1.9 MFA (Multi-Factor Authentication) 설정

취약점 설명

MFA, 흔히 말하는 **2**차인증 **, OTP,** 다중 인증 과 같다 **.** 사용자의 아이디 **,** 패스워드 뿐만 아니라 다른 방법으로 추가 인증을 진행하는 것

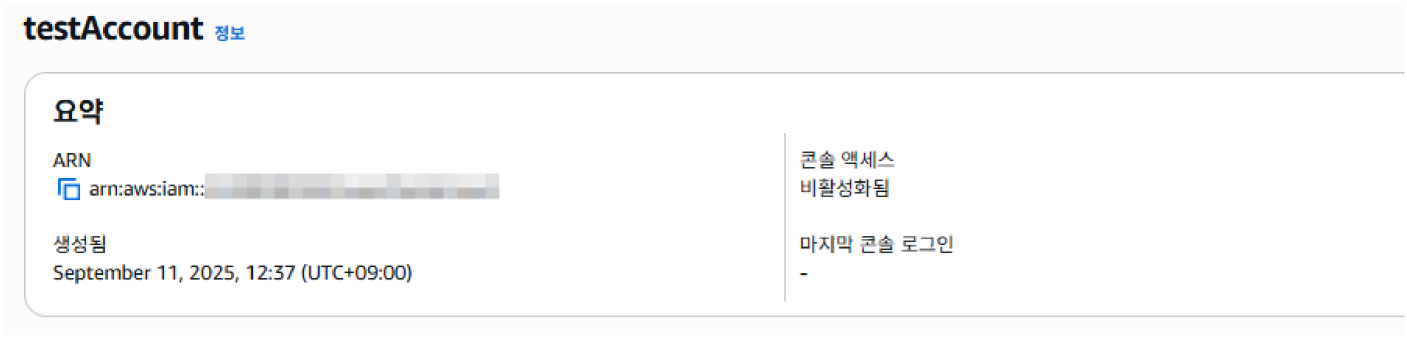
요즘은 다른 곳에서 유출된 계정 정보를 가지고 다른 서비스에도 대입해보는 크리덴셜 스터핑 공격이 성행하기 때문에

사용자의 추가 인증이 거의 필수가 되는 듯 하다 **.**

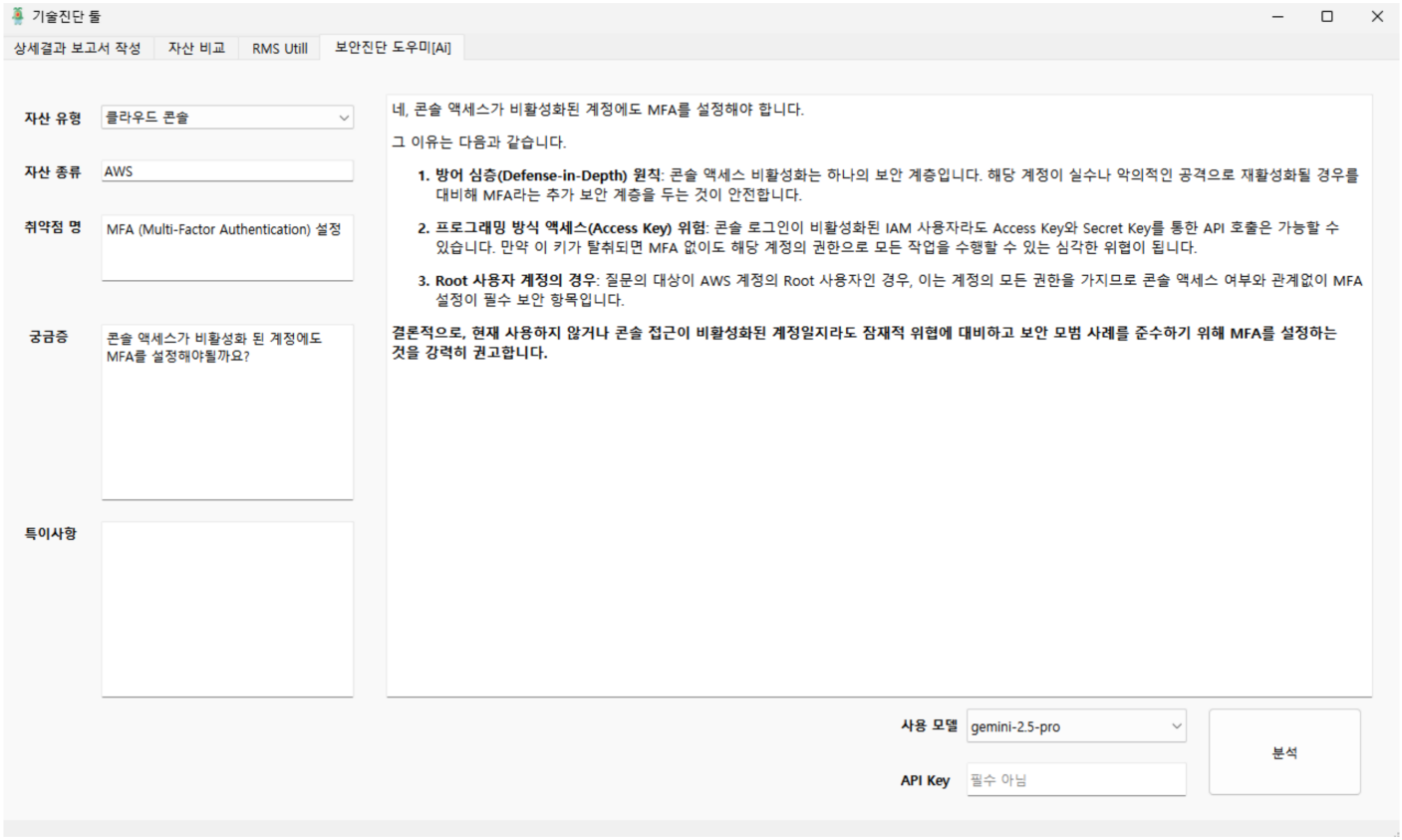
딴소리

MFA인증 방식은 아래와 같다 **.**

테스트를 해보다 보니 궁금점 콘솔 액세스가 비활성화 된 계정에 **MFA**를 설정하는게 의미가 있을까 **?**

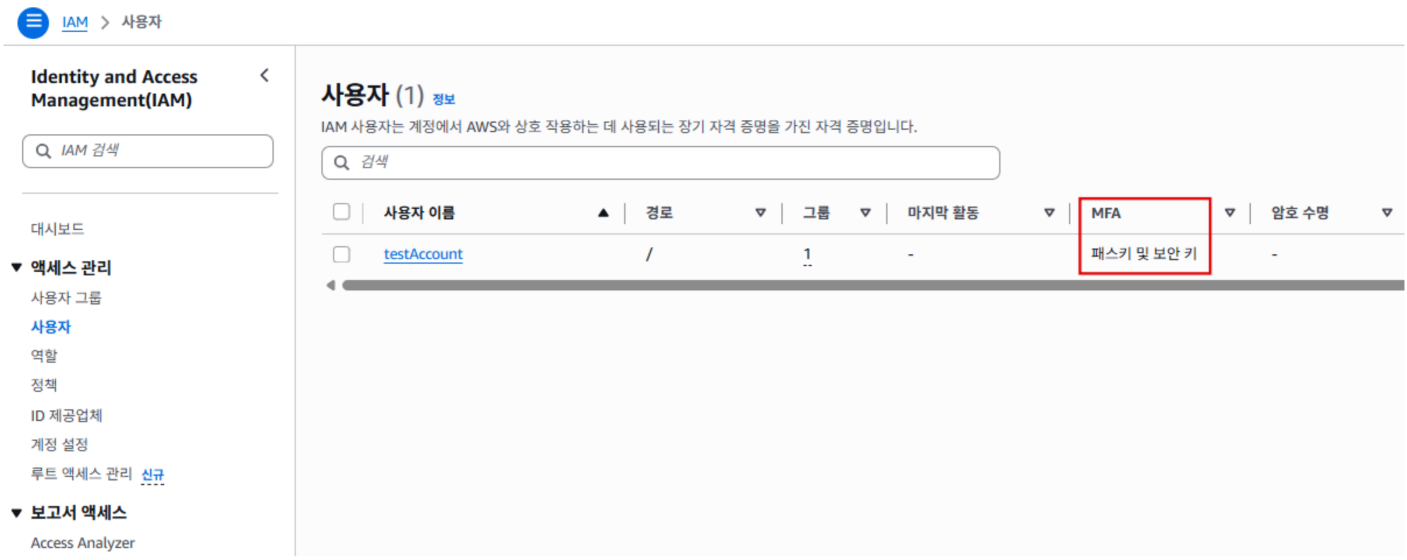


개인적으로 만들어서 쓰고 있는 보안 컨설턴트 페르소나를 가지고 있는 **ai api**에 물어보니 그렇다고 한다 .



> 진단 방법

01. [IAM] -> [사용자 **] ->** 사용자 목록에 **MFA**가 활성화 되어 있는지 확인



양호 취약 기준

진단 기준	**양호기준** : AWS 계정 및 IAM 사용자 계정 로그인 시 MFA가 활성화 되어 있을 경우 **취약기준** : AWS 계정 및 IAM 사용자 계정 로그인 시 MFA 가 비활성화 되어 있을 경우
비고	MFA 인증을 사용하지 않고 SSO 인증을 통해서 로그인할 경우 양호로 처리될 수 있음

양호 : 사용자 계정 로그인 시 **MFA**를 사용하고 있을 시

취약 : **MFA**가 활성화 되어 있지 않은 계정이 존재할 경우

참고

Revision #2
Created 2025-09-19 22:15:37 UTC by minwoo
Updated 2025-09-19 22:34:37 UTC by minwoo