

46

공격그래프 기반 자동화된 보안성 평가 기술

기술개요

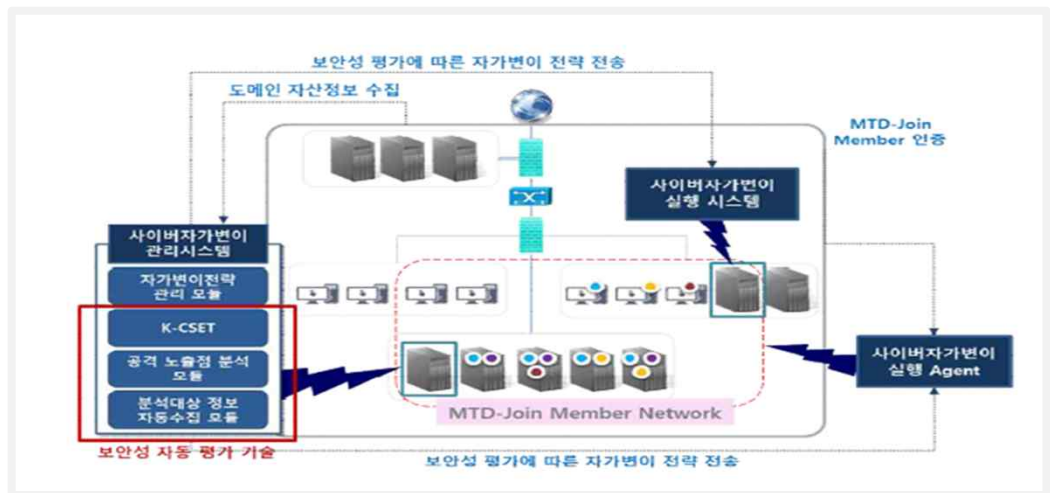
■ 공격그래프 기반 자동화된 보안성 평가 기술

- 취약점 분석 기술 발전으로 사이버 공격이 가능한 경로가 급증함에 따라 효과적인 대응 및 방어 전략을 수립 할 수 있도록 사전에 자동화된 방법으로 조직의 자산을 탐색하고 공격가능 경로를 분석해서 보안 노출점을 식별하기 위한 기술

기술의 특징점

■ 개별 취약점 및 연결성을 반영해 사이버 공격 가능 경로 탐색 가능

- 네트워크기반의 토폴로지 탐색 및 가시화 기능 제공
- 자산에 대한 상세 정보 획득을 위한 에이전트 기반의 호스트 수집 기능 제공
- CVE 기반의 공격 그래프 생성을 통한 공격가능 경로 식별 가능
- 특정 Target에 공격 가능한 모드 Attack Path 생성 및 최적 공격 경로 식별 가능



적용분야

■ 네트워크 보안/빅데이터 기반 보안관제 서비스/EDR 솔루션 개발 등

네트워크 보안	빅데이터	네트워크 보안성 평가	보안 컨설팅
<ul style="list-style-type: none"> • EDR 솔루션 개발 • 데이터 손실 방지 제품 개발 • 백신 개발 • 침입 탐지 시스템 개발 • 네트워크 보안 시스템 개발 • 빅데이터 기반 보안관제 시스템 개발 	<ul style="list-style-type: none"> • 빅데이터 기반 보안관제 서비스 • EDR 솔루션 개발 • 백신 개발 	<ul style="list-style-type: none"> • 침입 탐지 예측 서비스 • 네트워크 보안 평가 서비스 • 사이버 보험 평가 기준 제공 	<ul style="list-style-type: none"> • 사이버 보안 컨설팅 서비스 • 사이버 보험 솔루션 • 보안 담당자 교육 서비스 • 보안 전문가 양성 서비스

기술완성도 (TRL)

- TRL 5단계 : 확정된 소재/부품/시스템시작품 제작 및 성능평가 단계



기술이전 내용 및 범위

- 자산 상태정보 자동 수집 기술
 - 네트워크 기반의 토폴로지 탐색 및 가시화 기능
 - 에이전트 기반의 호스트 상태정보 수집 기능
- 공격 그래프 생성 기술
 - CVE 기반의 공격 그래프 생성을 통한 공격가능 경로 식별 기능
 - 공격가능 경로별 계산을 통한 보안강화 공격 경로 확인 기능
 - 특정 Target에 공격 가능한 모든 Attack Path 생성 및 최적 공격경로 식별 기능

관련 지재산권 현황

No.	출원번호	특허 명	상태
1	2017-0101671	네트워크 보안 강화 장치 및 그 방법	출원

기술이전 문의

- 연구성과확산실 (042-860-4946 / hjchoi2@etri.re.kr)