47 NLP 기반 PowerShell 악성 스크립트 탐지 툴 개발

소속 정보컴퓨터공학부 분과 D 팀명 어쩔보안 참여학생 김서영, 박지연, 최연재 지도교수 최윤호

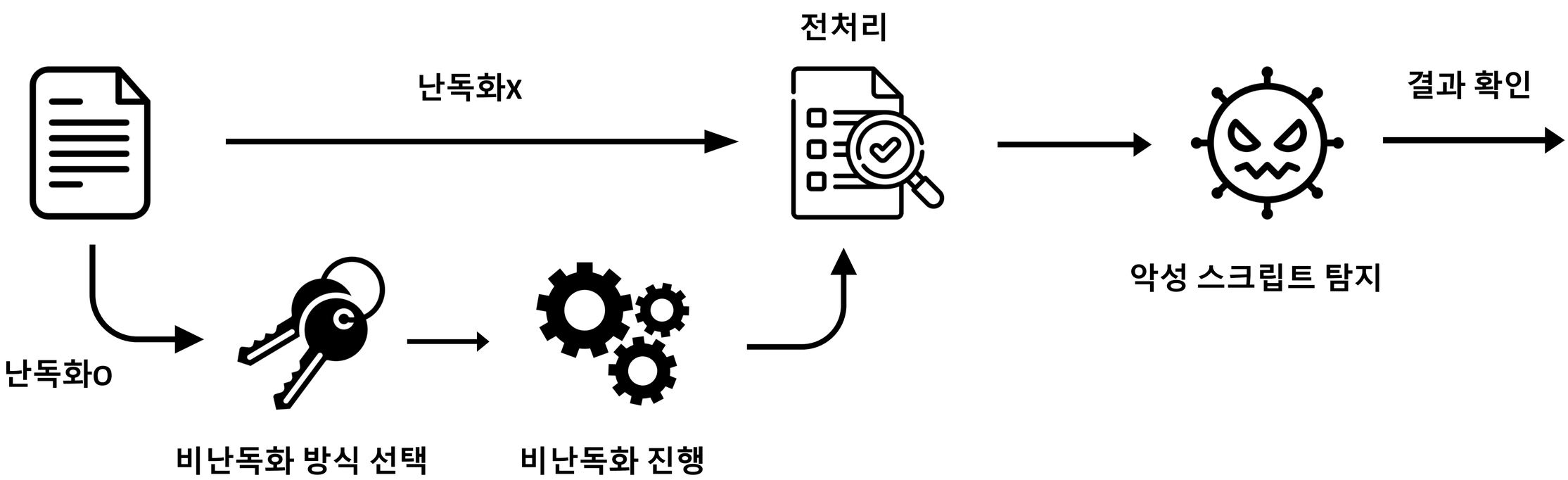
과제 목표

❖ 난독화 스크립트 분석을 위한 비난독화 모듈 개발

❖ 딥 러닝 / 머신 러닝 기법을 활용한 악성 스크립트 분류 모듈 개발

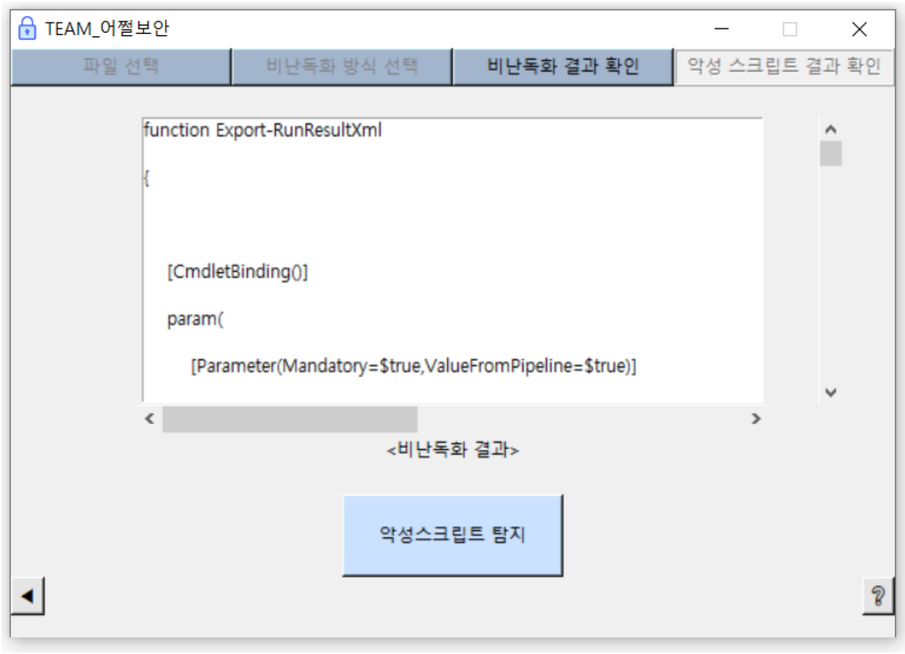
❖ GUI 시각화 도구 개발

시스템 구성

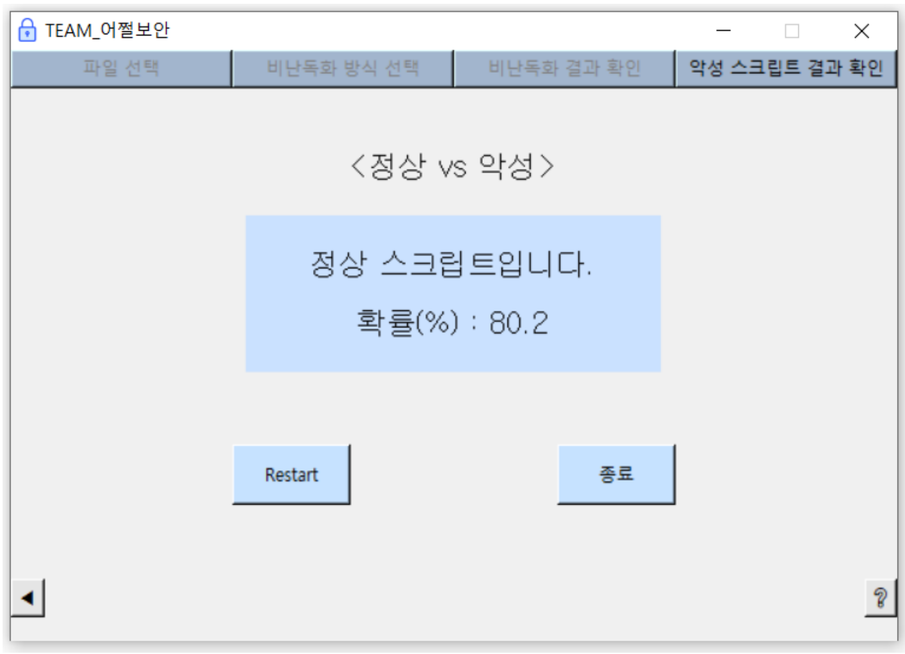


1. 비난독화는 BASE64와 16진수를 이용한 방식으로 진행된다.
2. PowerShell 스크립트에서 필요한 명령어만을 뽑아내는 전처리 과정을 거친다.
3. AdaBoost, GBM, XGBoost 세가지를 앙상블한 모델을 사용하여 악성 스크립트를 탐지한다.

과제 결과



<비난독화 결과>



<악성 스크립트 탐지 결과>

1. 비난독화된 스크립트의 결과를 확인할 수 있다.
2. 머신러닝을 활용한 앙상블 모델로 악성 스크립트를 탐지하고 그에 해당하는 확률을 확인할 수 있다.