Building Visibility into

Identity Governance

with AWS IAM Identity Center

AWS IAM Identity Center 기반 아이덴티티 거버넌스 가시성 구축

Stevenson Koo

AWS Community Builder (Security)
Based on open-source work by Alfred Koh · Crypto.com

AWS User Group Korea · 19 May 2026

MIT License | Terraform | Serverless | Python · React

Today's Session

What we'll cover

01 **The Problem** 문제 정의

Why Identity Center visibility is broken today

02 **The Solution** 솔루션 개요

Dashboard overview — 4 tabs, architecture, cost

03 **Security Design** 보안 설계

Risk scoring, built-in controls, least-privilege IAM

04 **Live Demo** 라이브 데모

Assignments · Permission Sets · Security · Audit Trail

05 **Key Takeaways** 핵심 정리

What to take away for your own org

06 **Q & A** 질의응답

Open floor — architecture, code, or anything else

About This Project

Open-source, community-driven

Created by Alfred Koh

Senior Manager, Identity Security · Crypto.com

Originally presented at AWS Security Users Group Singapore · 8 April 2026

What I'm presenting today

- Deployed the project in my own AWS environment
- Built and configured the PoC demo you'll see today
- Walking through the architecture, security design, and lessons learned

github.com/alfredkzr/aws-iam-identity-center-security-governance-dashboard

The Problem · 문제 정의

"Who has access to what across your AWS Organization?"

No native visibility 네이티브 가시성 부재

No unified view of SSO assignments across 100+ accounts — you'd have to click through every account manually.

Risky permission sets go undetected 위험한 권한 세트 미탐지

Overly permissive policies accumulate silently over time with no automated alerting or risk scoring.

No audit trail without heavy setup 감사 추적 부재

Tracking who assigned access requires complex CloudTrail queries — no security-focused view exists.

Compliance reporting is manual 수동 컴플라이언스 보고

Auditors need access evidence. Manual CSV exports from the Console can't scale.

The Solution · 솔루션

Four views, one dashboard

하나의 대시보드, 네 가지 뷰

Assignments 액세스 할당

- Full-org SSO crawl across all accounts
- Search & filter by principal, account, permission set
- Access heatmap visualization
- Historical snapshots
- Export to CSV or PDF

Permission Sets 권한 세트

- All permission sets with provisioned count
- AWS & customer managed policy labels
- Inline policy viewer with syntax highlighting
- Session duration & boundary visibility
- Resizable columns

Security Risk 보안 위험

- Risk scoring: Critical / High / Medium / None
- Based on CIS & Rhino Security research
- Flags dangerous policies automatically
- Custom rule editor — add / edit / delete
- Export risk policies to CSV or PDF

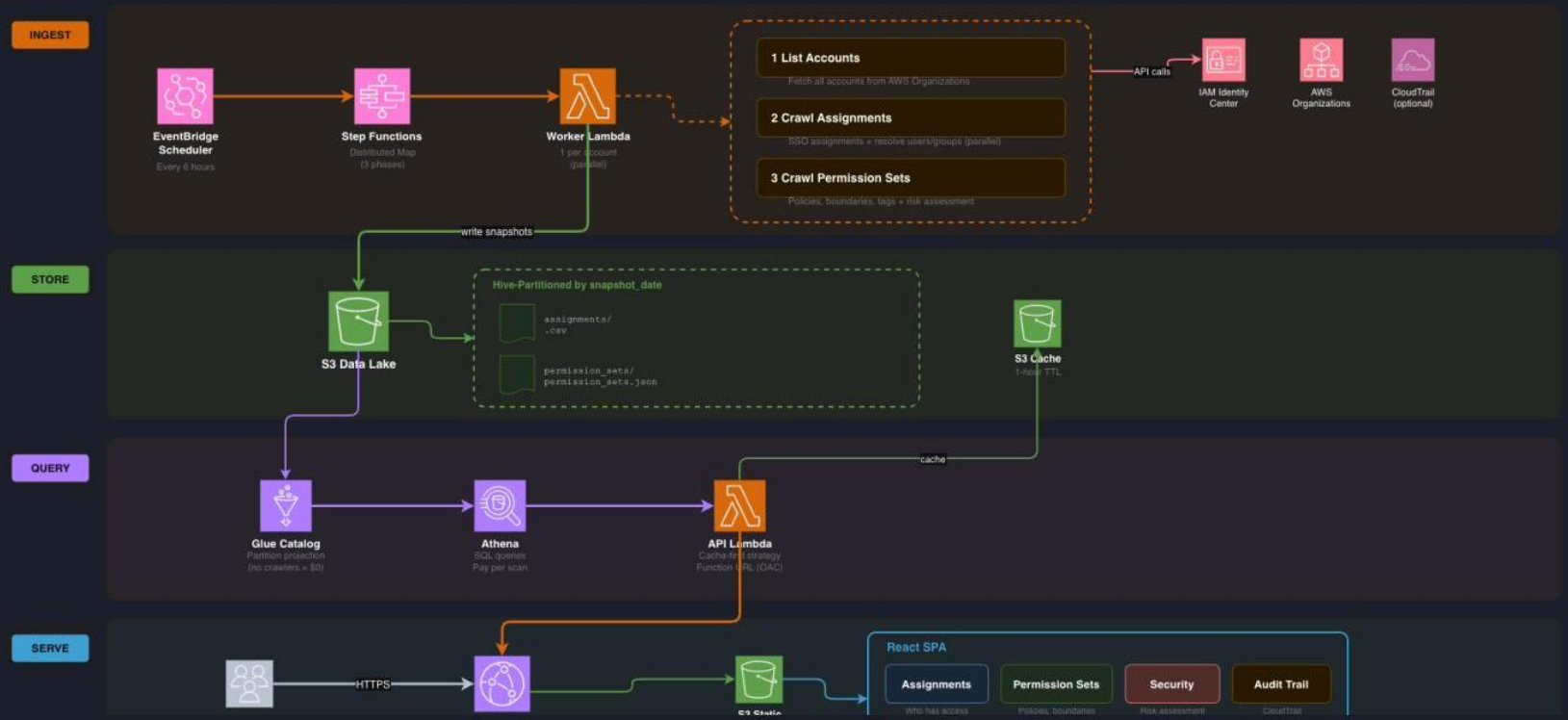
Audit Trail 감사 추적

- CloudTrail-powered change history
- Tracks assignment & permission set changes
- Filter by date range, event type, actor
- Full CloudTrail JSON details
- Who assigned access — with timestamps

Architecture · 아키텍처

Serverless — zero fixed costs

서버리스 — 고정 비용 없음



Layer 1 · 1계층 · 수집

Ingestion pipeline

Crawling 100+ accounts in parallel

1

ListAccounts

Organizations API lists all ACTIVE accounts in the org

→

2

CrawlAccounts

Distributed Map fans out — 1 Lambda per account, writes CSV to S3

→

3

CrawlPermissionSets

Single Lambda collects all PS configs and evaluates risk rules

- Step Functions Distributed Map — built-in fan-out with MaxConcurrency control
- Python 3.12 ARM64 (Graviton2) — boto3 only, zero pip dependencies
- Adaptive retry mode — exponential backoff handles API throttling

Layer 2 · 2계층 · 데이터 레이크

Data lake

Querying terabytes without a database

```
/assignments
  /snapshot_date=2026-03-15
    111111111111.csv
    222222222222.csv
/permission_sets
  /snapshot_date=2026-03-15
    permission_sets.json
```

Hive-partitioned storage

Partition Projection

- Glue Catalog defines table schema (no ETL jobs)
- projection.snapshot_date.type = date
- projection.snapshot_date.range = 2024-01-01,NOW
- Athena calculates S3 paths mathematically
- Zero cost — no Glue Crawlers needed

Inventory
Raw snapshots — 7-day

Athena Results
Query scratch — 1-day

Cache
Pre-computed JSON — 1h TTL

Frontend
React SPA — Persistent

Layer 3 · 3계층 · 프레젠테이션

Presentation layer

프레젠테이션 계층

CloudFront as your API Gateway

CloudFront + S3

React SPA served globally. Path-based routing: /* → S3, /api* → Lambda

Origin Access Control

SigV4 signing to both S3 and Lambda. Neither origin is publicly accessible.

OIDC Authentication

Okta / Azure AD / Google Workspace. Authorization Code + PKCE (S256)

SPA Routing

Custom error responses: 403/404 → /index.html. Enables React client-side routing.

Cache-First Strategy

S3 cache (1h TTL) → sub-second response. Miss: Athena query (2-5s), write to cache.

Risk Engine · 위험 평가 엔진

44 built-in rules, two rule types

44개 내장 규칙, 두 가지 규칙 유형

CRITICAL 심각
3 rules
*, *:*, AdministratorAccess

HIGH 높음
25 rules
IAM escalation, audit evasion

MEDIUM 중간
16 rules
Service wildcards, secrets access

LOW 낮음
No flags
No flagged patterns detected

```
managed_policy_name

"AdministratorAccess" → critical
"PowerUserAccess" → high
"*FullAccess" → medium
```

```
inline_policy_action

"*" or "*:*" → critical
"iam:PassRole" → high (priv esc)
"cloudtrail:StopLogging" → high (evasion)
```

Audit Trail · 감사 추적

Who changed what, and when?

Problem: Identity Center APIs don't tell you who made changes. No built-in attribution.

- 19 SSO event types tracked (CreateAccountAssignment, UpdatePermissionSet, etc.)
- Resolves deleted entities: historical snapshots + Identity Store API fallback
- Attribution enrichment: maps CloudTrail userIdentity to human-readable names

FinOps · 비용 분석

What does it actually cost?

Small
20 accounts · 4 crawls/day

~$0.10/month

Medium
100 accounts · 4 crawls/day

~$0.50/month

Large
500 accounts · 4 crawls/day

~$2.75/month

Most small-to-medium deployments fall within the AWS Free Tier.

Technology Stack

React 18	Python 3.12	Terraform ≥ 1.5	Amazon Athena	Step Functions

Live Demo

라이브 데모

1

Assignments

Search for a user — see every account they can access

2

Heatmap

Spot accounts with too many principals on powerful PS

3

Security Risk

Watch the risk engine flag AdministratorAccess

4

Custom Rules

Add a banned policy rule — live, no redeploy

5

Audit Trail

Who made access changes and when — CloudTrail

Key Takeaways · 핵심 정리

1. **Serverless is the right model for governance tooling**
   거버넌스 도구에는 서버리스가 정답입니다
   No EC2, no RDS, no NAT Gateway. Step Functions + Lambda + Athena at near-zero cost.

2. **Risk scoring should be configurable, not hardcoded**
   위험 점수는 하드코딩이 아닌 구성 가능해야 합니다
   Every org has different risk appetite. The rule engine lets you define your own patterns.

3. **Access visibility is a prerequisite for Zero Trust**
   액세스 가시성은 제로 트러스트의 전제 조건입니다
   You can't enforce least privilege if you can't see what's assigned.

4. **CloudTrail + Athena = free, scalable audit trail**
   CloudTrail + Athena = 무료로 확장 가능한 감사 추적
   No SIEM required. Org CloudTrail logs already exist — Athena queries them for cents.

5. **IaC-first means reproducibility for free**
   코드형 인프라(IaC)는 무료 재현성을 제공합니다
   One terraform apply. Fork the repo and deploy in 5 minutes.

Remember that question?

그 질문을 기억하시나요?

"Who has access to what across your AWS Organization?"

Now your security team opens one page, sees every assignment across every account, and the risk engine has already flagged the violations. The audit trail shows exactly who made each change and when.

Deploy in 5 minutes. The code is open source.

Thank you

Stevenson Koo

AWS Community Builder (Security)

Questions?

감사합니다 · 질문 있으신가요?

LinkedIn

linkedin.com/in/stevenson-k

GitHub

github.com/alfredkzr/aws-iam-identity-center-security-governance-dashboard

MIT License · Fork & deploy

Original project by Alfred Koh · Crypto.com