TEAM 뭉살흩죽

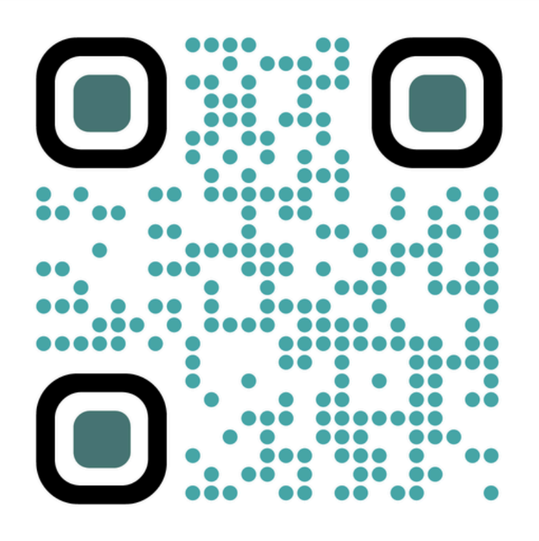
Baby Beavers
최종 발표

기업 성장에 따른 규모별 안전한 인프라 설계 및 IaC 배포

김민수, 이지향, 이호영, 조휘정 | **멘토** 홍성진 | **PL** 박민서 | Babybeavers 1기

목차

BABY BEAVERS



01

프로젝트 소개

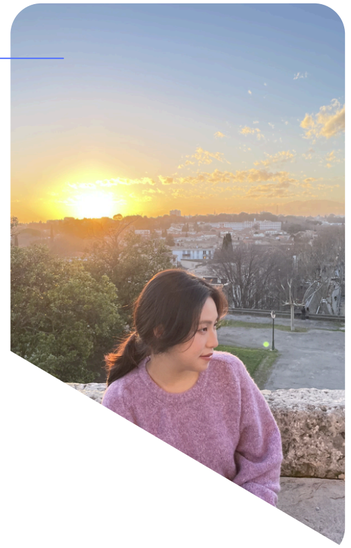
팀원 소개

프로젝트 목표와 개요

팀원 소개

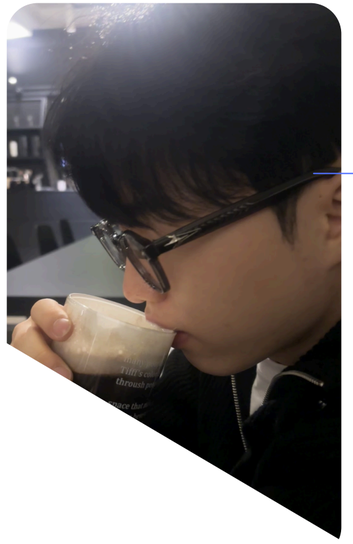
조휘정 PM

프로젝트 매니저



이지향 Member

이호영 Member



김민수 Member

MENTOR

홍성진

PROJECT LEADER

박민서

프로젝트 목표

기업 성장에 따른 규모별 인프라 설계

- 바이브 코딩부터 1,000만 유저까지

목표 1

기업 규모에 따른 보안 아키텍처 설계

1인 기업에서 점차 회사 규모가 커지면서 그에 맞는 보안을 고려한 인프라 아키텍처를 구성해보자

목표 2

도움되는 산출물 공유하기

설계한 아키텍처를 기반으로 IaC 자동화/문서화하여 다수에게 공유해 더욱 발전해나가는 결과물 체인을 만들어보자

목표 3

커뮤니케이션 역량 강화

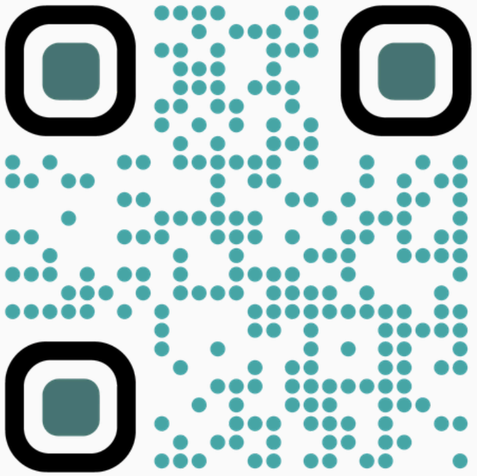
아키텍처 설계 과정에서 발생할 수 있는 갈등을 겪고 해결하면서 논리적인 설득력을 기르자

프로젝트 소개

규모별 아키텍처 선정 기준

규모	임직원 수	사용자 수	회사
바이브코딩	1	50~	1인 기업
소	4	1천~1만	신생 스타트업
중	100	100만~	인프런, 화해, 클래스101
중~대	300	700만~	무신사, 티빙, 마켓컬리
대	2,000	1,000만~	쿠팡, 배달의 민족

BABY BEAVERS



02

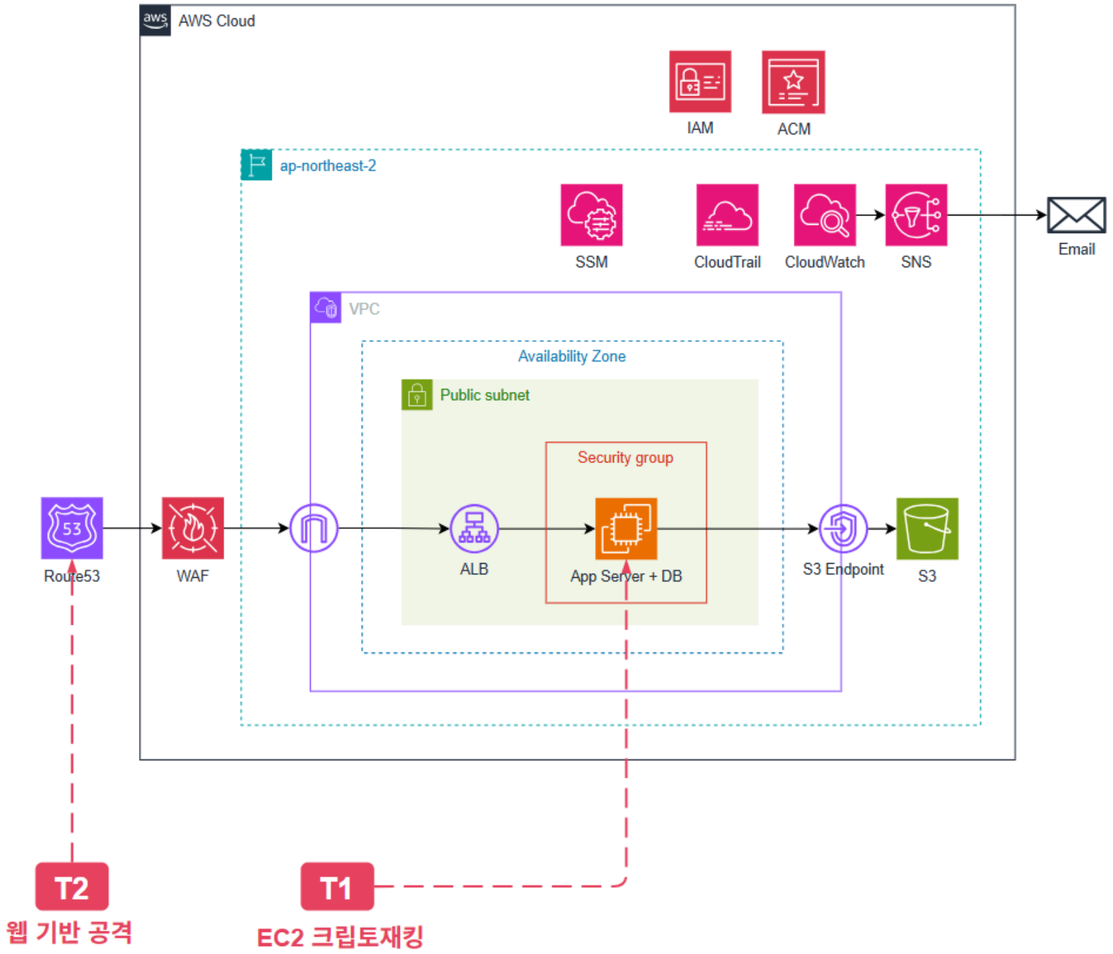
보안 아키텍처 설계 (1)

중간발표까지의 여정

바이브코딩 / 소규모 아키텍처

Previously - 바이브코딩 아키텍처

| 임직원 1명 | 사용자 50명~ | 1인 기업 |



이 아키텍처에서 고려한 주요 위협

- SQLi / XSS 등 웹 공격
- 크립토재킹 / EC2 리소스 남용 등

→ **웹 위협이 가장 위협적일 것으로 예상**

대응 방법

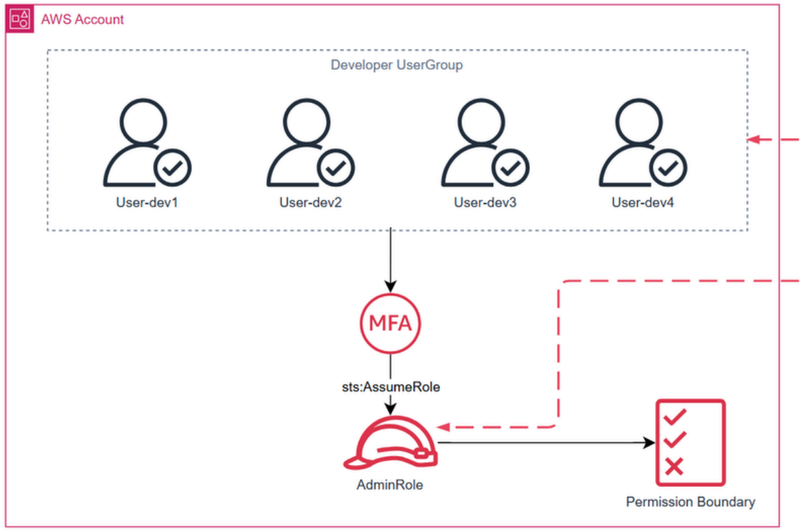
- CloudWatch CPU 이상 급증 알람으로 채굴 시도 탐지
- ALB에 WAF를 붙여 L7 공격 방어
- ALB, EC2 Security Group 설정을 통해 퍼블릭 서브넷으로의 인바운드 공격 방어
- ACM을 통해 통신 / 데이터 암호화

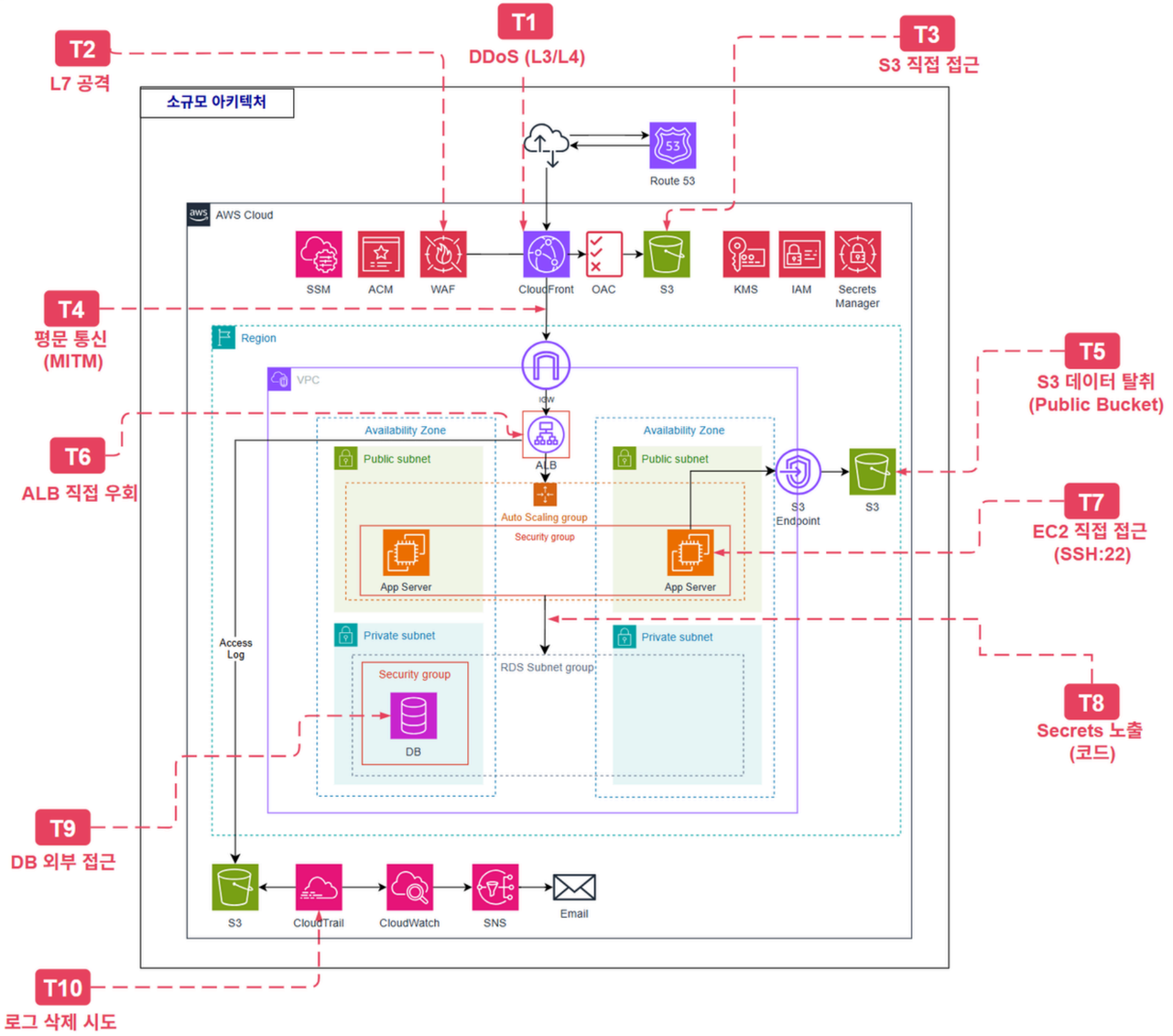
Previously - 소규모 아키텍처

| 임직원 4명 | 사용자 1천 ~ 1만명 | 신생 스타트업 |

이 아키텍처에서 고려한 주요 위협

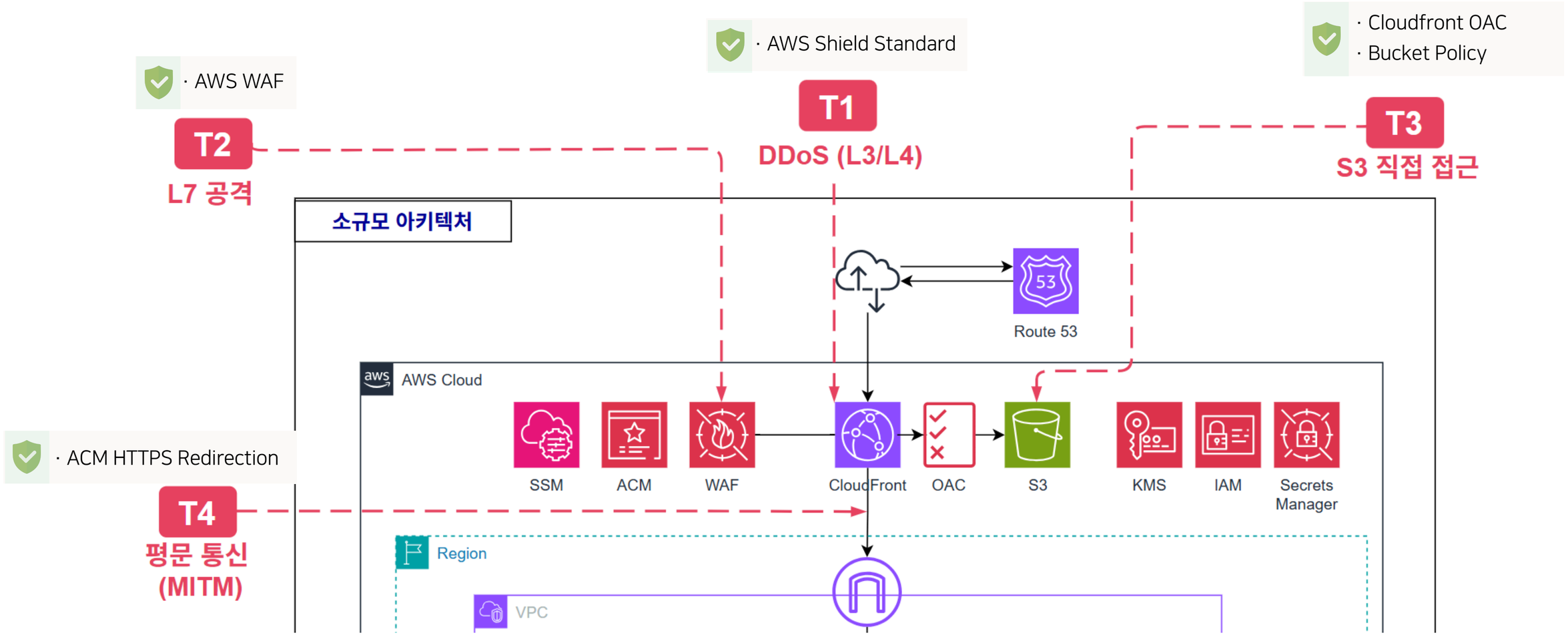
- DDoS, SQLi, 경로 우회 접근 등 네트워크 공격
- 평문 통신, Secrets 노출 등 정보 유출 위협





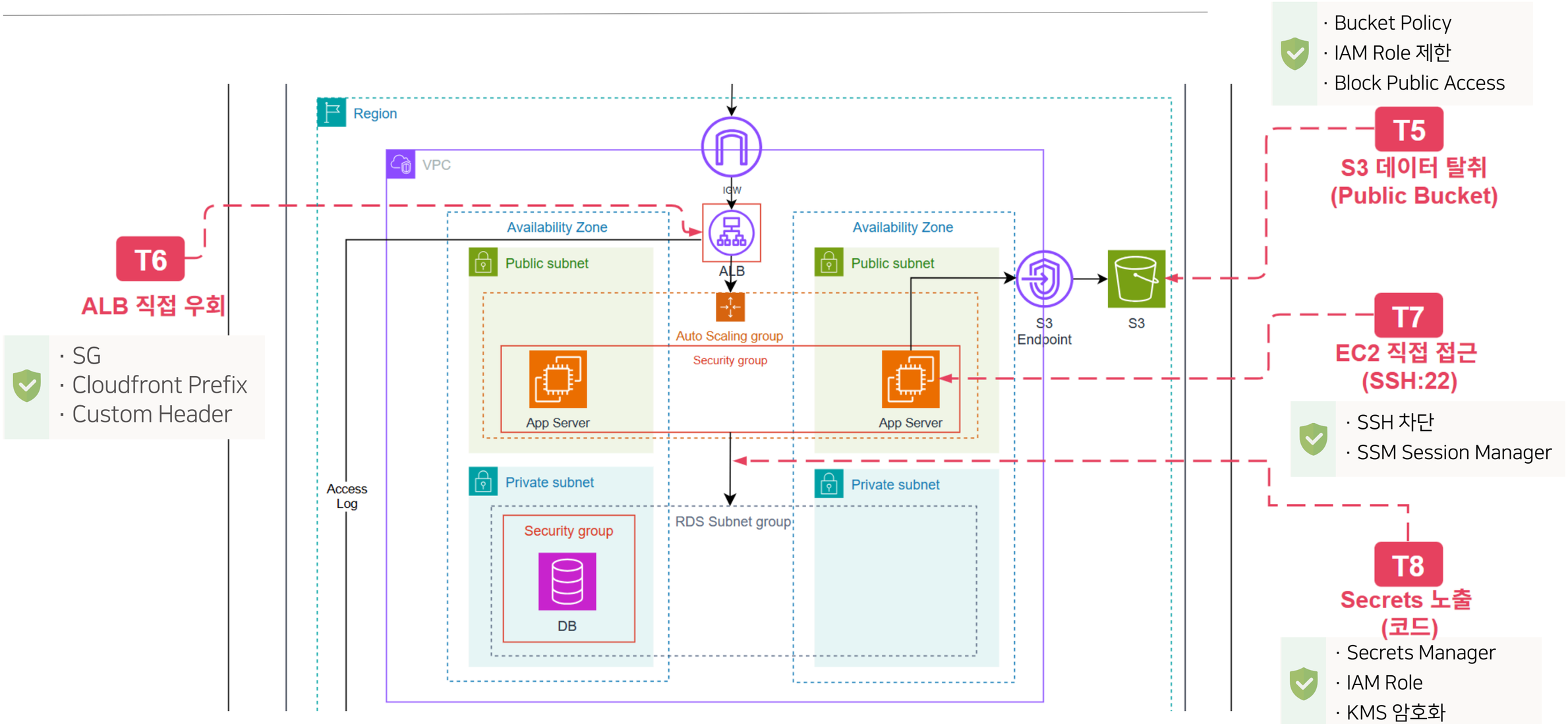
Previously - 소규모 아키텍처

| 임직원 4명 | 사용자 1천 ~ 1만명 | 신생 스타트업 |



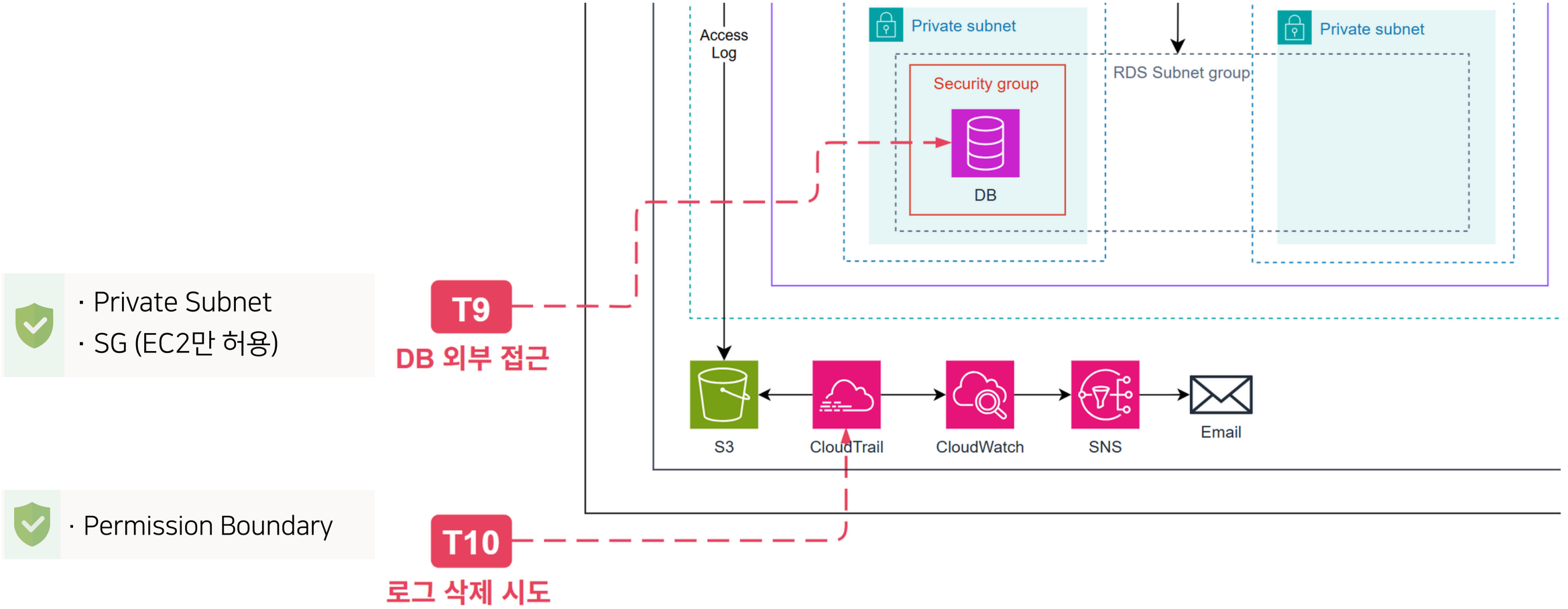
Previously - 소규모 아키텍처

| 임직원 4명 | 사용자 1천 ~ 1만명 | 신생 스타트업 |



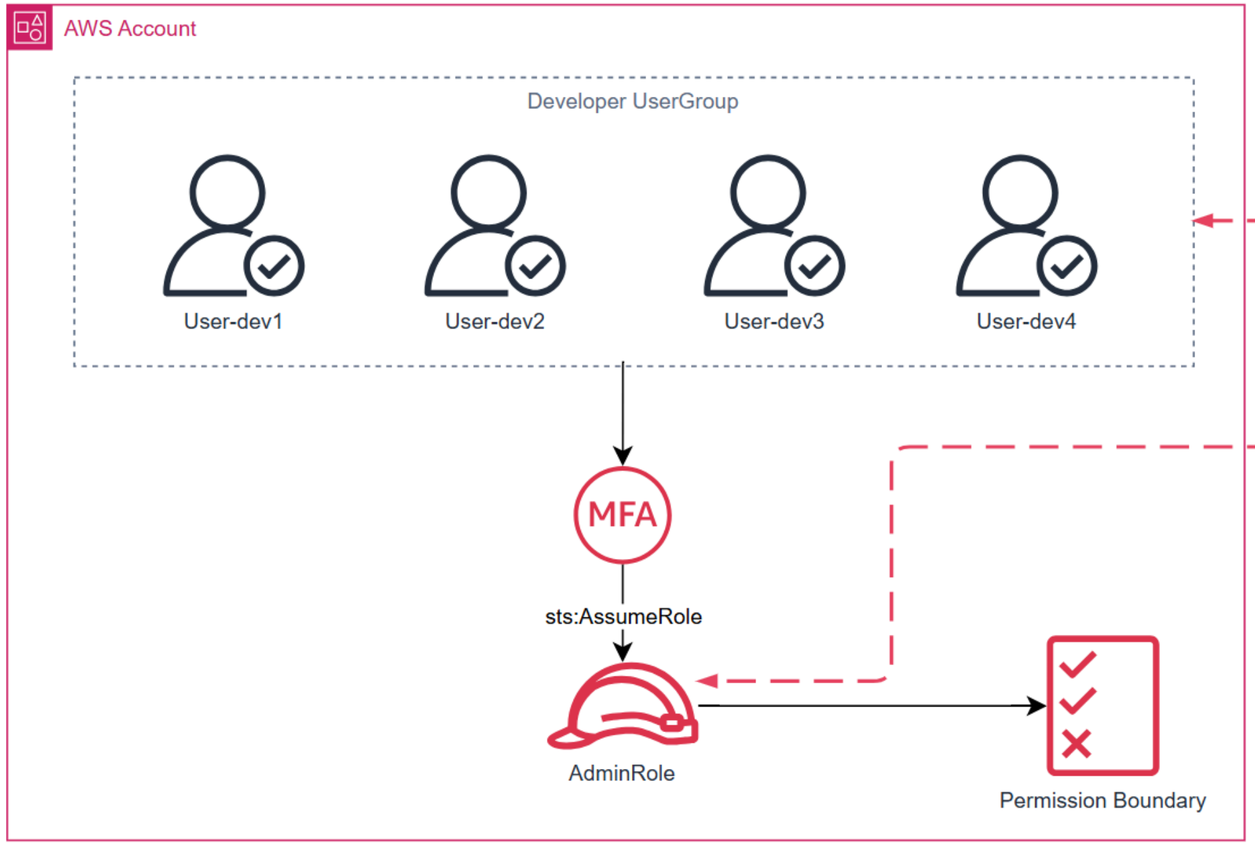
Previously - 소규모 아키텍처

| 임직원 4명 | 사용자 1천 ~ 1만명 | 신생 스타트업 |



Previously - 소규모 아키텍처

| 임직원 4명 | 사용자 1천 ~ 1만명 | 신생 스타트업 |



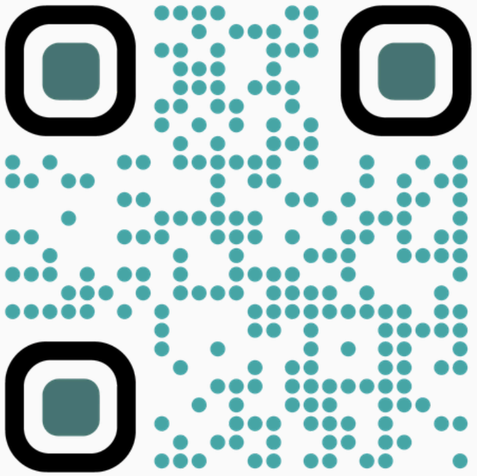
T11
Access Key 탈취

- MFA 강제
- AssumeRole 전환

T12
IAM 권한 남용
(Admin 상시 노출)

- AssumeRole
- ReadOnly 기본 정책

BABY BEAVERS



02

보안 아키텍처 설계 (2)

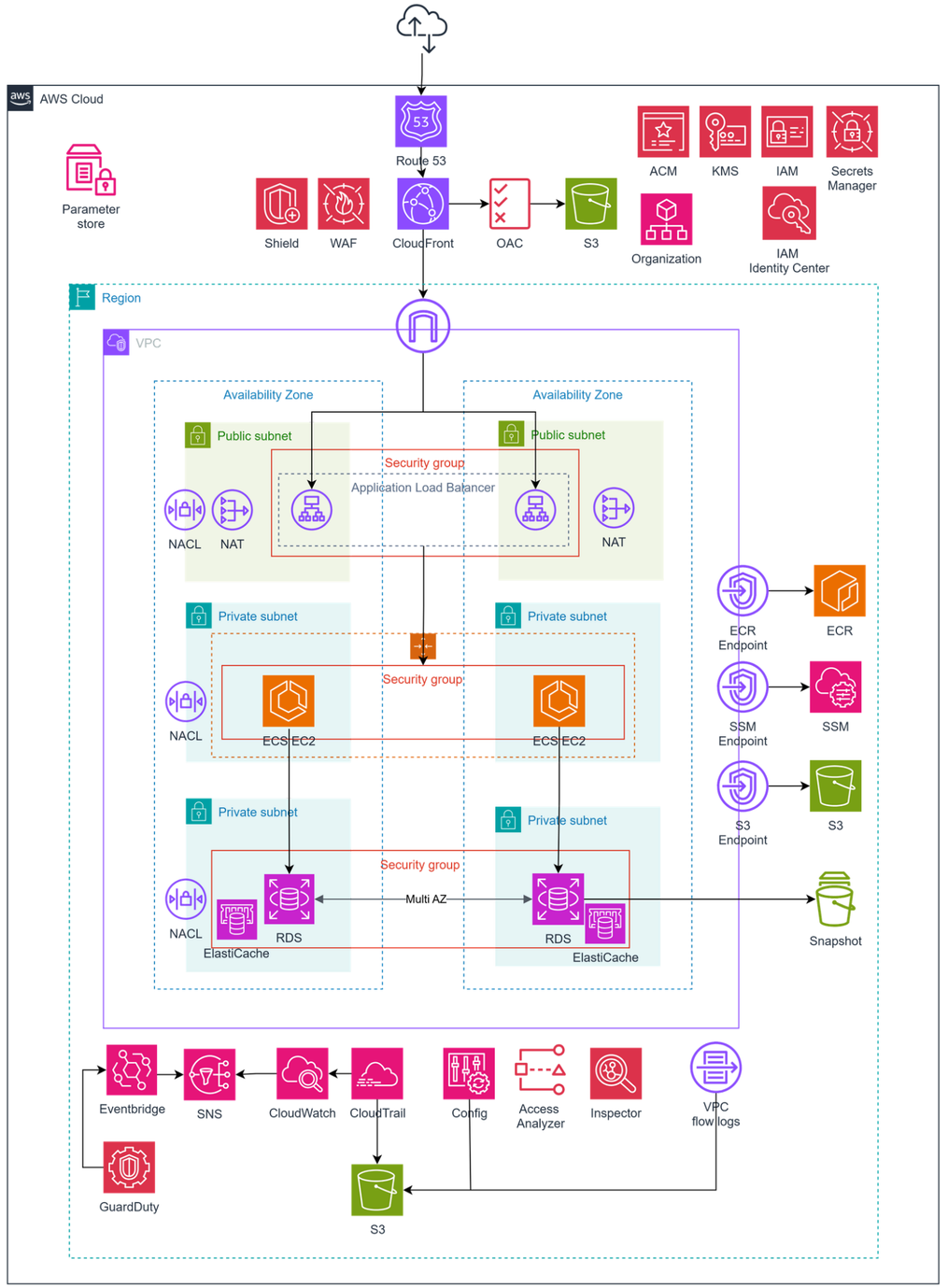
중간발표 이후

중 / 중대 / 대규모 보안 아키텍처

1. 중규모 아키텍처

아키텍처 개요

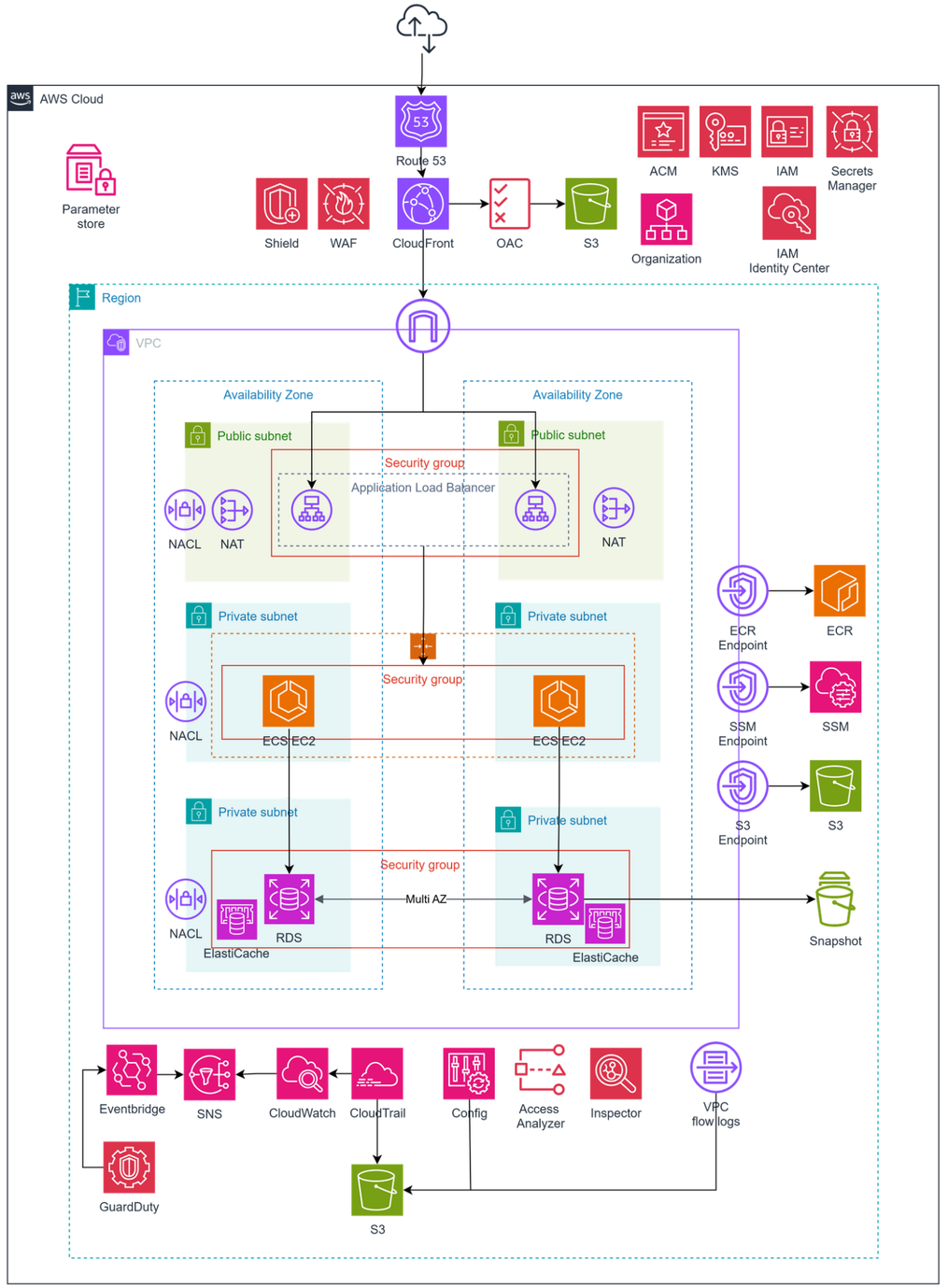
- 가정
  - 임직원 100명(AWS 접근 인원 약 30명 가정)
  - 사용자 100만명 ~
  - 인프런, 화해, 클래스101
- 아키텍처 상세 설명



1. 중규모 아키텍처

아키텍처 가정

- 임직원 100명(AWS 접근 인원 약 30명 가정)
- 사용자 100만명 ~
- 인프런, 화해, 클래스101



1. 중규모 아키텍처

중규모 전환 시 주요 보안 과제 – “사람이 위협이 된다”

조직 규모 확대 및 다중 계정 관리

SITUATION

임직원 수가 늘어나고 여러 팀이 생성되면서,
단일 AWS 계정으로는 리소스 격리와
비용 추적이 어려워짐.

SOLUTION

AWS Organizations + SCP

과도한 권한 부여 및 내부자 위협 증가

SITUATION

직원들에게 개별적으로 많은 권한을 부여하게 되어,
권한 남용이나 탈취로 인한
내부자 보안 위협 리스크가 크게 증가함.

SOLUTION

**IAM Identity Center
+ Permission Set**

운영 실수로 인한 리소스 외부 노출

SITUATION

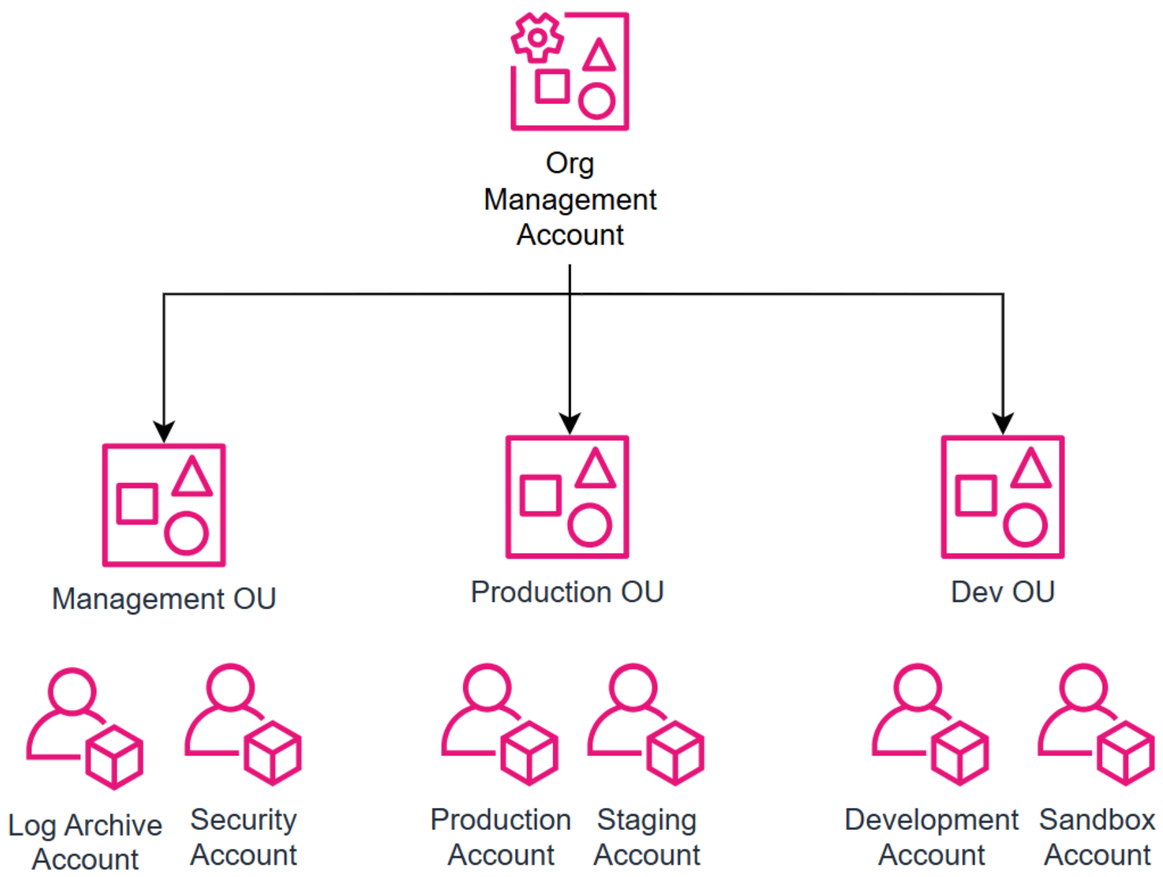
관리해야 할 리소스가 많아지면서,
담당자의 설정 실수(Human Error)로 인해
중요 리소스가 외부에 노출될 위험이 발생함.

SOLUTION

**IAM Access Analyzer
+ AWS Config**

1. 중규모 아키텍처

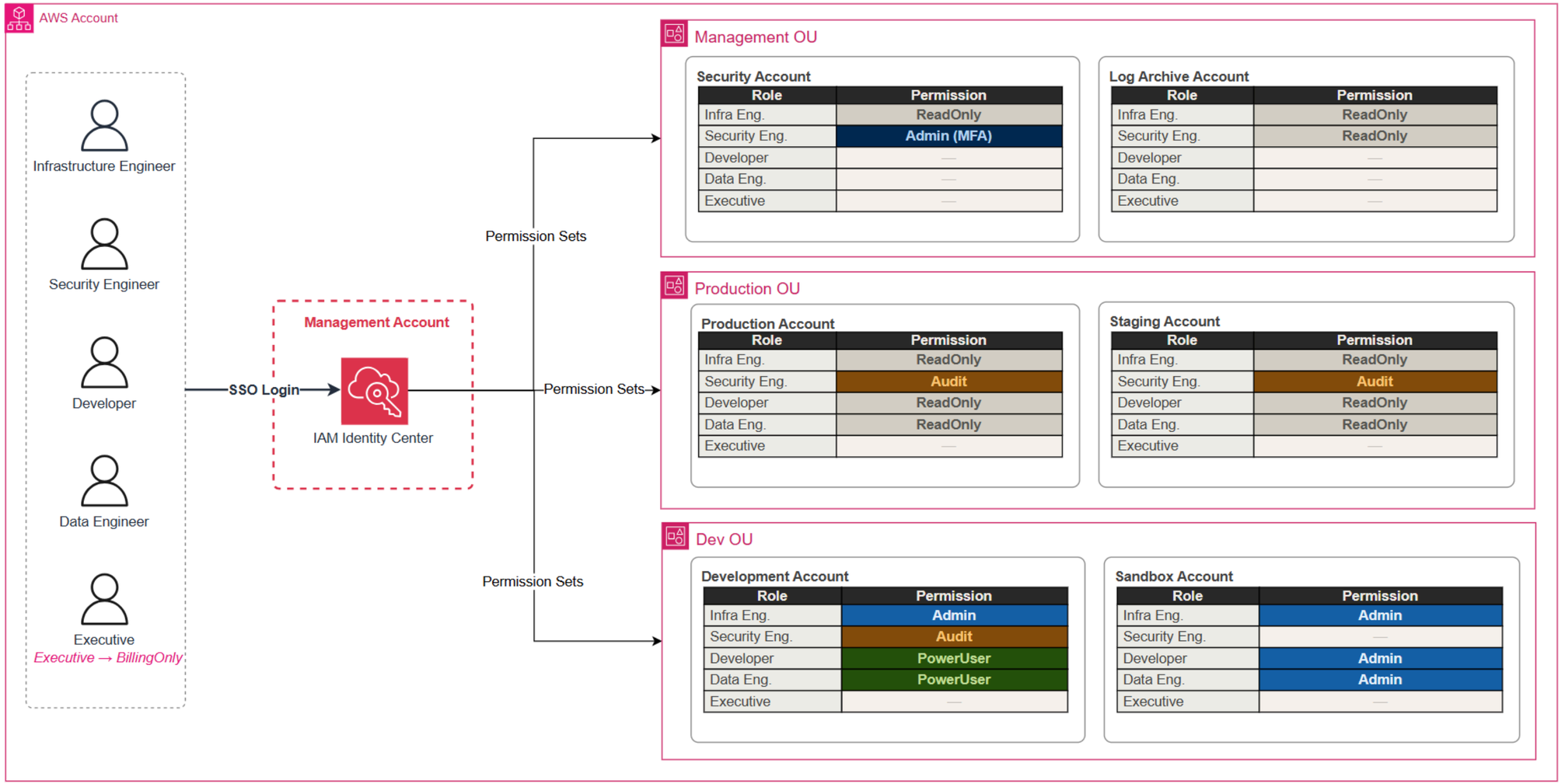
(1) 조직 규모 확대 및 다중 계정 관리



Foundation SCP
Root User 차단
사용 리전 외 차단
Organizations 탈퇴 금지
IAM User / Access Key 생성 금지
S3 Bucket Owner Enforced 강제
EBS 암호화 비활성화 금지
IAM 패스워드 정책 보호
Identity Perimeter 강제

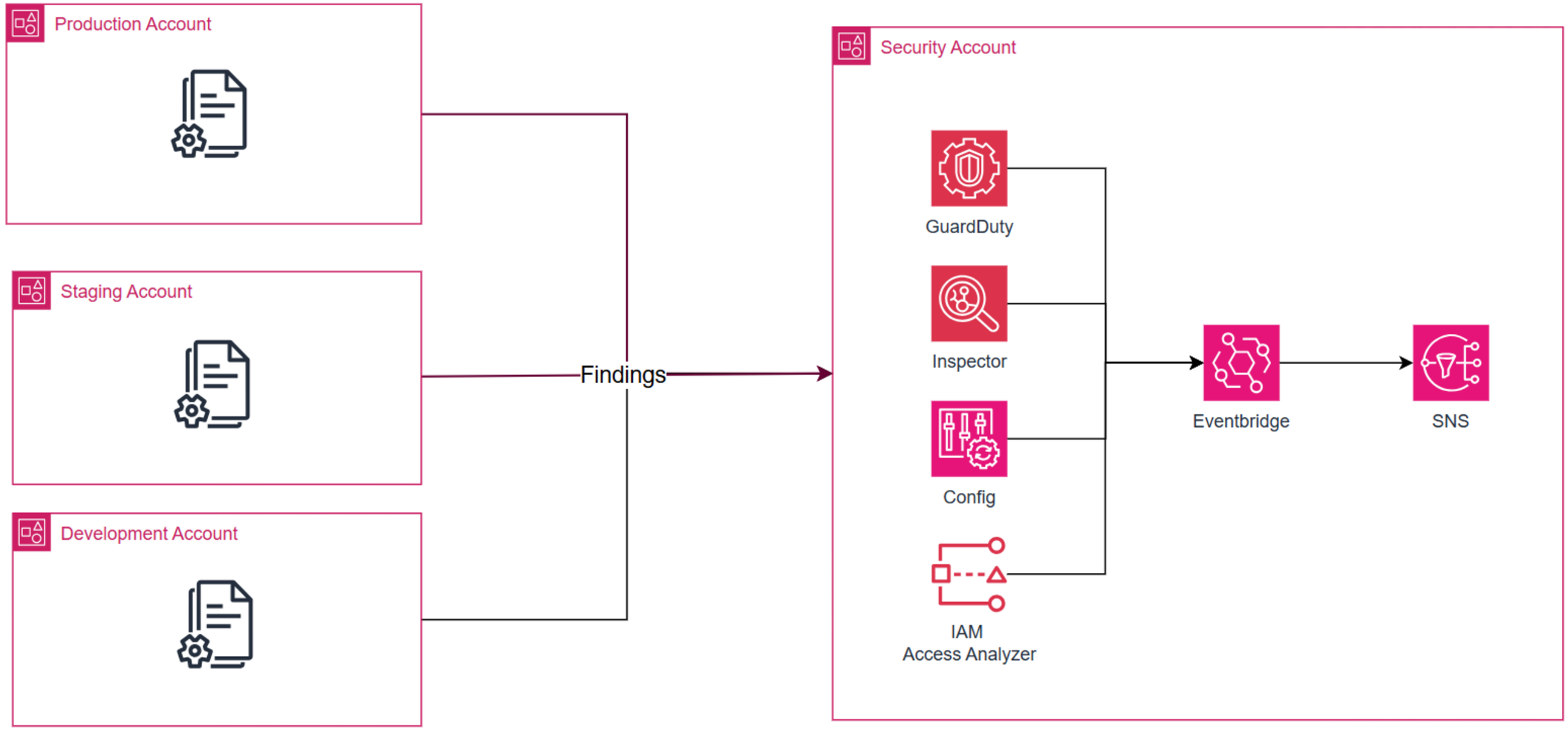
1. 중규모 아키텍처

(2) 과도한 권한 부여 및 내부자 위협 증가



1. 중규모 아키텍처

(3) 운영 실수로 인한 리소스 외부 노출



1. 중규모 아키텍처

위협 모델링 및 대응 - 접근/인증 위협

T1 퇴사자 위협

IAM Identity Center에서 사용자 비활성화를 통해 전 계정 세션 즉시 만료되고 신규 로그인을 차단

T2 내부 임직원 위협 (실수, 악의적)

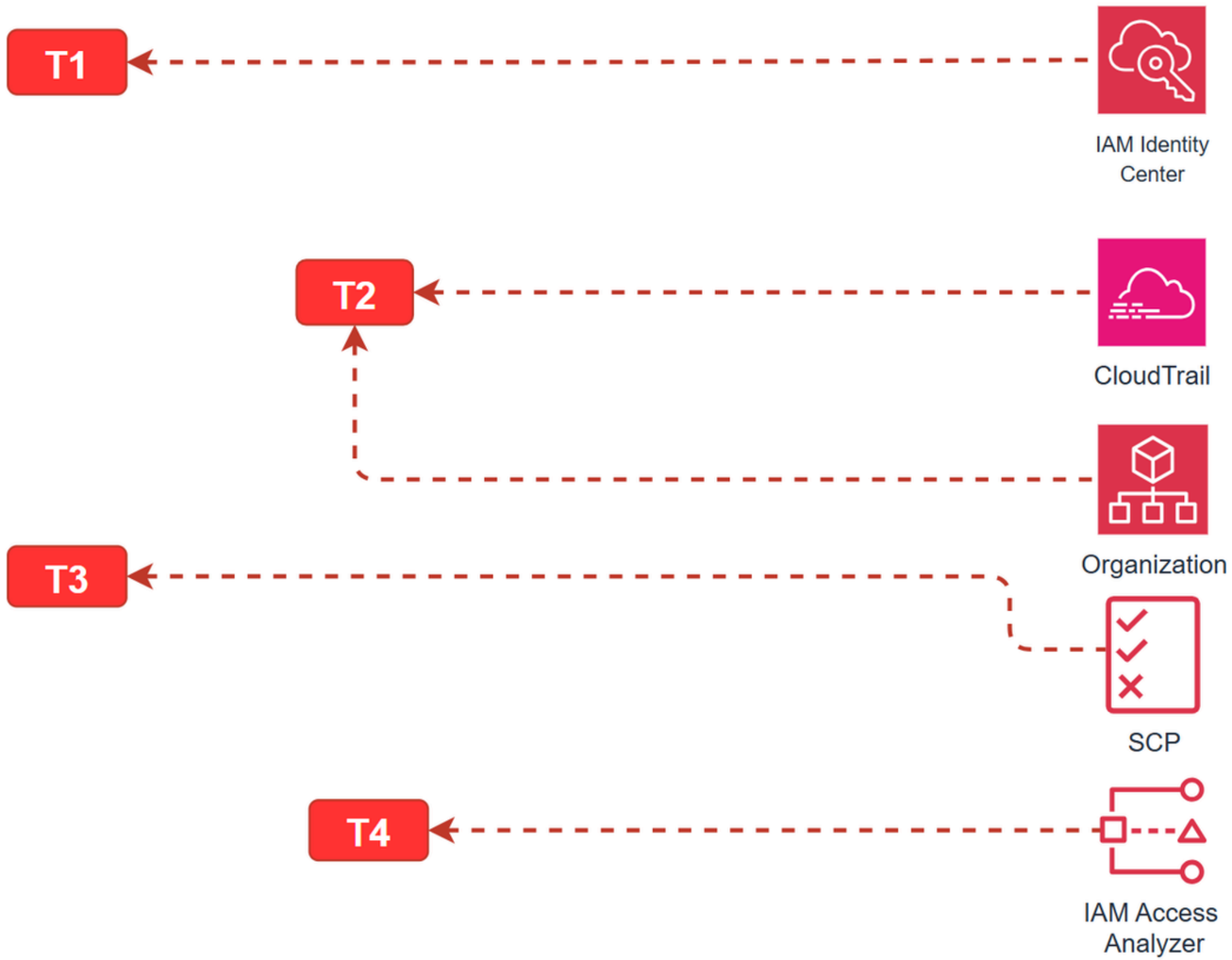
계정 분리를 통한 최소 권한으로 접근을 제한하고, 모든 API 호출을 CloudTrail로 기록하여 추적

T3 권한 에스컬레이션

SCP로 위험 IAM 행동(예: iam:PassRole 등)을 조직 단위에서 차단

T4 IAM 자격증명 유출

Access Analyzer로 자격증명 노출을 탐지하고, Secrets Manager로 코드 내 하드코딩을 방지



1. 중규모 아키텍처

위협 모델링 및 대응 - 워크로드/데이터 위협

T5 CI/CD 파이프라인 침해 및 내부자에 의한 악성 이미지 삽입

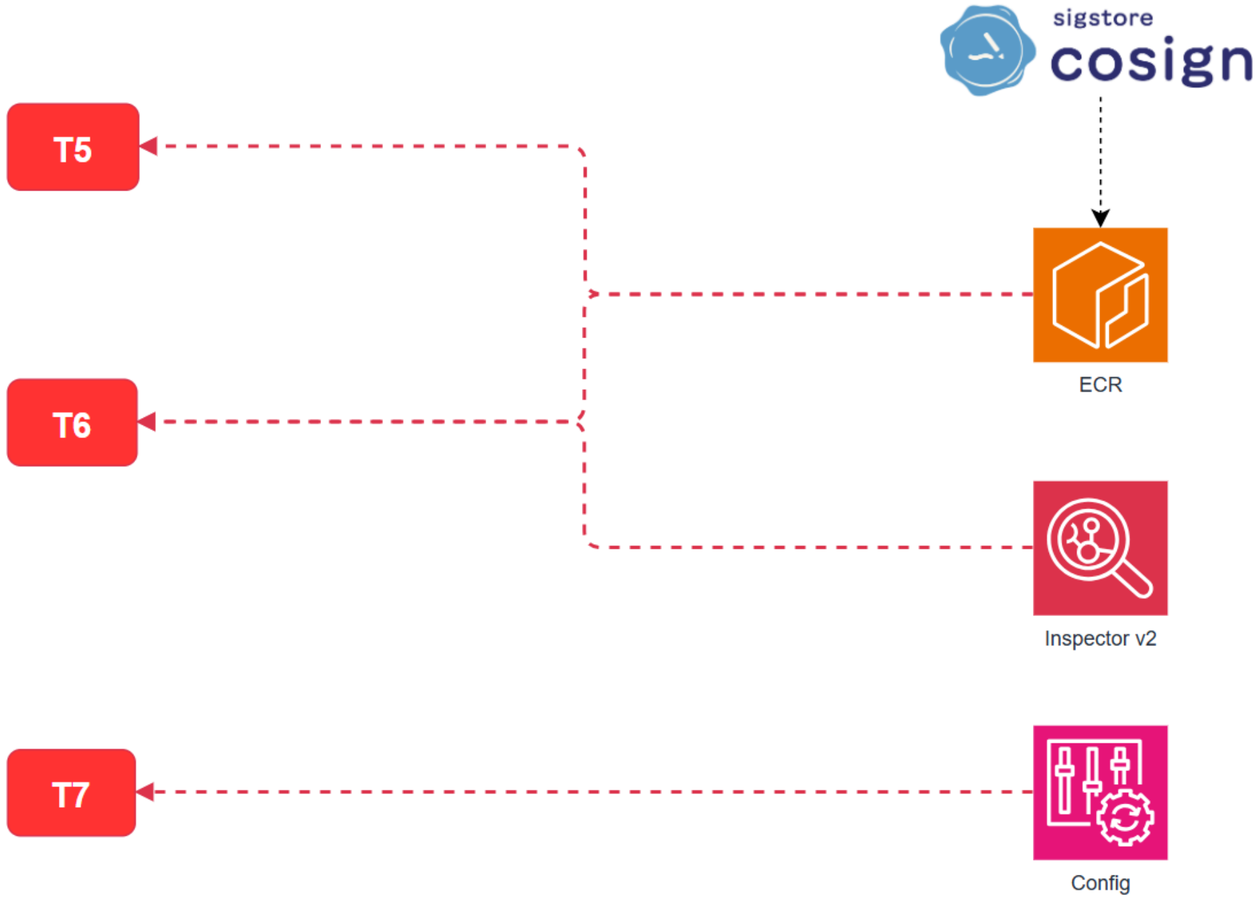
ECR push 시 Image Signing(cosign)으로 서명 검증해
변조되거나 서명되지 않은 이미지 배포를 차단

T6 앱 레이어에서의 공급망 공격

ECR push 시 Inspector Enhanced Scanning이
앱 의존성 레이어까지 스캔하여 오염된 라이브러리를 탐지

T7 S3 버킷(로그, 스냅샷) 공개 노출

Config 규칙으로 퍼블릭 스냅샷 설정을 자동 탐지하고,
암호화를 적용하여 외부 노출 시에도 평문 데이터를 보호



1. 중규모 아키텍처

위협 모델링 및 대응 - 네트워크/트래픽 위협

T8 비정상 트래픽 및 포트 스캔

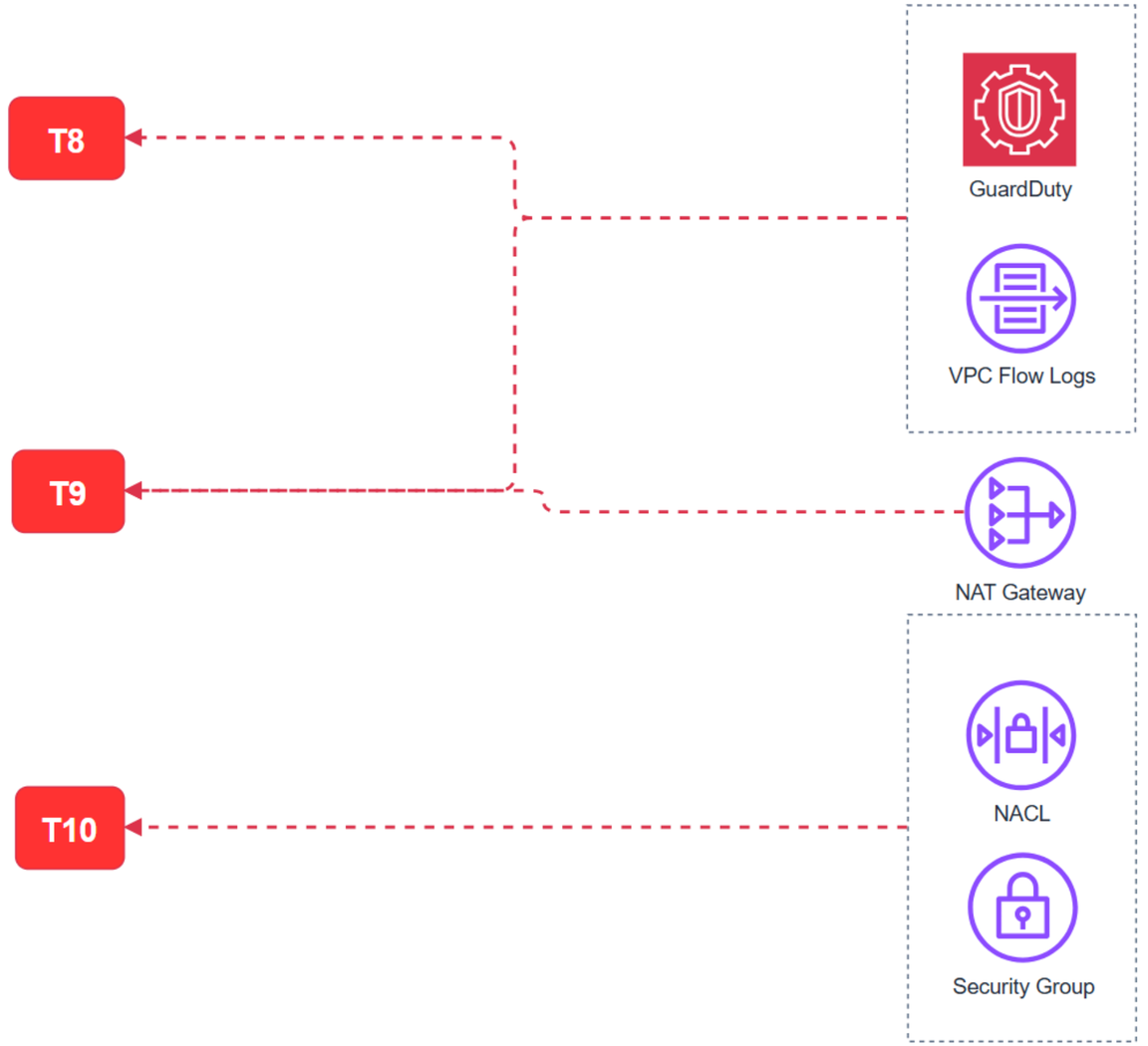
VPC Flow Logs로 트래픽 패턴을 수집하고,
GuardDuty가 포트 스캔 및 알 수 없는 외부 IP 통신을 탐지

T9 C2 서버 등 외부로 데이터 유출

GuardDuty와 VPC Flow Logs로
비정상 아웃바운드 트래픽을 탐지하고,
NAT GW로 허용된 엔드포인트 외의 통신을 차단

T10 내부 서비스 횡적 이동

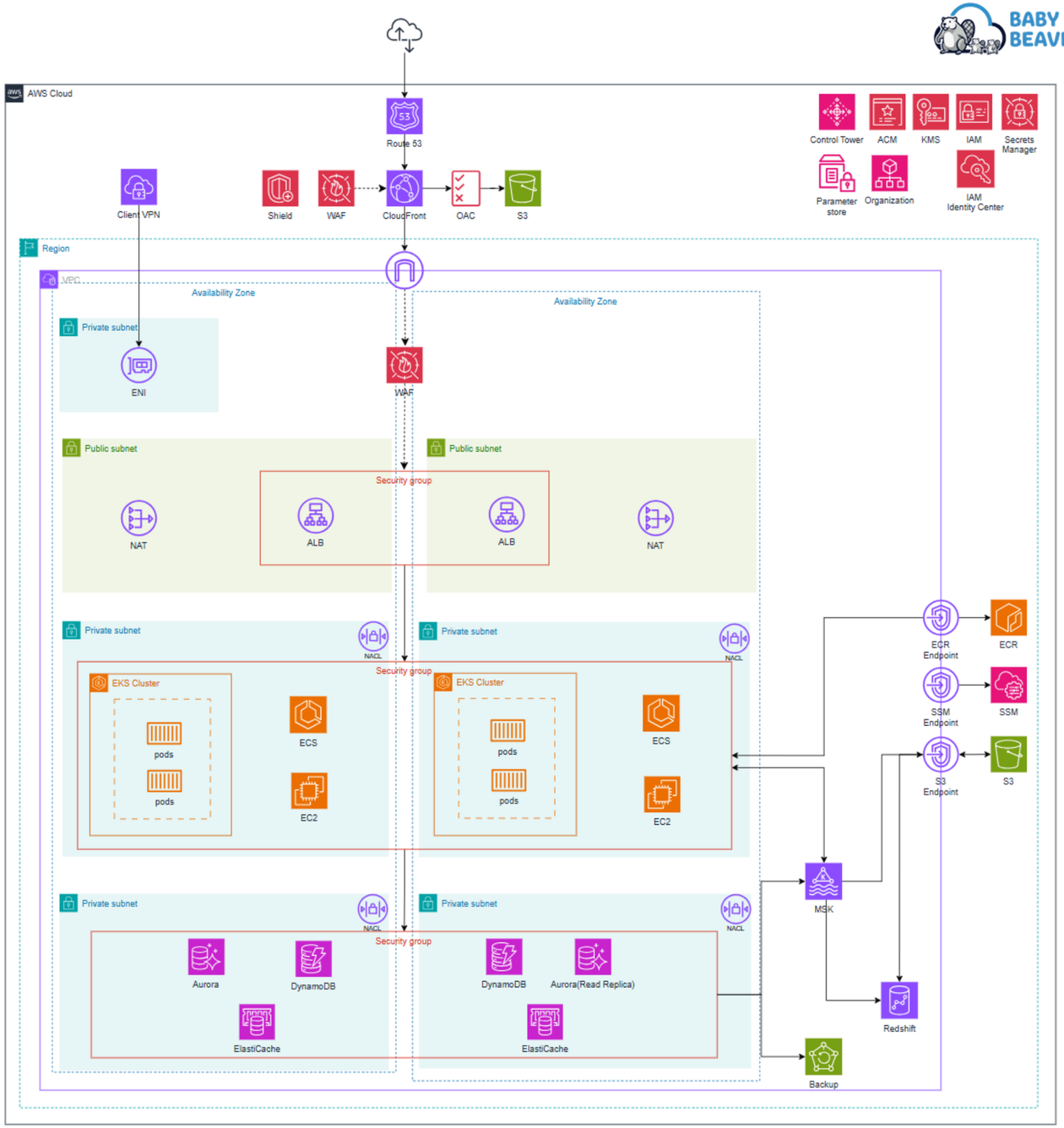
Security Group을 계층별로 최소 개방하여
서비스 간 불필요한 접근을 차단하고 NACL로 추가 방어



2. 중대규모 아키텍처

아키텍처 개요

- 가정
  - 임직원 300명(AWS 접근 인원 약 30명 가정)
  - 사용자 700만명 ~
  - 무신사, 티빙, 마켓컬리
- 아키텍처 상세 설명



2. 중대규모 아키텍처

중대규모 전환 시 주요 보안 과제 – “조직이 커지면 수동 관리에 한계가 생긴다”

방대한 양의 로그 분석의 어려움

SITUATION

규모가 점점 더 커지면서, 방대한 양의 로그를 사람이 직접 분석하는 것이 불가능해짐.

SOLUTION

SIEM 구조 도입 (Opensearch)

수동 위협 탐지의 한계

SITUATION

사람이 일일이 이상 탐지 결과를 확인할 수 없어 중요한 위협들을 놓칠 수 있음

SOLUTION

Security Hub + Eventbridge + Lambda

다중 계정의 통제 어려움

SITUATION

계정 수가 크게 증가해 조직 관리가 어려워짐.

SOLUTION

Control Tower 도입

2. 중대규모 아키텍처

중대규모 전환 시 주요 보안 과제 – “조직이 커지면 수동 관리에 한계가 생긴다”

이미지 취약점 관리 한계

SITUATION

검증되지 못한 AMI에 CVE 취약점 등이 포함되어도 모를 수 있음.

SOLUTION

Golden AMI Pipeline

네트워크 보안 Rule 파편화

SITUATION

VPC가 증가하면서 일관된 방화벽 규칙을 적용하거나 전체 현황을 통제할 수 없게 됨

SOLUTION

Firewall manager

아키텍처 복잡성 증가

SITUATION

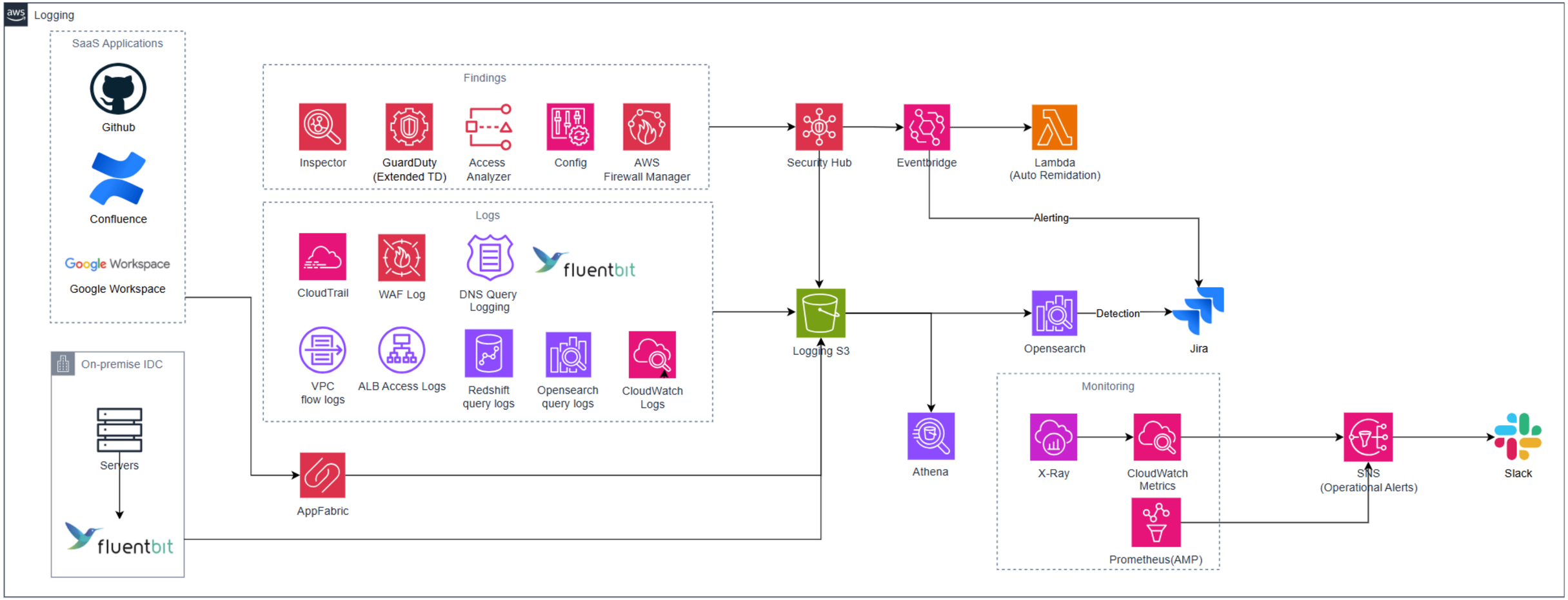
아키텍처를 콘솔로 관리하기 매우 어려워짐

SOLUTION

인프라를 모두 IaC로 관리 강제 (IaC를 검증하는 Checkov)

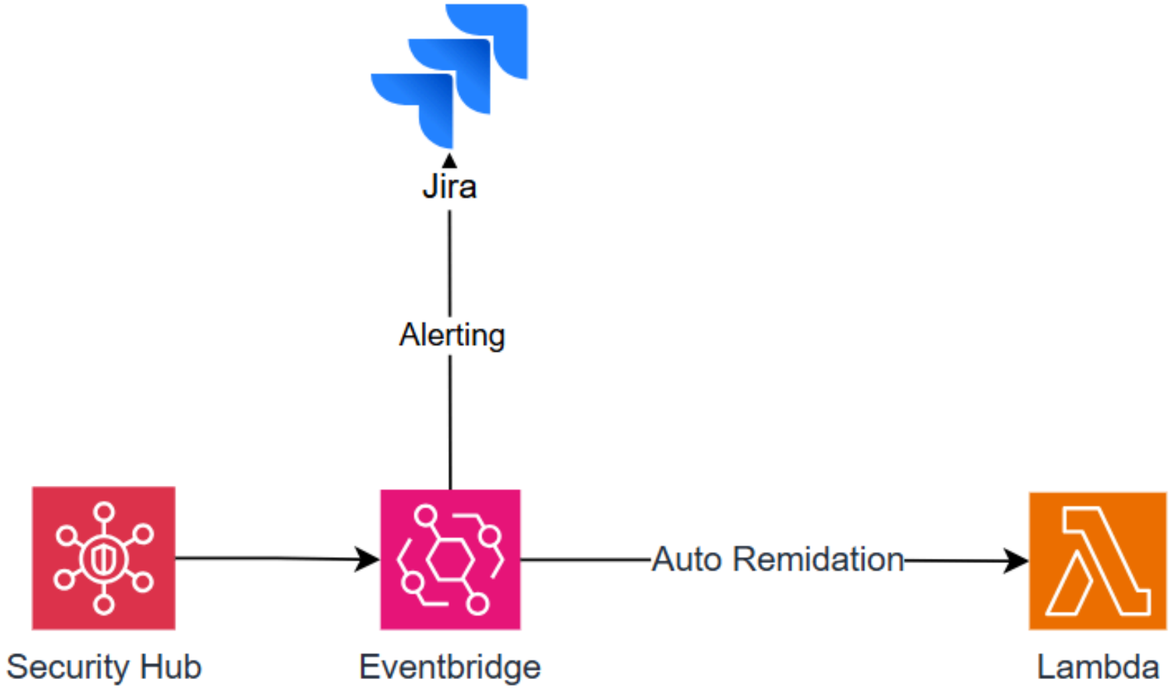
2. 중대규모 아키텍처

(1) 방대한 양의 로그 분석의 어려움



2. 중대규모 아키텍처

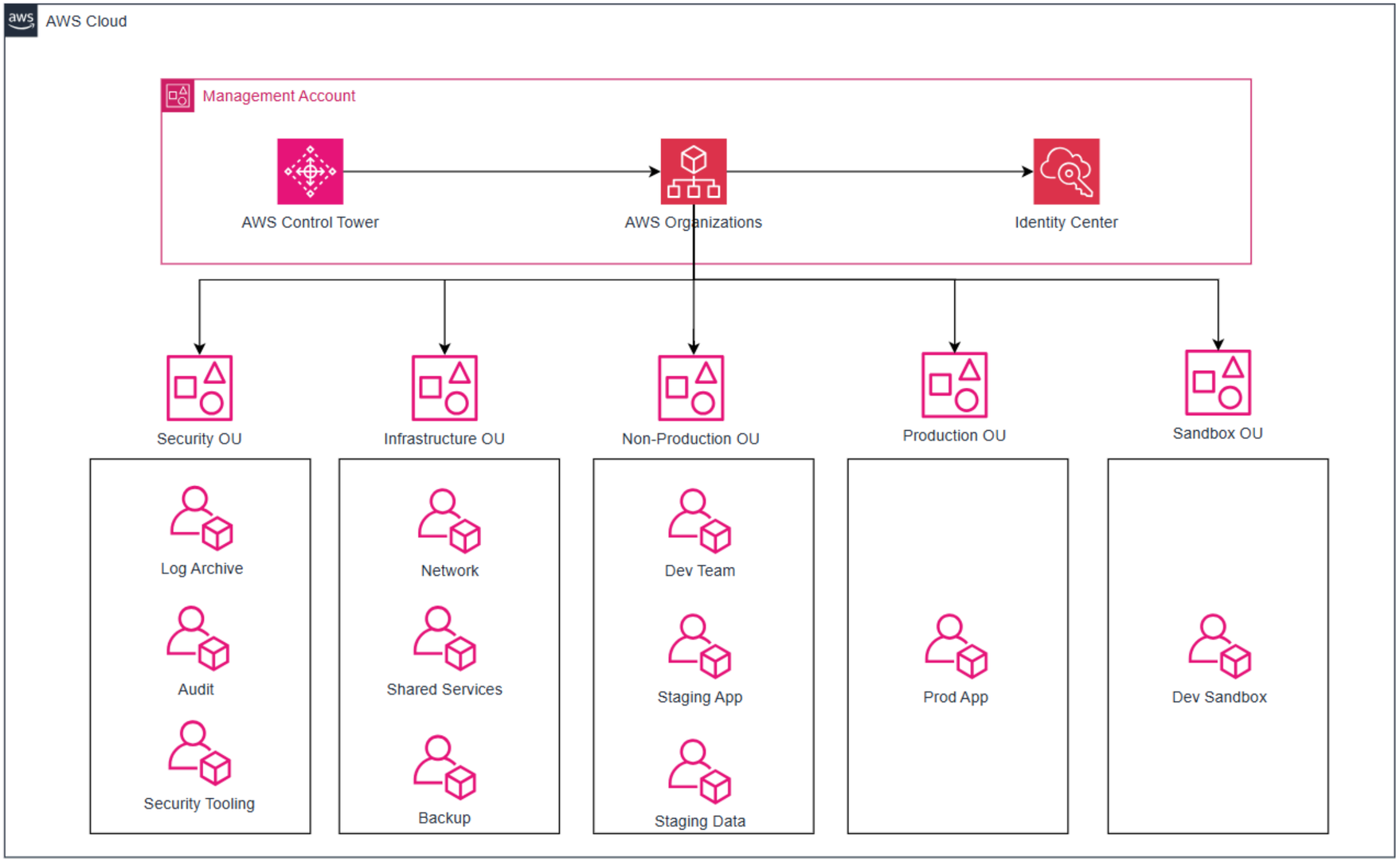
(2) 수동 위협 탐지의 한계



Security Hub Findings	위협
악성 IP IAM API 호출	공격 진행 중
EKS 크립토마이닝	코드 실행 중
EKS 포트 포워딩	백도어 진행 중
CloudTrail 비활성화	공격 은닉 시도
EC2·EKS 악성 아웃바운드	악성코드 감염·C2 통신 중
GuardDuty 비활성화 탐지	탐지 회피 의도
Route53 퍼블릭 호스팅 존 변조	전체 트래픽 탈취 위험
MSK 비인가 접근	이벤트 스트림 전체 노출
Self-hosted Runner 침해	CI/CD 전체 장악 가능
ECR 이미지 변조	컨테이너 환경 전체 침해

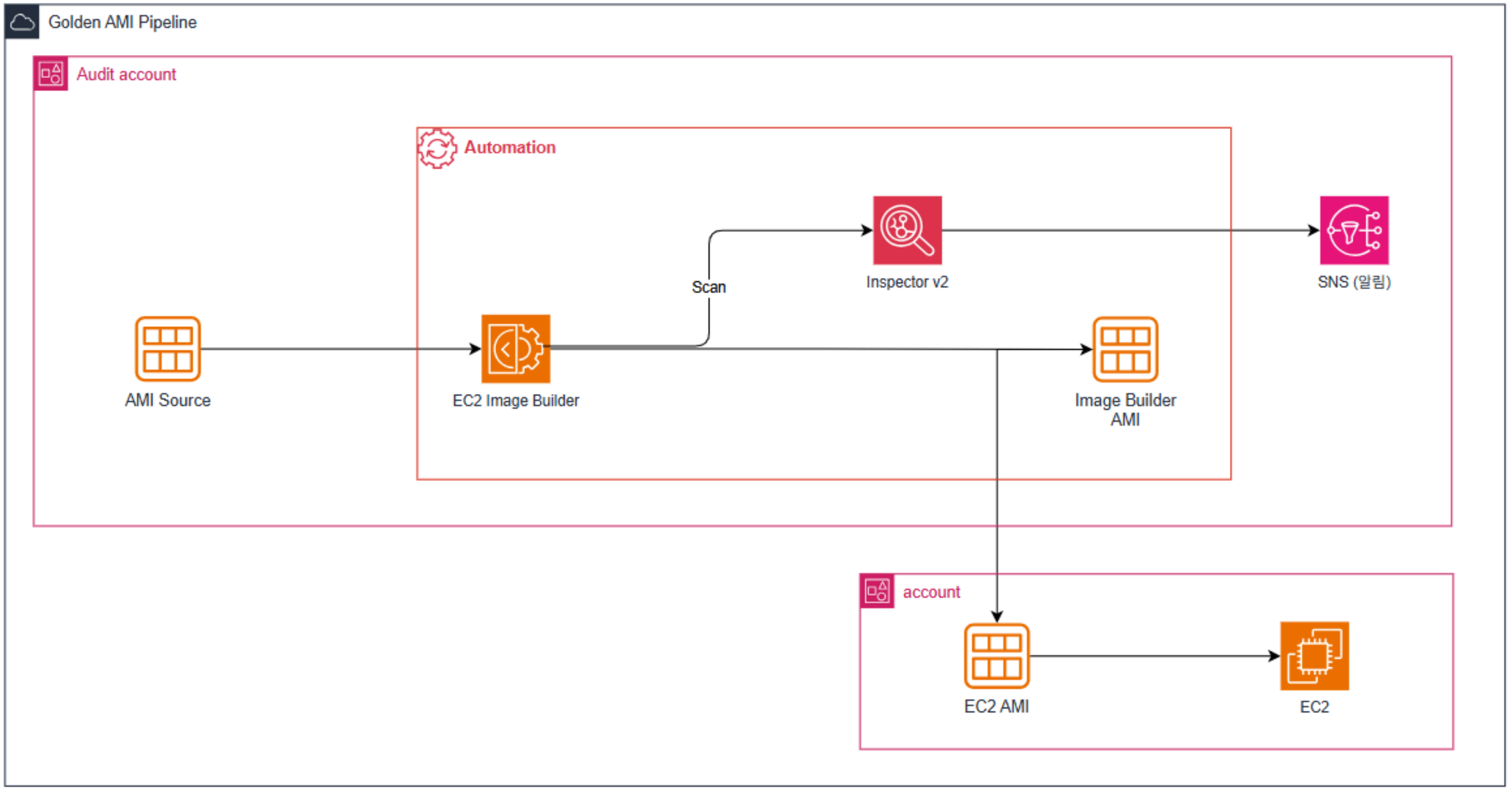
2. 중대규모 아키텍처

(3) 다중 계정의 통제 어려움



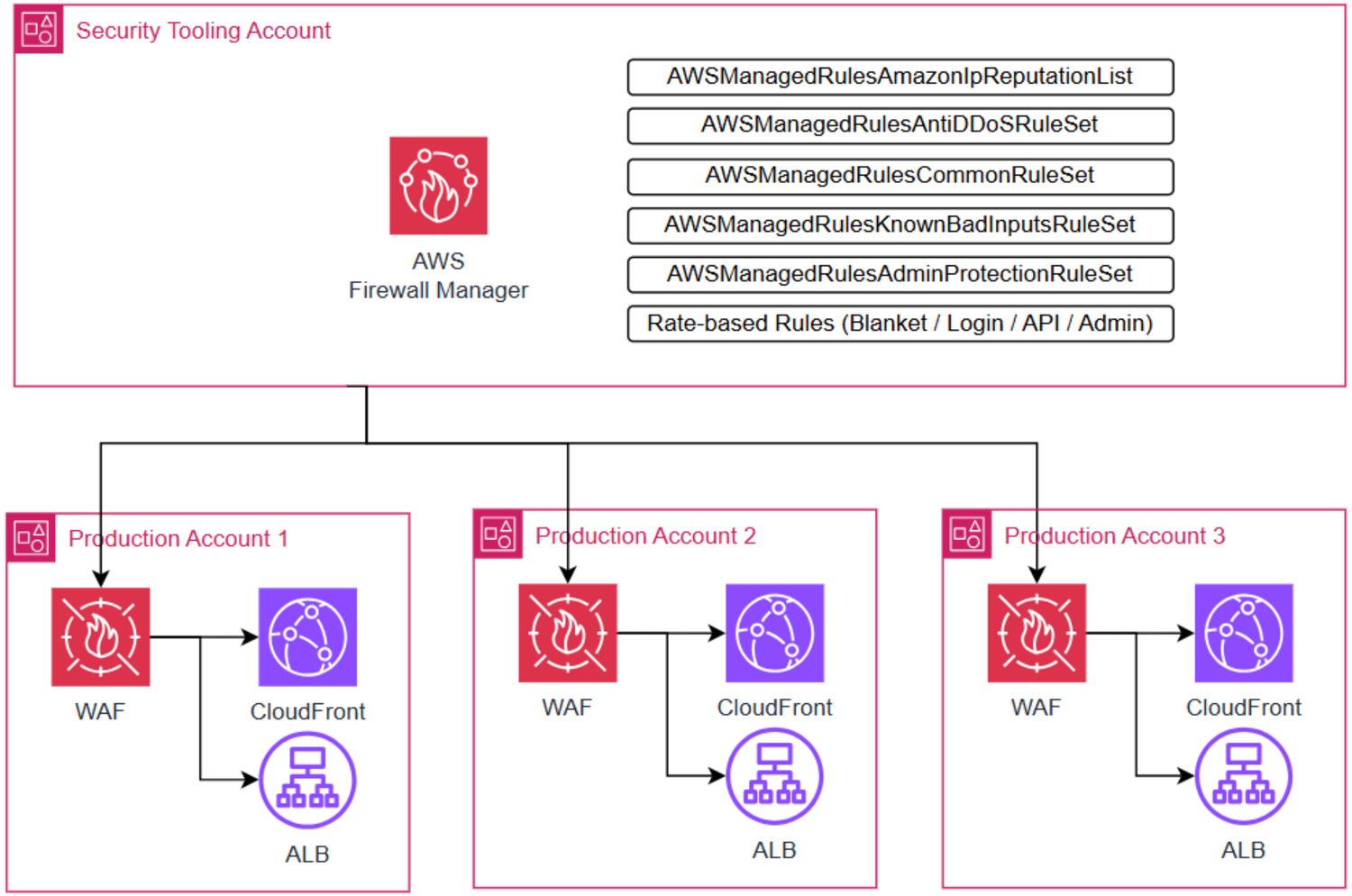
2. 중대규모 아키텍처

(4) 이미지 취약점 관리 한계



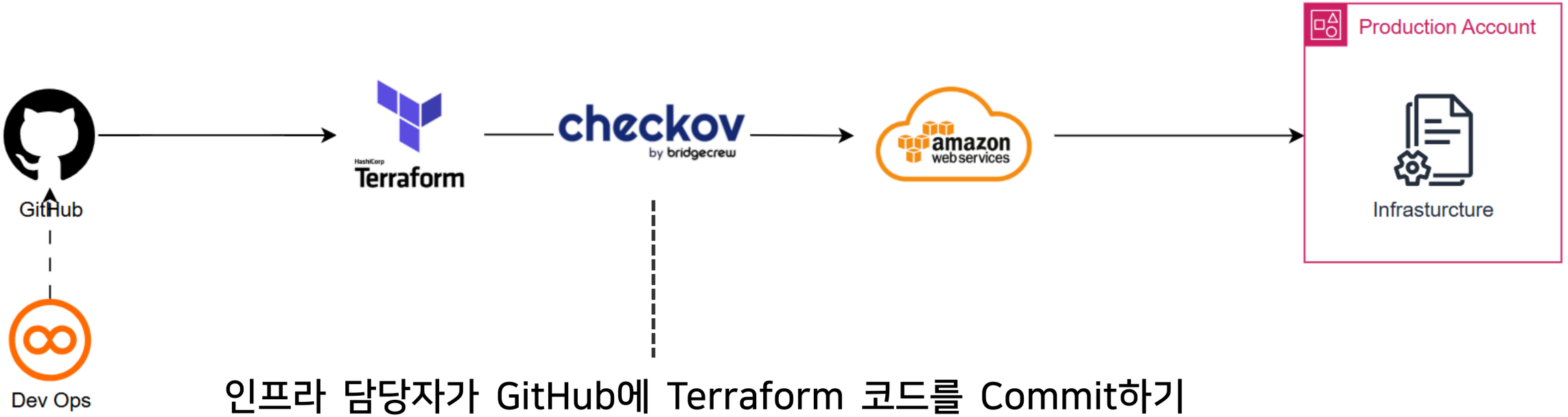
2. 중대규모 아키텍처

(5) 네트워크 보안 Rule 파편화



2. 중대규모 아키텍처

(6) 복잡한 아키텍처의 관리 어려움



인프라 담당자가 GitHub에 Terraform 코드를 Commit하기 전 Checkov로 보안 취약점을 사전 점검하고, PR 단계에서도 동일하게 점검하여 문제가 발견될 경우 Commit 및 Merge를 차단한다.

2. 중대규모 아키텍처

(1) 위협 모델링 및 대응

T1 취약한 워커 노드 배포

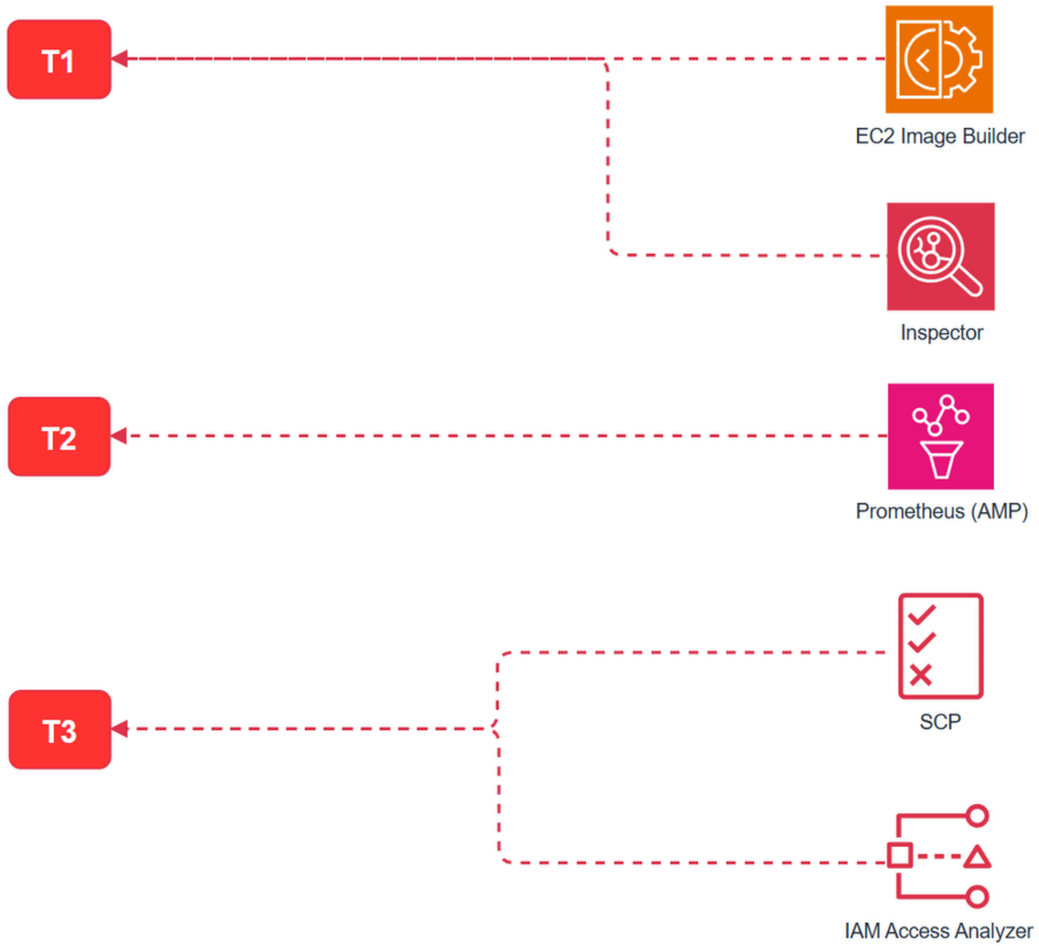
EC2 Image Builder 기반 Golden AMI 생성 후
Inspector 검증 및 승인 기반 배포

T2 컨테이너·노드 상태 가시성 부족

Prometheus 기반 CPU·메모리·네트워크 메트릭 수집으로 클러스터 및 워크로드 상태를 모니터링

T3 멀티계정·멀티클러스터 권한 오남용

서비스 계정별 최소 권한 적용,
조직 단위 SCP 제한 및 교차 계정 권한 탐지



2. 중대규모 아키텍처

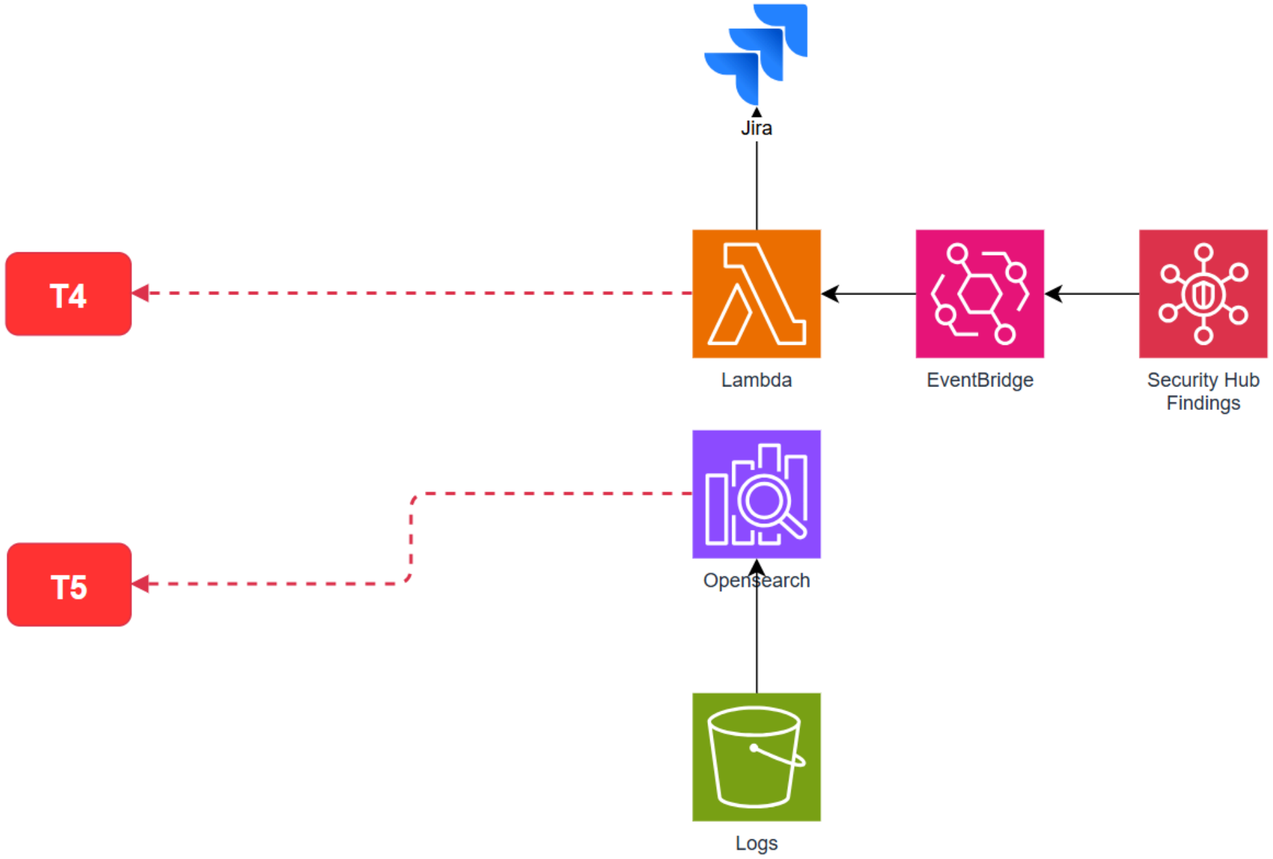
(2) 위협 모델링 및 대응

T4 탐지 후 수동 대응 지연

Finding 발생 시 Lambda가 자동으로 Security Group 격리·노드 차단 수행 및 Jira Ticket 자동 발행

T5 로그 분석 누락

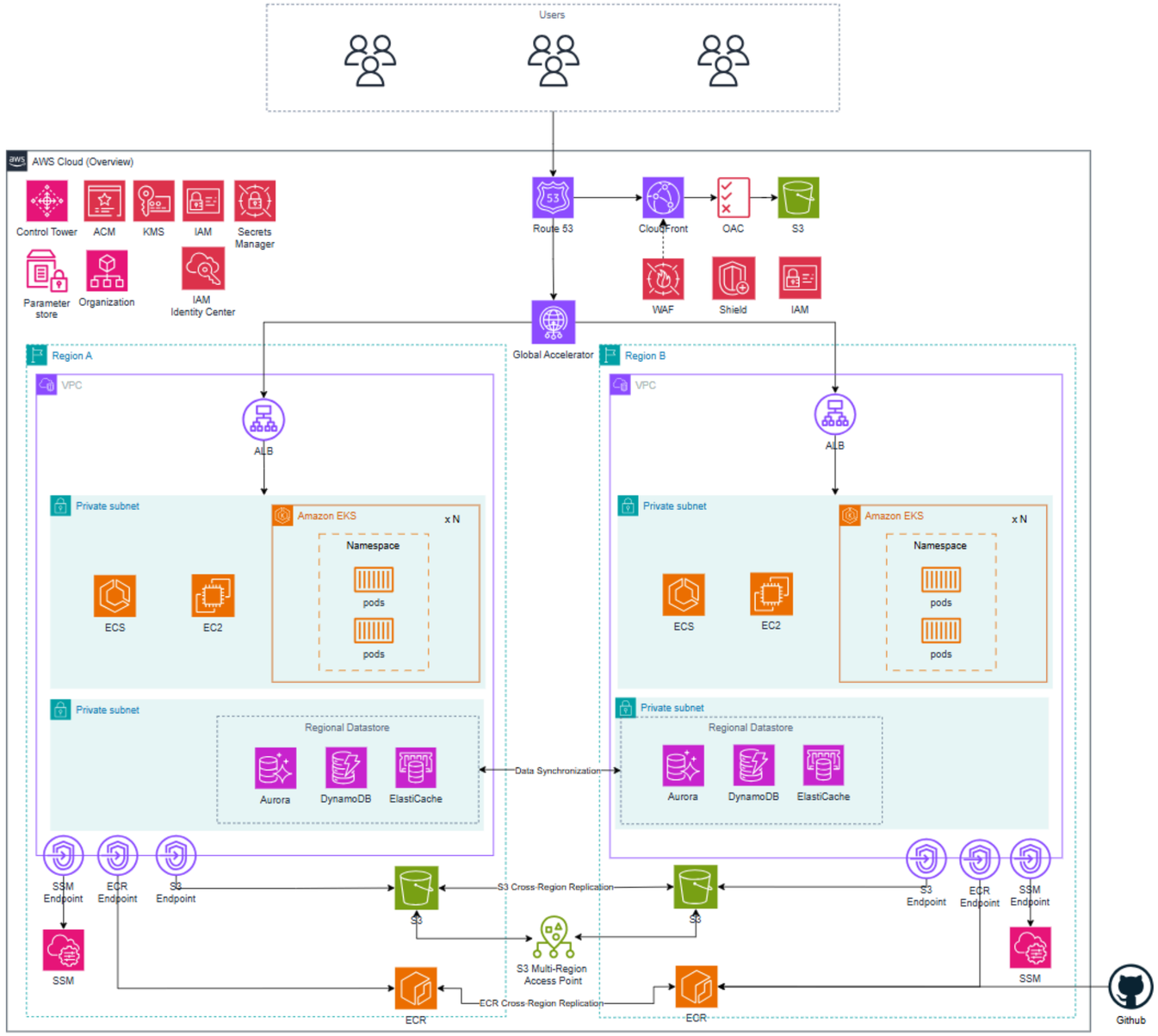
OpenSearch 기반 SIEM 구조를 도입해 로그 자동 인덱싱, Dashboards 실시간 시각화 · 이상 패턴 알림 룰 설정 가능



3. 대규모 아키텍처

아키텍처 개요

- 가정
  - 임직원 2000명
    - AWS 접근 인원 약 200~250명 가정
  - 사용자 1000만명 이상 ~
- 아키텍처 상세 설명



3. 대규모 아키텍처

대규모 전환 시 주요 보안 과제 – “공격 포인트가 글로벌로 확대된다”

글로벌 서비스 확장

SITUATION

서비스가 여러 리전에 걸쳐 확장됨

SOLUTION

멀티 리전 보안, ZTNA, Shield Advanced

임직원수가 크게 증가

SITUATION

글로벌화 및 서비스 규모의 증가로 임직원수가 폭발적으로 증가했음

SOLUTION

보안 OU 권한 세분화로 횡적 이동 방지, EDR

규제 및 컴플라이언스

SITUATION

규모가 커지며 사용자 수가 크게 증가하면서 컴플라이언스 고려가 필요해짐

SOLUTION

Macie, SCP, Detective 도입

위협 대응 한계

SITUATION

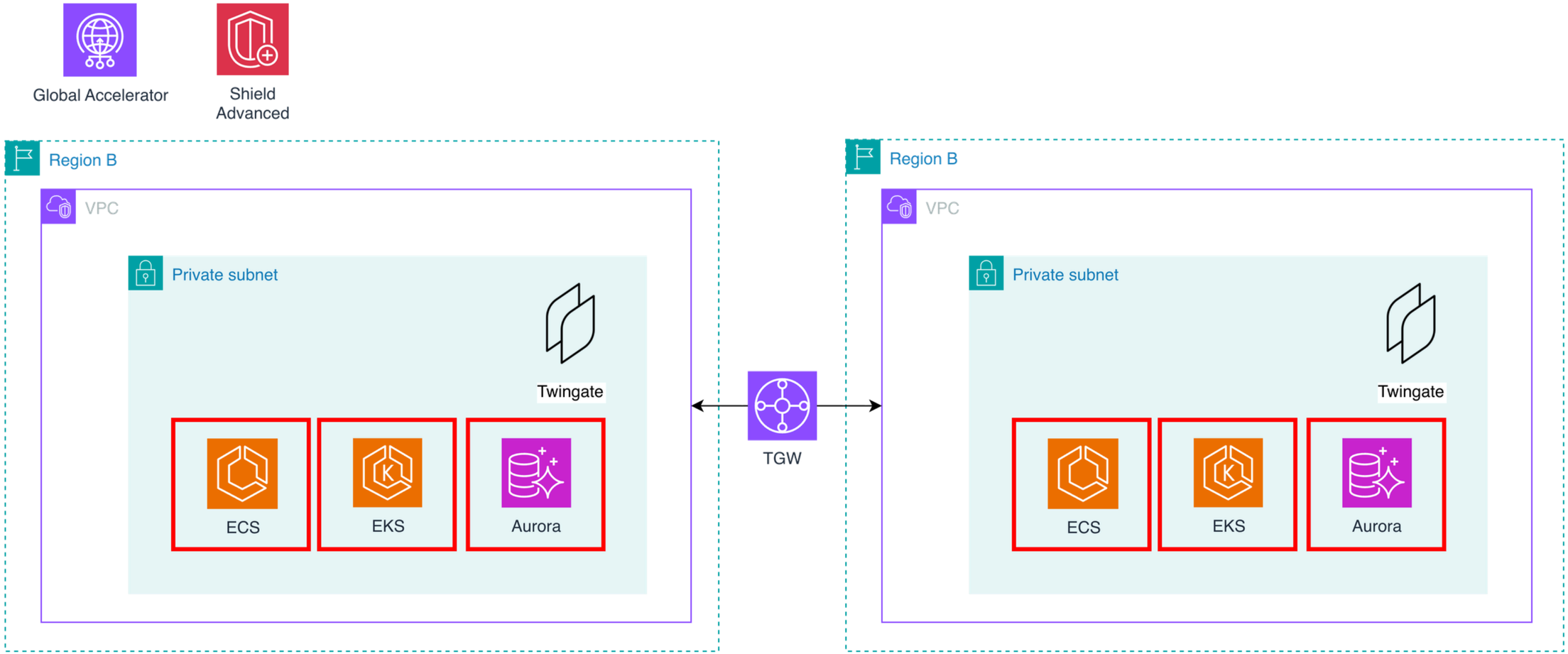
로그 양의 증가 및 다양한 위협의 대두로, 위협 대응 및 탐지 Rule 관리가 어려워짐

SOLUTION

상용 SIEM / SOAR 도입

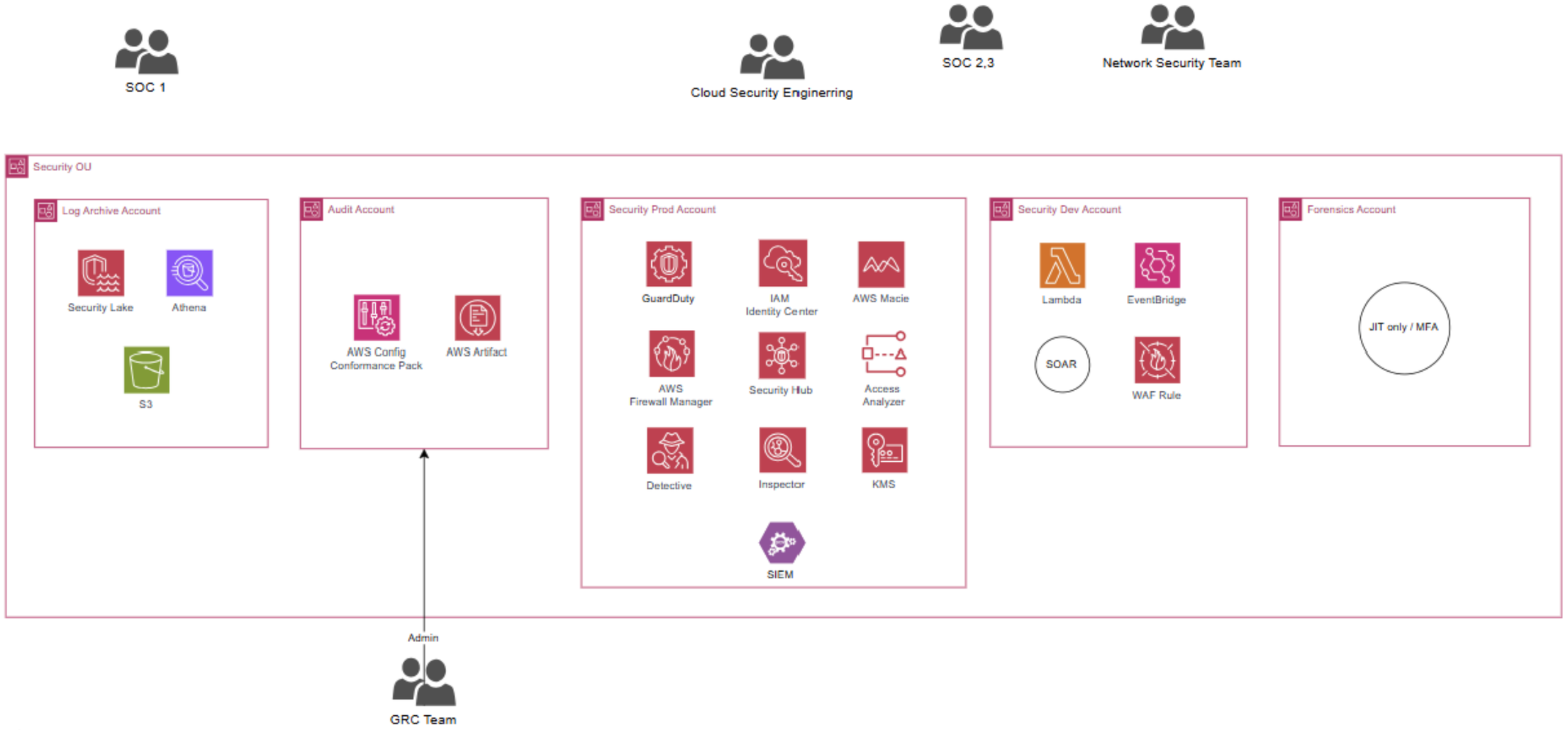
3. 대규모 아키텍처

(1) 서비스가 여러 리전에 걸쳐 확장



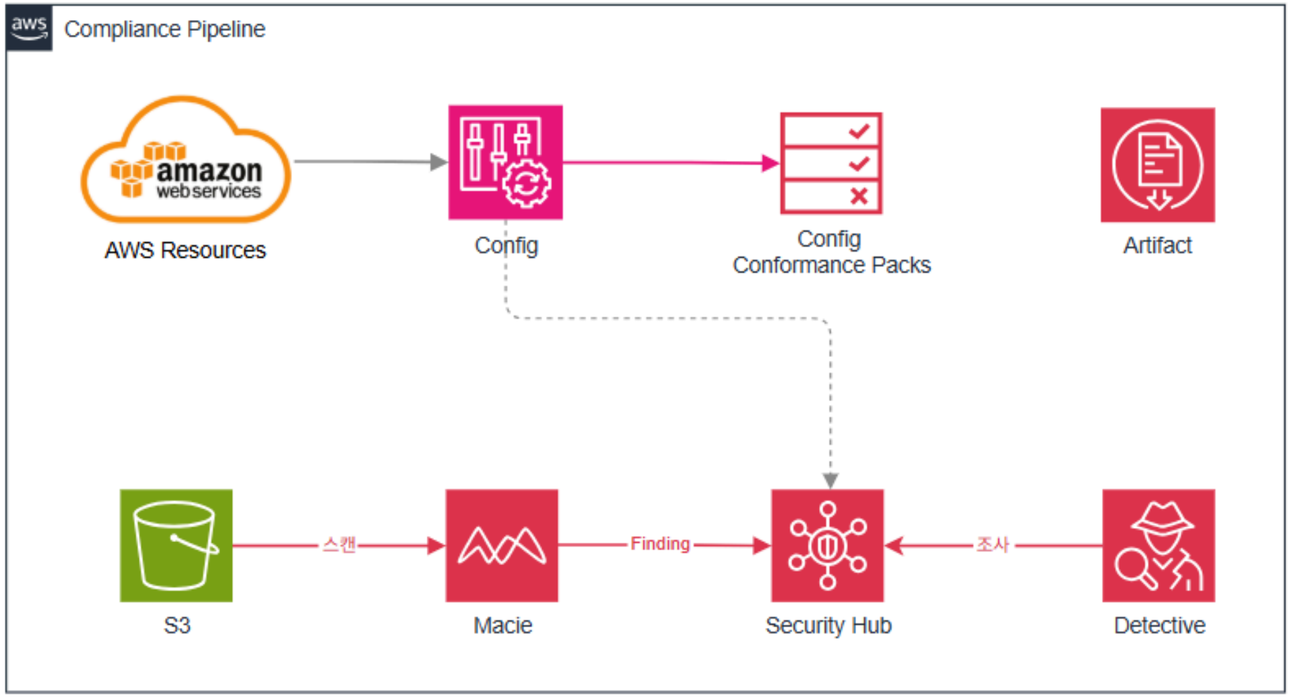
3. 대규모 아키텍처

(2) 임직원수가 크게 증가



3. 대규모 아키텍처

(3) 컴플라이언스 대응



Macie

- 중요 데이터에 대한 지속적인 식별 및 모니터링 체계를 구축하여 데이터 유출 위험 최소화
- 민감정보 탐지 결과를 중앙 보안 체계(Security Hub)와 연계해 컴플라이언스 대응 가시성 확보

Detective

- GuardDuty Findings 기반으로 CloudTrail API 호출, IAM 활동, VPC Flow Logs 네트워크 흐름을 연관 분석하여 침해 원인 추적
- 조사 과정에서 변경 이력과 행위 로그를 확보해 감사 대응 및 증적 수집 체계를 강화

3. 대규모 아키텍처

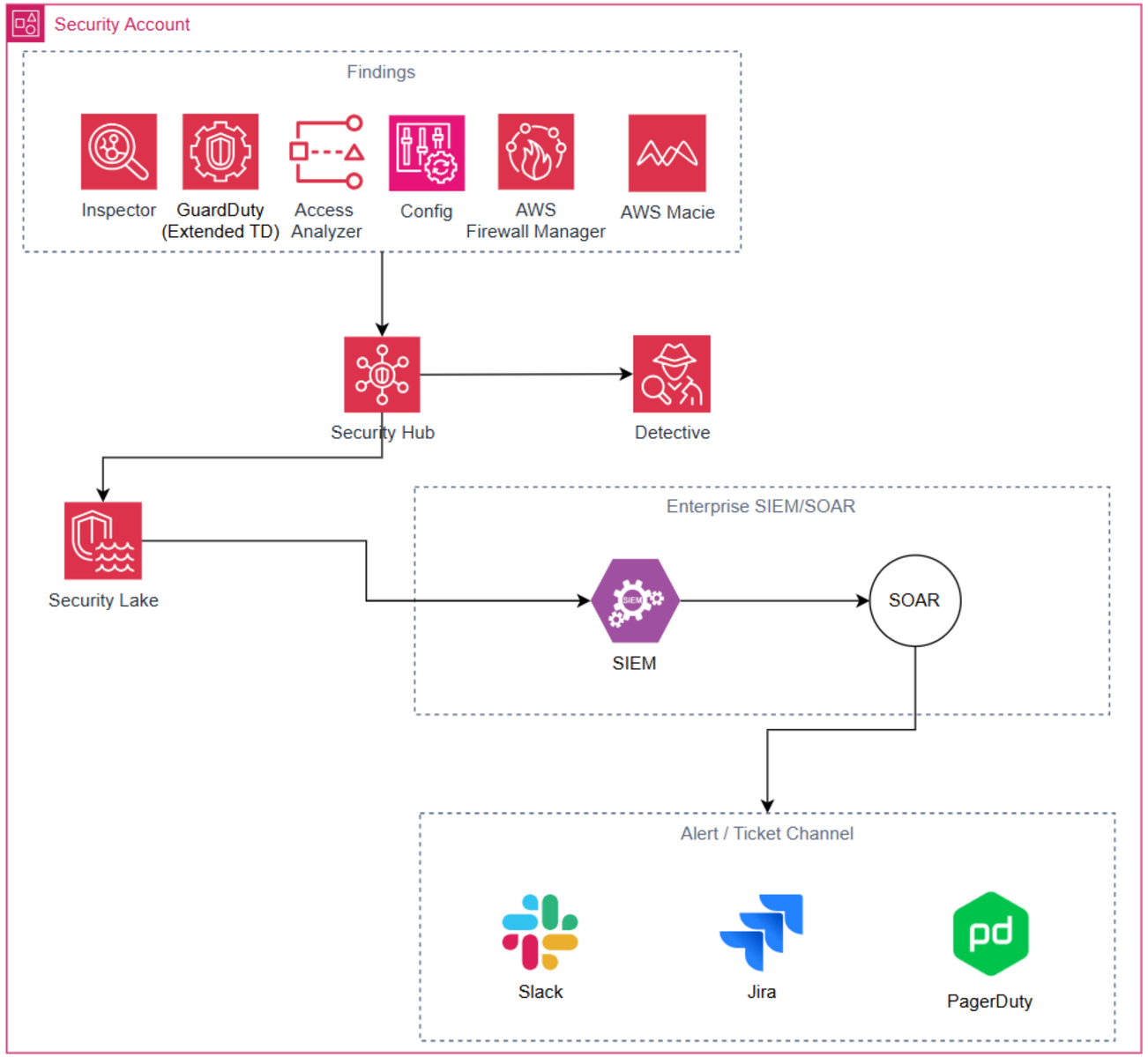
(4) 위협 대응 및 Rule 관리가 어려워짐

기존 OpenSearch / Lambda 기반 대응의 한계

- 이벤트 증가로 Lambda 탐지·대응 로직 관리 복잡도 증가
- OpenSearch 기반 장기 운영 시 비용·성능 부담 발생
- 멀티 계정·리전 확장 시 중앙 가시성 확보 한계

Enterprise SIEM / SOAR 도입

- Security Hub·Security Lake 기반 중앙 수집 및 통합 분석
- 상용 SIEM의 사전 정의된 탐지 Rule 및 위협 인텔리전스를 활용해 운영 효율성 향상



3. 대규모 아키텍처

(1) 위협 모델링 및 대응

T1 VPN의 과도한 권한으로 인한 내부망 침투

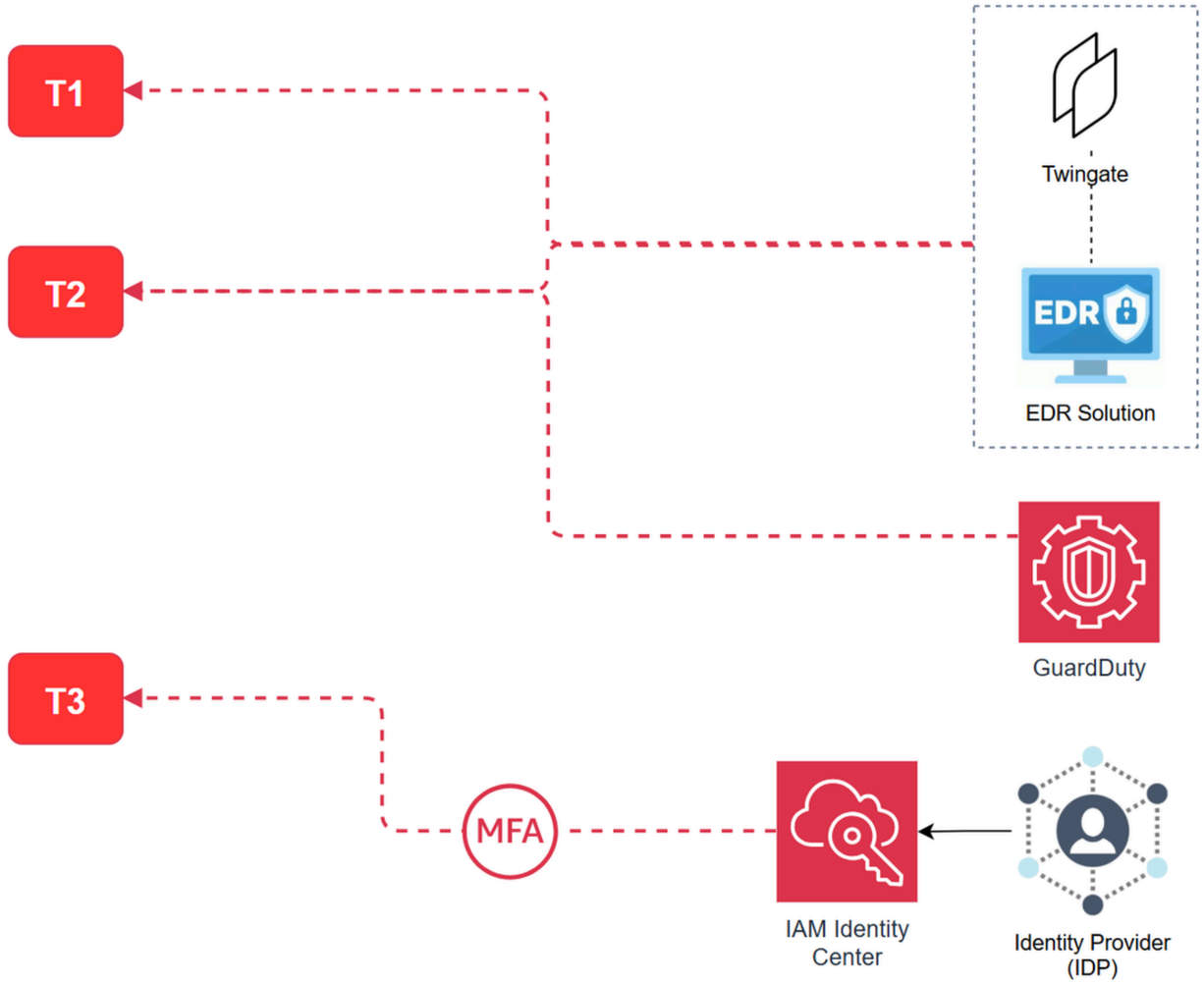
VPN을 제거하고 Twingate 기반 ZTNA로 전환, 애플리케이션 단위 최소 권한 접근만 허용

T2 감염된 디바이스를 통한 내부망 침투

CrowdStrike 등 EDR을 Verified Access 디바이스 신뢰 공급자로 연동해, 감염 디바이스 접근 차단

T3 IdP 침해를 통한 ZTNA 우회

IdP를 통해 AWS에 접근하는 모든 계정에 IAM Identity Center 추가 MFA를 필수 적용



3. 대규모 아키텍처

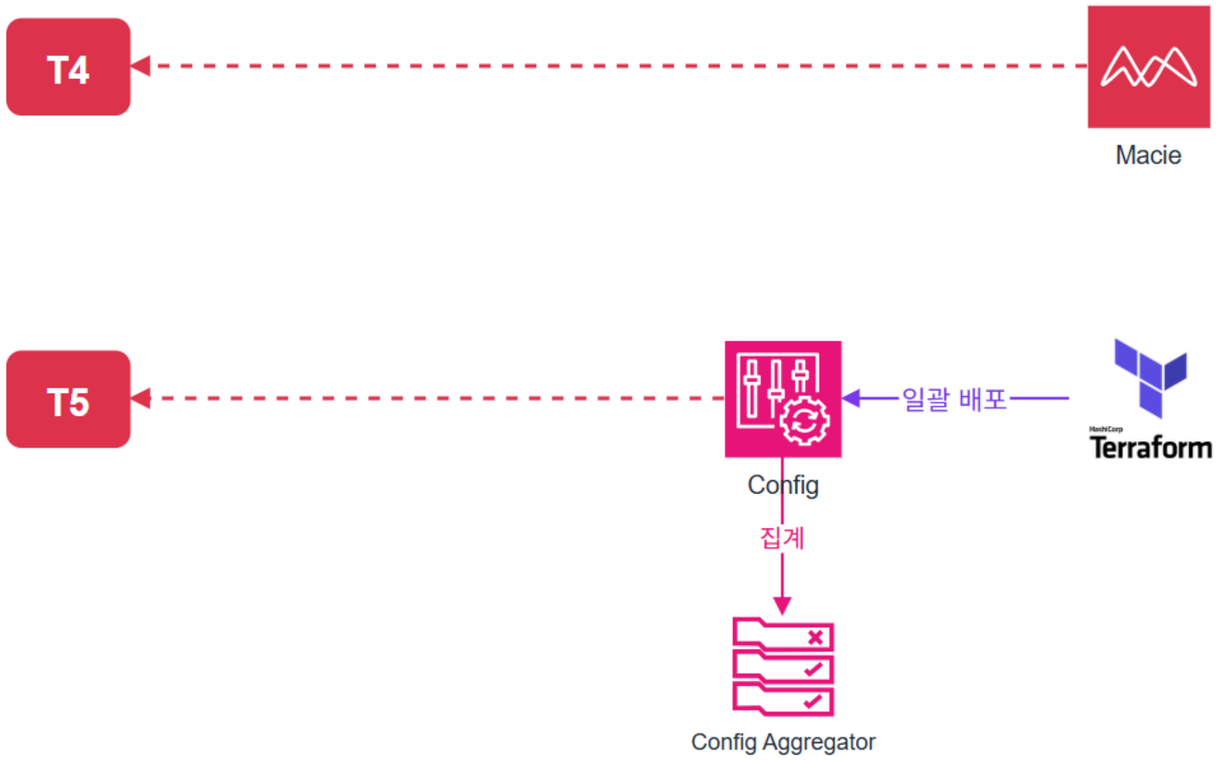
(2) 위협 모델링 및 대응

T4 S3 내 민감 데이터 노출 및 유출

Macie가 S3 버킷 전체를 자동 스캔하여 PII 포함 객체를 탐지

T5 멀티리전 설정 불일치로 인한 보안 공백

Terraform으로 Config Rules를 전 리전에 일괄 배포,
Config Aggregator로 전 계정 및 리전 준수 현황 중앙 집계



4. 비용

예상 비용

요청/사용량 기반 비용

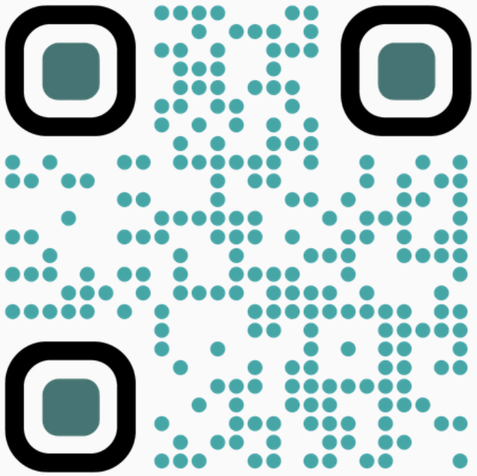
서비스	단위	단가	가정 사용량	월 비용	산출 근거
WAF	요청 수	$0.60 / 100만 건	6,000만 건	$36.00	DAU 20만 × 5req × 30일 = 3,000만, 봇 포함 ×2배
CloudFront	인터넷 데이터 전송	$0.12 / GB	1,440 GB	$172.80	6,000만 요청 × 800 KB × 캐시히트율 30% 만 실제 전송 = 약 1,440 GB
CloudFront	오리진 데이터 전송	$0.06 / GB	90 GB	$5.40	캐시 MISS 30% → 1,800만 요청 × 동적 응답 5 KB
CloudFront	HTTPS 요청	$0.01 / 10,000건	6,000만 건	$6.00	WAF와 동일 요청 기준
NAT Gateway	데이터 처리	$0.059 / GB	300 GB	$17.70	외부 API 호출·CloudWatch Logs·SSM 아웃바운드 (S3·ECR은 VPC Endpoint 경유 제외)
KMS	API 요청 (대칭키)	$0.03 / 10,000건	10만 건	$0.30	ECS Task 기동·Secrets 조회 시 발생, S3 Bucket Key 적용으로 객체당 호출 제거

비용 계산 일부

최종 정리

구분	합계
고정 비용	$121.37 / 월
요청/사용량 기반 비용	$682.37 / 월
보안·거버넌스 서비스 총합 (추정)	약 $804 / 월

중규모 예상 비용



03

프로젝트 성과

프로젝트 산출물

프로젝트 회고

프로젝트 산출물

과제와 문서화, Terraform 모듈화

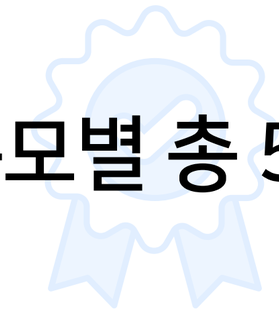
01

침해 사고 및
아키텍처 사례 분석

총 50개

02

OUR
BEST PRACTICE



규모별 총 5개

03

아키텍처 모듈화

Terraform

프로젝트 회고

두 달 간의 여정 마무리

클라우드 보안에 눈을 뜨다.

Baby beavers

- VPC가 뭐지?
- EC2/Fargate 차이가 뭐지?
- IAM이 뭐지?

Beavers

- 어떻게 안전하게 SCP를 Attach 할 수 있을까?
- 여러 서비스에서 발생하는 로그는 어떻게 안전하게 관리할 수 있을까?
- 조직이 커지면 권한 분리를 어떻게 해야할까?

TEAM 뭉살흩죽

감사합니다.

김민수 velog.io/@alstnalstn2 alstnuu22@gmail.com

이호영 lhywk.tistory.com lhywkd22@gmail.com

이지향 talk3130.tistory.com hyanglee0508@gmail.com

조휘정 velog.io/@hvvup hvvijung@gmail.com

Q&A