#AWSKRUG

현실성 있는 AWS 보안 가이드라인 작성기 : 침해사고 사례 분석부터 가이드라인 및 체크리스트 작성까지

송지예

Team. IAM 절대지켜

2025. 10. 23

CONTENTS

01 Intro

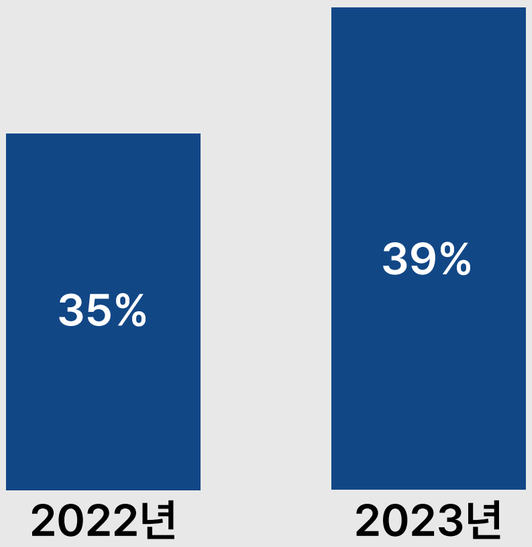
- 현황 및 추세
- ISMS-P 인증 실효성
- 필요성
- CloudDoctor?

01

현황 및 추세

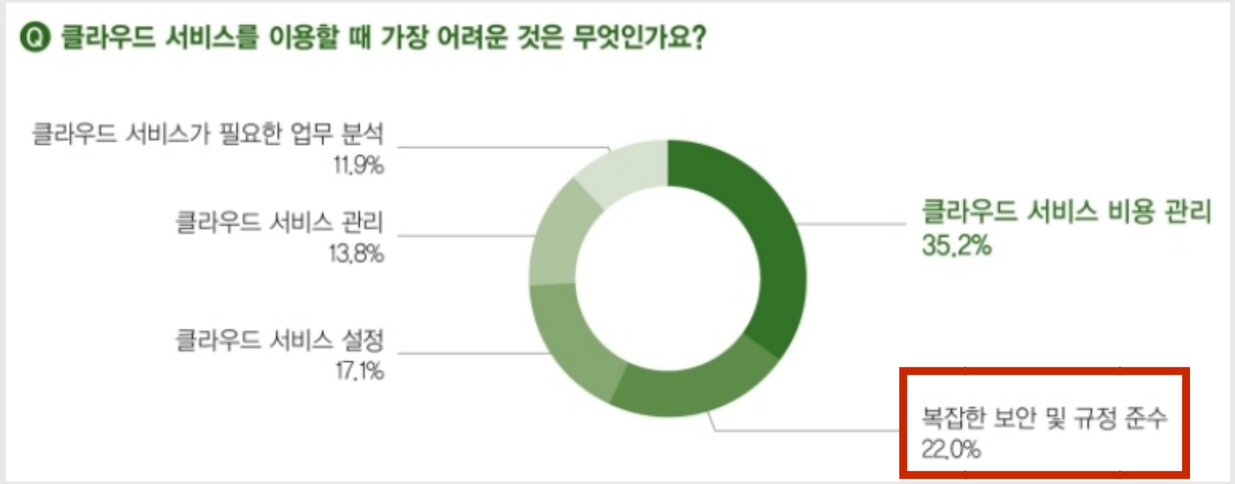
: 연이어 발생하는 퍼블릭 클라우드 침해사고 및 보안 규정 준수의 어려움

퍼블릭 클라우드 침해사고 증가 추세



*Source: 2023 Thales Cloud Security(Thales, 2023)

클라우드 서비스 이용 시 어려운 점



*Source: 2025 클라우드 보안 리포트(보안뉴스, 2025)

현황 및 추세

: 기업에서 서비스 보안을 판단하는 기준인 ISMS-P와 ISO27001

기업에서 서비스 보안을 판단하는 기준인
ISMS-P와 ISO27001

ISMS-P 인증 실효성

: ISMS-P 인증 실효성에 대한 의문

ISMS 인증 실효성 국회 청문회서 도마…개편 목소리 높아

최고 수준 보안인증 받은 기업들 줄줄이 해킹, 정부는 책임 없나

SK텔레콤, 예스24, 롯데카드, KT...사전인증·사후대응 다 뚫려 "컨트롤타워 및 새 보안 패러다임 필요"

[단독] 개인정보 분야 최고 수준이라고? ISMS-P 인증 취득 기관 32곳서 털렸다

송혜리 기자 · 2025. 10. 14. 05:01

ISMS-P 인증 취득 기업 중 SKT·예스24·KT·롯데카드 포함...인증 제도 신뢰성 도마 위
한창민 의원 "제도 전면 손질하고 공공·금융권까지 확대해야"

정보보호 및 개인정보보호 관리체계 인증

ISMS-P

Personal information & Information Security Management System

필요성

: 실제 퍼블릭 클라우드를 반영하지 않은 기존의 클라우드 보안 안내서

≠ 퍼블릭 클라우드 서비스

필요성

: 현업에서 사용하는 서비스들을 자세하게 다루고 있지 않은 클라우드 보안 가이드라인

영역	항목코드	항목명	중요도
계정 관리	1.1	사용자 계정 관리	상
	1.2	IAM 사용자 계정 단일화 관리	상
	1.3	IAM 사용자 계정 식별 관리	중
	1.4	IAM 그룹 사용자 계정 관리	중
	1.5	Key Pair 접근 관리	상
	1.6	Key Pair 보관 관리	상
	1.7	Admin Console 관리자 정책 관리	중
	1.8	Admin Console 계정 Access Key 활성화 및 사용주기 관리	상
	1.9	MFA (Multi-Factor Authentication) 설정	중
	1.10	AWS 계정 패스워드 정책 관리	중
	1.11	EKS 사용자 관리	상
	1.12	EKS 서비스 어카운트 관리	중
	1.13	EKS 불필요한 익명 접근 관리	상
권한 관리	2.1	인스턴스 서비스 정책 관리	상
	2.2	네트워크 서비스 정책 관리	상
	2.3	기타 서비스 정책 관리	상
가상 리소스 관리	3.1	보안 그룹 인/아웃바운드 ANY 설정 관리	상
	3.2	보안 그룹 인/아웃바운드 불필요 정책 관리	상
	3.3	네트워크 ACL 인/아웃바운드 트래픽 정책 관리	중
	3.4	라우팅 테이블 정책 관리	중
	3.5	인터넷 게이트웨이 연결 관리	하
	3.6	NAT 게이트웨이 연결 관리	중
	3.7	S3 버킷/객체 접근 관리	중
	3.8	RDS 서브넷 가용 영역 관리	중
	3.9	EKS Pod 보안 정책 관리	상
	3.10	ELB(Elastic Load Balancing) 연결 관리	중
운영 관리	4.1	EBS 및 볼륨 암호화 설정	중
	4.2	RDS 암호화 설정	중
	4.3	S3 암호화 설정	중
	4.4	통신구간 암호화 설정	중
	4.5	CloudTrail 암호화 설정	중
	4.6	CloudWatch 암호화 설정	중
	4.7	AWS 사용자 계정 로깅 설정	상
	4.8	인스턴스 로깅 설정	중
	4.9	RDS 로깅 설정	중
	4.10	S3 버킷 로깅 설정	중
	4.11	VPC 플로우 로깅 설정	중
	4.12	로그 보관 기간 설정	중
	4.13	백업 사용 여부	중
	4.14	EKS Cluster 제어 플레인 로깅 설정	중
	4.15	EKS Cluster 암호화 설정	중

IAM, EC2, EKS, VPC, S3, ECS, RDS, ELB, EBS, CloudTrail, CloudWatch 등

필요성

: 현업에서 사용하는 서비스들을 자세하게 다루고 있지 않은 클라우드 보안 가이드라인

영역	항목코드	항목명	중요도
계정 관리	1.1	사용자 계정 관리	상
	1.2	IAM 사용자 계정 단일화 관리	상
	1.3	IAM 사용자 계정 식별 관리	중
	1.4	IAM 그룹 사용자 계정 관리	중
	1.5	Key Pair 접근 관리	상
	1.6	Key Pair 보관 관리	상
	1.7	Admin Console 관리자 정책 관리	중
	1.8	Admin Console 계정 Access Key 활성화 및 사용주기 관리	상
	1.9	MFA (Multi-Factor Authentication) 설정	중
	1.10	AWS 계정 패스워드 정책 관리	중
	1.11	EKS 사용자 관리	상
	1.12	EKS 서비스 어카운트 관리	중
	1.13	EKS 불필요한 익명 접근 관리	상
권한 관리	2.1	인스턴스 서비스 정책 관리	상
	2.2	네트워크 서비스 정책 관리	상
	2.3	기타 서비스 정책 관리	상
가상 리소스 관리	3.1	보안 그룹 인/아웃바운드 ANY 설정 관리	상
	3.2	보안 그룹 인/아웃바운드 불필요 정책 관리	상
	3.3	네트워크 ACL 인/아웃바운드 트래픽 정책 관리	중
	3.4	라우팅 테이블 정책 관리	중
	3.5	인터넷 게이트웨이 연결 관리	하
	3.6	NAT 게이트웨이 연결 관리	중
	3.7	S3 버킷/객체 접근 관리	중
	3.8	RDS 서브넷 가용 영역 관리	중
	3.9	EKS Pod 보안 정책 관리	상
	3.10	ELB(Elastic Load Balancing) 연결 관리	중
운영 관리	4.1	EBS 및 볼륨 암호화 설정	중
	4.2	RDS 암호화 설정	중
	4.3	S3 암호화 설정	중
	4.4	통신구간 암호화 설정	중
	4.5	CloudTrail 암호화 설정	중
	4.6	CloudWatch 암호화 설정	중
	4.7	AWS 사용자 계정 로깅 설정	상
	4.8	인스턴스 로깅 설정	중
	4.9	RDS 로깅 설정	중
	4.10	S3 버킷 로깅 설정	중
	4.11	VPC 플로우 로깅 설정	중
	4.12	로그 보관 기간 설정	중
	4.13	백업 사용 여부	중
	4.14	EKS Cluster 제어 플레인 로깅 설정	중
	4.15	EKS Cluster 암호화 설정	중

IAM, EC2, EKS, VPC, S3, ECS, RDS, ELB, EBS, CloudTrail, CloudWatch 등

→ **서비스 종류 부족 + 항목 부족**

+ 두루뭉술한 각 항목의 내용

CloudDoctor?

: 실제 침해사고 및 공격 기법 기반의 효용성 있는 보안 가이드라인과 체크리스트

실제 AWS 침해사고 및 공격 기법을 기반으로

효용성 있는 보안 가이드라인과 체크리스트를 제작해보자!

그리고 이를 웹에서 가시성 좋게 지원하자!

CloudDoctor?

: 현실성 있는 AWS 보안 가이드라인과 체크리스트를 제작하고 점검 도구도 제공하자!

가이드라인

체크리스트

점검 도구

CloudDoctor

02 가이드

- AWS 침해사고 사례 분석
- 진행 흐름

02

AWS 침해사고 및 공격 기법 분석

1. 총 약 350건의 사례 분석
- aws-customer-security-incidents, Hacking The Cloud, Datadog, DEFCON, CloudGoat 등

2. 분석 항목
- 이름, 날짜, 근본 원인, 공격 확장 벡터, 영향, AWS 서비스명, 상세 발생 원인 등

3. 데이터 취합 및 분류
- 취합 후 유사한 root cause별 분류
- 27개의 AWS 서비스

AWS 침해사고 사례 분석

: 사례 1 - Identity Federation을 통한 비인가자의 역할 취득 및 리소스 접근

사례 1:
Identity Federation을 통한 비인가자의 역할 취득 및 리소스 접근

Okta SSO 사용으로 인한 AWS 침해

출처: Expel (2025, 01)

공격 흐름:

공격자가 외부 IdP(Okta) 계정의 세션/토큰 탈취

→ AWS IAM 역할의 잘못된 연동 설정(신뢰 정책 오류) 악용

결과:

IdP 계정 침해만으로 AWS 내부 리소스 접근 및 악의적 활동 수행 가능

시사점:

Identity Federation 설정 오류는 외부 IdP 침해가 즉시 AWS 내부 침해로 이어지는 경로를 제공

사례 1:
Identity Federation을 통한 비인가자의 역할 취득 및 리소스 접근

⚠ 왜 위험한가?

- 외부 IdP(AD, Okta 등) 계정으로 AWS 역할 획득 허용
  → IAM 역할 신뢰 정책(Assume Role Policy) 설정 오류 시 위험

⚠ 어떤 일이 벌어질까?

- IdP 토큰 탈취하여 AssumeRoleWithSAML/WebIdentity 호출, 임시 AWS 자격증명 획득
  → 획득한 자격증명으로 역할 권한 내 악의적 활동 수행 (리소스 열람/수정/삭제, 권한 생성 등)

AWS 침해사고 사례 분석

: 사례 1 - Identity Federation을 통한 비인가자의 역할 취득 및 리소스 접근

취약 조건

- AssumeRolePolicy의 Principal이 모든 IdP/Principal: "*" 또는 특정 IdP의 모든 사용자로 허용
- IAM Role과 IdP 매핑에서 Condition으로 특정 IdP 속성값(특정 SAML attribute, OIDC sub/aud/iss 등)을 검사

조치 방안

- 역할의 AssumeRolePolicy에 허용되는 Principal을 명확히(특정 IdP ARN만) 할 것
- 가능한 경우 Condition을 추가해 허용되는 IdP 속성값(특정 SAML attribute 값, OIDC sub/aud/iss 등)으로만 할당 가능하게 제한

경로: IAM → 역할 → Federation 연동 역할 선택 → 신뢰 관계

경로: IAM → 역할 → Federation 연동 역할 선택 → 신뢰 관계

사례 1:
Identity Federation을 통한 비인가자의 역할 취득 및 리소스 접근

이 항목의 가치 & 차별점

- 단순 IAM 역할 신뢰 문제를 넘어, Identity Federation 프로토콜(SAML/OIDC) 및 IdP 속성 검증이라는 구체적이고 기술적인 설정 오류 지적
- 외부 IdP 연동 환경이라는 특정 시나리오에서의 고유한 보안 위협 제시

사례 2:
SendCommand(RunCommand)를 통한 EC2에서의 악성 셸 명령 실행

출처: Medium (2024. 08)

AWS Systems Manager(SSM) Run Command 악용을 통한 시스템 수준 랜섬웨어 배포

공격 흐름:

ssm:SendCommand 권한 탈취

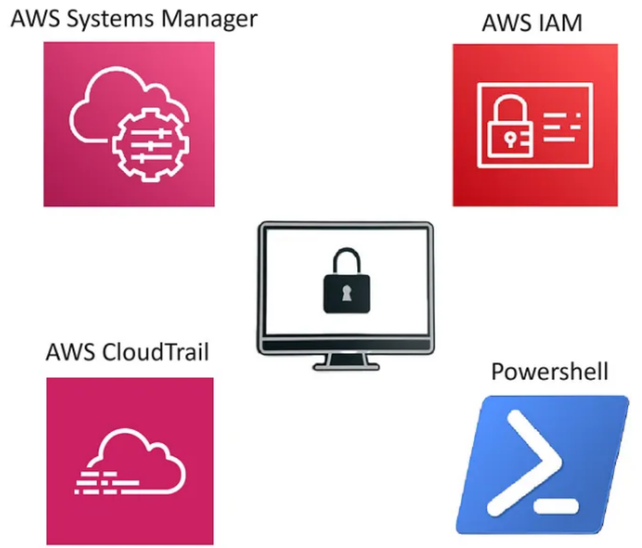
→ 다수 EC2에 랜섬웨어 원격 실행 (네트워크 보안 우회)

결과:

직접 시스템 감염 및 서비스 마비

시사점:

SendCommand 권한 = 네트워크 방어 무력화 및 광범위/치명적 공격 가능



사례 2:
SendCommand(RunCommand)를 통한 EC2에서의 악성 셸 명령 실행

⚠ 왜 위험한가?

- SSM RunCommand: EC2에 원격 + 비대화형 명령/스크립트 실행
  → ssm:SendCommand 권한만으로 네트워크 보안(보안 그룹 등) 우회 가능

⚠ 어떤 일이 벌어질까?

- AWS-RunShellScript 등으로 악성 코드 대규모 원격 실행
  → 기밀 정보 탈취, 백도어 설치, 로그 삭제, 랜섬웨어 실행

AWS 침해사고 사례 분석

: 사례 2 - SendCommand(RunCommand)를 통한 EC2에서의 악성 셸 명령 실행

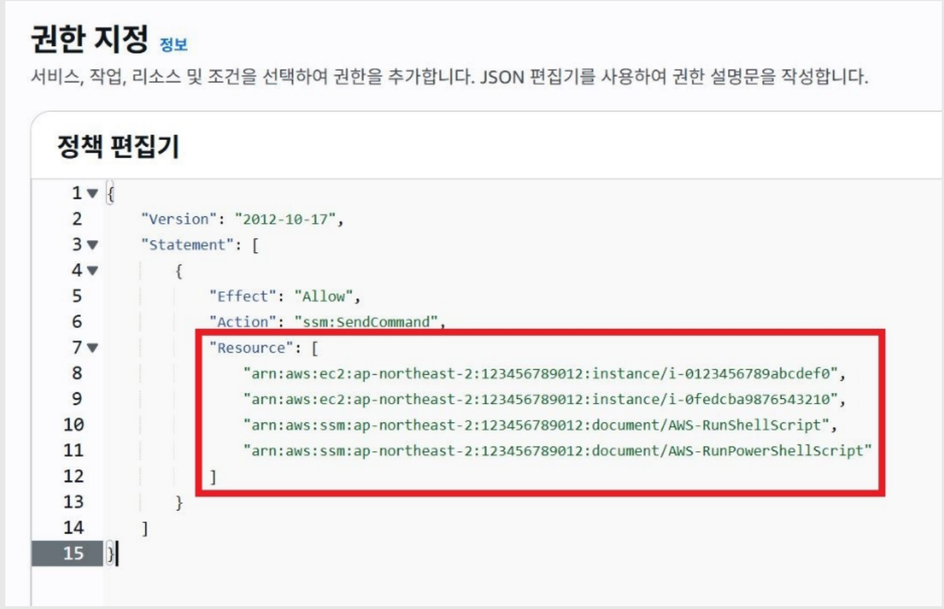
취약 조건

- ssm:SendCommand가 Principal:"*" 또는 Resource:"*"로 허용
- 대상 인스턴스 제한(태그/리소스 ARN 조건) 없이 임의 인스턴스에 AWS-RunShellScript/AWS-RunPowerShellScript 실행 가능

경로: IAM → 정책 → [정책명] → 정책 편집

조치 방안

- ssm:SendCommand 권한을 실행 대상의 구체적 리소스 ARN(예: 특정 인스턴스 ARN, 특정 Document ARN)으로 제한



경로: IAM → 정책 → [정책명] → 정책 편집

사례 2:
SendCommand(RunCommand)를 통한 EC2에서의 악성 셸 명령 실행

이 항목의 가치 & 차별점

- AWS 관리 도구(SSM) 악용 위험성 제시 (단순 네트워크 보안 X)
- 네트워크 방화벽 우회 가능한 현실적 공격 경로 강조
- 타 가이드에서 부족한 클라우드 네이티브 서비스 기능 악용 시나리오 구체화 (타 가이드 부족)

사례 3:
Bedrock의 과도한 접근 권한으로 인한 LLM 서비스 남용 위험

Bedrock InvokeModel을 이용한 LLM 하이재킹

출처: Wiz(2024, 12)

공격 흐름:

Bedrock API 호출 권한 (bedrock:InvokeModel)이 포함된 AWS 자격증명 탈취

→ LLM 모델을 무단으로 대량 호출하여 과도한 비용을 발생

결과:

내부 민감 데이터 유출 시도 및 프롬프트 인젝션을 통한 추가 공격 가능성

시사점:

Bedrock 접근 권한 탈취는 즉각적인 비용 폭증과 데이터 유출, 서비스 남용으로 이어질 수 있음

사례 3:
Bedrock의 과도한 접근 권한으로 인한 LLM 서비스 남용 위험

⚠ 왜 위험한가?

- 자격증명 유출 시 즉시 Bedrock LLM 호출/배포 권한 악용 가능
  → 대량 모델 호출/모델 프로비저닝/설정 변경

⚠ 어떤 일이 벌어질까?

- 비용 폭증: 탈취된 키로 대량 API 호출 또는 고비용 모델 프로비저닝
- 데이터 유출: 모델 입출력 통해 민감 데이터 주입/추출
  → 탐지를 회피하며 비용, 데이터, 권한 관련 2차 피해 확산

AWS 침해사고 사례 분석

: 사례 3 - Bedrock의 과도한 접근 권한으로 인한 LLM 서비스 남용 위험

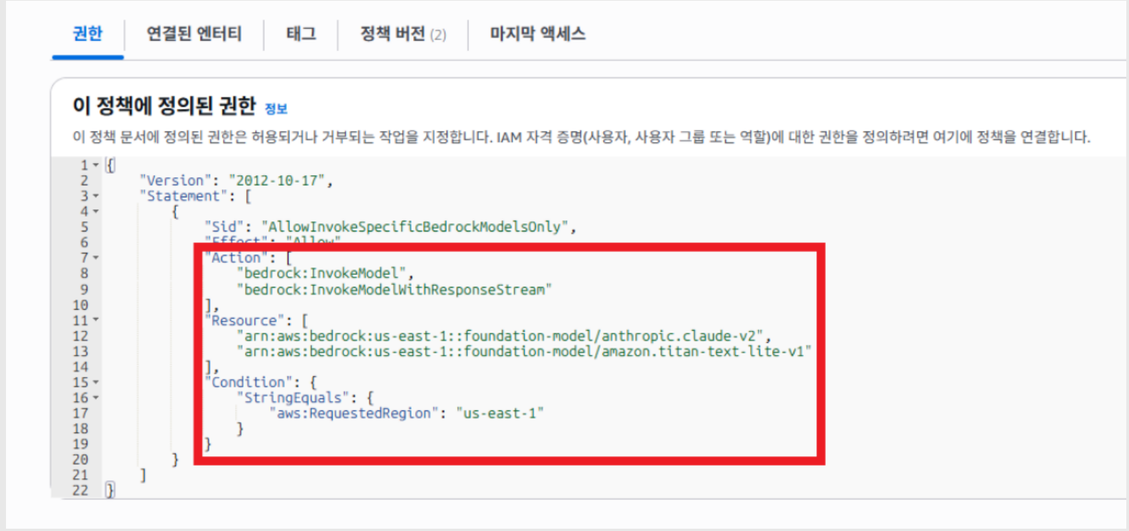
취약 조건

• IAM 정책에 bedrock:InvokeModel 또는 bedrock:List* 등 권한이 Resource:"*" 또는 조건 없이 광범위하게 허용

경로: IAM → BedRock을 호출할 사용자 혹은 역할 선택 → 정책 추가

조치 방안

• Bedrock 모델 활성화/호출 계열 API 권한은 특정 모델 ARN(또는 허용 모델 목록)과 호출 리전/주체 조건으로만 명시적으로 제한



경로: IAM → 정책 → [정책명] → 정책 편집

사례 3:
Bedrock의 과도한 접근 권한으로 인한 LLM 서비스 남용 위험

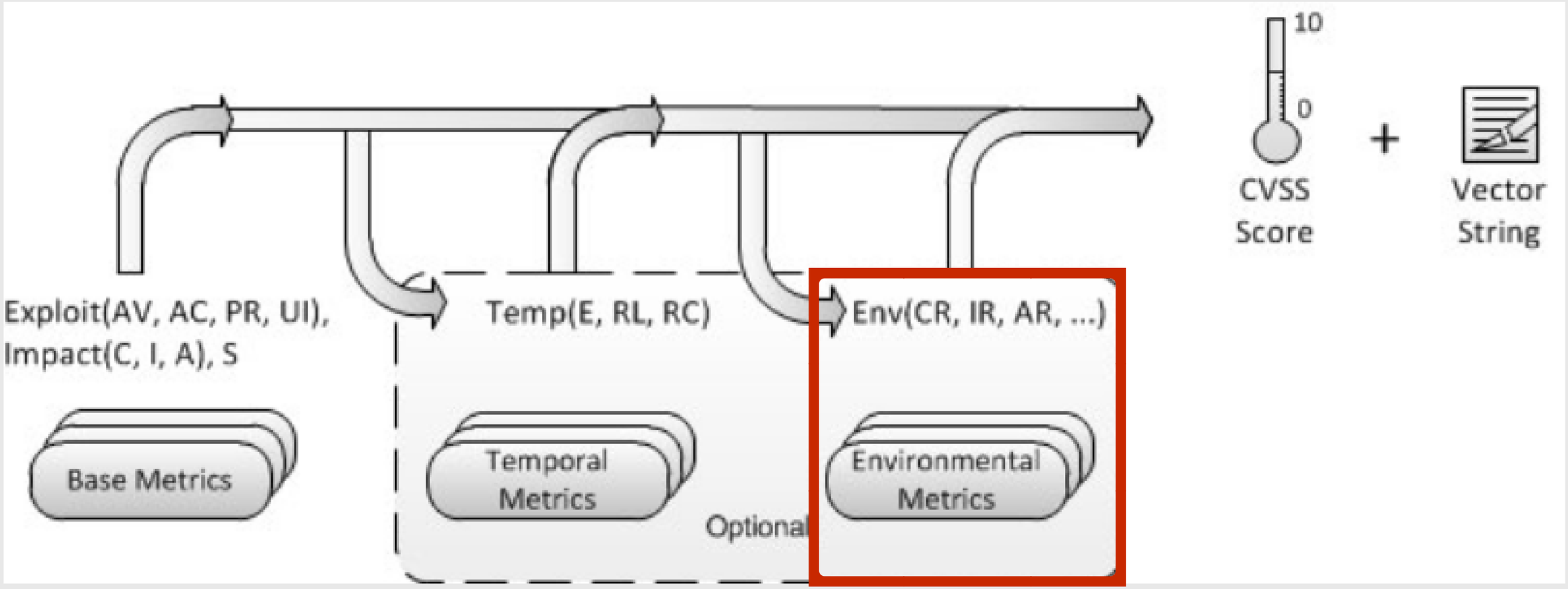
이 항목의 가치 & 차별점

- 최신 기술(LLM/Generative AI) 서비스인 Bedrock의 고유한 보안 위험 분석
- 타 가이드에서 아직 다루지 않는 새로운 유형의 클라우드 보안 위협을 포함

진행 흐름

: CVSS 기반 중요도 산정 기준

중요도 산정 기준



진행 흐름

: CVSS 기반 중요도 산정 기준 + 우리만의 "유사 사례" 기준 추가

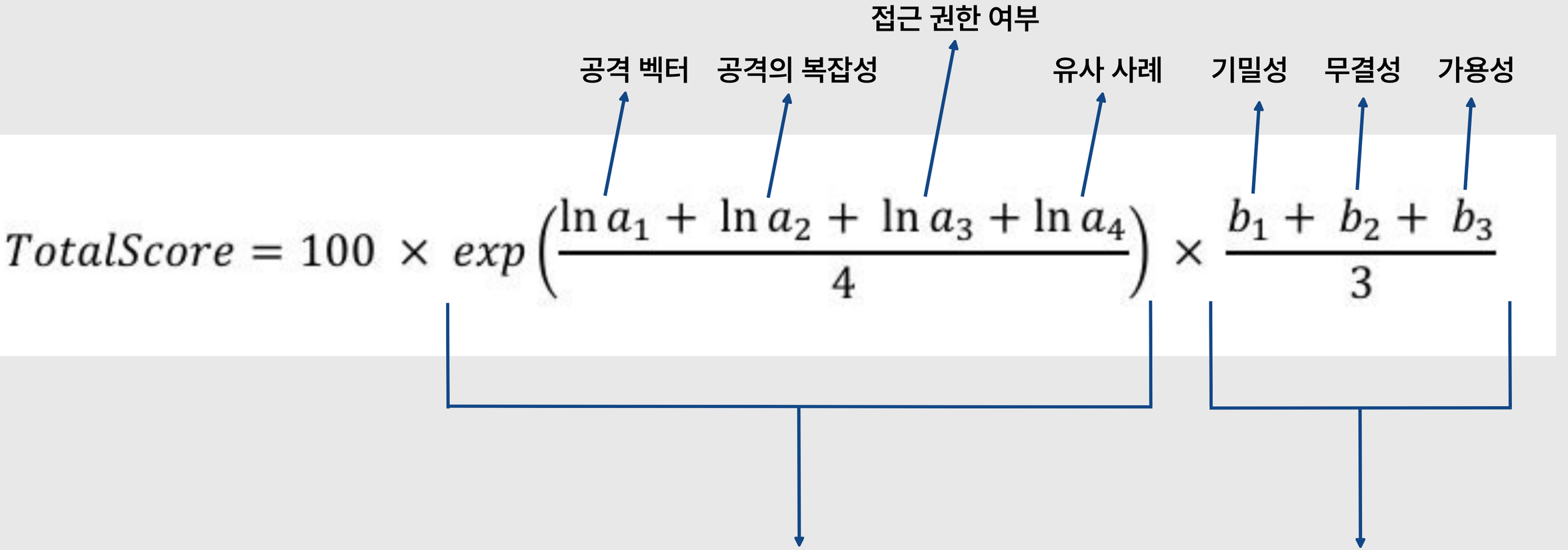
중요도 산정 기준

공격 벡터 MAX 1	공격의 복잡성 MAX 1	접근 권한 여부 MAX 1	ENV CIA MAX 1			유사 사례 MAX 1
			기밀성	무결성	가용성	
local : Access key 탈취 후 Local 상태 (1)	복잡하지 않음 (1)	권한없이 접근가능 (1)	민감 데이터가 직접 공격자에게 노출될 수 있음 (1)	공격자 또는 내부자에 의해 전체 리소스 수정/삭제 가능 (1)	주요 서비스 다운, 데이터 영구 손실, 대규모 중단 가능 (1)	4건 이상 (1)
Adjacent : 낮은 권한에서 높은 권한 상태로 확대 (0.8)	무난함 (0.5)	일반 사용자/제한적 권한 필요 (0.6)	애플리케이션 데이터가 공격자에게 노출될 수 있음 (0.6)	일부 리소스나 설정이 오염될 수 있으나 전체 영향은 제한적 (0.6)	일시적 장애나 성능 저하 수준 (0.6)	2~3건 (0.6)
Network : 퍼블릭 네트워크 상태 (0.3)	매우 복잡함 (0.3)	많은 수준의 IAM 권한 또는 root 권한 (0.2)	데이터가 공격자에게 노출되지 않음 (0)	리소스 침해되지 않음 (0)	가용성 침해되지 않음 (0)	1건 (0.1)

진행 흐름

: 중요도 산정 기준을 바탕으로 한 계산식

중요도 산정 계산식



진행 흐름

: ISMS-P와 ISO27001 매핑

ISMS-P와 ISO27001 전 항목 매핑

2. AWS 서비스 ISMS-P/ISO 27001 매칭 해당/부합 항목

각 AWS 진단 항목은 ISMS-P 및 ISO/IEC 27001 보안 통제 기준과의 부합 관계를 매핑하였습니다. 이를 통해 AWS 환경 진단 결과를 국제 표준 및 국내 인증 기준의 관점에서 함께 검토할 수 있습니다.

[표] 2. AWS 보안 가이드와 ISMS-P, ISO 27001 항목 매칭

서비스명	항목코드	항목명	ISMS-P 기준항목	ISO 기준항목
EC2	1.1	IMDS 보안 통제 미적용으로 인한 임시 자격 증명 탈취	2.6.2 정보시스템 접근 2.6.6 원격접근 통제	8.9 Configuration Management
	1.2	EC2 User Data 관리 실패	2.7.1 암호정책 적용 2.7.2 암호키 관리	8.3 Information Access Restriction 8.24 Use of cryptography
	1.3	AMI 공개 설정으로 인한 정보 노출	2.1.3 정보자산 관리 2.6.2 정보시스템 접근 2.7.2 암호키 관리	8.3 Information Access Restriction 8.12 Data leakage prevention
	1.4	AMI owner 속성 미설정시 위험성	2.1.3 정보자산 관리	5.9. Inventory of information and other associated assets 8.2. Privileged access rights
	1.5	Public에 공개된 SSH/RDP를 통한 자원 탈취	2.5.1 사용자 계정 관리 2.6.1 네트워크 접근 2.6.6 원격접근 통제	5.15. Access control 8.20. Networks security
	1.6	EBS 스냅샷 공개 설정시 시스템 공격 위험	2.5.6 접근권한 검토	8.2. Privileged access rights 8.12.Data leakage prevention
S3	2.1	S3 버킷 정책의 공개 설정과 Get/Put 권한으로 인한 데이터 탈취/악성코드 주입 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.6.1 네트워크 접근	5.15.Access control 8.3.Information access restriction 8.12. Data leakage prevention
	2.2	S3 객체/버킷 ACL에 의한 외부 접근 허용 및 정보유출 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.6.1 네트워크 접근	5.15. Access control 8.3. Information access restriction 8.12 Data leakage prevention
	2.3	S3 버킷 복제 권한 악용에 의한 데이터 유출 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.14. Information transfer 5.9. Inventory of information and other associated assets
IAM	3.1	IAM 자격증명 평문 저장으로 인한 유출	2.7.1 암호정책 적용 2.7.2 암호키 관리	5.17 Authentication Information 8.24 Use of Cryptography
	3.2	장기 Access Key 보관 및 변경 주기 미흡	2.5.1 사용자 계정 관리 2.5.4 비밀번호 관리 2.7.2 암호키 관리	5.15 Access control 5.16 Identity management 5.17 Authentication Information 5.18 Access Rights
	3.3	IAM 루트 계정 Access Key 관리 실패	2.5.3 사용자 인증 2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.15 Access Control 5.17 Authentication Information 5.18 Access Rights 8.2 Privileged access rights 8.3 Information access restriction
	3.4	IAM Role의 Trust Policy 속 광범위한 Principal	2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한관리 2.5.6 접근 권한 검토	5.15 Access control 5.18 Access rights 8.2 Privileged access rights 8.3 Information access restriction
	3.5	IAM PassRole으로 비인가자의 영구적 권한 획득	2.5.1 사용자 계정 관리	5.3 Segregation of Duties
			2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.15 Access control 5.18 Access Rights 8.2 Privileged Access Rights
	3.6	Identity Federation을 통한 비인가자의 역할 취득 및 리소스 접근	2.5.3 사용자 인증 2.5.6 접근권한 검토	5.16 Identity Management 5.17 Authentication Information 8.5 Secure authentication
	3.7	Cross-Account 접근 설정 미흡	2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.15 Access control 5.18 Access rights 8.3 Information Access Restriction
	3.8	퇴직자의 IAM 권한 미철회로 인한 유출 위협	2.2.5 퇴직 및 직무변경 관리 2.5.1 사용자 계정 관리 2.5.6 접근권한 검토 2.11.3 이상행위 분석 및 모니터링	5.15 Access control 5.16 Identity management 8.3 Information access restriction 8.15 Logging
	3.9	MFA 미설정	2.5.3 사용자 인증 2.5.5 특수 계정 및 권한관리	5.17 Authentication Information 8.5 Secure authentication
VPC	4.1	Security Group의 광범위한 공개 규칙 설정으로 인한 서비스 노출 및 권한 탈취 위협	2.5.6 접근권한 검토 2.6.1 네트워크 접근	5.15. Access control 5.18. Access rights 8.20 Network Security 8.22. Segregation of networks
	4.2	배스천 호스트 미사용으로 인한 프라이빗 서브넷 자원 직접 접근 위협	2.6.1 네트워크 접근 2.5.6 접근권한 검토 2.6.6 원격접근 통제	5.15. Access control 8.20 Network Security 8.22 Segregation of Networks
Lambda	5.1	Lambda 코드/환경변수에 중요정보 노출	2.5.5 특수 계정 및 권한관리 2.7.1 암호정책 적용 2.7.2 암호키 관리	5.17. Authentication information 8.5 Secure Authentication 8.12. Data leakage prevention 8.24. Use of cryptography
	5.2	Lambda 함수 내부 입력값 미검증으로 인한 인젝션 위협 노출	2.8.5 소스 프로그램 관리	8.28 Secure Coding
RDS	6.1	RDS 스냅샷 공개 오설정으로 인한 데이터 유출	2.5.5 특수 계정 및 권한관리 2.6.4 데이터베이스 접근 2.9.3 백업 및 복구관리	8.9. Configuration management 8.12. Data leakage prevention
	6.2	공개 RDS 인스턴스로 인한 데이터 유출	2.6.1 네트워크 접근 2.6.4 데이터베이스 접근 2.6.7 인터넷 접속 통제	5.15. Access control 8.20. Networks security 8.22. Segregation of networks
Cloud Trail	7.1	CloudTrail 비활성화 시 로그 미수집으로 인한 추적 불가 위험성	2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및 모니터링	5.7. Threat intelligence 8.15. Logging 5.28. Collection of evidence
	7.2	CloudTrail 비정상적인 API 호출 감시 미흡	2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검	5.7. Threat intelligence 5.28. Collection of evidence 8.2. Privileged access rights 8.15. Logging
EKS	8.1	EKS 과도한 권한 설정으로 인한 Pod 침투와 자격증명 탈취	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.6.1 네트워크 접근	5.18. Access rights 8.2. Privileged access rights
KMS	9.1	KMS 권한/키 관리 오설정으로 인한 랜섬웨어 위협	2.7.2 암호키 관리 2.5.5 특수 계정 및 권한관리	8.2. Privileged access rights 8.24. Use of cryptography
SNS	10.1	SNS 주제 액세스 정책 과다 허용으로 인한 SMS 스미싱 악용	2.5.5 특수 계정 및 권한관리 2.6.3 응용프로그램 접근	5.15. Access control 5.18. Access rights 8.3. Information access restriction
SQS	11.1	SQS 큐 정책 과도 권한	2.5.5 특수 계정 및 권한관리 2.6.3 응용프로그램 접근	5.15. Access control 5.18. Access rights 8.3. Information access restriction
Route 53	12.1	Route 53 DNS 레코드 미정리로 인한 Takeover	2.1.3 정보자산 관리 2.6.1 네트워크 접근 2.10.3 공개서버 보안	5.9. Inventory of information and other associated assets 8.9. Configuration management 8.21. Security of network services
Organizations	13.1	Organizations Trusted Access 관리 미흡으로 조직 전체 계정 장악	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.6.2 정보시스템 접근	5.18. Access rights 8.2. Privileged access rights 8.3 Information Access Restriction
	13.2	Organizations SCP 미적용으로 인한 불필요 API 호출	2.5.5 특수 계정 및 권한관리 2.6.2 정보시스템 접근	8.2 Privileged Access Rights 8.3 Information Access Restriction 8.9. Configuration management
ECR	14.1	잘못된 ECR 관련 정책으로 인한 악성코드 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	8.2 Privileged Access Rights 8.3 Information Access Restriction
SSM	15.1	SendCommand(RunCommand)를 통한 EC2에서의 악성 셸 명령 실행	2.5.5 특수 계정 및 권한관리 2.6.6 원격접근 통제	8.2. Privileged access rights
	15.2	SSM 문서 공개 설정으로 인한 자격 증명 노출	2.1.3 정보자산 관리 2.5.6 접근권한 검토 2.6.2 정보시스템 접근	5.12.Classification of information 5.15. Access control 8.3 Information access restriction
GuardDuty	16.1	GuardDuty 비활성화로 인한 위협 탐지 실패	2.11.3 이상행위 분석 및 모니터링 2.10.1 보안시스템 운영 2.11.3 이상행위 분석 및 모니터링	5.7. Threat intelligence 5.24. Incident management planning & preparation 8.15. Logging 8.16. Monitoring activities
Cognito	17.1	Cognito Identity Pool에 연결된 IAM Role의 과도 권한	2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.15 Access Control 8.2 Privileged Access Rights 8.3 Information Access Restriction
	17.2	Cognito Self-sign-up 허용으로 인한 비인가 계정 생성 위협	2.5.1 사용자 계정 관리 2.5.3 사용자 인증 2.5.4 비밀번호 관리	5.16 Identity Management 5.17 Authentication Information
	17.3	Cognito 토큰 클레임 신뢰 오류로 인한 계정 하이재킹	2.5.1 사용자 계정 관리 2.5.3 사용자 인증	5.16 Identity Management 5.17 Authentication Information
Cloud Formation	18.1	CloudFormation의 PassRole으로 인한 권한 상승	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.18. Access rights 8.2. Privileged access rights
OpenSearch	19.1	OpenSearch 도메인 공개 접근 및 광범위 권한 정책으로 인한 데이터 유출	2.6.1 네트워크 접근 2.5.5 특수 계정 및 권한관리	8.20. Networks security 8.22. Segregation of networks 8.3. Information access restriction
Elastic Beanstalk	20.1	Elastic Beanstalk 환경 속성/애플리케이션 번들 내 민감정보 노출로 인한 데이터 유출	2.5.4 비밀번호 관리 2.8.5 소스 프로그램 관리 2.7.1 암호정책 적용 2.7.2 암호키 관리	8.9. Configuration management 8.24. Use of cryptography
Redshift	21.1	Redshift 클러스터 암호화 미설정으로 인한 운영/보안 리스크	2.7.1 암호정책 적용 2.7.2 암호키 관리 2.9.3 백업 및 복구관리	8.9. Configuration management 8.24. Use of cryptography
Glue	22.1	Glue 개발 엔드포인트 생성/수정 시 PassRole을 통한 권한 상승	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.6.6 원격접근 통제	8.2. Privileged access rights 8.9. Configuration management
Service Catalog	23.1	Service Catalog 관리자 권한 탈취 시 Launch Constraint 악용으로 IAM 권한 상승	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.18. Access rights 8.2. Privileged access rights
DocumentDB	24.1	DocumentDB 스냅샷 공개 오설정으로 인한 데이터 노출	2.5.6 접근권한 검토 2.6.1 네트워크 접근 2.7.1 암호정책 적용 2.7.2 암호키 관리 2.9.3 백업 및 복구관리	8.3 Information access restriction 8.12. Data leakage prevention 8.24. Use of cryptography
Bedrock	25.1	Bedrock의 과도한 접근 권한으로 인한 LLM 서비스 남용 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	8.2. Privileged access rights
SES	26.1	SES 접근 권한 과다로 인한 대량 피싱/스팸 발송 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.9.2 성능 및 장애관리	8.2. Privileged access rights
AppStream 2.0	27.1	AppStream 2.0 환경을 통한 과도한 권한 및 자격 증명 탈취	2.5.5 특수 계정 및 권한관리. 2.5.1 사용자 계정 관리 2.5.6 접근권한 검토 2.6.3 응용프로그램 접근	5.18. Access rights 8.2. Privileged access rights 8.9. Configuration management

진행 흐름

: ISMS-P와 ISO27001 매핑

ISMS-P와 ISO27001 전 항목 매핑 → 인증 마크 효용성 의문

2. AWS 서비스 ISMS-P/ISO 27001 매칭 해당/부합 항목

각 AWS 진단 항목은 ISMS-P 및 ISO/IEC 27001 보안 통제 기준과의 부합 관계를 매핑하였습니다. 이를 통해 AWS 환경 진단 결과를 국제 표준 및 국내 인증 기준의 관점에서 함께 검토할 수 있습니다.

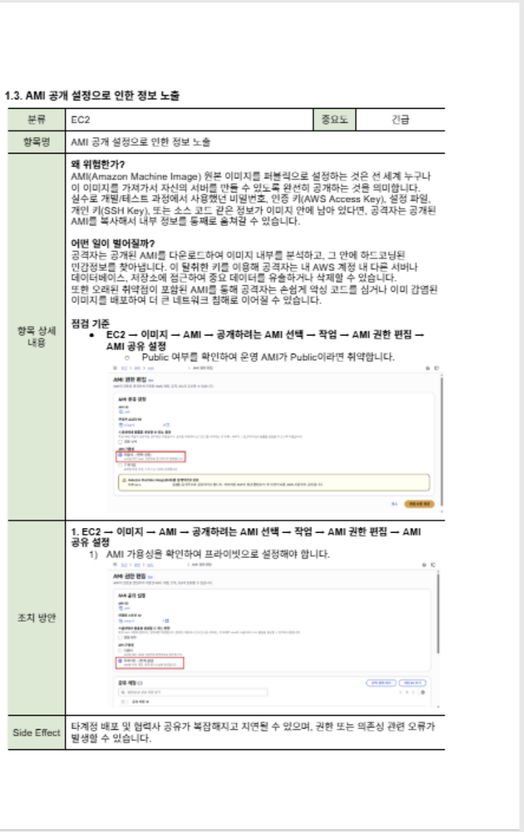
[표] 2. AWS 보안 가이드와 ISMS-P, ISO 27001 항목 매칭

서비스명	항목코드	항목명	ISMS-P 기준항목	ISO 기준항목
EC2	1.1	IMDS 보안 통제 미적용으로 인한 임시 자격 증명 탈취	2.6.2 정보시스템 접근 2.6.6 원격접근 통제	8.9 Configuration Management
	1.2	EC2 User Data 관리 실패	2.7.1 암호정책 적용 2.7.2 암호키 관리	8.3 Information Access Restriction 8.24 Use of cryptography
	1.3	AMI 공개 설정으로 인한 정보 노출	2.1.3 정보자산 관리 2.6.2 정보시스템 접근 2.7.2 암호키 관리	8.3 Information Access Restriction 8.12 Data leakage prevention
	1.4	AMI owner 속성 미설정시 위험성	2.1.3 정보자산 관리	5.9. Inventory of information and other associated assets 8.2. Privileged access rights
	1.5	Public에 공개된 SSH/RDP를 통한 자원 탈취	2.5.1 사용자 계정 관리 2.6.1 네트워크 접근 2.6.6 원격접근 통제	5.15. Access control 8.20. Networks security
	1.6	EBS 스냅샷 공개 설정시 시스템 공격 위험	2.5.6 접근권한 검토	8.2. Privileged access rights 8.12.Data leakage prevention
S3	2.1	S3 버킷 정책의 공개 설정과 Get/Put 권한으로 인한 데이터 탈취/악성코드 주입 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.6.1 네트워크 접근	5.15.Access control 8.3.Information access restriction 8.12. Data leakage prevention
	2.2	S3 객체/버킷 ACL에 의한 외부 접근 허용 및 정보유출 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.6.1 네트워크 접근	5.15. Access control 8.3. Information access restriction 8.12 Data leakage prevention
	2.3	S3 버킷 복제 권한 악용에 의한 데이터 유출 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.14. Information transfer 5.9. Inventory of information and other associated assets
IAM	3.1	IAM 자격증명 평문 저장으로 인한 유출	2.7.1 암호정책 적용 2.7.2 암호키 관리	5.17 Authentication Information 8.24 Use of Cryptography
	3.2	장기 Access Key 보관 및 변경 주기 미흡	2.5.1 사용자 계정 관리 2.5.4 비밀번호 관리 2.7.2 암호키 관리	5.15 Access control 5.16 Identity management 5.17 Authentication Information 5.18 Access Rights
	3.3	IAM 루트 계정 Access Key 관리 실패	2.5.3 사용자 인증 2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.15 Access Control 5.17 Authentication Information 5.18 Access Rights 8.2 Privileged access rights 8.3 Information access restriction
	3.4	IAM Role의 Trust Policy 속 광범위한 Principal	2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한관리 2.5.6 접근 권한 검토	5.15 Access control 5.18 Access rights 8.2 Privileged access rights 8.3 Information access restriction
	3.5	IAM PassRole으로 비인가자의 영구적 권한 획득	2.5.1 사용자 계정 관리	5.3 Segregation of Duties
			2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.15 Access control 5.18 Access Rights 8.2 Privileged Access Rights
	3.6	Identity Federation을 통한 비인가자의 역할 취득 및 리소스 접근	2.5.3 사용자 인증 2.5.6 접근권한 검토	5.16 Identity Management 5.17 Authentication Information 8.5 Secure authentication
	3.7	Cross-Account 접근 설정 미흡	2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.15 Access control 5.18 Access rights 8.3 Information Access Restriction
	3.8	퇴직자의 IAM 권한 미철회로 인한 유출 위협	2.2.5 퇴직 및 직무변경 관리 2.5.1 사용자 계정 관리 2.5.6 접근권한 검토 2.11.3 이상행위 분석 및 모니터링	5.15 Access control 5.16 Identity management 8.3 Information access restriction 8.15 Logging
	3.9	MFA 미설정	2.5.3 사용자 인증 2.5.5 특수 계정 및 권한관리	5.17 Authentication Information 8.5 Secure authentication
VPC	4.1	Security Group의 광범위한 공개 규칙 설정으로 인한 서비스 노출 및 권한 탈취 위협	2.5.6 접근권한 검토 2.6.1 네트워크 접근	5.15. Access control 5.18. Access rights 8.20 Network Security 8.22. Segregation of networks
	4.2	배스천 호스트 미사용으로 인한 프라이빗 서브넷 자원 직접 접근 위협	2.6.1 네트워크 접근 2.5.6 접근권한 검토 2.6.6 원격접근 통제	5.15. Access control 8.20 Network Security 8.22 Segregation of Networks
Lambda	5.1	Lambda 코드/환경변수에 중요정보 노출	2.5.5 특수 계정 및 권한관리 2.7.1 암호정책 적용 2.7.2 암호키 관리	5.17. Authentication information 8.5 Secure Authentication 8.12. Data leakage prevention 8.24. Use of cryptography
	5.2	Lambda 함수 내부 입력값 미검증으로 인한 인젝션 위협 노출	2.8.5 소스 프로그램 관리	8.28 Secure Coding
RDS	6.1	RDS 스냅샷 공개 오설정으로 인한 데이터 유출	2.5.5 특수 계정 및 권한관리 2.6.4 데이터베이스 접근 2.9.3 백업 및 복구관리	8.9. Configuration management 8.12. Data leakage prevention
	6.2	공개 RDS 인스턴스로 인한 데이터 유출	2.6.1 네트워크 접근 2.6.4 데이터베이스 접근 2.6.7 인터넷 접속 통제	5.15. Access control 8.20. Networks security 8.22. Segregation of networks
Cloud Trail	7.1	CloudTrail 비활성화 시 로그 미수집으로 인한 추적 불가 위험성	2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및 모니터링	5.7. Threat intelligence 8.15. Logging 5.28. Collection of evidence
	7.2	CloudTrail 비정상적인 API 호출 감시 미흡	2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검	5.7. Threat intelligence 5.28. Collection of evidence 8.2. Privileged access rights 8.15. Logging
EKS	8.1	EKS 과도한 권한 설정으로 인한 Pod 침투와 자격증명 탈취	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.6.1 네트워크 접근	5.18. Access rights 8.2. Privileged access rights
KMS	9.1	KMS 권한/키 관리 오설정으로 인한 랜섬웨어 위협	2.7.2 암호키 관리 2.5.5 특수 계정 및 권한관리	8.2. Privileged access rights 8.24. Use of cryptography
SNS	10.1	SNS 주제 액세스 정책 과다 허용으로 인한 SMS 스미싱 악용	2.5.5 특수 계정 및 권한관리 2.6.3 응용프로그램 접근	5.15. Access control 5.18. Access rights 8.3. Information access restriction
SQS	11.1	SQS 큐 정책 과도 권한	2.5.5 특수 계정 및 권한관리 2.6.3 응용프로그램 접근	5.15. Access control 5.18. Access rights 8.3. Information access restriction
Route 53	12.1	Route 53 DNS 레코드 미정리로 인한 Takeover	2.1.3 정보자산 관리 2.6.1 네트워크 접근 2.10.3 공개서버 보안	5.9. Inventory of information and other associated assets 8.9. Configuration management 8.21. Security of network services
Organizations	13.1	Organizations Trusted Access 관리 미흡으로 조직 전체 계정 장악	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.6.2 정보시스템 접근	5.18. Access rights 8.2. Privileged access rights 8.3 Information Access Restriction
	13.2	Organizations SCP 미적용으로 인한 불필요 API 호출	2.5.5 특수 계정 및 권한관리 2.6.2 정보시스템 접근	8.2 Privileged Access Rights 8.3 Information Access Restriction 8.9. Configuration management
ECR	14.1	잘못된 ECR 관련 정책으로 인한 악성코드 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	8.2 Privileged Access Rights 8.3 Information Access Restriction
SSM	15.1	SendCommand(RunCommand)를 통한 EC2에서의 악성 셸 명령 실행	2.5.5 특수 계정 및 권한관리 2.6.6 원격접근 통제	8.2. Privileged access rights
	15.2	SSM 문서 공개 설정으로 인한 자격 증명 노출	2.1.3 정보자산 관리 2.5.6 접근권한 검토 2.6.2 정보시스템 접근	5.12.Classification of information 5.15. Access control 8.3 Information access restriction
GuardDuty	16.1	GuardDuty 비활성화로 인한 위협 탐지 실패	2.11.3 이상행위 분석 및 모니터링 2.10.1 보안시스템 운영 2.11.3 이상행위 분석 및 모니터링	5.7. Threat intelligence 5.24. Incident management planning & preparation 8.15. Logging 8.16. Monitoring activities
Cognito	17.1	Cognito Identity Pool에 연결된 IAM Role의 과도 권한	2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.15 Access Control 8.2 Privileged Access Rights 8.3 Information Access Restriction
	17.2	Cognito Self-sign-up 허용으로 인한 비인가 계정 생성 위협	2.5.1 사용자 계정 관리 2.5.3 사용자 인증 2.5.4 비밀번호 관리	5.16 Identity Management 5.17 Authentication Information
	17.3	Cognito 토큰 클레임 신뢰 오류로 인한 계정 하이재킹	2.5.1 사용자 계정 관리 2.5.3 사용자 인증	5.16 Identity Management 5.17 Authentication Information
Cloud Formation	18.1	CloudFormation의 PassRole으로 인한 권한 상승	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.18. Access rights 8.2. Privileged access rights
OpenSearch	19.1	OpenSearch 도메인 공개 접근 및 광범위 권한 정책으로 인한 데이터 유출	2.6.1 네트워크 접근 2.5.5 특수 계정 및 권한관리	8.20. Networks security 8.22. Segregation of networks 8.3. Information access restriction
Elastic Beanstalk	20.1	Elastic Beanstalk 환경 속성/애플리케이션 번들 내 민감정보 노출로 인한 데이터 유출	2.5.4 비밀번호 관리 2.8.5 소스 프로그램 관리 2.7.1 암호정책 적용 2.7.2 암호키 관리	8.9. Configuration management 8.24. Use of cryptography
Redshift	21.1	Redshift 클러스터 암호화 미설정으로 인한 운영/보안 리스크	2.7.1 암호정책 적용 2.7.2 암호키 관리 2.9.3 백업 및 복구관리	8.9. Configuration management 8.24. Use of cryptography
Glue	22.1	Glue 개발 엔드포인트 생성/수정 시 PassRole을 통한 권한 상승	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.6.6 원격접근 통제	8.2. Privileged access rights 8.9. Configuration management
Service Catalog	23.1	Service Catalog 관리자 권한 탈취 시 Launch Constraint 악용으로 IAM 권한 상승	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	5.18. Access rights 8.2. Privileged access rights
DocumentDB	24.1	DocumentDB 스냅샷 공개 오설정으로 인한 데이터 노출	2.5.6 접근권한 검토 2.6.1 네트워크 접근 2.7.1 암호정책 적용 2.7.2 암호키 관리 2.9.3 백업 및 복구관리	8.3 Information access restriction 8.12. Data leakage prevention 8.24. Use of cryptography
Bedrock	25.1	Bedrock의 과도한 접근 권한으로 인한 LLM 서비스 남용 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토	8.2. Privileged access rights
SES	26.1	SES 접근 권한 과다로 인한 대량 피싱/스팸 발송 위협	2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토 2.9.2 성능 및 장애관리	8.2. Privileged access rights
AppStream 2.0	27.1	AppStream 2.0 환경을 통한 과도한 권한 및 자격 증명 탈취	2.5.5 특수 계정 및 권한관리. 2.5.1 사용자 계정 관리 2.5.6 접근권한 검토 2.6.3 응용프로그램 접근	5.18. Access rights 8.2. Privileged access rights 8.9. Configuration management

진행 흐름

: 웹에서 가시성 좋게 현실성 있는 AWS 보안 가이드라인 제작

현실성 있는 AWS 보안 가이드라인 제작 (총 27개 서비스, 50개 항목)



1.3. AMI 공개 설정으로 인한 정보 노출

분류	EC2	중요도	긴급
항목명	AMI 공개 설정으로 인한 정보 노출		
항목 상세 내용	**왜 위험한가?** AMI(Amazon Machine Image) 원본 이미지를 퍼블릭으로 설정하는 것은 전 세계 누구나 이 이미지를 가져가서 자신의 서버를 만들 수 있도록 완전히 공개하는 것을 의미합니다. 실수로 개발/테스트 과정에서 사용했던 비밀번호, 인증 키(AWS Access Key), 설정 파일, 개인 키(SSH Key), 또는 소스 코드 같은 정보가 이미지 안에 남아 있다면, 공격자는 공개된 AMI를 복사해서 내부 정보를 통째로 출처할 수 있습니다. **어떤 일이 벌어질까?** 공격자는 공개된 AMI를 다운로드하여 이미지 내부를 분석하고, 그 안에 하드코딩된 인증정보를 찾아냅니다. 이 탈취한 키를 이용해 공격자는 내 AWS 계정 내 다른 서버나 데이터베이스, 저장소에 접근하여 중요 데이터를 유출하거나 삭제할 수 있습니다. 또한 오래된 취약점이 포함된 AMI를 통해 공격자는 손쉽게 악성 코드를 심거나 이미 감염된 이미지를 배포하여 더 큰 네트워크 침해로 이어질 수 있습니다. **점검 기준** • **EC2 — 이미지 — AMI — 공개하려는 AMI 선택 — 작업 — AMI 권한 편집 — AMI 공유 설정** ○ Public 여부를 확인하여 운영 AMI가 Public이라면 취약합니다.
조치 방안	**1. EC2 — 이미지 — AMI — 공개하려는 AMI 선택 — 작업 — AMI 권한 편집 — AMI 공유 설정** 1) AMI 가용상은 확인하여 프라이빗으로 설정해야 합니다.
Side Effect	타계정 배포 및 협력사 공유가 복잡해지고 지연될 수 있으며, 권한 또는 의존성 관련 오류가 발생할 수 있습니다.		

- 중요도
- 왜 위험한가?
- 어떤 일이 벌어질까?
- 점검 기준
- 조치 방안
- 미조치 사례
- side effect

진행 흐름

: 웹에서 가시성 좋게 현실성 있는 AWS 보안 가이드라인 제작

현실성 있는 AWS 보안 가이드라인 제작 (총 27개 서비스, 50개 항목)

- 중요도
- 왜 위험한가?
- 어떤 일이 벌어질까?
- 점검 기준
- 조치 방안
- 미조치 사례
- side effect

진행 흐름

: 웹에서 가시성 좋게 현실성 있는 AWS 보안 가이드라인 제작

가이드라인의 실행을 돕는 체크리스트 제작 필요성 (총 63개 항목)

NO	항목명	가이드 매핑	O/X	자동 점검 가능
1	EC2 인스턴스 메타데이터 옵션의 IMDSv2를 필수로 선택	1.1		O
2	민감 정보가 안전하게 보관(ex. 환경변수에 민감정보를 평문 저장하지 말고 Secrets Manager에서 보안 암호 형태로 저장)	1.2 3.1 5.1		O
3	EC2 AMI 가용성이 프라이빗으로 설정	1.3		O
4	Organizations SCP 정책 설정에서 사전 허용된 계정 목록의 AMI만 리스트에 등록	1.4		X
5	보안그룹 인바운드 규칙이 원격(SSH, RDP), DB, 관리 포트 소스의 CIDR을 좁은 범위(/16~)로 설정	1.5 4.1 6.2		O
6	EBS 스냅샷의 공유 옵션이 프라이빗으로 설정	1.6		O
7	퍼블릭 용도의 S3 버킷이 아닐 경우, 모든 퍼블릭 액세스 차단 활성화	2.1		O
8	S3 버킷 정책 속 Principal이 특정 ARN으로 제한되어 있고 Resource는 버킷 안 특정 폴더로 지정	2.1		O
9	S3 ACL 설정 속 모든 사람, 인증된 사용자 그룹의 나열, 읽기, 쓰기 권한 체크 해제	2.2		O
10	S3 ACL의 Grantee 목록에 12자리 숫자(외부 AWS 계정 ID)가 있으면 해당 공유를 검증	2.2		X
11	S3 복제 규칙에 사용되는 IAM 역할의 정책 속 Resource에 대상 버킷 ARN 지정	2.3		O
12	시크릿 스캐닝 도구를 통한 자격증명 평문 저장 여부 점검(ex. Trufflehog, Gitleaks 등으로 외부/공개 저장소 속 자격증명 평문 저장 점검)	3.1		X
13	액세스 키가 생성된 후 90일 이내	3.2		O
14	민감 정보의 자동 교체 로직이 존재(ex. Secrets Manager의 보안 암호 자동 교체 구성 활성화)	3.2		X
15	루트 계정의 Active 액세스 키 비활성화	3.3		O

03 CloudDoctor

- 소개
- 시연 영상

03

소개

: CloudDoctor

가이드

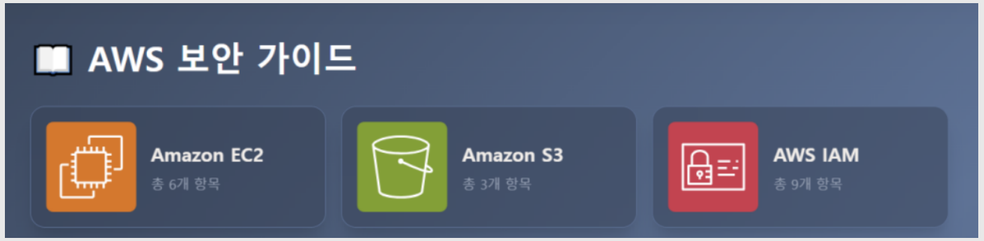
- 실제 침해사례 기반의 대응 가이드
- 상세내용 / 점검 기준 / 조치 방안 / Side Effect 등 제공

체크리스트

- 가이드를 바탕으로 산출된 항목들을 O / X 로 체크
- 결과값에 대한 등급을 Nice/ Warning / Critical 로 제공

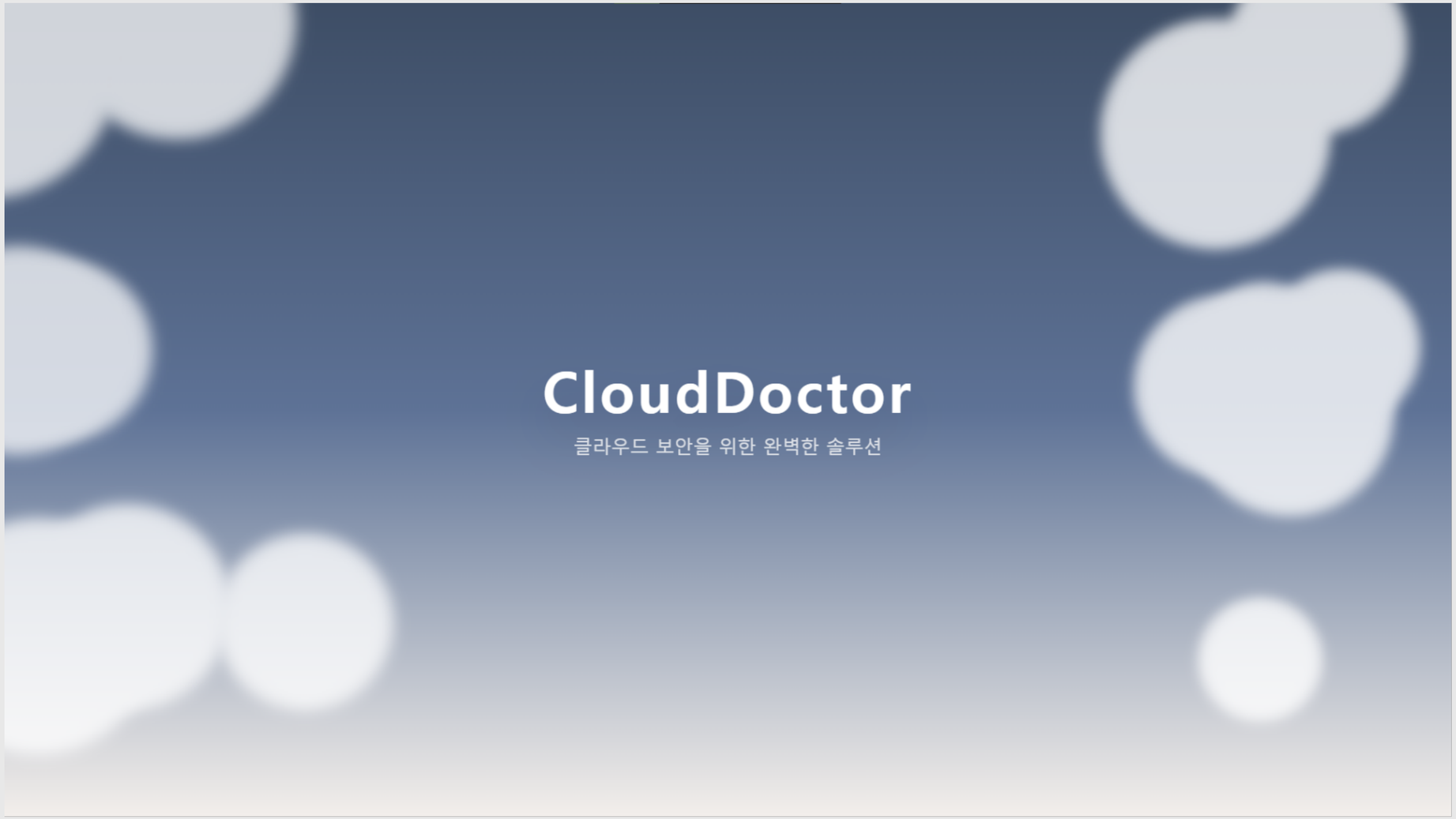
보안 점검

- 가이드와 체크리스트를 토대로 보안 상태를 자동 점검
- 보안 점검 결과, raw data, 조치 가이드 링크 형식의 결과 제공



시연 영상

: CloudDoctor 시연 영상



04 Outro

- 향후 계획

04

향후 계획

: AWS 침해사고 추가 조사 및 가이드라인/체크리스트/웹 기반 자동 점검 도구 디벨롭

클라우드 침해사고 추가 조사

기존 가이드라인 및 체크리스트 디벨롭

타 CSP 대상(Azure, GCP..)
가이드라인 및 체크리스트 제작

LLM 기반 자동 점검 및
조치 가이드 챗봇 제작

#AWSKRUG

현실성 있는 AWS 보안 가이드라인 작성기

: 침해사고 사례 분석부터 가이드라인 및 체크리스트 작성까지

Thank you

#AWSKRUG

현실성 있는 AWS 보안 가이드라인 작성기
: 침해사고 사례 분석부터 가이드라인 및 체크리스트 작성까지

Q&A