안전한 생성형 AI 플랫폼

S·AIP

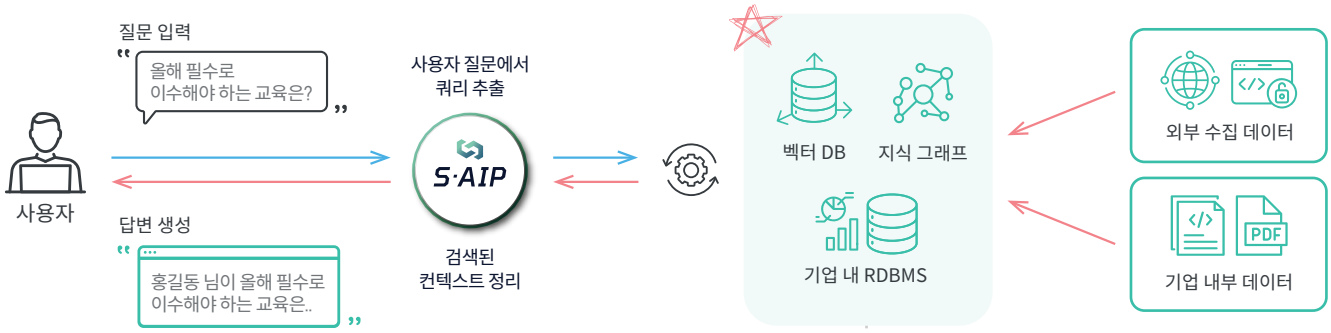
S2W

S-AIP

데이터 인텔리전스 회사가 만드는 안전한 생성형 AI 플랫폼

S-AIP는 빅데이터와 RAG를 활용한 기업용 맞춤 sLLM입니다. S2W는 수년간 축적해온 비정형 다크웹 데이터 처리 역량과 노하우를 바탕으로 도메인 학습에 특화된 언어 모델을 구축했습니다. S-AIP는 기업 내 존재하는 모든 정형, 비정형 데이터를 중앙화해 사용자의 질문에 가장 근접한 사실 기반 답변과 데이터를 생성, 제공합니다. 또한, 실제로 존재하는 데이터를 조직 내부에서만 활용할 수 있도록 언어 모델을 구축해 기존 LLM의 문제점이었던 환각 현상과 발생할 수 있는 보안 취약점 문제를 해결하였습니다.

S-AIP 워크플로우

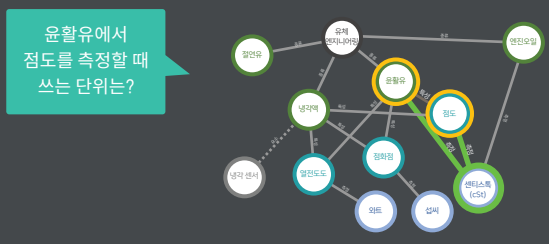


check point

- ✓ 기업 내부 데이터 활용으로 데이터 신뢰성 향상
- ✓ 정형, 비정형 데이터 중앙화를 통해 방대한 DB 구축
- ✓ 데이터 벡터화를 통한 의미기반 검색 엔진 구축

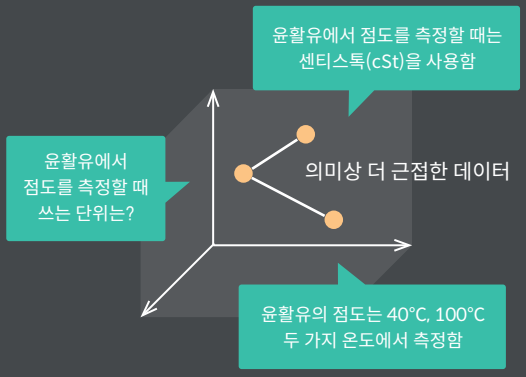
*지식그래프 구조 (Knowledge Graph)

Knowledge Graph는 사용자의 질문에서
각 개체들을 분리하고 개체 간 관련성/관계성을 추출합니다.



*벡터화: Semantic Search Engine

기존의 키워드(단어) 매칭 기반 검색의 한계를 넘어, 두 텍스트(문장) 간 서로 겹치는 단어가 전혀 없더라도, 의미가 유사한 두 문장을 서로 가까운 좌표(벡터)로 변환하여 의미 기반 검색을 수행하는 검색 엔진입니다.



S-AIP의 차별점

보안성이 보장된 프라이빗 sLLM

기업 보안 수준에 맞춘 아키텍처 및 데이터 보안 기술을 활용하여 안전하고 효율적인 기업용 프라이빗 sLLM 구축 및 사용을 지원합니다.

맞춤형 sLLM 아키텍처

기업 보안 환경에 맞춘 안전한
LLM 아키텍처로 내부 데이터 유출
걱정 없이 내부 전용 서버에 구축

역할 기반 액세스 제어(RBAC)

사내 IT 시스템 내에서 사용자/직급별로
접근 권한을 다르게 설정하여
효율적인 데이터 보안 지원

검색 · 증강 · 생성 (RAG)

대규모 언어 모델(LLM)이 생성한 답변을
외부 데이터(검색 결과)로 보강하여
대답의 정확성과 유용성 개선

상용 LLM의 한계점 보완

도메인 학습 최적화

지속적인 실제 도메인 특화 학습 모델 구축 경험을
통한 노하우를 보유하고 있습니다.

- 사이버 위협 도메인 특화 언어 모델(DarkBERT) 구축 경험
- 도메인 최적화 학습/튜닝 노하우 보유
- 수 십억 개의 비정형 다크웹 데이터 전처리 역량 바탕

환각 현상 해결

결과를 신뢰하기 어려운 환각 효과를 방지하기 위해
생성된 답변 확인 및 검증 방식을 제공합니다.

- 환각 현상 개선/최소화 위해서 RAG/지식 그래프 활용
- 대규모 언어 모델(LLM)이 생성한 답변을 외부 데이터
  (검색 결과)로 보강하여 대답의 정확성과 유용성 개선

실시간 최신정보 참조

외부 수집 DB 별도 구축 및 운용에 기반하여
실시간으로 최신 정보를 참조합니다.

- 실시간 데이터 연계
- Knowledge base를 통해 기업 내부에 있는 데이터
  접근뿐만 아니라 가장 최신 정보 접근 가능

독보적인 비정형 데이터 수집 및 처리 역량

비정형화 데이터 운용의 핵심은 데이터 전처리로, S2W는 다크웹, 텔레그램 등 다양한 채널로부터 위협 정보를 수집하고 고객사에게 제공하는 과정에서 폭넓은 비정형 데이터 전처리 역량과 노하우를 확보하고 있습니다.

***수집 데이터 유형**

웹 데이터, 공개 데이터
예) OSINT

쉽게 검색하고 열람할 수 있는
외부 공개 정보

정형 데이터
예) BigQuery, JSON 등

데이터가 잘 정제되어 있고
특정 포맷이나 스키마에 잘
매칭되어 있는 유형의 데이터

비정형 데이터
예) PDF, Word 등

자연어와 같이 데이터가
특정 스키마에 따르지 않고
포맷이 자유로운 유형의 데이터

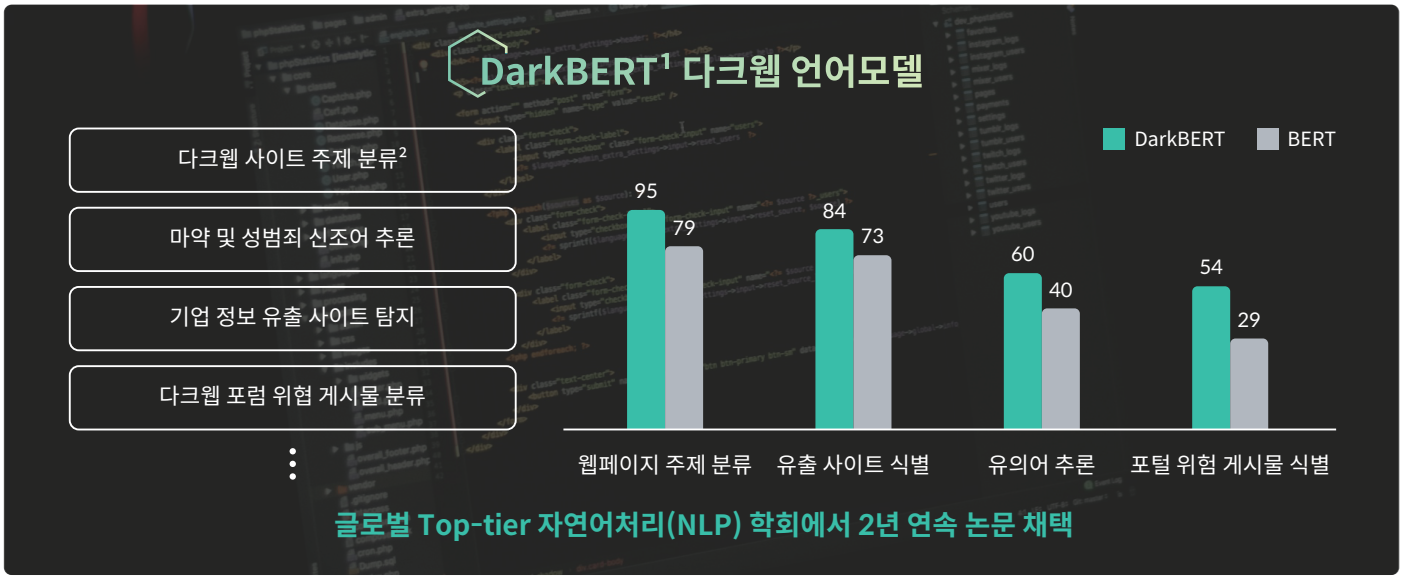
S-AIP 활용 예시

세계 최초 다크웹 특화 언어모델 DarkBERT

대량의 다크웹 문서 + 트랜스포머 기반 범용 언어 모델

DarkBERT

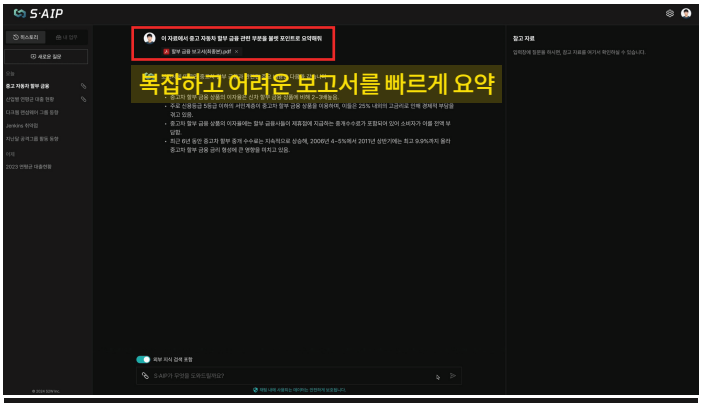
- S2W와 KAIST 연구진이 공동 개발한 다크웹 특화 언어모델
- 600만 건 이상의 다크웹 페이지 학습 모델로 다양한 카테고리 별 위험 정보를 효과적으로 탐지 및 분류
- Interpol, UN, 국내외 정부기관에서 활용

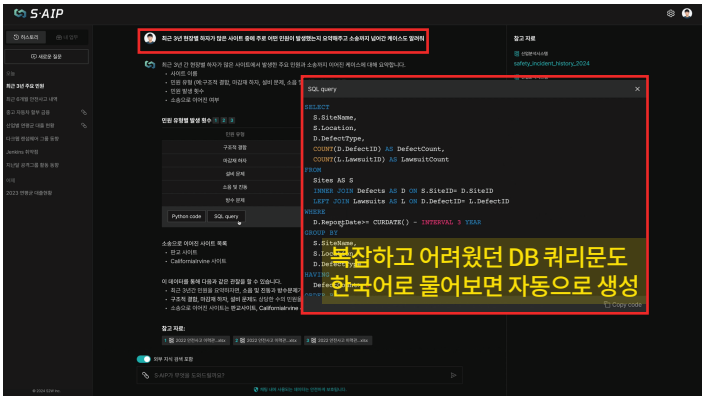


1) DarkBERT 논문. 2023년 ACL 학회 등재.
2) 2022년 NAACL 학회 눈문 등재 (ACL. EMNLP와 함께 전 세계 3대 탑티어 자연어처리 학회. 구글, MS, 메타, 네이버, 카카오브레인 등 국내외 빅테크 기업들이 논문 실적 보유 중)

산업 별 최적화된 AIP 솔루션 구축

S-AIP는 기업 내부에서 질의응답 기반의 검색, 문서 요약, 문서 생성 등 기본적인 업무 효율 향상 기능과 더불어 특정 산업(도메인)에 특화된 생성형 AI 플랫폼으로 구축됩니다. 또한, S-AIP는 제조, 보안, 소프트웨어, 금융, 지주회사, 통신사, 교육, 건설, 유통, 이커머스 등 다양한 산업에 적합한 도메인과 기업 내부 데이터를 같이 학습해 특정 기업 맞춤형으로 설계가 가능합니다.

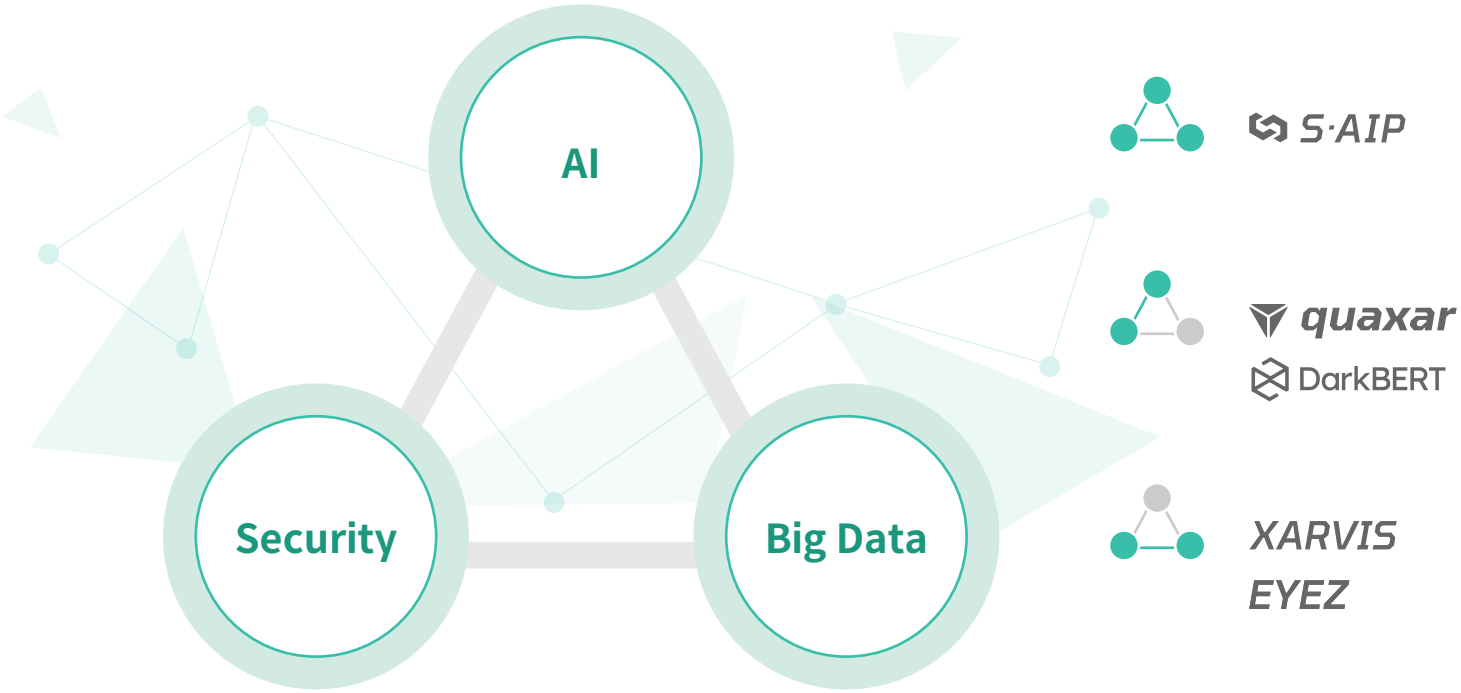




WHY S2W?

S2W는 데이터 인텔리전스 기업으로 기술의 융합을 통해 창의적인 솔루션을 제안합니다.

S2W는 믿을 수 있는 AI 기반 데이터 인텔리전스 제공을 목표로 합니다. 정교한 AI 기술을 기반으로 빅데이터를 분석하고 그것을 안전한 울타리로 보호합니다. 숨겨진 데이터를 탐지해, 전에는 볼 수 없었던 데이터 간의 관계를 찾아내 가시화합니다. 보안을 잘 아는 회사가 만들어가는 AI 기반 데이터 인텔리전스 플랫폼, 그것이 안전한 데이터 사회를 만들어가기 위한 우리의 역할이자 목표입니다.



국제 논문

NDSS 2024
DRAINCLoG: Detecting Rogue Accounts with Illegally-obtained NFTs using Classifiers Learned on Graphs

61 ACL 2023
DarkBERT: A Language Model for the Dark Side of the Internet

NAACL 2022
Shedding New Light on the Language of the Dark Web

NDSS 2019
Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web

THE WEB CONFERENCE 2019
Doppelgängers on the Dark Web: A Large-scale Assessment on Phishing Hidden Web Services

수상 이력

WORLD ECONOMIC FORUM — World Economic Forum 100대 기술선도 스타트업 선정 (2023)

K STARTUP — 한국 대표 혁신 스타트업 선정 (2022)

KOREA STARTUP 100 — Korea AI Startup 100 선정 (2022)

NCSC — 국가정보원 사이버 안보센터 참여기업 (2022)

info@s2w.inc | +82 70 5066 5277 | www.s2w.inc