2025 생성형AI활용 프로젝트아이디어 제안서

학번	이름	팀명	이메일
20251233	김정민	일조	charamin6709@naver.com

제목	강화학습 기반 사이버 공격 방어 AI		
분야	□ 머신 러닝 □ 딥러닝 □ 컴퓨터 비전 ■ 강화 학습 □ 자연어 처리 □ 멀티 모델 □ 기타 ( )	AI 응용 기술 분야	□ 자율 주행 □ 의료 □ 추천 시스템 □ 생성형 AI □ 교육용 AI ■ AI 보안 □ 기타 ( )
프로젝트 개요	사이버 공격은 점점 정교해지고, 빠르게 실시간 대응이 어려워지고 있다. 이에 강화학습을 사용하여 최근 발생한(skt 해킹사건, kt유령 기지국사건), 과거 발생한 사이버 공격 패턴들을 학습시키고 방어하는 것을 어느정도 학습시켜 스스로 방어 전략을 생성하는 ai 보안 시스템을 개발하려 한다.		
목표 및 기대효과	- 목표 1. 보안 프로그램에 ai를 활용해 사이버 공격 빠른 탐지 및 방어에 걸리는 시간 단축 2. 지금까지 존재하던 공격 시나리오외 다양한 공격 방법에 자동 적응하는 ai개발 - 기대 효과 1. 개발된 ai를 활용해 보안 관리자도 새로운 패턴을 배우고, 연구 역량히 향상 가능하다.		
활용 생성형 AI 도구	1. ChatGPT :공격 및 방어 전략 시뮬레이션을 생성 가능하다. 2. Microsoft Azure AI Security Tools : 인공지능 시스템 설계, 개발, 배포 과정에서 보안을 강화하고 위협을 사전에 탐지, 대응할 수 있도록 지원하는 다양한 도구와 서비스로 실시간 공격 데이터를 분석 가능하다.		
프로젝트 주요 기능 및 구현 방법	- 주요 기능 1. 실시간 침입 감지 : 네트워크를 통해 들어오는 패킷을 분석해 비정상적인 활동들 감지 2. 자동 대응 전략 생성 : 공격 유형에 따라 방어하는 방법을 강화학습을 통해 자동 업데이트 3. 위협 데이터 시각화 : 보안 로그와 네트워크 분석 현황을 시각적으로 대시보드에 표시 4. 모델 자가 학습 : 처음보는 유형이나 새로운 유형의 공격 패턴이 발생시 ai가 스스로 그 공격 방법을 학습하고 방어를 해보며 방어 성능 향상 - 구현 방법 1. 데이터 수집 : 공개 보안 데이터셋이나 실제 네트워크 로그 활용 2. 전처리 : 수집된 데이터를 ip, 포트, 패킷 특징 등으로 쉽게 구분 가능한 자료로 가공 후 ai가 학습 가능한 형식으로 변환 3. 강화학습 모델 설계 : ai에이전트가 공격을 탐지 -> 보상을 통해 방어전략 개선, DQN 알고리즘을 활용해 설계 4. 시뮬레이션 환경 : 공격자와 방어자의 공방 상호작용을 가상 시뮬레이션 환경에서 테스트 5. 대시보드 개발 : Flask와 연동해 ai 탐지 결과를 실시간으로 모니터링, 기록		
AI 관련 기술 및 해결 방안	- AI 관련 기술: 1. 강화학습 알고리즘으로 DQN이 존재한다. 2. 학습시 필요한 공격 데이터 부족한 경우 GAN을 활용해 가상 공격 데이터 생성해 학습한다.		

	- 문제 및 해결 방안 1. ai 보안 문제는 ai 모델의 오탐지를 최소화 하고 ai 자체의 보안을 위해 개발진이 지속적으로 업데이트를 한다. 2. 공격 패턴이나 방어 방식에 관한 데이터는 클라우드 시스템인 Azure를 활용해 실시간 데이터 처리 및 확장성을 확보해서 사용