**화이트햇 스쿨 2단계 팀 프로젝트 보고서**

**차세대 보안리더 양성 프로그램**

**한국정보기술연구원 BoB 교육센터**

|  |  |  |  |
| --- | --- | --- | --- |
| **멘토명 / PL명** | 손승호 멘토님 / 김두영 PL님 | **팀 명** | 알파고를 이을 악파고 |
| **프로젝트 주제** | MITRE ATT&CK TTPs 행위 분석  데이터(capa-rule)를 활용한 악  성코드 분석 및 머신러닝 기반  악성코드 탐지 | **제출일** | 2024.06.28. |
| **팀원** | 오태호(참여), 김상훈(참여), 김나연(참여), 임나현(참여),허라영(참여), 이시언(참여) | | |
| **추진현황** | 1. 데이터셋 수집 완료   6월26일에 빅데이터 센터에 방문하여 최종 데이터를 수거하여 왔습니다.   1. 사이트 제작   PE파일을 넣어 서버에서 모델을 돌려 해당 파일의 바이러스 유뮤를 판별하는 사이트를 Python Flask를 이용하여 만들기로 결정함. 데이터 전처리팀이 맡아, 현재 스티디 진행중입니다.   1. 데이터 엔지니어링 및 모델 학습   원핫-차원축소 등을 이용하여 데이터 엔지니어링을 거의 마무리단계 수순을 밟고 있습니다. 코렙과 AWS의 Sage Maker를 활용하여 다양한 머신러닝 기법을 활용하여 제작중입니다. 정확도는 XGBoost은 0.925 정도 나오며, , 지속적으로 정확도를 올릴 예정입니다. | | |

|  |
| --- |
| **활동사진**  **(회의 사진 등)** |
|  |