CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

개방형 보안체계(OCSF)를 통한 Amazon Security Lake 보안 이벤트 대시보드 구현 방안

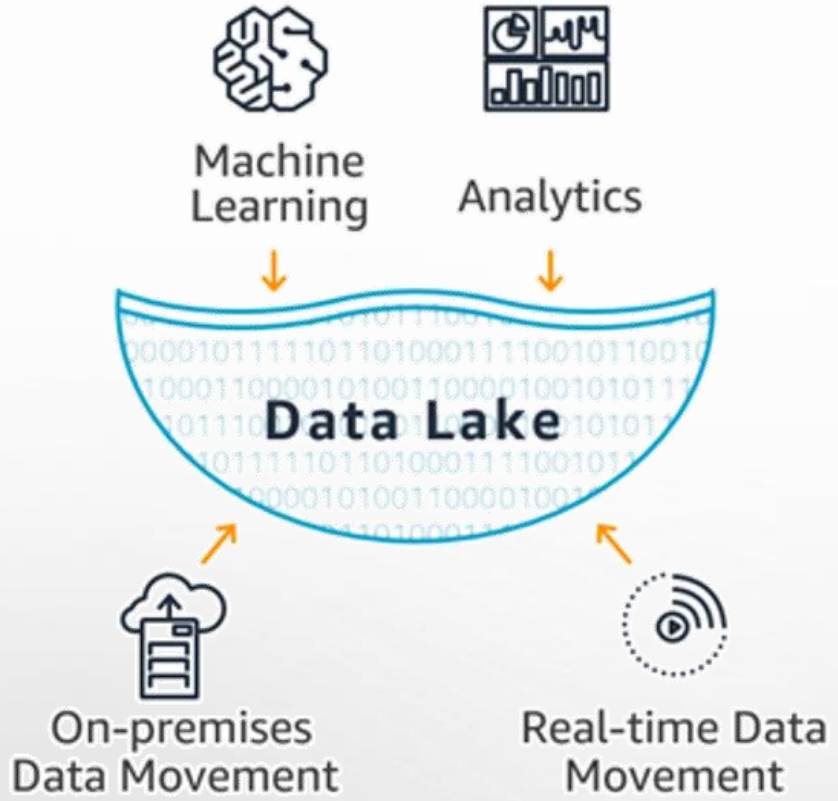
왜 우리는 Security Lake 도입을 검토해야 하는가?

MEGAZONE CLOUD

Data Lake

- 데이터 레이크(Data Lake)는 데이터의 구조화 여부와 상관없이 대량의 원시 데이터를 저장, 처리, 관리하기 위한 중앙집중식 저장소

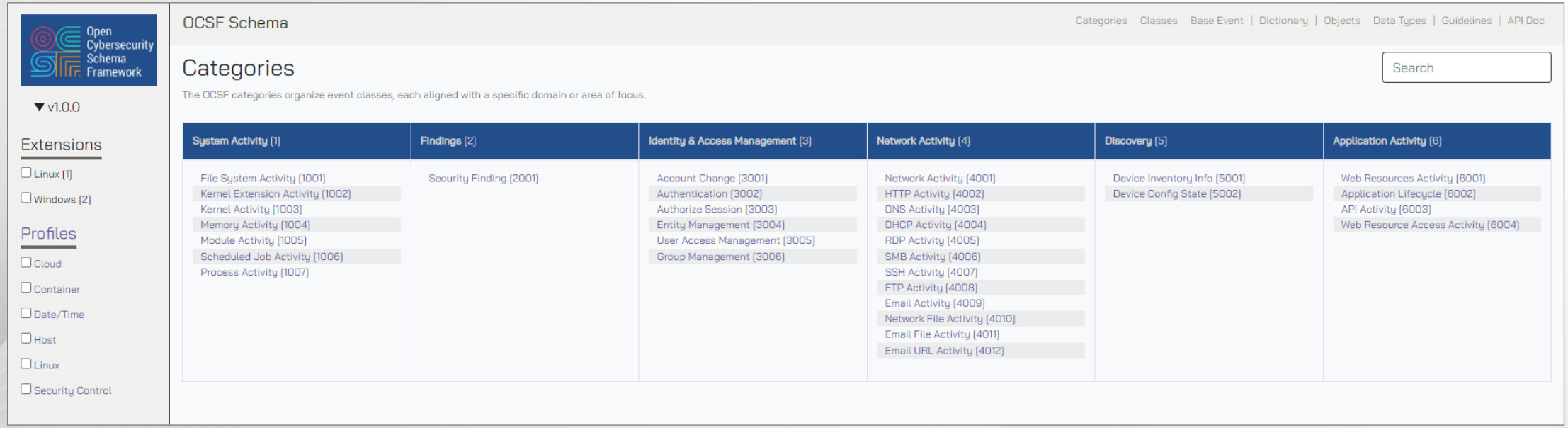
- 데이터 레이크는 "데이터의 사용 목적"이 아직 결정되지 않았더라도 이후 필요한 목적에 맞추어 능동적으로 대응하기 위해 사전에 한 곳에 집중하여 저장



출처 : https://aws.amazon.com/ko/blogs/korea/aws-lake-formation-now-generally-available/

Data Lake

- "데이터를 잘 이용하기 위함" → 데이터는 축적이 목표가 아닌 활용이 최종 목표
- 데이터의 효과적인 활용을 위해서는 사용자의 필요에 맞추어 데이터 전처리가 필수
- 보안 데이터를 효과적으로 활용하기 위해 표준화와 정규화가 필요



출처 : https://schema.ocsf.io/

MEGAZONE CLOUD

OCSF (Open Cybersecurity Schema Framework)

- 보안 데이터의 솔루션 공급자와 소스에 구애 받지 않으며, 보안 스키마 확장성을 제공하되 공통적으로 사용하는 주요 보안 데이터의 스키마를 제공하여 편의성과 개발 간소화와 함께 벤더 중립성을 제공하는 오픈소스 프로젝트

Open-source project to deliver a simplified and vendor-agnostic taxonomy for security data that can be adopted in any environment, application, or solution provider

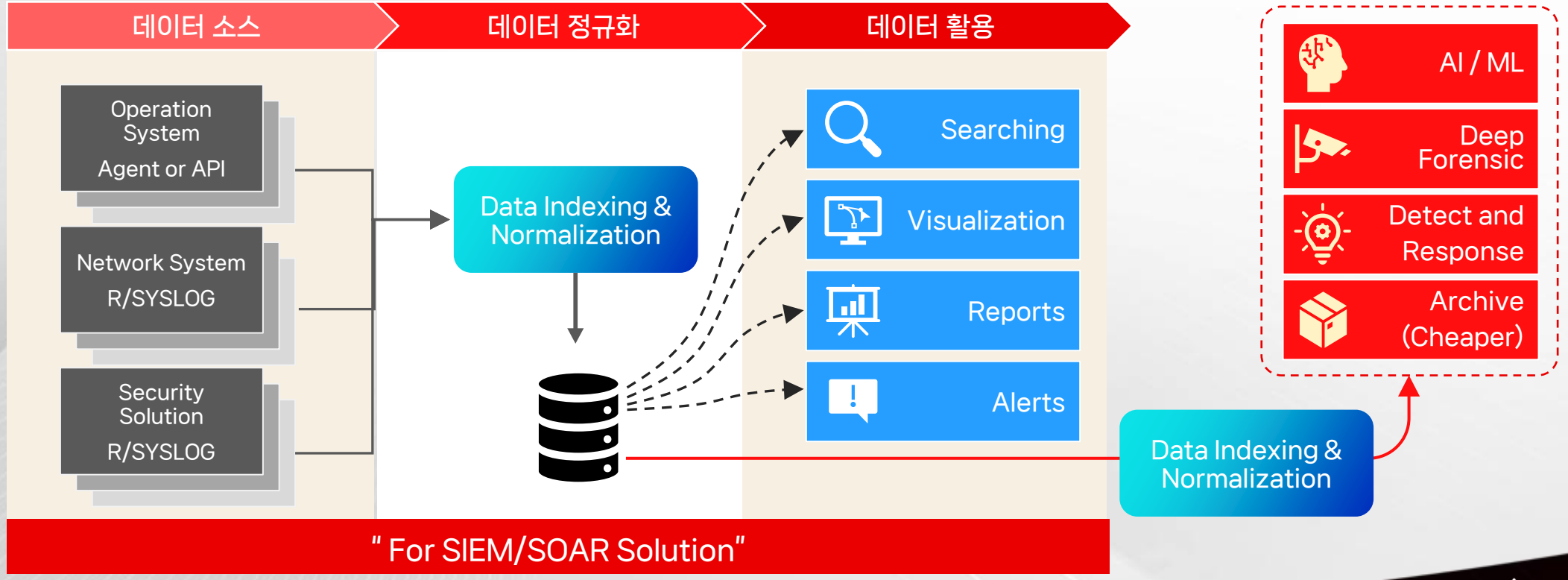
Speed up data ingestion and analysis without the time-consuming, upfront normalization tasks

Combine data from OCSF-compliant sources to break down data silos that slow security teams

MEGAZONE CLOUD

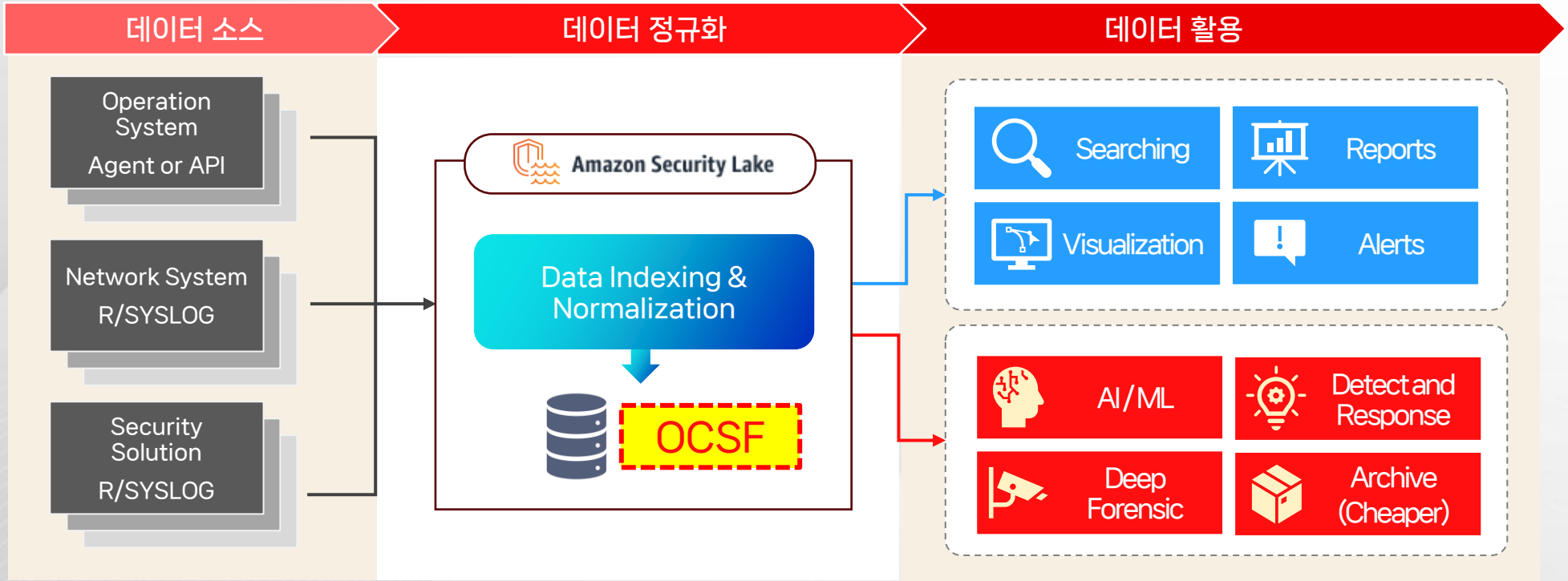
OCSF - 미적용시 발생 가능한 문제점

- 보안 데이터는 보안 서비스 사용자의 목적과 무관하게 솔루션 공급자의 기준에 맞추어 설계되어 제공
- 보안 서비스 사용자의 입장에서는 보안 업무를 위한 여러 보안 데이터들의 연동과 분석에서 제약이 발생
- 보안 데이터를 효율적으로 사용하고 활용하기 위해 목적에 맞추어 데이터 재가공이 필요



Amazon Security Lake

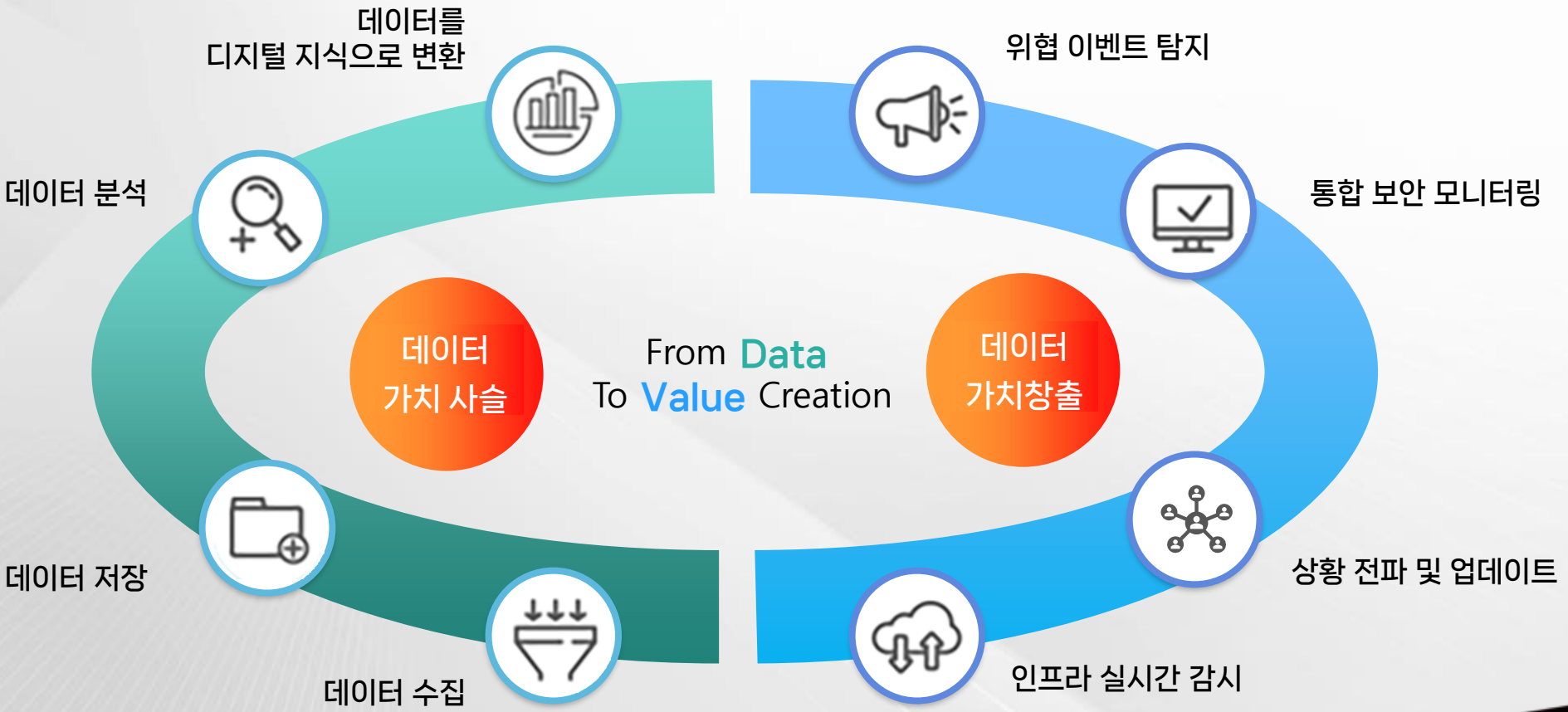
- OCSF는 보안 데이터의 정규화를 지원하는 표준 프레임워크
- Amazon Security Lake는 OCSF 기반으로 데이터를 정규화하여 제공
- 데이터 활용을 위한 재가공 불필요



MEGAZONE CLOUD

Data Sovereignty (데이터 주권)

- 데이터의 진정한 소유자가 보안 솔루션 공급자에 종속되지 않고, 보안 데이터를 능동적이고 효과적으로 접근하고 활용할 수 있도록 하기 위함



Amazon Security Lake 서비스 파트너
MegazoneCloud의 보안 데이터 활용 제안

MEGAZONE CLOUD

Issues

- 보안 데이터 활용에 있어서 여전히 대다수는
  보안 솔루션 공급자의 솔루션에 의존하여 활용하고 있음

- 전문 보안 솔루션을 도입하는 이유는
  솔루션 공급자의 노하우를 활용하기 위해서임

- 보안 이벤트 수집부터 활용까지
  전 과정에 걸친 전문가가 필요

MEGAZONE CLOUD

Amazon Security Lake Partners

- Amazon Security Lake를 활용하여 OCSF 규격의 보안 데이터 레이크 구축 공식 인증 프로그램으로, 영역에 따라 소스 파트너 / 구독 파트너 / 서비스 파트너로 구분

데이터 생성
· 정규화

Amazon Security Lake

데이터 활용
· 의사결정

소스 파트너

OCSF 형식으로 로그와 보안 이벤트를 Security Lake로 전송하는 역할

구독 파트너

위협 탐지, 조사 및 인시던트 대응과 같은 다양한 보안 사용 사례를 분석하고 해결하기 위한 서비스

서비스 파트너

OCSF 규격의 Security Lake 구축 및 활용을 위한 전반적인 기술지원 활동

MEGAZONE CLOUD

Amazon Security Lake Partners

소스 파트너

TREND MICRO
orca security
WIZ
okta
CYBERARK
paloalto NETWORKS
LACEWORK
uptycs
aqua
zscaler
netskope
CROWDSTRIKE
cisco SECURE
vmware
CONFLUENT
Gigamon
Trellix
ExtraHop
VECTRA
Barracuda
TANIUM
DARKTRACE
sentra
Falco
Ping Identity
SailPoint
Contrast SECURITY
torq
monad
CLAROTY
NETSCOUT
TALON
Laminar

구독 파트너

IBM
sumo logic
splunk>
RAPID7
securonix
elastic
DATADOG
new relic.
SentinelOne
SWIMLANE
STELLAR CYBER
Trellix
SOC PRIME
DEVO
RIPJAR
CHAOSSEARCH
tines
torq
wazuh.

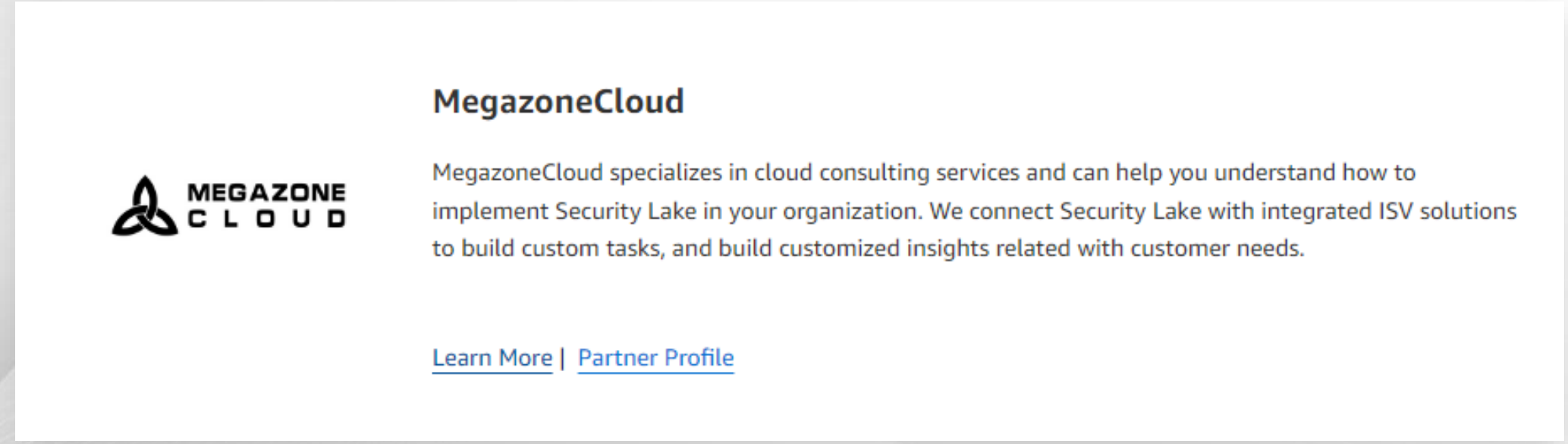
서비스 파트너

MEGAZONE CLOUD
accenture
Deloitte.
IBM
kyndryl
Infosys
pwc
leidos
Booz Allen
CMD
insbuild
Growing with the cloud
EVIDEN
SOC PRIME
DXC TECHNOLOGY
tcs
TATA CONSULTANCY SERVICES
wipro
HOOP cyber

MEGAZONE CLOUD

MegazoneCloud as ASL Service Partner

- Security Data Lake를 구축하고 활용을 지원하는 파트너
- MegazoneCloud는 국내 최초로 Amazon Security Lake의 Service Partner로 정식 인증 받음



출처 : https://www.megazone.com/us/amazon_security_lake/
https://aws.amazon.com/security-lake/partners/?nc1=h_ls

MegazoneCloud as ASL Service Partner

보안분석 역량 강화

AWS 클라우드 환경 내 데이터를 분석하고, 리소스, 애플리케이션 및 데이터에 대한 보호를 개선

가시성 확보

모든 AWS 계정과 리전에서 클라우드 보안 서비스와 3rd Party 솔루션에서 발생되는 다양한 데이터 가시성을 한 곳으로 집중

데이터 정규화

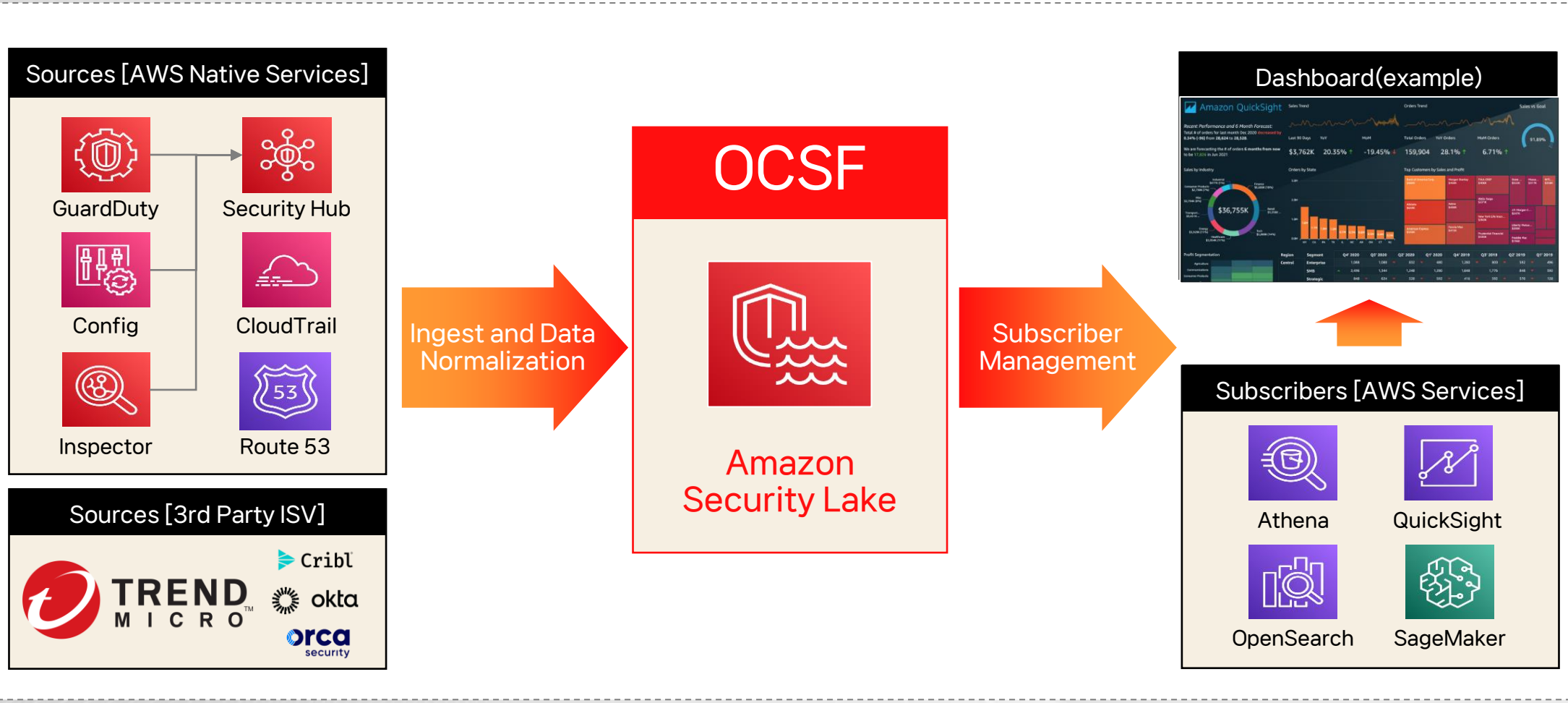
데이터를 개방적 표준으로 정규화하여 효율적으로 공유하고 다양한 분석 도구를 통해 광범위한 보안 소스 데이터를 결합

효율성

보안 데이터를 개선, 관리함에 따라 스토리지의 효율성과 데이터 쿼리 역량을 향상

MEGAZONE CLOUD

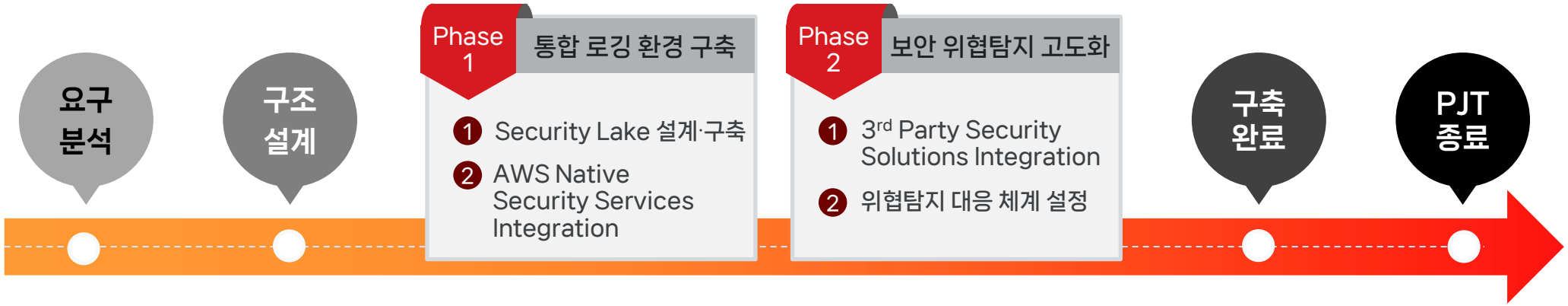
Workflow



MEGAZONE CLOUD

Consulting Services

Consulting 요구사항 분석·설계를 위한 컨설팅을 수행하고, 고객 목적에 따른 단계별 컨설팅 제공



Phase-1	Amazon Security Lake 환경을 설계하고 AWS Native 보안 서비스를 활용하여 보안 위협 탐지체계 구축
Phase-2	3rd Party 솔루션을 통해 리소스, 애플리케이션, 클라우드 환경에서 발생될 수 있는 다양한 위협탐지 대응 체계 구축

Implementation Services

계획 / 설계

1. 고객 요구사항 분석
2. Success Criteria 및 일정 수립
3. Log 대상 선정, 이벤트 뷰 설계
4. AWS 아키텍처 설계

AWS 인프라 구축

1. Security Lake 구성
2. Source Logs 수집
3. Subscriber Dash Board 구성

검증

1. 테스트 (모의해킹)
2. 대시보드 및 이벤트 알람 검증

프로젝트 종료

1. 구축 종료
2. 워크로드 내 보안 개선을 위한 Next Step 제시

MEGAZONE CLOUD

Benefits

Key Points

- 보안 데이터 소유의 주체 확보, 벤더 종속성 탈피
- 보안 솔루션 공급자 제공 기능의 일부를 이용하기 위한 과도한 금액 지출을 최소화

✓ 보안 가시성을 개선하고 위협대응 환경을 최소화

- OCSF(Open Cybersecurity Schema Framework), 단일화된 규격으로 변환/저장하여 데이터 분석 과정에서의 사일로를 제거
- 단일 리포지토리를 활용, 보안 로그 중앙 집중화를 통해 자체 맞춤형 보안 분석 플랫폼 체계 구축
- 워크로드 내 모든 리소스에서 발생되는 데이터 수집 및 저장 가능
- 보안 가시성 확보를 위해 다양한 Subscriber Tool 활용 가능

✓ 보안 거버넌스 및 침해사고 대응 체계 확보

- 다중 계정 환경과 3rd Party 보안 솔루션에서 발생되는 이벤트를 중앙에서 일관된 보안통제를 통해 거버넌스 체계 확보
- 로그 중앙 집중화를 통해 신속한 위협 대응
- 잠재적 위협 및 취약성 개선 적용을 통해 보안 위협 감소
- 사용자 인증, 인프라 보호, 데이터 보호, 통합 로깅 및 감사 역할을 구조화, 단순화하여 워크로드 확장성 확보

MEGAZONE CLOUD

Amazon Security Lake 활용 사례

MEGAZONE CLOUD

Use Case Scenario

- Web Application 공격과 Credential Stuffing 공격 탐지 시나리오를 통한 위협 대응

Case #1 웹 공격 실시간 탐지 및 전파

	정보수집	목표접근·공격
행위	IP/Port Scanning Attack	File/Shell Upload Attack
위협	순간 트래픽 상승	악성코드 감염
탐지방법	Network Traffic Trend	악성코드, 웹쉘 공격 이벤트
Source	VPC Flow Log	WAF, Inspector, GuardDuty **Trend Micro** Deep Security **Cribl:** Linux OS Logs
Subscriber	QuickSight, OpenSearch	QuickSight, OpenSearch

Case #2 계정 탈취 공격 실시간 탐지 및 전파

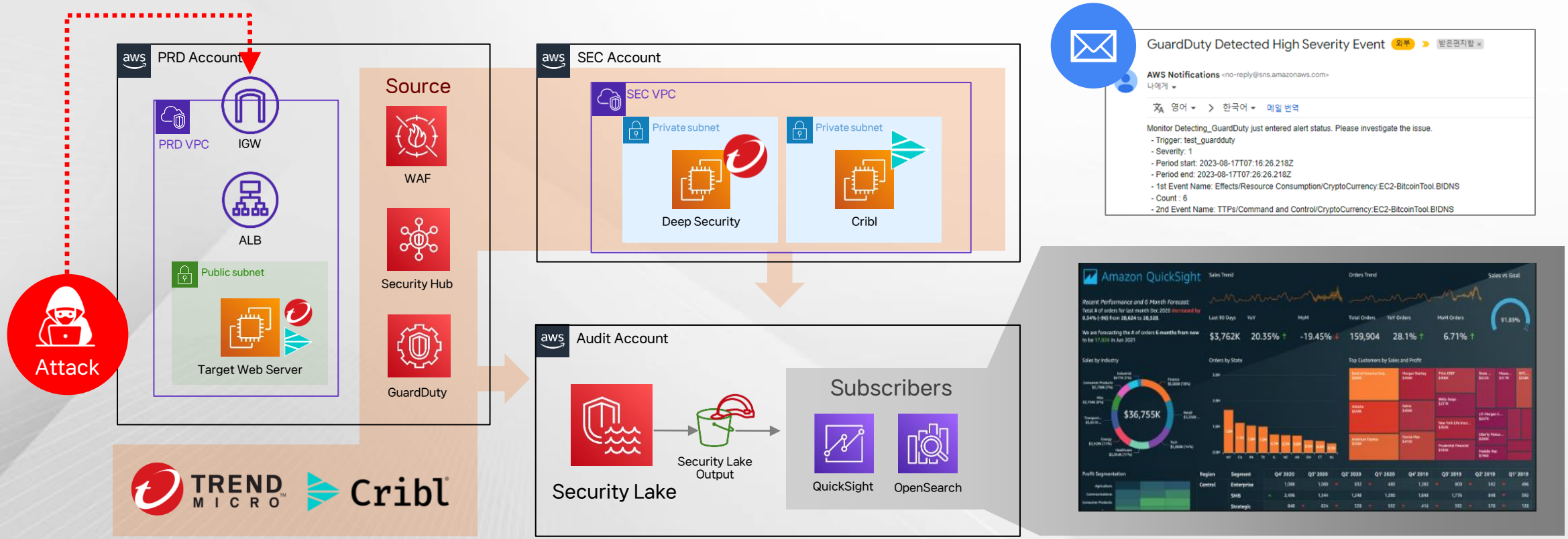
	정보수집	목표접근·공격
행위	Credential Key Exposure	AWS Workload Access
위협	자격 증명 노출	AWS 권한 탈취, 무단 사용
탐지방법	Key Access Error Count	비인가 IP 접근 이벤트 리소스 생성, 삭제 이벤트
Source	CloudTrail, Config **Orca Security**	CloudTrail **Orca Security**
Subscriber	QuickSight, OpenSearch	QuickSight, OpenSearch

MEGAZONE CLOUD

Use Case Scenario

Case #1 웹 서비스 공격 실시간 탐지 및 전파

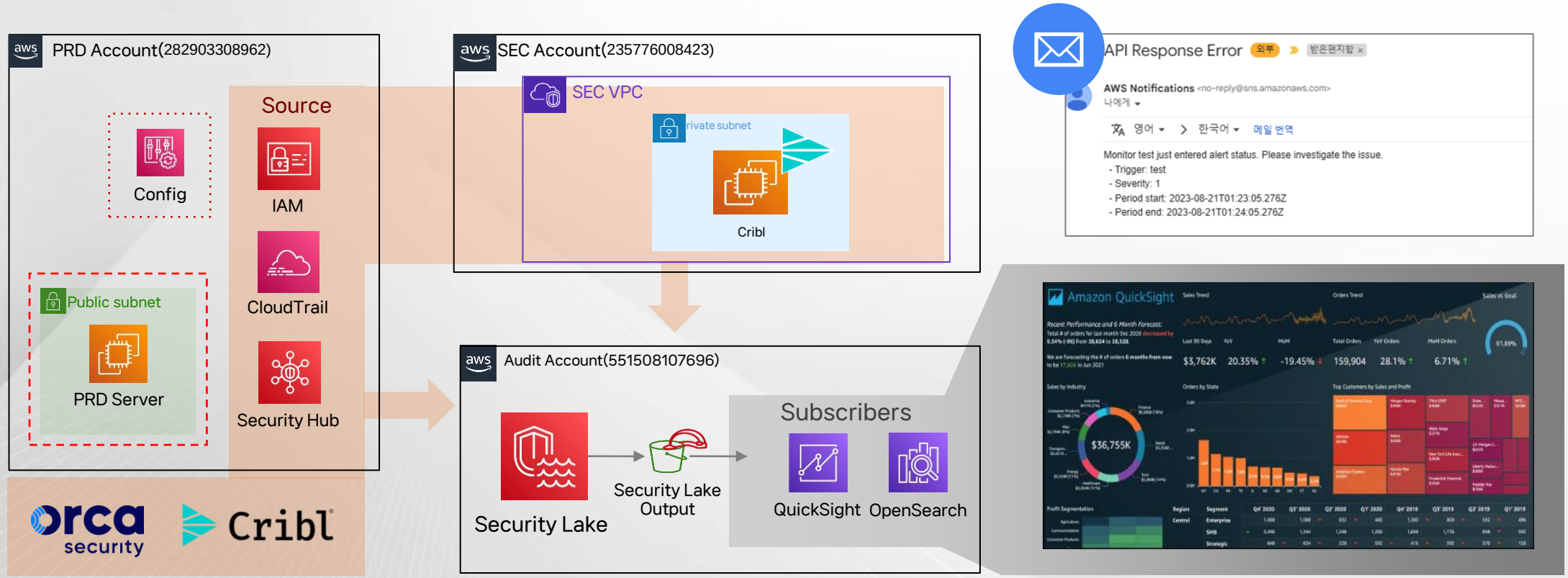
: 웹 서비스 보호 및 탐지를 위한 AWS Native Security 서비스와 3rd Party ISV 보안 솔루션 이벤트를 수신 후 QuickSight를 통한 분석과 상황 전파



Use Case Scenario

Case #2 계정 탈취 공격 실시간 탐지 및 전파

: 계정 탈취 공격 탐지를 위한 IAM과 AWS 이벤트 로그, CNAPP 등 전문적인 보안 솔루션의 이벤트 취합과 상관분석을 통한 위협 탐지 및 전파



MEGAZONE CLOUD

대표전화: 1644-2243

CNAPP/SECaaS 솔루션 문의: security@megazone.com