140

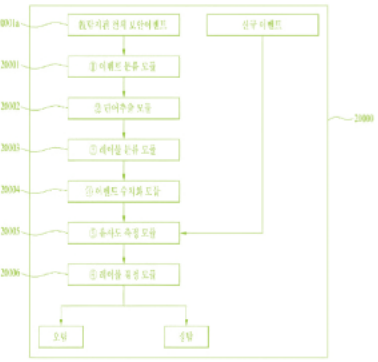
기술 분류_ 사이버보안

인공지능 기반 사이버위협정보 자동분석 기술

01 기술 개요

보안관제 기술 사용에 미숙한 사용자가 최적의 인공지능 모델을 생성할 수 있도록 대량의 원천 데이터를 이용하여 인공지능 모델 개발과 구축까지의 전 과정을 사용자 요구 방식에 따라 논스톱으로 처리할 수 있는 시스템에 관한 기술

- 기존의 보안관제 서비스는 담당자의 전문지식과 경험에 의존하여 분석결과의 편차, 업무 편중 등의 문제점으로 업무능력이 저하하고, 보안 관제 요원의 분석에 의존하는 기본 보안 관제 서비스 구조자체를 혁신할 필요성 증가
- 인공지능 모델 성능에 직결되는 데이터 정제 및 특징 정보 추출 방식을 최적으로 적용함으로써 비전문가도 단시간에 최적의 인공지능 모델 생성 가능



[대표도면]

02 기술 차별성

사이버 공격 등의 비정상행위와 정상 행위 판단에 대해 99.9%의 정확도로 자동 분류할 수 있는 고성능의 인공지능 보안 관제 모델 생성 가능

- 인공지능 모델 개발 프로세서의 전 과정을 자동화하여 고성능 모델을 생성하고 특징 분석을 위한 다양한 솔루션 제공 가능
- 대규모 사이버 공격과 이상행위 발생 징후를 효율적으로 분석하여 인공지능 기반의 침해 대응 체계를 구축 및 원천 기술 확보 가능

다양한 시각화와 인사이트를 제공하고 고성능 모델의 중요 특징 자동 분석 및 추적 가능

- 사용자 정의 상관 특징(시공간 정보 표현 등)을 생성할 수 있는 기능 제공 가능
- 하루평균2000만건이상,연평균100억건의대용량침해위협데이터수집가능
- 기본정보,시·공간정보,그리고페이로드(전송데이터)특징을사용자정의에따라무한대로생성가능

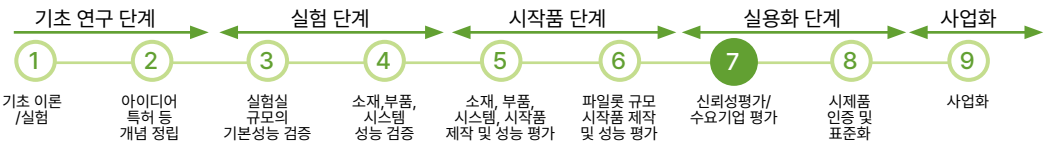
본 기술은 수집, 특징추출, 정규화, 모델생성, 실제환경적용 단계로 구성되어 있음

- 각각의 필드 및 기간정보등을 활용하여 데이터를 수집하고 학습 데이터를 생성한 후 데이터의 기본정보, 시·공간(통계/상관)정보 등의 다양한 특징을 추출함
- 이후, 정규화 방법을 통해 특징 간 편차를 최소화하고, 인공지능 알고리즘을 자유롭게 선택하여, 다양한 파라미터조합에 대한 성능 평가를 통해 최적의 인공지능 모델을 생성함
- 실제 테스트 데이터에 기반하여 인공지능 모델에 관한 유효성 및 실효성 평가 후, 실제 환경에 적용하여 자동분류 및 사이버공격을 실시간으로 처리할 수 있음

03 기술 키워드

사이버보안, APT, 실시간 분석

04 기술의 TRL 단계



140

기술 분류_ 사이버보안

인공지능 기반 사이버위협정보 자동분석 기술

05 사업화 포인트

인공지능은 기술의 발전과 변화속도가 매우 빠르고, 기술완성도가 7단계(유사 상용품 개발)이기 때문에 기업 및 시장 환경에 맞는 최적화를 통한 상용품 제작 후 신속한 시장 진입 전략 수립 필요

06 활용 분야 및 시장 규모

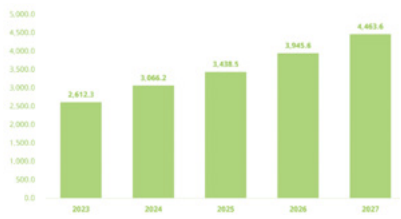
활용 분야

보안관제, 사어버보안

시장 규모 및 전망

국내 AI 시장이 2023년에는 전년 대비 17.2% 성장해 2조 6,123억 원에 이를 것으로 예상되며, 향후 5년간 CAGR 14.9%를 기록하며 2027년까지 4조 4,636억 원 규모에 이를 것으로 전망됨

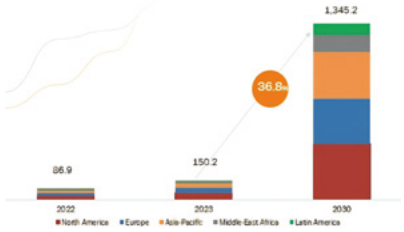
[국내 인공지능(AI) 시장 전망 (단위: 십억 원)]



(출처: 한국IDC, 국내 인공지능 분석 시장 전망, 2023-2027)

세계 AI 시장은 2023년 1,502억 달러로 평가되었으며, 2023~2030년 동안 CAGR 36.8%로 성장할 것으로 예상되어 2030년에는 1조 3,452억 달러에 이를 것으로 전망됨

[세계 인공지능(AI) 시장규모]



(출처: Marketsandmarkets, Artificial Intelligence Market, 2023)

07 지식재산권 현황

권리현황

특허명	보안 이벤트 학습데이터 생성 방법 및 보안 이벤트 학습데이터 생성 장치
출원번호	10-2020-0163134
권리자	한국과학기술정보연구원
관리기관	한국과학기술정보연구원
담당자	주용하
문의처	042-869-0977