ETRI

25

지능형 SIEM *을 위한 인공신경망 기반 데이터 분석 및 탐지 기술

*SIEM : Security Information and Event Management

기술개요

▪ 정탐 로그(True Alert) 를 실시간 분석하여 실시간 침해위협(Threat)을 탐지하는 기술

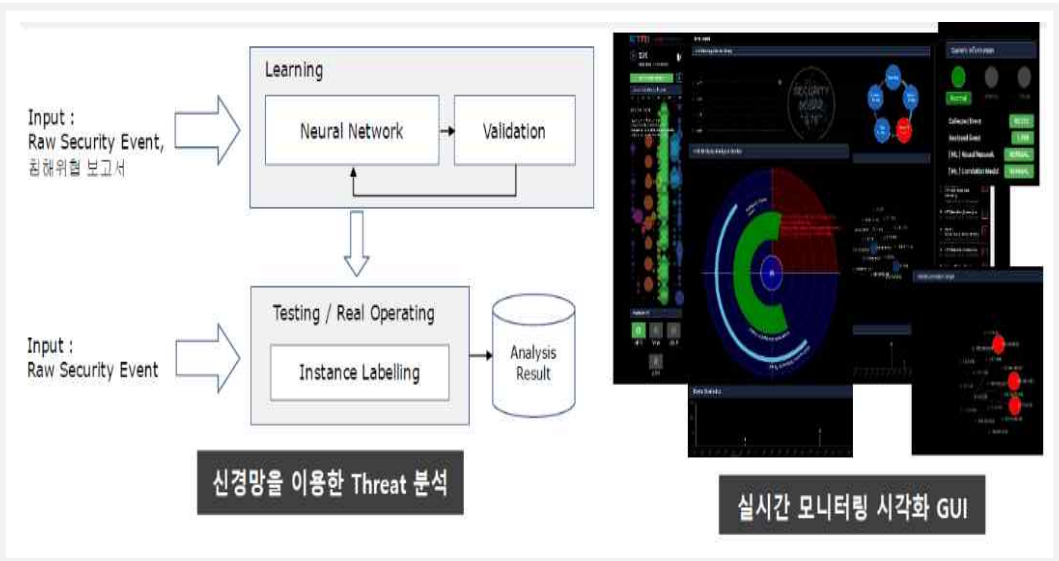
– 보안 이벤트와 로그를 기계학습과 딥러닝 기술을 이용해 학습하고 학습된 모델을 기반으로 정탐 로그를 실시간 분석하여 실시간 침해위협을 탐지하는 기술

기술의 특장점

▪ 실시간 침해위협을 탐지하는 기술

– AI 적용을 위한 데이터 전처리, 딥러닝 기반 학습, 실시간 분석 탐지, 학습모델 관리, 사용자 GUI가 포함된 인공지능 기반 보안 이벤트 학습 및 탐지 기술

– 보안이벤트 데이터 학습, 모델 생성, 실시간 추론을 위한 AI 기반 지능형 분석 기술이 적용된 AI-SIEM 시스템으로, 텐서플로우 기반 인공신경망을 이용한 침해위협 분석 기술



적용분야

▪ 지능형 보안 분석 분야의 SIEM 솔루션 개발 및 SOC를 위한 보안 관제 AI 분야

– 실시간 보안 데이터 처리 자동화, APT 공격 탐지, 네트워크 데이터 분석, 실시간 이벤트 처리 및 분석

– 데이터 마이닝 및 머신 러닝을 통한 인공지능 기반 침해 위협 탐지 솔루션

– 소규모 네트워크를 위한 보안 관제 및 Small 플랫폼형의 AI 보안관제 솔루션

▪ 클라우드 기반 보안 솔루션 분야

– 클라우드 기반 SIEM 확장을 통한 SecaaS 서비스 제공

– 클라우드 기반 맞춤형 보안 서비스 제공

기술완성도 (TRL)

▪ TRL 5단계; 확정된 소재/부품/시스템 시작품 제작 및 성능 평가 단계

기술이전 내용 및 범위

▪ AI SIEM 을 위한 보안 데이터 학습 및 탐지 엔진 기술

- 데이터 처리 및 연관성 분석 위한 K-NN, TF-IDF, 벡터공간모델기반 사전 학습 기술
- DNN, RNN, LSTM 딥러닝 알고리즘 학습 및 실시간 분석 기술
- 지도학습(Supervised Learning) 기반 데이터 학습 및 모델 관리 기술
- 데이터 전처리 및 학습을 위한 사용자 도구
- 기술이전 범위 : 소스 코드, 관련 문서, 특허 3개

▪ AI SIEM 을 위한 사용자 실시간 모니터링 시각화 도구

- 딥러닝 탐지/관리를 위한 웹기반 사용자 GUI 기술
- 딥러닝 학습 및 모델 관리 사용자 GUI
- 기술이전 범위 : 소스 코드, 관련 문서

관련 지재권 현황

No.	출원번호	특허 명	상태
1	2018-0071694	심층 신경망을 이용한 사이버 위협 탐지 방법 및 장치	출원
2	2017-0001183	보안 이벤트의 연관 분석을 통한 사이버 침해 위협 탐지 방법	등록
3	2017-0010978	네트워크 보안 기능 가상화 기반의 클라우드 보안 분석 장치, 보안 정책 관리 장치 및 보안 정책 관리 방법	출원

기술이전 문의

▪ 연구성과확산실 (02-597-1260 / curl@etri.re.kr)