



AI 악성 위협 자동 분석 시스템

OnAppScan

보이스피싱 악성 앱 탐지 및 분석 최적화 솔루션

2025.01

Contents

1. 제안배경
2. 제품소개
3. 기대효과
4. 적용분야
5. 인증 및 수상
6. 특허
7. 레퍼런스



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

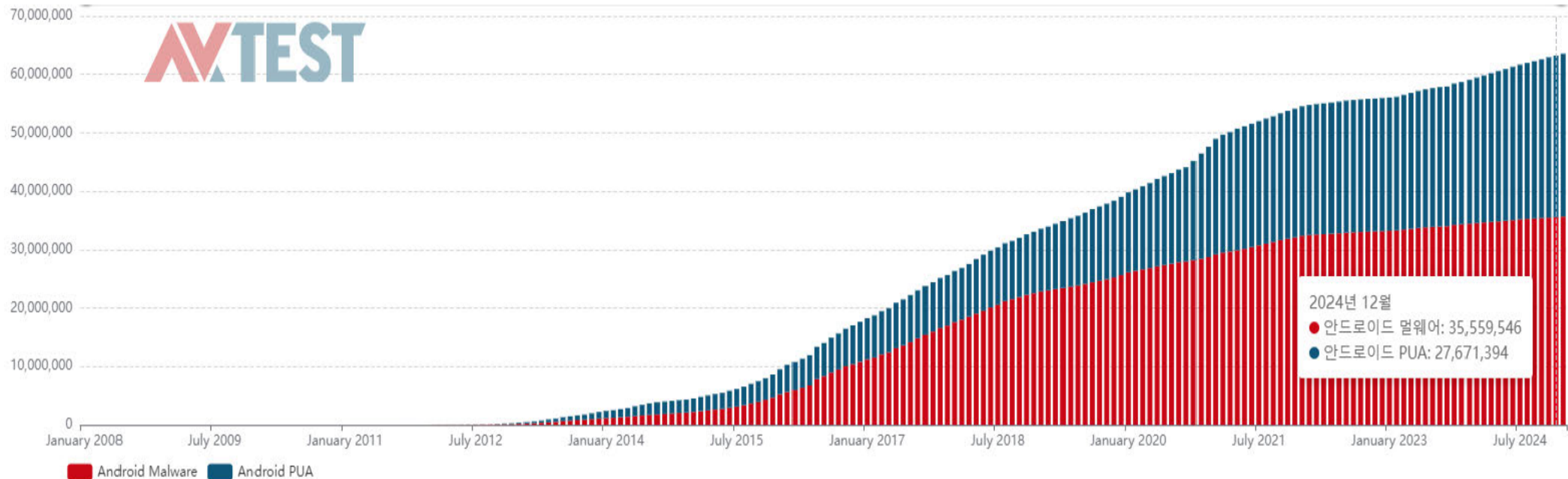
 OnAV for
Linux Desktop

리눅스 OS 안티바이러스
OnAV for Linux Desktop

1. 제안배경 (1)잠재적 악성 앱 증가

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

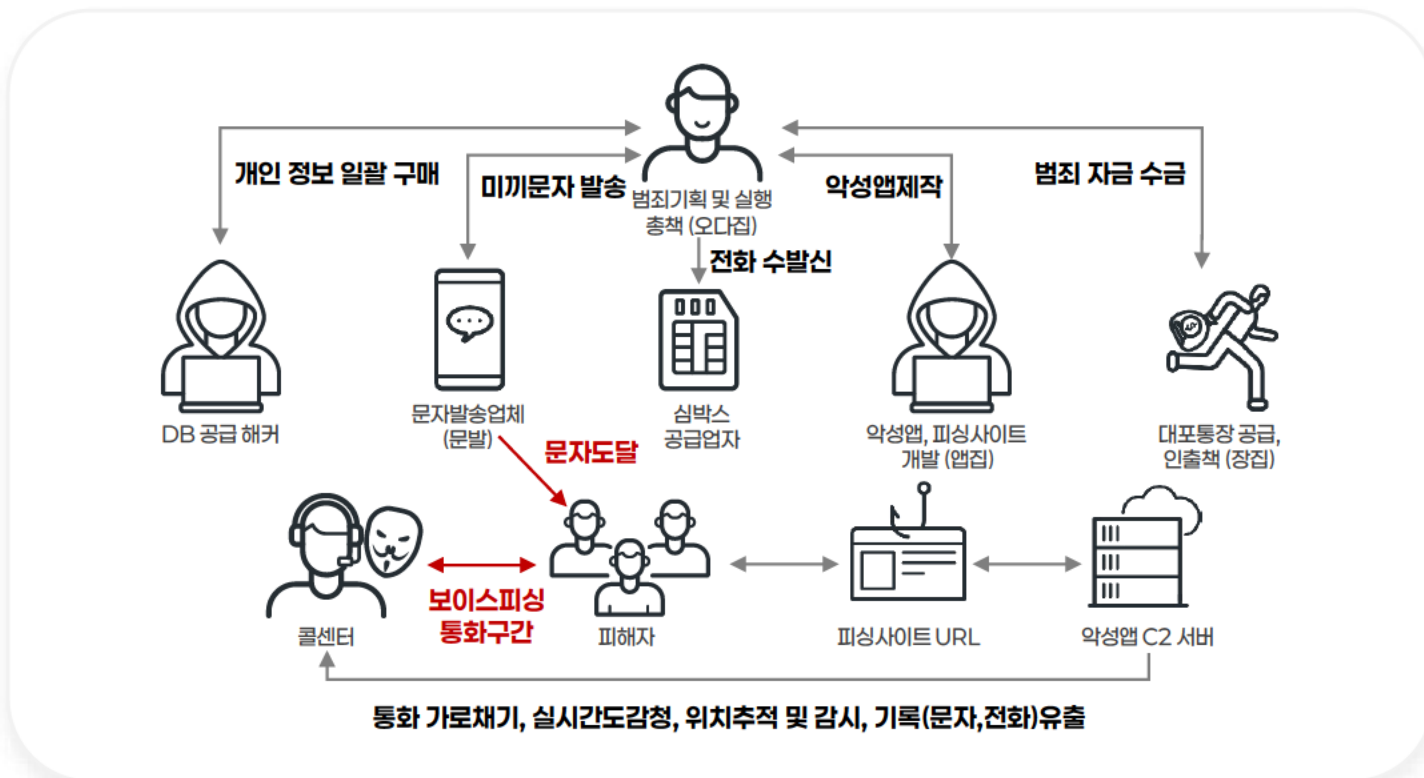
패턴 기반 AV, 정상 앱을 가장해 유포되는 PUA 등 탐지에 한계→수동 분석 업무 과부하



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

1. 제안배경 (2)정교해진 피싱 범죄 생태계

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



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

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

1. 제안배경 (3)대응 방안

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

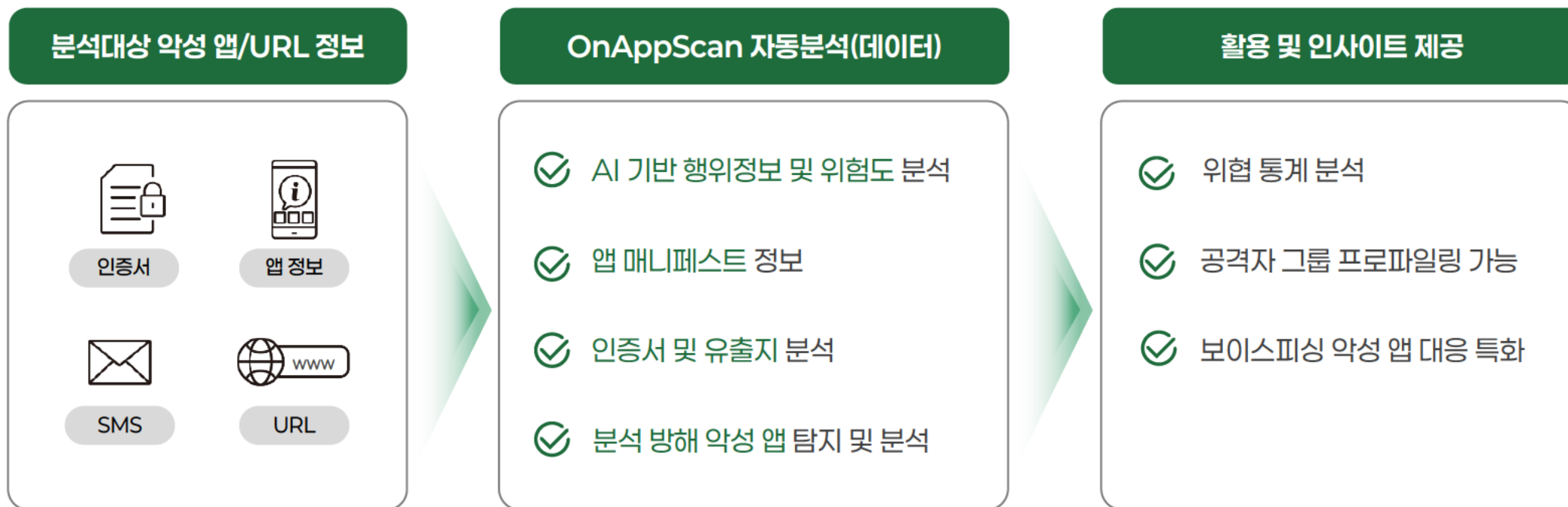
시큐리온 솔루션 대응 전략

- 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



2. 제품소개 (1)개요

AI 기반 악성 위협 자동분석 시스템 OnAppScan 위협 통계 및 분석 인사이트 제공, 보이스피싱 대응 특화



2. 제품소개 (2)제공 형태

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

2. 제품소개 (2)주요기능

세분화된 기능으로 판정, 분석, 연관 정보 제공
판정된 악성 앱 정보(위험도, 평판) 外 부가 정보 제공

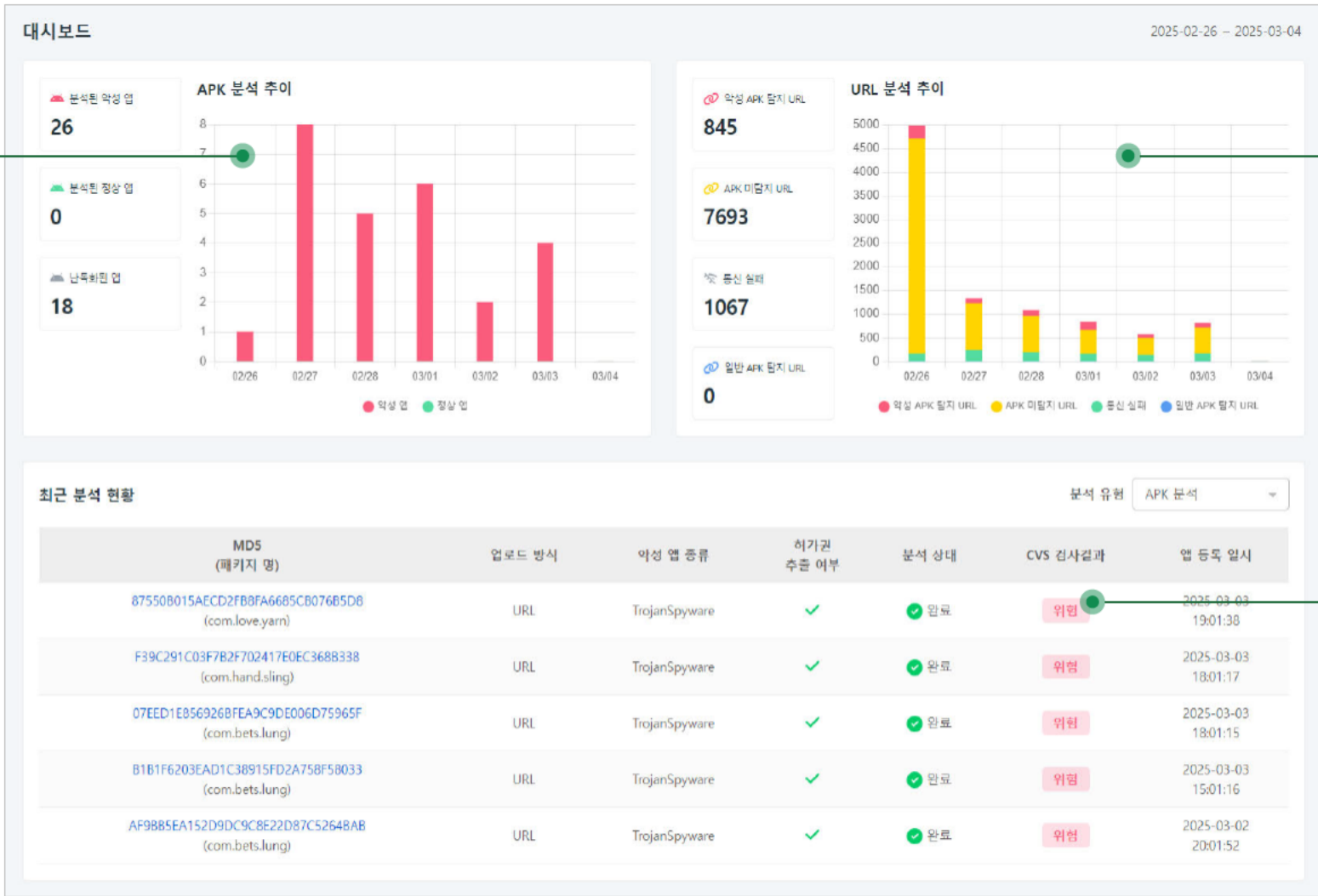
글로벌 유사 제품 기능 비교 *앱 분석, 글로벌 제품 V, A, J 등 대비 150% 수준의 기능 제공

구분	자체판정		앱 분석					위험도 분석				연관 앱 정보			리소스 뷰어	자동적 분석
	점수	등급	앱 정보	난독화 여부	인증서 정보	매니 페스트	유출지 정보	행위 정보	권한	String	API	동일 인증서	유출지	유사도 분석		
OnAppScan	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Malware.com	○	X	○	X	○	○	△	X	X	X	X	X	X	X	X	X
Hybrid-Analysis	○	○	○	X	○	○	X	△	○	X	X	X	X	X	X	○
AVAST	○	X	X	X	X	X	X	X	△	X	X	X	X	X	X	△
Avast	X	○	○	X	X	X	X	X	X	X	X	X	X	X	X	X
AVG Antivirus	○	X	○	X	X	○	X	X	○	X	○	X	X	X	X	X
BitDefender	X	○	○	△	X	X	X	X	X	X	X	X	X	X	X	X
AVG Secure	○	○	○	X	X	○	○	○	X	X	△	X	X	X	X	○

2. 제품소개 (2)주요기능

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 요청

APK 분석 요청

URL 분석 요청

업로드하려면 이곳에 파일을 올려놓으세요
또는
파일을 선택하세요.

최근 분석 현황

MD5 (패키지 명)	업로드 방식	악성 앱 종류	허가권 주출 여부	분석 상태	CVS 검사결과	업 종 류
9582f16140900410591bf9a37304b32a (net.lourtwentyfive.tek.views.20210512)	사용자 업로드	voicePhishing	✓	완료	위험	2025-02-04 10:56:07
2ED99FFEC7C800334A9D45DDC16A39BE (com.sitech.tianyinclient)	사용자 업로드	Adware	✓	완료	위험	2025-01-22 11:14:16
94f1b300d073e9a806168bd4502a72ec (com.square.cycles)	사용자 업로드	Trojan	✓	완료	위험	2025-01-22 11:13:42
C629FAD9336AC1F170C9AFA6E056F933 (com.wegweweg.weg.wsedrgweweg)	사용자 업로드	TrojanDropper	✗	완료	위험	2025-01-22 11:13:15
01C92FFBDBFC57DF7999C7426642308F (zjqicwq.qiohngnu)	사용자 업로드	Adware	✓	완료	위험	2025-01-21 15:13:13

- 분석 이력 검색

- 분석 내역

APK 분석 현황

내 분석

불러오기

Hash

MD5 / SHA1 / SHA256

업로드 방식

전체

권한

권한 유형 선택

등록 · 분석일

업 등록일

등록 분석일 선택

일제 검색

초기화

내보내기

MD5 (패키지 명)	업로드 방식	악성 앱 종류	허가권 주출 여부	분석 상태	CVS 검사결과	업 종 류
9582f16140900410591bf9a37304b32a (net.lourtwentyfive.tek.views.20210512)	사용자 업로드	voicePhishing	✓	완료	위험	2025-02-04 10:56:07
2ED99FFEC7C800334A9D45DDC16A39BE (com.sitech.tianyinclient)	사용자 업로드	Adware	✓	완료	위험	2025-01-22 11:14:16
94f1b300d073e9a806168bd4502a72ec (com.square.cycles)	사용자 업로드	Trojan	✓	완료	위험	2025-01-22 11:13:42
C629FAD9336AC1F170C9AFA6E056F933 (com.wegweweg.weg.wsedrgweweg)	사용자 업로드	TrojanDropper	✗	완료	위험	2025-01-22 11:13:15
01C92FFBDBFC57DF7999C7426642308F (zjqicwq.qiohngnu)	사용자 업로드	Adware	✓	완료	위험	2025-01-21 15:13:13
01C44C6A92AA4E7B743E81EE6D40435 (coic.ikeebcz.hzepauzd)	사용자 업로드	Adware	✓	완료	위험	2025-01-21 15:43:46
01B6BC68C82CF1DDC8AF79E61F1C10F (lvmidg.gwp.js)	사용자 업로드	Trojan	✓	완료	위험	2025-01-21 15:16:18
6AE8FF2790B4D2D85988F4B19C3654D (NULL)	사용자 업로드	NULL	✗	완료	안전	2025-01-17 10:13:16
4A91191E14C05538E1F07CB22A16165 (kr.co.secution.ontusts.agent)	사용자 업로드	NULL	✗	완료	안전	2025-01-03 13:40:58
8DC305C1F07B7A7463246ECF57F59779C (com.kero.dskmclient)	URL	Trojan	✓	완료	위험	2024-11-12 18:14:19

4페이지 중 1페이지

1

2

3

4

2. 제품소개 (2)주요기능

APK 분석 상세 기능

2. 제품소개 (2)주요기능

APK 분석 상세 기능

- 인증서 정보 및 동일 인증서 추적

인증서

이름	값	이름	값
SHA1	52E380550BBC9E09CAE5B2C6DACD8FB2B51AB40A		
SHA256	9A04829076D132D37CC42166A5B786CD15B588B750C1861FCAD35A9D2C7E6871		데이터가 없습니다.
지역			
국가	CN		

같은 인증서를 사용하는 다른 앱

앱 이름	패키지 이름	MD5	위험도
장례식장	com.kero.dsksmdkmf	5B03F8F0AB1F13F66C0FC9F7042851F6	위험

- Fuzzyhash를 통한 유사도 추적 결과

Manifest

Feature

유출지

유사도

APKID

VPDT

유사도

분석한 앱과 유사한 앱

앱 이름	패키지 이름	MD5	유사도	위험도
모바일 부+고(개인용).	com.kero.googlecom	C6D81F30CB17232A0EA7A099FEA5C4FC	66%	위험
모바일 부+고.	com.kero.slimming	C3689EA46473C7FDD644E169895DA7B9	71%	위험
모바일 부+고(개인용).	com.kero.googlecomkr	10296C54D3D2B970061A7A60ED3549E5	68%	위험
모바일 부+고(개인용).	com.kero.slimming	0A1EB5C1C6E932AA5441EFCB42DE1DAE	68%	위험
모바일 부고장(개인용).	com.kero.googlemsmsmsmsmsms	C64EFA2A5FE91740D8DDDCD3D1C810B0	65%	위험

55페이지 중 1페이지

1

2

3

4

...

>

>1

2. 제품소개 (2)주요기능

APK 분석 상세 기능

- 앱 평판 정보 제공
(바이러스토탈 연계)

분석 결과

Checks I App

패키지 이름: com.aj.VnIKmEkgvU
파일 크기: 3-377KB
MD5: 8f54e121d57ADF12676226BAAD579840
SHA256: A4593CAE9107687AA307D53A8388DA216

최소 SDK: API 23
앱 버전: 2.0
난독화: X

보통서 다운로드 v.t. 결과 재분석

23 / 64

23 security vendors and no sandboxes flagged this file as malicious

Size: 33.57 MB | Last Analysis Date: 1 month ago

android | obfuscated | apk | infection | contains obf

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Join the X2 Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.fakecalls.bankbot

Threat categories: trojan | trojan | trojan | trojan

Family labels: trojan | trojan | trojan

Security vendors' analysis

Vendor	Threat name	Category	Family
AlhLab V3	DroppeAndroiskash.024837	AlhLab	Trojan.Banker.Android.Fakecalls.7558F000
Avast Mobile	AndroidTrojan.792	Avast (no cloud)	Android.BankBot.FRG.Gen
BitDefenderBase	Android.Trojan.Banker.ZF	DrWeb	Android.Spy.KISD.origin
ESET-NOD32	A Variant Of Android.Trojan.Dropper.Agent	F-Secure	Makarov.ANDROID.BankBot.FRG.Gen
Fortinet	AndroidAgent.0248	Google	Detected
Ikarus	Trojan-Dropper.AndroidOS.Agent	K7GW	Trojan (900752d6f3)
Kaspersky	HEUR:Trojan-Banker.AndroidOS.Fakecalls.k	Linnix	Trojan.AndroidOS.Fakecalls.Cic
McAfee	AntivirusC188F507042	McAfee-GW-Editor	Antivirus.Trojan

- SDK를 통한
대량 분석 요청

OnAS SDK

1. settings.json 에 설정 값 입력

[settings.json]

VALUE

VALUE
onappscan 솔루션 email
onappscan 솔루션 비밀번호
onappscan 솔루션 url - KISA 서버: 175.106.98.232

command

nx_sdk.py {file_path}

sh 에 디렉터리 경로 입력시 내부 모든 파일 upload

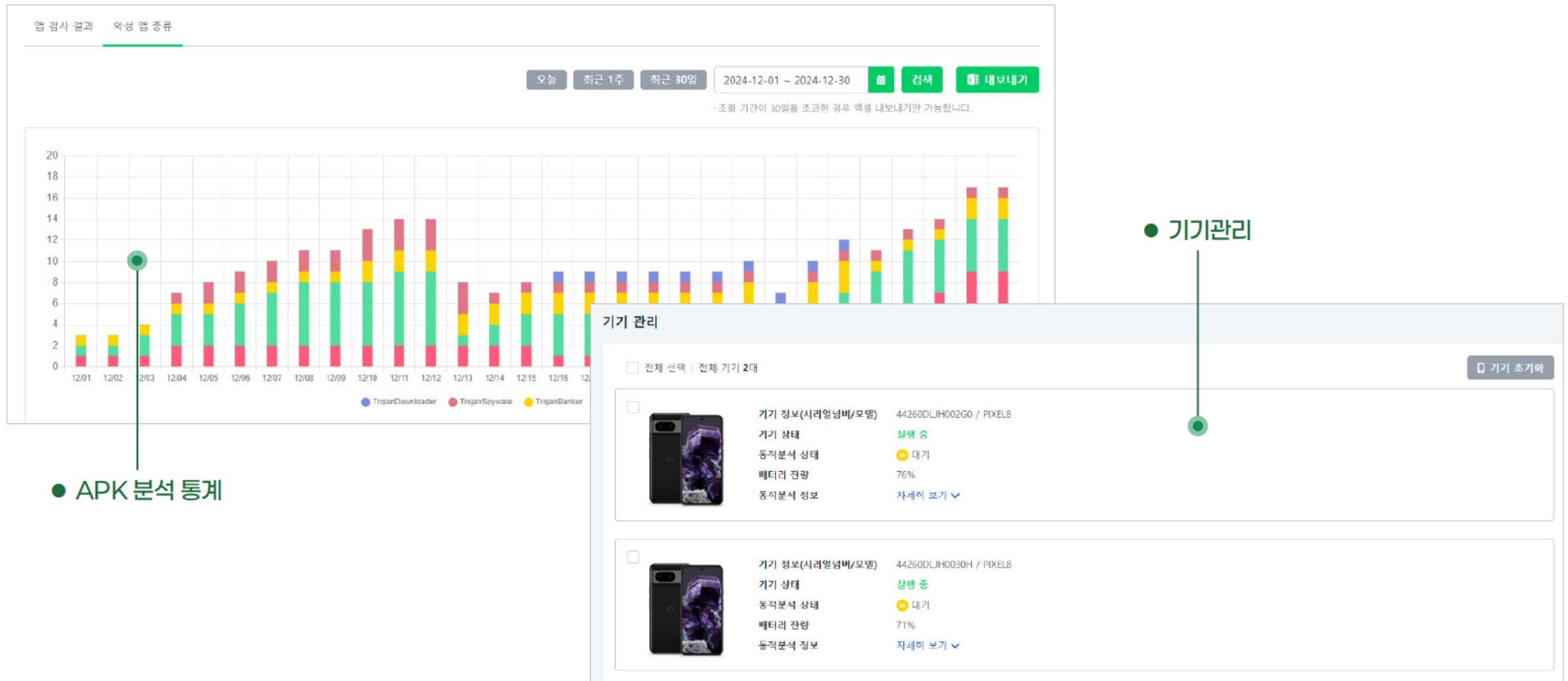
sh 에 apk 경로 입력시 1개 apk 만 upload

로드된 apk 는 재분석 됩니다.

```
{
  "is_succeeded": true,
  "response": {
    "failed_apk_paths": [
    ],
    "succeeded_apk_paths": [
      "C4AD5DD7FE30A61B57B8F3B08E2A8C8D.apk",
      "46A1D9A8E93ED39C6D5054D24D21555B.apk",
      "8F2A242A745E8688006380C24541457E.apk",
      "3C19378AE9CA9B7EE81D320F4429E933.apk",
      "C33C054C79A61626CD879CBCE9F5DA.apk",
      "C248B0E667AE5EF4E628CBCEB14BA8B.apk",
      "AE5B38D12AA75764EF46F46559B3F083.apk",
      "9DOC2185D86AB12028B25F521E0F4E3C.apk",
      "BB9C44CF131D8C7F63DC3B5B2445C57.apk",
      "08F974F9A92CA58202A144D7A4445696.apk",
      "A23F3F3499AD6F79171DE22FAB327111.apk",
      "9B586FEDC97802A4A0F3A0AD3D416769.apk",
      "86F29E5062755BDA3F2DDDF5078BEC85.apk",
      "FE3B90D47C38A23E1EEC4C27B62A6C7A.apk",
      "B26C342E0F6D57FABFB9ACD945D87C2B.apk",
      "840CA72AA6E4B3B667F296E9A9154A2.apk",
      "68C5998248F60DC22CE32EBAB868D6F6.apk",
      "8F43FD0005DFF750DE080AF006A9F20D.apk",
      "8630EF8E700EC3F8468D8FCB8C9FB986.apk",
      "4074152B83DFA07FFC8AC006A650B8CE.apk",
      "CC447B9019474846DA051482583E47BD.apk",
      "83C24EA96CDE6EB9812982436BA1C7A9.apk",
      "com.nhn.android.band.apk",
      "7E972CB5EAB1E0CA19D71489886BEF44.apk",
      "6BF8A06D223ACC13D0A4D28DDCF201C5.apk",
      "52397AAFE2B8B461DE486EEF44CE9AFB.apk",
      "F7F0332CDE548E947B6876A2DA43E60.apk",
      "A9B3535273A358AB3E1D6C23EABBE28F.apk",
      "AF09DEEC02F7F84482043EEC8452D24E.apk",
      "8B9F43C9B124CC595714E1D67C11AA73.apk",
      "E858DF5CB4CCEDE270141EF3D8DD1D07.apk"
    ]
  }
}
```

2. 제품소개 (2)주요기능

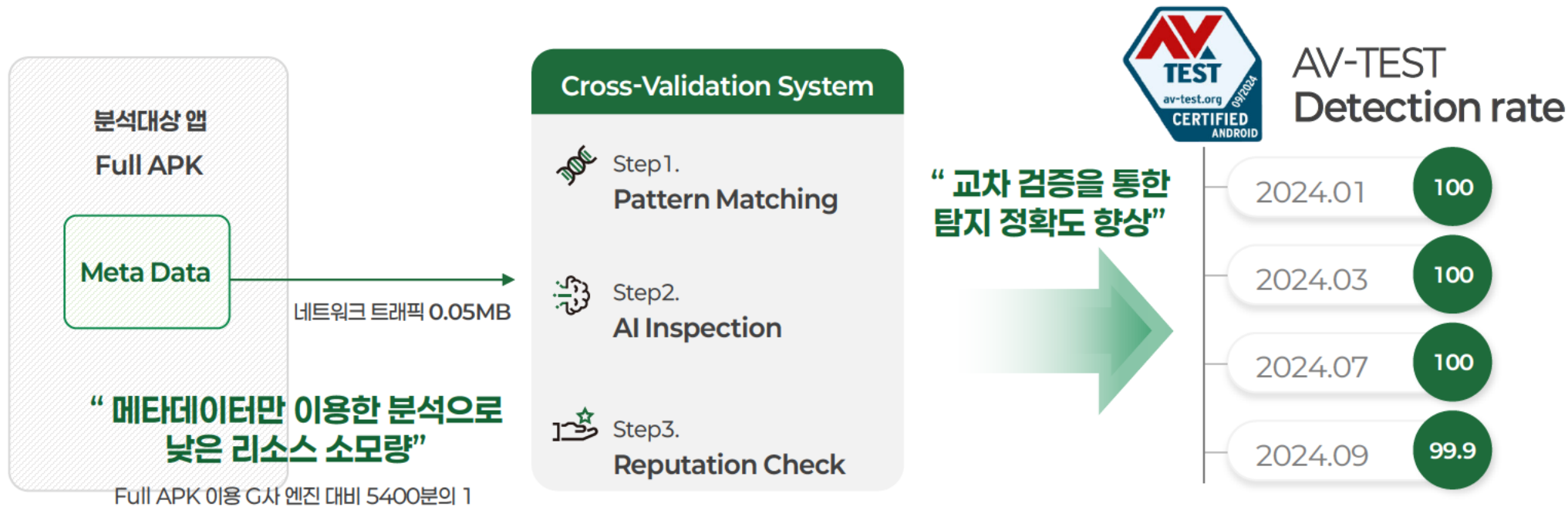
관리 기능



2. 제품소개 (3)핵심기술

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”



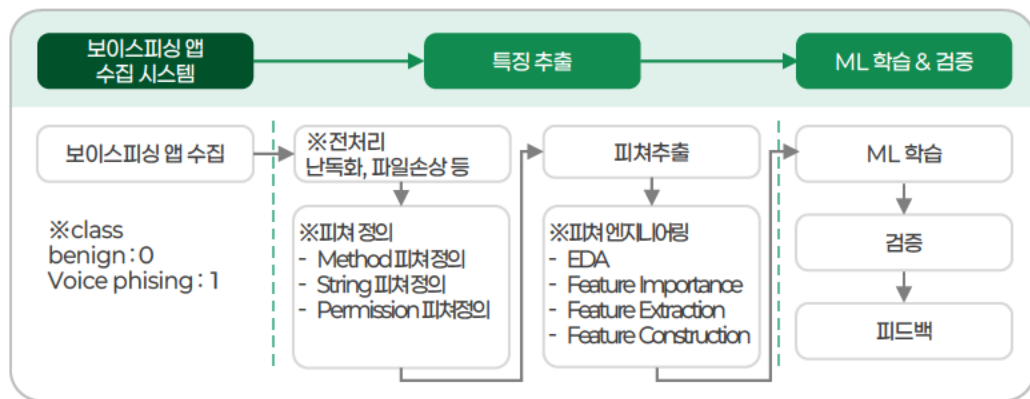
2. 제품소개 (3)핵심기술

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

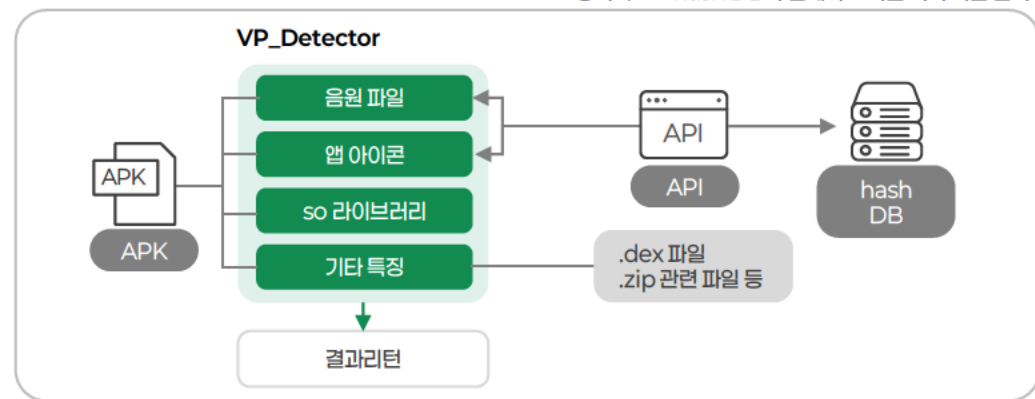


파일의 구조적 특징을 활용한 휴리스틱 탐지
(파일 내부 ARS 음원, APK, ZIP, DEX, SZ 파일 포함 유무 검사)

보이스피싱 디텍터
탐지율
99.3%

총 수집 악성 앱 139개
2023년 STA ICT 시험인증 연구소

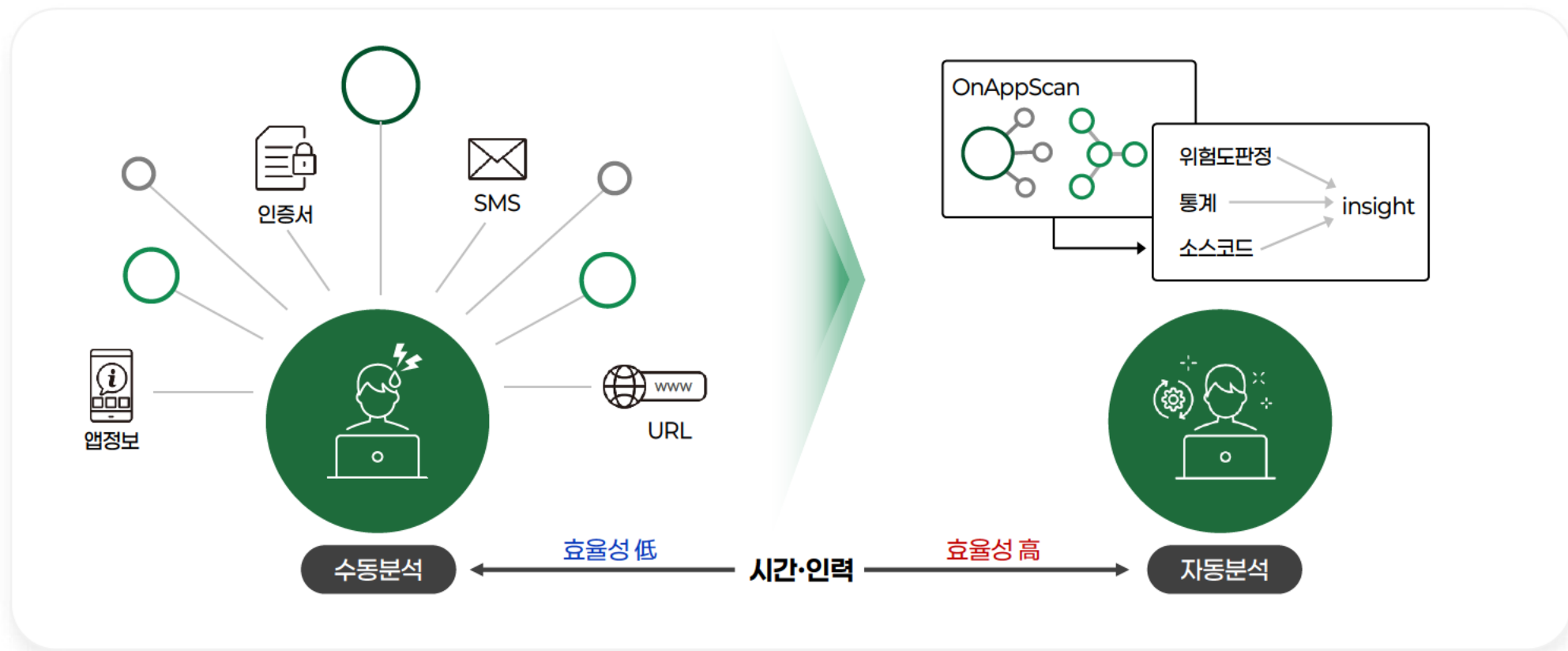
*정기적으로 hash DB가 업데이트 되는 서버 기반 검사



* IITP ‘휴대폰 단말에서의 보이스피싱 탐지, 예방 기술 개발’ 사업 성과를 상용화 제품(관계사 아이넷캡 수행)

3. 기대효과

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 ”



3. 기대효과

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
피쳐 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
피쳐 추출 불가1개(파일손상)

4. 적용 분야

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



통신·금융·게임 등 고객 피해 방지

사칭 앱, 피싱 범죄 많은 특수 산업군 대상
이용 고객 및 비즈니스 보호



앱마켓 등 대량 분석 수요처 효율 강화

대량의 앱 데이터를 실시간 자동검사, 마켓 침투 악성 앱 제거
맞춤형 SI 모델링으로 탐지 정확도 향상



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)

5. 인증 및 수상

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

시험 성적서

STA ICT (한국정보보호진흥원)

평가번호: 24-A001-C029

평가사명: STA ICT (한국정보보호진흥원)

평가사주소: 서울특별시 강남구 테헤란로 119, 11F (강남구)

평가사전화: 02-558-1234

평가사팩스: 02-558-1235

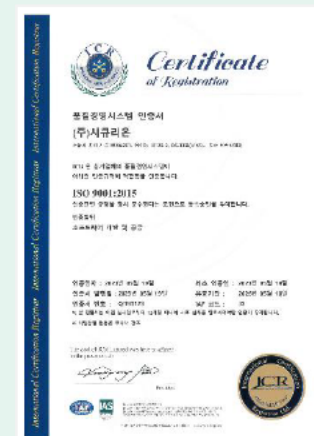
평가사홈페이지: www.sta-ict.com

시험 결과 요약

No.	시험항목	시험기준	시험결과
1	음성 탐지율 (음성 탐지율)	95% 이상	합격 (95%)
2	음성 탐지 정확도 (음성 탐지 정확도)	90% 이상	합격 (90%)
3	음성 탐지 속도 (음성 탐지 속도)	10초 이하	합격 (10초)
4	음성 탐지 정확도 (음성 탐지 정확도)	95% 이상	합격 (95%)
5	음성 탐지 정확도 (음성 탐지 정확도)	95% 이상	합격 (95%)
6	음성 탐지 정확도 (음성 탐지 정확도)	95% 이상	합격 (95%)
7	음성 탐지 정확도 (음성 탐지 정확도)	95% 이상	합격 (95%)
8	음성 탐지 정확도 (음성 탐지 정확도)	95% 이상	합격 (95%)
9	음성 탐지 정확도 (음성 탐지 정확도)	95% 이상	합격 (95%)

본 성적서에 기재된 시험 결과는 STA ICT (한국정보보호진흥원)에서 시험한 결과입니다. 시험 결과에 따라 시험 합격 여부를 결정합니다.

시큐리온 ISO9001 품질경영시스템 인증



6. 특허

핵심기술 국내 IP 확보



리눅스 커널 무결성 검사 및
데이터 복구



현대 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

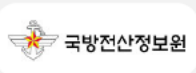


스미싱으로 인한 고객 피해 방지

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

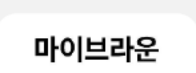
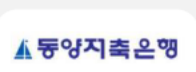
공공 보안

- 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