



# Capa-rule과 머신러닝을 활용한 악성코드 분석 및 탐지

MITRE ATT&CK TTPs 행위분석데이터(capa-rule)

WhiteHat School 2기 악파고팀

악파고

# CONTENTS

화이트햇 스쿨  
WhiteHat School



## 01 / 프로젝트 개요

- 팀 소개
- 프로젝트 배경
- 프로젝트 소개
- 프로젝트 진행 요약

## 02 / 프로젝트 수행

- 프로젝트 개념도
- 데이터 수집 프로세스
- 인공지능 모델 개발 프로세스

## 03 / 프로젝트 성과

- 프로젝트의 의의
- 웹 사이트 제작

## 04 / 프로젝트 추후계획

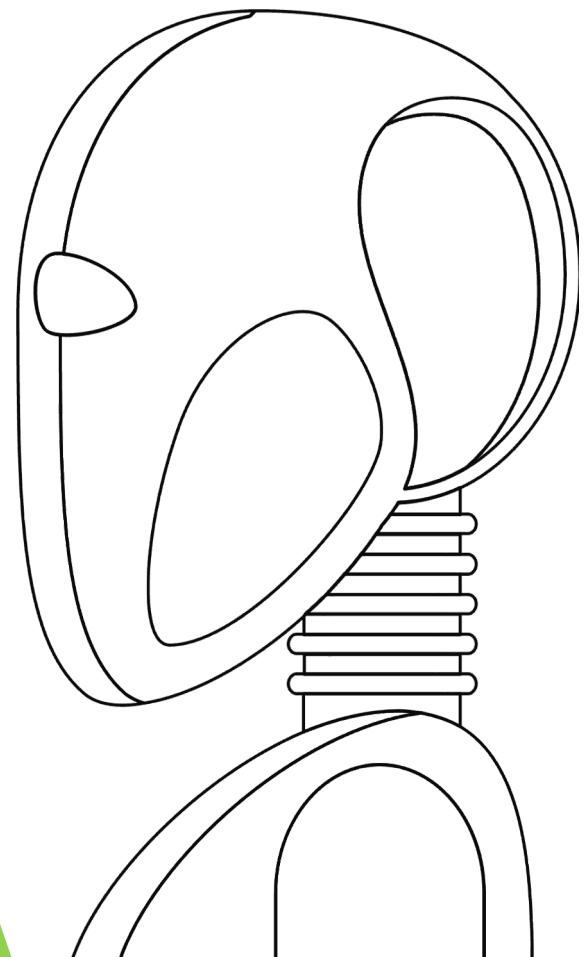
- 앞으로의 계획

•  
•  
•

# 1. 프로젝트 개요

- 팀 소개
- 프로젝트 배경
- 프로젝트 소개
- 프로젝트 진행 요약

⋮

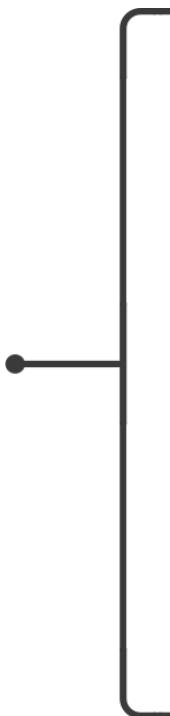


# 팀 소개

악파고 팀은 데이터 전처리팀 3명, AI모델개발팀 3명으로 구성되어 있습니다.



악파고



Mentor



손승호

PL



김두영

PM



오태호

팀원



임나현



김상훈



김나연



이시언



허라영



# 프로젝트 배경

프로젝트 주제 선정 배경입니다.

고도화 악성코드 사전 유입…대응 쉽지 않아

2013-03-20 17:13:53

[보안칼럼] 난독화된 악성앱, AI 기술로  
분석 AI로 사이버위협 사전 탐지…KISA, 데이터셋 구축한다

속수무  
악성코  
에 대비  
정부 힘  
조직의  
또 해커  
설명했  
피해사  
정상적  
마' 방소  
PC가 4  
등 추가  
정부는  
[박재윤  
영카인  
나라 흥  
보안 솔루션  
1일 정부  
회'를 우

올해 들어 랜섬웨어(Ransomware)를 비롯해 다양한 신·변종 악성코드가 범람하면서 보안 업계에 '화이  
하루에도 수십만개의 악성코드가 새로 등장하면서 특정 위협이 갖는 행동양식을 데이터베이스(DB)로 만  
막는 것이 사실상 불가능하다는 판단에서다.

한국인  
응할 수  
최우선!  
이다.  
보안 업계에 따르면, 세계적으로 누적된 악성코드의 수는 5억개에 달하며 매달 1000만개의 새로운 악성  
전통적인 백신(안티바이러스) 솔루션은 유입된 파일이나 공격을 미리 만들어둔 악성코드 DB와 대조해  
악성코드라면 가장 확실하게 차단할 수 있다는 것이다. 대신 해당 보안 기업이 미처 분석하지 못한 일려자

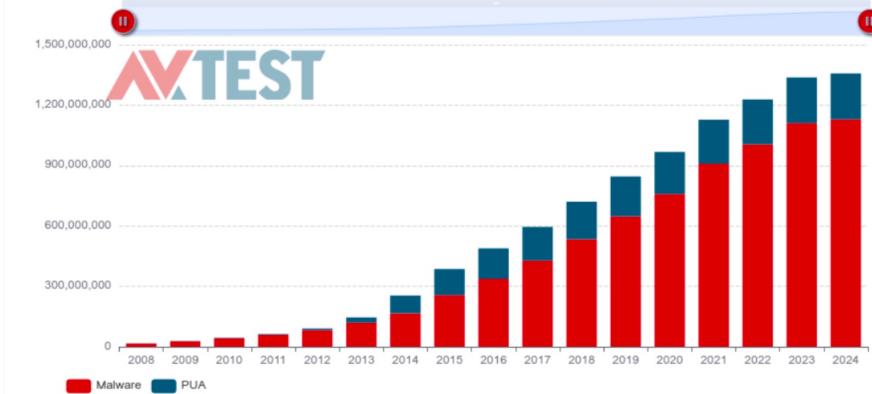
f 최고관리자  
연구  
챗GF  
이전글  
다음글



## 매년 새로운 악성코드 수 증가

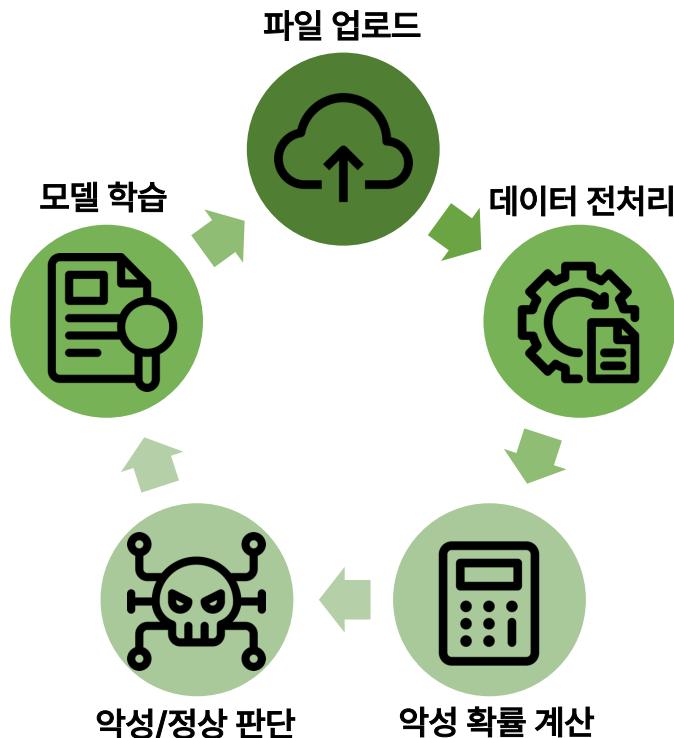
새로운 악성코드 등장 시  
패턴 분석까지의 무방비 구간 존재

TOTAL AMOUNT OF MALWARE AND PUA



# 프로젝트 소개

카파룰(capa-rule)을 이용한 악성코드 분석 및 탐지하는 기능을 제공합니다.



지속적인 AI 모델 학습을  
통한 성능 향상 및 속도 개선

# 프로젝트 진행 요약

저희 프로젝트 진행 현황의 요약입니다.



# 프로젝트 진행 요약

저희 프로젝트 진행 현황의 요약입니다.

화이트햇 스쿨  
WhiteHat School



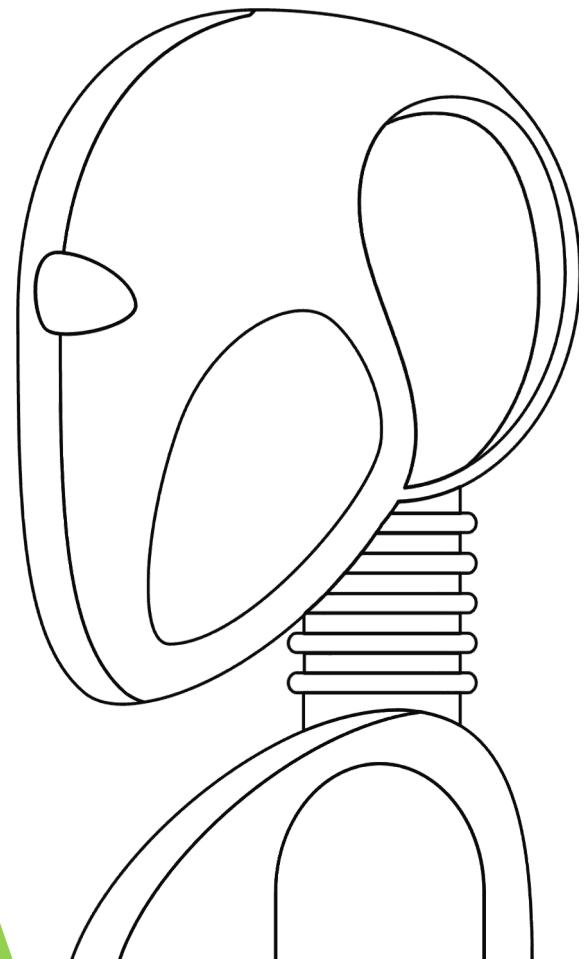
사전계획대비 100% + α 수행



## **2. 프로젝트 수행**

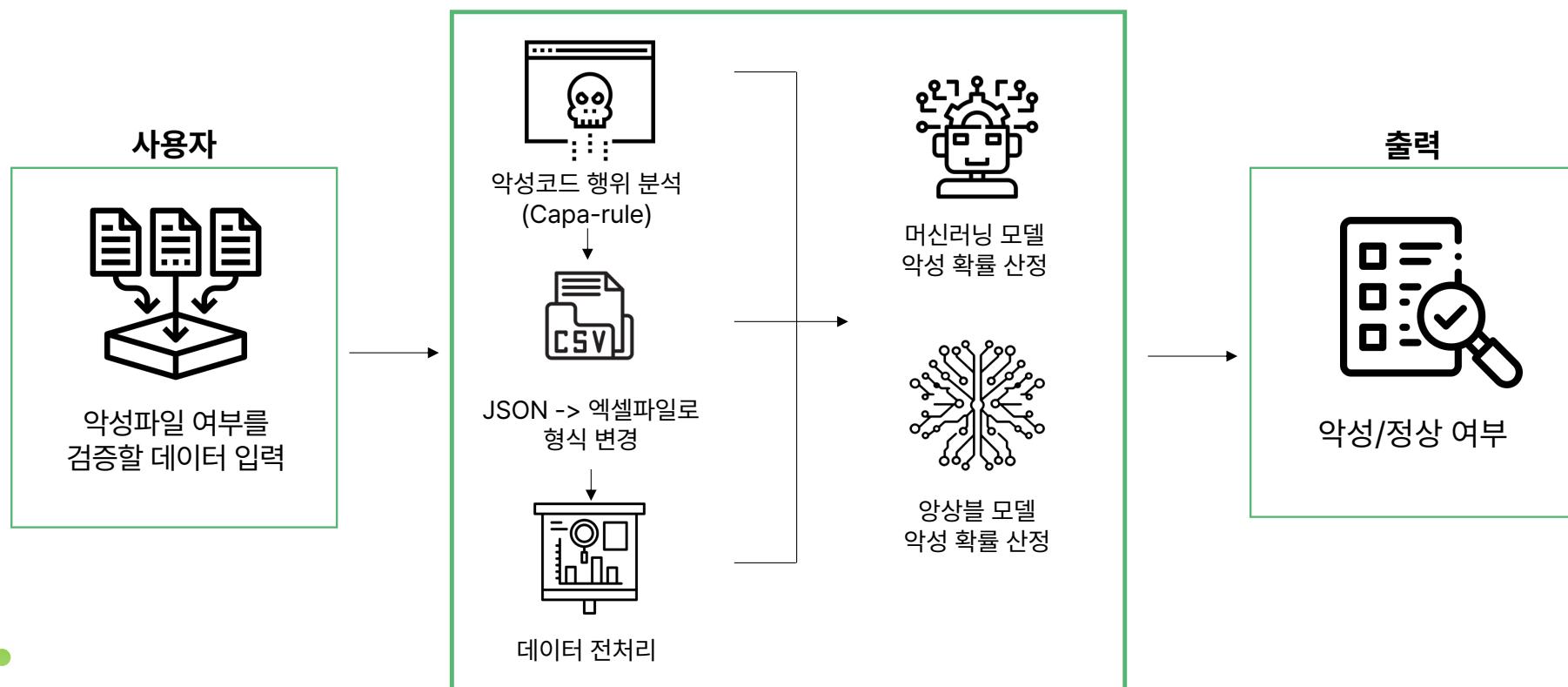
- 프로젝트 개념도
- 데이터 수집 프로세스
- 인공지능모델 개발 프로세스

⋮



# 프로젝트 개념도

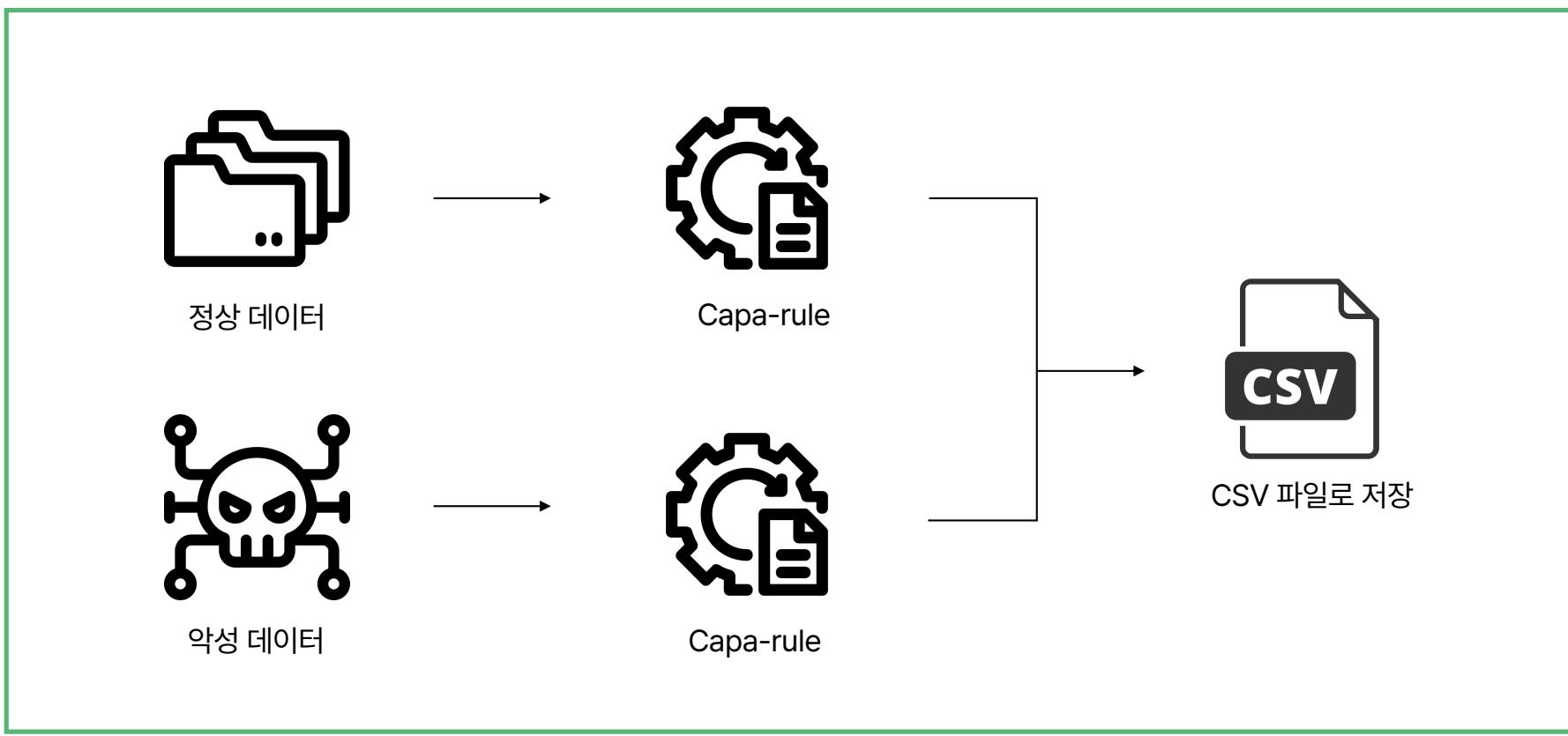
저희가 제시하는 프레임워크 개념도입니다.



- 
- 
-

# 데이터 수집

데이터 전처리를 위한 정상/악성 데이터셋 수집 과정입니다.



# 데이터 수집

Capa-rule 결과에서 가져오는 값들입니다.

화이트햇 스쿨  
WhiteHat School



ATT&CK Tactic	ATT&CK Technique
DEFENSE EVASION	Deobfuscate/Decode Files or Information T1140 Obfuscated Files or Information T1027 Obfuscated Files or Information::Indicator Removal from Tools T1027.005
DISCOVERY	File and Directory Discovery T1083 Process Discovery T1057 Query Registry T1012 Software Discovery T1518 System Information Discovery T1082 System Network Configuration Discovery T1016
EXECUTION	Shared Modules T1129
MBC Objective	MBC Behavior
ANTI-STATIC ANALYSIS	Executable Code Obfuscation::Argument Obfuscation [B0032.020] Executable Code Obfuscation::Stack Strings [B0032.017]
COMMAND AND CONTROL	C2 Communication::Send Data [B0030.001]
Capability	Namespace
contain obfuscated stackstrings get MAC address on Windows send data (5 matches) resolve DNS get HTTP content length	anti-analysis/obfuscation/string/stackstring collection/network communication communication/dns communication/http

# 데이터 수집

수집한 정상/악성 데이터셋들의 출처입니다.



## 정상 데이터셋

43455개

- KISA 보호나라
- Window OS
- 공인 프로그램

## 악성 데이터셋

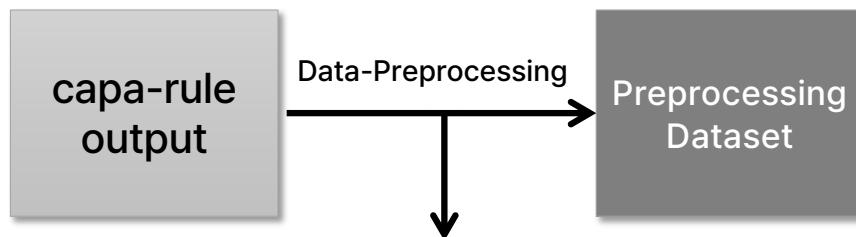
52706개

- KISA 사이버 보안 빅데이터 센터
- Malware Bazaar



# 인공지능모델 개발 – 데이터 전처리

수집한 데이터셋을 활용한 머신러닝 모델 개발 과정입니다.



Entropy	ATT&CK	MBC	Namespace	Capability
추출된 원본 데이터 활용			상위 디렉토리만	수량 정보만 추출

**Dataset1** : Accuracy 0.9453

Entropy	ATT&CK	MBC	Namespace	Capability
수치형 데이터			범주형 데이터(원핫 인코딩만)	

**Dataset2** : Accuracy 0.9465

Entropy	ATT&CK	MBC	Namespace	Capability
수치형 데이터			범주형 데이터(차원 축소)	

**Dataset3** : Accuracy 0.9479

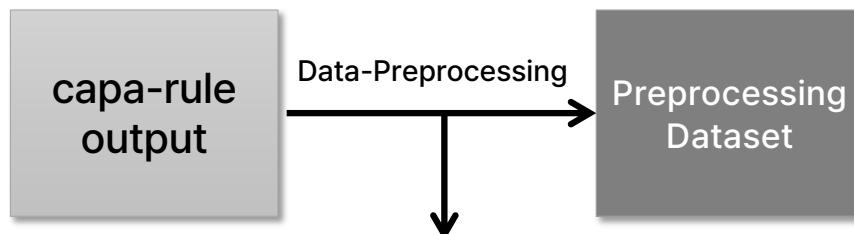
Entropy	Namespace	ATT&CK	MBC	Namespace	Capability
수치형 데이터	범주형 데이터(원핫 인코딩만)			범주형 데이터(원핫인코딩 + 차원 축소)	

● **Dataset4** : Accuracy 0.9475

Entropy	ATT&CK Tactic, MBC Objective, Namespace	ATT&CK Technique, MBC Behavior, Capability
수치형 데이터	범주형 데이터(원핫 인코딩만)	범주형 데이터(원핫인코딩 + 차원 축소)

# 인공지능모델 개발 – 데이터 전처리

수집한 데이터셋에 대한 학습 전 데이터 전처리 과정입니다.



**Dataset1** : Accuracy 0.9453

Entropy	ATT&CK	MBC	Namespace
수치형 데이터	범주형 데이터(원핫 인코딩)		

**Dataset2** : Accuracy 0.9465

Entropy	ATT&CK	MBC	Namespace	Capability
수치형 데이터	범주형 데이터(차원 축소)			

**Dataset3** : Accuracy 0.9479

Entropy	Namespace	ATT&CK	MBC	Namespace	Capability
수치형 데이터	범주형 데이터(원핫 인코딩만)				

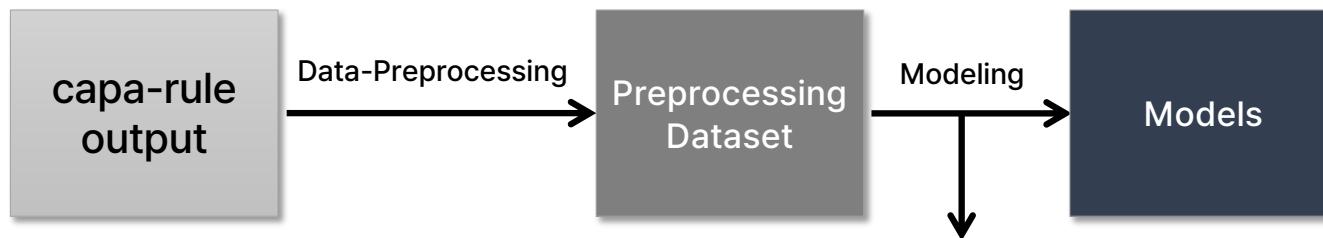
● **Dataset4** : Accuracy 0.9475

Entropy	ATT&CK Tactic, MBC Objective, Namespace	ATT&CK Technique, MBC Behavior, Capability
수치형 데이터	범주형 데이터(원핫 인코딩만)	범주형 데이터(원핫인코딩 + 차원 축소)

정확도가 가장 높은  
데이터셋3로 결정!

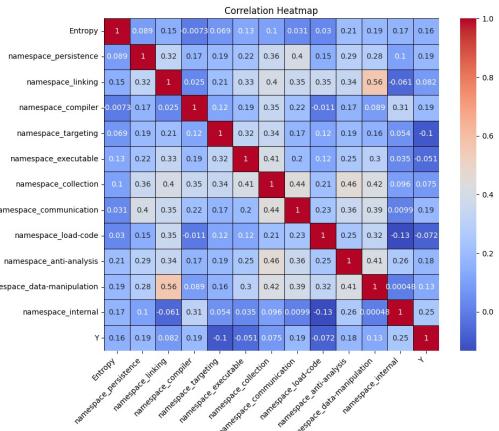
# 인공지능모델 개발 – 머신러닝 모델

수집한 데이터셋을 활용한 머신러닝 모델 학습 과정입니다.



## Y-Namespace Correlation

- 상관 계수 0.05이하 삭제



## 하이퍼파라미터 튜닝

- Bayesian Optimization
- Grid Search



### Bayesian Optimization 검색공간

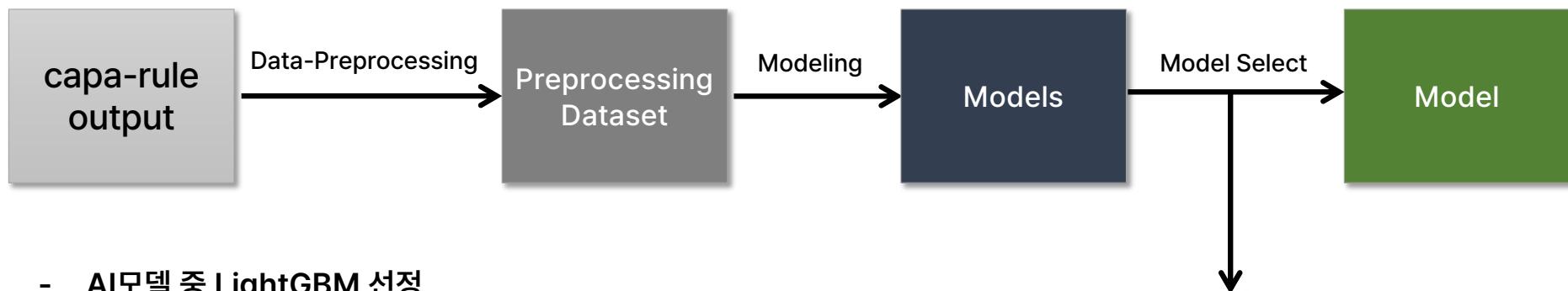
```
param_space = {  
    'model__n_estimators': Integer(50, 300),  
    'model__max_depth': Integer(3, 20),  
    'model__min_samples_split': Integer(2, 10),  
    'model__min_samples_leaf': Integer(1, 10),  
    'model__max_features': Categorical(['sqrt', 'log2']),  
    'model__bootstrap': Categorical([True, False])  
}
```

### <하이퍼파라미터 튜닝>

```
params = {  
    'max_depth' : [11, 12, 13, 14, 15, 16, 17, 18, 19, 20],  
    'num_leaves' : [64, 128, 256, 512],  
    'boosting_type' : ['gbdt', 'dart', 'goss'],  
    'feature_fraction' : [0, 0.63, 0.65, 0.67, 0.69, 1],  
    'bagging_fraction' : [0, 0.63, 0.65, 0.67, 0.69, 1],  
    'num_iterations' : [100, 200, 300, 400, 500, 1000],  
    'learning_rate' : [0.01, 0.02, 0.03, 0.04, 0.05]  
}
```

# 인공지능모델 개발 – 머신러닝 모델

최종 머신러닝 모델 선정입니다.



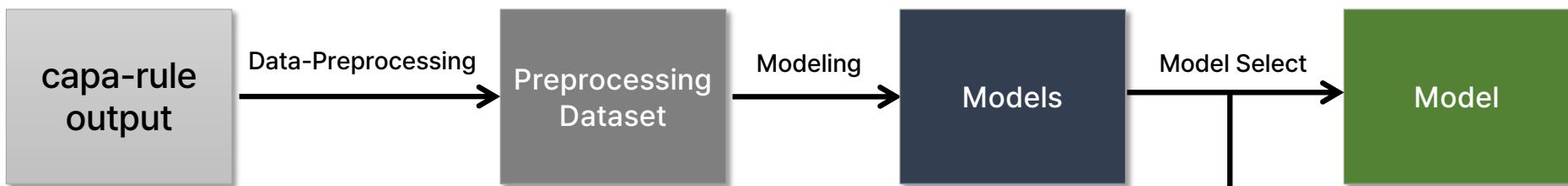
- AI모델 중 LightGBM 선정
- 악성 확률 측정

Model	Accuracy (정확도)	Precision (정밀도)	Recall (재현율)	F1-score
XGBoost	0.9465	0.9431	0.9395	0.9413
LightGBM	0.9503	0.9472	0.9438	0.9455
Random Forest	0.9459	0.9489	0.9318	0.9413
CatBoost	0.9439	0.9465	0.9414	0.9439



# 인공지능모델 개발 – 머신러닝 모델

최종 머신러닝 모델 선정입니다.



- AI모델 중 LightGBM 선정
- 악성 확률 측정

Model	Accuracy (정확도)	Precision (정밀도)	Recall (재현율)	F1-score
XGBoost	0.9465	0.9431	0.9395	0.9413
LightGBM	0.9503	0.9472	0.9438	0.9455
Random Forest	0.9459	0.9489	0.9318	0.9413
CatBoost	0.9439	0.9465	0.9414	0.9439



file id : ae13e0, 실제값 : 1.0, 예측값 : 1.0, 악성 확률 : 99.07%
file id : e1f1a8, 실제값 : 1.0, 예측값 : 1.0, 악성 확률 : 99.95%
file id : b9e2d6, 실제값 : 0.0, 예측값 : 0.0, 악성 확률 : 0.36%
file id : 5f1b35, 실제값 : 0.0, 예측값 : 0.0, 악성 확률 : 2.39%
file id : a54197, 실제값 : 1.0, 예측값 : 1.0, 악성 확률 : 99.91%
file id : b23449, 실제값 : 1.0, 예측값 : 1.0, 악성 확률 : 96.39%
file id : b04ca7, 실제값 : 1.0, 예측값 : 1.0, 악성 확률 : 98.21%
file id : 8cc543, 실제값 : 0.0, 예측값 : 0.0, 악성 확률 : 34.77%
file id : 2c7e8d, 실제값 : 1.0, 예측값 : 1.0, 악성 확률 : 97.56%

<악성확률 측정 결과>

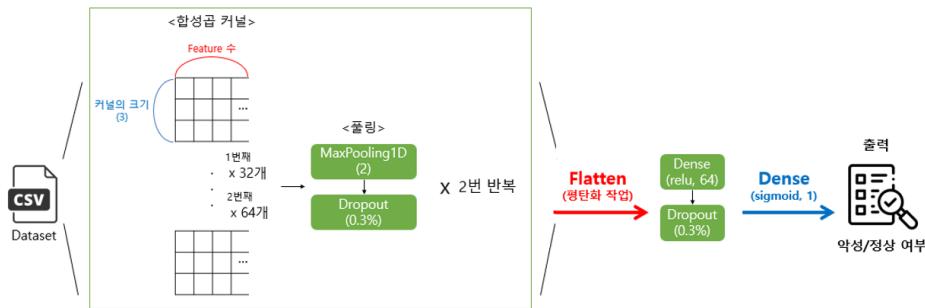
# 인공지능모델 개발 – 암상블 모델

머신러닝/딥러닝 암상블 모델 개발 과정입니다.

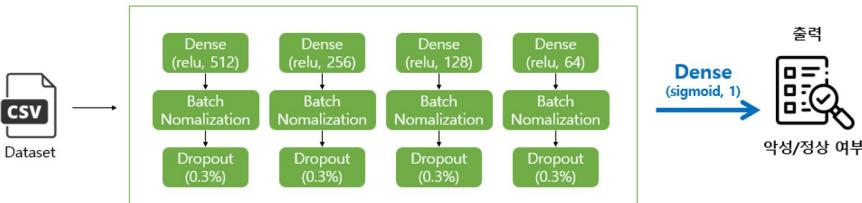


- 스테킹 암상블 사용
- 딥러닝(Keras,CNN) 모델 제작
- 암상블한 모델과 전체 모델 성능 비교해 최종 모델 선정

## CNN layer



## Keras layer



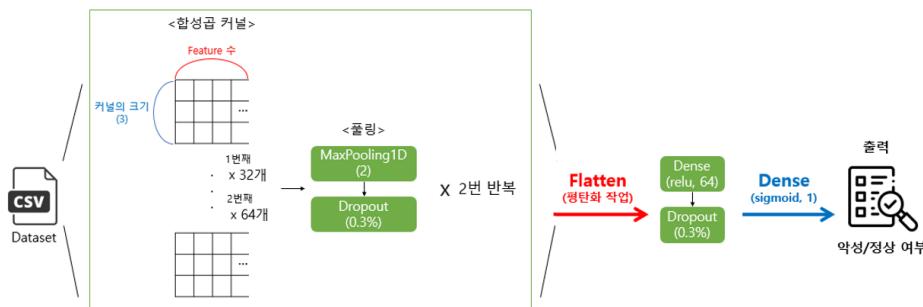
Model	Accuracy
LightGBM	0.9503
Keras	0.8796
CNN	0.9030
LightGBM + Keras	0.9506
LightGBM + CNN	0.9548
LightGBM + CNN + Keras	0.9507

# 인공지능모델 개발 – 암상블 모델

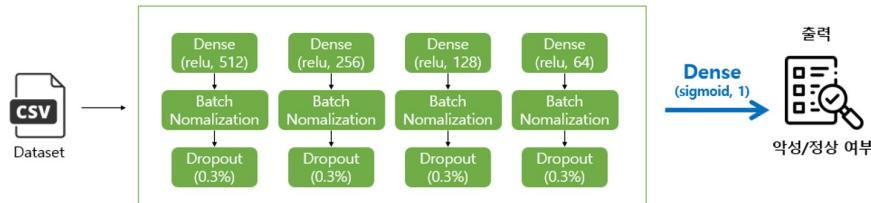
머신러닝/딥러닝 암상블 모델 개발 과정입니다.

- 딥러닝(Keras,CNN) 모델 제작
- 스테킹 암상블 사용
- 암상블한 모델과 전체 모델 성능 비교해 최종 모델 선정

## CNN layer



## Keras layer



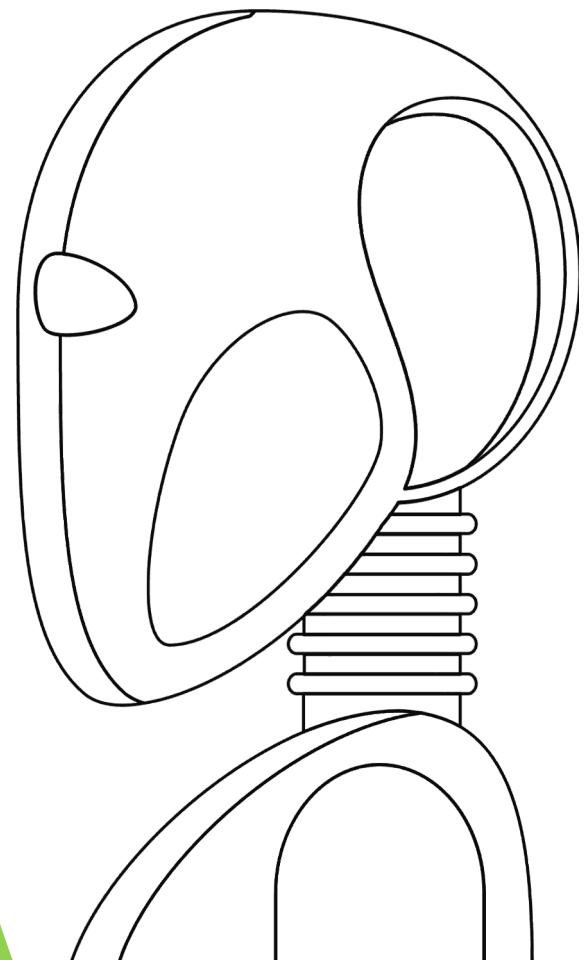
Model	Accuracy
LightGBM	0.9503
Keras	0.8796
CNN	0.9030
LightGBM + Keras	0.9506
<b>LightGBM + CNN</b>	<b>0.9548</b>
LightGBM + CNN + Keras	0.9507

**정확도  
95.5% 달성**

### **3. 프로젝트 성과**

- 프로젝트의 의의
- 웹사이트 제작

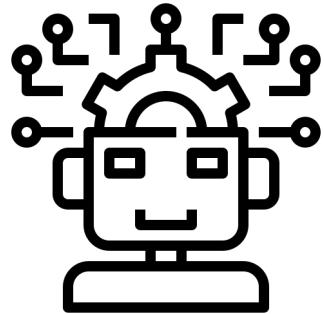
⋮



# 프로젝트의 의의

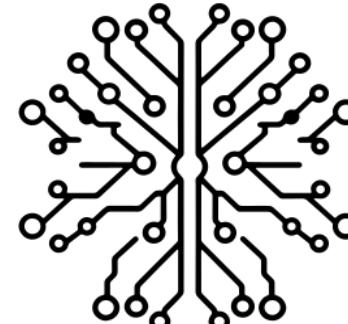
프로젝트를 통해 도출한 결론입니다.

화이트햇 스쿨  
WhiteHat School



머신러닝 모델

VS



양상블 모델

**정확도 95.03%**

**정확도 95.50%**

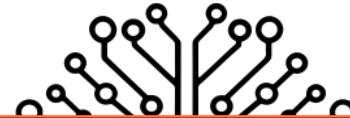
- 머신러닝 모델 LGBM을 활용했을 때, 약간의 과적합이 있음을 확인
- 과적합을 해결하기 위해 딥러닝 알고리즘 내 드롭아웃 기법 활용
- 이를 통해 양상블을 진행하여 과적합이 일정 부분 해결된 양상블 모델을 선정



# 프로젝트의 의의

프로젝트를 통해 도출한 결론입니다.

화이트햇 스쿨  
WhiteHat School



탐지 기술에서 양상을 모델의  
활용 가능성 존재!

**정확도 95.03%**

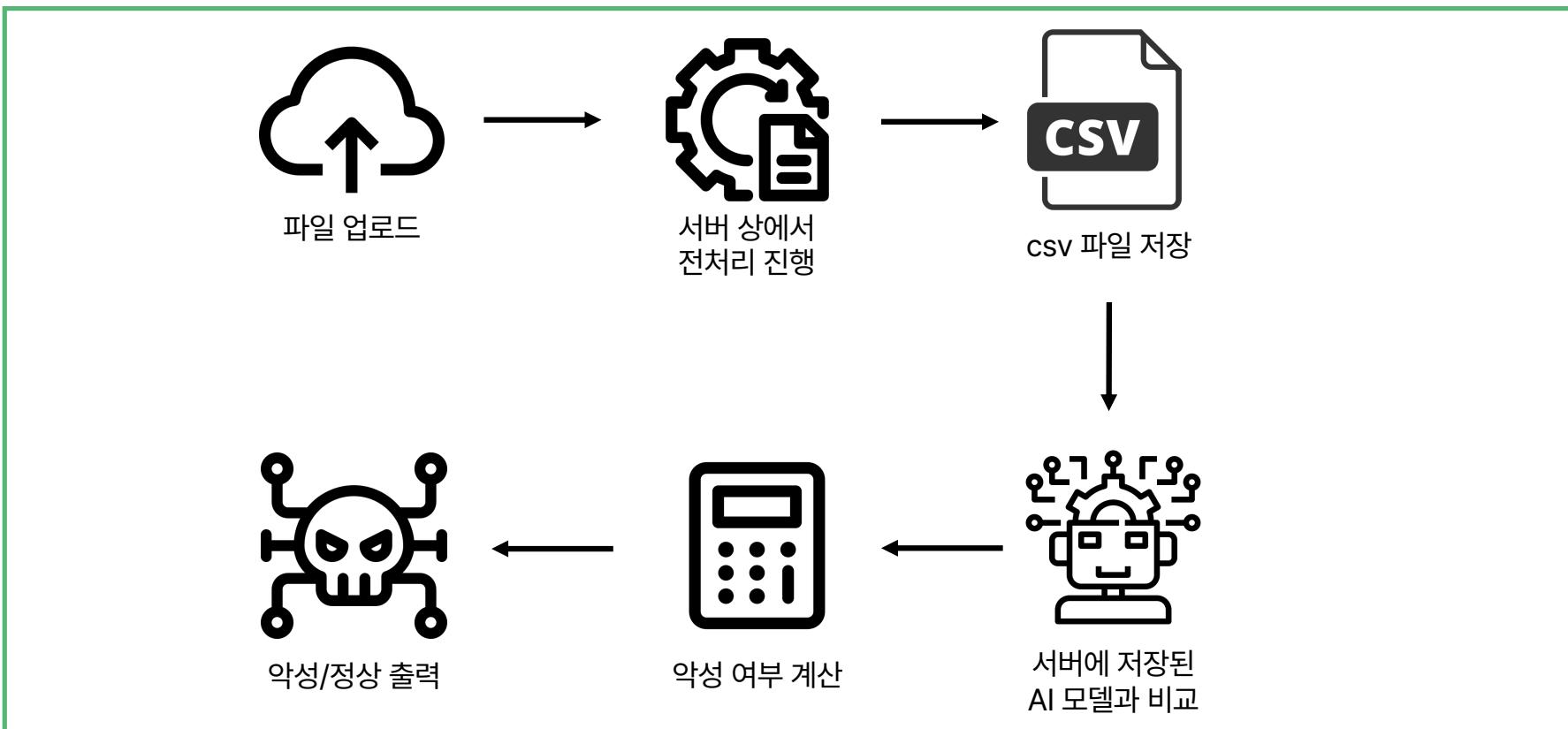
**정확도 95.50%**

- 머신러닝 모델 LGBM을 활용했을 때, 약간의 과적합이 있음을 확인
- 과적합을 해결하기 위해 딥러닝 알고리즘 내 드롭아웃 기법 활용
- 이를 통해 양상을 진행하여 과적합이 일정 부분 해결된 양상을 모델을 선정



# 웹사이트 제작

Flask를 통한 웹사이트 제작 후, 파일을 업로드하여 악성/정상 유무를 판단합니다.

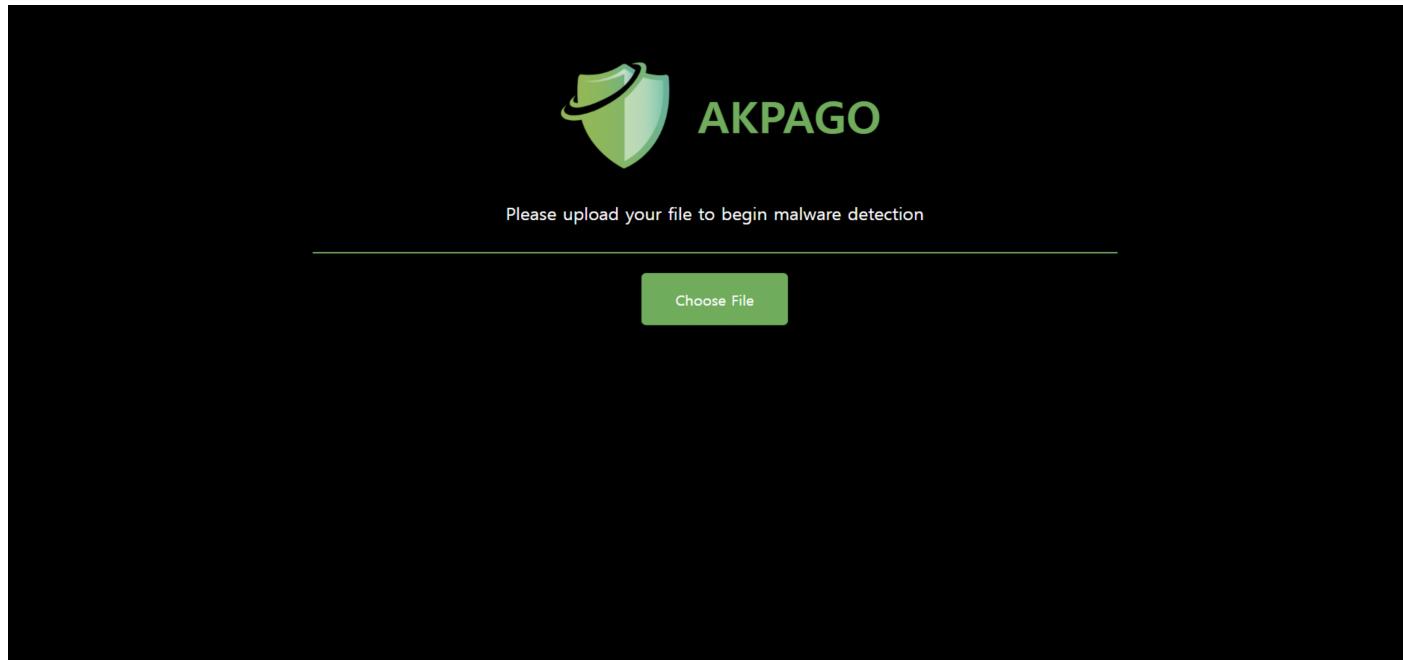


# 웹사이트 제작

Flask를 통한 웹사이트 제작 후, 파일을 업로드하여 악성/정상 유무를 판단합니다.



## 1. 웹사이트 접속 후 파일 선택 클릭



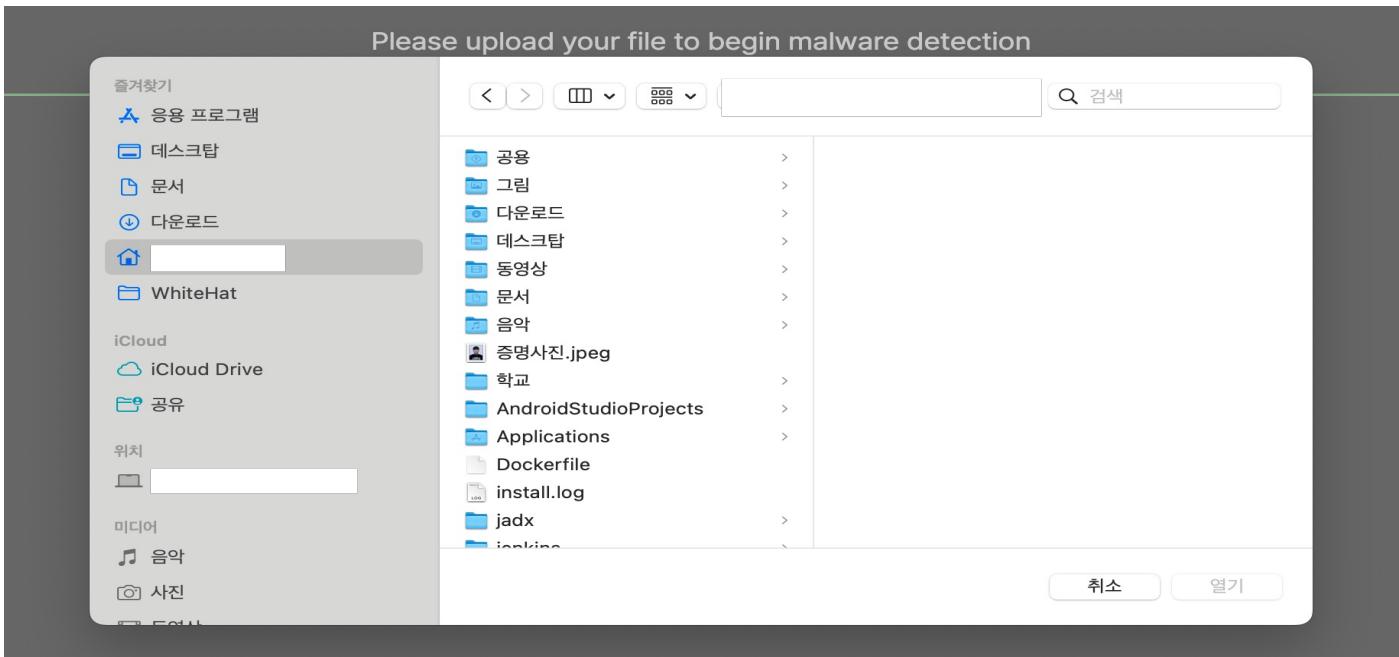
- 
- 
-

# 웹사이트 제작

Flask를 통한 웹사이트 제작 후, 파일을 업로드하여 악성/정상 유무를 판단합니다.



## 2. 분석하고자 하는 파일 선택

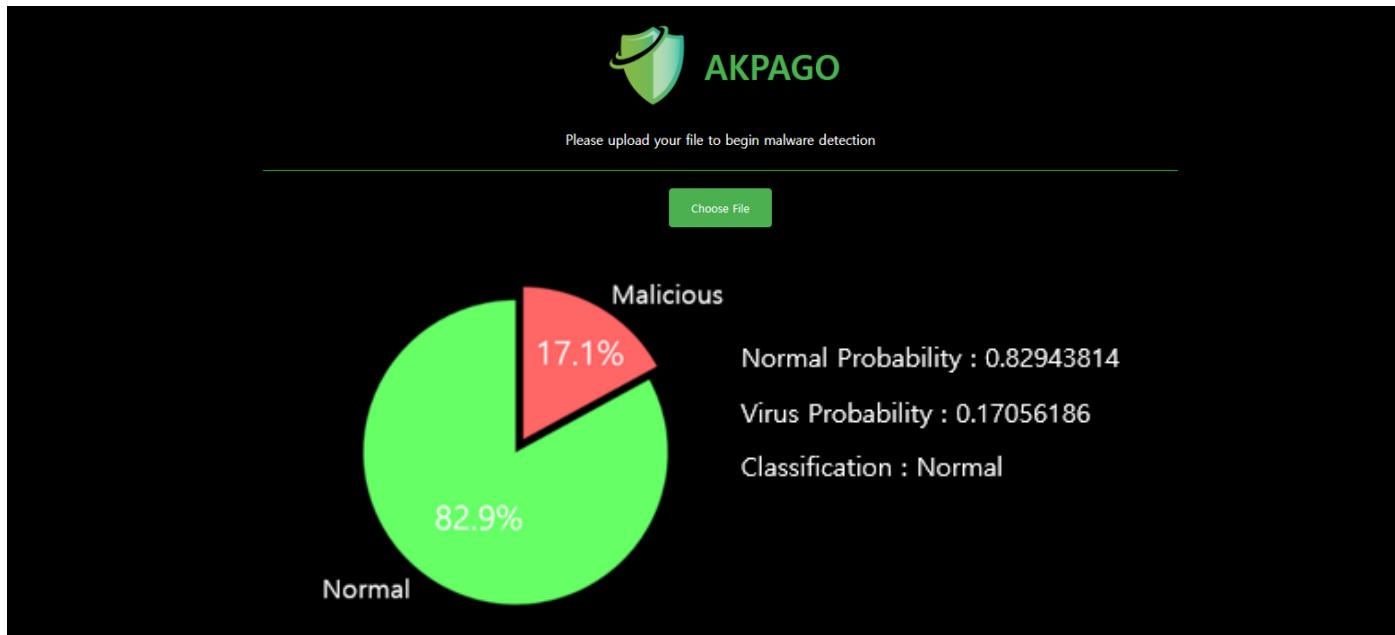


# 웹사이트 제작

Flask를 통한 웹사이트 제작 후, 파일을 업로드하여 악성/정상 유무를 판단합니다.

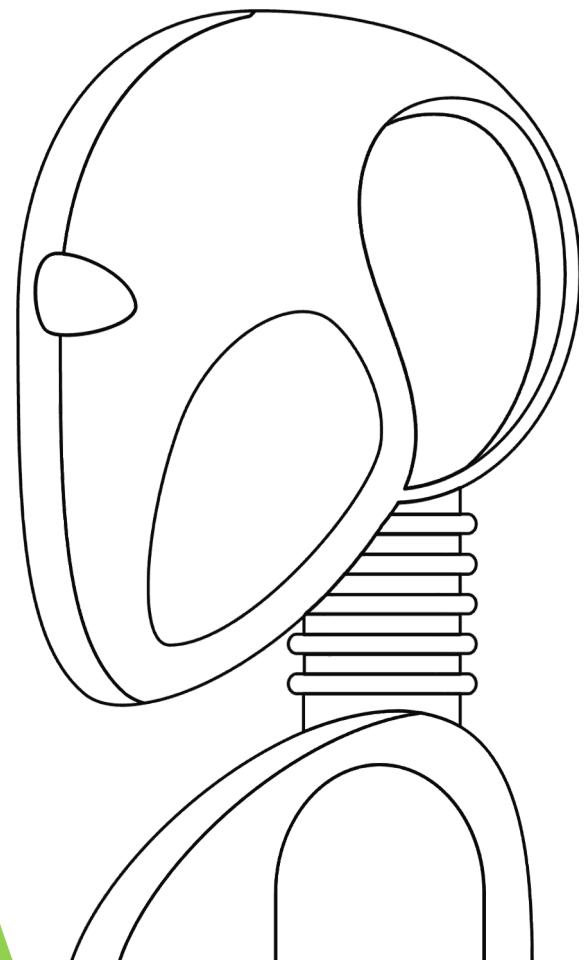


## 3. 정상/악성 데이터 여부 판단



## **4. 프로젝트 추후 계획**

- 앞으로의 계획



# 앞으로의 계획

프로젝트 최종 평가 이후 계획입니다.

화이트햇 스쿨  
WhiteHat School



## 기능 고도화

- 양상블에 사용된 딥러닝 모델 개선 및 추가적 튜닝을 통해 성능 향상
- 악성코드 탐지 AI를 활용한 앱 개발
- 악성코드 탐지 자동화
- 시각화 및 모니터링 시스템
- 악성코드 감지 경보 체계 구축

## 논문 작성

- 악성코드 탐지 기술에서 양상블 모델 활용 가능성에 대해 논문 작성



## 프로젝트 이후의 계획

## 악성 패키지 탐지

- 실제 공급망에서 악성 패키지 탐지 및 제보 진행

## 대외 활동

- 국제 산업보안 논문 경진대회
- KIISC, KSCI에 논문 투고 예정
- 영어 논문 작성 후, AAMAS, AAAI 등 논문 투고 예정



# 프로젝트를 마무리하며

프로젝트 진행하며 느낀 팀원들의 소감입니다.

화이트햇 스쿨  
WhiteHat School



## 김상훈

새로운 분야에 대해 알아갈 수 있던  
좋은 시간이었던 것 같습니다!! 재밌었다..

## 이시언

이번 기회를 통해 많은 것을 배웠으며,  
성장할 수 있었습니다. 또한 좋은 팀원분들과  
함께하여 의미있는 시간을 보낸 것 같습니다.

## 오태호

이번 프로젝트를 통해 고등학생 신분에서 가능한  
것을 뛰어 넘어 함으로써 배운 것이 많았습니다.  
팀원분들께서 열심히 해주셔 가지고 프로젝트 성  
과 또한 좋았던 것 같습니다.



## 임나현

이번 프로젝트로 짧은 시간에 많은 것을  
배워 빠르게 성장할 수 있었습니다. 다들 열심히  
하는 모습이 큰 자극이 되었습니다. 감사합니다.

## 허라영

처음에는 어떻게 해야 할지 막막했는데,  
다들 열심히 한 결과, 프로젝트를 완성할  
수 있었던 거 같습니다. 감사합니다!

## 김나연

많은 것들을 배울 수 있어 정말 뜻깊었습니다.  
함께 힘냈던 악파고 팀원들, 많은 도움을 주셨던  
손승호 멘토님과 김두영 PL님 모두 감사드립니다!

- 
- 
-



**Thank You**