지능형 보안 체계 수립을 위한
국내 최초 AI 보안관제 솔루션

spiderAI

IGLOO

Background

인공지능(AI) 기술, 기대만큼 잘 활용하고 계십니까?

디지털 트랜스포메이션이 가속화됨에 따라 기존의 방어 체계로는 예측하기 어려운 복합적인 사이버 공격이 증가하고 있습니다.
오늘날의 보안 조직은 보안 위협을 보다 정확히 분석하고 또 보안 사고에 기민하게 대응해야 한다는 중요한 역할을 맡게 되었지만,
진화하는 공격에 발맞춰 늘어나는 보안 장비와 기하급수적으로 쌓이는 경보는 사람이 처리할 수 있는 한계를 넘어섰습니다.

한정된 인력과 예산으로 조직을 보호하기 위해 단순 소모적인 업무 절감, 위협 수준에 맞는 명확한 보안 이벤트 대응 등
'보안 지능화'의 필요성이 높아졌고, AI는 이를 구현하기 위한 핵심 기술 중 하나로 자리 잡게 되었습니다.

AI의 진정한 가치는 AI 알고리즘과 함께 AI 알고리즘이 잘 학습할 수 있는 양질의 학습 데이터가 있을 때 비로소 구현할 수 있습니다.
하지만 현실적으로는 AI 알고리즘이 학습할 수 있는 데이터가 너무 부족한 상태일 뿐만 아니라
이러한 데이터를 보안 목적에 맞추어 학습 데이터로 가공할 수 있는 데이터 사이언티스트를 확보하기 어렵습니다.
오늘날 대부분의 AI가 예측 결과에 대한 근거 데이터 및 이유를 제시하지 못하는 이른바 '블랙박스' 형태라는 점 역시
책임 추적과 판단 근거가 중요한 보안 분야에서 지적되는 사항 중 하나입니다.

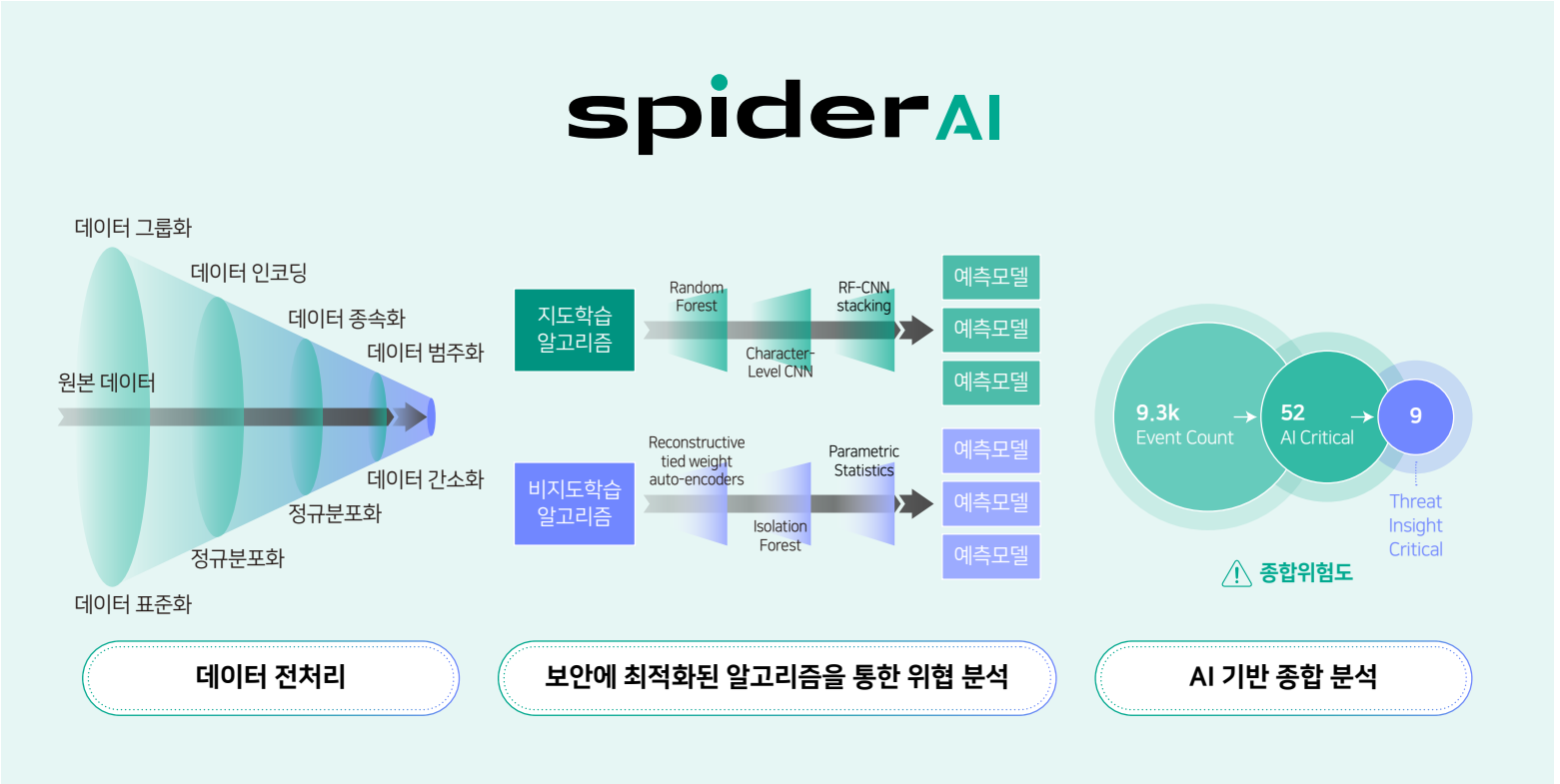
AI 예측 결과에 대한 정확도와 신뢰도를 높여
실질적인 성과를 낼 수 있는 AI 보안 솔루션이 필요합니다.

Overview

스파이더 티엠 에이아이 에디션(SPiDER TM AI Edition)은
이글루코퍼레이션 고유의 AI 및 보안 역량이 집약된 보안 특화 AI 알고리즘과 데이터를 토대로,
고도화된 사이버 공격에 대한 대응력을 한 단계 높여주는 AI 보안관제 솔루션입니다.

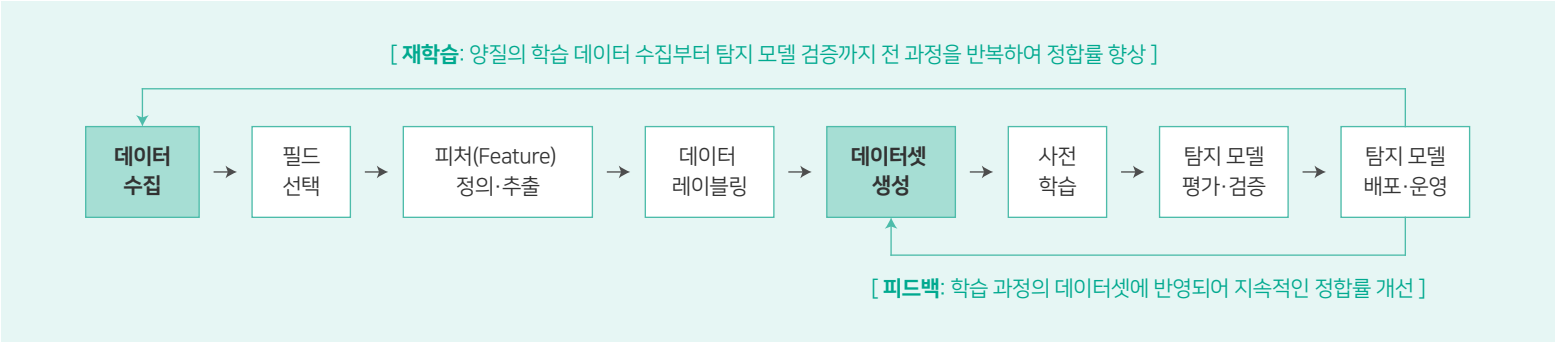
정상·비정상 이벤트에 대한 지도 학습과 이상 행위·공격자 특성 등에 대한 비지도 학습을 거친 AI 알고리즘을 기반으로
사용자는 알려진 위협에 대한 탐지·대응시간을 단축시키고, 알려지지 않은 위협에 대한 가시성을 높일 수 있습니다.

SPiDER TM AI Edition을 통해 방대한 보안 데이터 분석의 어려움을 해소하고,
걸러진 핵심 정보와 고위험 이벤트에 집중하면서 상향된 대응 체계를 구현하세요.



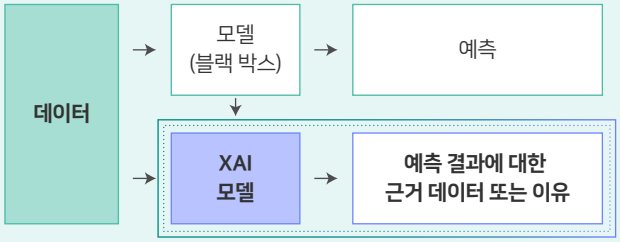
Why SPiDER TM AI Edition

AI 정확도를 높이는, 보안 특화 데이터셋



이글루코퍼레이션은 다년간의 보안 노하우와 AI 솔루션 구축·운영 역량을 토대로 보안에 최적화된 AI 데이터셋을 구축해 탐지 모델의 정확성을 높였습니다. 양질의 데이터를 학습해야 예측 결과의 수준도 높아질 수 있습니다. 이글루코퍼레이션은 전담 조직 운영을 통해, 원시데이터에서 학습 데이터를 선별해 추출·분석·가공하는 전처리 및 학습 방향을 정하는 레이블링 작업 등을 수행하며 학습 데이터의 품질을 지속적으로 고도화하고 있습니다. 또한 이러한 보안 경험에 기반하여 구축된 학습 데이터와 탐지 모델은 솔루션 구축 및 운영 시 투입되는 전문 인력을 최소화하는 효과도 제공해 줍니다.

AI 신뢰도를 높이는, 설명 가능한 AI (eXplainable AI)

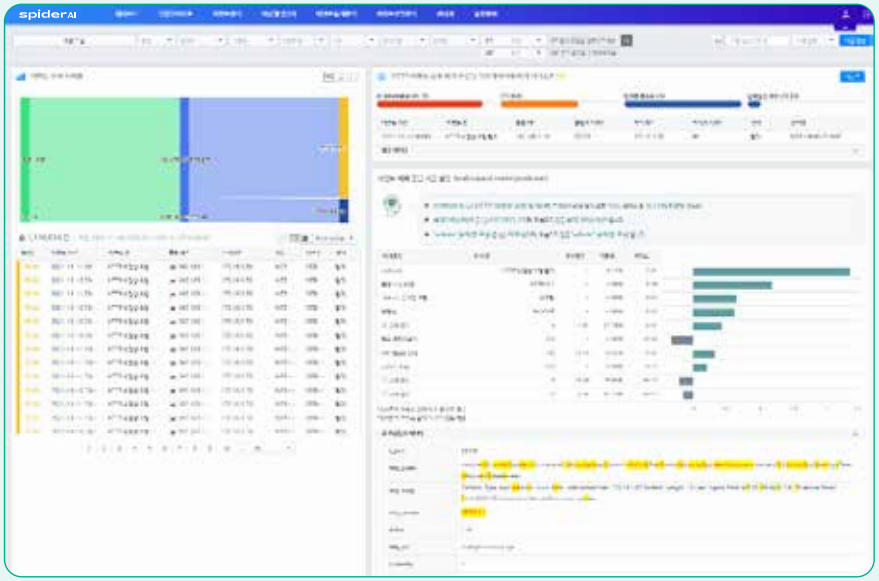


이글루코퍼레이션은 AI가 내린 예측에 대한 근거를 제시하는 '설명 가능한 AI(XAI, eXplainable AI)' 기술을 적용해 AI 알고리즘의 신뢰성을 높였습니다. AI 기술을 토대로 고위험 이벤트를 빠르게 선별하는 것에서 더 나아가 AI 알고리즘이 왜 이 이벤트를 고위험 이벤트라고 판단했는지, 결과의 도출 과정을 이해할 수 있도록 알려줌으로써 보안 전문가는 AI가 의도한 대로 잘 학습되었는지 또 신뢰할 만한 예측 결과가 도출되었는지를 판단할 수 있습니다. 그리고 이와 같이 결과에 대한 이해와 해석은 학습 모델의 편향(bias) 등을 비롯한 예측 성능의 문제를 파악할 수 있도록 도와줘 궁극적으로는 최적의 학습 모델과 학습 데이터셋 도출하고, AI 탐지 모델의 성능을 향상시킬 수 있습니다.

Features

머신러닝 알고리즘 학습을 위하여 220개 이상의 피처(Feature)와 80개 이상의 위협 탐지 모델을 적용할 수 있습니다.
사용자들은 경보 분석과 이상행위 탐지를 통해 도출된 위협 요소를 통합적으로 분석함으로써,
보안 위협에 대한 높은 가시성을 확보할 수 있습니다.

경보 분석



이벤트 예측 판단 기준 설명

AI 예측 결과에 대해 4가지 측정 지수 표현
· AI Score, CTI, 탐지명 중요도, 불확실성 지수

XAI 기반 이벤트 예측 판단 기준 설명
· 예측 기여도 상위 피처에 대한 설명
· 피처 별 설명, 값, 기여도, 학습 데이터 대비 백분위 제공

AI 주요 탐지 데이터
· 예측 기여도 상위 피처를 페이로드(Payload)와 비교해 하이라이트하여 분석

지도 학습을 통해 심각도와 예측률을 기반으로 한 이벤트 분석 기능 제공

보안정보 및 이벤트 관리(SIEM) 솔루션에서 수집된 경보 및 이벤트를 심각도와 예측 신뢰도를 기반으로 분석해 방대한 보안 이벤트 중 우선 처리해야 할 고위험 이벤트를 빠르게 선별해냄으로써 분석 효율성 및 정확도를 높여줍니다.

XAI 엔진 기술을 활용하여 모델 및 예측 결과에 대한 근거 제공

설명 가능한 인공지능(XAI) 기술을 적용하여 모델 및 예측 결과에 대한 근거를 제공함으로써 사용자에게 더욱 신뢰도 있는 결과를 제시, AI 모델 관점에서의 예측과 보안 전문가 입장 간의 간극(GAP)을 줄여줍니다.

Features

이상 행위 탐지

이상 행위 탐지 시각화

비지도 학습을 통한 이상 행위 탐지 기능 제공

- 이상 행위·공격자 특성 등 양질의 학습 데이터를 통해 검증된 이상치 탐지 알고리즘을 활용해 심각한 위협으로 발전할 수 있는 이상행위를 선제적으로 판별함으로써, 미탐을 최소화하고 복합적인 위협에 대한 폭넓은 가시성을 확보할 수 있습니다.
- 또한 그 결과를 시각화하여 표현함으로써 사용자가 이상치를 더욱 직관적으로 인지하고 신속한 의사결정을 내릴 수 있도록 지원합니다.

위협 인사이트

시계열 및 공격 단계(Cyber Kill Chain) 분석

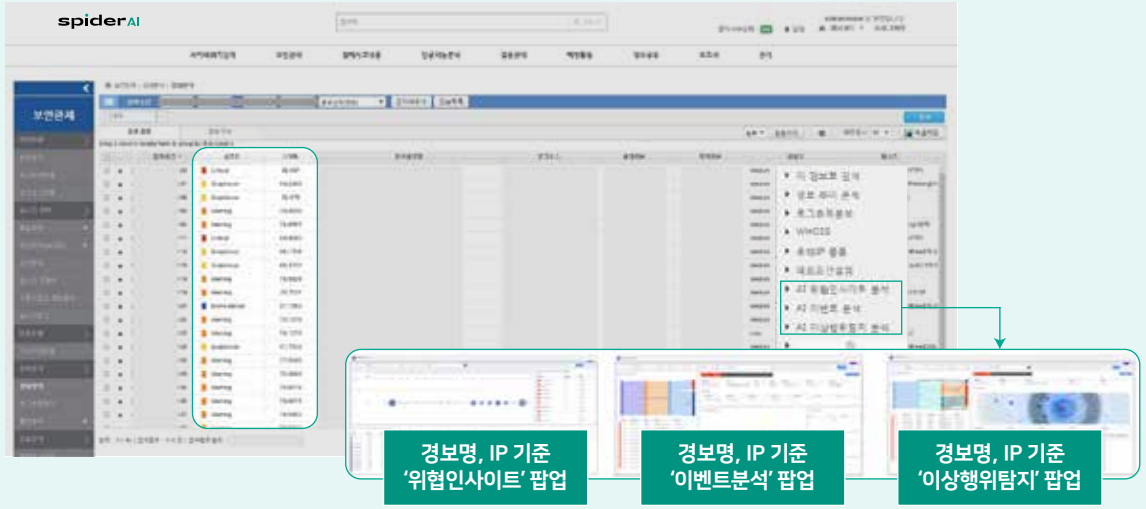
지도/비지도 학습 결과를 종합한 위협 인사이트 제공

- 경보 분석 및 이상 행위 탐지 결과를 기반으로 사용자 중심의 종합 위험도를 제공합니다.
- 시계열 분석, 공격 단계(Cyber Kill Chain) 분석 등 다양한 형태의 연계 분석을 지원함으로써 더욱 심층적이고 종합적인 위협 인사이트를 제시해 줍니다.

Features

기존 솔루션과의 유기적 연동이 가능한 AI 기반 보안관제 플랫폼입니다.
보안 환경의 면밀한 분석을 기반으로 연계가 유연한 플랫폼 기술을 적용하여
유기적인 보안 관리 및 운영을 통한 통합적인 보안 체계 구현이 가능합니다.

솔루션 연동 및 플랫폼 관리



솔루션 연동 기능 제공

· AI 분석 결과를 기존 보안 정보 및 이벤트 관리(SIEM) 솔루션과 연계하여 위험도를 통합 화면으로 제공함으로써 보다 효율적인 보안관제 운영을 지원합니다.
· 이글루코퍼레이션의 SPiDER TM, IGLOO CTI, Smart[Guard] 등과의 손쉬운 연동을 통해 빅데이터 + AI + 위협 인텔리전스 + 자산 및 취약점 정보를 모두 아우르는 통합적인 보안관제 체계 구축이 가능합니다.

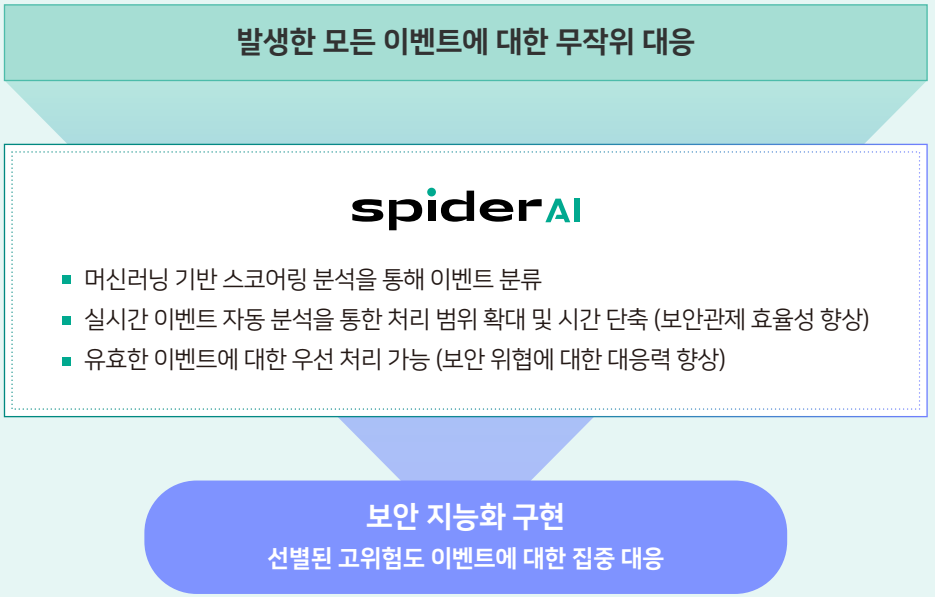
인공지능 플랫폼 관리 기능 제공

· 플랫폼에서 동작하는 수집, 전처리, 위협 모델(지도/비지도: 이벤트 분석, 이상행위 탐지) 전반에 대한 사용자의 손쉬운 관리가 가능합니다.

Benefits

SPiDER TM AI Edition은 보안 분야에 최적화된 AI 기술을 바탕으로 보안 지능화를 구현합니다.

고도화된 보안 위협을 보다 정확히 탐지하고, 방대한 보안 데이터 분석에 소요되는 시간을 단축시킴으로써
보안관제 역량을 상향 평준화시키는 데 중점을 두고 있습니다.



1999년 보안 벤처 기업으로 시작한 이글루코퍼레이션은 국내 최초 보안 정보 및 이벤트 관리(SIEM) 솔루션을 시작으로 수많은 정보보호 핵심 중추 기관과 기업에 보안 솔루션 및 서비스를 제공하며 정보보안 시장의 성장을 이끌어왔습니다. 또한, 디지털 전환 시대 흐름에 맞는 꾸준한 기술 고도화 및 미래 기술 준비를 통해 사업 영역을 확장해 나가며 보안을 넘어 인공지능, 클라우드, 빅데이터 분야를 아우르는 종합 IT 기업으로 성장했습니다. 이글루코퍼레이션은 세계의 고객에게 고유의 보안과 데이터 역량에 기반한 최적의 솔루션, 서비스를 제공하며 급변하는 비즈니스 환경에 최적화된 혁신적인 디지털 경험을 선사하는 기업으로 나아가고자 합니다.

서울특별시 송파구 정의로8길 7 한스빌딩 6층 | TEL 02-3452-8814 | FAX 02-3452-8815 | www.igloo.co.kr

IGLOO