캡스톤 디자인 2024-1 최종 발표

PLATFORM **GIPS**

생성형 침입방지 기술 기반 보안 플랫폼

| 국민대학교 정보보호연구실 & (주)누리랩 | 산학협력 34조 |

| 지도교수 윤명근 | 엄석현 김태경 김태윤 박준서 |

KMU 국민대학교 KOOKMIN UNIVERSITY

nurilab

CONTENTS

목차

PLATFORM **GIPS**

생성형 침입방지 기술 기반 보안 플랫폼

KMU 국민대학교 KOOKMIN UNIVERSITY

nurilab

프로젝트 배경

01

생성형 AI으로 인한 악성코드 **폭발적 증가**

- 공격자들의 생성형AI (WormGPT 등) 악용
- 변종 악성코드 대량 생산 및 유포 건수 증가

02

악성코드 대응을 위한 **보안인력 부족**

- 악성코드 발생 수는 하루 40~50만개
- 악성코드 발생 수 대비 보안인력 절대적 부족

03

사용자에게 **설명 가능한** 탐지방법 필요성 증대

- 악성코드를 판단한 기준 설명 필요성 증대
- 사용자에게 정확한 정보 제공 필요

프로젝트 목표

생성형 침입방지 기술기반 보안 플랫폼

PLATFORM **GIPS**

01

탐지 규칙 생성 및 적용

- 파일로부터 공통 시그니처 추출 후 탐지 규칙 생성
- 생성된 탐지 규칙을 적용하여 악성 파일 탐지

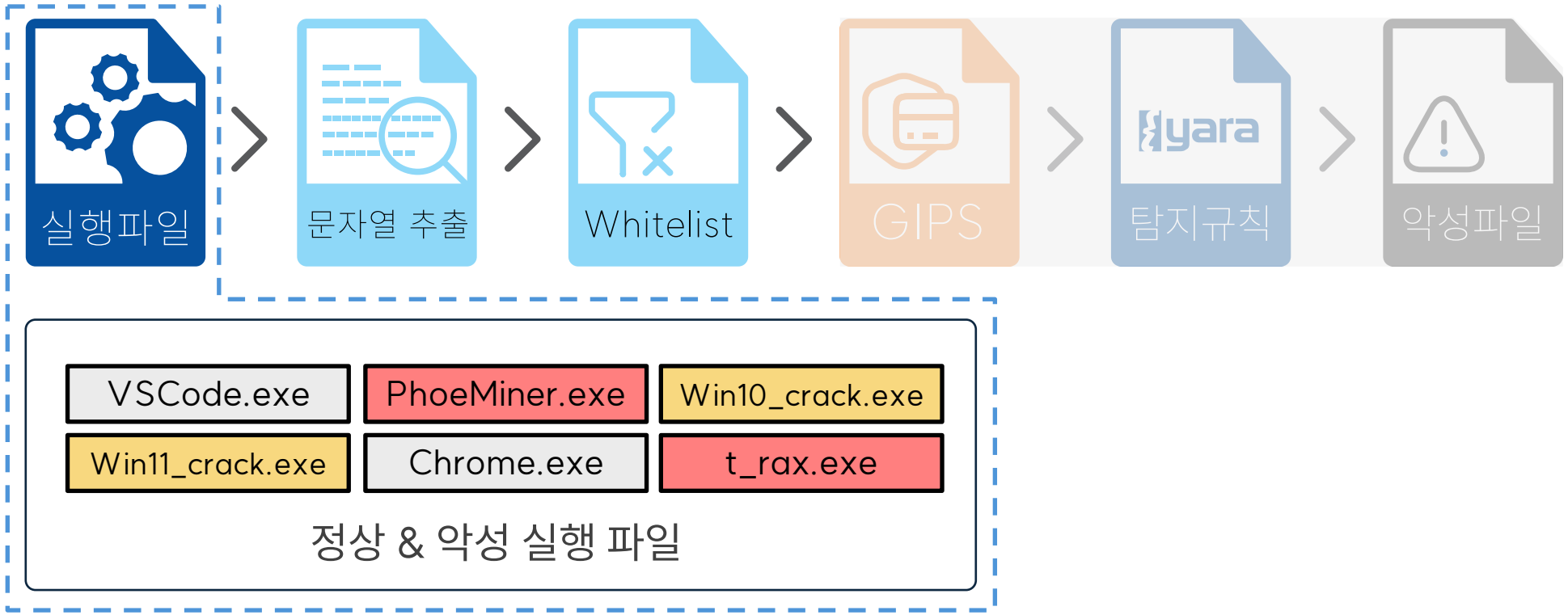
02

공격 시각화

- 다양한 기법으로 플랫폼에서 탐지한 공격을 시각화
- 보안 전문가가 위협을 시각적으로 파악 가능

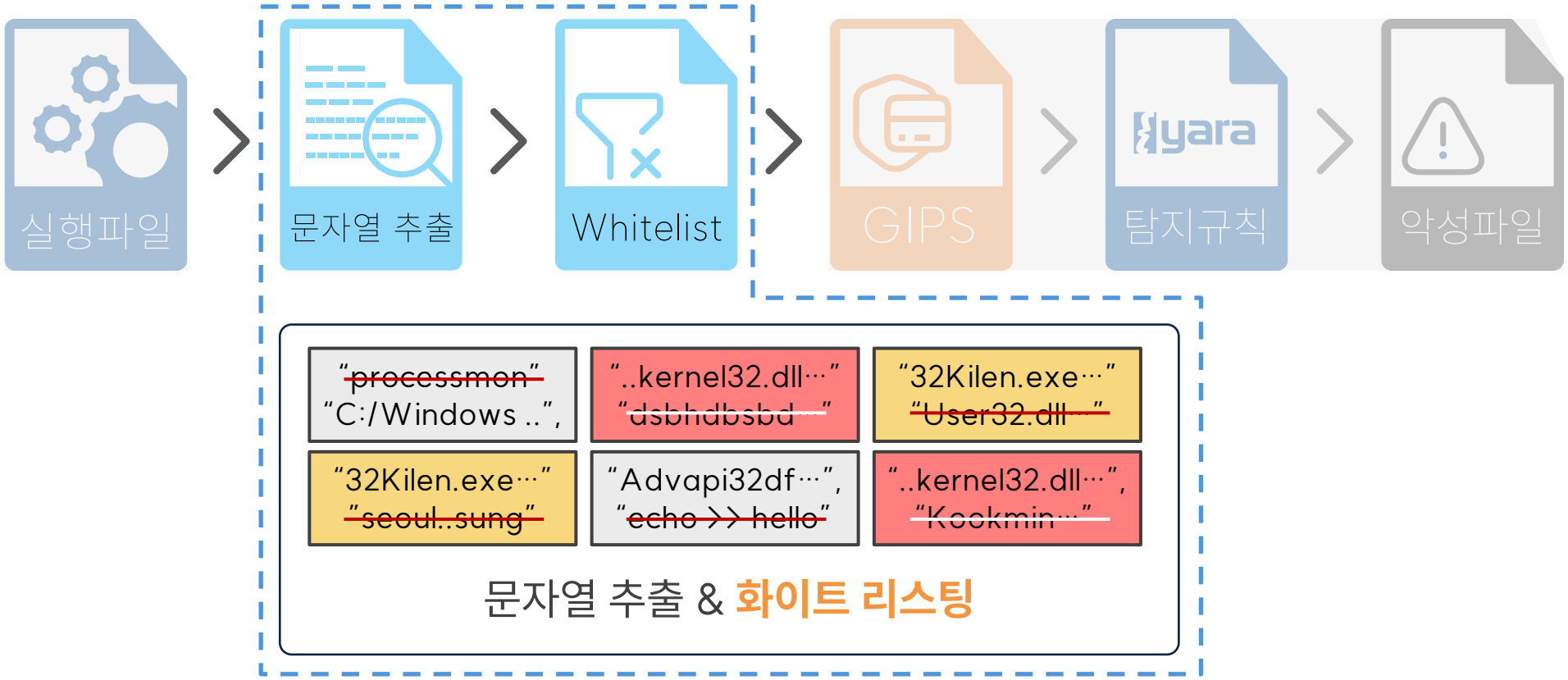
01

실행 파일 업로드


실행파일
문자열 추출
Whitelist
GIPS
yara
탐지규칙
악성파일
VSCode.exe
PhoeMiner.exe
Win10_crack.exe
Win11_crack.exe
Chrome.exe
t_rax.exe
정상 & 악성 실행 파일

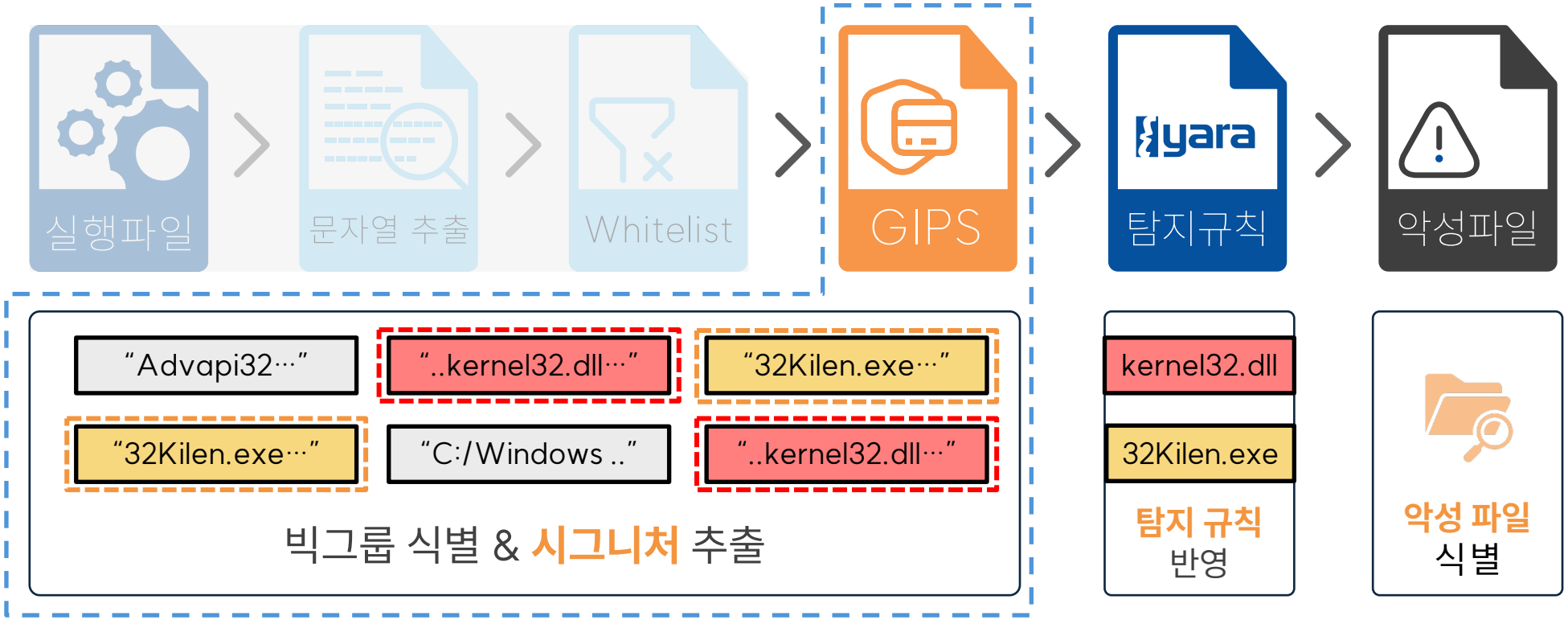
02

데이터 전처리

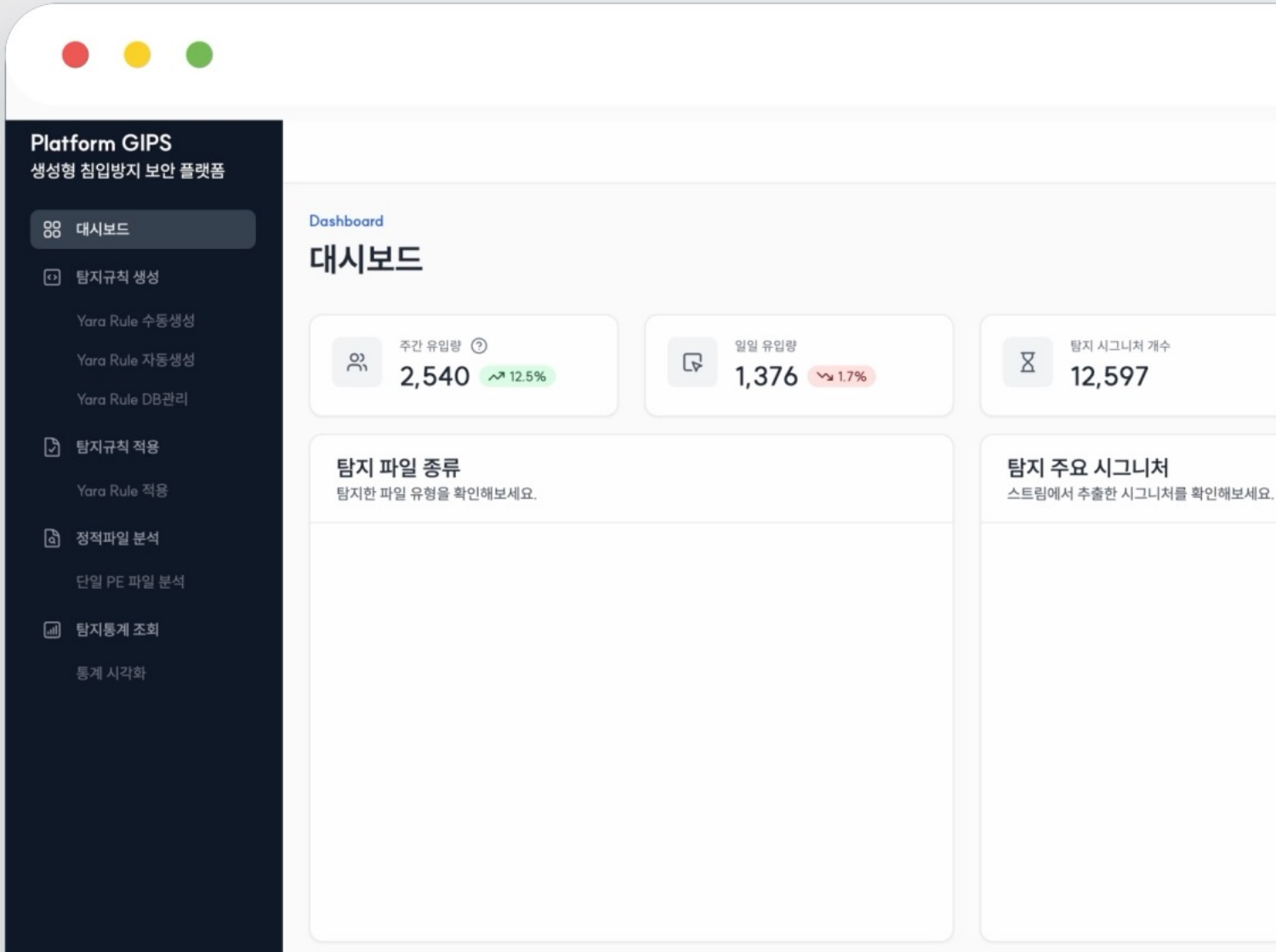

실행파일
문자열 추출
Whitelist
GIPS
yara
탐지규칙
악성파일
"processmon"
"C:/Windows ..",
"..kernel32.dll…"
"dsbhdbsbd…"
"32Kilen.exe…"
"User32.dll…"
"32Kilen.exe…"
"seoul..sung"
"Advapi32df…",
"echo >> hello"
"..kernel32.dll…",
"Kookmin…"
문자열 추출 & 화이트 리스팅

03

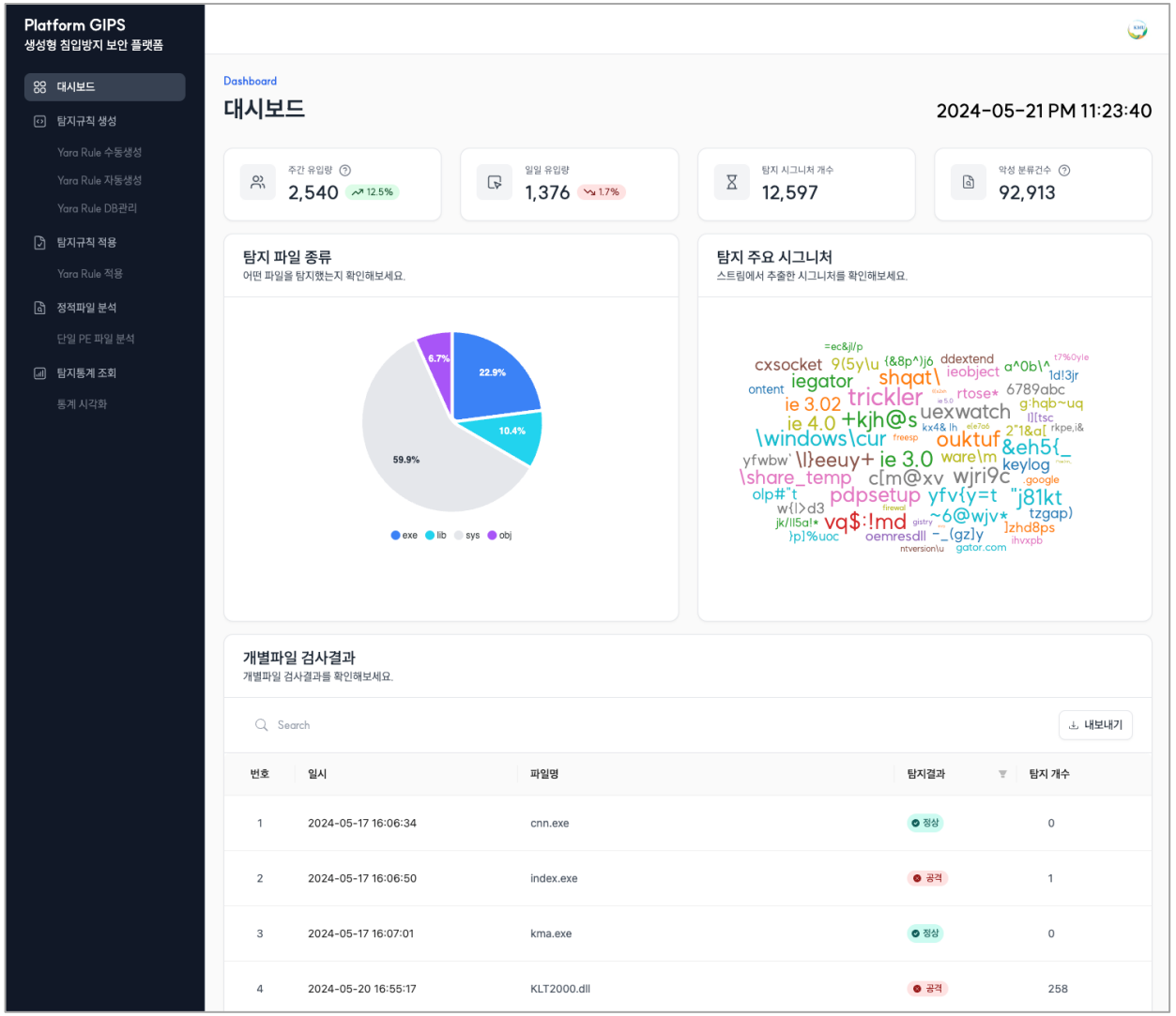
생성형 침입 방지 기술(GIPS*: Generative Intrusion Prevention on data Stream)을 사용해 유의미한 시그니처가 나올 수 있는 그룹을 식별하고 이를 이용해 시그니처를 추출



* HyungBin Seo, and MyungKeun Yoon. "Generative intrusion detection and prevention on data stream." *32nd USENIX Security Symposium (USENIX Security 23)*. 2023.


Platform GIPS
생성형 침입방지 보안 플랫폼
대시보드
탐지규칙 생성
Yara Rule 수동생성
Yara Rule 자동생성
Yara Rule DB관리
탐지규칙 적용
Yara Rule 적용
정적파일 분석
단일 PE 파일 분석
탐지통계 조회
통계 시각화
Dashboard
대시보드
주간 유입량
2,540
12.5%
일일 유입량
1,376
1.7%
탐지 시그니처 개수
12,597
탐지 파일 종류
탐지한 파일 유형을 확인해보세요.
탐지 주요 시그니처
스트림에서 추출한 시그니처를 확인해보세요.

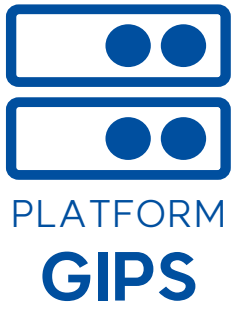
기능 | 대시보드



플랫폼 주요정보를 한눈에 확인 할 수 있도록
대시보드 형태의 메인 화면 구성

- 카드 UI 형태로 보기 쉽게 구성
- 기본적인 통계 정보 시각화
- 개별 파일 검사 결과 정보 확인 가능

기능 I Yara RULE




```
rule yara : banker
{
    meta:
        description = "This is just an example"
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

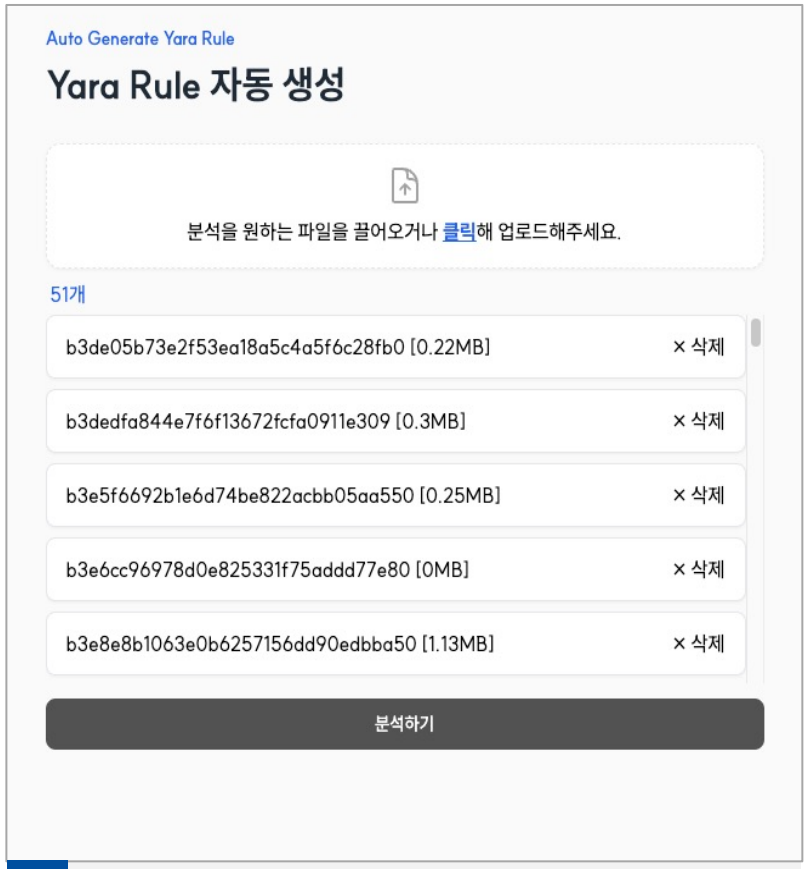
프로젝트 사용 조건

String 시그니처
생성후 사용

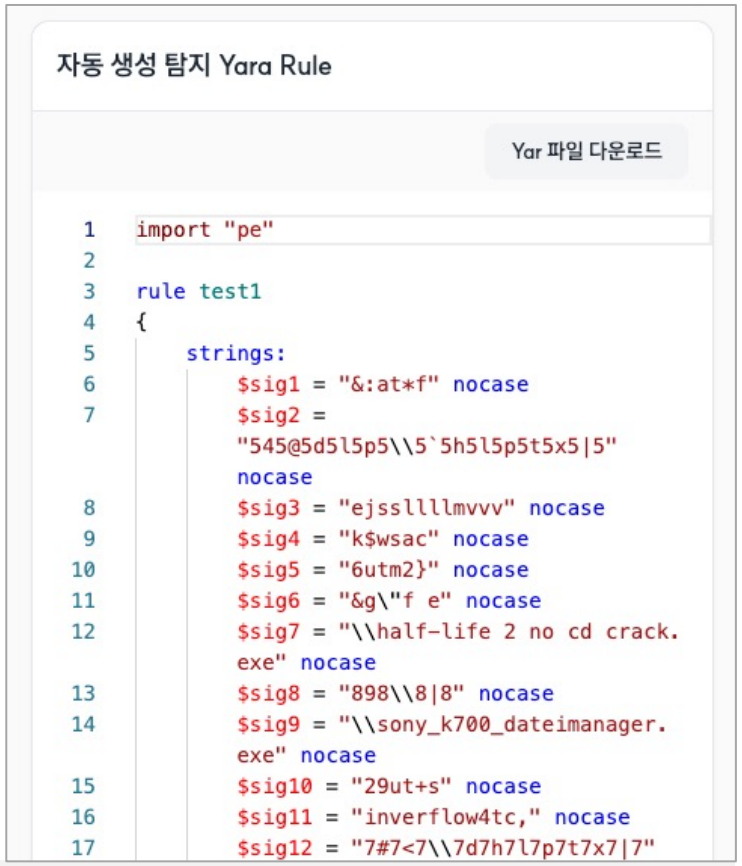
YARA RULE? 악성코드 시그니처를 이용해서 악성 코드의 종류를 식별하고 분류하는 목적으로 사용되는 규칙

- VirusTotal사 개발 & 보안분야에서 널리 사용되는 규칙
- 오픈 소스 & 멀티 플랫폼 지원 [Windows, Linux, Mac]

기능 I 탐지규칙 자동 생성

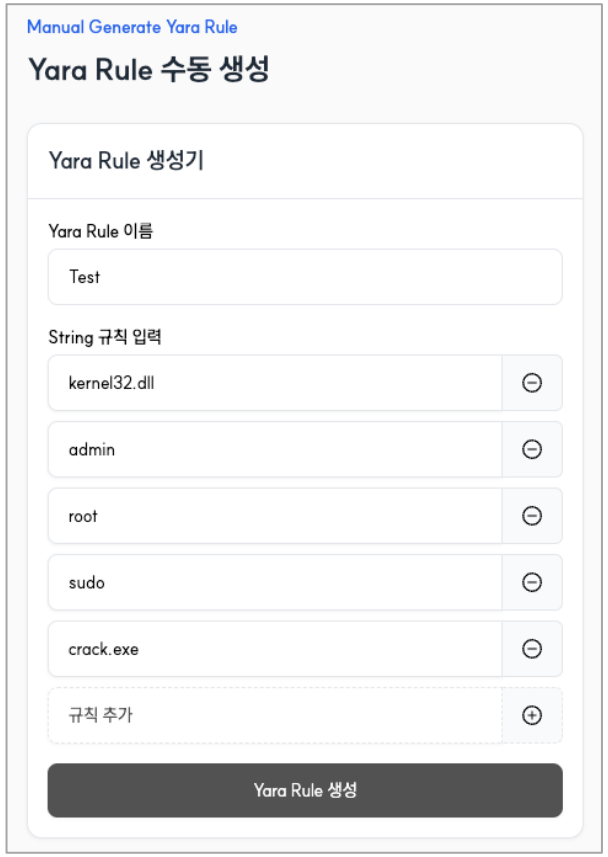


01 탐지 규칙 자동 생성을 위한 **파일 업로드**



02 **자동** 분석하여 **시그니처 추출 및 탐지 규칙 생성**

기능 I 탐지규칙 수동 생성



01

규칙 문자열 입력

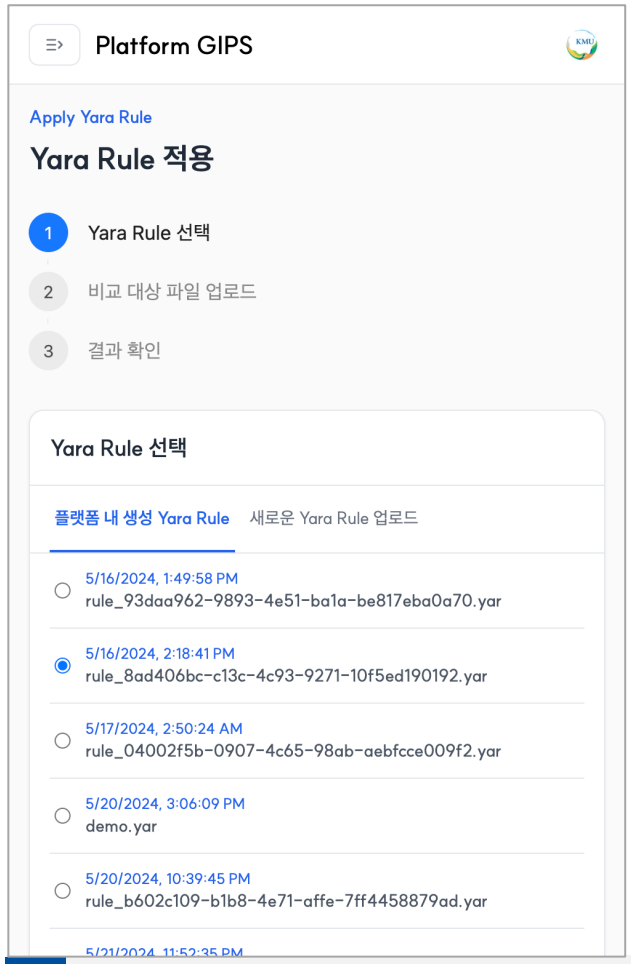
02

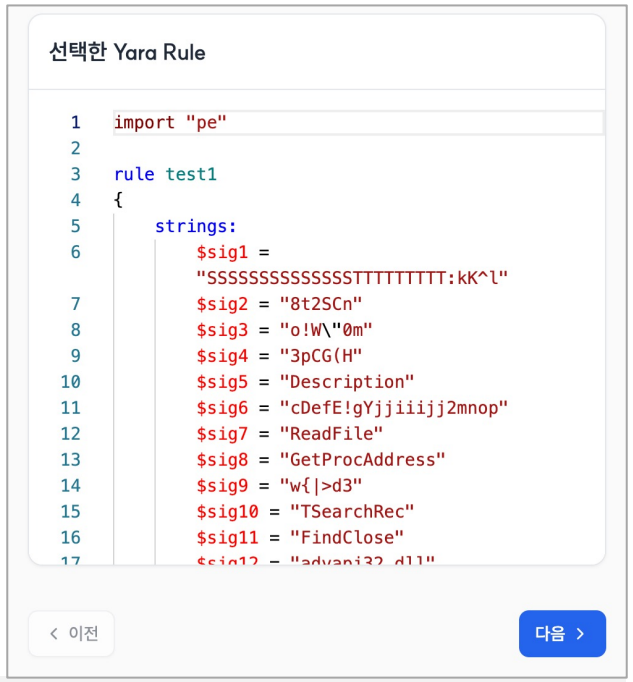
탐지규칙 생성

조건 입력 시
탐지규칙 생성

- 문자열을 입력하면 탐지규칙을 **생성 및 편집 가능**
- **플랫폼 내 저장**하거나 내 기기로 **다운로드** 기능 제공

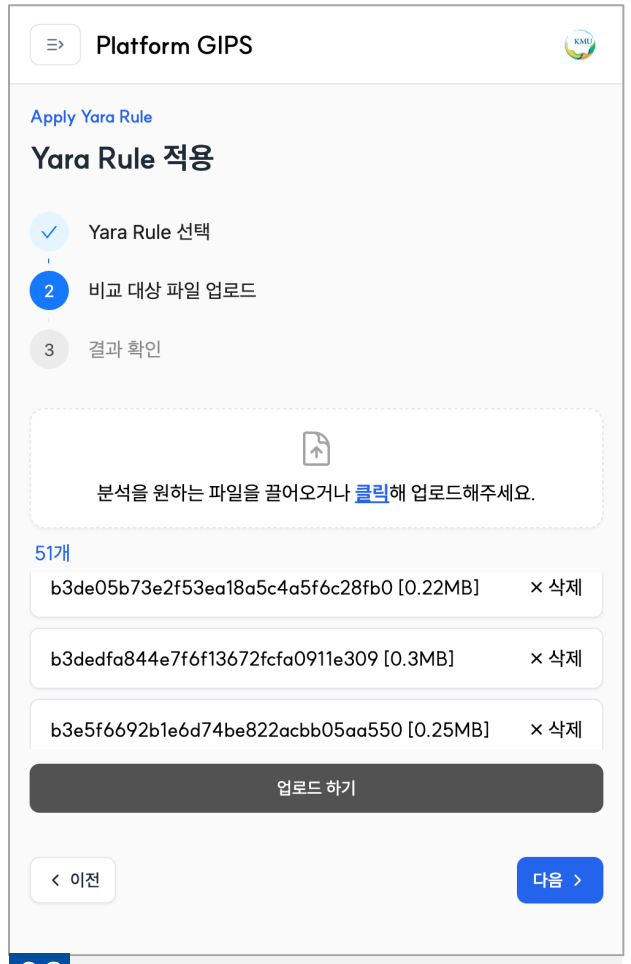
기능 | 탐지규칙 적용





01

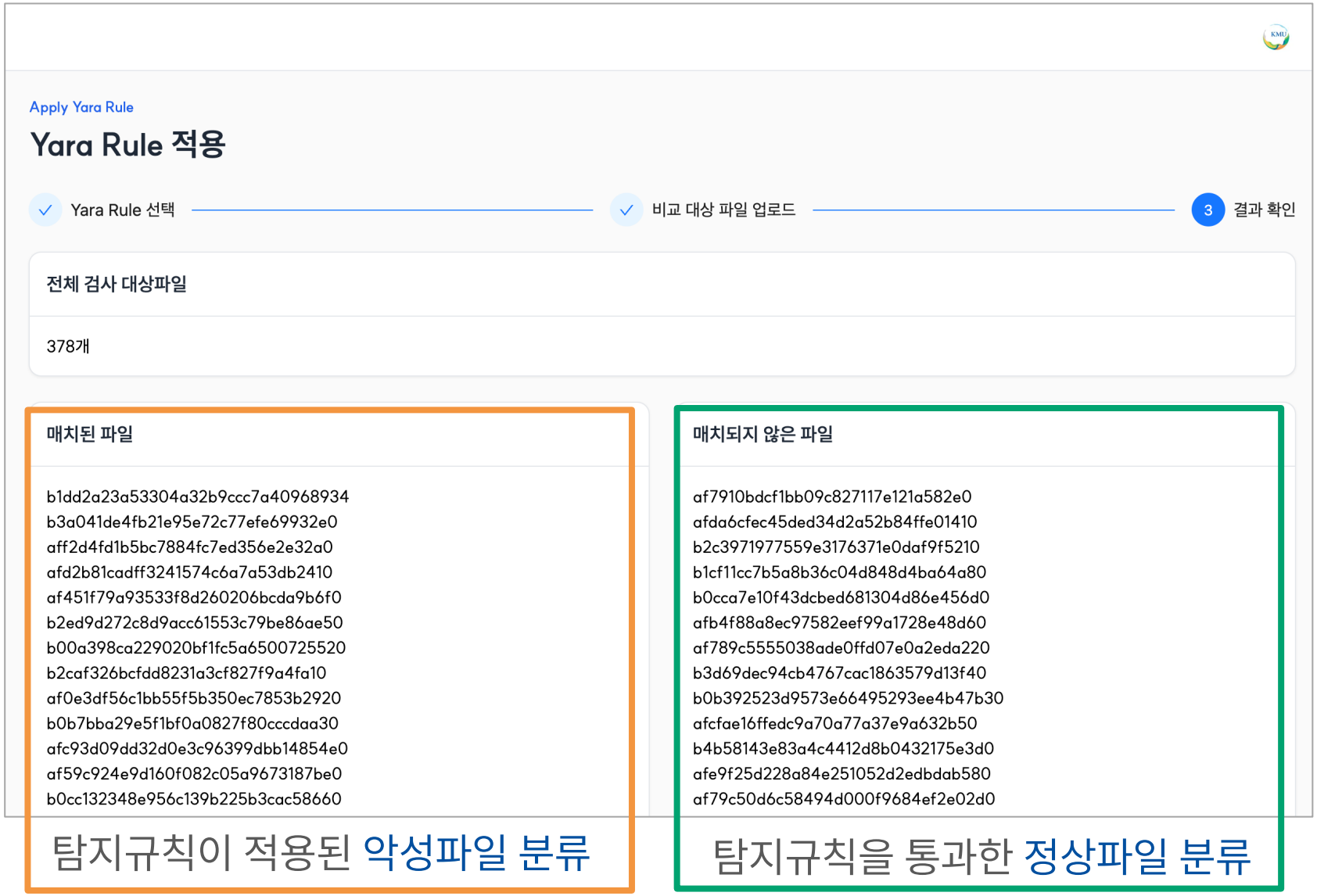
적용시킬 탐지규칙 선택



02

검사할 파일 업로드

기능 | 탐지규칙 적용



03

분류 적용 결과 확인

- 선택한 탐지규칙을 적용하여 **정상/악성파일 분류**

기능 I 탐지규칙 생성 및 적용

적용 결과 검증 진행

Cisco의 오픈소스 백신 소프트웨어 ClamAV *, 국산 백신프로그램인 하우리의 바이로봇에서
탐지하지 못한 악성 파일도 탐지하는 **우수한 성능 검증 완료**

테스트 악성파일

정보보호연구실 보유
악성 실행파일 Dataset

총 2종류의 **악성파일 3개**	
Trojan	facc
W64/ Ipamor.A	cf56 ff81

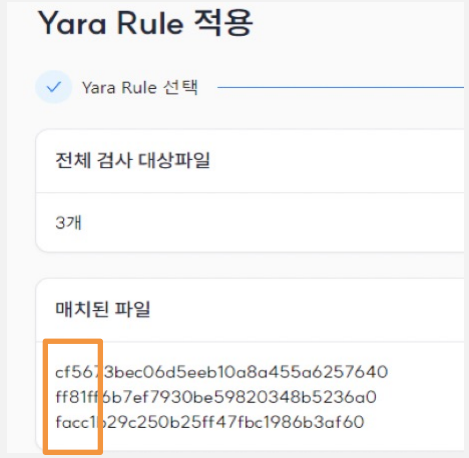
오픈소스 백신 SW – ClamAV

```
-2024-34/PE/datasets/demo_mal$ clamscan ./
l/cf5673bec06d5eeb10a8a455a6257640: OK
l/facc1b29c250b25ff47fbc1986b3af60: OK
l/ff81ff6b7ef7930be59820348b5236a0: OK

----------- SCAN SUMMARY -----------
Known viruses: 8693043
Engine version: 0.103.11
Scanned directories: 1
Scanned files: 3
Infected files: 0
Data scanned: 2.91 MB
Data read: 2.74 MB (ratio 1.06:1)
```

악성 파일 **미탐(탐지실패)** > 정상파일로 탐지

PLATFORM GIPS

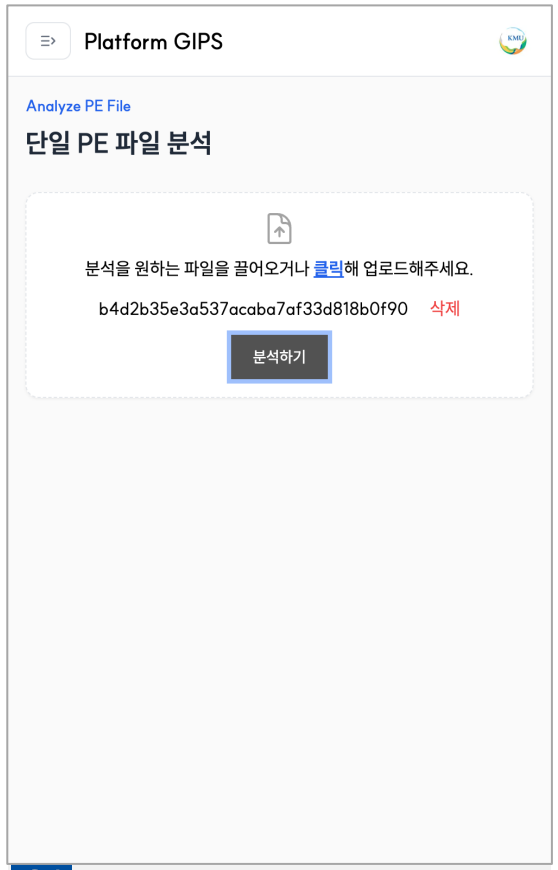


악성 파일 **정탐(탐지성공)** > 악성파일로 탐지

* https://www.clamav.net/

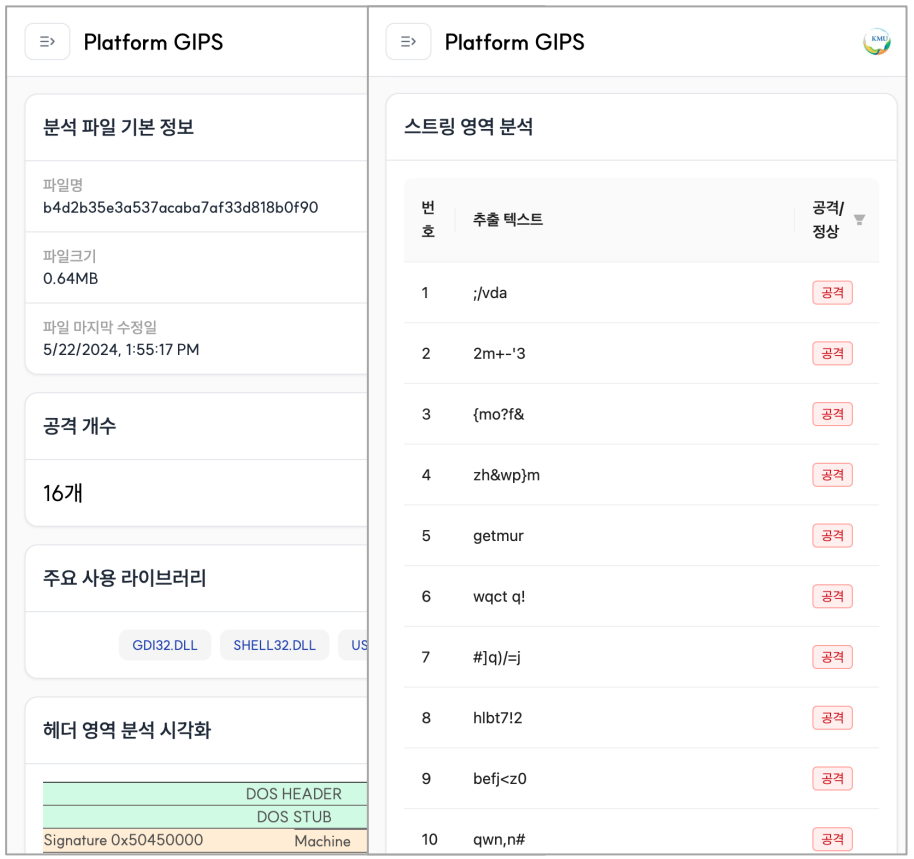
기능 | 악성 파일 분석

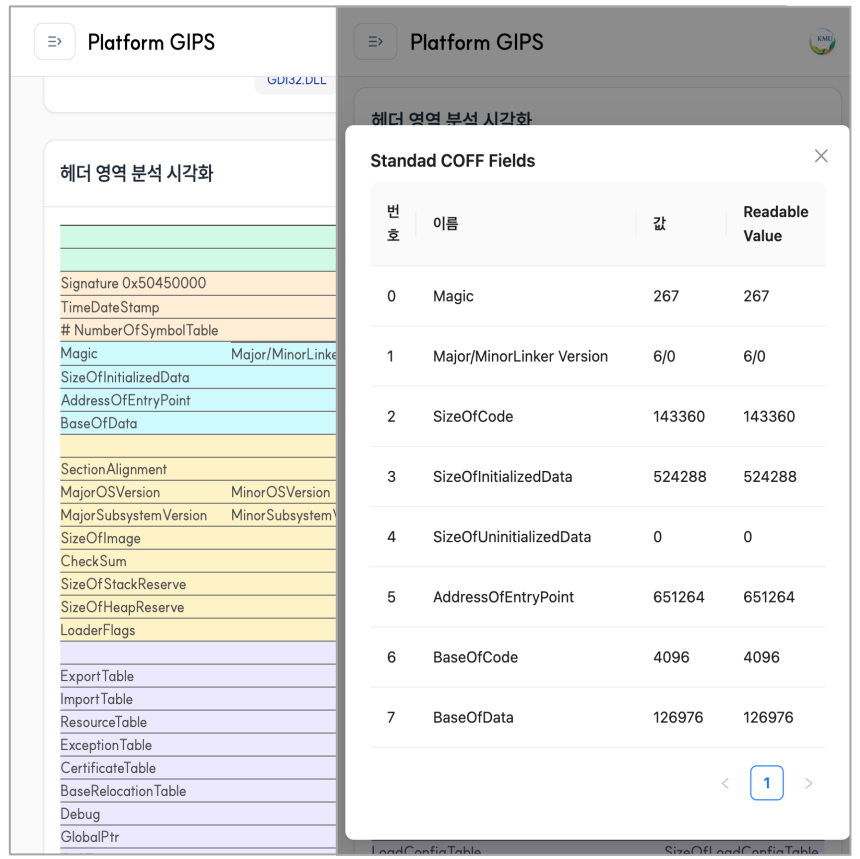
국민대학교 KOOKMIN UNIVERSITY



01

분석할 파일 업로드



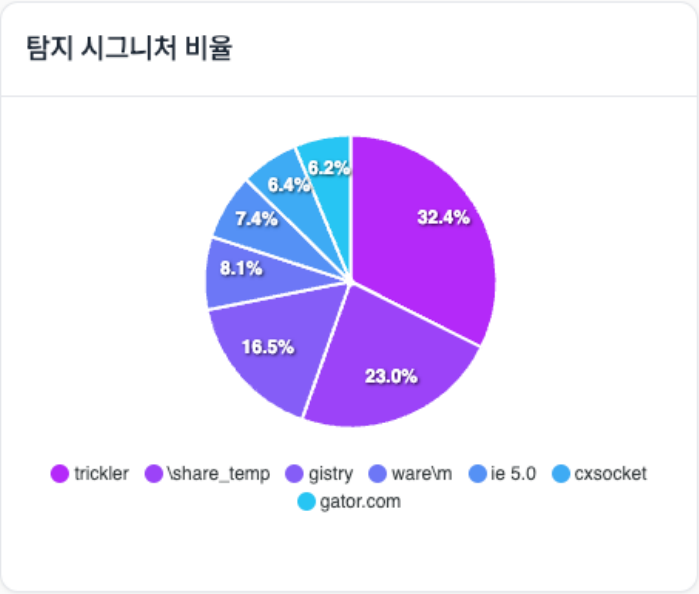


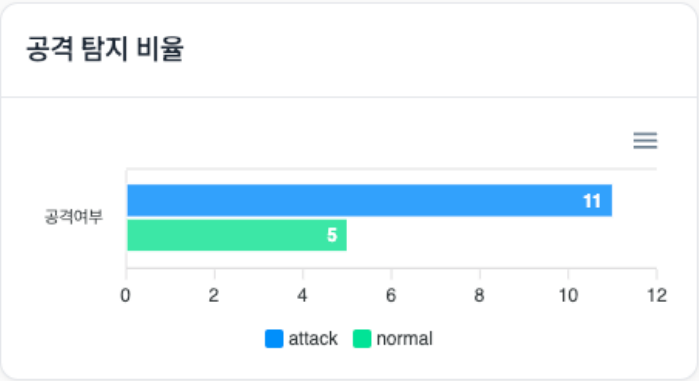
02

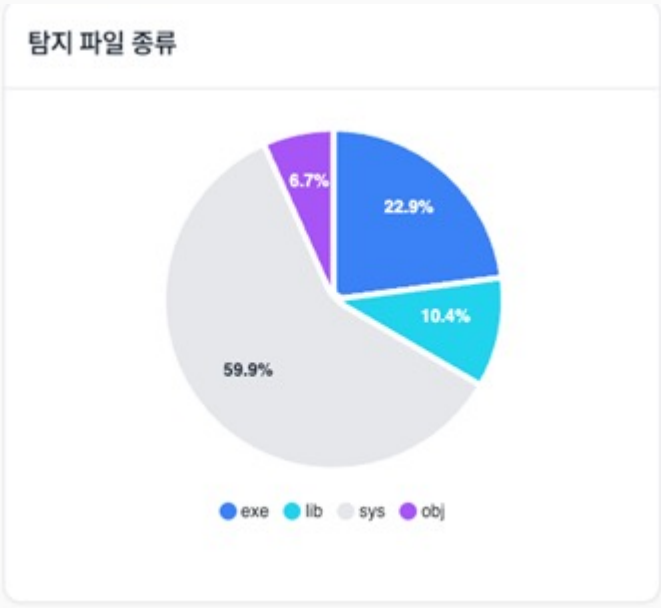
파일 내 공격 문자열 및 개수, 헤더 영역 분석 결과 시각화

파일을 분석하여 악성 여부 판단 정보 제공

기능 I 통계 시각화







플랫폼 내에서 탐지한
여러 파일 정보의 통계값을
시각화하여 효과적으로 전달

- 보안 관리자가 통계 정보를 확인후 적절한 대응을 계획할 수 있도록 구성
- 주요 탐지 **시그니처 비율**
- 분석 대상 파일 중 **공격 비율**
- 탐지 **파일 종류**, 시그니처 **워드클라우드**

중간 피드백 반영 내역

- 테스팅 환경을 먼저 구축 후 실효성 검증필요
  - 테스트 데이터셋을 만들어 개발 초기 실험 환경을 구축함
  - 이후 연구실에서 보유하고 있는 악성파일 데이터셋을 적용하여 검증 완료
- 완성도를 높이기 위해서는 웹(UI) 구축, 시각화 도출 필요
  - 핵심 기술 개발 뿐만 아니라 사용하기 편리한 웹 플랫폼 구축 완료
  - 다양한 방식의 시각화 기능로 효과적인 정보 전달
- 핵심이 되는 코어 기술 정리 필요
  - 발표 초반 핵심 기술에 대해 자세하게 설명
  - 슬라이드 5~7 참조

우수한 성능 검증

- 바이로봇과 ClamAV같은 백신 미탐지 악성파일 탐지

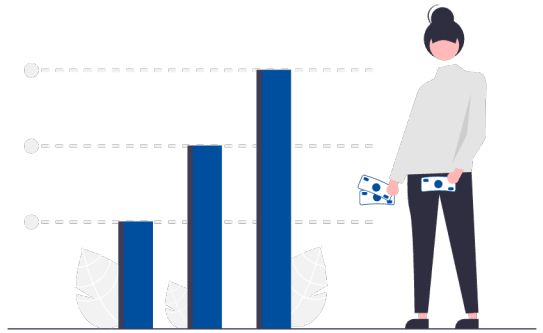
산업체 수요 기술 개발

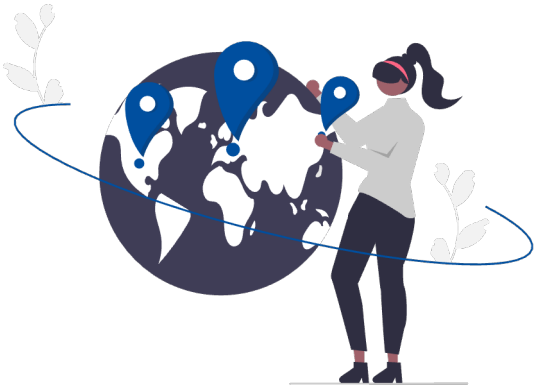
- 산학협력으로 진행, 기업과 사회가 실제로 필요로 하는 기술 개발

선행 연구 기술 고도화

- 기존 네트워크 기반 선행 연구를 악성 코드에 적용해 고도화 기술 개발

기대효과





기술적 효과

신속한 악성파일 식별 및 처리

- 기업별 맞춤형 탐지규칙 생성 가능
- 보안수준 및 위협 대응 기술 고도화

경제적 효과

보안 전문인력 부족 해소

- 획기적인 오탐률 감소
- 자동 탐지 규칙 생성으로 효율적인 업무 가능

사회적 효과

신종공격으로 인한 사회적 피해 감소

- 증가되는 침해사고 예방 가능
- Zero-Day Attack 등 공격 대응 시간 저감

국민대학교 KOOKMIN UNIVERSITY

팀 구성원 후속 연구 과제 지속 참여 | 2024년 AI 보안 제품 및 서비스 사업화 지원사업

과학기술정보통신부 KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

"생성형AI의 순기능과 역기능을 이용한 악성코드 야라룰 자동 생성 및 공유 서비스"

AS-IS

- 기술 검증을 위한 테스트 베드 환경 구축
- 시그니처 포함 기초 탐지 규칙

TO-BE

- 악성 파일 처리를 위한 GIPS 변형 알고리즘 연구 개발
- 악성 코드 시그니처 그룹 생성을 위한 스트리밍 통계 처리 기술 개발

감 사 합 니 다

KMU 국민대학교 KOOKMIN UNIVERSITY

nurilab