



리소스 구성 시각화 CSPM on AWS

What's in my Cloud?

한태경(taekyung@)
Solutions Architect
AWS

"클라우드 보안사고의 99%는
운영자의 설정오류로 발생할 것"

가트너, IT 리서치

클라우드 운영/보안의 많은 고민들

WHAT ARE YOUR CHALLENGES

우리가 사용하는 서비스가
뭐가 있지?

개발자가 클라우드 구성을
변경했나?

현재 설정이 컴플라이언스를
만족하고 있단가??

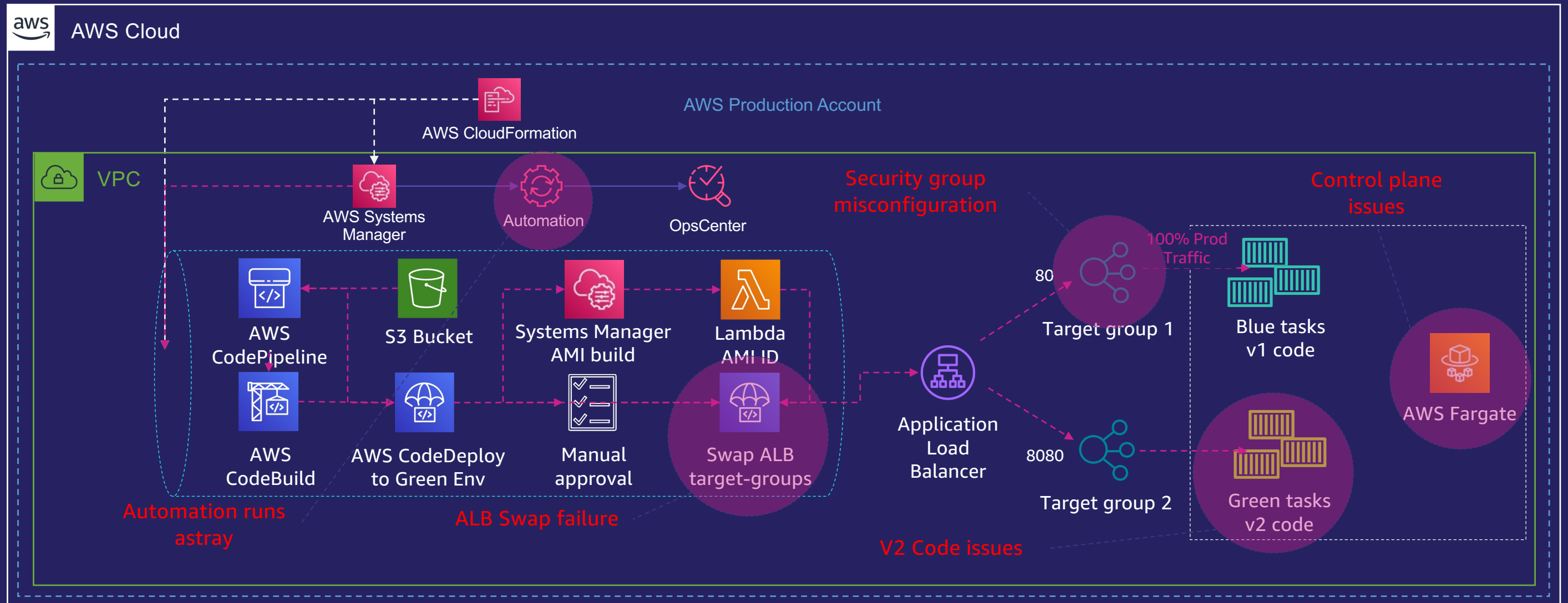


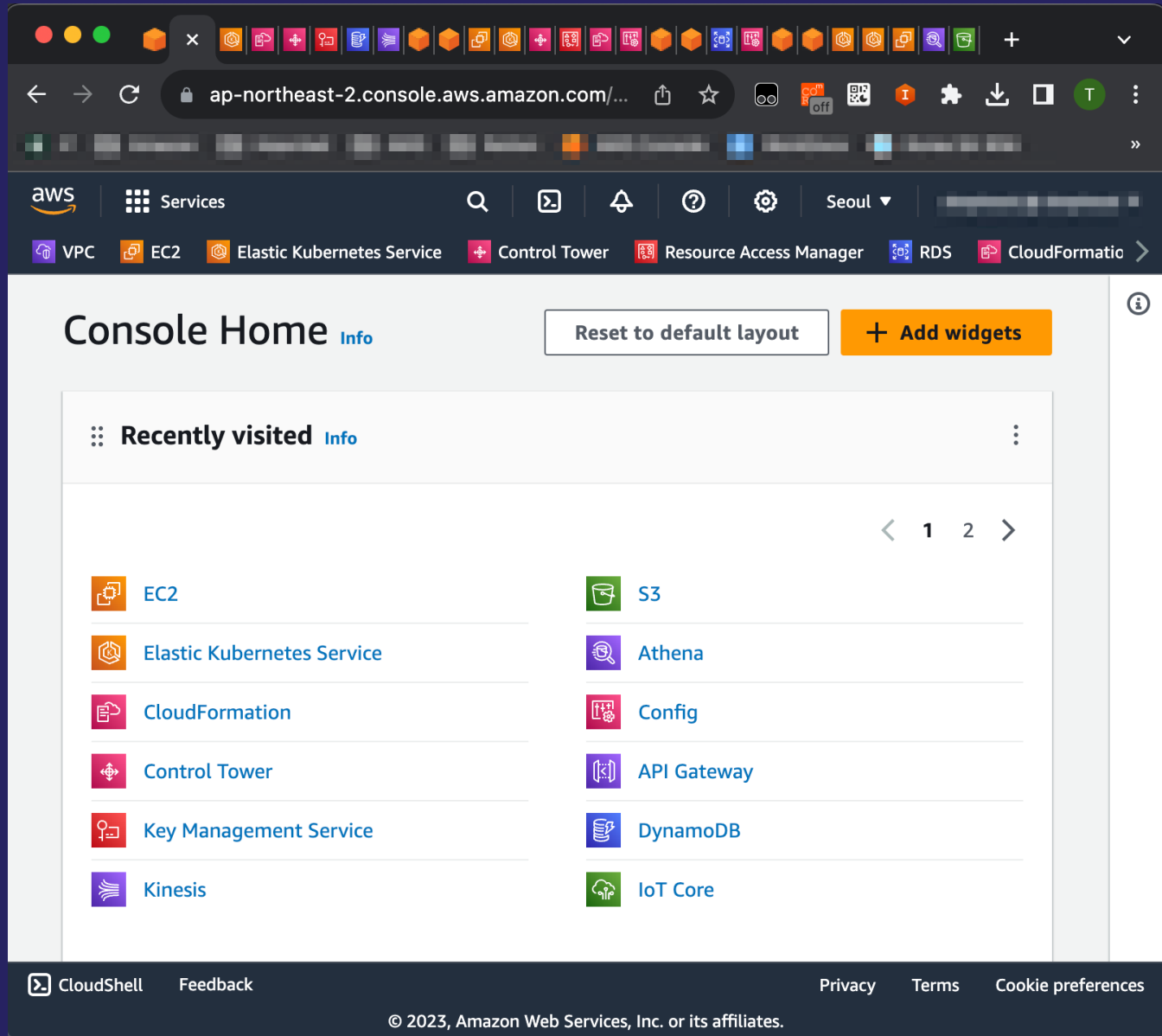
전체 리소스 설정을
쉽게 볼 수 있을까?

관리자 권한 있는 계정을
누가 가지고 있지?

그리고 다양한 운영 상의 이슈 상황들

운영환경에 적용 전에 실패할 수 있는 원인을 파악하여 시뮬레이션('pre-mortem' tabletop exercise) 수행, **실패 원인 제거 및 완화 전략 수립**





장애 및 운영 파악할 때,
리소스 구성을 확인하기 위한
수많은 탭들....

어떻게 개선할 수 있을까?

전체 클라우드
리소스 구성 파악

낮은 비용

어떻게 운영, 보안상의
이슈들을 파악할 수 있을까?

지속적인 모니터링

가시성 확보

리소스 구성 시각화의 장점



구성 오류 파악



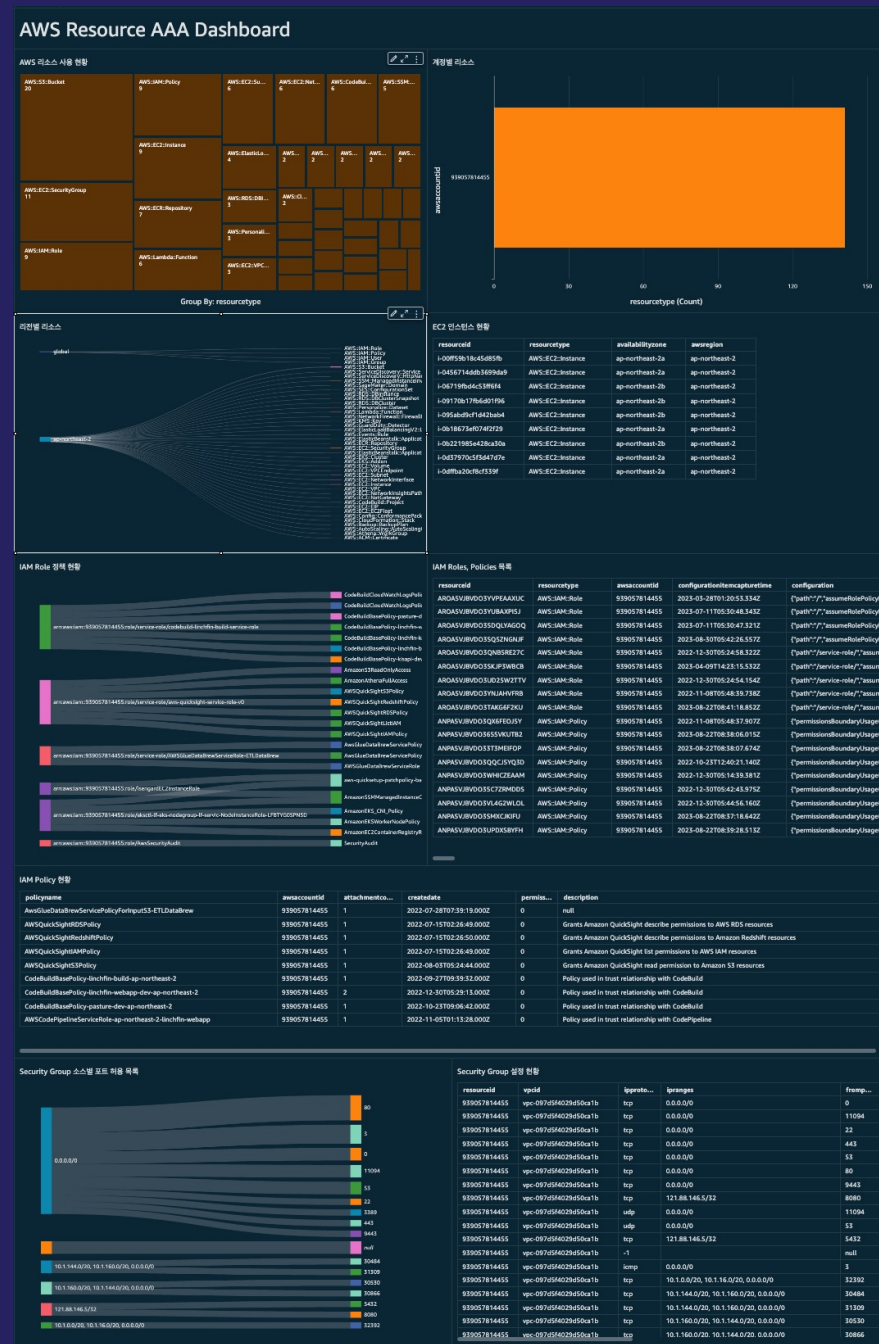
가시성 확보



위협 모델링

리소스 구성 시각화 소개

AWS Config 기반 리소스 구성 시각화 – CSPM 솔루션



CSPM(Cloud Security Posture Management)

다양한 클라우드 인프라에 대한 잘못된 구성 검색, 가시성 확보, 모니터링

→ Config 데이터를 Amazon QuickSight로 시각화

장점

1. 리소스 설정에 대한 가시성 확보
2. 잘못된 리소스 설정에 대한 빠른 대응 가능
(IAM, 보안 그룹 등)

AWS Config

리소스의 구성과 관계를
지속적으로 기록, 평가 및 감사



리소스 구성 설정 및 변경 기록, 평가



리소스 변경 관리 자동화



원클릭으로 손쉽게 시작

Amazon Athena

S3 저장 데이터에 대해
SQL 기반의 쿼리 분석



설치 없이 즉시 쿼리 실행



사용한 만큼 과금



Open, powerful, standard

Amazon QuickSight

조직에 인사이트를 제공하는
클라우드 네이티브 BI 솔루션



서버리스로 별도의 서버 관리 X



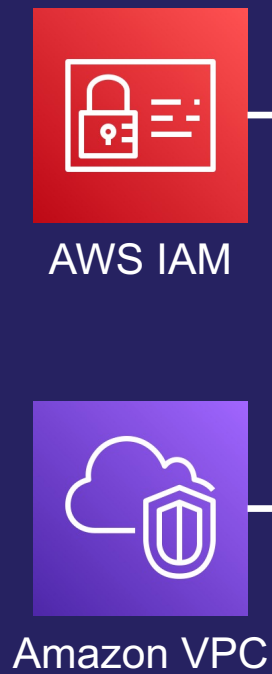
내부 / 외부 유저 계정 제어



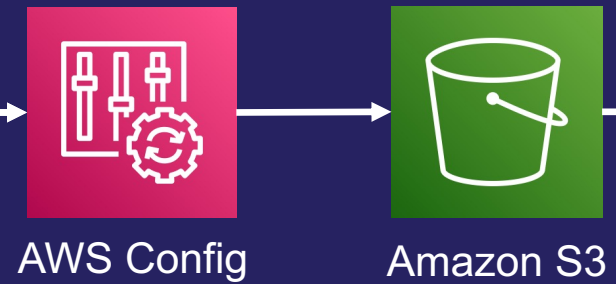
AWS 서비스와 손쉽게 연동

리소스 구성 시각화 솔루션 아키텍처

1. 리소스 구성



2. 리소스 구성 데이터 수집

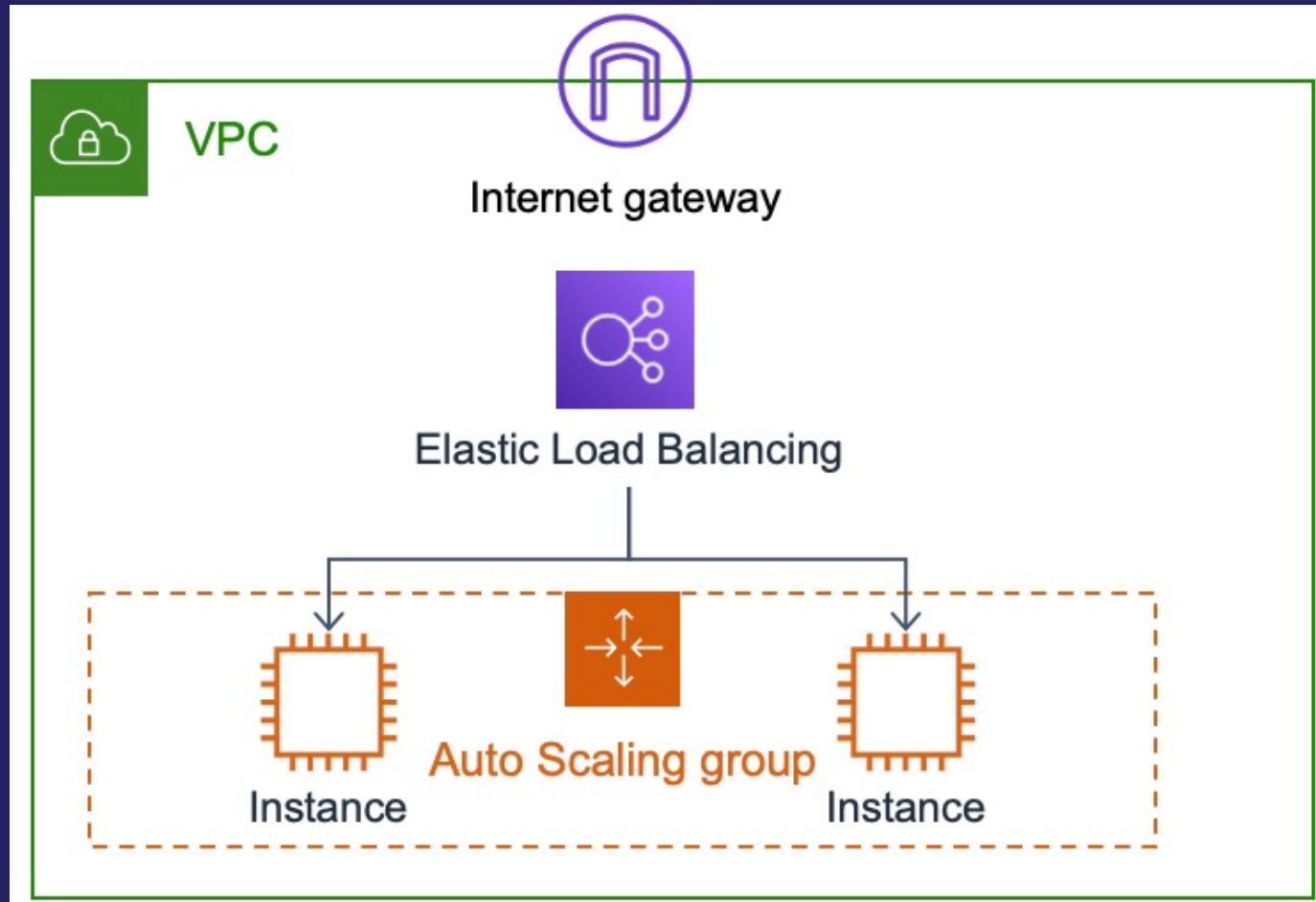


3. 분석 및 시각화



리소스 구성 시각화 워크샵 소개

워크샵 순서 – 1. Demo VPC 배포 및 IAM 설정

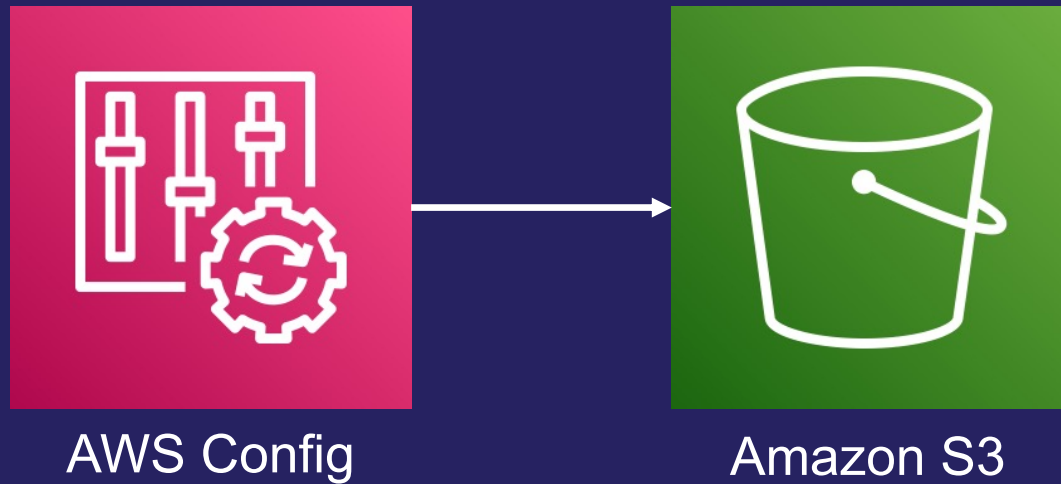


AWS CDK를 이용하여 리소스들을 배포합니다.

DevVPC, ProdVPC 2개가 다음과 같은 구성으로 배포됩니다.

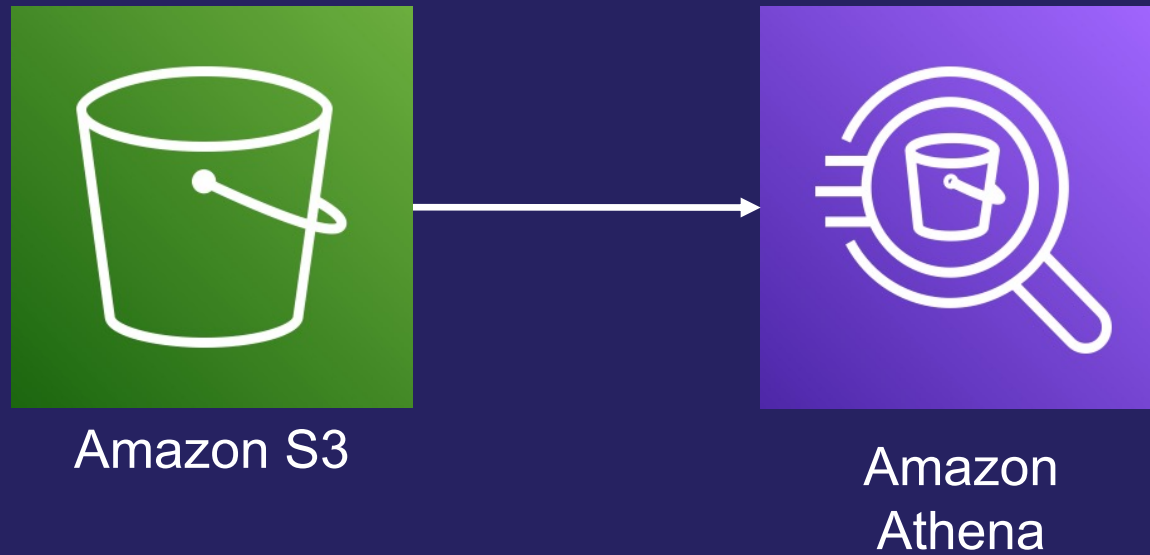
AWS CLI로 IAM 계정, 그룹 및 권한을 추가합니다.

워크샵 순서 – 2. AWS Config 활성화






AWS Config를 활성화하고,
현재 리소스 기준 스냅샷을 S3에 저장합니다.
(글로벌 리소스 수집 설정으로 IAM 구성도 수집 가능)

워크샵 순서 – 3-a. 리소스 구성 분석



S3 저장된 리소스 스냅샷 구성을 기반으로
테이블과 뷰를 생성합니다.

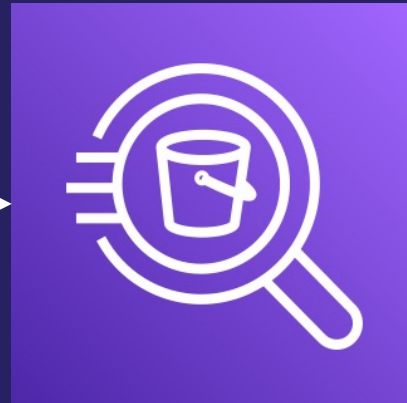
워크샵 순서 – 3-a. 리소스 구성 분석

Results (10)				 Copy	Download results
 Search rows				< 1 > 	
configurationitemstatus ▾	resourcetype ▾	resourceid ▾	arn		
ResourceDiscovered	AWS::EC2::SecurityGroup	sg-079cdf4f086152ba2	arn:aws:ec2:ap-northeast-2:515555555555:security-group/sg-079cdf4f086152ba2		
OK	AWS::EC2::VPC	vpc-09dd2cc81aab32857	arn:aws:ec2:ap-northeast-2:515555555555:vpc/vpc-09dd2cc81aab32857		
ResourceDiscovered	AWS::EC2::DHCOPTIONS	dopt-0b00b02de580cbfa8	arn:aws:ec2:ap-northeast-2:515555555555:dhcp-options/dopt-0b00b02de580cbfa8		
ResourceDiscovered	AWS::EC2::Subnet	subnet-006ca6f0c2671b32b	arn:aws:ec2:ap-northeast-2:515555555555:subnet/subnet-006ca6f0c2671b32b		
ResourceDiscovered	AWS::EC2::Subnet	subnet-067eb6a782a1e75c0	arn:aws:ec2:ap-northeast-2:515555555555:subnet/subnet-067eb6a782a1e75c0		
ResourceDiscovered	AWS::EC2::Subnet	subnet-09584f78c60ec4bf8	arn:aws:ec2:ap-northeast-2:515555555555:subnet/subnet-09584f78c60ec4bf8		
ResourceDiscovered	AWS::EC2::Subnet	subnet-0bc036f88a86e5d8b	arn:aws:ec2:ap-northeast-2:515555555555:subnet/subnet-0bc036f88a86e5d8b		
ResourceDiscovered	AWS::EC2::NetworkAcl	acl-04dc6c4effa5bf961	arn:aws:ec2:ap-northeast-2:515555555555:network-acl/acl-04dc6c4effa5bf961		
ResourceDiscovered	AWS::Route53Resolver::ResolverRule	rslvr-autodefined-rr-internet-resolver	arn:aws:route53resolver:ap-northeast-2::autodefined-rule/rslvr-autodefined-rr-internet-resolver		

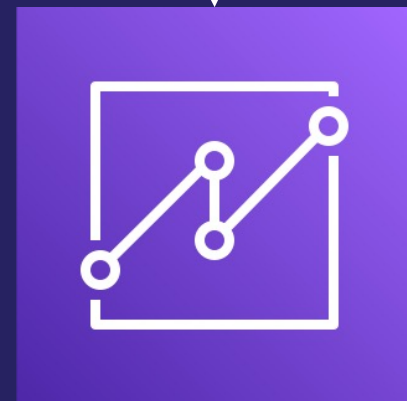
워크샵 순서 – 3-b. 리소스 구성 시각화



Amazon S3



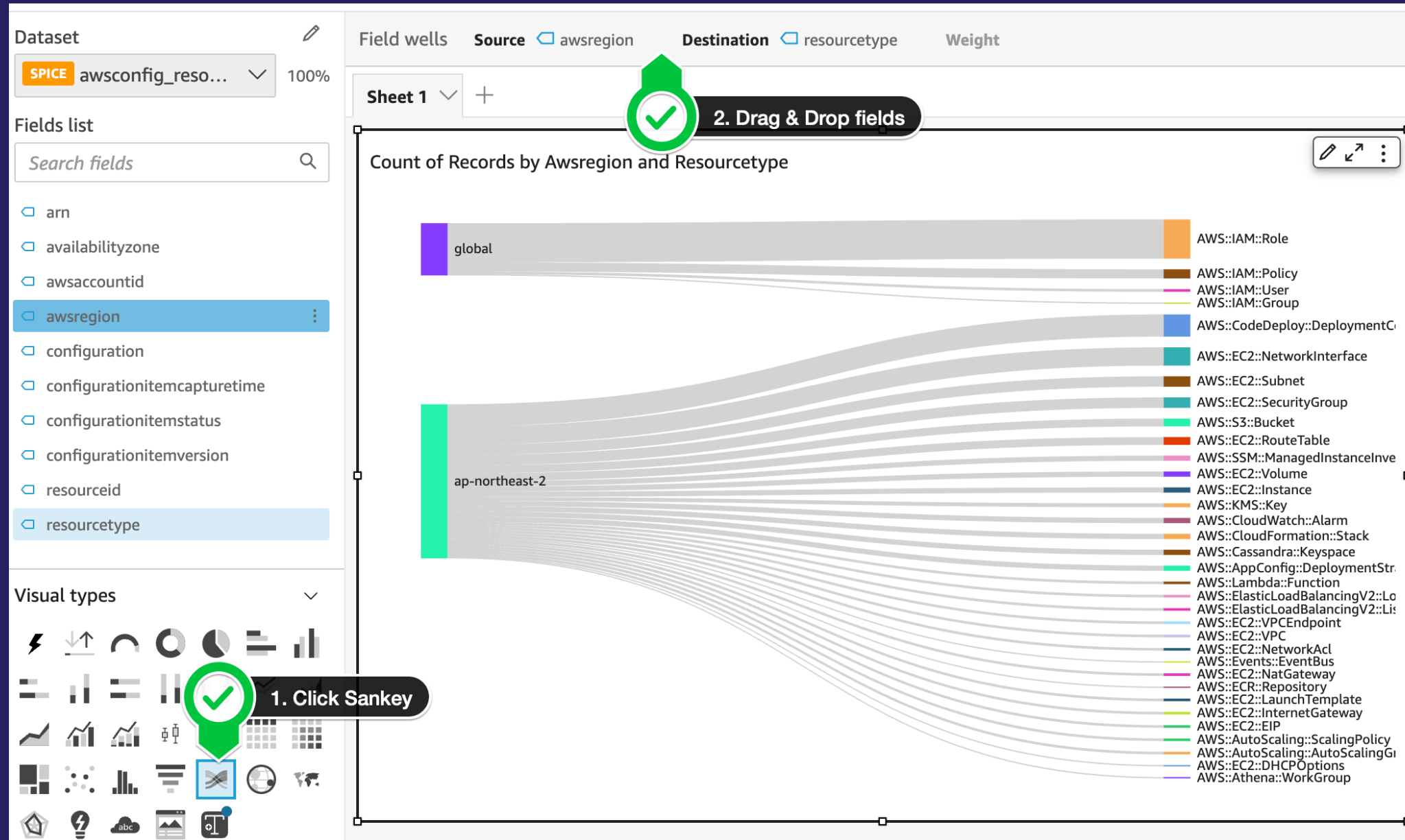
Amazon
Athena



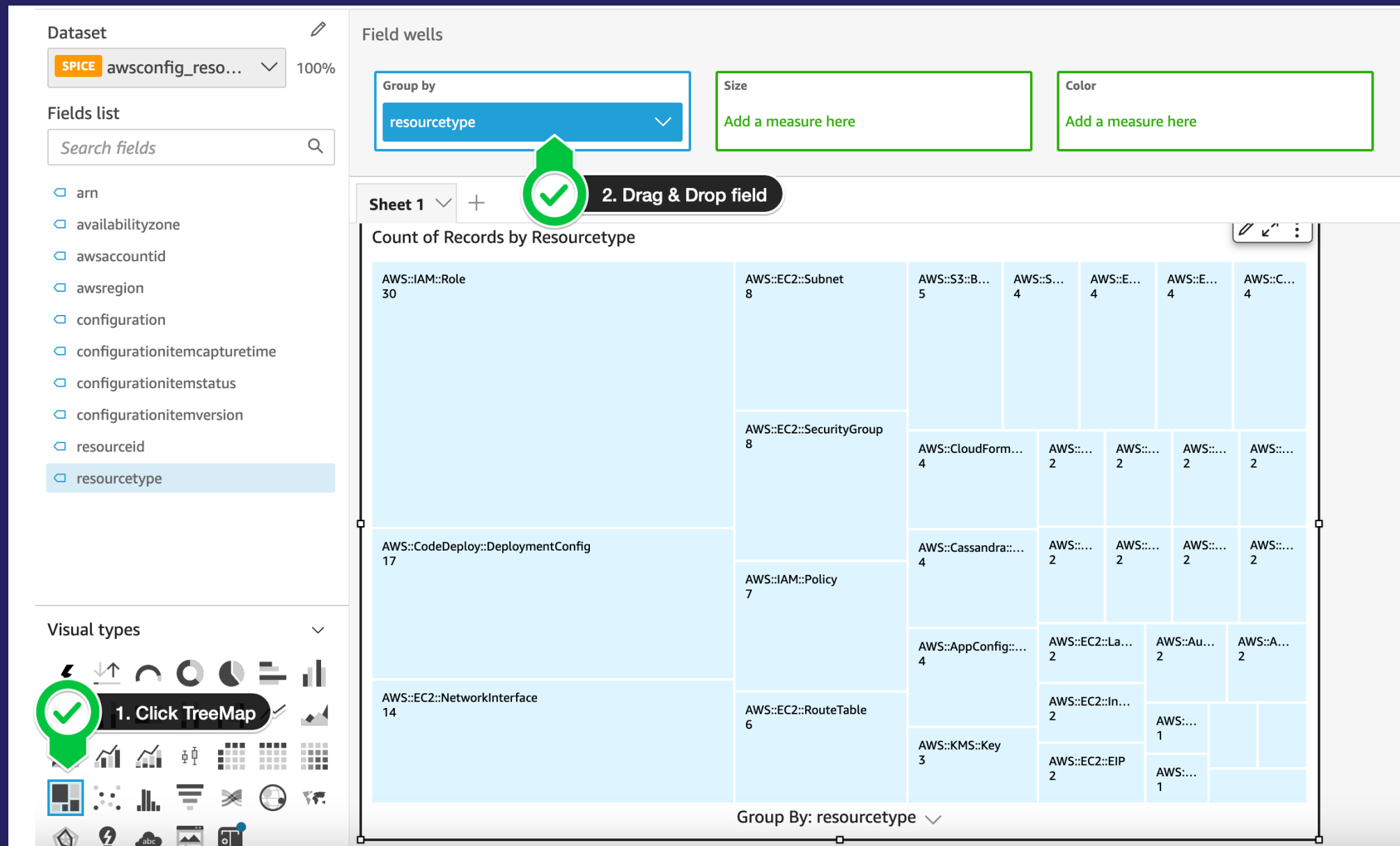
Amazon
QuickSight

**Amazon QuickSight를 구성하고,
Amazon Athena 테이블과 뷰의 데이터를 시각화합니다.**

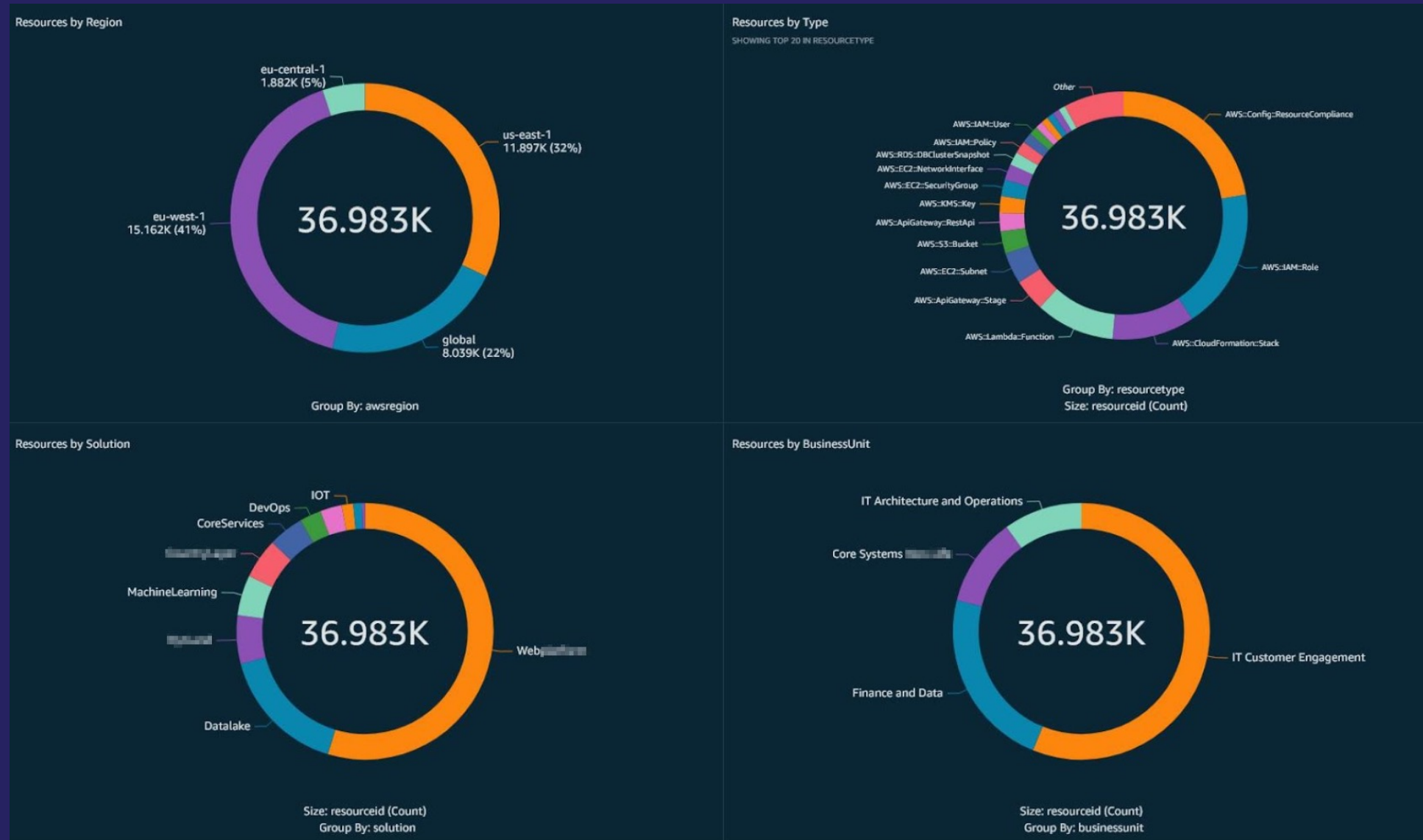
워크샵 순서 – 3-b. 리소스 구성 시각화



워크샵 순서 – 3-b. 리소스 구성 시각화

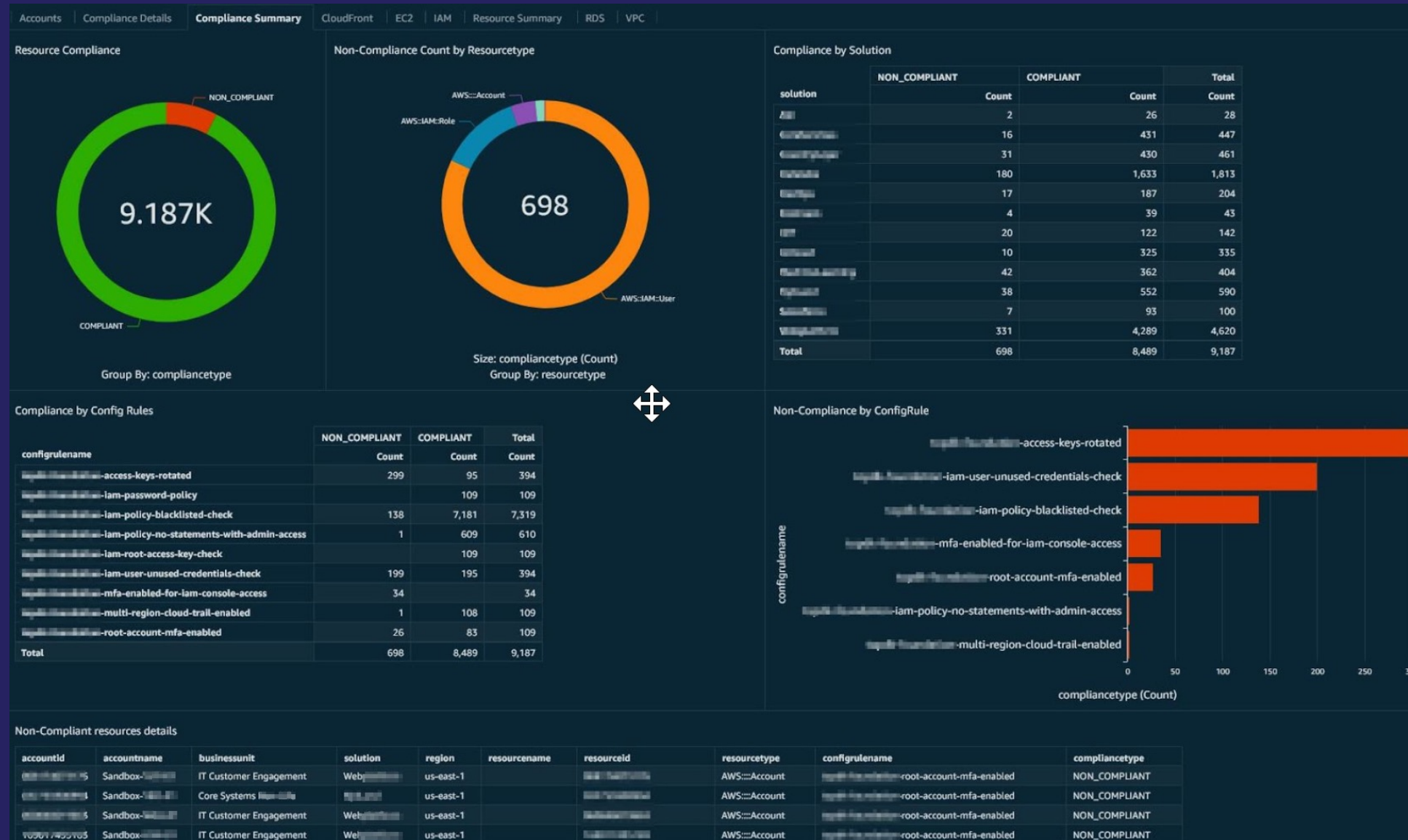


구성 시각화 Case #1 – 운영중인 리소스



<https://aws.amazon.com/blogs/mt/visualizing-aws-config-data-using-amazon-athena-and-amazon-quicksight/>

구성 시각화 Case #2 – 컴플라이언스 모니터링



<https://aws.amazon.com/blogs/mt/visualizing-aws-config-data-using-amazon-athena-and-amazon-quicksight/>

레퍼런스 자료

[실습 관련]

CSPM - 리소스 시각화 워크샵: <https://catalog.us-east-1.prod.workshops.aws/workshops/42262efb-5385-413d-b2a5-a533c35a88fd/ko-KR>

AWS Config 리소스 스키마 GitHub: <https://github.com/aws-labs/aws-config-resource-schema>

Amazon Athena 쿼리 공식 문서: https://docs.aws.amazon.com/ko_kr/athena/latest/ug/querying-JSON.html

[인벤토리 관리 관련]

AWS EC2 자산관리 AWS Blog: <https://aws.amazon.com/ko/blogs/tech/aws-systems-manager-amazon-inspector-amazon-ec2-automation/>

AWS EC2 자산관리 AWS samples GitHub (VPC 배포 코드 포함): <https://github.com/aws-samples/inventory-management-for-amazon-ec2>



Thank you

궁금한 내용이나 피드백 편하게 질문 주셔도 됩니다.

KRUG Slack - Taekyung Han

Email - taekyung@amazon.com

