S-AIP 런칭 데이 QnA

현장에서 미처 답변드리지 못한 온라인/오프라인 설문 질문에 대한 답을 정리하여 보내드립니다.

1. S2W 의 AI 다크웹 위험 탐지와 차단 등 관련하여 타 솔루션 차별점은 무엇인지요? 산업별, 기업별 보안 유형에 맞는 AI 모델링과 추론 최적화와 적용은 어떻게 지원되는지요?

   S2W 의 다크웹 위협 탐지는 DarkBERT AI 모델을 활용하여 탐지하기 때문에 기존 키워드 exact match 를 넘어 유사한 위협까지도 탐지합니다. 산업별, 기업별 보안 유형에 맞는 AI 모델링은 지금도 적용되어 있고, 추론 최적화는 Knowledge Graph 관점으로 지속적으로 발전시켜나가고 있습니다.

2. 다크웹 데이터 특성상 할루시네이션과 정보오염의 발생이 잦을 것 같습니다. 이러한 할루시네이션이나 정보오염은 어떻게 대응하고 있으신가요? 정규화 처리가 어렵고 정크 데이터가 많아 무효한 데이터가 상당할 것으로 우려됩니다. 고객 입장에서 데이터를 신뢰할 수 있게 하는 어떠한 방안이 적용되었을까요?

   할루시네이션 문제를 해결하기 위해 RAG 기술을 탑재하였고, RAG 에서조차 해결하지 못하는 문제들도 있기에 Knowledge Graph 기술을 같이 활용하여 문제를 해결하고 있습니다. 고객 입장에서 데이터를 신뢰할 수 있도록 답변의 출처가 되었던 항목들을 같이 보여주는 형태로 제공하고 있습니다.

3. 비정형 다크웹 데이터를 분석하여 정규화 하는 과정은 자동화가 되었나요? 비정형 데이터 특성상 휴먼 리소스 없이 분석 정규화가 어려울 것 같은데, 휴먼 리소스일 경우 휴먼 에러나 사람의 업무량 한계점 때문에 방대한 다크웹 데이터를 AI 에 적용이 가능할지 궁금합니다.

   초기 분석은 사람이 해야 하는 부분입니다. 분류 방법과 학습 방향을 정하고 AI 모델을 정하면 이후는 AI 가 하게 됩니다. 방대한 다크웹 데이터는 사람이 할 수 있는 양이 아니고 휴먼 에러도 막기 위해 AI 모델을 가지고 훈련시켜야 합니다. 다크웹/텔레그램에 대해서는

이미 AI 를 적용해서 사업을 하고 있습니다.

4. 생성형 AI 의 데이터, 이미지, LLM 등 특화 분야 차이에 따른 AI 보안의 차별화 방안의 모델링 지원은 어떻게 될까요? 또, S2W 생성형 AI 가 다양화됨에 따라 어떻게 지원하게 될까요?

   새로운 LLM 이 나왔을 때 그 모델을 S-AIP 에 채택하여 쓰는 것도 가능합니다. 즉, 한 가지 Foundation Model 만 쓰는 것이 아니라 여러 가지를 고려하여 사용 가능합니다.
   S-AIP 의 핵심은 해당 산업과 기업에 특화된 온톨로지의 구성이며, 다양한 부수적인 기능들은 다른 모듈이나 기능을 함께 사용하거나 연동할 수 있습니다.

5. S-AIP 에 질문한 내용에 대한 답변을 excel, pdf 등으로 출력도 가능할까요?
   (예: 22 년 A 공장의 주물 관련 결함보고서를 결함 유형별로 엑셀로 정리해줘)

   현재 CSV, PDF export 를 지원하며 액셀 등 기타 다양한 포맷도 확장이나 연동이 가능하도록 추가해 나갈 계획입니다. 포맷 다양성 부분은 기술적인 문제라기 보다는 코파일럿 등 타 제품과의 연동을 위한 상업적 라이선스 연계가 필요합니다.

6. 다크웹, 랜섬웨어 등 생성형 AI 등장 이후, 보안에 대한 새로운 유형의 위험과 기존 패턴에서 주요한 변화는 무엇일까요? 생성형 AI 를 통한 보안을 구축 시에 새로운 위험 유형에 대한 분석 소요 시간을 줄이기 위한 방안과 주요 요소는 어떻게 변경, 변화해야 할까요?

   아직까지는 AI 가 신종 공격을 하는 도구는 아닙니다. 그러나, 개인화된 피싱과 같은 생산성과 효율로 인해서 보안에 취약한 대상들이 대거 공격에 노출될 것으로 전망되어 보안에 대한 투자는 높아져야 할 시점입니다.

7. S-AIP 는 on-premise 형태로 구축된다고 말씀하셨는데, 타사 ASM 서비스의 API 를 활용하여 S-AIP 와 결합할 수 있는지 궁금합니다.

   가능합니다. (S2W 의 ASM 도 검토해 주신다면 감사하겠습니다.)

8. S2W 에서는 어떠한 sLLM(LLaMA or 자체 구축 등)을 사용하고 계시는지 궁금합니다.

   자체적으로 보유한 sLLM 을 포함하여 가용한 sLLM 중에서 고객 DATA 의 온톨로지 구성에 적합하고 고객 환경에서 성능이 가장 잘 나오는 LLM 을 선정하여 권장 드립니다. 고객이 보유한 LLM(혹은 지정한 LLM)이 있는 경우에는 이를 적용합니다.

9. 구축형, 하나에 평균적으로 몇 사람이 어느 정도로 투입되나요?

   고객의 DATA 복잡도와 시스템 환경에 따라 다르며, AI 인력 외에도 인프라 분석, 빅데이터 분석, 데이터베이스 전문가 등 사내 여러 인력이 계속 함께 사업을 진행합니다. 6 개월 size 의 프로젝트 기준으로는 PM 1 명을 포함한 5 명 내외의 전담팀이 진행하게 됩니다.

10. 엔드유저 입장에서 데이터가 잘 분석이 되었는지 체크하는 방법이 있을까요?

    각 단계별로 고객사 TF (혹은 실무진) 함께 체크해 나가면서 DATA 의 투입 규모를 늘여 나갑니다. 이러한 프로세스를 통해서 예상치 못한 결과가 나오는 경우를 방지하고 실무에 직접 도움이 되는 시스템으로 구축됩니다. 해당 프로세스와 점검 루틴도 S-AIP 만의 노하우입니다.

11. 현재 컨설팅/구축 또는 PoC 하고 있는 공개 가능한 고객 credential 공유 가능할까요?

    생성형 AI 도입 과제가 전략적으로 진행되는 경우가 다수입니다. 고객사 동의 없이 진행 중인 사업들을 공개하는 것은 무리가 있어 양해를 구합니다. 성공적인 도입이 완료되면 조만간 미디어를 통해서 순차적으로 확인이 가능하실 것 같습니다. 산업 분야로는 현재 금융, 제조, 건설, 커머스 업권에서 컨설팅과 구축을 진행하고 있습니다.

12. 산업 군 별로 sLLM 모델을 커스터마이징하여 사용할 수 있는지 궁금합니다.
    (예: 금융 기관과 같이 법 제도적 측면에서 시스템 망 분리 등 환경적 제약이 있는 경우에는 그에 맞춰서 구축 및 연동할 수 있는지)

망 분리 환경 고려해서 구현 가능합니다. 실제로 구축 사례도 가지고 있습니다. S-AIP 는 요구하는 시스템 구성 환경이 따로 없습니다. 고객의 인프라 및 제약 구조에 맞춰서 구현합니다. 망 분리 환경에서는 DATA 의 분리도 이에 맞춰 구현되어야 하는지, 보안성에서 고려되어야 할 부분 등을 사전에 고객사와 함께 논의하고 설계하여 진행합니다.

13. 트레이닝과 인퍼런스 각 영역에서 클라우드 자원 활용하지 않고 on-premise 로만 구축하시나요? 아니면 하이브리드 형태로 인프라 구성하고 있는지 궁금합니다.

고객 시스템 환경이나 구축 요구에 맞게 하이브리드 인프라 구성도 가능합니다. 고객의 환경에 따릅니다.

14. 컴퓨팅 자원 활용 측면에서 H100 의 경우 공급 제약과 TCO 관점에서 LLM 대비 부담이 될 수 있을 것 같은데, 어떤 형태로 리소스 투입해 시스템 구축하고 있는지 궁금합니다.

고객이 활용할 수 있는 인프라를 활용하는 것을 최우선시 합니다. sLLM 은 H100 이 아니어도 가능하기 때문에 그보다 성능 낮은 그래픽카드를 수량만 맞춰서 사용 가능합니다.