rule 연구 예시

2022.08.26.~2022.12.17.

강대명(주멘토), 정승기(부멘토), 이재상(PL)

배경석(PM), 박병제, 임태인, 정금종, 차유담

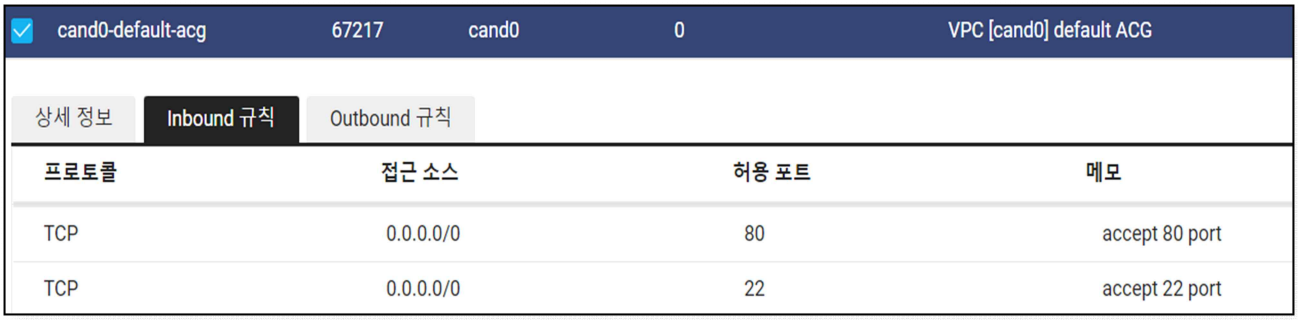
보안 위협

- 예시

: 0.0.0.0으로 22번 포트를 Open하면 비인가자가 SSH 접근이 가능하여 취약

```
resource "ncloud_access_control_group_rule" "fail1_2" {
  access_control_group_no = ncloud_access_control_group.acg.id
  inbound {
    protocol    = "TCP"
    ip_block    = "0.0.0.0/0"
    port_range  = "22"
    description = "accept 22 port"
  }
```

Terraform Code



ACG 생성

■ NCP 보안 위협 체크리스트 제작

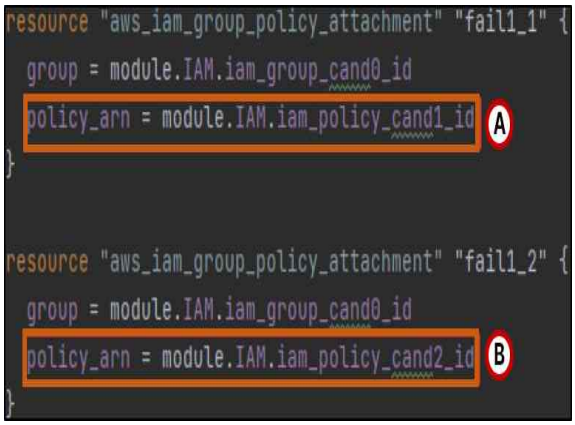
▶ 서버(2) ▶ 스토리지(2) ▶ 키(1)
▶ 네트워크(11) ▶ 로드밸런서(5) ▶ 오토스케일링(2) ▶ 쿠버네티스(3)

잘못된 구성

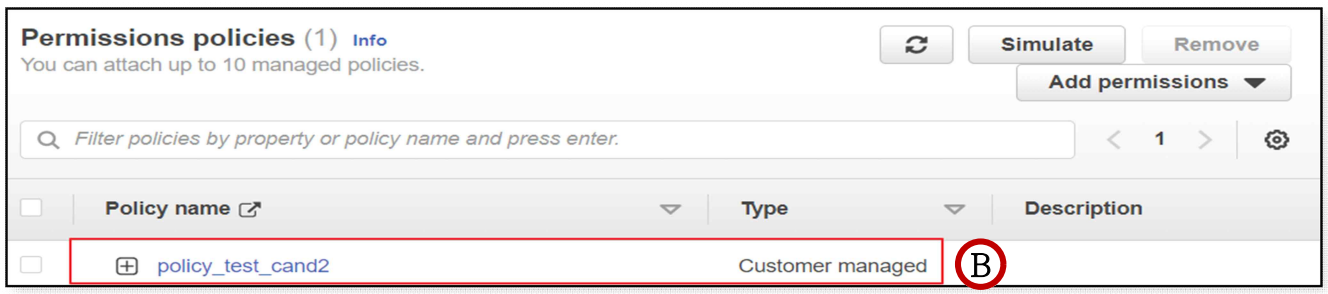
- 예시

: 사용자의 실수로 같은 정책을 두 번 선언한 후 하나의 정책을 변경하면 최종적으로 두 개의 정책이 선언되는 것이 아닌 하나의 정책만 적용이 된다.

Step 1



Step 2



Result

Step 1) 사용자는 같은 그룹과 정책을 두 번 선언한 후 배포한다.
Step 2) 하나의 리소스를 변경한다.
Step 3) 최종적으로 A 그룹에 A와 B 정책이 선언되어있어야 하지만 B만 선언되는 것을 확인할 수 있다.

■ AWS 구성상 오류 체크리스트 제작 ▶ 총합 : 33개

▶ IAM(7) ▶ VPC(8) ▶ EC2(4)
▶ EBS(4) ▶ S3(10)

■ NCP 구성상 오류 체크리스트 제작 ▶ 총합 : 6개

▶ 네트워크(4) ▶ 서버(2)