

# Security With Amazon Q Developer CLI

이지영  
놀 유니버스

## 보안 엔지니어가 하는 일들

외부에 오픈된 보안그룹 점검

기사에 나온 CVE가 우리 회사에  
해당되는지 확인하기

어제밤 발견된 Findings 찾기

보안 로그 분석하기

...

## Amazon Q Developer CLI 시작하기

```
brew install --cask amazon-q
```

A silver laptop is shown from a front-facing perspective, slightly angled to the right. The screen is dark gray and displays the command 'brew install --cask amazon-q' in white text. The laptop is set against a dark blue background with a subtle gradient and some faint, light blue circular patterns on the left side.

## Amazon Q Developer CLI에서 Agent 만들기

q chat --agent AgentName 으로 실행

/agent list

/agent create --name AgentName

/agent schema

경로

Global~/.aws/amazon/cli-agents/{agent-name}.json

Project-level.amazon/cli-agents/{agent-name}.json

작성 예 : <https://docs.aws.amazon.com/amazonq/latest/qdeveloper-ug/command-line-custom-agents-examples.html>

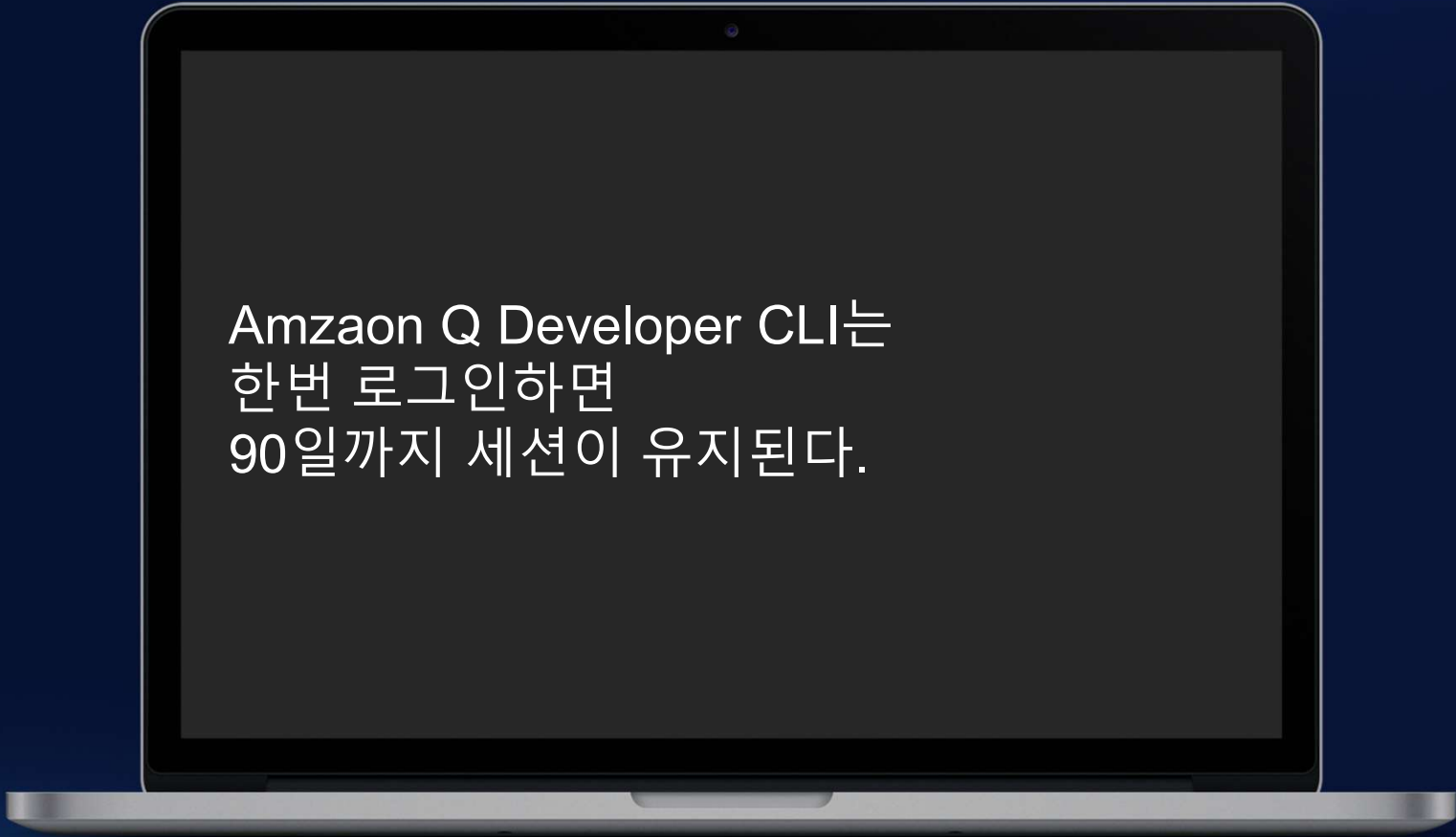
## Amazon Q Developer CLI의 공통 rules 설정

```
# 프로젝트 보안 표준 파일 생성
mkdir -p .amazonq/rules

cat > .amazonq/rules/security-standards.md
<< 'EOF'
# 보안 표준 및 모범 사례

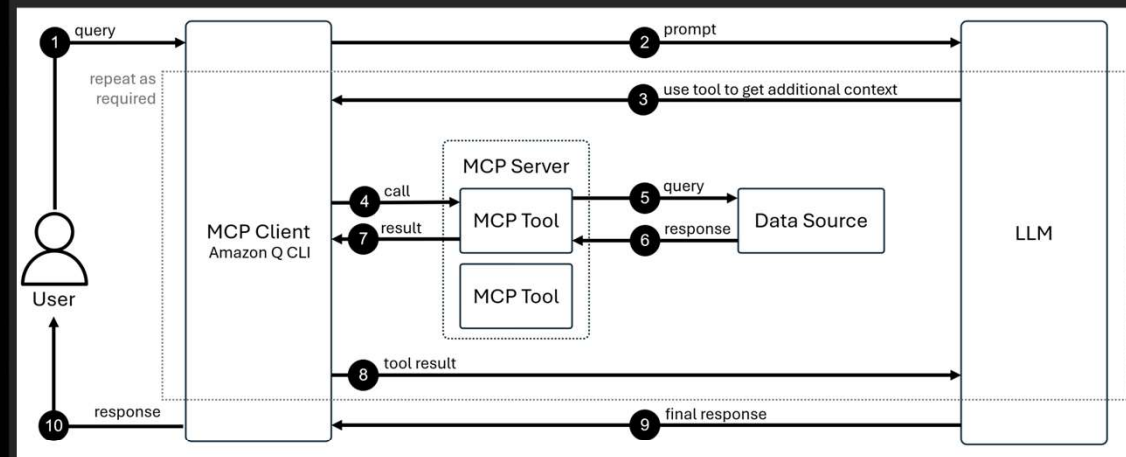
## 필수 보안 요구사항
- 모든 API 엔드포인트는 인증 및 인가
EOF
```

## Amazon Q Developer CLI의 로그인 세션 타임



Amazon Q Developer CLI는  
한번 로그인하면  
90일까지 세션이 유지된다.

## Amazon Q Developer CLI 시작하기 – MCP 서버 추가



## Amazon Q Developer CLI 시작하기 – MCP 서버 추가

MCP를 사용하지 않는 경우 :

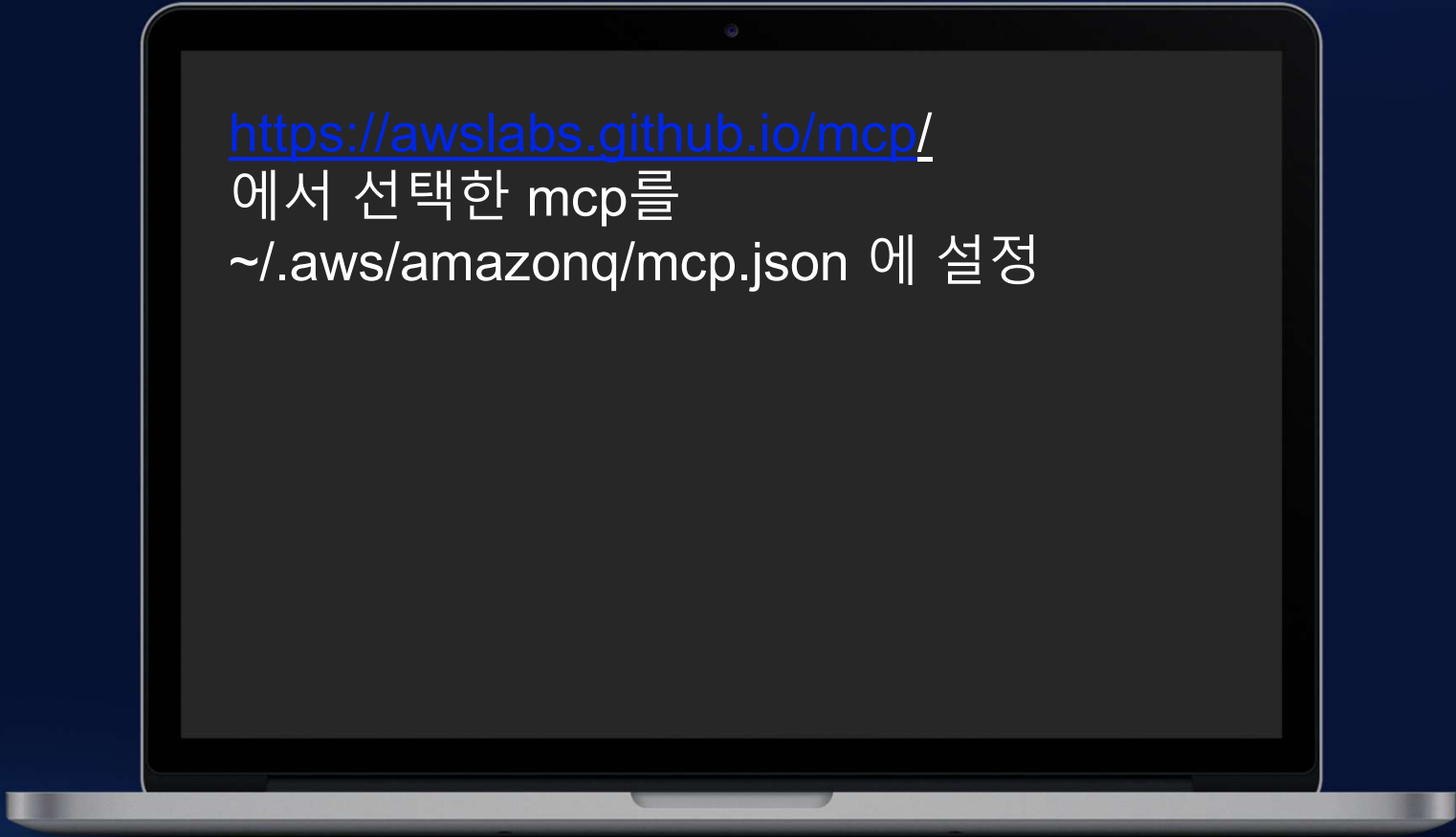
boto3 등의 스크립트를 짜서 접근 시도

MCP를 사용하는 경우 :

API를 사용해서 바로 접근

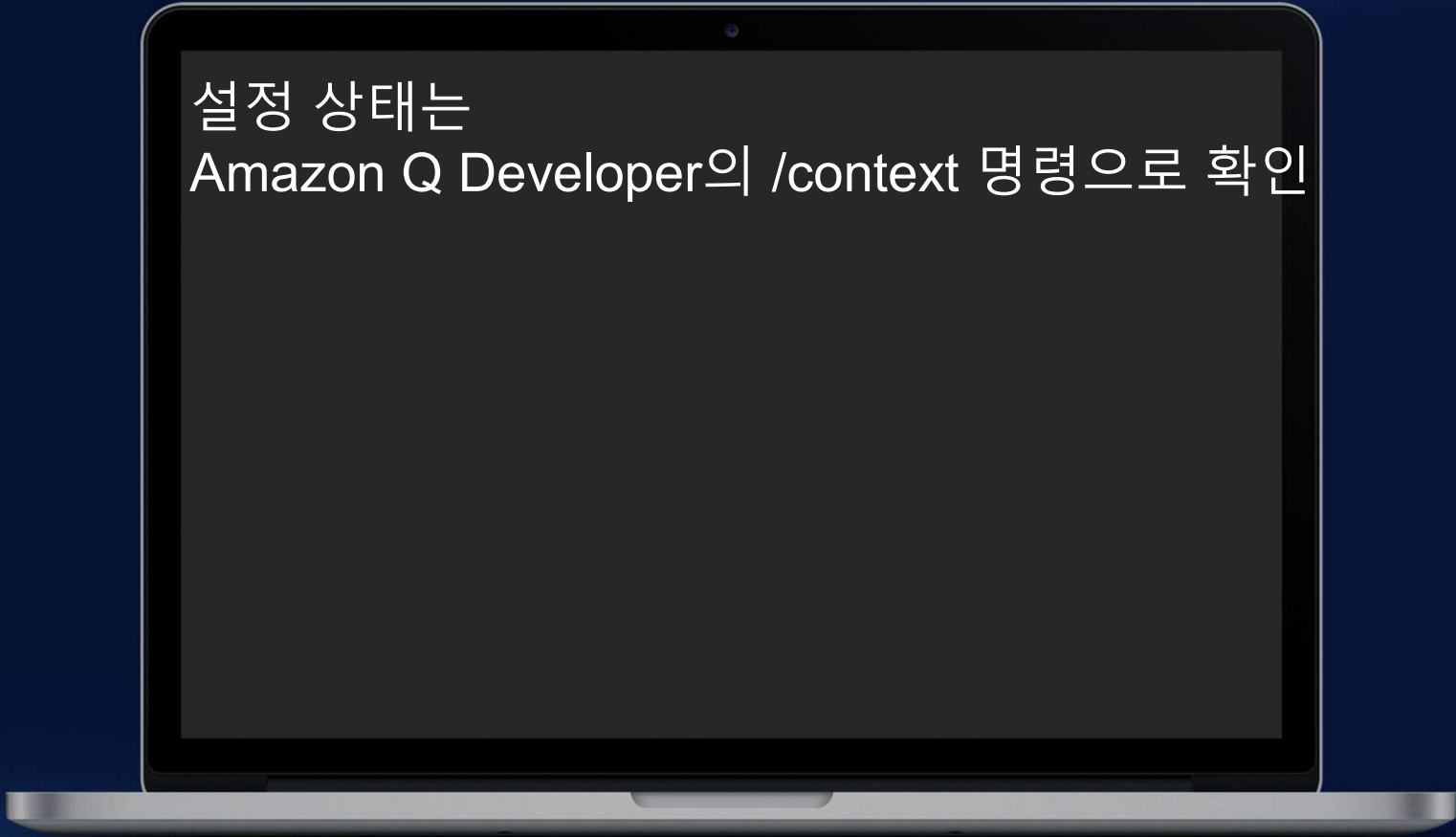


## Amazon Q Developer CLI 시작하기 – MCP 서버 추가



<https://awslabs.github.io/mcp/>  
에서 선택한 mcp를  
~/.aws/amazonq/mcp.json 에 설정

## Amazon Q Developer CLI의 공통 rules 설정



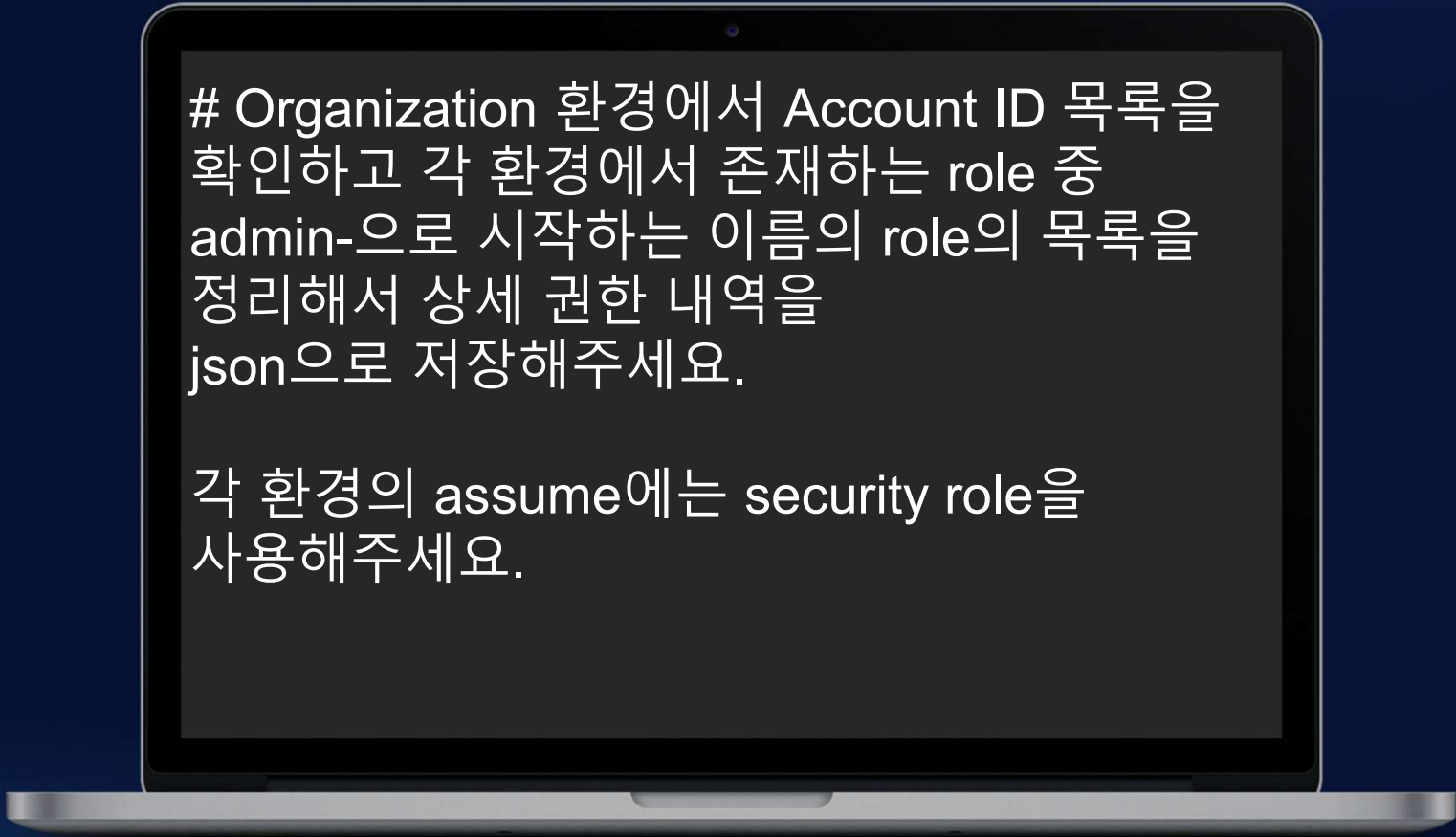
설정 상태는  
Amazon Q Developer의 /context 명령으로 확인

## Amazon Q Developer CLI의 에디터 모드

A laptop is shown from a front-facing perspective, centered against a dark blue gradient background. The laptop screen is dark gray and displays two lines of white Korean text. The text explains that using the `/editor` command allows for entering the editor mode to write prompts.

`/editor` 명령 사용하면 편집기 모드로  
프롬프트 작성 가능

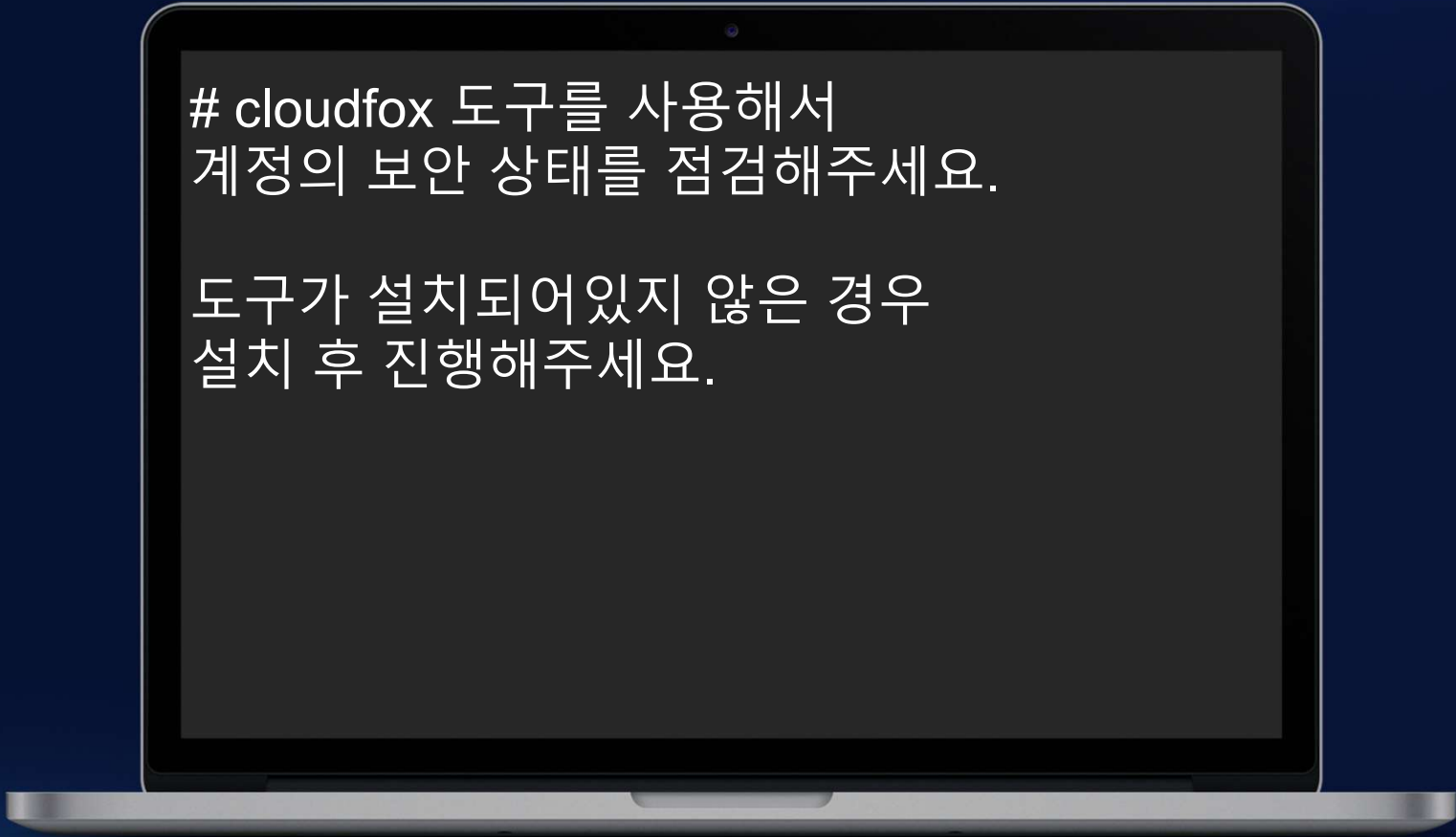
## Amazon Q Developer CLI의 커맨드 팁 – Organization 환경에서 사용



# Organization 환경에서 Account ID 목록을  
확인하고 각 환경에서 존재하는 role 중  
admin-으로 시작하는 이름의 role의 목록을  
정리해서 상세 권한 내역을  
json으로 저장해주세요.

각 환경의 assume에는 security role을  
사용해주세요.

## Amazon Q Developer CLI의 커맨드 팁 – 서드파티 툴 사용

A laptop screen is shown against a dark blue background. The screen displays two lines of white text. The first line is a command prompt instruction, and the second line is a note about installation.

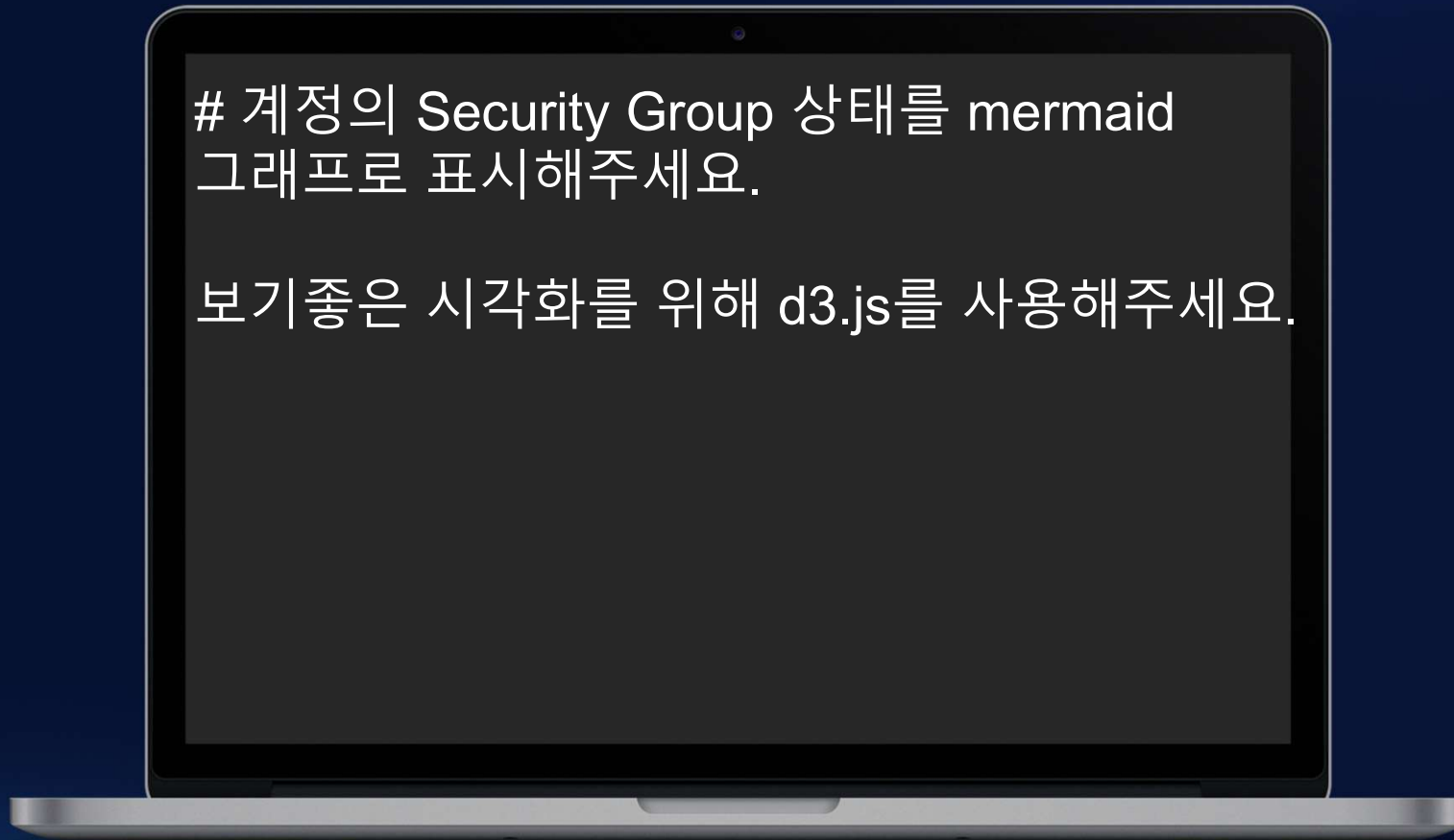
# cloudflox 도구를 사용해서  
계정의 보안 상태를 점검해주세요.

도구가 설치되어있지 않은 경우  
설치 후 진행해주세요.

## Amazon Q Developer CLI의 커맨드 팁 – 시각화

# 계정의 Security Group 상태를 mermaid  
그래프로 표시해주세요.

보기좋은 시각화를 위해 d3.js를 사용해주세요.





AI 도구는 고민에 필요한  
시간을 벌어주는 도구