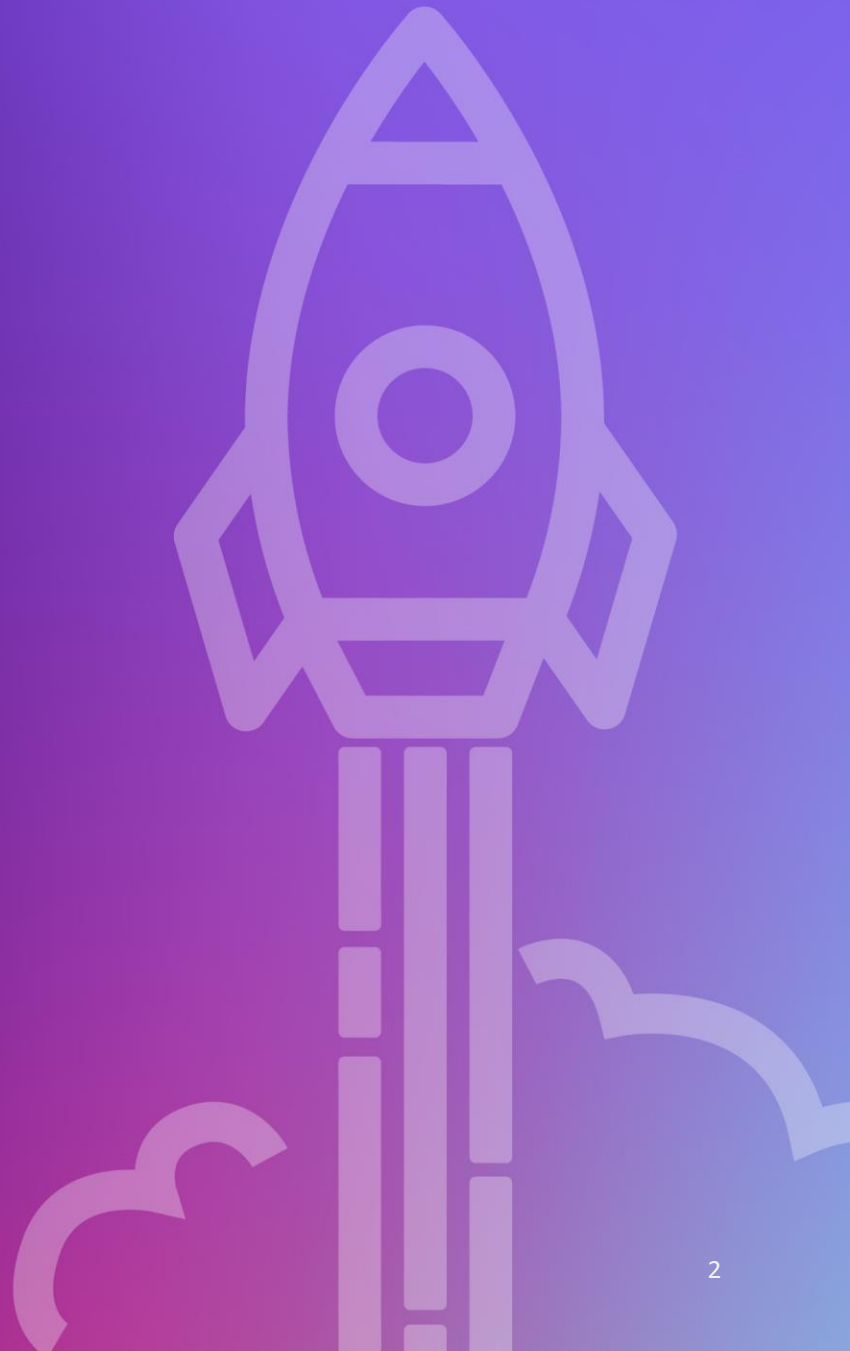
클라우드 네이티브 환경에서 오픈소스를 활용해 ISMS 인증을 성공적으로 취득한 노하우

공지훈

Security Compliance Engineer
Rapportlabs

Agenda

1. 들어가며
2. 보안 아키텍처 구성
3. Teleport를 통한 DB 접근제어
4. Prowler를 활용한 AWS 취약점 점검 및 관리
5. 마치며



RAPPORT LABS

패션 버티컬 커머스

4050 여성 3명 중 1명 사용

누적 다운로드 720만 이상

산지직송 식품 커머스

누적 다운로드 300만 이상

4050이 신뢰하는 전국팔도 제철 먹거리 판매

1. 들어가며

오늘의 발표가 정답은 아닙니다.

ISMS 취득을 위한 최선의 선택을 하는데 고려할 수 있는 선택지를 소개합니다.

1. 들어가며

- ISMS-P 개요
  - 기업이 (개인)정보보호를 위해 수립·운영하는 관리체계의 **최소 수준을 인증**
  - ISMS-P 와 ISMS 두 종류가 존재하며, 일정 규모 이상의 사업자는 취득 의무

- 의무 대상
  - 정보통신서비스 부문 전년도 **매출액이 100억원 이상인 자**
  - 전년도 일일평균 정보통신서비스 **이용자 수가 100만명 이상인 자**

2. 보안 아키텍처 구성 – 인증기준

- ISMS-P 인증기준
  - 2.6.1 네트워크 접근
  - 2.6.6 원격접근 통제
  - 2.10.6 업무용 단말기기 보안

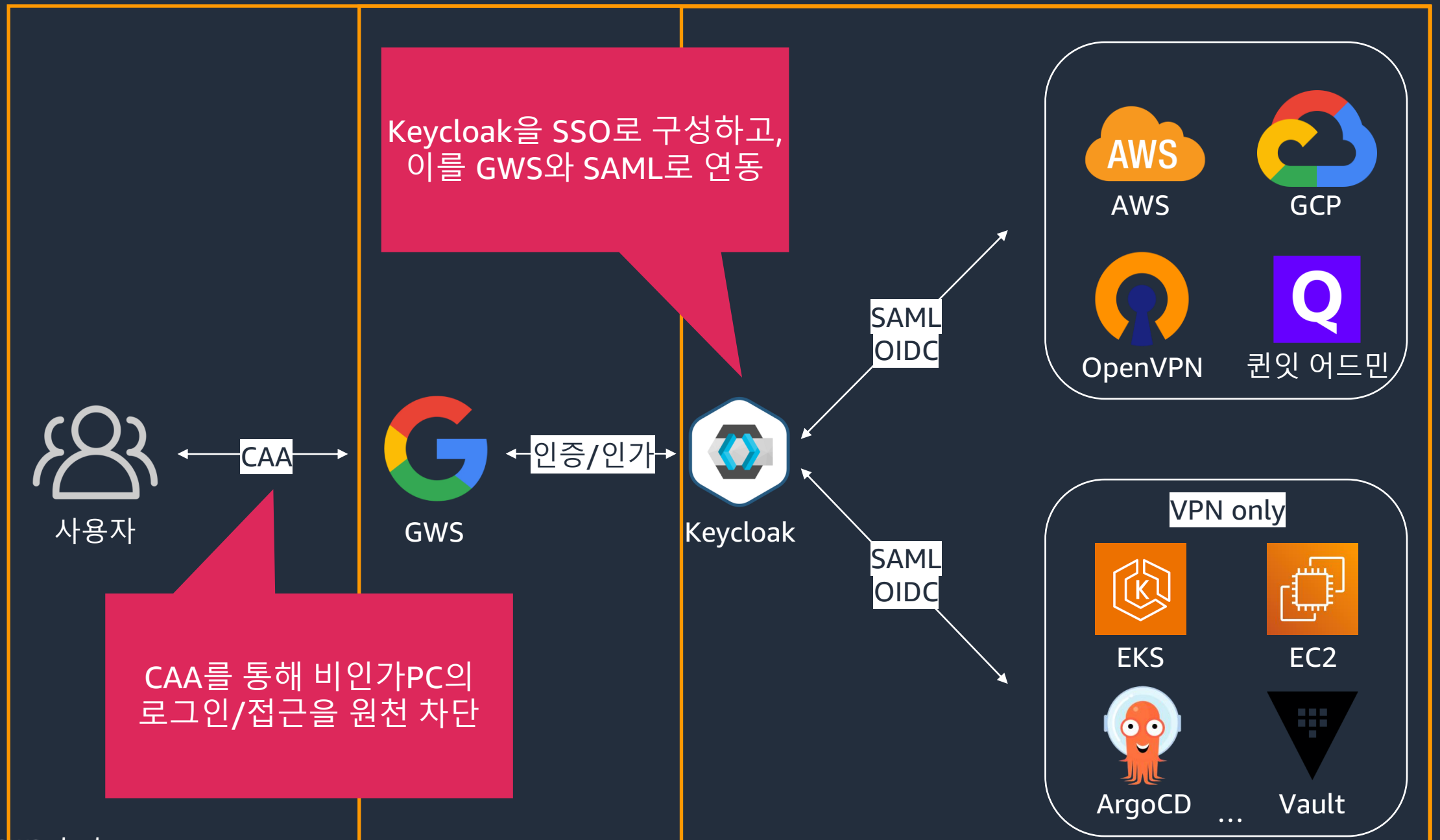
인가된 PC만 내부 네트워크 및 인프라에 접근 허용

2. 보안 아키텍처 구성 - 개요

- Keycloak
  - CNCF Foundation에서 관리하는 오픈소스 IAM 도구
  - 인증 / 인가를 간편하게 구현할 수 있는 SSO 시스템
  - OAuth 2.0, OIDC, SAML, LDAP 등 지원

- Google WorkSpace Context-Aware Access(GWS CAA)
  - IP, Geo, 기기값, OS를 기반으로 GWS 서비스(공유 드라이드 등) 접근통제
  - Enterprise 플랜 기능

이미지 출처 : ArgoCD Docs / Hashicorp Docs / Flaticon



이미지 출처 : ArgoCD Docs / Hashicorp Docs / Flaticon / Keycloak Docs / OpenVPN Docs / GCP Docs

2. 보안 아키텍처 구성 - 효과

- 시스템별 계정 생성, 삭제 등의 불필요한 작업을 효과적으로 제거
- GWS CAA와 Keycloak SAML을 활용해 제로트러스트와 유사한 효과
- 뛰어난 확장성으로 신규 시스템, SaaS 도입 시 인증 관리가 수월

인가된 PC만 내부 네트워크 및 인프라에 접근 허용

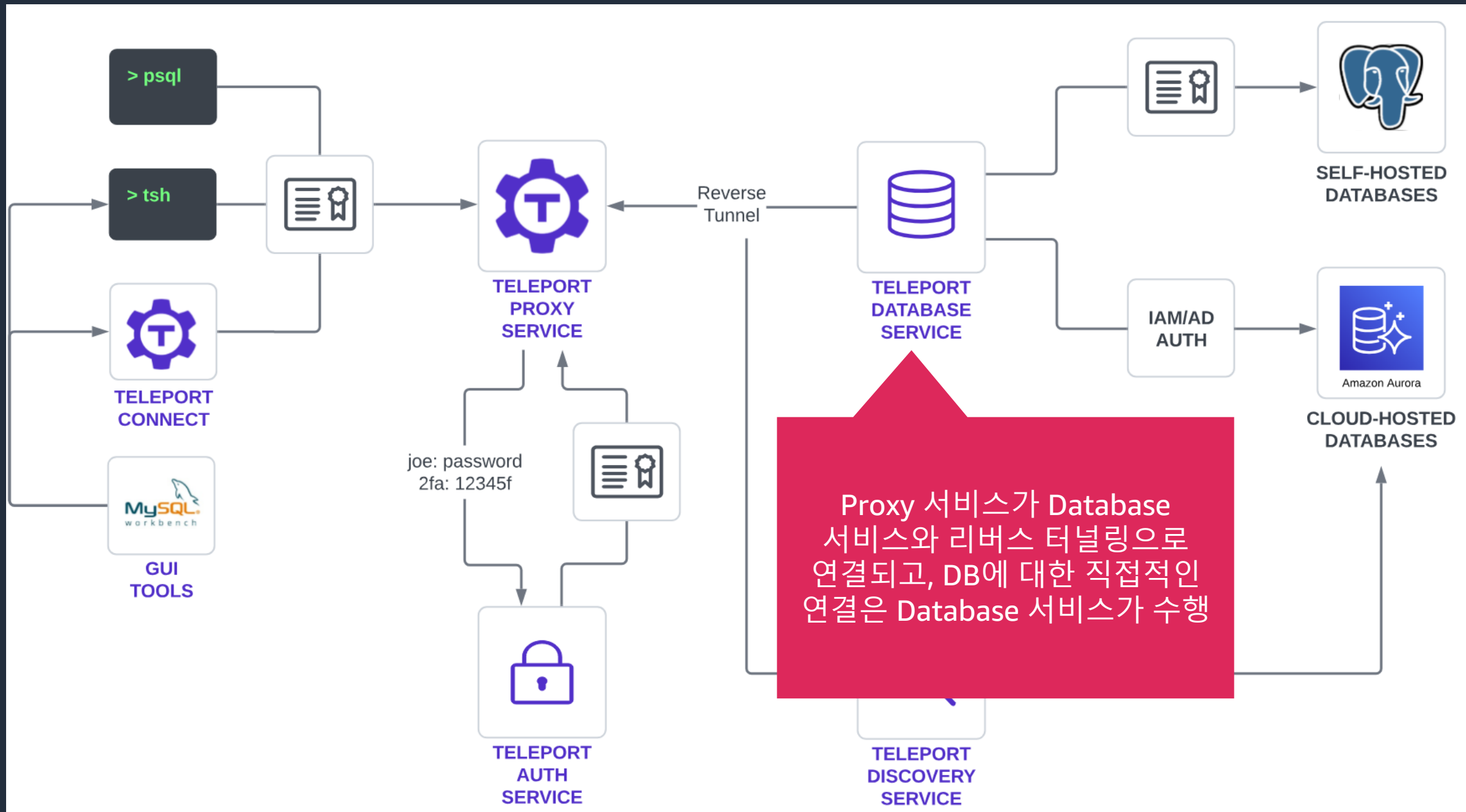
3. Teleport를 통한 DB 접근제어 - 인증기준

- ISMS-P 인증기준
  - 2.6.4 데이터베이스 접근
    - 접속 권한을 구분하고 직무별 접근통제
    - 최소권한 원칙에 따른 테이블, 뷰, 컬럼, 쿼리 레벨에서 접근통제
    - 일정시간 이상 업무를 수행하지 않는 경우 자동 접속차단
    - 데이터베이스 접근을 허용하는 IP주소, 포트, 응용프로그램 제한

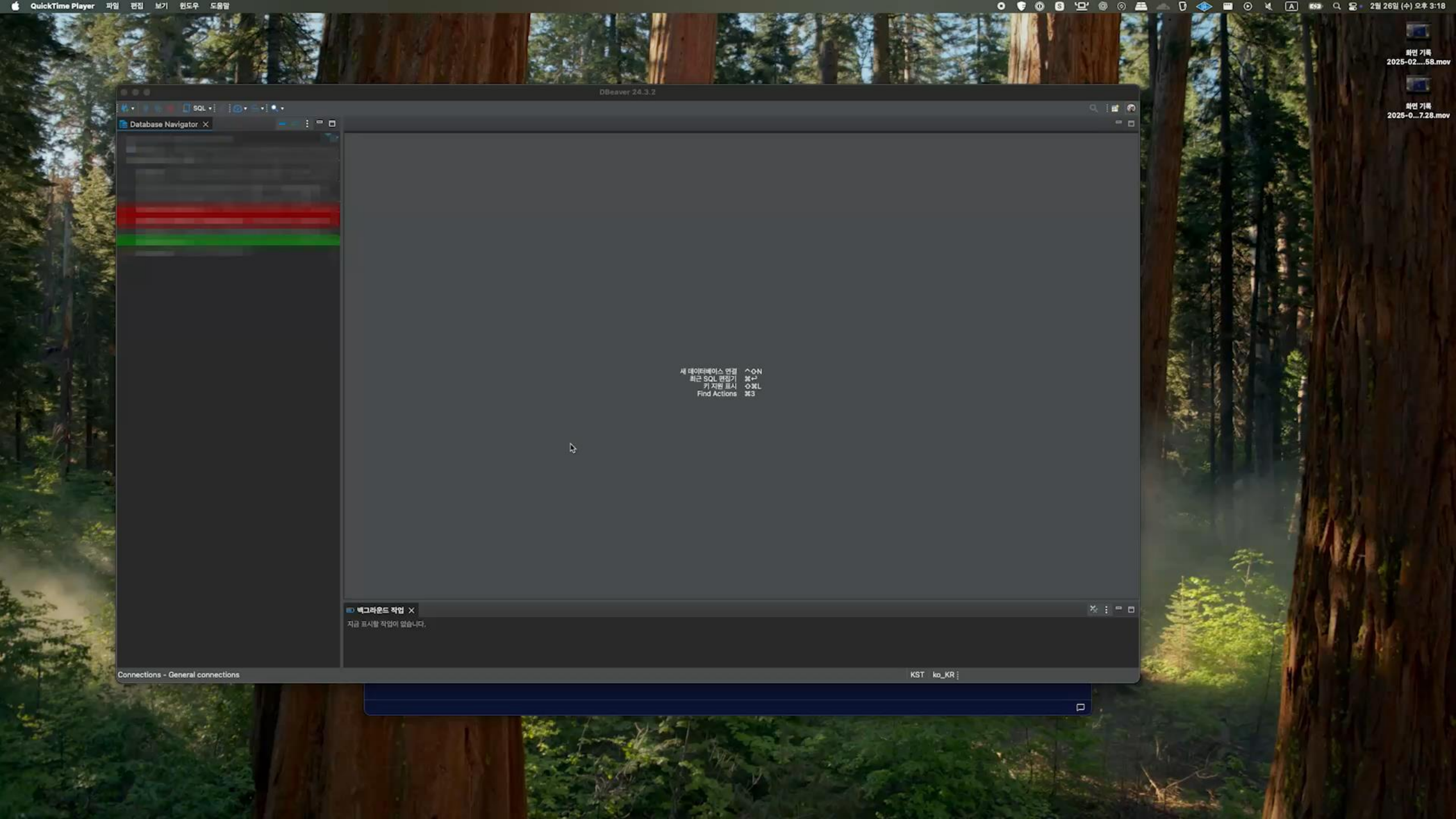
DB에 최소 접근권한 할당 및 비인가 접근 차단

3. Teleport를 통한 DB 접근제어 - 개요

- Teleport
  - EC2, RDS, K8s 등 다양한 리소스의 접근통제를 구현할 수 있는 오픈소스
  - 다양한 부가 기능(MFA, SSO, RBAC 등) 제공
  - 리버스 터널링을 통해 VPN 없이도 안전한 접근환경 구성 가능
  - 상용 솔루션이나 Community Edition에서도 주요 기능 지원



이미지 출처 : https://goteleport.com/docs/enroll-resources/database-access/


QuickTime Player 파일 편집 보기 윈도우 도움말
2월 26일 (수) 오후 3:18
화면 기록 2025-02....58.mov
화면 기록 2025-0...7.28.mov
DBeaver 24.3.2
SQL
Database Navigator
새 데이터베이스 연결 ^⇧N
최근 SQL 편집기 ⌘↵
키 지원 표시 ⇧⌘L
Find Actions ⌘3
백그라운드 작업
지금 표시할 작업이 없습니다.
Connections - General connections
KST
ko_KR

3. Teleport를 통한 DB 접근제어 - 효과

- 상용 솔루션 도입 시 연간 소요되는 N천만원 ~ N억원 비용 절감
- RBAC 기반의 세밀한 권한 관리 및 뛰어난 관리 기능 사용성
- 엔지니어가 사용하는 DB 핸들링 도구에 제약없이 적용 가능

DB에 최소 접근권한 할당 및 비인가 접근 차단

4. Prowler를 활용한 AWS 취약점 점검 및 관리 - 인증기준

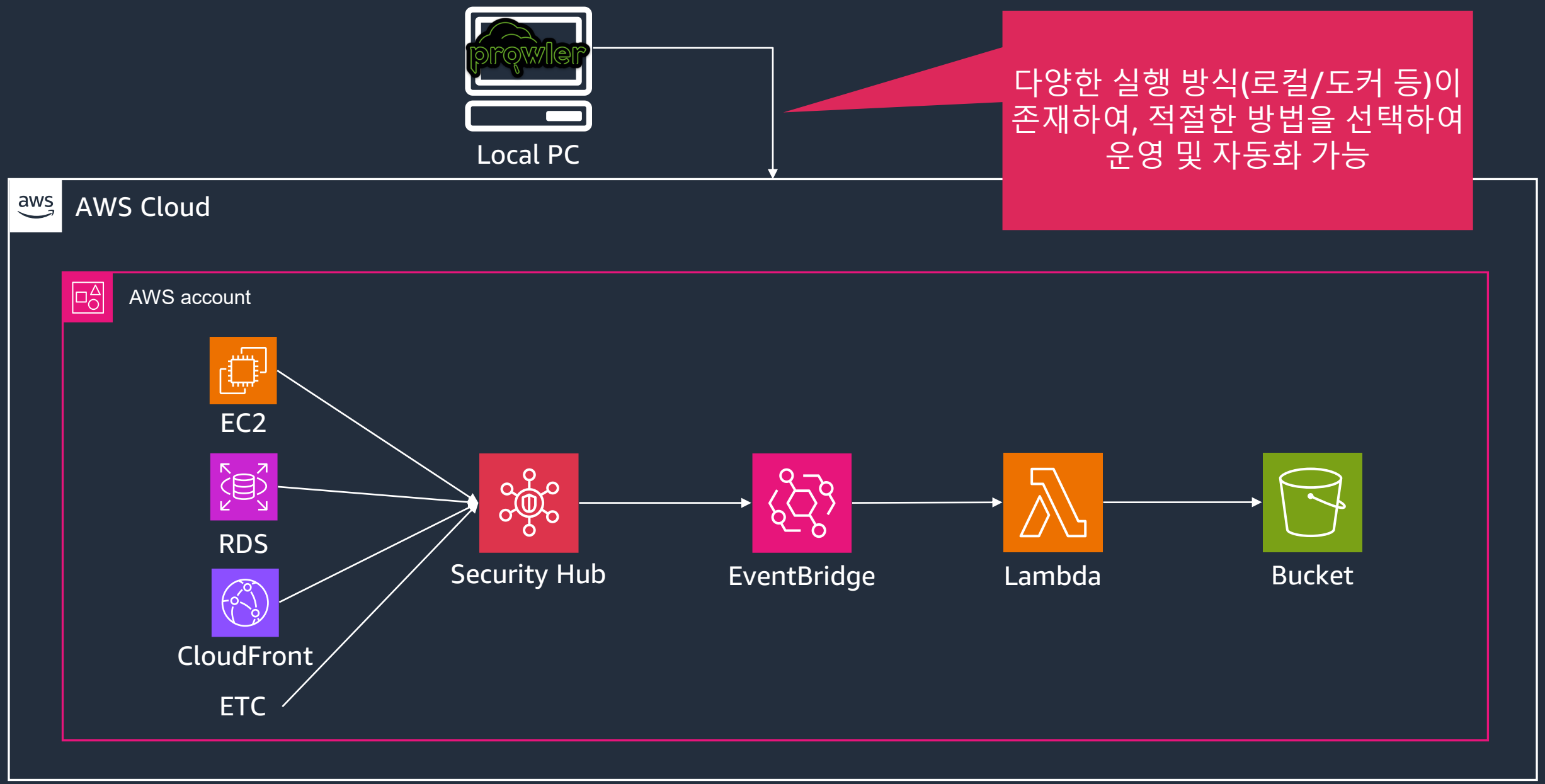
- ISMS-P 인증기준
  - 2.10.2 클라우드 보안
  - 2.11.2 취약점 점검 및 조치

클라우드 인프라, 리소스, 서비스에 대한 취약점 관리

4. Prowler를 활용한 AWS 취약점 점검 및 관리 - 개요

- Prowler
  - AWS를 비롯한 클라우드 환경의 보안 취약점을 스캔하는 오픈소스
  - CIS Benchmark, SOC2, PCI-DSS, K-ISMS 등 다양한 규정 준수 검사
  - EC2, RDS, CloudFront 등 약 30종류 이상의 서비스에 대해 점검

- Security Hub
  - AWS 내 보안 상태를 중앙에서 모니터링하고 관리하는 서비스
  - 다양한 보안 도구(GuardDuty, Config, Macie 등)와 통합 가능
  - PCI-DSS 등 미리 정의된 보안 컴플라이언스에 대해 점검 가능



이미지 출처 : https://docs.prowler.com/

```
zero@DESKTOP-NTS9VFC:~$ prowler aws --security-hub --region ap-northeast-2 --send-sh-only-fails

                                 _
 _ __  _ __ _____      _| | ___ _ __
| '_ \| '__/ _ \ \ /\ / / |/ _ \ '__|
| |_) | | | (_) \ V  V /| |  __/ |
| .__/|_|  \___/ \_/\_/ |_|\___|_|v5.3.0
|_| the handy multi-cloud security tool

Date: 2025-02-17 20:19:05

-> Using the AWS credentials below:
   · AWS-CLI Profile: default
   · AWS Regions: ap-northeast-2
   · AWS Account:
   · User Id: AIDA
   · Caller Identity ARN:

-> Using the following configuration:
   · Config File: /home/zero/.local/lib/python3.10/site-packages/prowler/config/config.yaml
   · Mutelist File: /home/zero/.local/lib/python3.10/site-packages/prowler/config/aws_mutelist.yaml
   · Scanning unused services and resources: False

Executing 565 checks, please wait...
-> Scanning cloudwatch service |██████                          | / 88/565 [16%] in 1:10
```

Overview Results:

31.19% (305) Failed	68.51% (670) Passed	0.0% (0) Muted

Account [redacted] Scan Results (severity columns are for fails only):

Provider	Service	Status	Critical	High	Medium	Low	Muted
aws	accessanalyzer	FAIL (1)	0	0	0	1	0
aws	account	FAIL (1)	0	0	1	0	0
aws	lambda	FAIL (7)	1	0	0	6	0
aws	backup	FAIL (1)	0	0	0	1	0
aws	bedrock	FAIL (1)	0	0	1	0	0
aws	cloudformation	FAIL (1)	0	0	1	0	0
aws	cloudtrail	FAIL (7)	0	0	4	3	0
aws	cloudwatch	FAIL (71)	0	0	71	0	0
aws	config	FAIL (1)	0	0	1	0	0
aws	drs	FAIL (1)	0	0	1	0	0
aws	ec2	FAIL (27)	1	2	17	7	0
aws	emr	PASS (1)	0	0	0	0	0
aws	eventbridge	PASS (3)	0	0	0	0	0

Security Hub

요약
제어
보안 표준

인사이트
분석 결과
통합

관리
자동화
사용자 지정 작업

설정
일반
리전
구성 신규
사용량

새로운 소식

분석 결과 (20+)

작업 | 워크플로 상태 | 인사이트 세부 정보 | 인사이트 생성

조사 결과는 보안 문제 또는 실패한 보안 검사입니다. '그룹화 기준'을 선택한 다음 인사이트를 생성하여 관련 조사 결과를 저장할 수 있습니다.

필터 추가

그룹화 기준: 없음

제품 이름 일치함 Prowler | 필터 지우기

1 ...

조사 결과	심각도	워크플로 상태	리전	계정 ID	제품	리소스	규정 준수 상태	업데이트 시간
Ensure all VPC has public and private subnets defined	MEDIUM	NEW	ap-northeast-2		Prowler	EC2 VPC vpc-0c56	FAILED	9분 전
Ensure VPC subnets do not assign public IP by default	MEDIUM	NEW	ap-northeast-2		Prowler	AwsEc2Subnet subnet-0adc	FAILED	9분 전
Ensure VPC subnets do not assign public IP by default	MEDIUM	NEW	ap-northeast-2		Prowler	AwsEc2Subnet subnet-0681	FAILED	9분 전
Ensure VPC subnets do not assign public IP by default	MEDIUM	NEW	ap-northeast-2		Prowler	AwsEc2Subnet subnet-06c5	FAILED	9분 전
Ensure VPC Flow Logging is Enabled in all VPCs.	MEDIUM	NEW	ap-northeast-2		Prowler	EC2 VPC vpc-0c56d	FAILED	9분 전
Ensure VPC Flow Logging is Enabled in all VPCs.	MEDIUM	NEW	ap-northeast-2		Prowler	EC2 VPC vpc-05aaf6	FAILED	9분 전
Amazon EC2 should be configured to use VPC endpoints that are created for the Amazon EC2 service.	MEDIUM	NEW	ap-northeast-2		Prowler	AwsEc2VpcEndpointService vpc-0c56d7	FAILED	9분 전

4. Prowler를 활용한 AWS 취약점 점검 및 관리 - 효과

- Amazon Inspector가 지원하지 않는 영역에 대한 취약점 관리
- K-ISMS와 SOC2를 비롯한 글로벌 컴플라이언스 기준 점검
- 별도 비용없이 편리하게 취약점 점검 및 결과 확인 가능

클라우드 인프라, 리소스, 서비스에 대한 취약점 관리