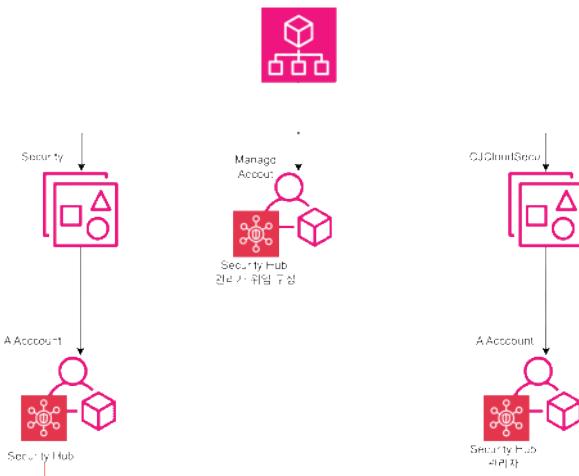


Security Hub 이벤트 통합방안

2025년 12월 11일 목요일 오전 10:56

1. 구성 목표

Security Hub 관리자 대시보드에서 위임 받은 타 계정의 보안 서비스 이벤트 통합



2. 위임 설정

- a. Organization 관리계정에서 Security hub 위임설정 #AWS 계정란에 Security Hub 관리계정 입력

aws

검색 [월트+]

아시아 태평양 (서울) AWSAdministratorAccess/jehwan.myeong@cj.net

보안 허브 > 온보드

Security Hub 구성

이렇게 하면 서비스 연결 험벌(SLR)을 생성할 수 있는 권한이 부여되고 Security Hub의 이용 약관에 동의하게 됩니다.

위임된 관리자 계정

이렇게 하면 선정한 계정은 Security Hub, Security Hub CSPM, GuardDuty 및 Inspector의 위임 관리자로 지정됩니다. 이미 이러한 서비스 중 하나에 위임 관리를 지정한 경우 해당 서비스의 위임 관리자는 업데이트되거나 변경되지 않습니다.

신뢰할 수 있는 액세스

위임된 관리자에 대한 신뢰할 수 있는 액세스 권한을 부여합니다.

이를 통해 위임받은 관리자는 엔비 계정에 악성코드 방지 기능과 같은 특정 기능을 구성할 수 있는 권한을 갖게 됩니다.

AWS 계정

962889423329

계정 ID는 12자리 숫자이어야 합니다.

위임 관리자 정책

이 정책 설명은 구심 정책 생성을 포함한 Security Hub 관리 권한을 위임 관리자에게 부여합니다.

① 위임 정책은 필요한 모든 정책 조항을 포함하여 최신 상태로 유지됩니다. 위임받은 관리자는 조직을 완벽하게 관리할 수 있습니다.

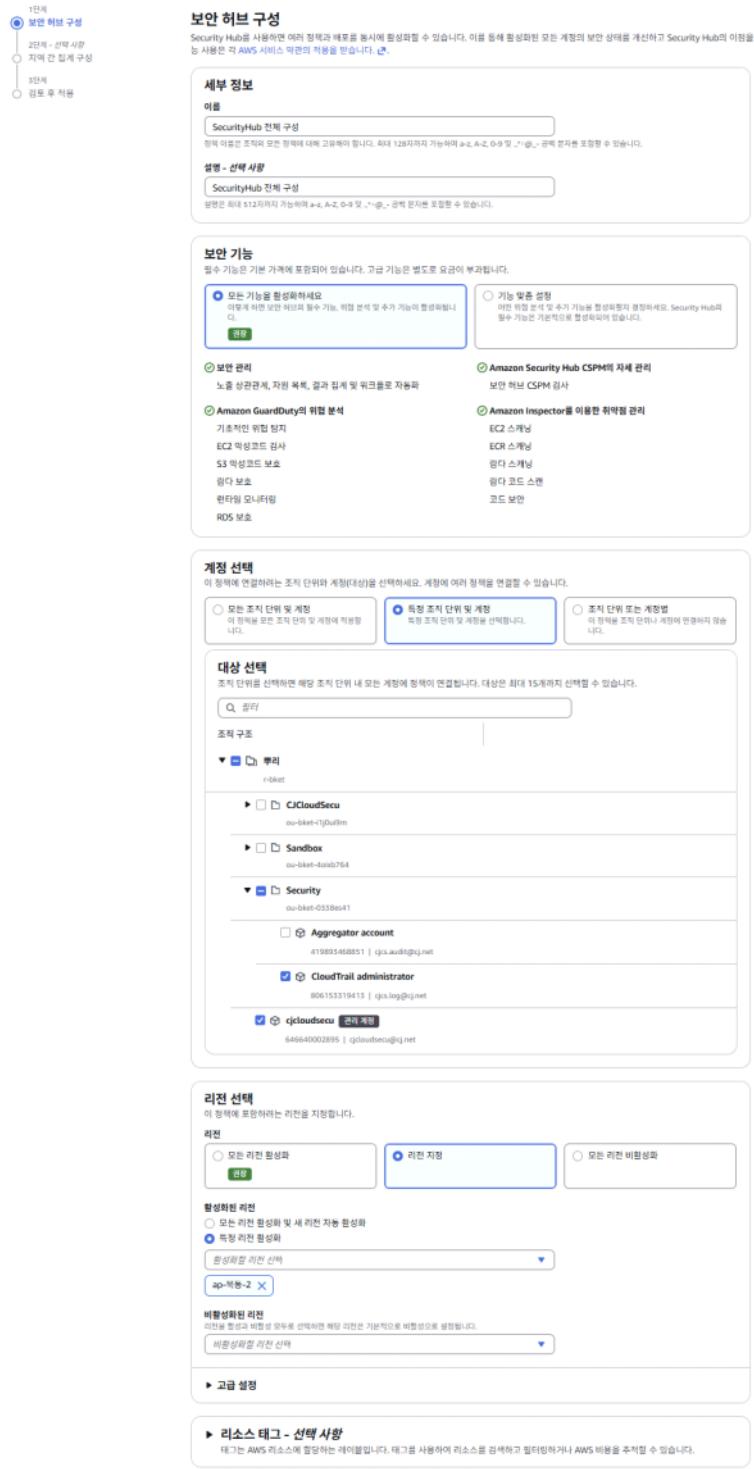
정책 세부 정보

61]
62	,
63	{
64	"Sid": "SecurityServicesDelegatingPolicyMutationActions",

- b. 위임 정책 생성 #Organization 관리계정에서 Security Hub 접속 시 자동으로 표시

The screenshot shows the AWS Security Hub interface. The left sidebar includes sections for 'Security Hub', 'Dashboard', 'Findings', 'Logs', 'Compliance', and 'AWS CloudTrail'. A 'Configuration' section is expanded, containing 'Configured policies' and 'Configuration catalog'. The main content area is titled '구성' (Configuration) and displays the 'Configured policies' tab. It includes a search bar, a table header with columns for '정책 이름' (Policy Name), '정책 유형' (Policy Type), and '정책 없음' (No policy). A large blue button labeled '구성' (Configure) is visible at the bottom right.

계정 범위 및 리전 선택 #특정 계정 및 서울 리전에만 활성화하도록 구성함



d. 완료

3. 통합 대시보드 적용

4. 후속 과제

- a. 이벤트 알림 발생: Lambda 또는 Step Function 적용해서 심각도 기준, Teams 알림 발생
 - b. 중적 저장: JIRA 연동해서 Lois Servin 내 티켓팅 생성