04 지능형 SIEM을 위한 인공신경망 기반 데이터 분석 및 탐지 기술

연구책임자	김종현 PL	소속	초연결통신연구소 지능보안연구그룹

기술 요약

기술 개요	• 네트워크 보안 장비에서 발생되는 대량의 보안 이벤트에 대해 운영자가 수동적으로 분석하여 탐지하는 한계를 극복하기 위한 인공신경망 기반 침해 위협 분석 및 탐지 기술 • 다양한 보안 이벤트에 대한 데이터 전처리 → 연관성을 분석을 통한 사전 학습 → 딥러닝 지도학습 → 모델 생성 → 공격 징후 판단
기술특징	• 데이터 학습, 모델 생성, 실시간 추론을 위한 AI 기반 지능형 분석 기술이 적용된 AI-SIEM 시스템 ✓ 텐서플로우 기반 인공신경망을 이용한 침해 위협 분석 기술 ✓ 데이터 전처리부, 데이터 학습부, 실시간 AI 탐지추론부, 모델 관리부로 구성된 AI-SIEM 시스템 ✓ K-NN, TF-IDF, Vector Space Model 을 통한 사전 학습 알고리즘 제공 ✓ DNN, RNN. LSTM 등 다중 딥러닝 학습 알고리즘 제공 ✓ AI 분석 실시간 모니터링과 모델 및 데이터 관리를 위한 웹기반 AI-SIEM 사용자 응용 제공 ✓ 실환경 IPS Event 80만건에 대한 Supervised Learning 실험 수행
기술완성도	TRL5 – 유사환경 테스트



기술이전 문의	ETRI 사업화협력실 김진경 선임 curl@etri.re.kr, 031)739-7262 김준성 기술원 junsung.kim@etri.re.kr, 031)739-7284