IGLOOSECURITY

AI BASED SECURITY INFORMATION &
EVENT MANAGEMENT

SPiDER TM AI Edition

왜 AI를 보안에 적용해야 하는가

방어자가 막아내야 할 보안 위협 급증, 하루가 다르게 새로운 보안 위협 출현 - 정확한 위협 분석, 빠른 사고 대응에 초점을 둔 AI 기술 도입 요구돼

기업의 생산성을 높이기 위한 디지털 전환에 발맞춰, 지금까지 방어자가 경험하지 못했던 지능적인 사이버 공격이 증가하고 있습니다. 오늘날의 사이버 공격자들은 '적대적 머신 러닝'을 토대로 기존의 방어 기법을 우회하여 시스템에 침투하거나, 수많은 사용자 - 기기 - 시스템이 연결된 디지털 환경의 보안 취약점을 파고드는 등 방어자가 예측하기 어려운 형태의 신·변종 사이버 공격을 감행하고 있습니다.

이에 맞서는 오늘날의 방어자들은 지능화된 보안 위협을 정확하게 분석하고 또 보안 사고에 빠르게 대응해야 한다는 중요한 역할을 맡고 있습니다. 하지만, 날로 진화하는 보안 위협과 기하급수적으로 쌓이는 보안 정보 속에서 이 모든 것을 해내기란 쉬운 일이 아닙니다. 기하급수적으로 생성되는 보안 정보를 쉬지 않고 연계 분석할 수 있는 숙련된 전문 인력, 시간, 자원이 절대적으로 부족하기 때문입니다.

이에, 보안업계에서는 인간보다 기계가 더 잘할 수 있는 분야는 AI 기술을 이용해 최대한 자동화시킴으로써, 빠르게 증가하는 복합적인 사이버 위협에 대한 리스크를 낮추려는 시도가 증가하고 있습니다. 방대한 보안 데이터를 장기간 연계 분석해 온 인간의 경험과 지식을 기계가 학습하게 함으로써, 새로운 유형의 보안 위협을 보다 효율적으로 분석하고 이에 기민하게 대응하기 위함입니다.

특히, 사고 예방 및 보안 위협 탐지·대응 분야에 AI 기술을 적용하고자 하는 움직임이 가속화되고 있습니다. 방대한 보안 이벤트 분석을 자동화하여 걸러진 핵심 정보만 집중적으로 분석하고, 룰·시그니처 기반 시스템으로는 탐지하기 어려운 고도화된 보안 위협을 보다 정확하게 찾아낼 수 있기 때문입니다.

미 탐지 위협 최소화

- 최신 위협 탐지
- 알려지지 않은 위협 행위 탐지
- 장기간에 걸쳐 진행되는 지속형 공격 탐지
- 오탐 및 미처리 경보 감소

신속한 위협 탐지

- 경보 분석 기술 학습 및 축적
- 분석 시간 단축
- 공격 차단 자동화

위협 대응 시간 단축

- 위협 식별의 스피드화
- 취약점 연관 대응
- 위협과 취약점 실시간 연관분석

어떻게 AI를 보안관제에 활용할 것인가

방어자들이 들여다보아야 할 정보의 양은 기하급수적으로 증가하고 있으나, 이 이벤트를 모두 분석하기 위한 전문 인력, 시간, 자원은 절대적으로 부족한 상황 - 한정된 시간과 자원 내 방대한 보안 데이터를 신속하고 정확하게 분석할 수 있는 AI 기반 보안관제시스템 필요

보안관제는 AI 기술이 적용될 시 높은 효과가 기대되는 분야 중 하나입니다. 오늘날 보안 전문가들은 보안 이벤트 증가와 함께 늘어나고 있는 오탐(false positive) 과 미탐(false negative) 경보를 한정된 시간 속에서 정확히 가려내야 한다는 막중한 부담에 직면하고 있습니다. 이글루시큐리티 자체 조사에 따르면, 하루 2만 건이 넘게 발생하는 보안 이벤트 중 분석하지 못한 미처리 경보는 44%, 분석한 이벤트 중 위협으로 잘못 간주한 오탐 경보는 72%에 달하는 것으로 나타났습니다.

AI 기반 보안관제시스템 기대 효과

AI 기반 보안관제시스템 구축을 통해 얻을 수 있는 기대 효과는 무엇인가

우선적으로, 매일 새롭게 생성되는 방대한 보안 이벤트 분석을 자동화함으로써, 보안 업무의 효율성을 높일 수 있습니다. 우선 처리해야 할 고위험 이벤트를 선별함으로써 방대한 보안 데이터 분석에서 소요되는 시간을 단축해 보다 빠른 대응이 가능해집니다.

AI 알고리즘에 적용할 학습 데이터를 생성하고 AI 시스템에 내린 결과에 피드백을 주는 과정을 반복함으로써 예측의 정확성을 끌어올릴 수 있습니다.

예를 들어, 기존 상태에서 약간의 변화만 있는 신·변종 악성코드의 경우, 이전에는 보안 관리자가 일일이 보안 이벤트를 분석해 처리해야 했습니다. 하지만, 방대한 데이터를 학습한 AI 시스템을 구축하여 단순한 공격은 자동 처리하게 하고 보안 담당자는 고위험군 이벤트 분석에 집중한다면, 데이터 분석의 정탐률과 이벤트 처리 효율성을 비약적으로 높일 수 있게 될 것입니다.

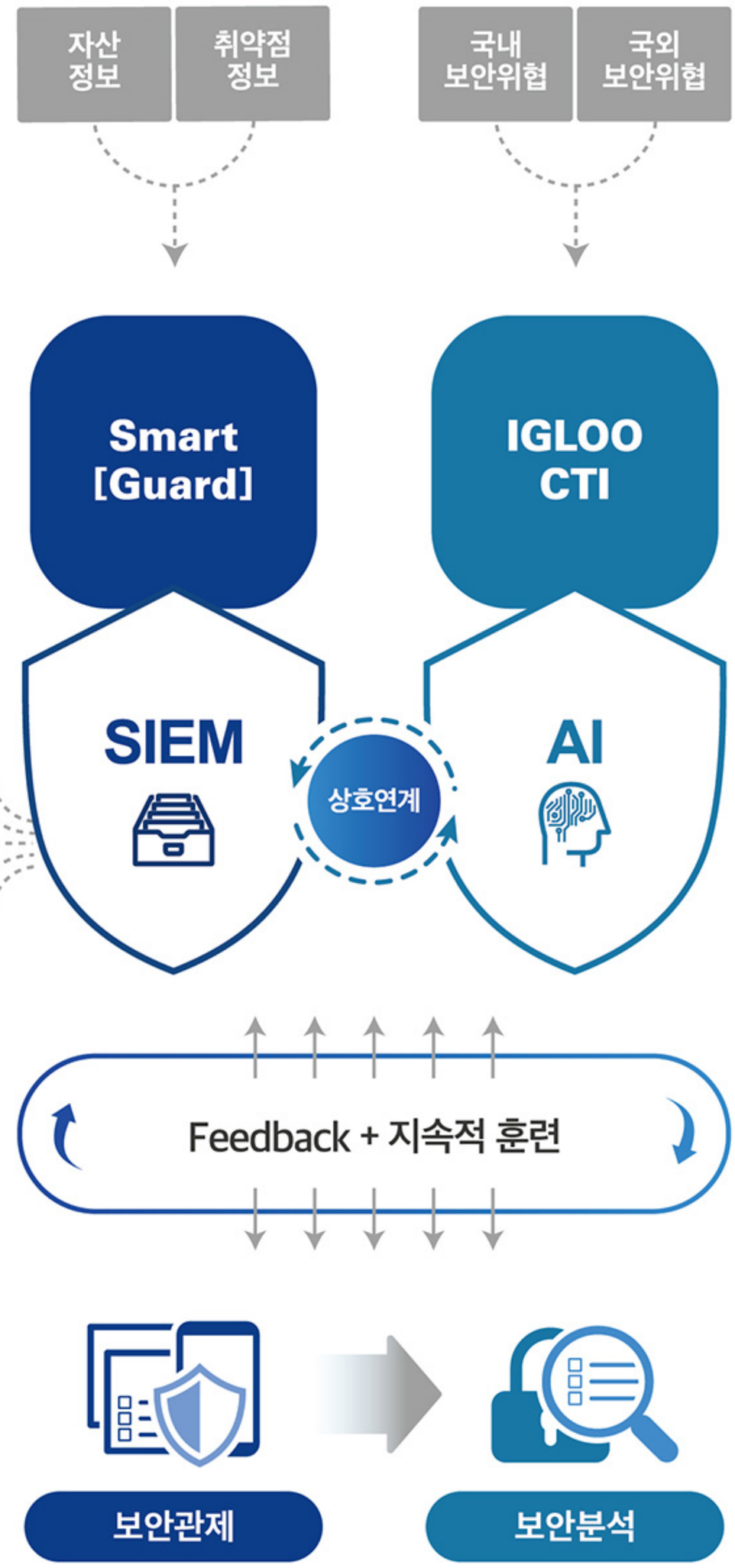
더불어, 장기간 축적된 보안 데이터를 AI 알고리즘을 통해 분석함으로써, 날로 진화하는 고도화된 보안 위협을 보다 빠르고 정확하게 탐지하고 위협 대응에 소요되는 시간을 단축시킬 수 있습니다. 공격자들이 장기간에 걸쳐 기업 내부 시스템들을 교묘히 옮겨 다니며 공격하는 만큼, 단기간 수집된 보안 데이터 분석만으로는 공격자의 행위를 정확하고 빠르게 탐지하기 어려웠던 것이 사실입니다.

머신러닝 기반의 AI 알고리즘을 통해 보안 데이터, 최신 위협 정보, 취약점 등 관련된 정보를 신속하게 연관 분석함으로써, 기업 전반을 아우르는 폭넓은 가시성을 확보할 수 있게 됩니다. 또한, 악의적 행위·공격자 특성 등이 담긴 양질의 학습 데이터에 대한 비지도 학습을 통해 심각한 위협으로 발전할 수 있는 알려지지 않은 변칙 활동 및 이상행위를 보다 빨리 식별할 수 있게 됩니다.

인공지능 통합보안관제 솔루션

SPiDER TM AI Edition

기하급수적으로 증가하는 고도화된 보안 위협에 맞서기 위해서는 인공지능 기반의 통합보안관제 솔루션이 필요합니다.



SPiDER TM AI Edition은

1. 이기종의 보안 장비에서 생성되는 방대한 로그를 수집·분석하는 '빅데이터 기반 보안관제 시스템(SIEM)'
2. 글로벌 최신 위협 정보를 실시간 수집·공유하는 '사이버 위협정보 공유시스템(IGLOO CTI)'
3. IT 자산 관리와 취약점 진단·조치 기능을 통합적으로 지원하는 '보안 취약점 자동진단 솔루션 Smart[Guard]'
4. 위협 정보에 대한 지속적인 학습을 통해 공격을 탐지·예측하는 '머신러닝 기반 AI 시스템'과 상호 연계되는 형태로 구성됩니다.

우수한 인공지능 설계

실시간 침해대응 학습이 가능하도록 데이터 수집 부터 데이터 모델 평가까지 검증된 기술을 적용 하였습니다.

고급두뇌형 시스템 구축

최적의 위협 및 예측모델을 개발하기 위해 최고의 보안 분석 전문가가 참여하였으며 최적의 학습 알고리즘을 적용하였습니다.

철저한 지능검증

학습데이터에 편향되지 않도록 검증하는 기법인 K겹 교차 검증을 사용하여 지속해서 학습과정을 개선합니다.

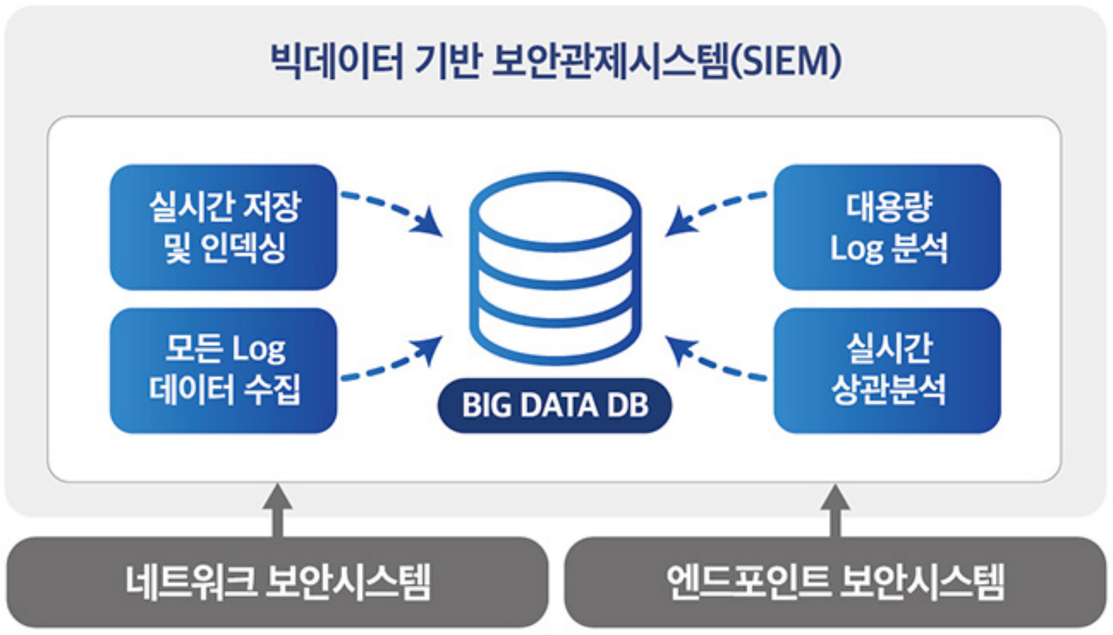
지능형 보안관제 체계

IGLOO CTI 및 취약점 자동진단 시스템과 연동 되어 종합위험도 분석을 통한 지능형 보안관제 체계를 구현합니다.

SPiDER TM AI Edition

위협의 식별 및 평가부터 대응까지 위험성을 실시간 연간 분석하는 오케스트레이션

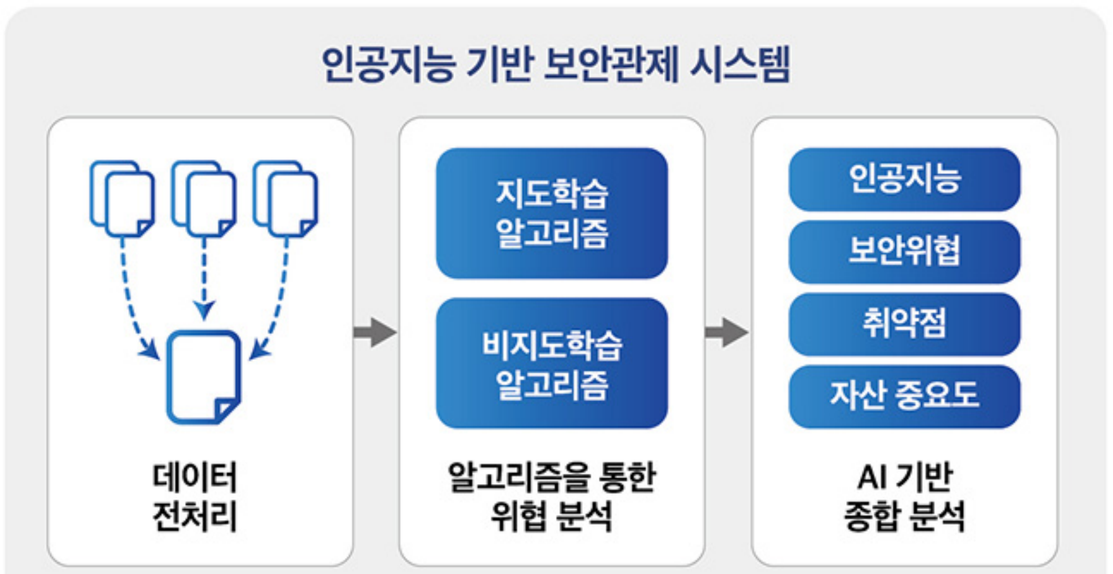
기하급수적으로 증가하는 신종 사이버 보안 위협 분석, 위협에 대한 정확성 및 예측 그리고 반복적으로 발생하는 IT 인프라의 자산 변동 및 보안 취약점을 통합적으로 관리하는 인공지능기반의 SIEM 솔루션



빅데이터 기반의 보안관제 (SIEM) 1

다양한 보안시스템과 내부 자산들의 로그를 수집하여
위협상황의 실시간 식별 및 분석이 가능한
보안관제 솔루션 SPiDER TM

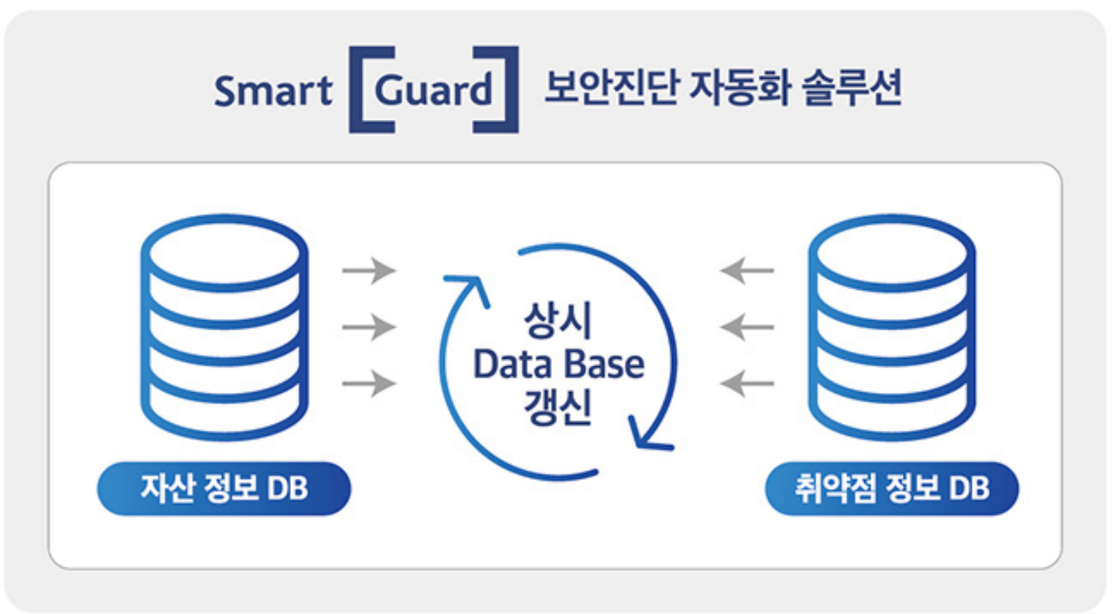
- 구축된 모든 보안시스템 및 주요 서버에 대한 로그를 수집하고, 이를 통해 위협에 대한 상관분석을 수행
- 실제 위협 발생 시, 사고 처리 프로세스를 통해 보안관제 업무 수행 - 보안관제센터에서 가장 기본이 되는 보안관제 시스템



머신러닝 기반의 인공지능(AI) 시스템 2

인공지능(AI) 기술을 접목한 지능형 보안관제체계를 통해
관제 효율성 극대화 및 정보 인프라 자기방어 능력 강화

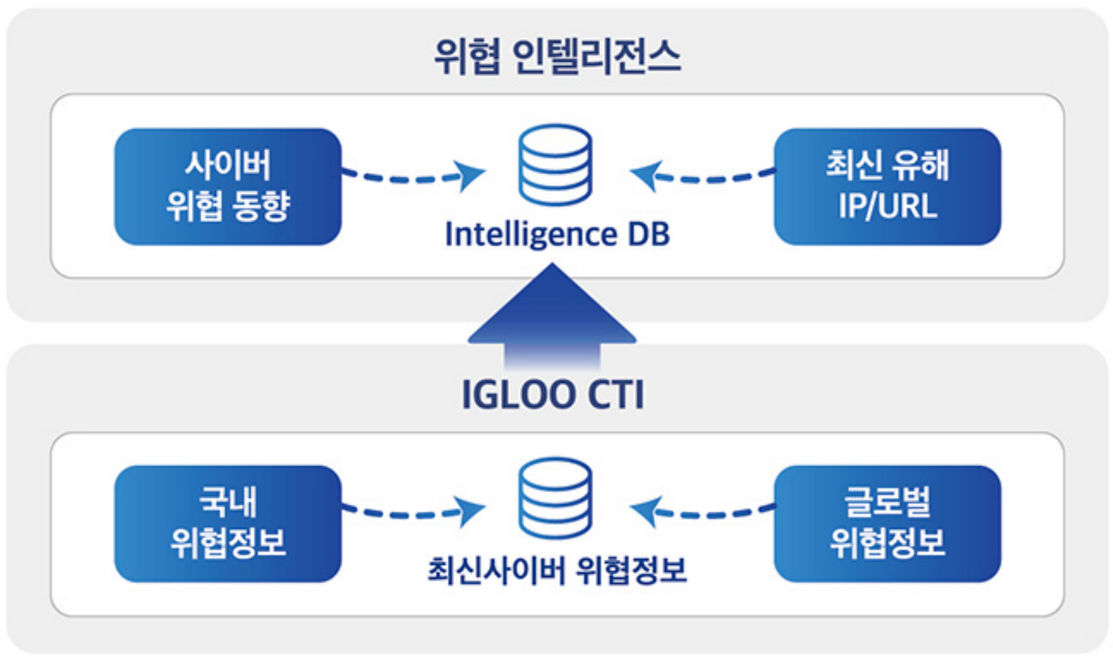
- 머신러닝 기반의 지도 학습을 통해 고 위험도 이벤트에 대한 집중 분석
- 실시간 침해 이벤트 자동 분석을 통한 처리 범위 확대 및 시간 단축
- 비지도 학습에 의한 데이터 학습을 통해 알려지지 않은 위협 탐지



이글루시큐리티 보안진단 자동화 솔루션과의 연동 3

실시간 취약점 관리·침해요인 제거를 통한 사이버 위협요인을
사전에 해소하는 보안진단 자동화 솔루션 Smart[Guard]

- S/W 중심의 IT 자산 관리 + 보안취약점 자동 진단 →
  One Pack 솔루션 - 하나의 솔루션으로 보안관점의 OS, S/W (DB, Web, WAS, App. 등) 정보 관리 및 취약점 진단
- 자산 및 취약점 정보 자동조회를 통한 침해대응 및 위험관리



사이버 위협 정보 공유 시스템 IGLOO Cyber Threat Intelligence 4

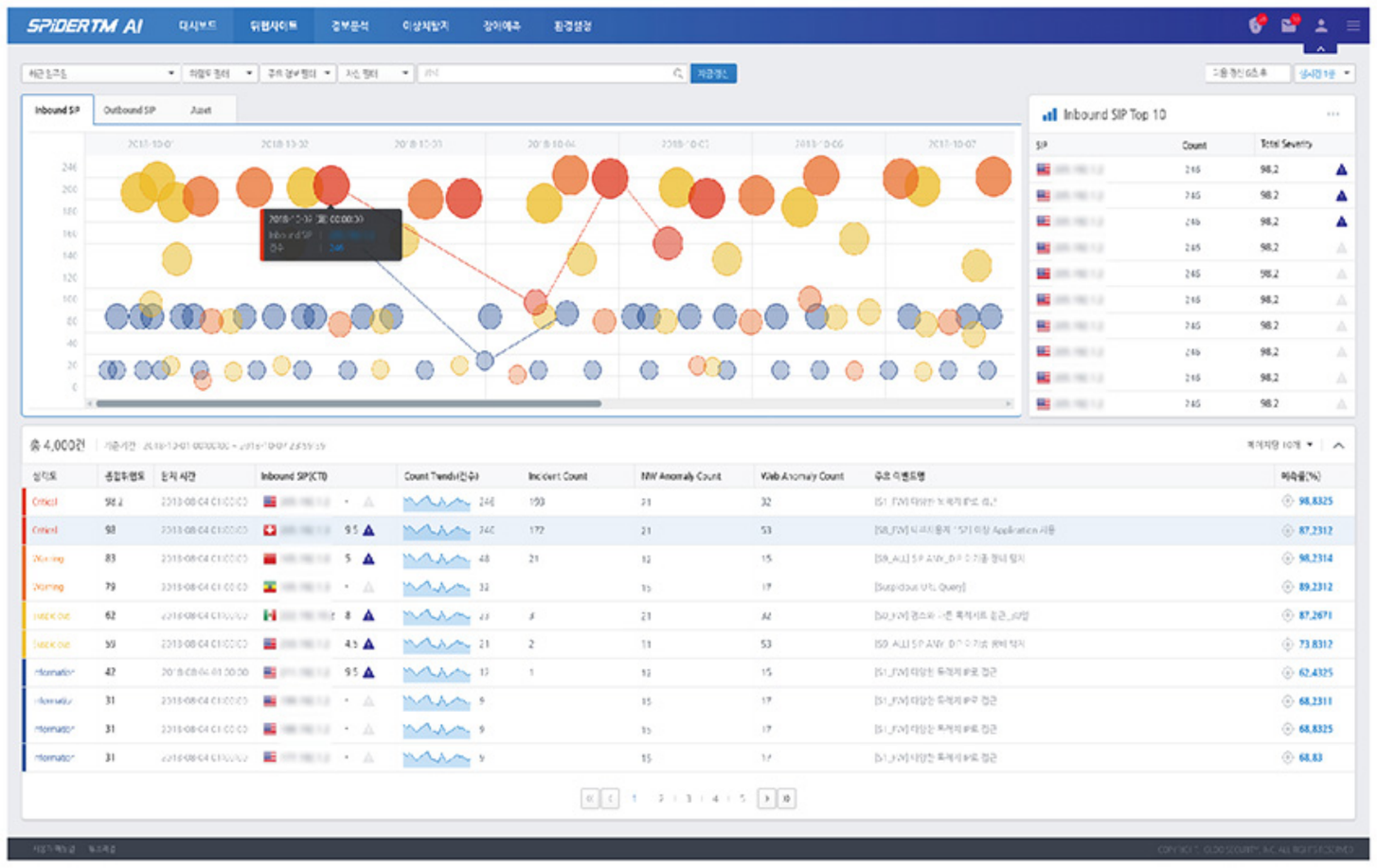
사이버 위협 사전 예방 및 신속한 식별을 위한
글로벌 위협 인텔리전스 정보를 제공

- IGLOO CTI는 국내외 위협정보 및 자체 보안관제센터에서 수집된 각종 위협정보를 DB화하고 보안관제시스템과의 자동 연계를 통해 최신 사이버 위협 예방 체계 구축

신속하고 정확한 위협식별

위협 인사이트
Threat Insight

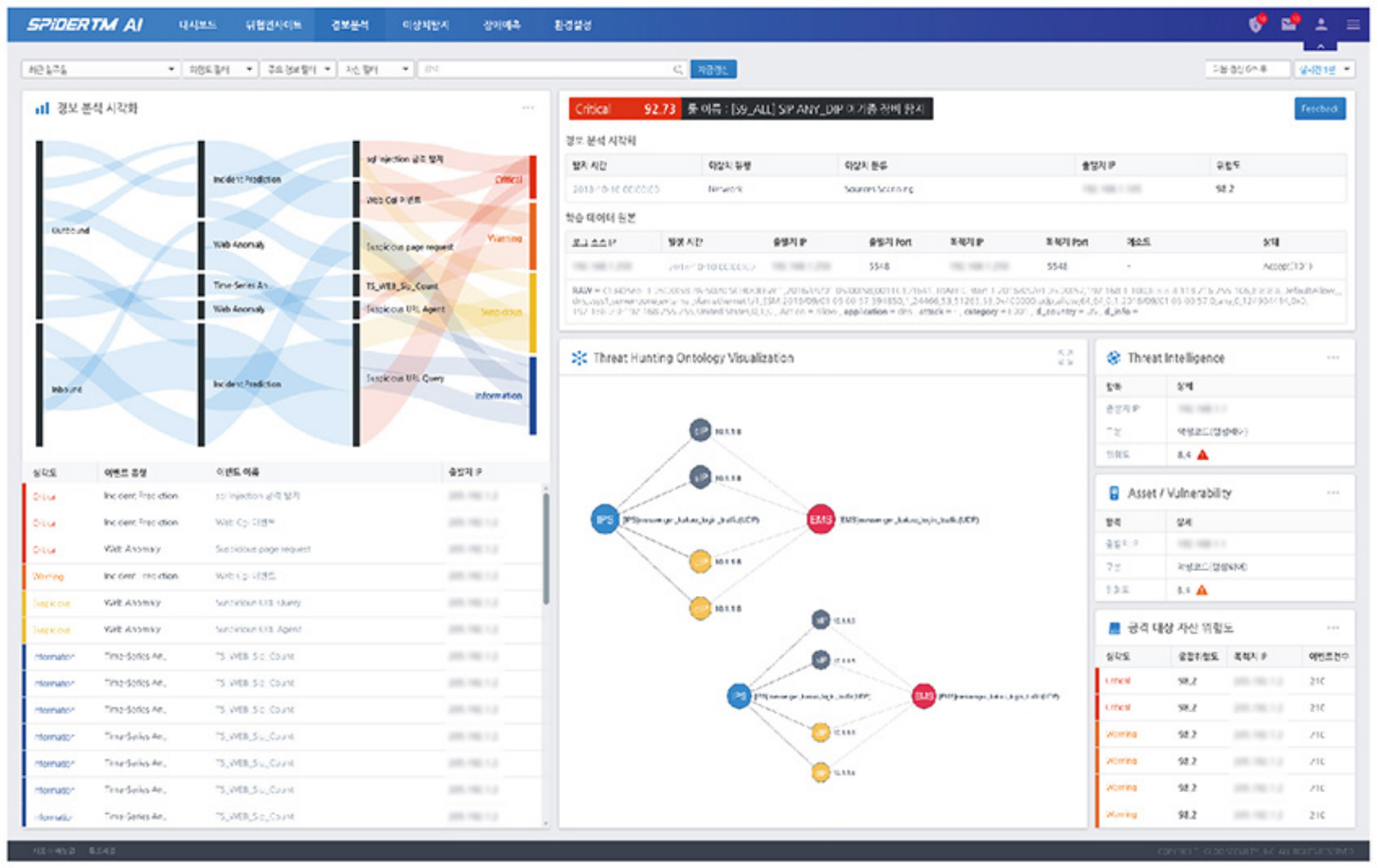
경보 이벤트 및 이상행위 이벤트의 학습을 종합적으로 분석하여 보안관리자에게 위협 인사이트를 제공합니다. 제공되는 분석으로는 위협에 대한 이벤트 시계열 분석, Kill chain 기반의 위협분석, 시계열 및 산키 차트 등이 있습니다.



관제효율성 향상

경보 분석
Incident Analysis

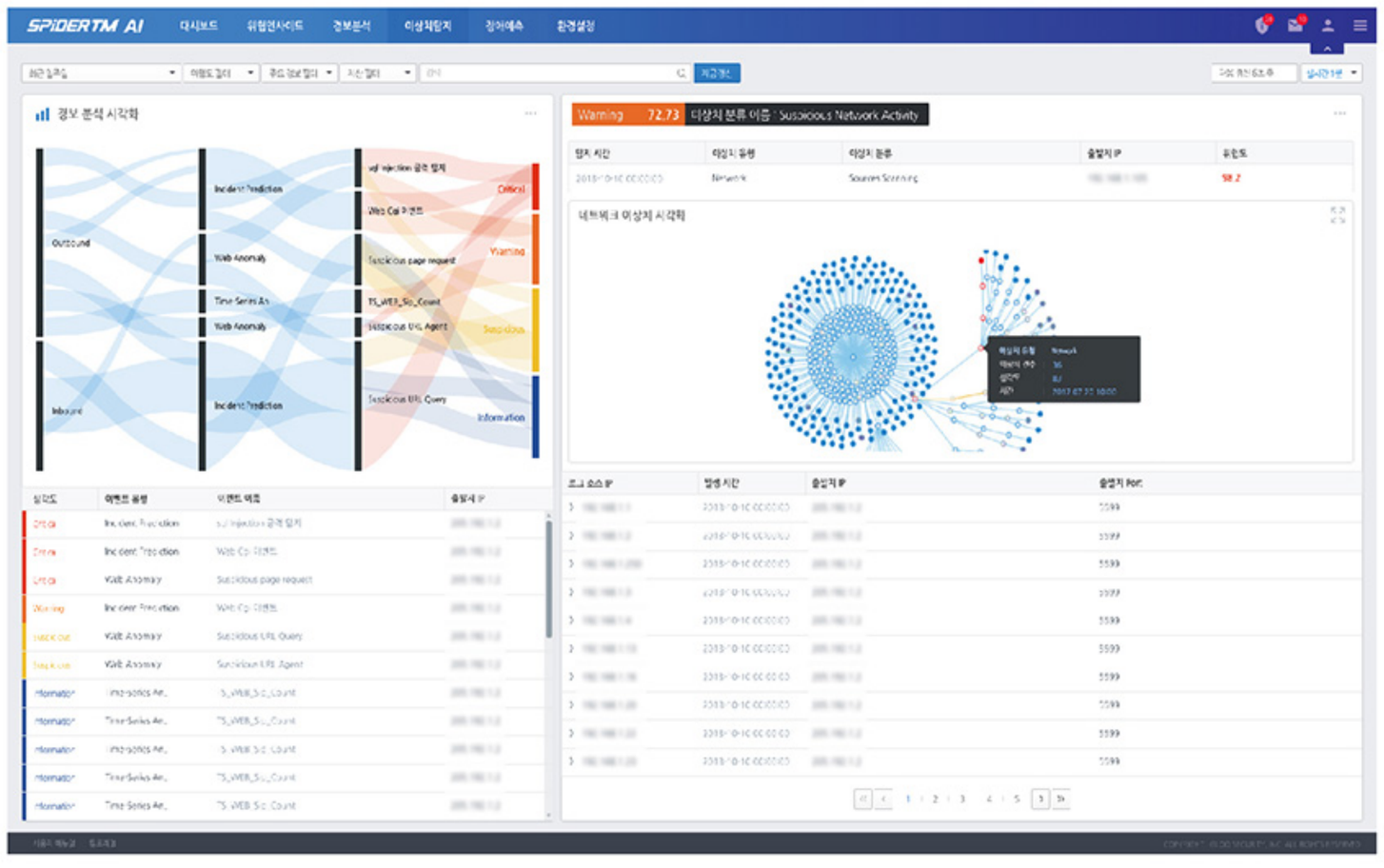
SPiDER TM AI Edition은 공격 유형에 따른 시나리오 기반의 데이터와 사고처리 내역(Labels)을 지도학습으로 학습하여 사고처리에 대한 예측을 제공합니다. 보안관리자는 머신러닝 기반의 스코어링 분석을 통해 이벤트 처리의 효율성을 높이고 위협에 선제적으로 대응할 수 있습니다.



미 탐지 위협 최소화

이상행위 탐지
Anomaly Detection

SPiDER TM AI Edition은 검증된 보안 플랫폼 및 방법론으로 모델링한 82종의 위협탐지 모델을 활용하여 이상행위를 탐지합니다.
이러한 이상행위 탐지 경보는 보안로그 및 경보이벤트의 이상치 탐지와 위협도 예측 결과를 종합하여 이상치 스코어와 함께 제공됩니다.



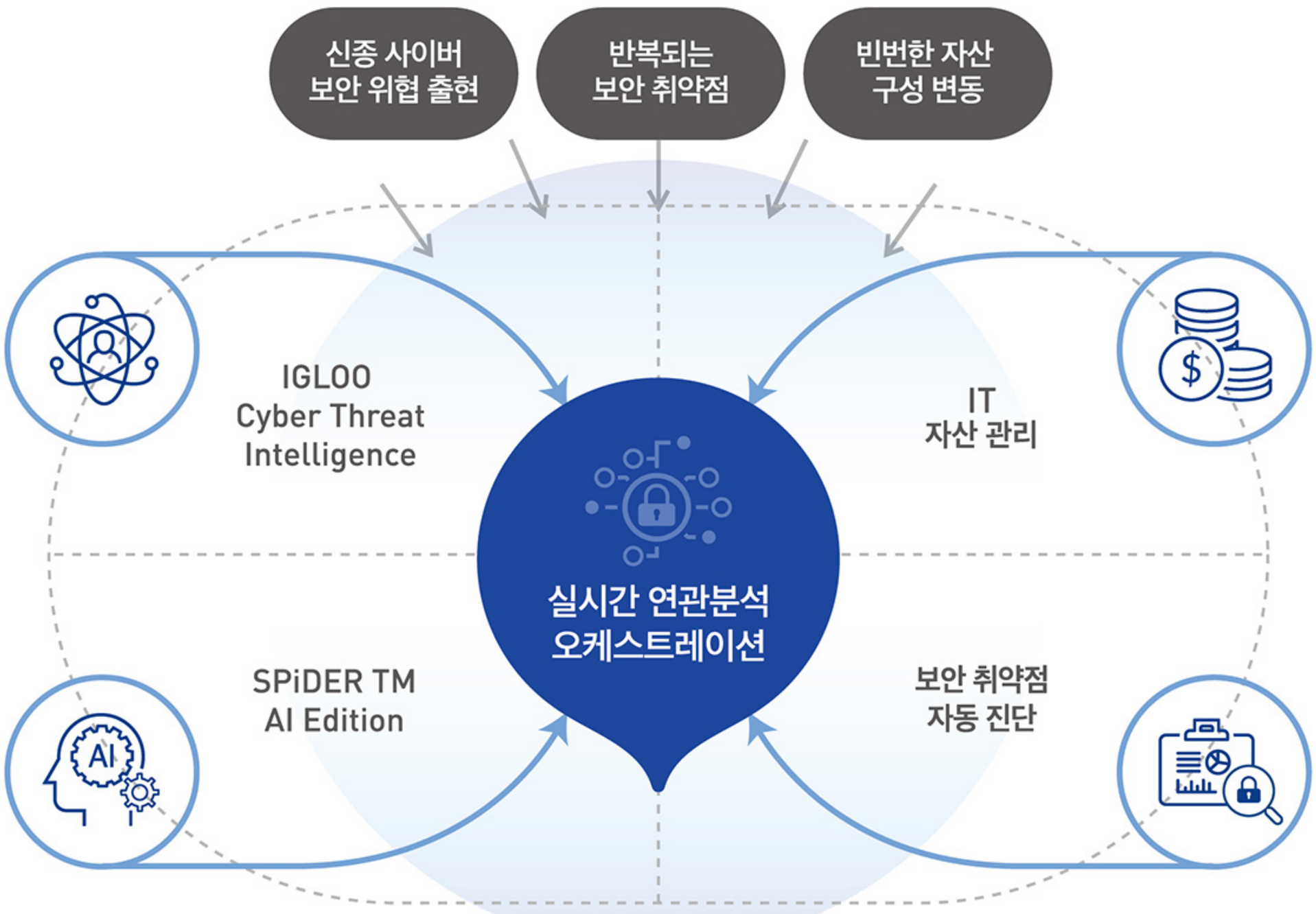
위협의 식별, 평가 및 대응까지 **위험성**을 실시간 연관 분석하는 **오케스트레이션**

기하급수적으로 증가하는
신종 사이버 보안 위협 분석의 어려움
위협식별의 스피드, 정확성 확보 및 예측이 필요

이글루시큐리티는 IGLOO CTI를 통해 수집하는 보안 데이터와 기술 취약점, 정보·사회 공학적 위협을 활용하여 선제적인 예측 및 예방관리를 수행합니다.
인공지능 시스템에서 탐지한 정오탐 분석 및 비정상 행위 공격에 대한 연관성 분석으로 보안관제 대응 시 위협식별의 스피드와 정확성을 확보합니다.

반복적으로 발생하는
자산 변동 및 보안 취약점에 대한
자동화 진단을 할 수 없을까?

'IT 자산 관리'와 '보안 취약점 진단'을 한 번에 수행할 수 있는 이글루시큐리티 보안진단 자동화 솔루션 Smart[Guard]와의 연동을 통해 인공지능 시스템에서 탐지한 정오탐 분석 및 비정상행위 공격에 대한 연관성 분석으로 위험도 스코어링 별 우선순위 대응을 처리합니다.



IGLOOSECURITY

㈜이글루시큐리티(대표 이득춘)는 글로벌 정보보안기업을 목표로 1999년 11월 설립되었습니다. 방화벽과 안티바이러스 제품이 보안의 전부로 여겨지던 초창기 정보보호 시장에서 국내 통합보안관리 시장을 개척하고 이끌어온 이글루시큐리티는 기업의 업무 환경, 업무 수행 방식의 혁신을 앞당기고 보안성을 강화할 수 있는 핵심 기술을 구현하는 데 역점을 두고 매진하여 왔습니다.
무엇을 누구에게서 학습하느냐에 따라 인공지능의 탐지력에는 현격한 차이가 발생합니다. 수십 명의 인공지능 보안 전문가 Pool과 20년간의 보안관제 경험, 노하우는 이글루시큐리티만의 차별화된 강점입니다.

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