

Q. 로그들이 방대하고 상호 연관 분석이 어려운데, 이를 자동으로 감지할 수 있나?

A. 이상 탐지용 AI 기반 보안 모니터링 기술(특히 보유)로 로그 이상 탐지 및 자동 대응 가능.Elastic기반 기술이 풍부한 로이드케이에서는 Elastic기반으로 해서 우수한 품질의 로그 분석을 지원 가능합니다. 예를 들어 사용자나 장비 시간 기준으로 로그를 조회 분석 할 수 있도록 구현이 가능합니다.

하지만 본격적인 연관 분석을 위하여는 그래프DB나 AI 활용한 추가 분석을 위한 아키텍처를 별도 구성해서 진행할 필요가 있습니다. 또한 연관성을 사람과 함께 LLM 이 찾아 나가는 과정에서 분석을 도와 줄 수 있습니다

Q. 로컬 데이터 활용이 AI 활용 시 문제점으로 꼽히는 이유는?

A. 사내·로컬 데이터만 사용하면 여러 위험이 발생할 수 있다. 먼저 보안·프라이버시 측면에서, 내부 데이터를 적절히 격리·암호화하지 않으면 외부 모델로 전송 시 유출 위험이 생길 수 있습니다.

실제로 기업 데이터 통합 과정에서 데이터 프라이버시 및 보안 우려가 문제로 지적되는 경우도 있습니다.

또한 로컬 데이터만으로 AI를 구동할 경우 지식 범위가 제한되고 최신 정보가 반영되지 않아 모델의 부정확한 결과(할루시네이션) 가능성이 커집니다.

예를 들어 RAG 기법은 외부 신뢰 문서로 모델의 할루시네이션을 줄이는 데 사용되는데, 로컬 데이터가 부족하면 모델이 자체적으로 부정확한 답변을 생성할 위험이 높아질 수 있습니다.

Q. 할루시네이션 문제란 무엇인가?

A. 할루시네이션(Hallucination)은 AI 모델이 실제 사실과 다르거나 존재하지 않는 잘못된 정보를 생성하는 현상입니다.

예를 들어 LLM이 뉴스 기사를 요약할 때 기사에 없는 내용을 만들어내거나, 병원 진단 AI가 존재하지 않는 증상을 보고할 수 있습니다.

이러한 현상은 학습 데이터의 불완전성·편향성이나 맥락 정보 부족 등에 의해 발생할 수 있으며, 특히 의료·법률·금융 등 정확성이 중요한 분야에서 심각한 문제로 작용할 수 있습니다.