

테크비즈 파트너링 기술분류 + D.N.A.융합산업

029

## 사용자 기반의 보안관제 전용 인공지능 자동화 플랫폼

- + 연구자\_한국과학기술정보연구원\_송중석
- + 기술완성단계\_TRL 7(유사 상용품 개발)
- + Keyword\_인공지능, 사이버보안, APT, 빅데이터, 자동화플랫폼, 데이터모델링

### 지재권현황

권리현황	특허번호	발명의 명칭
출원	PCT/KR2018/015476	인공지능 모델 플랫폼 및 인공지능 모델 플랫폼 운영 방법(PCT)
출원	10-2018-0142166	인공지능 모델 플랫폼 및 인공지능 모델 플랫폼 운영 방법
출원	10-2020-0165605	인공지능 알고리즘 수행방법
출원	10-2020-0163134	보안 이벤트 학습데이터 생성방법
출원	10-2020-0163135	보안 데이터 전처리 장치 및 방법

### 기술성

#### 기존 기술의 문제점

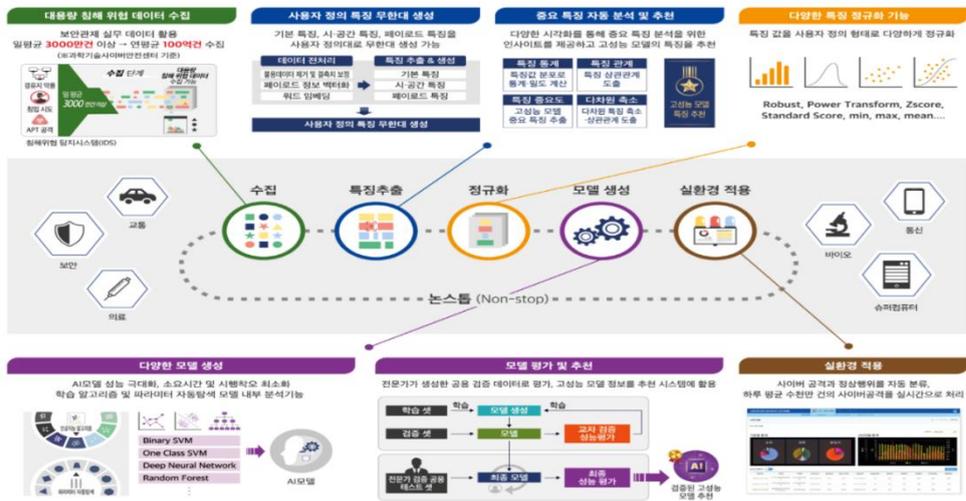
- ▶ 대량의 보안이벤트 수의 증가로 인한 사이버위협 정보를 보안관제 담당자가 수동으로 분석하기 어려운 한계점 존재
- ▶ 기존의 보안관제 서비스는 담당자의 전문지식과 경험에 의존하여 분석결과의 편차, 업무편중 등의 문제점으로 업무능력 향상 저하
- ▶ 따라서, 보안관제 요원의 분석에 의존하는 기본 보안관제 서비스 구조 자체를 혁신할 필요성 증가

#### 기존 기술과의 차별성(기술의 특징점 또는 효과 등)

- ▶ 특징
  - 인공지능 모델 성능에 직결되는 특징정보와 정규화 방식을 최적으로 적용함으로써 비전문가도 단기간에 최적의 인공지능 모델 생성 가능
  - 사용자 정의 상관 특징(시·공간정보 표현 등)을 생성할 수 있는 기능 제공 가능
- ▶ 우수성
  - 하루평균 3000만 건 이상, 연평균 100억 건의 대용량 침해 위협 데이터 수집 가능
  - 사이버공격 등의 비정상 행위와 정상행위 판단에 대해 99.9%의 정확도로 자동분류 할 수 있는 고성능의 인공지능 보안관제 모델 생성 가능
  - 다양한 시각화와 인사이트를 제공하고 고성능 모델의 중요 특징 자동분석 및 추적 가능
  - 기본정보, 시·공간 정보, 그리고 페이로드(전송 데이터) 특징을 사용자 정의에 따라 무한대로 생성 가능

➤ 주요기술구성(상세설명 등)

- ▶ 본 기술은 수집, 특징추출, 정규화, 모델생성, 실제환경 적용 단계로 구성되어 있음
- ▶ 각각의 필드 및 기간 정보 등을 활용하여 데이터를 수집하고 학습데이터를 생성한 후 데이터의 기본정보, 시·공간(통계/상관)정보 등의 다양한 특징을 추출함
- ▶ 이후, 정규화 방법을 통해 특징간 편차를 최소화하고, 인공지능 알고리즘을 자유롭게 선택하여, 다양한 파라미터 조합에 대한 성능평가를 통해 최적의 인공지능 모델을 생성함
- ▶ 마지막으로, 실제 테스트데이터에 기반하여 인공지능 모델에 관한 유효성 및 실효성 평가 후, 실제환경에 적용하여 자동분류 및 사이버공격을 실시간으로 처리할 수 있음



논스톱 인공지능 모델 생성 플랫폼

활용분야

➤ 적용분야 및 적용제품

- ▶ 머신러닝/딥러닝 자동화 플랫폼(차량공유, 금융, 유통, 보험 등 대규모 데이터)
- ▶ 자동화 보안시스템(자동화 보안/사이버 위협 대응 서비스, 신·변종 바이러스 조기 탐지 서비스)

문의처



담당자 심원보 행정원  
 연락처 042-869-0911  
 이메일 wbsim@kisti.re.kr



담당자 조현철 대리  
 연락처 070-4333-8665  
 이메일 hcjo@doohopat.or.kr