AI로 연결된 최적의 AI 안전 경로 (AI Road)
분류형·설명형·생성형 AI 기술 기반
AI 탐지 모델 서비스

AiR
AI
Road

IGLOO

Background

바야흐로 인공지능(AI) 시대
AI를 악용한 사이버 공격, AI 기반 보안 기술들로 맞선다.

전 세계적인 인공지능(AI) 열풍 속에 이를 악용하는 사이버 공격도 폭발적으로 증가하면서, AI 내재화는 오늘날 성공적인 비즈니스 운영에 있어 필수불가결한 조건으로 떠올랐습니다. 특히 ChatGPT로 대표되는 생성형 AI(Generative AI)의 등장은 AI 보안의 중요성을 더욱 부각시키고 있습니다.

각각의 단일 기술을 기반으로 한 대응으로는 한계가 있습니다.
더 많은 공격 시도를 빠르게 분류하고, 또 정확히 판단해 내기 위해서는 여러 AI 기술들의 연계를 통한 또 한 번의 진화, 확장이 필요한 시점입니다.
날로 복잡해지는 IT 환경 속에서 더욱 현명한 결정을 보다 쉽게 내릴 수 있도록 길을 안내해 주는, AI 기술의 장점만을 모아둔 보안 서비스가 필요합니다.

Overview

에어(AiR, AI Road)는 분류형 AI, 설명 가능한 AI, 그리고 생성형 AI를 토대로 특정 보안 데이터에 대해 AI 모델이 판단한 근거를 알려주는 서비스입니다.
AI가 내린 판단의 신뢰성과 정확성을 높여 공격에 더욱 기민하게 대응할 수 있도록 지원합니다.

AiR를 통해 사용자는 AI 분류 모델이 예측한 결과와 이 예측에 영향을 미친 공격 특징(feature)의 중요도,
ChatGPT를 통한 자연어 형태의 설명을 비교 확인함으로써, AI 답변에 대한 이해도를 높이고 신뢰도를 평가할 수 있습니다.

AiR와 대화하며 복잡한 보안 위협을 보다 신속하게 탐지하고,
활용도 높은 인사이트를 이해하기 쉬운 형태로 받아보면서 보안 조직의 역량을 상향 평준화하세요.

Why AiR

AiR는 AI로 연결된 최적의 안전 경로(Road)입니다.

이글루코퍼레이션의 검증된 AI 기술력을 바탕으로 사용자를 안전하게 보호하는 동시에
이들이 보안의 복잡성에서 벗어나 최적의 안전 경로를 쉽고 빠르게 찾을 수 있도록 도와줍니다.

또한, 보이진 않지만 누구에게나 꼭 필요하고 어디에서나 존재하는 공기처럼,
AiR는 높은 접근성과 편의성, 연동성을 보장합니다.

가벼워 보이지만 절대 가볍지만은 않은,
보안을 완성해 주는 AiR를 만나보세요.

누구에게나 쉽고 스마트한 서비스
손쉬운 사용 및 연계

AiR는 설치 및 개발 부담이 없는 온라인 서비스입니다. 복잡한 별도의 과정 없이 웹페이지 접속만으로 쉽고 빠르게 이용할 수 있습니다. 또한 응용프로그램인터페이스(API) 형태로도 제공돼 다양한 보안 제품과의 연동을 지원합니다. SPiDER SOAR를 비롯한 자사 제품은 물론, 타사 제품과도 연계가 가능한 높은 확장성 및 활용도를 갖췄습니다.

정확도 높은 인사이트의 즉각적인 제공
차별화된 프롬프트 엔지니어링

차별화된 프롬프트 엔지니어링(Prompt Engineering) 기술을 바탕으로 생성형 AI가 내놓는 답변의 정확도를 높이고 오답변 가능성을 최소화합니다. 이글루코퍼레이션은 다년간의 AI 학습 데이터 구축 및 AI 솔루션 운영 경험을 토대로, 보안에 최적화된 '프롬프트'를 제시하며 높은 정확성을 갖췄습니다. 검색어에 따라 검색 결과가 달라지듯이, 똑같은 페이로드(Payload)를 입력했다고 할지라도 AiR를 통해서라면 질문 의도에 가장 적합한 답변을 얻을 수 있습니다.

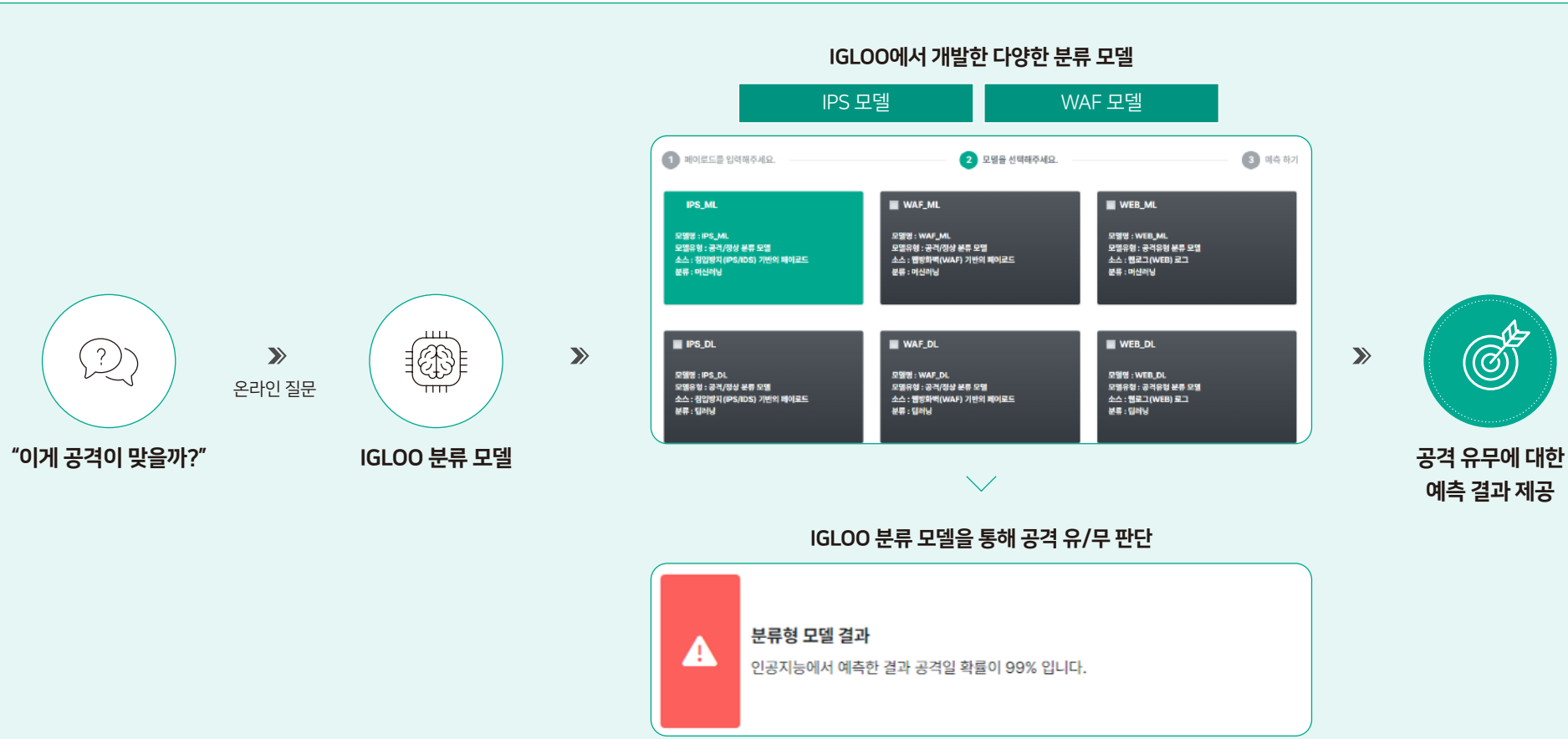
신뢰할 수 있는 안전한 서비스
고유의 비식별화 기술

고유의 보안 기술을 바탕으로 민감한 데이터가 외부로 노출되는 것을 사전에 방지합니다. 중요 정보에 대한 비식별화 과정(변환 또는 삭제)을 거친 프롬프트 제작을 비롯한 여러 보안 조치로 강력 보안성을 갖췄습니다. 국내 보안업계를 선도하는 이글루코퍼레이션의 검증된 보안 역량과 다년간 AI 학습 데이터를 개발하며 획득한 노하우를 토대로, 그 누구보다 높은 안정성을 보장합니다.

Features

이글루코퍼레이션이 자체 개발한 양질의 학습 데이터를 학습한
IGLOO AI 분류 모델이 스스로 판단 기준을 세워 공격의 유/무를 판단합니다.
이를 통해 사용자는 보다 정확하고 신속하게 위협을 탐지할 수 있을 뿐만 아니라
날로 고도화되는 사이버 공격에 대한 대응력을 한 단계 높일 수 있습니다.

IGLOO 분류형 AI



Features

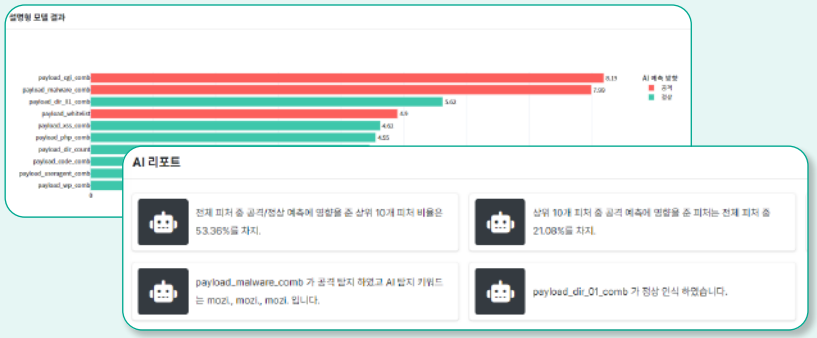
IGLOO AI 분류 모델의 예측 결과에 영향을 미친 공격 특징(feature)의 중요도를 보여줍니다.
AI가 왜 이 이벤트를 공격이라고 판단했는지, 결과의 도출 과정과 이유에 대한
납득 가능한 근거를 토대로 사용자에게 더욱 신뢰도 있는 답변을 제시합니다.

IGLOO 설명형 AI

"AI는 왜 이렇게 판단했지?"

IGLOO XAI 모델

설명 가능한 AI를 통해 판단 결과에 대한 근거 확인



기존 시그니처 기반의 분석과 비교 &
탐지 가능한 장비 및 공격에 대한 설명과 대응 방안 제시

예측 결과에 대한
근거 제시

Features

IGLOO AI 모델(분류형/설명형)이 내놓은 결과를
ChatGPT와 연계한 자연어 형태의 답변으로 확인할 수 있습니다.
이를 통해 사용자는 결과를 보다 직관적으로 인지하고, 신속한 의사결정을 내릴 수 있습니다.

생성형 AI
(with OpenAI's ChatGPT)

Benefits

AiR는 이글루코퍼레이션 고유의 AI 기술력이 집약된 보안 전문 AI 어시스턴트입니다.

AiR는 AI가 판단한 공격 결과에 대한 신뢰성과 이해도를 높임으로써
보안 조직 전반의 지식 격차를 해소하고, 언제나 최상의 조치가 신속하게 실행될 수 있도록 도와줍니다.

**3개의 AI 모델이 내놓은 답변을 비교 확인함으로써,
보안 조직의 분석 역량을 높여줍니다.**

분류형 모델 결과
특정 보안 데이터에 대한 예측 결과

설명형 모델 결과
이 예측에 영향을 미친 공격 특징(feature)의 중요도

생성형 모델 결과
자연어 형태의 대답

+

**2단계 피드백 및 주기적인 재학습을 통해
AI 모델의 정확성을 지속 개선합니다.**

1단계
AiR가 내놓은 예측 결과에 대한 실 사용자의 피드백

2단계
이글루코퍼레이션 보안 전문가들의 주기적인 피드백 및 결과 점검

»

**보안 조직
전문성 강화**

Roadmap

AiR를 통해 더 많은 조직이 보다 현명한 결정을 내릴 수 있도록,
지속적으로 서비스 모델을 다양화하고 적용 기술을 고도화할 계획입니다.

- 분류형 AI 모델: 현재 적용된 보안 이벤트 분류 모델에 이어 엔드포인트 및 행위 기반 모델 등 추가
- 설명형 AI 모델: 위협 인텔리전스(CTI)와의 연계 분석 등 표현 방법 지속 고도화
- 생성형 AI 모델: 복수의 생성형 AI 모델 연계 및 이글루코퍼레이션 고유의 생성형 AI 모델 적용

STAGE 1	STAGE 2	STAGE 3
AiR AI Road		
IGLOO 분류형 AI 정·오탐 분류 모델(IDS/IPS, WAF)	**탐지/분류 모델 연계 확대** WEB, EDR, MITRE ATT&CK 등	**IGLOO 생성형 AI 모델 탑재** **이글루코퍼레이션 보안 특화 소형 언어 모델(sLLM)** GREEN Ai
IGLOO 설명형 AI SHAP, 시그니쳐 기반	**표현 방법 고도화**	
생성형 AI 오픈AI(ChatGPT)	**생성형 AI 모델 연계 확대** 구글(Google PaLM), 메타(Meta AI), 카카오(KoGPT)	

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