**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** | 2024.05.17. |
| **팀원** | 오태호(참여), 김상훈(참여), 김나연(참여), 임나현(참여), 허라영(참여), 이시언(참여) | | |
| **추진현황** | 데이터 전처리팀(오태호,김상훈,임나현)과 AI모델팀(김나연,허라영,이시언)을 구성하여 스터디를 진행하였습니다.   1. 데이터 전처리팀  * CAPA-RULE의 사용법과 효율적 분석법 * CAPA-RULE 추출 결과를 CSV에 저장법  1. AI 모델팀  * 넘파이, 판다스 학습 * CSV 텍스트 형태의 데이터셋 * 지도학습(Random Forest, LGBM, XGBOOST 위주) * 딥러닝 (텍스트 형태의 데이터셋 학습 가능한 모델 위주)   다음주부터 본격적으로 정상/악성 데이터 수집, 모델 개발을 진행할 예정입니다. | | |

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