제로트러스트 클라우드 보안 연구센터

SecurityHero RMF: Cloud Risk Management Framework

클라우드 자산 분석과 정량적 위험 평가, 권한 상승 탐지 및 대응을 통합 및 자동화한 **클라우드 위험 관리 프레임워크(RMF)**

적용분야

- 클라우드 보안
- 자산 관리
- 공격 경로 분석
- 보안 위험 평가

연구목적

· 클라우드 환경 복잡성 증가로 자산 간 접근 경로가 다양해지면서 공격 가능 경로가 식별되지 않고 방치될 위험이 증가함에 따라, **자산 관계 및 접근 경로 기반의 체계적인 보안 위험 분석·관리 필요**

· 클라우드 자산의 위험을 정량적으로 평가하는 체계 부재로 심각도 판단이 주관적이고 대응 우선순위 도출이 어려움에 따라, **위험 평가, 대응 및 영향 분석을 연계하는 통합 관리 체계 구축 필요**

· **As-Is**: 클라우드 자산 관계를 반영한 위험 분석과 정량적 평가 체계가 부족하여, **실제 공격 가능 경로가 식별되지 않고 위험 대응 우선순위와 영향 범위 판단이 주관에 의존함**

To-Be: 자산 관계 분석 및 접근 경로 분석, 정량적 위험 평가를 통해 **대응 우선순위 도출과 영향 분석까지 통합 지원하는 위험 관리 체계 구축**

**관련 표준 : NIST SP 800-30(Assessment), NIST SP 800-37(RMF), NIST SP 800-53(Controls)

연구내용

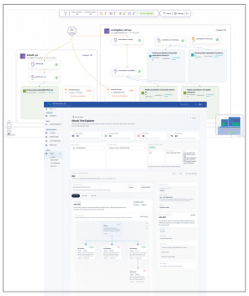
통합형 클라우드 위험 관리 프레임워크

· **자산 관계 정의 및 시각화**
클라우드 내 **자산을 수집 및 관계를 시각화하는 토폴로지** 제공
- Network Graph: 네트워크 구성 및 트래픽 흐름 시각화
- Asset Graph: 권한 및 리소스 간 관계 시각화

· **공격 경로 분석**
IAM 권한 상승 경로 분석을 통한 **권한 탈취 및 공격 확산 가능성** 식별

· **자산 위험 평가**
클라우드 **설정 오류 기반 자산의 위험 수준** 평가
- 위험 평가 기준: NIST SP 800-30 참고

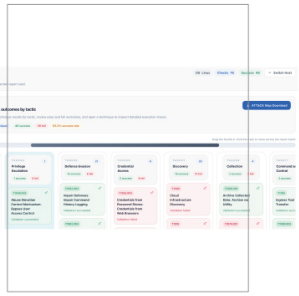
· **대응 및 영향 분석**
분석한 위험에 대한 **수정 방안 제시 및 보안 상태 변화** 분석



1. 자산 관계 정의 및 시각화

2. 공격 경로 분석

3. 자산 위험 평가



4. 대응 및 영향 분석

기술 경쟁력

기존기술 ▸▸▸▸ **기술 차별성** ▸▸▸▸ **대상기술**

기존기술	대상기술
· 자산 관계 및 접근 경로를 통합하여 고려하지 못해 전체 보안 위험 구조 파악이 어려움 · 위험을 정량적으로 평가하는 체계가 부족하여 대응 우선순위 도출이 어려움	· 자산 관계 및 접근 경로를 시각화하여 보안 위험을 구조적으로 파악 · 위험 평가 결과와 대응 방안 및 영향 분석을 연계하여 통합적 위험 관리 체계 제공
기술적 한계 · 자산 시각화: 자산 관계 및 접근 경로 통합 분석 미지원 · 위험 평가: 표준 기반 정량적 위험 평가 체계가 미흡 · 공격 분석: 자산 간 공격 경로 및 확산 가능성 분석 제한 · 대응 연계: 대응에 따른 영향 분석 미제공	**기술적 우위** · 자산 시각화: 자산들의 관계를 기반으로 접근 경로 시각화 · 위험 평가: 설정 오류 기반의 정량적 위험 평가 수행 · 공격 분석 자산 간 공격 확산 가능성을 식별 · 대응 연계: 대응 방안 적용 시 보안 상태 변화 분석

지식재산권

발명의 명칭	출원(등록)번호	출원(등록)일자
클라우드 컴퓨팅 환경의 IT 자산에 대한 시각화/위험 관리 방법 및 장치	10-2024-0142299	2024.10.17

제로트러스트 클라우드 보안 연구센터 ZeroTrust Cloud Security Research Center
부산대학교 PUSAN NATIONAL UNIVERSITY
문의처 제로트러스트 클라우드 보안 연구센터 csrc@pusan.ac.kr 051.510.7212