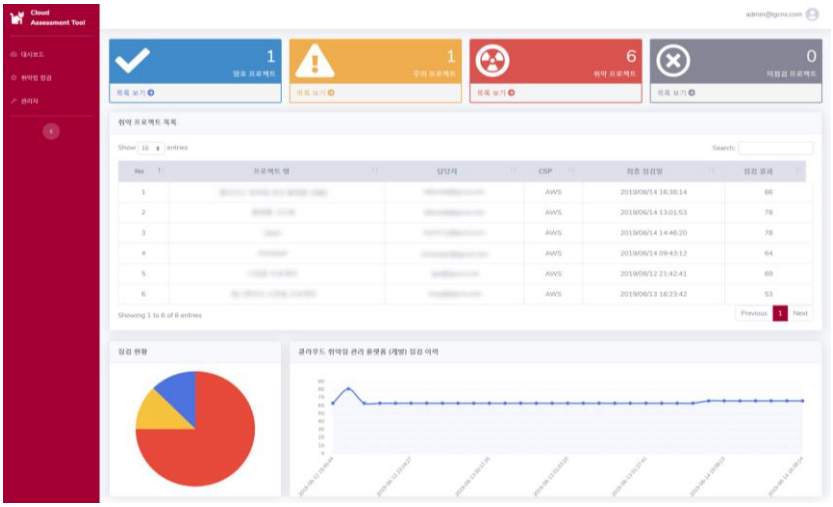
SecuXper CAT(Cloud Assessment Tool)

멀티 클라우드 대응 보안 취약점 점검 도구

Cloud Assessment Tool은,

고객사에서 운영 중인 클라우드 서비스의 보안 취약점을
통합 점검하여 해결방안을 제시하고, 점검 이력을 관리하여
높은 보안수준을 유지하기 위한 도구입니다.

서비스 이미지



주요 특징

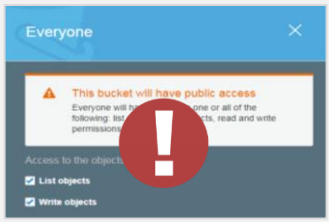
- **One-Click Diagnosis**
  AWS, Azure 등 멀티 클라우드 보안설정에서 발생하는
  취약점은 한 번 클릭으로 점검 및 자동 조치할 수 있습니다.
  ※ 멀티 클라우드 지원 및 취약점 자동 조치 기능은 추후 제공

- **Comprehensive Reports**
  취약점 발견 시 관련 법률 및 세부 조치 방법을 안내하는
  보고서를 제공합니다.

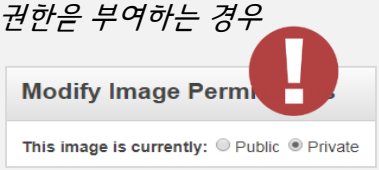
- **One-Stop Dashboard**
  대시보드에서 점검 대상 서비스/프로젝트 별 보안 점검 결과,
  양호/취약 계정 및 이력을 한 눈에 확인할 수 있습니다.

AWS에서 자주 발생하는 취약한 설정들

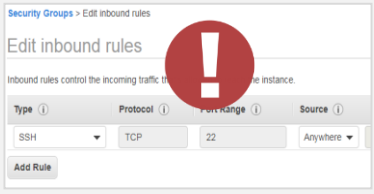
S3 Bucket은 Public Access도 설정하는 경우



서버 이미지에 Public 접근 권한을 부여하는 경우



방화벽 In-bound Rule을 Anywhere도 선택하는 경우

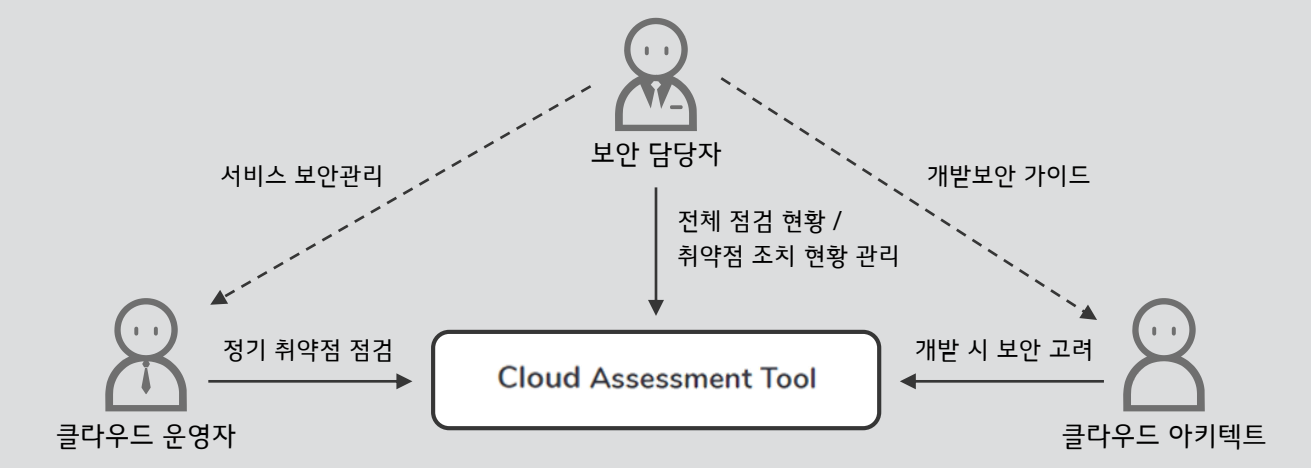


주요 점검항목

※ 점검항목은 수시 업데이트 됩니다.

구분	점검 대상	항목 수	주요 점검항목
COMPUTING	EC2, ELB	10개	• EBS Volume 암호화 적용 여부 • Load Balancer의 오래된 SSL/TLS 정책 금지 여부 등
DATABASE	RDS	5개	• 저장 시 암호화 적용 여부 / 백업 설정 여부 등
MANAGEMENT	Cloud Trail 등	7개	• Cloud Trail 설정 및 로깅 활성화 여부 등
NETWORKING	VPC	6개	• ACL 기본 값으로 모든 Traffic 외부 전송 및 내부 접근 허용 여부 등
SECURITY	IAM	21개	• Root 계정 사용 여부 / MFA 적용 여부 • 전체 역할에 대한 권한 부여 금지 / 최소 권한 원칙 준수 여부 등
STORAGE	S3	10개	• S3 Bucket에 대한 접근로그 생성 설정, 암호화 통신 및 저장 시 암호화 여부 등

Use Case



- **보안 담당자**
  조직 내 전체 계정에 대한 점검 여부를 모니터링하여 서비스 운영자에게 미점검 계정의 점검을 요청할 수 있으며, 발견된 취약점에 대한 조치 현황을 관리합니다.

- **클라우드 운영자**
  운영 중인 서비스의 보안 취약점을 정기적으로 파악하여 즉시 조치 또는 예외처리 함으로써 보안관리 업무 부담을 경감하고 안전하게 서비스를 운영합니다.
  ※ LG CNS는 월 1회 정기 점검 및 서비스 변경 시 수시 점검을 권장합니다.

- **클라우드 아키텍트**
  CAT의 점검 항목을 보안 가이드로 활용하여 설계 초기부터 보안을 고려하여 보안성 제고 및 설계 기간을 단축합니다.

서비스 문의

LG CNS Security
서울특별시 강서구 마곡중앙8로 71, LG 사이언스파크 E13
http://safezone.lgcns.com