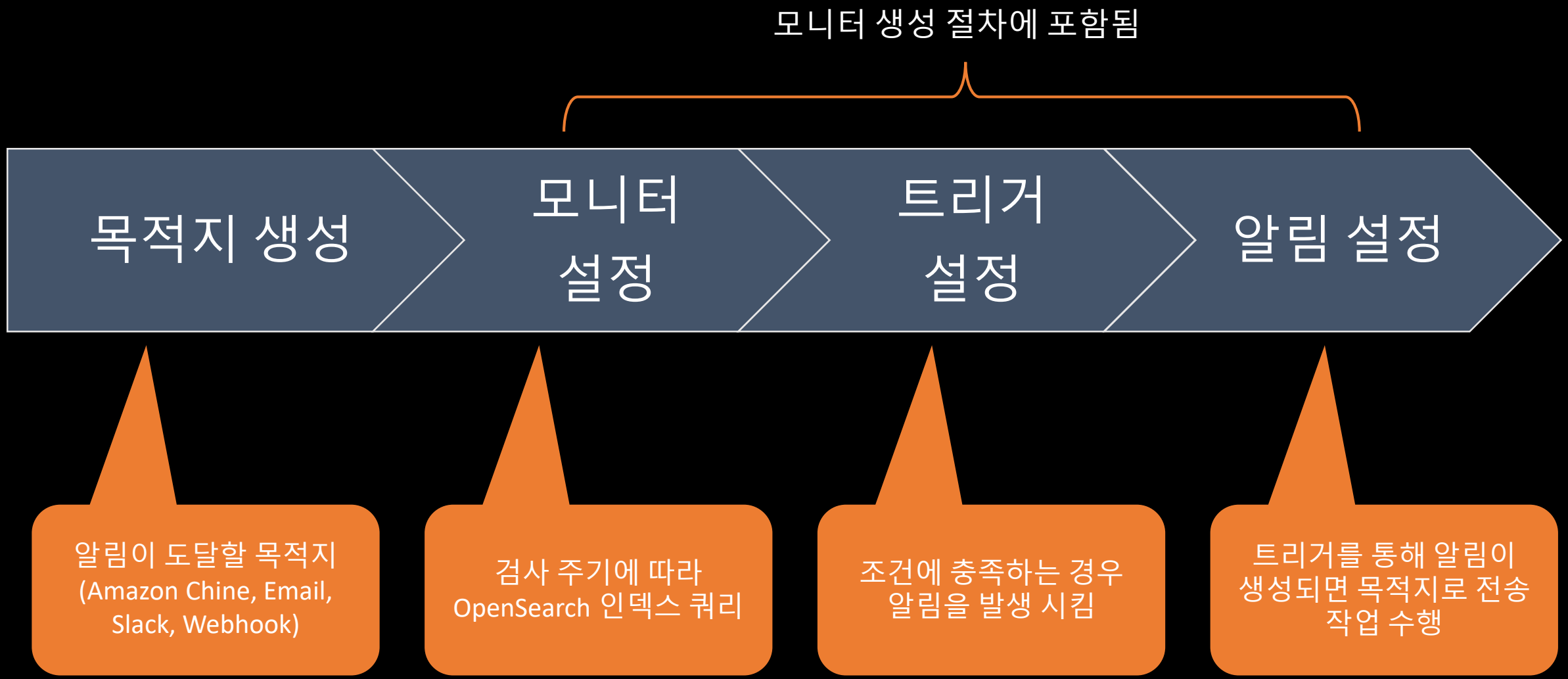
다양한 시각화 타입 제공



대시보드 만들기 – 추가된 차트 확인 및 크기 조정



Alert 설정



모니터 생성 - Alert 수신 예시

메시지는 OpenSearch에 저장된 도큐먼트의 값을 참조하여 작성됨

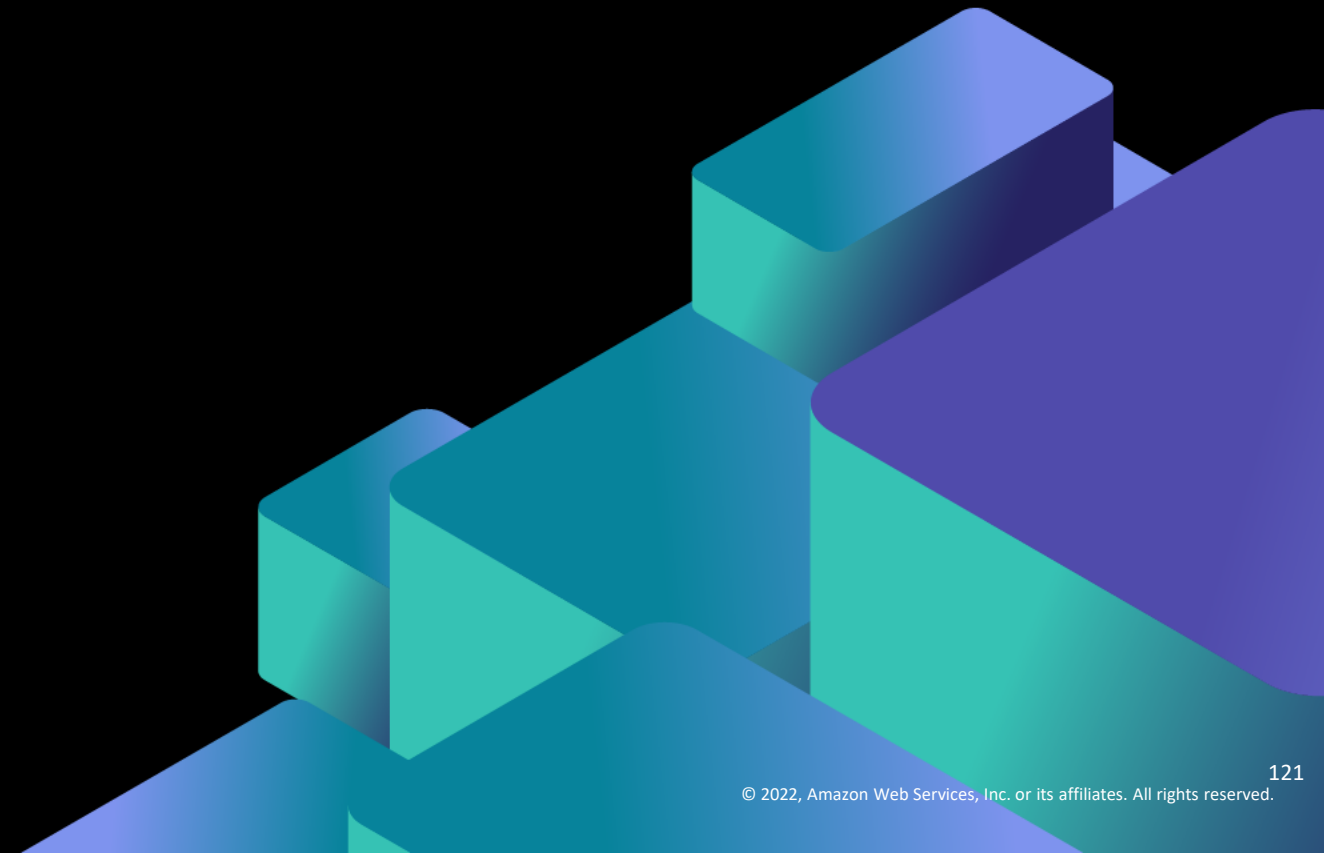
GuardDuty에서 심각도 Medium 알림이 발생하였습니다.

Monitor GuardDutySevertyMedium just entered alert status. Please investigate the issue.
- Service : GuardDuty
- Trigger: GuardDutySevertyMedium
- Severity: 3
- Period start: 2022-09-22T05:49:22.990Z
- Period end: 2022-09-22T05:50:22.990Z
- Account : 478965505605
- Description : EC2 instance i-0e32c4981e02a79eb is communicating with a disallowed IP address 95.163.121.33 on the list DP-GuardDuty-ThreatIP.
- URL : https://ap-northeast-2.console.aws.amazon.com/guardduty/home?region=ap-northeast-2#/findings?macros=current&fId=00c1b1cc9fcfcb5019ccd8e3890bd2e2

GuardDuty에서 심각도 Medium 알림이 발생하였습니다.

Monitor GuardDutySevertyMedium just entered alert status. Please investigate the issue.
- Service : GuardDuty
- Trigger: GuardDutySevertyMedium
- Severity: 3
- Period start: 2022-09-22T05:50:22.990Z
- Period end: 2022-09-22T05:51:22.990Z
- Account : 478965505605
- Description : EC2 instance i-0e32c4981e02a79eb is communicating with a disallowed IP address 95.163.121.33 on the list DP-GuardDuty-ThreatIP.
- URL : https://ap-northeast-2.console.aws.amazon.com/guardduty/home?region=ap-northeast-2#/findings?macros=current&fId=00c1b1cc9fcfcb5019ccd8e3890bd2e2

Summary



Thank you!