SECURI ON

AI 악성 위협 자동 분석 시스템

OnAppScan

보이스피싱 악성 앱 탐지 및 분석 최적화 솔루션

2025.01

Contents

SECURI ON

AI based Cyber Security Company

OnAppScan

AI 악성 앱 자동분석 시스템
OnAppScan

OnAV

AI 기반 모바일 안티바이러스
OnAV

OnTrust

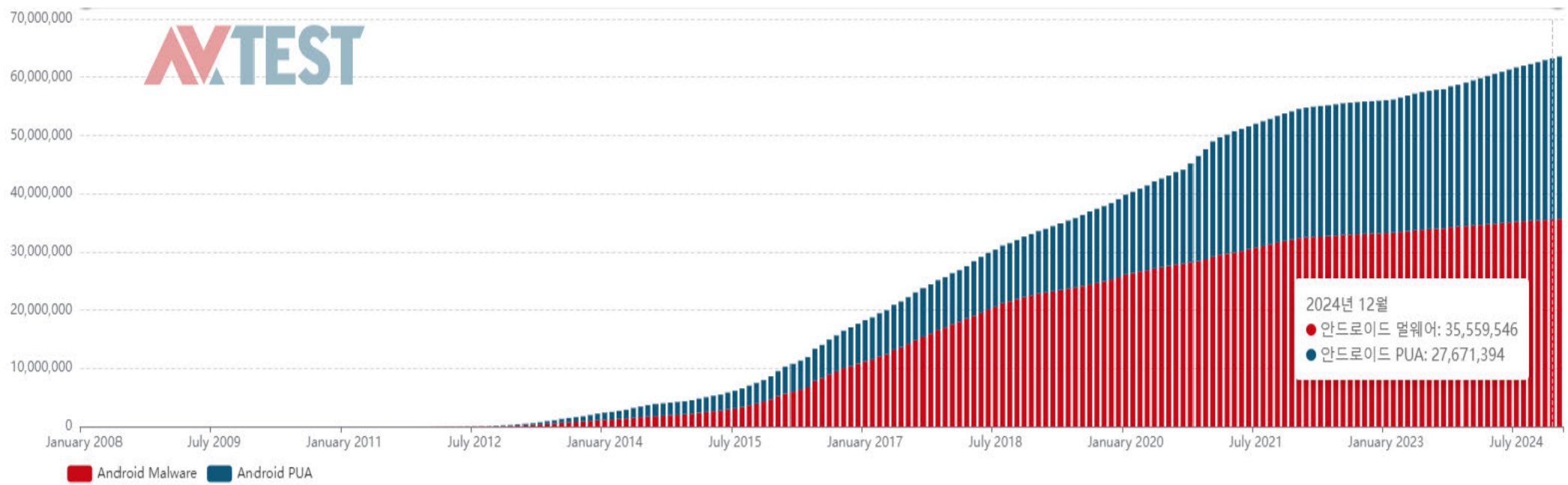
모바일·IoT 안티 해킹 솔루션
OnTrust

OnAV for Linux Desktop

리눅스 OS 안티바이러스
OnAV for Linux Desktop

악성 앱 공격 지능화, 신·변종 가능성 높은 잠재적 악성 앱(PUA) 증가

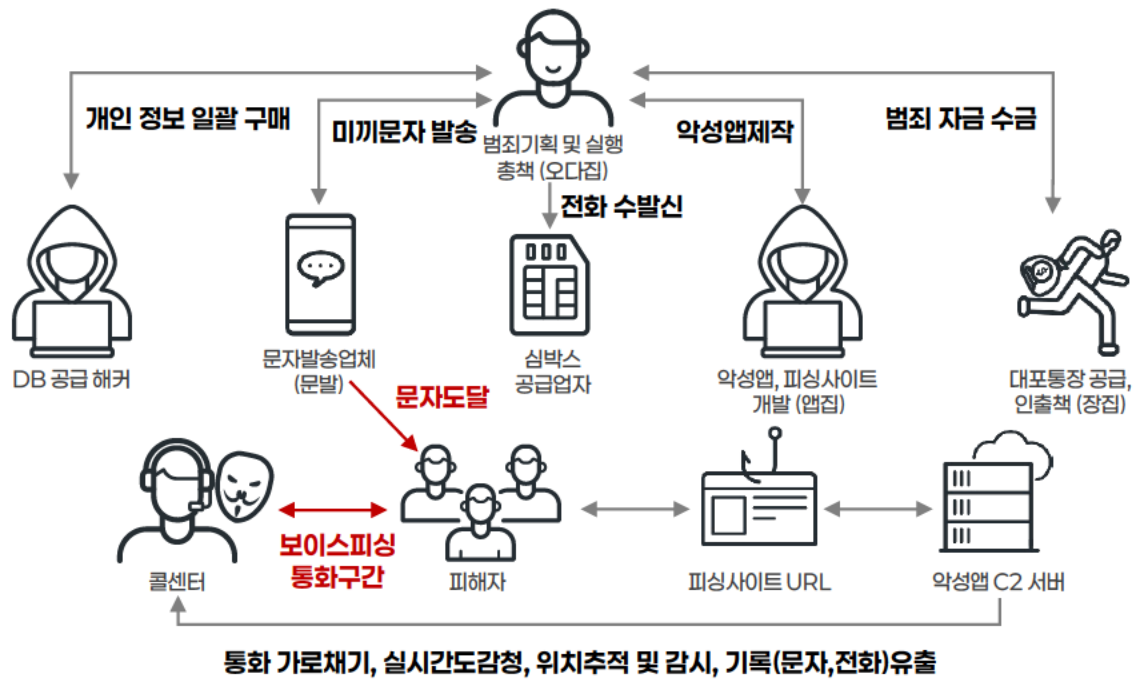
패턴 기반 AV, 정상 앱을 가장해 유포되는 PUA 등 탐지에 한계→수동 분석 업무 과부하



PUA: Potentially Unwanted Application, 주로 애드웨어/ 다운로드 및 브라우저 도구 모음 / 정상 앱과 함께 설치되는 번들웨어, 프록시웨어, 크립토 마이너 등을 포함

악성 앱 이용 피싱 범죄 생태계의 진화, 악성 앱 대량 생산 및 확산 진행 중

기존 보안 솔루션 우회 악성 앱 증가(신·변종, 난독화 등)로 탐지 및 분석 한계



최근 보이스피싱·스미싱 범죄 생태계

1. 텔레그램, 위챗, QQ 내 전문화된
   개별 업자와 연계해 범죄 기획 및 실행

2. SMS 문자 발송 업체를 통한 대량 발송,
   필터링 우회를 통한 높은 문자 도달률

3. 전문 업체 통한 악성 앱 외주 제작,
   피싱 사이트 및 URL 생성, C2 서버 구축
   → 악성 앱 전문 제작자의 지능형 악성 앱 대량 생산 및 배포
   → 누구나 손쉽게 악성 앱 구입, 공격 활용

C2 서버: Command & Control (C&C, 명령 및 제어) 서버 공격자가
공격 대상 장치와 통신을 유지하는 데 사용하며 공격자의 명령을 전달하고 추가 악성코드 다운로드, 데이터 탈취 용도로 사용

AI를 이용해 신·변종 악성 앱, 분석 방해 앱 탐지 가능
자동 판정/검증 시스템으로 분석 업무 효율화

시큐리온 솔루션 대응 전략

1. 앱(APK) 자동분석
2. 수집 방해 기술이 적용된 피싱 사이트 내 APK 도 자동 수집
3. 각종 난독화 및 압축 해제 방해 기술 적용 앱에 대한 자동 판정 및 검증

AI 기반 악성 위협 자동분석 시스템 OnAppScan

위협 통계 및 분석 인사이트 제공, 보이스피싱 대응 특화

분석대상 악성 앱/URL 정보


인증서


앱 정보


SMS

URL

OnAppScan 자동분석(데이터)

- AI 기반 행위정보 및 위험도 분석
- 앱 매니페스트 정보
- 인증서 및 유출지 분석
- 분석 방해 악성 앱 탐지 및 분석

활용 및 인사이트 제공

- 위협 통계 분석
- 공격자 그룹 프로파일링 가능
- 보이스피싱 악성 앱 대응 특화

고객 니즈에 따라 클라우드 또는 온프레미스 서비스 제공

예산 및 운영 환경에 따라 맞춤형 서비스 제공

클라우드 서비스

- 시큐리온 클라우드 서버를 통해 자동분석
- 별도의 내부 솔루션 구축 비용 없음
- 계정 별 이용량에 따른 비용 부과로 예산 절감

온프레미스 서비스

- Application 제공
- 고객사 내부 분석 시스템 구축
- 평판 검사/AI 검사/패턴 DB 검사 유료 라이선스

하이브리드 서비스

- 온프레미스와 클라우드 결합 시스템
- CVS 분석에 필요한 최소 데이터만 클라우드에 연동
- 온프레미스에 비해 구축 비용 일부 절감 가능

업데이트 주기

평판검사 DB	상시
AI 모델	6개월단위 1회
패턴검사 DB	상시

*패턴 DB, 평판 DB는 지속적으로 항시 업데이트 진행

세분화된 기능으로 판정, 분석, 연관 정보 제공

판정된 악성 앱 정보(위험도, 평판) 外 부가 정보 제공

글로벌 유사 제품 기능 비교 *앱 분석, 글로벌 제품 V, A, J 등 대비 150% 수준의 기능 제공

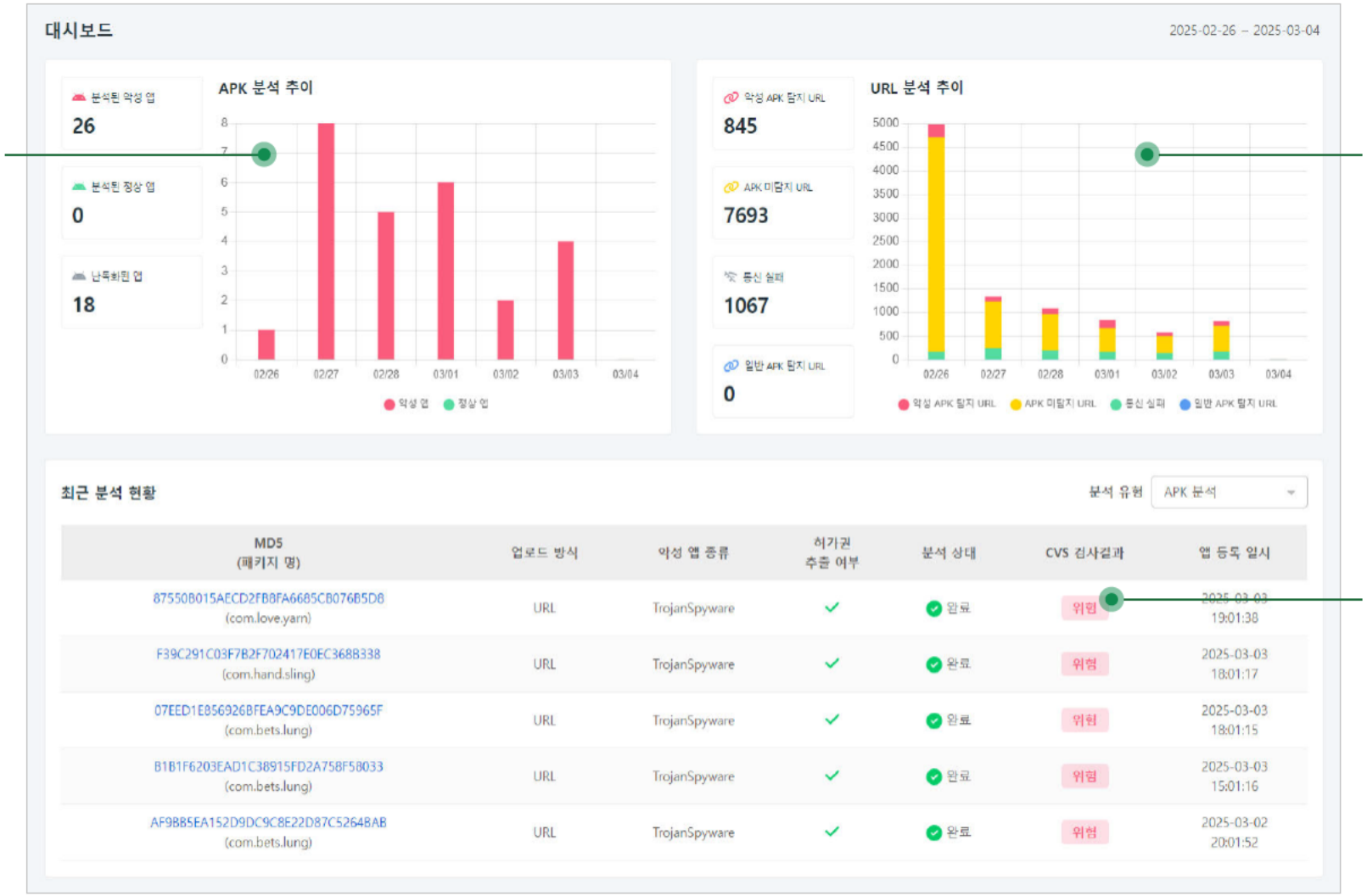
구분	자체판정		앱 분석					위험도 분석				연관 앱 정보			리소스 뷰어	자동 동적 분석
	점수	등급	앱 정보	난독화 여부	인증서 정보	매니페스트	유출지 정보	행위 정보	권한	String	API	동일 인증서	유출지	유사도 분석		
OnAppScan	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O
Malwares.com	O	X	O	X	O	O	△	X	X	X	X	X	X	X	X	X
Hybrid analysis	O	O	O	X	O	O	X	△	O	X	X	X	X	X	X	O
AhnLab	O	X	X	X	X	X	X	X	△	X	X	X	X	X	X	△
Koodous	X	O	O	X	X	X	X	X	X	X	X	X	X	X	X	X
AVC UnDroid	O	X	O	X	X	O	X	X	O	X	O	X	X	X	X	X
Intezer Analyze	X	O	O	△	X	X	X	X	X	X	X	X	X	X	X	X
JOE Sandbox	O	O	O	X	X	O	O	O	X	X	△	X	X	X	X	O

대시보드

● APK 분석현황

● URL 분석현황

● 인공지능 탐지시스템(CVS) 위험도 판정 결과



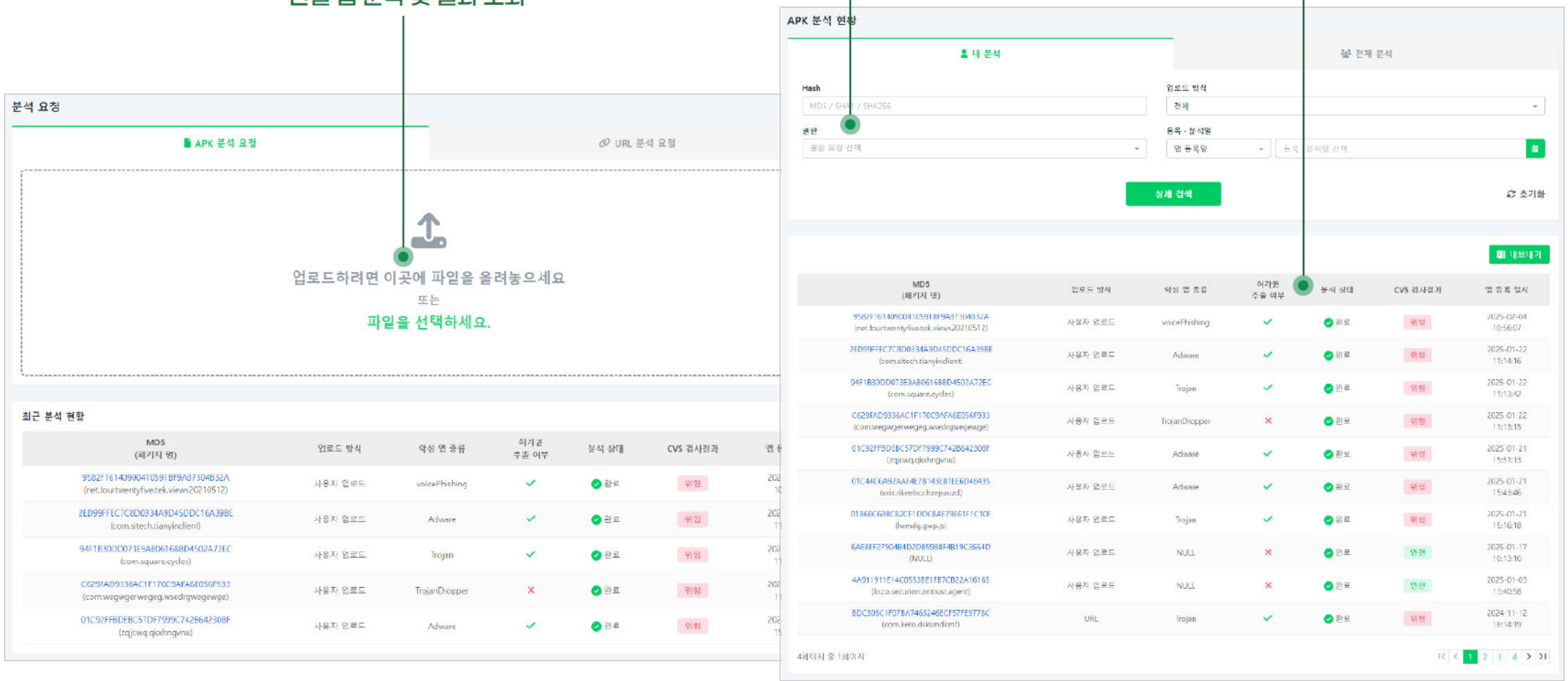
2. 제품소개 (2)주요기능

분석기능

● 웹 페이지를 통한
단일 앱 분석 및 결과 조회

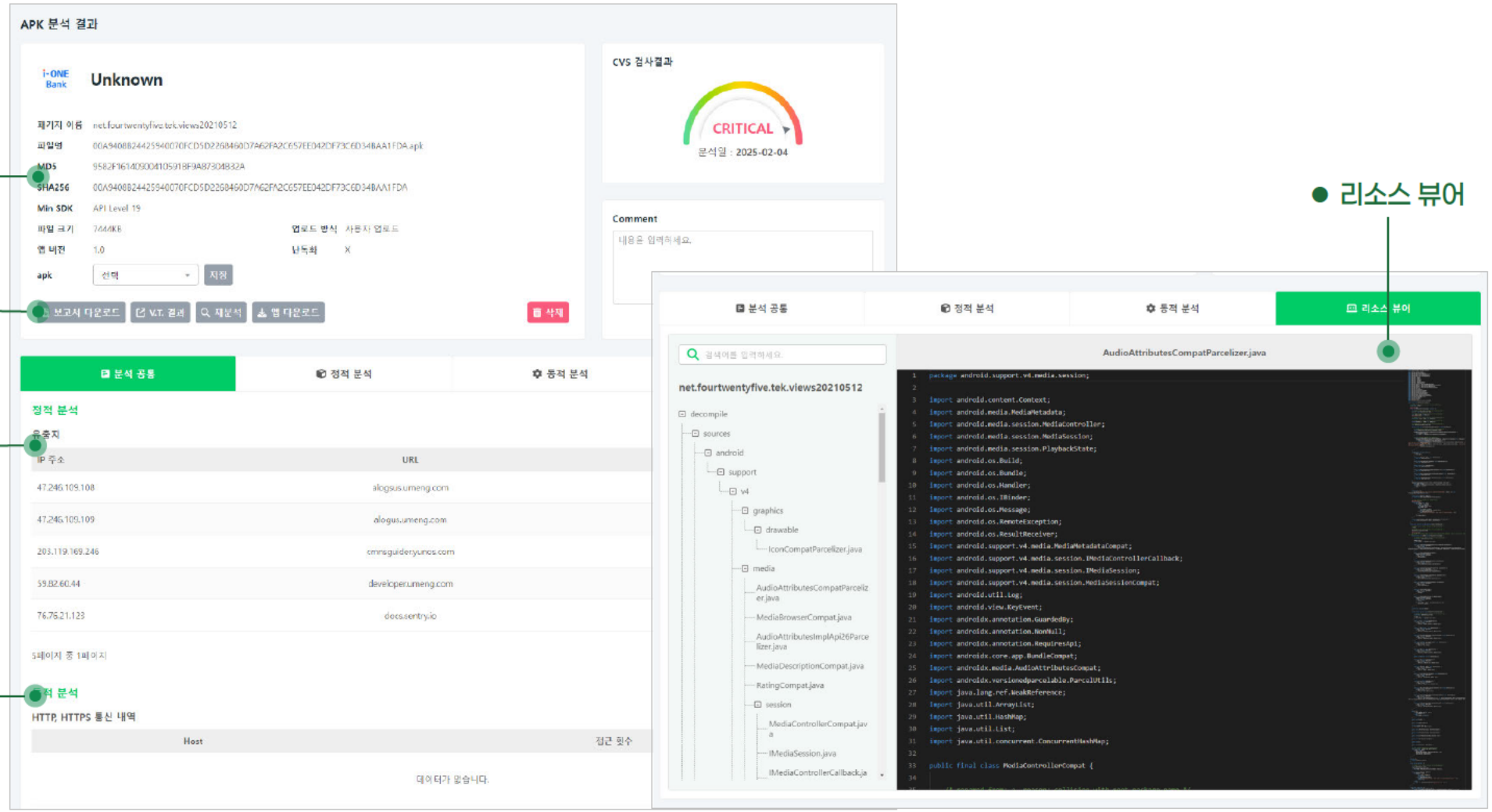
● 분석 이력 검색

● 분석 내역



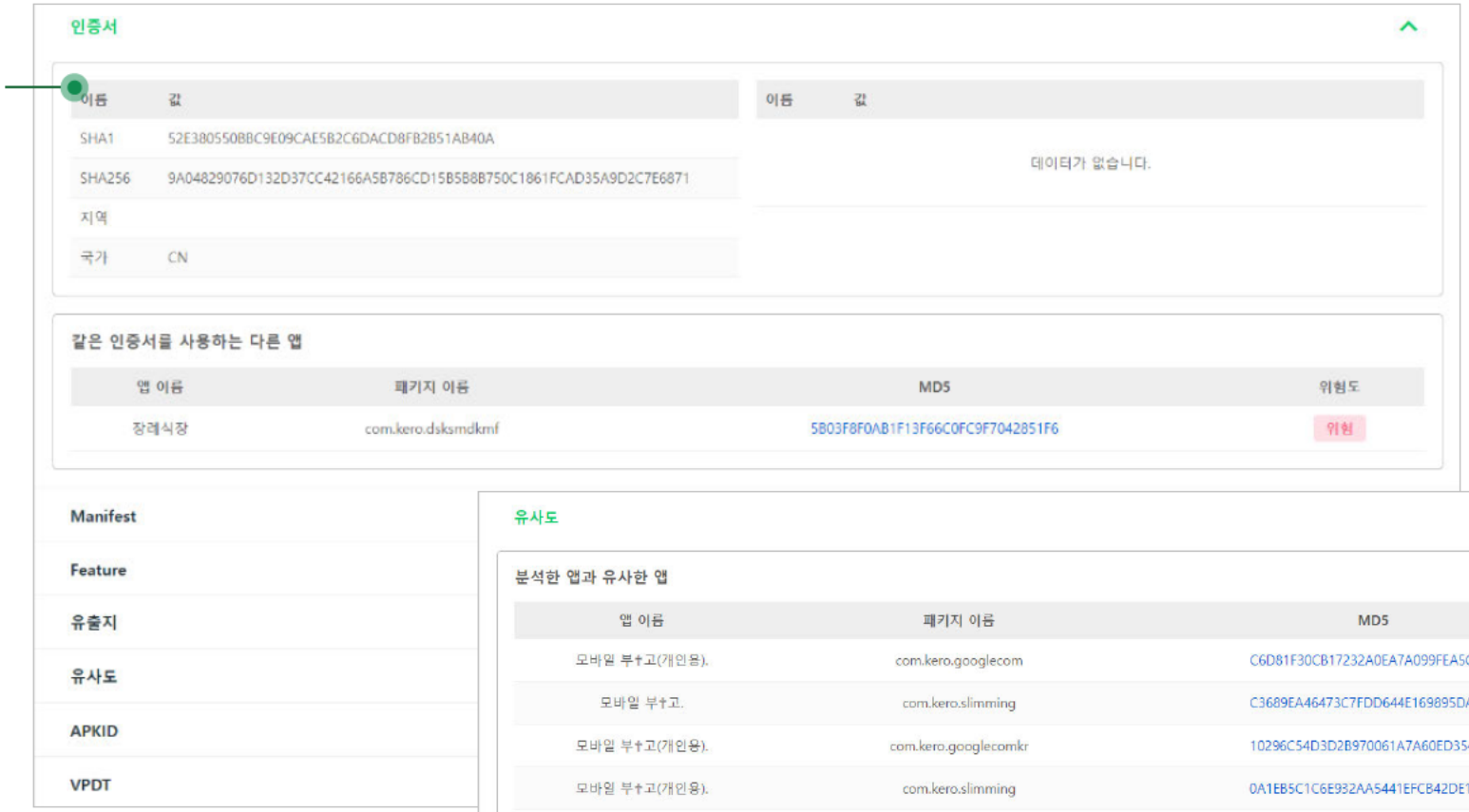
APK 분석 상세 기능

- 앱 기본 정보 제공
- 보고서 다운로드
- 정적 분석을 통한 유출지 확보
- 악성 행위 분석
- 리소스 뷰어



APK 분석 상세 기능

- 인증서 정보 및 동일 인증서 추적

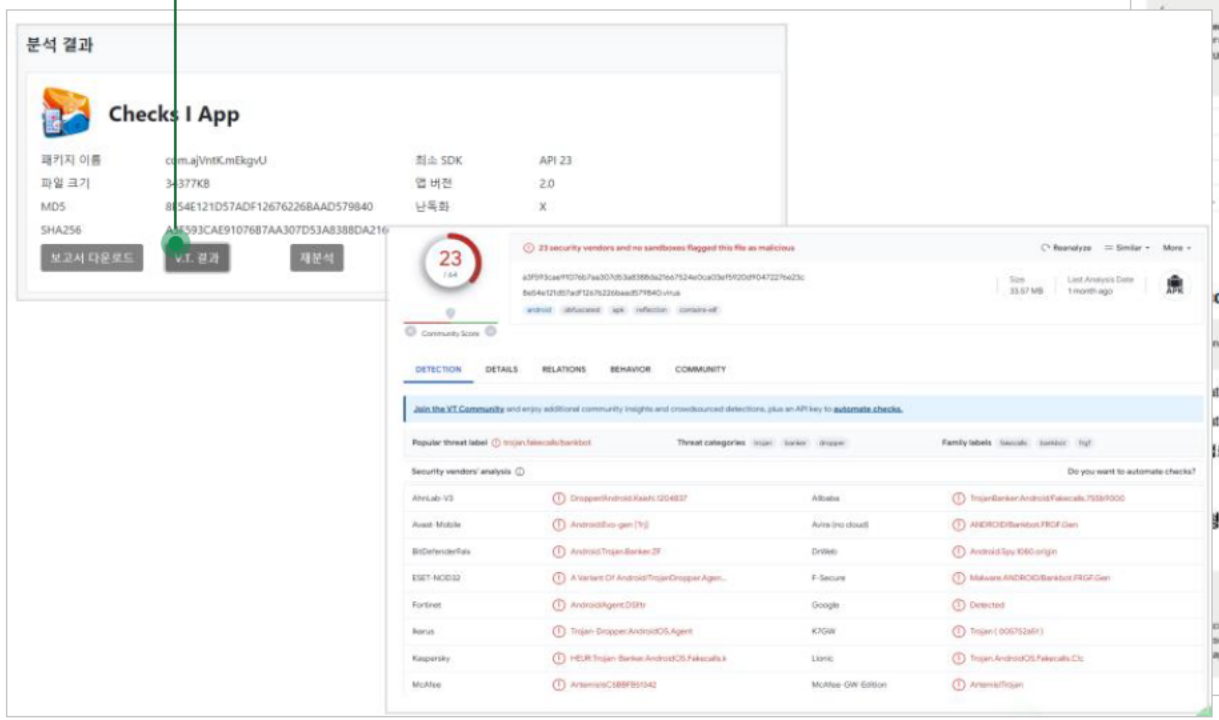


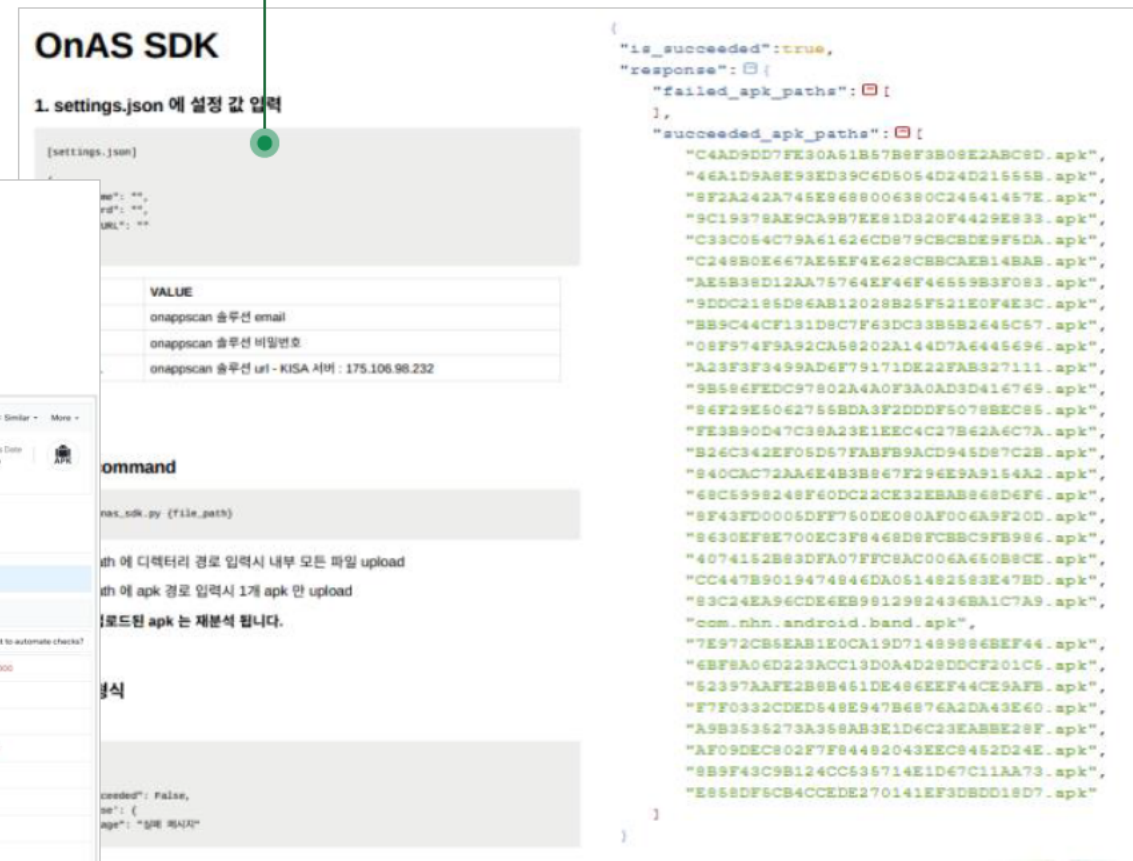
- Fuzzyhash를 통한 유사도 추적 결과

APK 분석 상세 기능

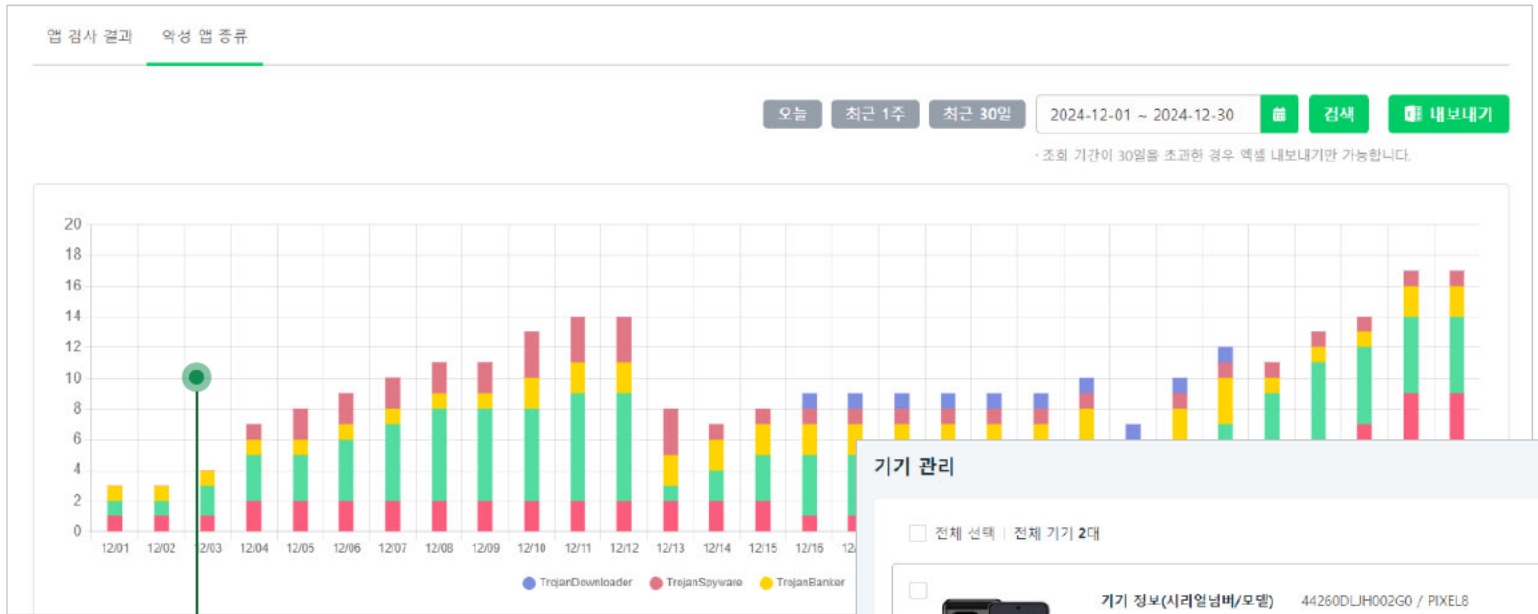
- 앱 평판 정보 제공
  (바이러스토탈 연계)

- SDK를 통한
  대량 분석 요청



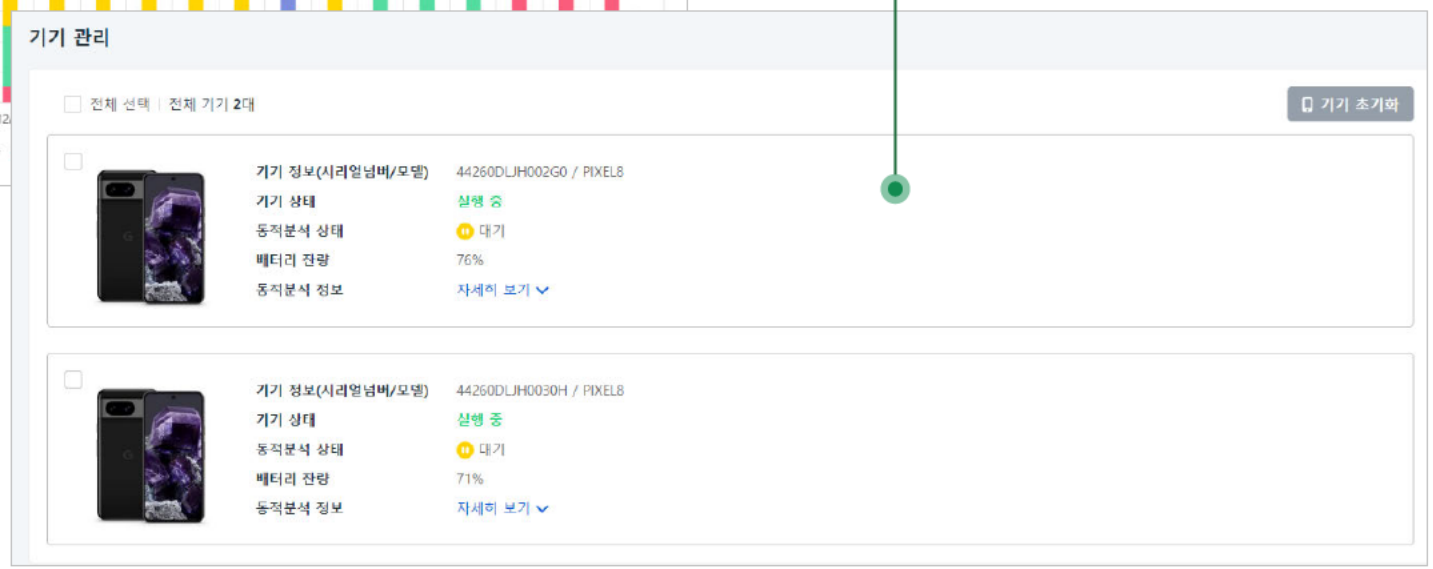


관리 기능



● APK 분석 통계

● 기기관리



AI 악성 앱 탐지 시스템 CVS(Cross-Validation System)로 위험도 판정

머신러닝 검사와 평판 검사, 패턴 검사 결합해 높은 탐지 정확도 구현

"정확도 높은 CVS로 악성 앱 위험도 자동 판정"

분석대상 앱
Full APK

Meta Data

네트워크 트래픽 0.05MB

" 메타데이터만 이용한 분석으로 낮은 리소스 소모량"

Full APK 이용 G사 엔진 대비 5400분의 1

Cross-Validation System

Step1.
Pattern Matching

Step2.
AI Inspection

Step3.
Reputation Check

" 교차 검증을 통한 탐지 정확도 향상"

AV-TEST
Detection rate

2024.01	100
2024.03	100
2024.07	100
2024.09	99.9

전문가의 경험을 집약하여 개발한 '보이스피싱 디텍터' 기술

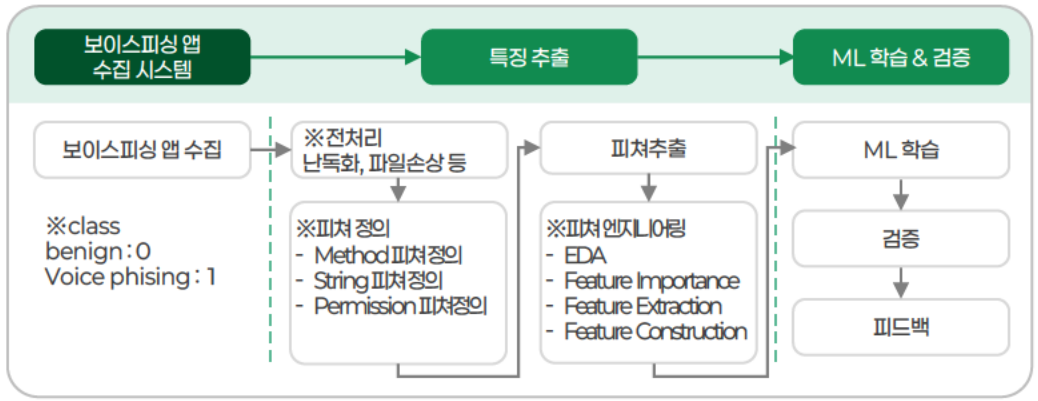
난독화, 압축 해제 방해 등 분석 방해 기술 적용 보이스피싱 악성 앱 탐지 특화

전화 가로채기 기능 포함 앱에 대한 ML 기반 탐지

머신러닝 분석모델 탐지율 **100%**

총 수집 악성 앱 2041개

2022년 STA ICT 시험인증 연구소



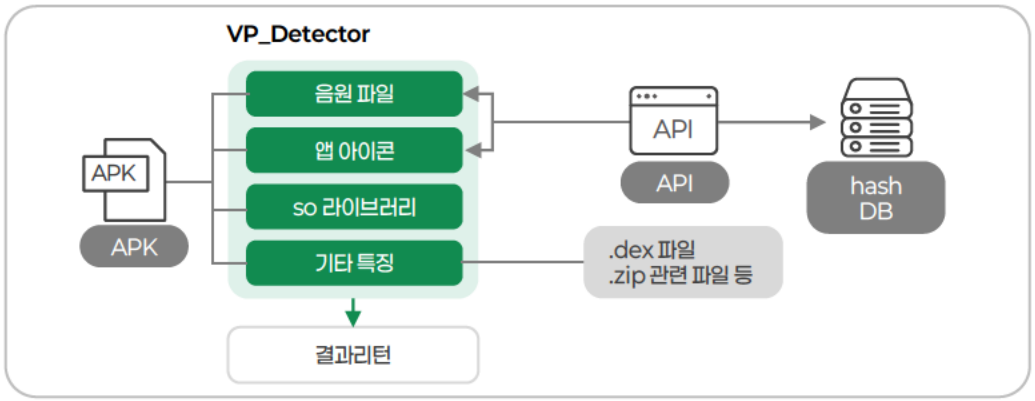
파일의 구조적 특징을 활용한 휴리스틱 탐지
(파일 내부 ARS 음원, APK, ZIP, DEX, SZ 파일 포함 유무 검사)

보이스피싱 디텍터 탐지율 **99.3%**

총 수집 악성 앱 139개

2023년 STA ICT 시험인증 연구소

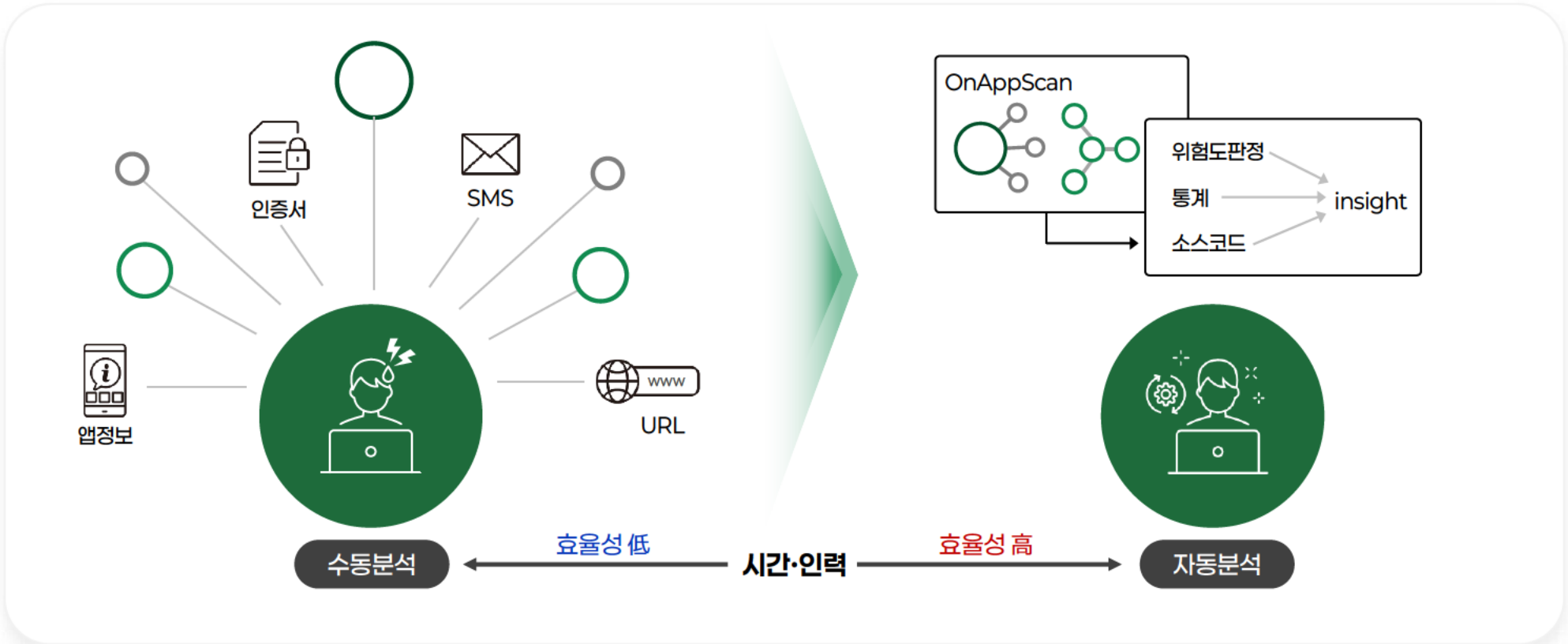
*정기적으로 hash DB가 업데이트 되는 서버 기반 검사



* IITP '휴대폰 단말에서의 보이스피싱 탐지, 예방 기술 개발' 사업 성과물 상용화 제품(관계사 아이넷캅 수행)

위협 분석에 소요되는 시간 및 인력 리소스 대폭 절감, 악성 앱 대량 분석 용이

솔루션 도입 기관 평가 “앱 당 분석 시간 2시간에서 5분으로 단축 "



분석 방해 기술 적용 보이스피싱 악성 앱 탐지율 향상

STA ICT 시험인증연구소 테스트 결과 ML모델 보이스피싱 앱 탐지율 100%

머신러닝 분석모델 테스트 결과 1 *앱 출처: 정상(Playstore), 보이스피싱(2022년 수집) 2022년 STA ICT 시험인증 연구소

구분	전체 개수	정탐 개수	오탐 개수	탐지율	전체 탐지율
정상	1500	1500	0	100%	100%
보이스피싱	2041	2041	0	100%	

머신러닝 분석모델 테스트 결과 2 *앱 출처: 보이스피싱(2023년 8월 수집), 2023년 STA ICT 시험인증 연구소

구분	전체 개수	정탐 개수	오탐 개수	전체 탐지율
보이스피싱	113	113	0	100%

총 수집 앱 139개
피처 추출 불가26개

보이스피싱 디텍터 테스트 결과 *앱 출처: 보이스피싱(2023년 8월 수집), 2023년 STA ICT 시험인증 연구소

구분	전체 개수	정탐 개수	오탐 개수	전체 탐지율
보이스피싱	139	138	0	99.28%

총 수집 앱 139개
피처 추출 불가1개(파일손상)

악성 앱 분석을 통해 고객 및 비즈니스 보호가 필요한 분야

보이스피싱 대응이 필요한 공공 부문 유관 기관 등

공공부문 보이스피싱·스미싱 피해 방지

KISA 및 경찰청, 금감원 등 공공기관 주도

피싱 범죄 피해 방지 사업

KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

통신·금융·게임 등 고객 피해 방지

사칭 앱, 피싱 범죄 많은 특수 산업군 대상

이용 고객 및 비즈니스 보호

LG유플러스

앱 마켓 등 대량 분석 수요처 효율 강화

대량의 앱 데이터를 실시간 자동검사, 마켓 침투 악성 앱 제거

맞춤형 AI 모델링으로 탐지 정확도 향상

ONE STORE

사용환경 및 사양

구분	OnAppScan appliance
Server OS	Linux
WAS / DB / JDK	NginX 1.10 / Postgres 9.5 / openjdk-8
CPU / Disk / Memory	1 CPU / 1TB / 32GB
Client Browser	-크롬 38~79(Stable), 80,81,82 -파이어폭스 72(Stable), 73,74 -오페라 66(Stable), 67,68 -IE 11(Edited) -엣지 44(EdgeHTML Stable), 81,82(Chromium Beta, Canary) -사파리 12(모하비), 13(Developer Preview)

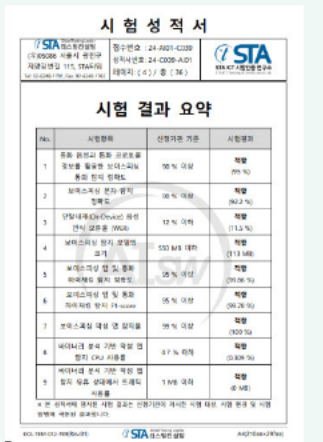
AI 탐지 시스템 CVS 적용 OnAV, 글로벌 Top 3인증 획득

휴대폰 단말에서의 보이스피싱 탐지, 예방기술 STA ICT 성능 평가 통과

독일 오스트리아 영국 대한민국 중국 중국

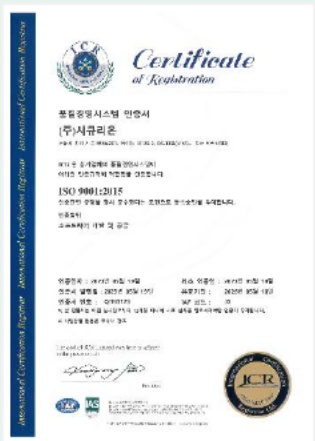
인증	횟수	내역	비고
AV-TEST	36회	2018년 7/9/11월, 2019년 1/3/5/7/9/11월, 2020년 1/3/5/7/9/11월, 2021년 1/3/5/9/11월, 2022년 3/5/7/9/11월, 2023년 1/3/5/7/9/11월, 2024년 1/3/7/9월, 2025년 1월	연6회 평가
AV-Comparatives	6회	2019년-2024년	연1회 평가
MRG Effitas	2회	2019년 2분기, 3분기	
SKD Labs	1회	2019년	
PCSL	4회	2018년 3분기,4분기, 2019년 1분기, 2분기	

STA ICT
보이스피싱 탐지기술 평가


시 험 성 적 서

시험 결과 요약

시큐리온 ISO9001
품질경영시스템 인증


Certificate of Registration

핵심기술
국내 IP 확보

리눅스 커널 무결성 검사 및
데이터 복구

휴대 단말에서의 악성코드
진단 및 제거

취약점 탐지 아키텍처로 구성된
메모리 관리 기술

취약점 보완을 위한
바이너리 패치 장치

머신러닝 이용 이상거래
탐지 장치 및 그 방법

유사도 기반 악성 어플리케이션
탐지 방법 및 장치

위험도 기반 악성 어플리케이션
탐지 방법 및 장치

악성 어플리케이션
탐지 방법 및 그 장치

7. 레퍼런스

대표 사례

보이스피싱·스미싱 대응 효율화

- 보이스피싱 및 스미싱 악성 앱 및 URL 분석
- 신·변종 및 난독화 등 지능형 악성 앱 대응 강화
- 분석 과정 자동화로 리소스 절감

스미싱으로 인한 고객 피해 방지

- 고객 보호를 위해 AI URL 분석 솔루션 도입
- 접속 차단 조치를 우회하는 변조 URL 탐지 강화
- 월 평균 약 1만건 악성 URL 차단

공공 보안

1. 주요 시설 폐쇄망
2. 스마트시티
3. 스미싱 대응

민간 보안

1. 엔드포인트 보안
2. 앱 서비스 보안
3. 이용자 단말 보안

Thank you

문의 pr@securion.co.kr

SECURI ON A : 서울시 송파구 송파대로 201 송파테라타워2 A동 G129-2 OS-33호 | T : 02-575-3339 | W : https://www.securion.co.kr