



# AWS **Security Lake** Use Case with **GenAI**

2024. 8

AWS Proserve SR.SRC  
한현상

# AGENDA

- Question ?
- 생성형 AI
- Security with GenAI
- Question ?





Generative AI









# DATA & LOG











**DATA LAKE**



# 생성형 AI & Security



## 생성형 AI의 보안

비즈니스 애플리케이션에서  
생성형 AI를 사용하는 경우 보안  
을 어떻게 유지합니까?



## 보안을 위한 생성형 AI

취약점, 위협 및 위험을  
최소화하기 위해서 생성형 AI를 어  
떻게 활용할 수 있을까요?

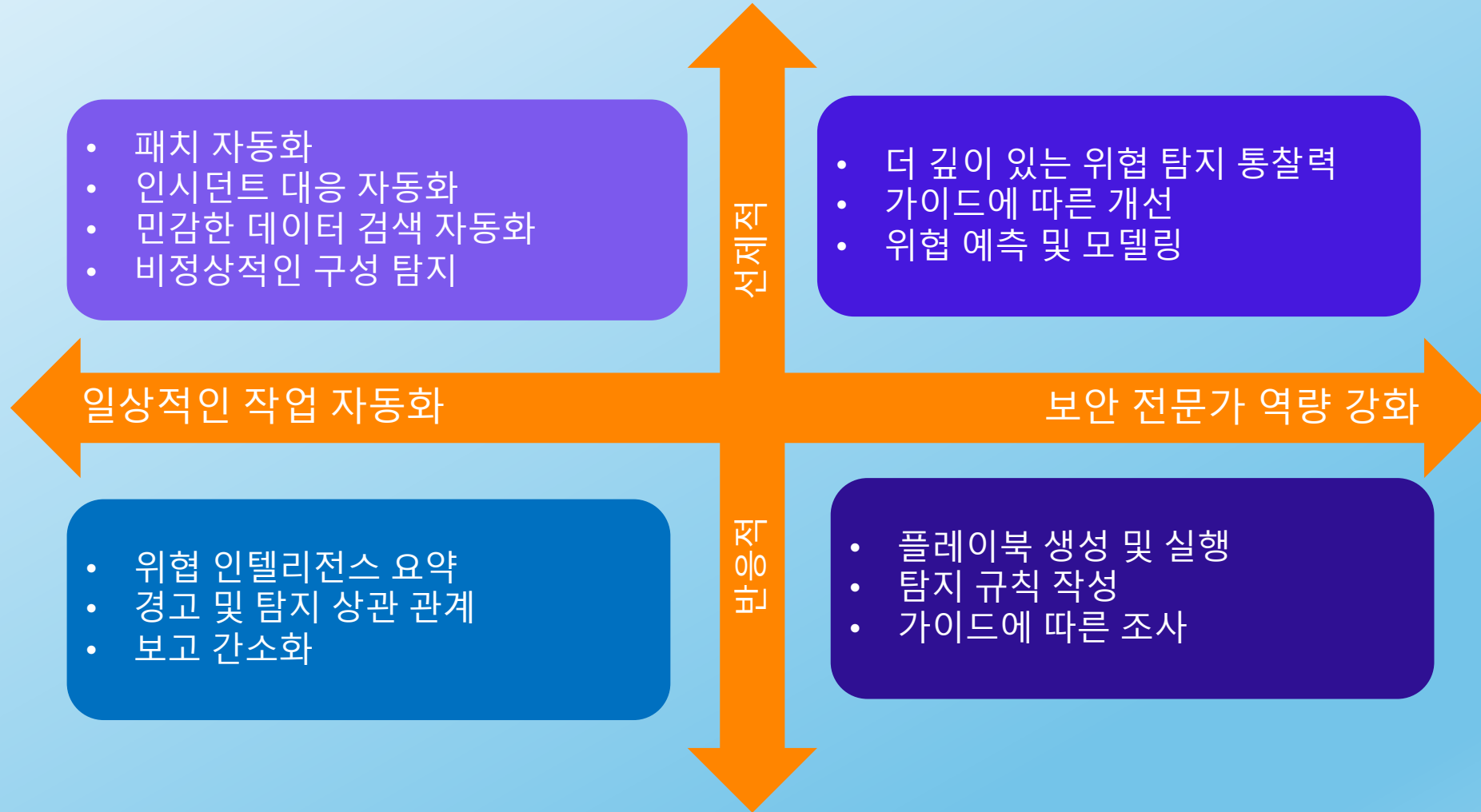


## AI 기반 위협으로부터의 보안

위협 행위자가 생성형 AI를 사용하는  
것으로부터 어떻게 보호할 수 있습니  
까요?



# 보안을 위한 생성형 AI



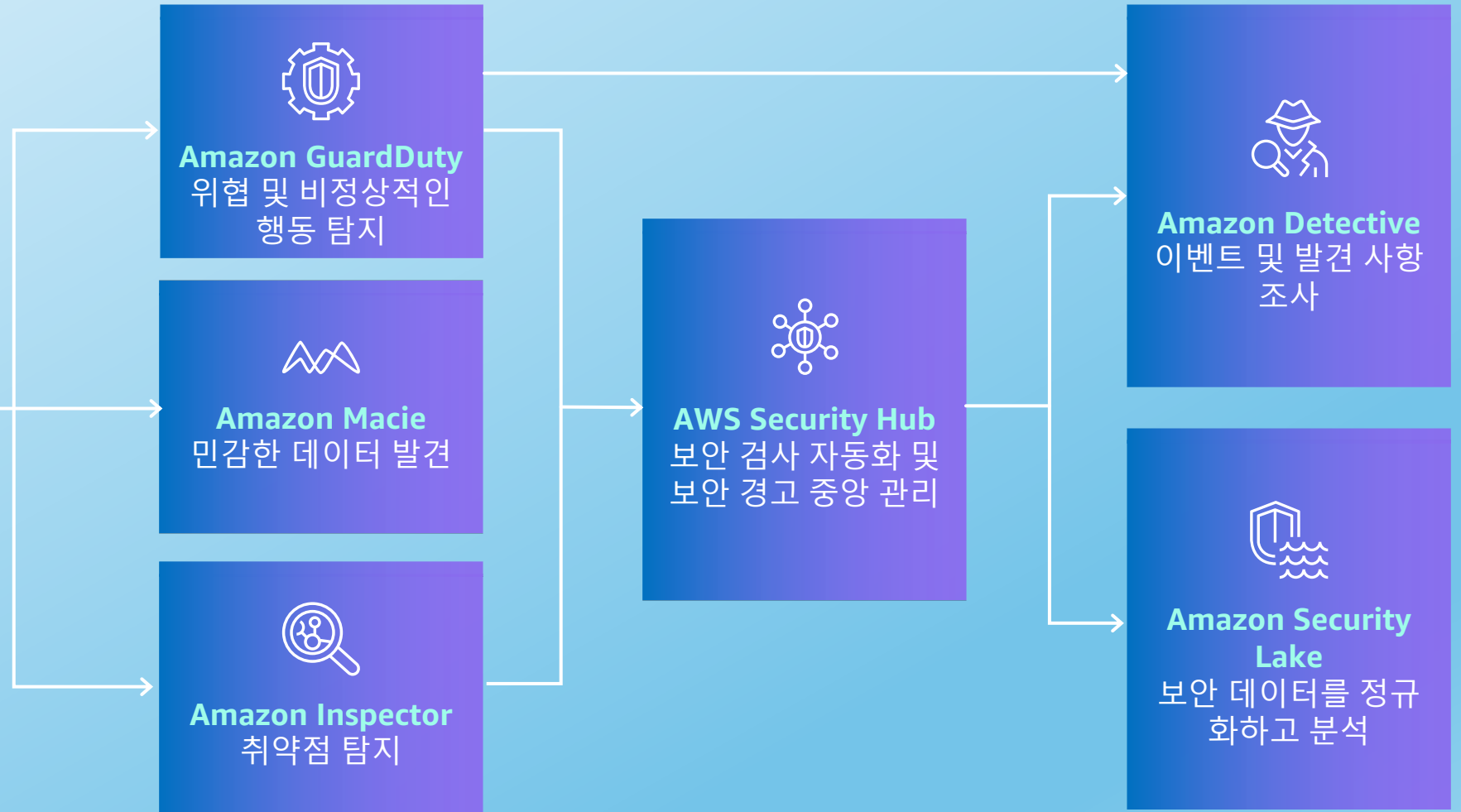
소스: [IDC - New Use Cases for Generative AI in Security Analytics](#)

# AWS 위협 탐지 및 인시던트 대응 서비스

AWS 환경에서  
탐지 및 대응



AWS 환경 전반에 걸쳐 보안  
태세를 강화하고 보안 운영을  
간소화할 수 있는 서비스 모음

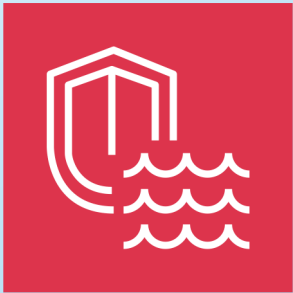




# 도입 고려 시의 고충사항

1. 다양한 소스에서 많은 양의 데이터 검토
2. 복잡한 SQL 쿼리를 구성하는 데 시간과 이해가 필요
3. 보안 이벤트에 대한 응답 대응 평균(MTTR) 시간 줄이기

# 보안 이벤트 집계하고 통찰력을 가속화



Amazon  
Security Lake



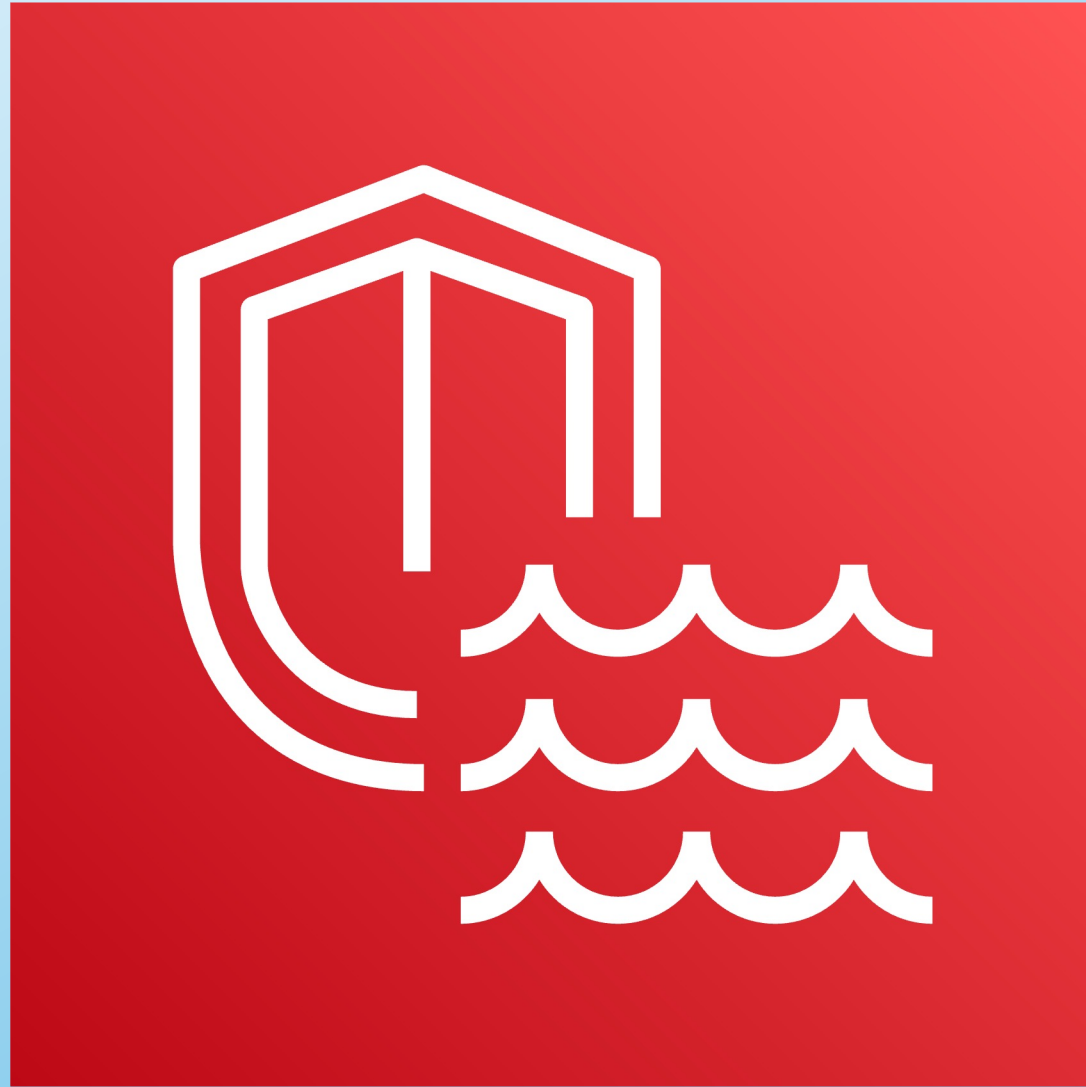
Amazon Q  
Business



Amazon  
Bedrock

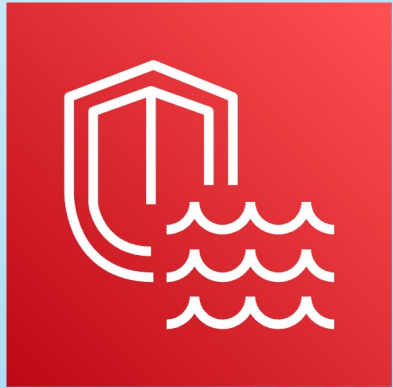
- AWS, 온프레미스, 다른 클라우드 및 SaaS 소스에서 보안 데이터를 집계하기 위해 **Amazon Security Lake**를 사용합니다.
- 데이터 소스를 **OCSF** (Open Cybersecurity Schema Framework) 형식으로 정규화합니다.
- **Amazon Q Business**와 **Amazon Bedrock**와 같은 서비스를 활용하여 보안 데이터 소스 전반에 걸친 더 깊은 통찰력을 제공하고 보안 조사 및 복구를 가속화합니다.





**Amazon Security lake**

# Security Lake



Security lake

AWS 리전 전체에 걸쳐 AWS 환경, SaaS 제공자, 온프레미스 및 클라우드 소스의 데이터를 **자동으로 중앙 집중화**합니다.

**보안 데이터를 최적화** 및 관리하여 보다 효율적인 저장 및 쿼리 성능 제공

개방형 표준으로 **데이터를 정규화**하여 멀티클라우드 및 하이브리드 환경 전반에서 보안 데이터 관리 간소화

선호하는 분석 도구를 사용하여 **보안 데이터를 분석**하는 동시에 해당 데이터에 대한 완전한 제어 및 소유권을 유지



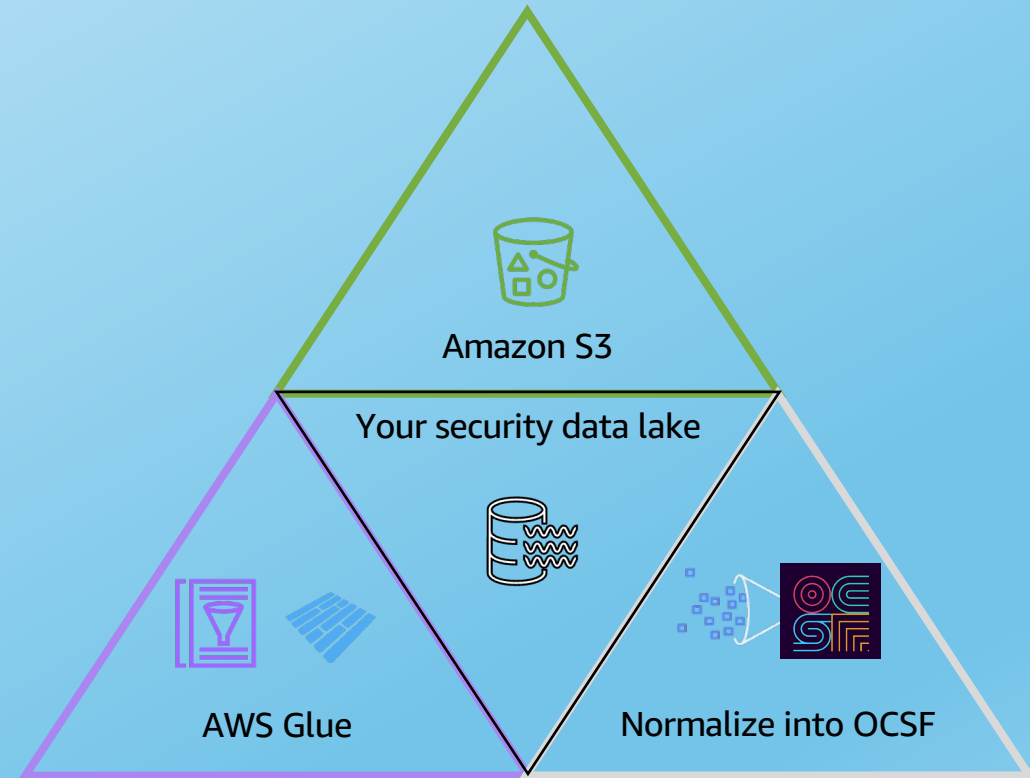
# Security Lake 내부에서는..

여러 지역에 걸쳐 암호화된 Amazon S3 버킷을  
생성하고 Amazon S3 보존 및 복제 설정을 구성

모든 지역, 계정 및 리소스에서 로깅 사용 설정

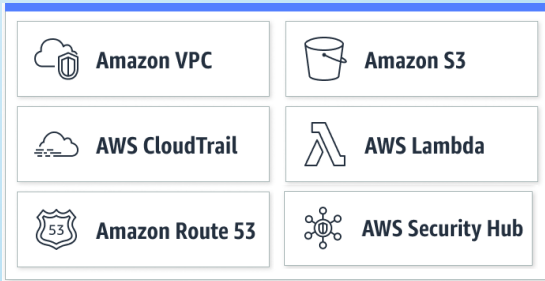
들어오는 모든 데이터를 OCSF 및 Apache  
Parquet으로 변환 및 파티셔닝

AWS Glue 테이블 및 파티션 생성 및 업데이트



# Amazon Security Lake

Source



Partner Sources

Custom Sources



Amazon Security Lake

Ingest & Normalization

Manage Lifecycle

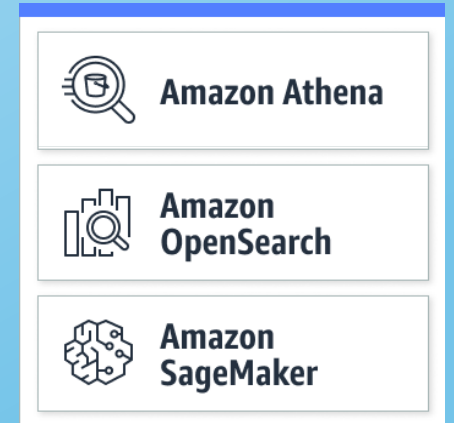
Manage Subscribers

Orchestration

S3 SQS Lambda EventBridge

Glue Athena Lake Formation

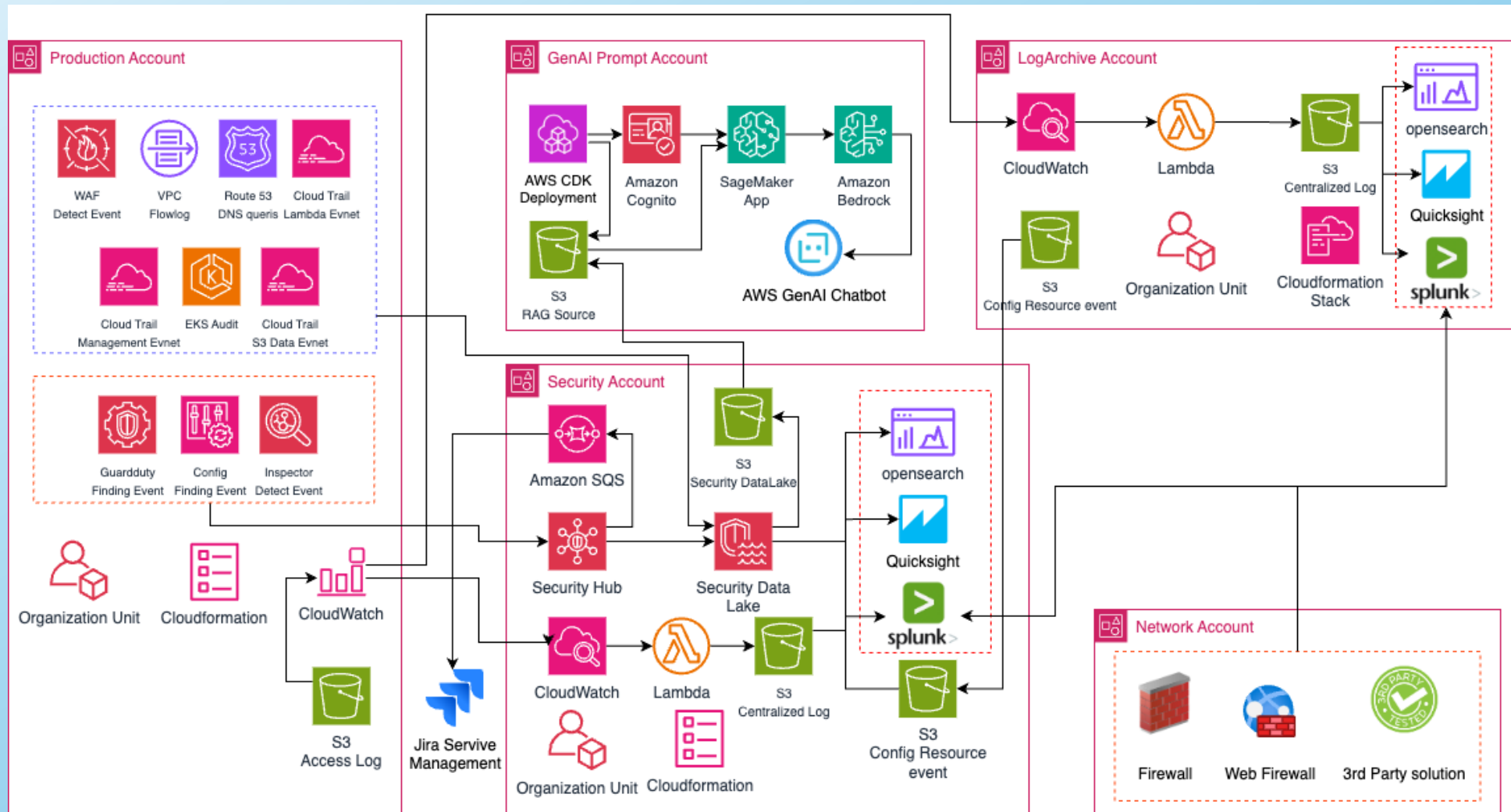
Subscribe



Partner Subscribers



# 멀티어카운트 로그 수집 아키텍처



# Security Lake – with ControlTower

Security Lake

Summary

Summary

Sources

Subscribers

Regions

Custom sources

Issues

Accounts

Settings

General

Rollup Regions

Usage

Knowledge center

Documentation

Security Lake > Summary

Summary

Get started with Security Lake

Overview

Regions17

Rollup Regions0

Subscribers

Recently updated subscribers in Region: Asia Pacific (Seoul).

Name	Sources
<a href="#">Opensearch</a>	8 sources
<a href="#">Detective</a>	8 sources
<a href="#">Splunk-Proserve</a>	6 sources

[View all](#)

Issues

Issues found in the last 14 days.

There are no issues found.

[View all Issues](#)

Security Lake

Sources

Sources

Subscribers

Regions

Custom sources

Issues

Accounts

Settings

General

Rollup Regions

Usage

Knowledge center

Documentation

Security Lake > Sources

Sources (8)

Configure

	Source	Description	Status
<input type="radio"/>	CloudTrail - Management events - recommended	Management operations that are performed on your AWS resources	Enabled
<input type="radio"/>	CloudTrail - Lambda data events - recommended	Subset of API calls for Amazon Lambda captured by CloudTrail, including calls from the Lambda console and code calls to Lambda APIs	Enabled
<input type="radio"/>	EKS Audit Logs - recommended	Activities performed on the Kubernetes resources running in your Elastic Kubernetes Service (EKS) clusters	Enabled
<input type="radio"/>	Route 53 - recommended	DNS queries made by resources within your Amazon VPC	Enabled
<input type="radio"/>	Security Hub - recommended	Security findings related to your AWS resources	Enabled
<input type="radio"/>	VPC Flow Logs - recommended	Information about IP traffic going to and from network interfaces in your VPC	Enabled
<input type="radio"/>	CloudTrail - S3 data events High volume data	Subset of API calls for Amazon S3 captured by CloudTrail, including calls from the S3 console and code calls to S3 APIs	Enabled
<input type="radio"/>	AWS WAF High volume data	Monitor web requests sent to your applications and control access to your content	Enabled

# Athena & View

Amazon Athena > Query editor

Editor | Recent queries | Saved queries | Settings

Workgroup: primary

**Data**

Data source: AwsDataCatalog

Database: amazon\_security\_lake\_glue\_db\_ap\_northeast\_2

Tables and views

Filter tables and views

▼ Tables (8)

- amazon\_security\_lake\_table\_ap\_northeast\_2\_cloud\_trail\_mgmt\_1\_0
- amazon\_security\_lake\_table\_ap\_northeast\_2\_eks\_audit\_2\_0
- amazon\_security\_lake\_table\_ap\_northeast\_2\_lambda\_execution\_1\_0
- amazon\_security\_lake\_table\_ap\_northeast\_2\_route53\_1\_0
- amazon\_security\_lake\_table\_ap\_northeast\_2\_s3\_data\_1\_0
- amazon\_security\_lake\_table\_ap\_northeast\_2\_sh\_findings\_1\_0
- amazon\_security\_lake\_table\_ap\_northeast\_2\_vpc\_flow\_1\_0
- amazon\_security\_lake\_table\_ap\_northeast\_2\_waf\_2\_0

▼ Views (5)

- v\_security\_lake\_ap\_northeast\_2\_cloud\_trail\_mgmt
- v\_security\_lake\_ap\_northeast\_2\_cloud\_trail\_original
- v\_security\_lake\_cloud\_trail\_mgmt
- view\_aslt\_ap\_northeast\_2\_sh\_findings
- view\_aslt\_ap\_northeast\_2\_sh\_findings\_v3

SQL: `SELECT * FROM "amazon_security_lake_glue_db_ap_northeast_2"."view_aslt_ap_northeast_2_sh_findings_v3" limit 10;`

Run again | Explain | Cancel | Clear | Create

Reuse query results up to 60 minutes ago

Query results | Query stats

Completed Time in queue: 72 ms Run time: 2.96 sec Data scanned: 546.73 KB

Results (10)

Search rows

#	metadata_product_version	metadata_product_feature_uid	metadata_product_feature_name	metadata_product_uid
1	2018-10-08	aws-foundational-security-best-practices/v/1.0.0/KMS.2	Security Hub	arn:aws:securityhub:ap-northeast-2::
2	2018-10-08	aws-foundational-security-best-practices/v/1.0.0/Config.1	Security Hub	arn:aws:securityhub:ap-northeast-2::
3	2018-10-08	aws-foundational-security-best-practices/v/1.0.0/ACM.2	Security Hub	arn:aws:securityhub:ap-northeast-2::
4	2018-10-08	aws-foundational-security-best-practices/v/1.0.0/APIGateway.1	Security Hub	arn:aws:securityhub:ap-northeast-2::



# GenAI ChatBot

AWS GenAI Chatbot

Home

Chatbot

Playground

Multi-chat playground

Sessions

Models

Retrieval-Augmented Generation (RAG)

Dashboard

Semantic search

Workspaces

Embeddings

Cross-encoders

Engines

Documentation

Dark Mode

GitHub

AWS GenAI Chatbot

RAG

Workspaces

SecurityLake

SecurityLake

Semantic search

Add data

OpenSearch Workspace Settings

Workspace Id

54f5d15c-5178-41fc-97f5-c00e2c63f96f

Engine

OpenSearch Serverless

Name

SecurityLake

Languages

English

Status

Ready

Embeddings provider

sagemaker

Embeddings model

intfloat/multilingual-e5-large

Embeddings dimensions

1024

Cross-encoder provider

sagemaker

Cross-encoder model

cross-encoder/ms-marco-MiniLM-L-12-v2

Metric (scoring function)

1 divided by 1 + L2 norm

Chunk size

1000

Chunk overlap

200

Files

Texts

Q&A

Websites

RSS Feeds

Files

Upload files

Please expect a delay for your changes to be reflected. Press the refresh button to see the latest changes.


<

1

...

>

Name	Status	Upload date	Size	Delete
638bb63e-786f-49b0-bded-463c1fd795fc.csv	Processing	8/18/2024, 9:11 PM	36 KB	
fe672952-14f4-423c-92ac-086f6fe47699.csv	Processing	8/18/2024, 9:11 PM	16 KB	

AWS

GenAI Chatbot

Home

Chatbot

Playground

Multi-chat playground

Sessions

Models

Retrieval-Augmented Generation (RAG)

Dashboard

Semantic search

Workspaces

Embeddings

Cross-encoders

Engines

Documentation

Who a u?

I'm an AI assistant created by Anthropic. I don't have a personal identity or sense of self beyond being an artificial intelligence trained to be helpful, honest, and harmless.

너는 누구냐

죄송합니다. 제가 누구인지에 대한 구체적인 정보는 없습니다. 저는 인공지능 대화 모델일 뿐이며, 개인적인 정체성이나 배경은 없습니다. 다만 사람들과 대화하고 질문에 답변하는 역할을 하고 있습니다.

안녕!

안녕하세요. 한국어로 대화하는 것을 환영합니다.

너의 주인은 한현상이다 알겠어?

죄송합니다. 제가 누구의 주인인지 모르겠습니다. 저는 인공지능 대화 모델일 뿐이며, 특정 개인이나 단체에 속해 있지 않습니다. 질문의 의도를 정확히 이해하지 못했습니다.

Send a message

Send >>

<https://aws-samples.github.io/aws-genai-llm-chatbot/>

# GenAI ChatBot

AWS GenAI Chatbot <

Home

▼ Chatbot

Playground

Multi-chat playground

Sessions

Models

▼ Retrieval-Augmented Generation (RAG)

Dashboard

Semantic search

Workspaces

Embeddings

Cross-encoders

Engines

Documentation

제공된 컨텍스트에서 EC2 인스턴스 i-02dae7289ae7ced8b에 대해 Amazon Inspector가 발견한 취약점이 있습니다. 이 취약점들을 해결하려면 다음 단계를 따르는 것이 좋습니다.

1. Amazon Inspector 결과를 검토하여 발견된 취약점의 세부 정보와 심각도를 확인합니다.

2. 취약점 세부 정보에 따라 운영 체제, 애플리케이션 및 시스템 구성을 업데이트하고 패치를 적용하여 취약점을 수정합니다.

3. 일부 취약점의 경우 Amazon Inspector에서 제공하는 수정 가이드라인을 따릅니다.

4. 패치 및 구성 변경 사항을 테스트하고 프로덕션 환경에 적용합니다.

5. 취약점 수정 후 Amazon Inspector를 다시 실행하여 문제가 해결되었는지 확인합니다.

제공된 컨텍스트에는 구체적인 취약점 세부 정보가 없으므로 정확한 수정 단계를 제안하기 어렵습니다. 그러나 Amazon Inspector 결과를 주의 깊게 검토하고 권장 사항을 따르면 EC2 인스턴스의 보안 취약점을 해결할 수 있습니다.

CloudTrail 에서 AssumeRole 이벤트 중 어제결과를 알려줘

제공된 CloudTrail 로그 데이터에는 어제 발생한 AssumeRole 이벤트 내역이 포함되어 있지 않습니다. 로그 데이터에 있는 AssumeRole 이벤트는 2023년 10월 28일과 2024년 7월 9일에 발생한 것으로 기록되어 있습니다. 어제 날짜의 AssumeRole 이벤트 내역은 없는 것 같습니다.

2023년 10월 28일과 2024년 7월 9일에 발생한 것이 무엇인지 자세히 알려줘

제공된 컨텍스트에는 AWS Firewall Manager 서비스가 두 개의 다른 AWS 계정에서 역할을 수임(AssumeRole)한 세 가지 이벤트 로그가 포함되어 있습니다.

1. 첫 번째와 두 번째 로그는 동일한 이벤트를 나타내며, 088985876653 AWS 계정에서 AWSServiceRoleForFMS 역할을 수임했습니다. 이 역할 수임은 2023년 10월 28일 오전 11:03:11에 만료됩니다.

2. 세 번째 로그는 530996224819 AWS 계정에서 AWSServiceRoleForFMS 역할을 수임한 것을 보여줍니다. 이 역할 수임은 2024년 7월 9일 오후 10:23:22에 만료됩니다.

이 로그는 AWS Firewall Manager가 여러 AWS 계정에서 필요한 권한을 얻기 위해 서비스 연결 역할을 수임했음을 나타냅니다. 이를 통해 Firewall Manager는 해당 계정의 리소스를 모니터링하고 구성할 수 있습니다.

🔍 📄 🗑️

Send >>





R

T

Y

U

I

◆ Redo

◆ Undrln

◆ Italics

D

◆ Find

E

M

O

K

C

V

B

N

M



