

AI기반 악성코드 탐지기술 학계 기술전수

□ 주요내용

- (제공범위) AI기반 악성코드 탐지기술 이론·실습·챌린지
 - AI기반 악성코드 탐지모델 및 사이버보안 AI기술 트렌드 및 방법론 교육
 - AI기반 악성코드 탐지 시스템 실습환경 제공 및 실습 가이드
 - 데이터셋(악성·정상코드 50,000개) 제공 및 기술 검증을 위한 정보보호 R&D 데이터 챌린지 대회 시스템 이용권한 부여 및 가이드
- (대학 준비사항) 강의실, 강의환경, 저장매체
 - 실습에 활용할 VMware가 설치되어 있는 PC 또는 학생 개인 노트북
 - 악성/정상코드 데이터셋 50,000개(14.36GB), 탐지시스템 이미지파일 (5.87GB), 가이드라인 저장용 및 배포용 30GB 이상의 저장매체

□ 상세 프로그램

| 단계 | 기술전수 내용 |
|------------------|---|
| 이론 (1시간) | 악성코드 분석론, AI 알고리즘 등 악성코드 탐지 기술 교육 * AI기반 사이버보안 분야 및 악성코드 분석 Feature, AI 기술 트렌드 등 * 정보보호 R&D 데이터 챌린지 소개 및 교육용 시스템 참여 방법 교육 |
| 실습 (1시간) | AI기반 악성코드 탐지 시스템 실험 환경 구성 및 사용법 교육 * 실습환경 구성이 불가능한 경우(PC 미설치 등) AI기반 악성 코드 탐지 시스템 가이드라인 설명 및 챌린지 시스템 이용 안내 교육으로 대체 |
| 챌린지 (교내 자유일정) | 정보보호 R&D 데이터 챌린지 대회 플랫폼을 활용한 교내 AI기반 악성코드 탐지 기술 챌린지 개최 |

※ 대학 별 세부 일정은 대학 강의 시간에 맞춰 변경 가능

- (챌린지) 교내 챌린지 담당자가 일정을 선택하여 대회 실시

