AWSKRUG

KRUG Security Meetup

Security Lake & Monitoring

ProServe Sr. SRC 한현상

23. 10. 19

Table of contents

AWSKRUG

WHAT ...the

What is for what ?

AWSKRUG

About me

- **Professional Service Team** > Sr.Security Risk & Compliance
- Until 3 years, 7 months, …few days
- Project – Landingzone, Controltower, Enhanced Security, Partner enablement, Public enablement, DW, Well Architecture Framwork, App Modernization, AWS Speaker 2, Mobilization, AWS CIRT,
- In my charge – Security, Network, Compliance, IAC, Automation, SOAR, APJC Security AOD Mentor
- Co-working, Hard-worker, Security Mentor, 도마뱀 아빠

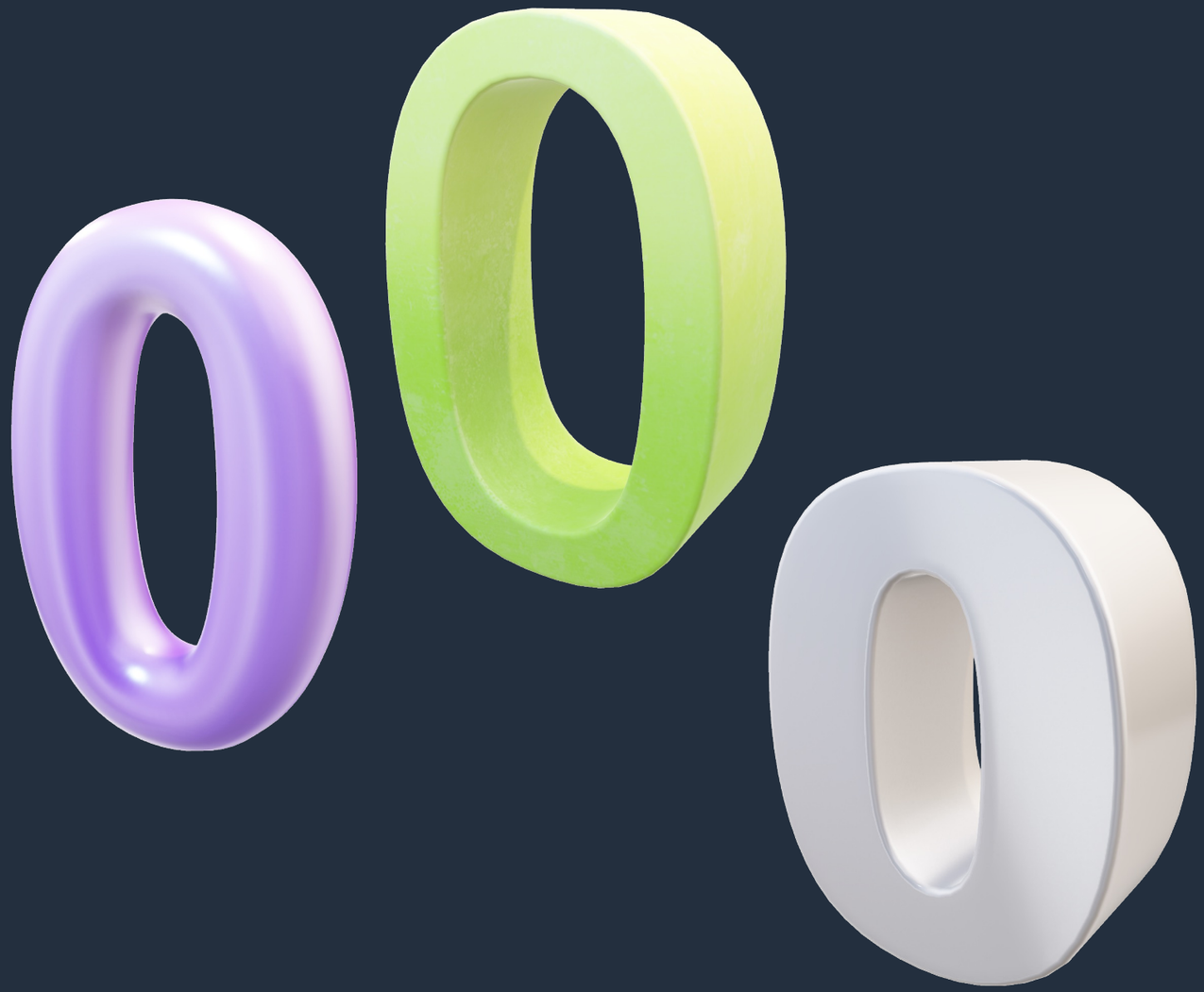
AWSKRUG


WHY
ARE
WE
HERE?

At AWS, cloud security is job zero.

모든 AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누리고 있습니다.

잡 제로가 ...



AWSKRUG

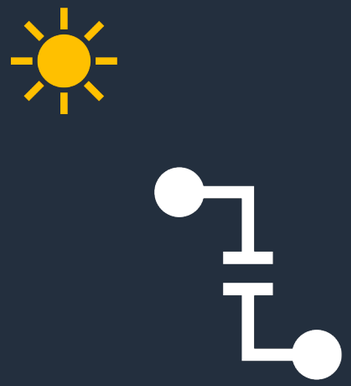
Security Information

Security Information

보안에 투자되는 회사의 예산은 어떠 한가요?

보통 IT 예산의 **10%**

Security Lake...



일관되지 않고 불완전한 데이터

다양한 형식의 로그와 알림이 찾기 어려운 데이터 사일로에 조직 전체에 흩어져 있습니다.

증가하는 보안 데이터의 양

대량의 보안 및 로그 데이터는 실제 분석보다 데이터 관리에 더 많은 시간이 소요된다는 것을 의미합니다.

사용 사례 전반에서 데이터의 비효율적 사용

각 사용 사례마다 전문화된 도구가 필요해 데이터 중복 및 재처리가 발생할 수 있습니다.

처리된 데이터를 직접 제어할 수 없음

특정 도구는 처리된 데이터를 자체 시스템에 저장하기 때문에 데이터 사용의 유연성이 떨어집니다.

AWSKRUG

Security Lake...

Analyze multiple years of security data quickly

S3 버킷을 이용하여 보안에 대한 분석을 가속화하고 도구로 활용

Simplify your compliance monitoring and reporting

로깅을 중앙집중화하고 규정 준수에 대하여 모니터링 하고 리포팅

Facilitate your security investigations with elevated visibility

보안 팀을 위한 사고 조사를 지원하고 신속하게 대응하도록 데이터를 제공

Unify security data management across hybrid environments

보안에 관련된 운영을 고도화하고 데이터를 효과적으로 활용할 수 있도록 지원

Security Lake ..

보안 데이터를 특정 목적에 맞게 구축된 데이터 레이크로 자동 중앙 집중화

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

AWSKRUG

Security Lake 가 왜 필요할까요?

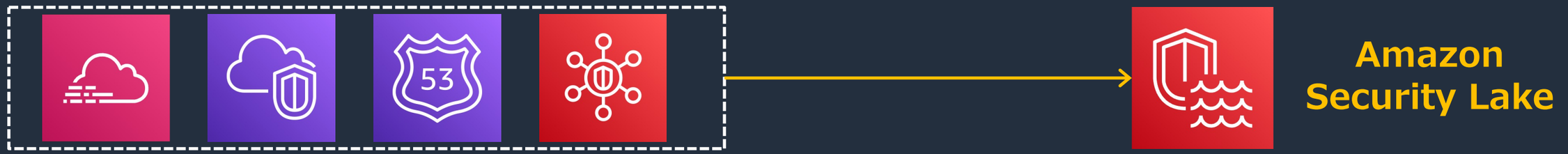
몇 단계만 거치면 보안 데이터를 전용 보안 데이터 레이크에 자동으로 수집

AWS CloudTrail, Amazon S3, AWS Lambda, Amazon VPC 및 Amazon Route 53에서 AWS 로그를 수집하고 정규화

데이터 레이크에 사용자 정의 로그 및 보안 데이터 추가 가능

AWSKRUG

Security Lake 수집 데이터



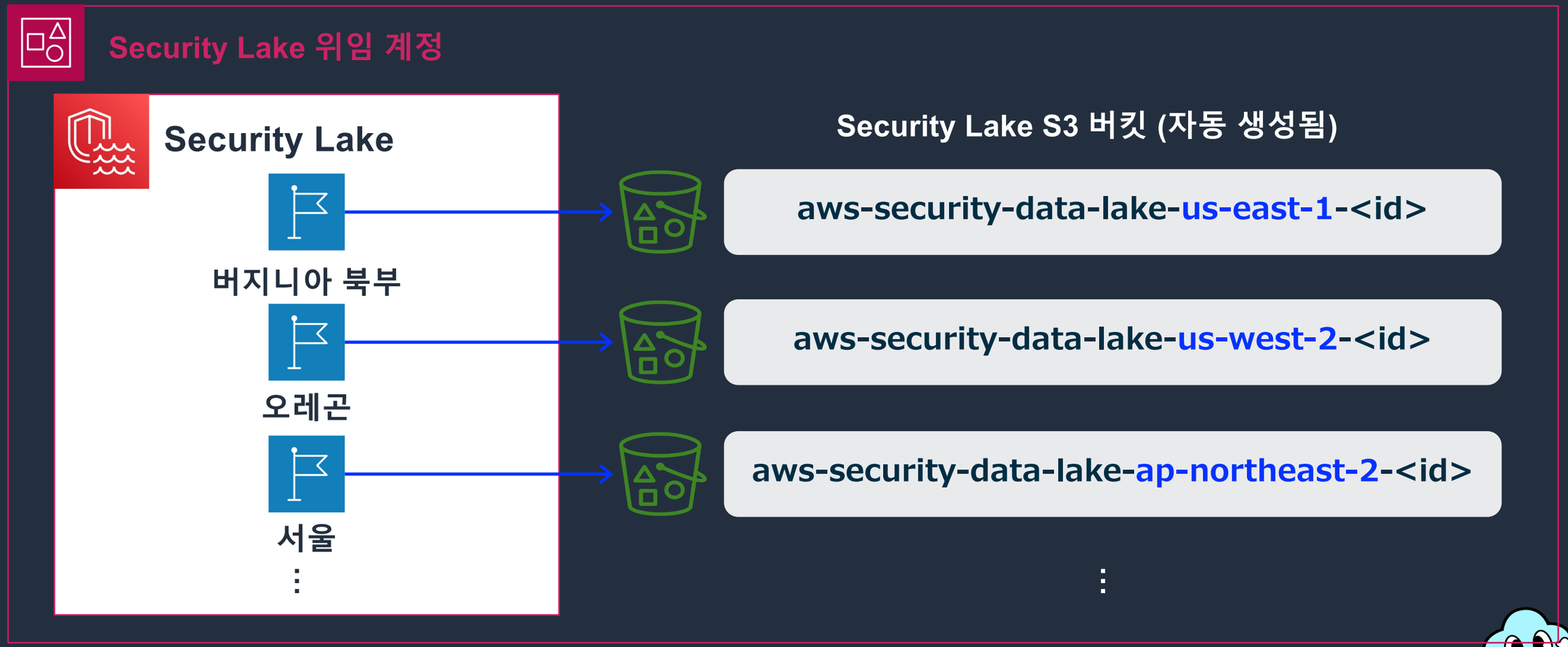
기본 지원되는 AWS 서비스

#	AWS 서비스	metadata.product.name 필드값
1	AWS CloudTrail (관리/데이터 이벤트)	"CloudTrail"
2	Amazon VPC 플로우 로그	"Amazon VPC"
3	Route 53 쿼리 로그	"Route 53"
4	AWS Security Hub 이벤트 (ASFF 포맷)	"Security Hub"

AWSKRUG

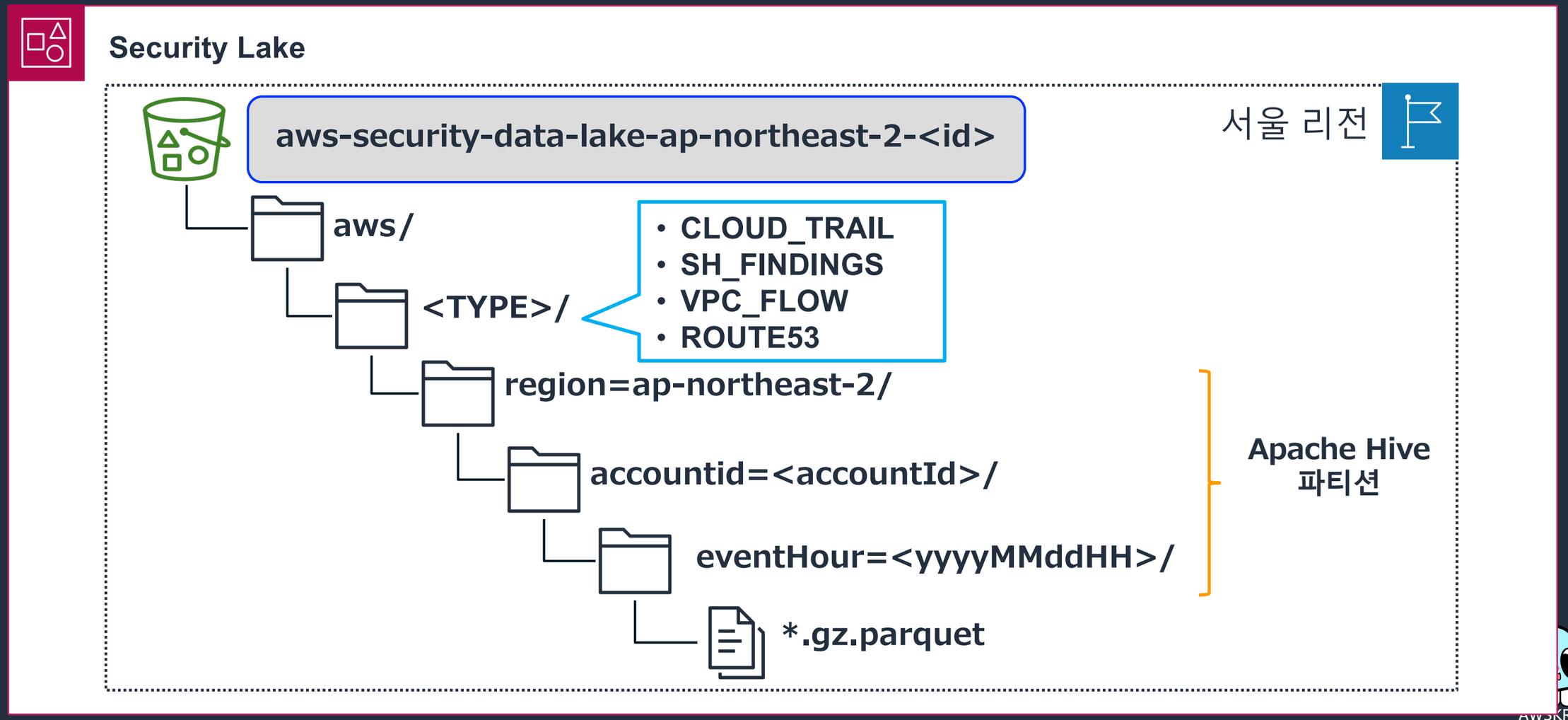
Security Lake - 데이터 레이크용 S3 버킷

"대상 지역"의 설정에 따라 Security Lake는 미리 결정된 이름을 사용하며, 위임 계정의 각 리전에 대한 S3 버킷 자동 생성



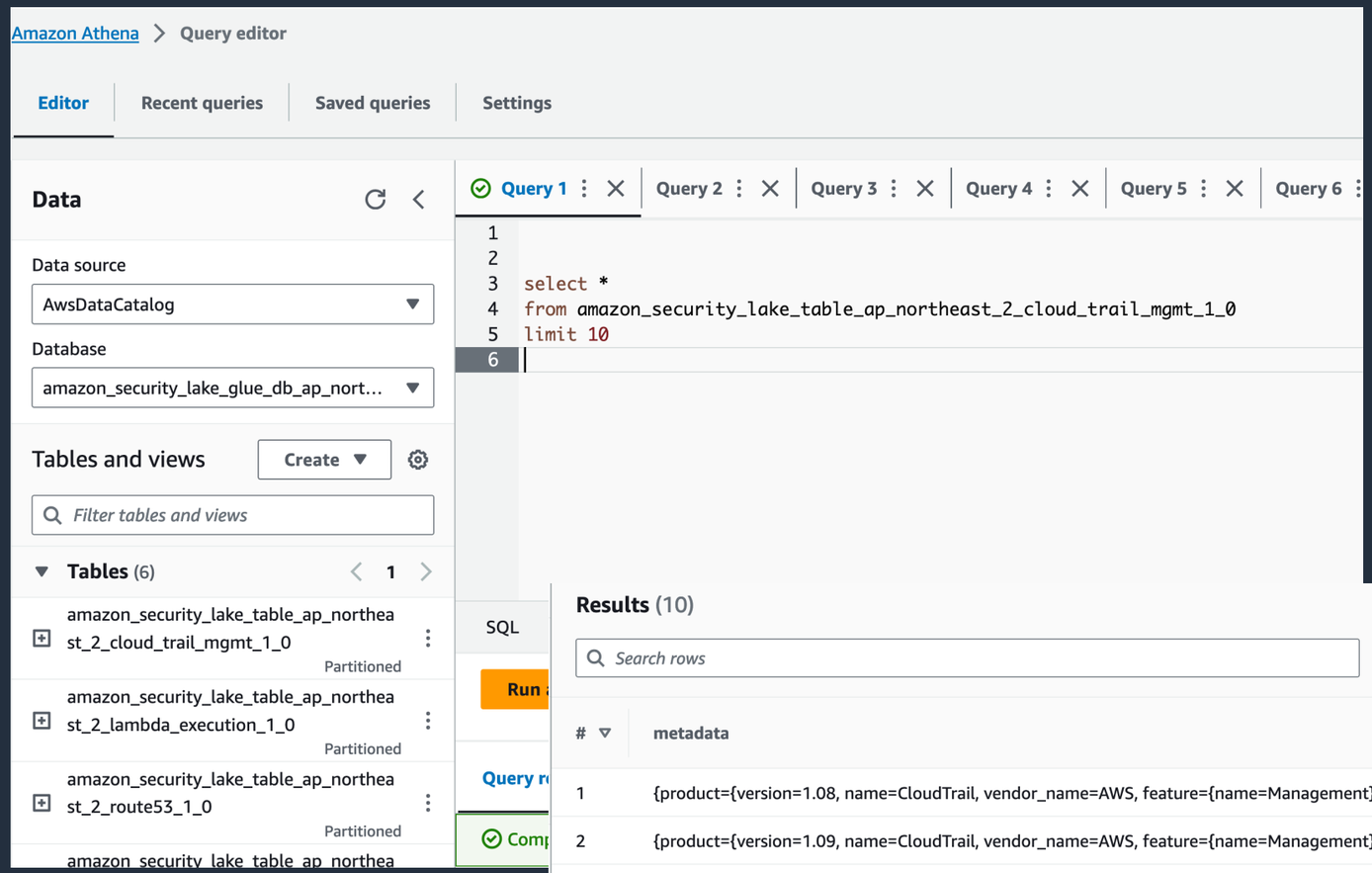
Security Lake S3 버킷 폴더 구조

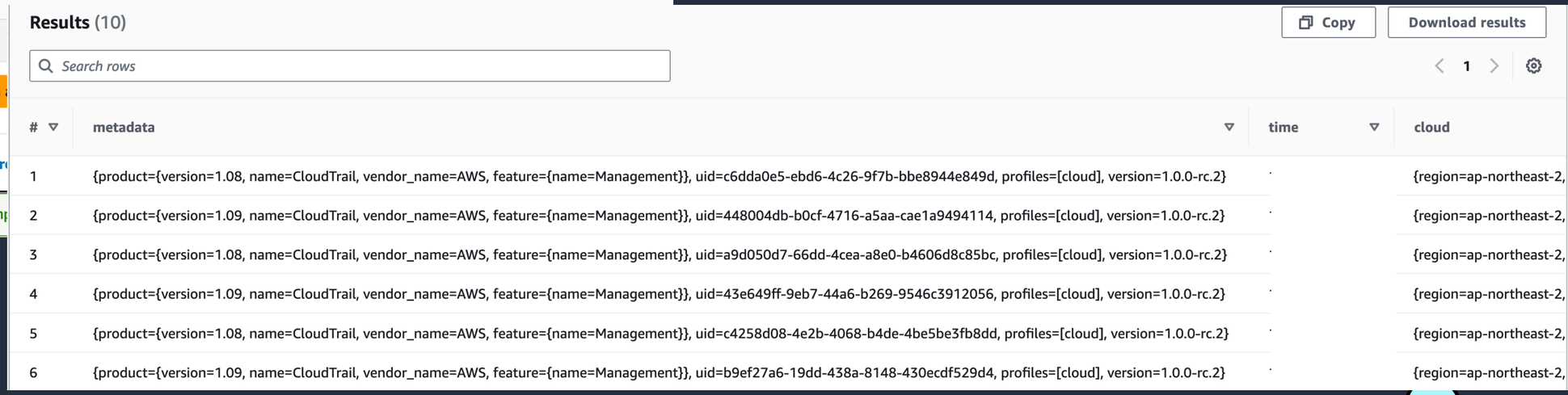
사전 정의된 폴더 구조를 가지고 있고 gzip 으로 압축된 Parquet 파일로 아래 구조 저장



데이터에 대해 바로 조회

Amazon Athena





AWSKRUG

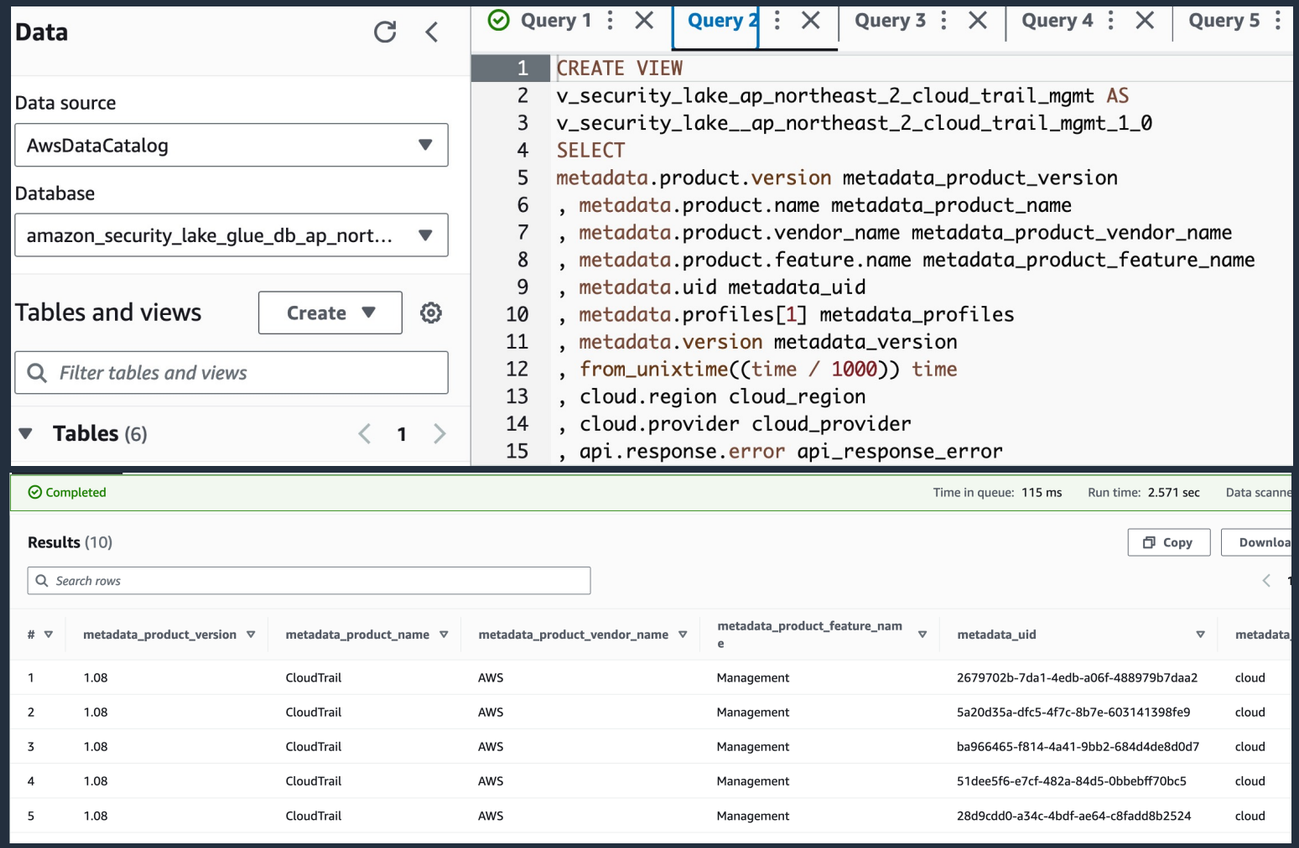
Next..

{"version":"0","id":"9a080879-27c3-1d22-c300-25a01750b945","detail-type":"Security Hub Findings - Imported","source":"aws.securityhub","account"[redacted],"time":"2023-10-09T23:13:39Z","region":"ap-northeast-2","resources":["arn:aws:securityhub:ap-northeast-2::product/aws/inspector/arn:aws:inspector2:ap-northeast-[redacted]:finding/37efdef71ce47472805e93523601cd9f"],"detail":{"findings":[{"ProductArn":"arn:aws:securityhub:ap-northeast-2::product/aws/inspector","Types":["Software and Configuration Checks/Vulnerabilities/CVE"],"Description":"The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a \"Sweet32\" attack.","ProductName":"Inspector","FirstObservedAt":"2023-06-03T07:57:28Z","CreatedAt":"2023-06-03T07:57:28Z","LastObservedAt":"2023-10-09T23:13:10Z","Vulnerabilities":[{"ReferenceUrls":["https://access.redhat.com/errata/RHSA-2020:0451","https://www.oracle.com/security-alerts/cpuapr2020.html","https://kc.mcafee.com/corporate/index?page=content&id=SB10310","https://access.redhat.com/errata/RHSA-2017:3240","https://support.f5.com/csp/article/K13167034","https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html","https://kc.mcafee.com/corporate/index?page=content&id=SB10197","https://www.oracle.com/security-alerts/cpuoct2020.html","https://wiki.opendaylight.org/view/Security_Advisories","https://kc.mcafee.com/corporate/index?page=content&id=SB10171","https://www.ietf.org/mail-archive/web/tls/current/msg04560.html","https://access.redhat.com/articles/2548661","https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02","https://access.redhat.com/errata/RHSA-2017:3239","https://access.redhat.com/errata/RHSA-2017:1216","https://security.gentoo.org/glsa/201612-16","https://access.redhat.com/errata/RHSA-2017:2708","https://www.oracle.com/security-alerts/cpujul2020.html","https://security.gentoo.org/glsa/201707-01","https://www.sigsac.org/ccs/CCS2016/accepted-papers/","https://www.openssl.org/blog/blog/2016/08/24/sweet32/","https://access.redhat.com/errata/RHSA-2017:2709","https://access.redhat.com/errata/RHSA-2018:2123","https://www.oracle.com/security-

AWSKRUG

DashBoard - 정규화

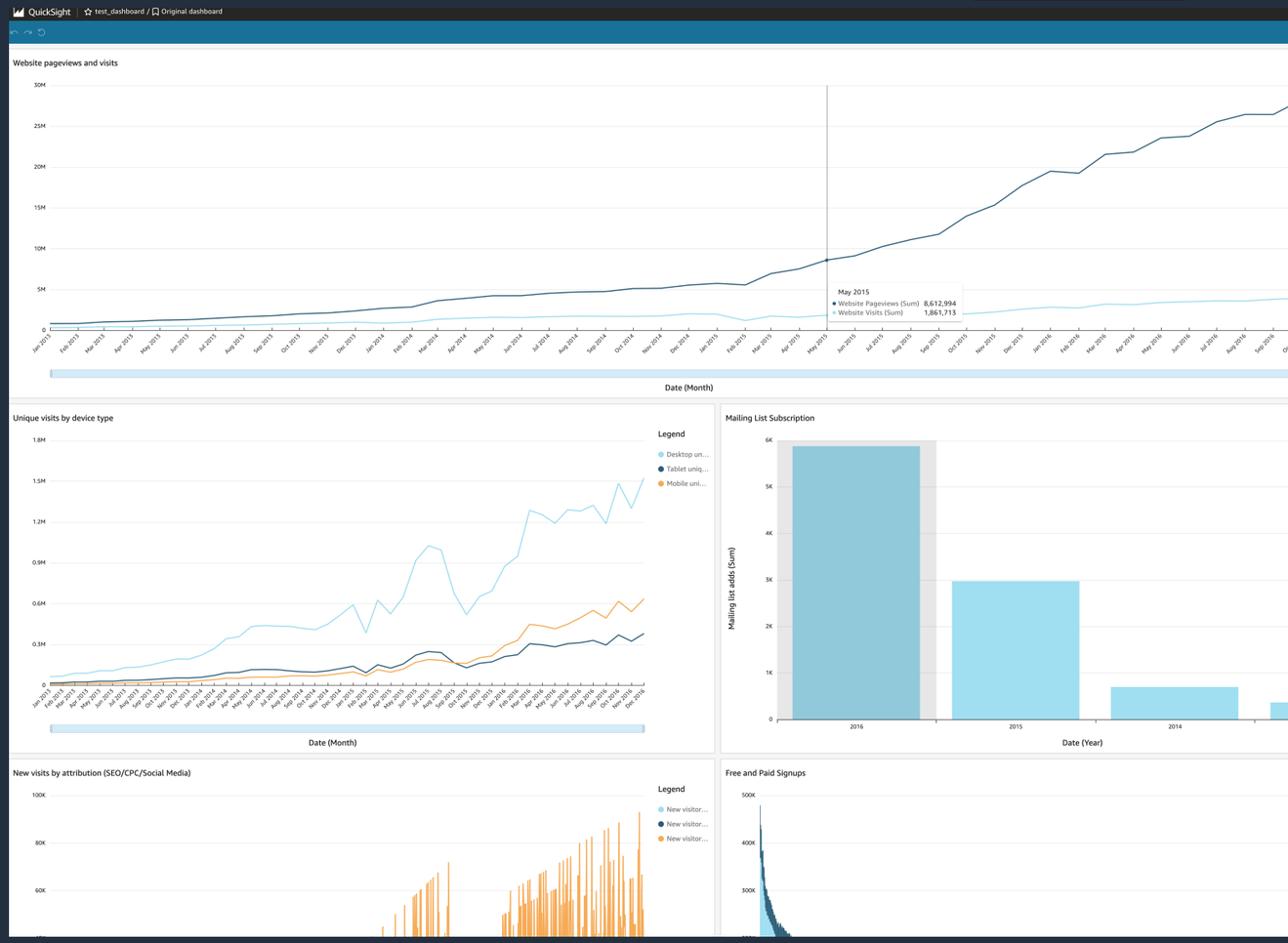
- 데이터 정규화 필요
  - Security lake 의 데이터를 직접 쿼리는 비 효율적
  - 각 필드를 대시보드 요건을 위한 슬라이스 작업 필요
- 데이터 시각화 필요
  - 비용 효율적 대시보드 요건 정의
  - Native 솔루션으로 시작



AWSKRUG

DashBoard - 대시보드

- Quick Sight 활용
  - Per Month 단돈 **12 딸라(Per User)**
  - 쿼리를 위한 **SPICE** 기능 사용 시 10GB 무료, 이후 **0.25 USD/GB**
- 대시보드 구성
  - 데이터 소스
    - Athena Table View 로 준비
  - 데이터 셋
    - Spice 10G 준비
  - Analysis
    - 대시보드 구성
  - 대시보드 완성
    - 퍼블리싱



AWSKRUG

Demo

Q&A

Hyeonsang Han
Preserve. Sr. Security Consultant

AWSKRUG