**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** | 2024.05.31. |
| **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 이전에 구성한 것처럼 진행하여 스터디를 완료하였습니다.   1. 악성코드 수집   5/22에 사이버 보안 빅데이터 센터에 방문하여 신청한 데이터 셋에 대해 CAPA-RULE을 돌렸습니다. 이후 센터에 분석 프로그램을 남겨, 센터에서 다돌리면 연락을 주실 예정입니다. 현재 8514개 수집되었습니다.   1. 정상 데이터 수집   사이버 빅데이터 센터의 정상 셋과 SourceForge, 공인된 프로그램(Chrome, Steam 등), 윈도우 기본 프로그램에 대해 지속적으로 수집 중에 있습니다. 현재 2023개 수집되었습니다.   1. 데이터 전처리   수집한 데이터를 수치형 데이터 등으로 변환작업을 진행중입니다. | | |

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