

문제점 목록

Project Name	BGP라우팅 데이터 분석 LLM 기술 개발
--------------	-------------------------

6조

- 202002567 진효겸
- 202002506 손봉우
- 202002518 양준혁

지도교수: 이영석 교수님 (서명)

Document Revision History

REV#	DATE	AFFECTED SECTION	AUTHOR
1	2023/03/06		홍길동

Table of Contents

1. 이해당사자(STAKEHOLDER)의 문제 이해	5
2. AS-IS 파악	6

List of Figure

그림 목차 항목을 찾을 수 없습니다.

1. 이해당사자(stakeholder)의 문제 이해

문제점	문제점 파악 방법	문제 상세 기술		
		이해당사자	고충/니즈	이유
오래된 데이터의 분석이 어려움	bgplay 사용	BGP 분야에 관심있는 학생	오래된 데이터도 분석할 수 있는 기능이 필요	기존 툴은 최근의 데이터만 제공
대량의 데이터 처리가 어려움	bgplay 사용	BGP 분야에 관심있는 학생	대량의 데이터를 신속하게 처리할 수 있어야 함	기존 툴에서 대량 데이터 처리 시도시 시간이 과도하게 소요됨
기존 툴의 사용이 어려움	학습	BGP 분야에 관심있는 학생	자연어로 BGP 데이터를 쉽게 분석하고 시각화할 수 있는 기능이 필요함	기존 툴은 사용이 어려워 업무 효율성이 떨어짐
기존 툴의 사용이 어려움	인터뷰	네트워크 엔지니어	직관적인 UI, 자동화된 분석	복잡한 명령어 사용으로 인해 시간이 지체됨
실시간 BGP 이상 탐지 시스템 부족	관찰	보안 팀 (SOC, CSIRT)	자동으로 경로 변경과 보안 위협을 탐지하는 시스템이 필요함	보안 사고 발생 시 실시간 대응이 어려움

2. AS-IS 파악

1. 기존 툴의 사용이 어려움 (네트워크 엔지니어 대상)

현재 상황

- 기존 BGP 분석 툴은 명령어 기반으로 복잡한 설정이 필요하여 사용이 어려움.
- 실무에서 데이터를 분석할 때, 직관적인 UI가 부족하여 시간이 많이 소요됨.
- 자동화된 분석 기능이 부족하여 수작업이 많음.

문제점

- 네트워크 장애 발생 시 신속한 대응이 어려움.
- 데이터 분석 시간이 길어 업무 효율성이 저하됨.

2. 실시간 BGP 이상 탐지 시스템 부족 (보안 팀 대상)

현재 상황

- 보안 위협(BGP 하이재킹, 경로 변경 등)이 발생해도 실시간으로 탐지하기 어려움.
- 대량의 로그 데이터를 수동으로 분석해야 하며, 탐지 및 대응 속도가 느림.
- 보안 사고 발생 시 신속한 대응이 어려워 피해 확산 가능성이 높음.

문제점

- 실시간 네트워크 이상 감지 시스템이 부족하여 보안 위협 대응 속도가 저하됨.
- 자동화된 경고 시스템이 없어 네트워크 관리자와 보안 담당자가 일일이 확인해야 함.

3. 기존 툴의 사용이 어려움 (BGP 분야에 관심 있는 학생 대상)

현재 상황

- BGP 데이터를 분석하려면 전문적인 네트워크 지식이 필요하여 접근성이 낮음.
- 자연어 기반의 분석 기능이 없고, 명령어를 익혀야만 데이터 분석이 가능함.
- 데이터 시각화 기능이 부족하여 직관적인 분석이 어려움.

문제점

- 학습자가 BGP 데이터를 쉽게 다룰 수 있는 환경이 제공되지 않음.
- 기존 툴은 사용법이 어렵고, 학습하는 데 많은 시간이 필요함.