01

보안이벤트 자동검증 기술

발명자 : 송중석, 최장원, 최상수, 김희석, 이윤수, 최지연
등록(출원)번호 : 10-2016-0017257
등록(출원)일 : 2016년 2월

TRL 9	상용품 출시
TRL 8	상용품 완성
TRL 7	Full-Scale 시제품 개발
TRL 6	구현환경 적용실험
TRL 5	유사환경에서의 Working Model 검증
TRL 4	Lab-Scal 시제품 개발단계
TRL 3	기술컨셉 증명
TRL 2	기술컨셉 설정
TRL 1	기술원리 발표

적용가능분야 및 목표시장

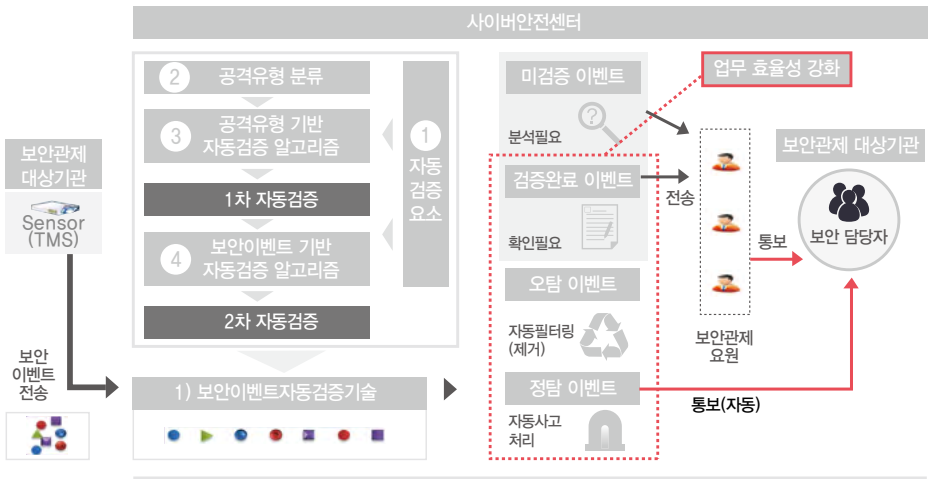
네트워크 시스템 보안, 사이버안전센터

기술 개요

본 기술은 탐지규칙 기반 보안장비(TMS, IDS/IPS 등)가 탐지한 보안이벤트를 정탐(실제 공격에 의해 발생한 보안이벤트)과 오탐(정상통신에 의해 발생한 보안이벤트)으로 자동분류하기 위한 기술임

기술의 특장점

- 본 기술을 각급 사이버안전센터(부문 및 단위 사이버안전센터 등)에 적용함으로써 현재의 분석 요원에 의한 수동분석 중심에서 시스템 기반의 자동분석 체계로 전환이 가능함
- 본 기술을 통해 국내 보안관제 체계의 효율성을 극대화할 수 있고, 국가 사이버안보를 위협하는 신·변종 및 대규모 해킹공격에 대한 조기탐지·대응이 가능함



기술이전 문의처
성과확산실 조재희/042-869-1832
jhcho87@kisti.re.kr