AI를 활용한 모바일 안드로이드 보안 위협 대응 기술

머신러닝을 활용한 모바일 보안 위협 대응

㈜시큐리온 유동훈 (x82)

2021-09-16

AIS 2021
2021인공지능 보안 컨퍼런스

SECURI ON

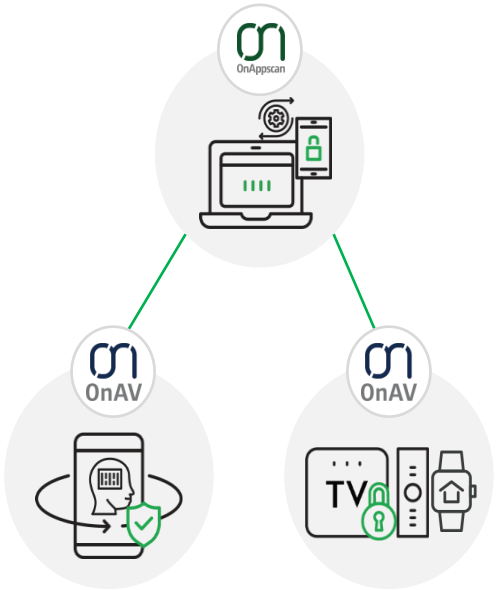
소개 - 회사


OnSecure Holdings
온시큐어홀딩스
• 법인. 2017~
• 법인. 2005~
• 무선. 2010~
아이넷캅
SECURI ON
시큐리온
• 개발. 2015~
• 법인. 2019~
2011~
정부 기관 포렌식 제품 납품 및 취약점 R&D
HARVESTER
framework
KISA
CONODONT
NAUTILUS
2011~2012 2년 앱 분석
2012~ 24시 스미싱 대응 및 공동 R&D
Smart Vaccine
AROWANA
2012~ 1200/300만
2014.09 Preload
Secured by Knox
COELACANTH
2013~2014
2년 공동 R&D
OnAppScan
OnAV
OnAV for TV
스마트 워치
커넥티드 카

소개 - 기술

1) 'ON' 브랜드 제품 라인업
- 안드로이드 기반 제품
- iOS 기반 제품

OnAppScan
- Cloud online (B2B/B2C)
- Server appliance (B2B)



OnAV For Mobile (B2B/B2C)

OnAV For IoT (TV/Watch)

2) 'ON' 브랜드 제품 취득 인증 자격

AV-TEST
2018.07 ~ (18회 연속)

AV-Comparatives
2019.03 ~ (3회 연속)

MRG-Effitas
2019.06 ~ (2회 연속)

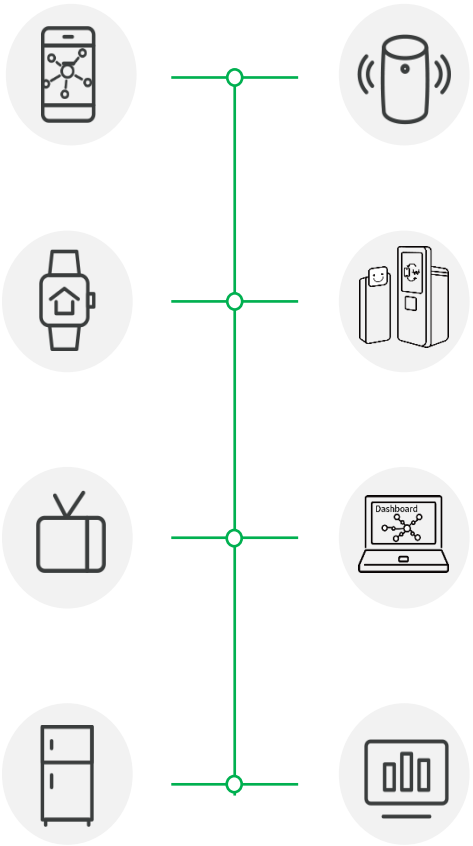
PCSL
2018 ~ 2019 (4회 연속)

SKDLabs
2019

GS인증

AMTSO

3) OnTrust 제품 라인업 확장
- 악성 및 Exploit 위협 탐지 기술
- TMS, Kiosk, Recovery-Box 등



배경 - 뉴노멀 코로나19 시대

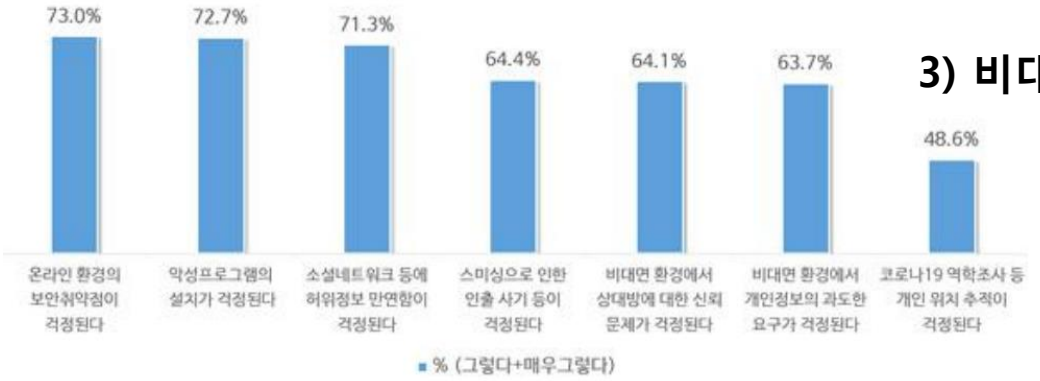
1) 전체 응답자 42.6%가 일 평균 4시간 이상 인터넷

- 전체 응답자의 86.3%가 스마트 기기 이용 접속
- 63.1%가 코로나19 이후 증가

출처: 한국인터넷진흥원

2) 비대면 업무 환경 변화

- 전체 응답자 36.7%가 코로나19 이후 재택근무 경험
  - 재택 근무로 인한 클라우드 활용 업무 증가
  - 모빌리티, BYOD, 스마트 기기 활용 업무 증가



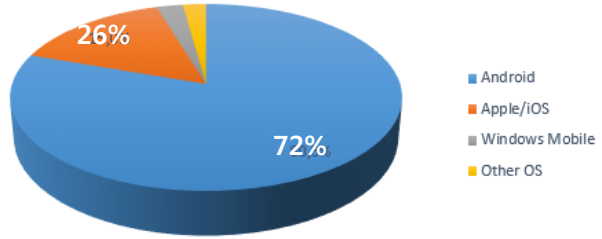
3) 비대면 환경의 보안 위협에 대한 불안감 증가

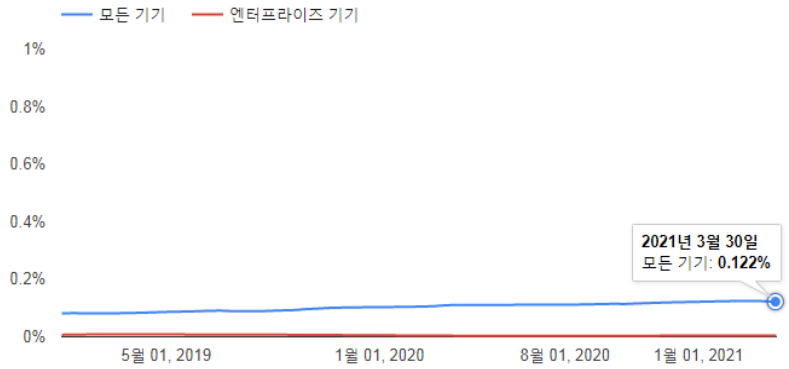
- 취약점(73%), 악성 프로그램(72.7%), 허위정보(71.3%), 스미싱(64.4%) 등

배경 - 해외 모바일 위협 현황

1) 21년 7월 기준 전세계 사용자 72% 이상 Android 이용

출처: https://gs.statcounter.com/os-market-share/mobile/worldwide





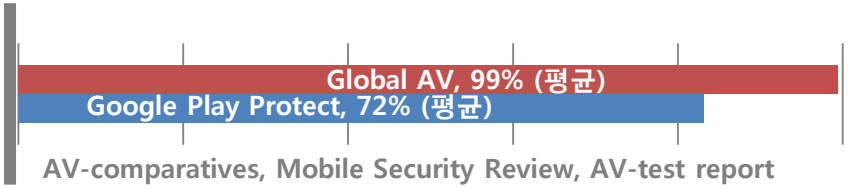
2) 구글에서 조사한 마켓 감염 사례

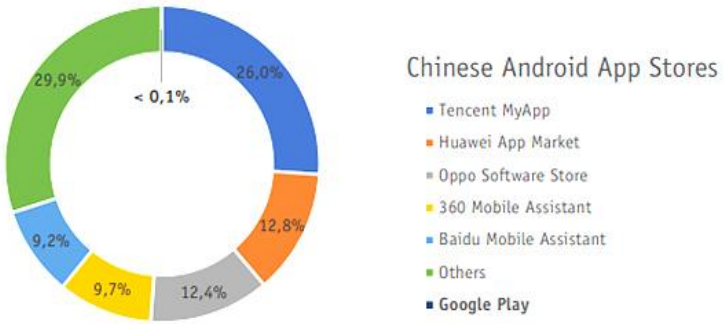
- 구글 보고서, 매일 20억대 기기 대상 800억 개 앱 검사
- 기기: 0.12%, 마켓 감염: 0.065% 수준

출처: 구글 안드로이드 생태계 보안 투명성 보고서:
https://transparencyreport.google.com/android-security/overview?hl=ko

3) 구글 조사 통계의 한계점

- 구글 플레이 프로젝트의 낮은 악성 탐지율 문제
- AV-Test 연평균 61%, Av-comparatives 83% 탐지율





4) 중국, 사용자 중 26% 가량만 구글 마켓 이용

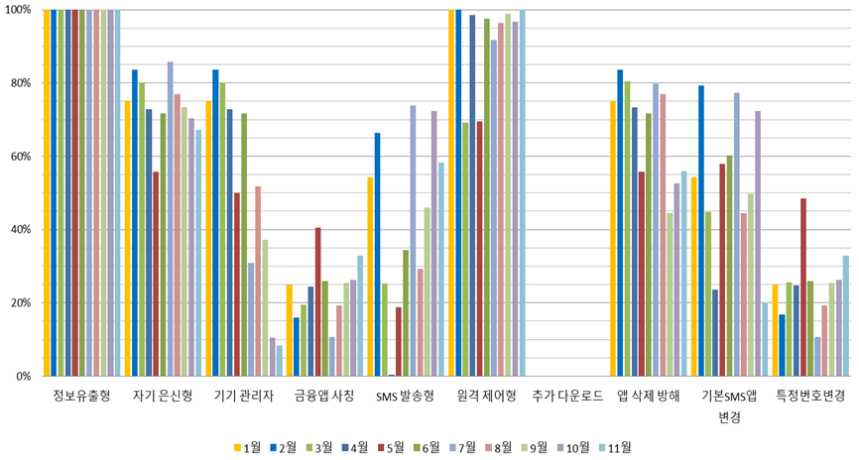
- 구글 노력에도 아시아 최대 시장 악성 앱 유통 이슈 해결 불가

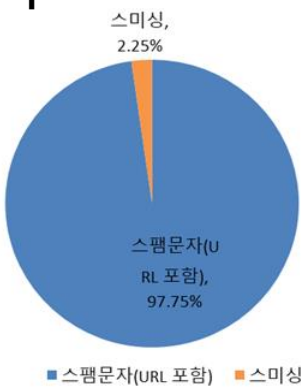
배경 - 국내 모바일 위협 현황

1) 20년 기준 SMS 스팸 문자 중 악성 앱 2.25% 차지

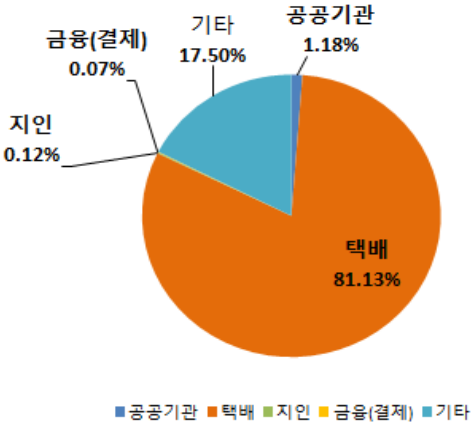
- 스팸 문자 3,800만 건 중 스미싱 문자 88만 건 차지
  - 생활 밀착형 (택배) 사칭 81.13%로 증가 추세
  - 난독화 된 앱로 73% 증가 추세

출처: 한국인터넷진흥원





2020년 스미싱 키워드별 분류

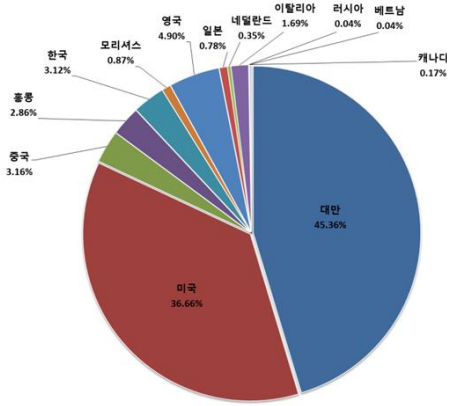


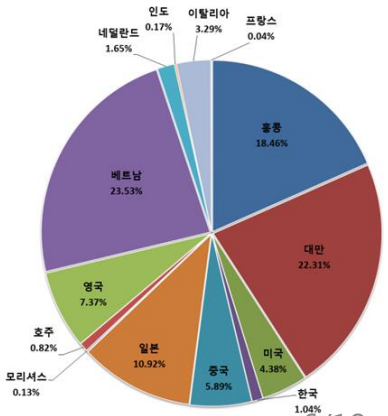
2) 악성 앱 대다수가 SMS로 전파

- 정보 유출, 원격 제어, 자기은신, 기기 관리자 등록 행위 순
  - 알려진 앱 사칭, 추가 기능 다운로드 설치 유도
  - SMS, 주소록, 기기 정보 유출, 금융 정보, 인증서 탈취

3) 악성 앱 유포지와 유출지 대부분이 해외

- 악성 앱 유포지는 대만(46%)이 압도적, 미국(38%)
- 정보 유출지는 베트남(23%)과 대만(22%)이 과반수 차지



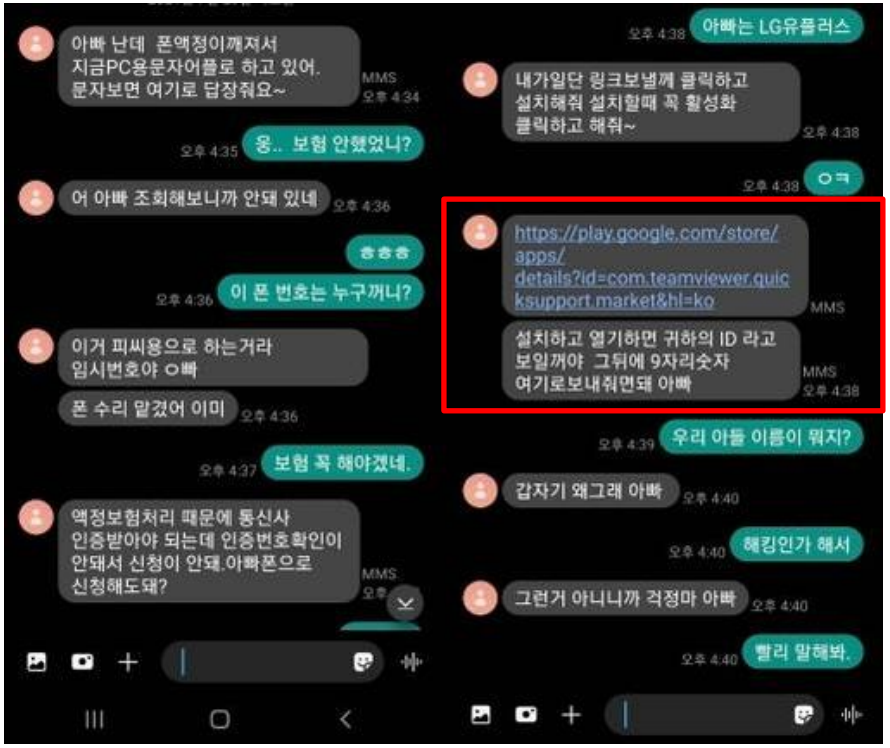


배경 - 최신 모바일 위협 현황

1) 원격 제어 앱 설치 유도 메신저 피싱 사례

- 팀 뷰어 등과 같은 “정상 범주 악용 앱” 설치 유도
  - 20년 373억 원으로 전년 대비 9.1% 증가
  - 실제 피해자 중 50대 여성(28.4%), 60대 여성(27.1%)이 가장 취약

출처: 경찰청



- 참고: https://github.com/mvt-project/mvt/
  https://mvt.readthedocs.io/en/latest/

Mobile Verification Toolkit

pypi v1.0.12

Mobile Verification Toolkit (MVT) is a collection of utilities to simplify and automate the process of gathering forensic traces helpful to identify a potential compromise of Android and iOS devices.

It has been developed and released by the Amnesty International Security Lab in July 2021 in the context of the Pegasus project along with a technical forensic methodology and forensic evidences.

Warning: this tool has been released as a forensic tool for a technical audience. Using it requires some technical skills such as understanding basics of forensic analysis and using command line tools.

Please check out the documentation.

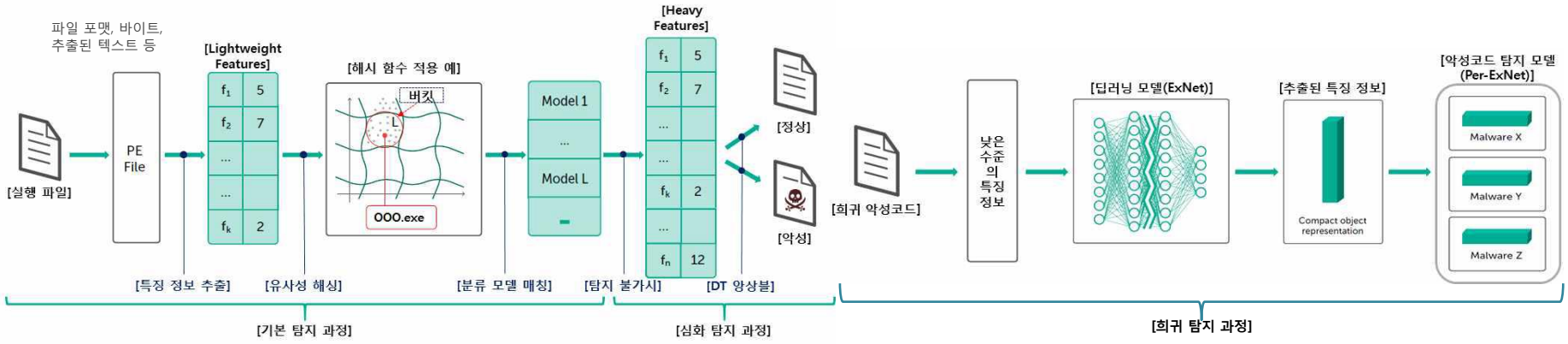
2) VIP 대상 공격 사례 증가

- 이스라엘 NSO 그룹의 페가수스 모바일 스파이웨어 사례
  - 각 국가별 VIP 위치 정보 유출, 각종 메신저, 문자 내역 등 주요 기기 정보 탈취

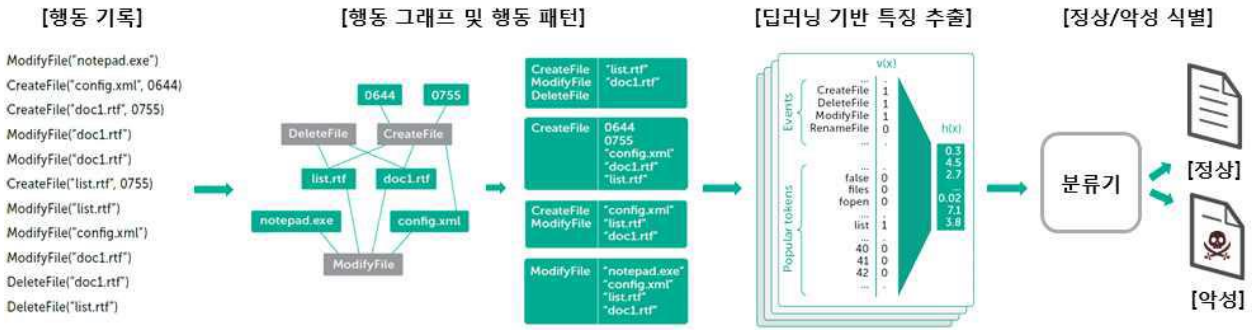
동향 - 해외 대응 기술 현황: 보안 업체

카스퍼스키랩: 실행 전, 후 단계로 구분된 다-단계의 머신러닝 탐지 기술

- 악성코드 실행 이전(Pre-execution) 단계
  - 기본 탐지: 실행파일의 기본 특정 정보로 LSH를 응용한 유사성 해싱 함수로 유사 악성 분류
  - 심화 탐지: 실행파일에서 추출 가능한 모든 특징 정보로 DT 앙상블 모델링을 통해 악성 분류
  - 희귀 탐지: 딥러닝 모델(ExNet)로 특징 정보 추출 후 Per-ExNet(Per-exemplar classifiers)으로 분류



- 악성코드 실행 이후(Post-execution) 단계
  - 악성코드 실행 후 수집한 정보(이벤트, 프로세스 행위)로 딥러닝 모델 학습
  - 실행 시 수집되는 프로세스 동작 기록으로 행동 그래프 및 행동 패턴 생성
  - 딥러닝 모델로 생성된 행동 패턴의 주요 특징 추출 및 분류

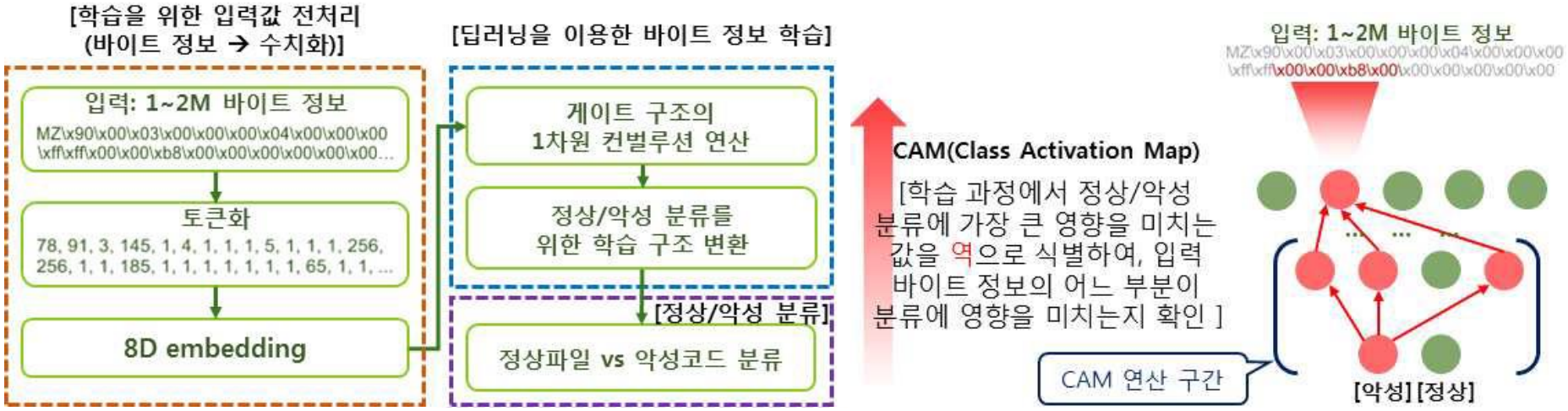


출처: 머신러닝을 활용한 해외 기업의 악성파일 탐지 연구 소개 – 금융보안원 보안기술연구팀

동향 - 해외 대응 기술 현황: ML H/W 개발사

엔비디아: 딥러닝 기반 악성코드 분류 모델(Malconv)을 통한 탐지 기술

- 정적 바이너리 대상(Pre-execution) 딥러닝 모델 적용 + CAM 연산 활용한 분류 근거 도출
  - 학습을 위한 입력 값 전처리: 실행파일 바이트 정보를 적합한 형태로 변환
  - 바이트 정보를 합성곱 신경망(CNN) 기반으로 딥러닝 학습 및 분류
  - 분류 기준 도출: CAM(Class Activation Map) 방식 활용, 실행파일이 악성코드로 분류된 근거 발견
  - 시험 검증: 바이트 블록, 파일 메타 정보 특징을 활용한 타-학습 모델과 정확도를 비교하여 타당성 검증



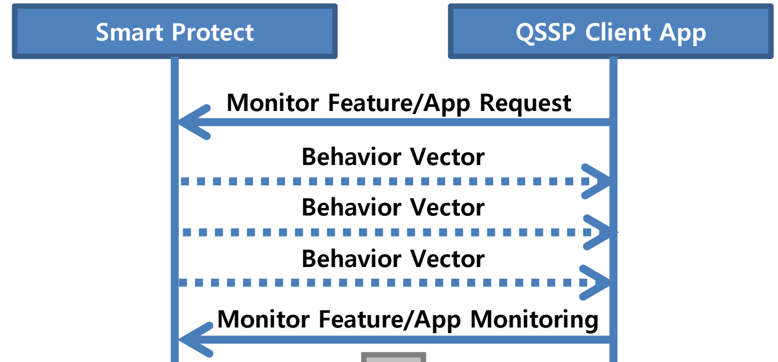
- 엔비디아에서 정리한 악성 분류 모델(Malconv) 특징
  - 두 개의 전혀 다른 출처로부터 데이터 세트를 수집하고 그룹 A,B로 구분
    그룹 A, B 중 하나의 그룹으로만 모델 학습 진행, 다른 그룹으로 성능 검증
  - 바이트 정보만 학습, 특징 추출 과정 축소 및 특징 의존성 낮춤, 변종 탐지율 강점
    (학습 과정의 계산 복잡도가 바이트 정보 길이에 선형적으로 증가)
  - 탐지 영향을 미치는 요인 추적, 바이트 정보와 맵핑 되는 부분을 식별하여 설명 가능

출처: 머신러닝을 활용한 해외 기업의 악성파일 탐지 연구 소개 – 금융보안원 보안기술연구팀

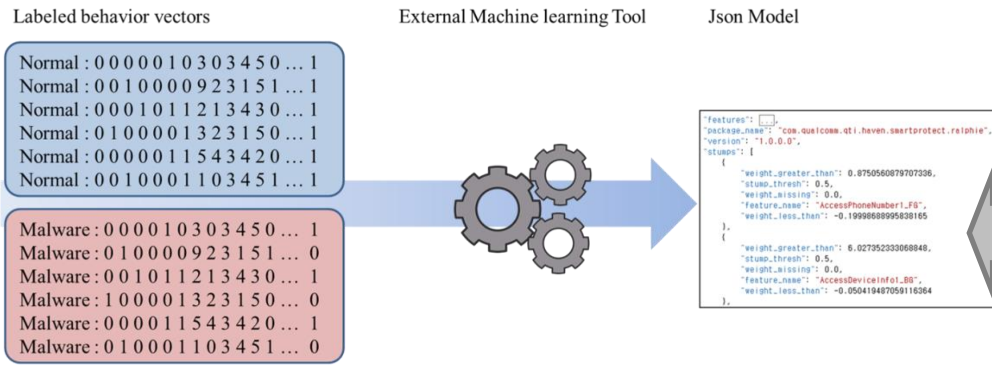
동향 - 해외 대응 기술 현황: SoC 제조사

퀄컴: QSSP 동적 행위 기반 머신러닝(Decision Stump) 악성 앱 탐지 기술

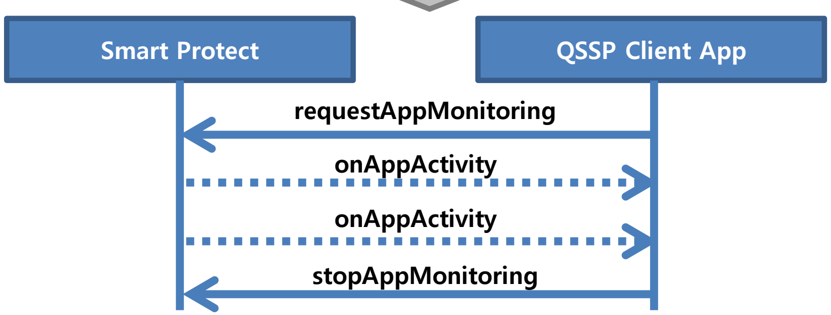
- OS 커널과 프레임워크 수정을 통한 앱의 행위 기반 정보 추출
  - 실제 앱 동작 후 모니터링 하여 동적 행위 정보를 얻는 방식
    - 전체 행위는 약 370개의 벡터(double 형)으로 구성
  - BDS 기반 ICSIBoost, AdaBoost 등을 통해 학습 모델링
  - 앱 실행 시 행위 모니터링으로 악성 여부 판정
    - 악성 행위는 약 130개의 원인 정보에 대한 근거 제공
    - 레벨 1-2: 악성, 3-5: 위험, 6-7: 의심



Code	Feature Name	Feature Type	Data Type
1	Comm1_FG	cumulative_rate	double
2	Comm1_BG	cumulative_rate	double
3	Comm2_FG	instantaneous_rate	double
4	Comm2_BG	instantaneous_rate	double
5	AccessUI_FG	cumulative	double



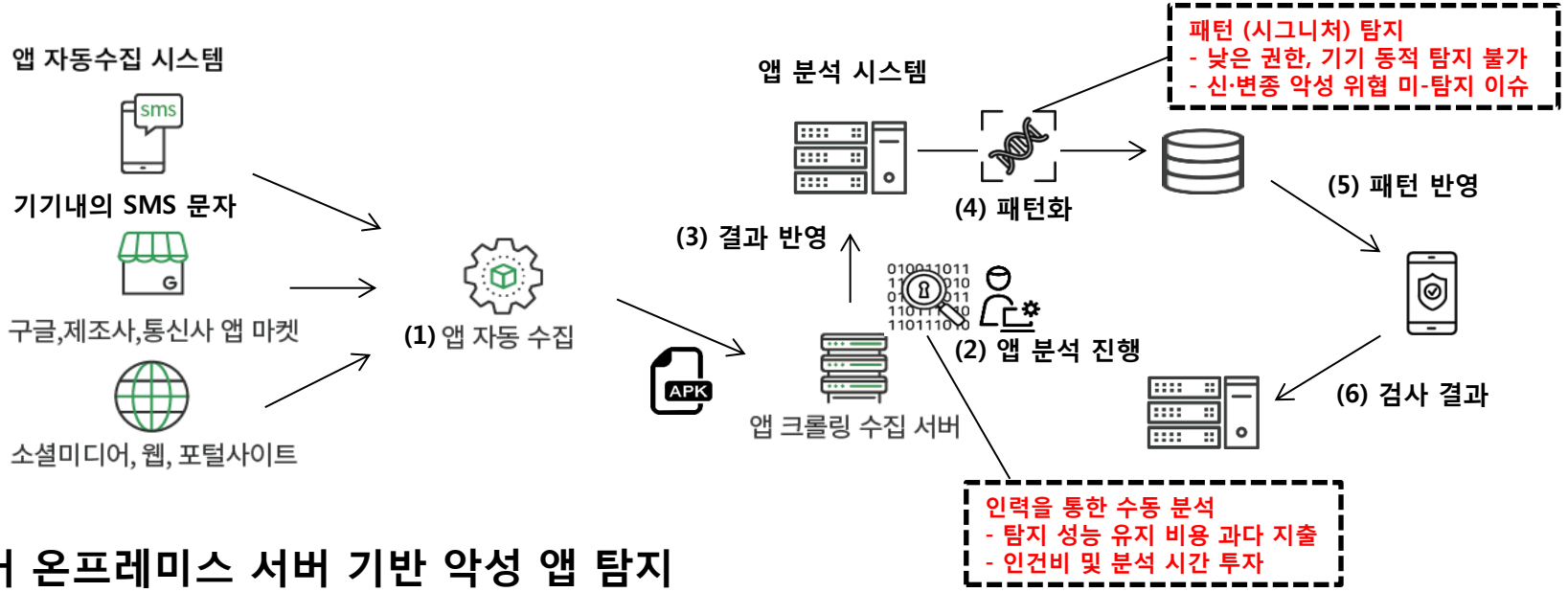
com.qualcomm.qti.haven.smartprotect.ralphie D/LibraryHandler: bv:
0.0,145.07654281736518,0.0,317.0,0.0,8.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0,
0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,
0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,...



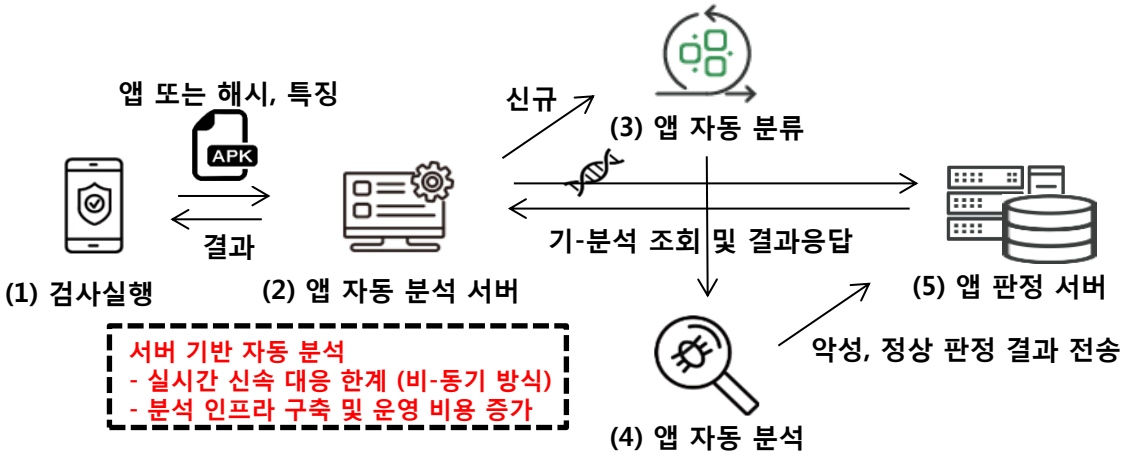
Index	Cause String
1	Snooping on UI while application not visible to user
2	Suspicious usage of android ID
3	Suspicious usage of android ID in background
4	Accessing of device info (like IMEI)
5	Accessing of devuce info (like IMEI) in background
6	Accessing of phone number
7	Accessing phone number in background

본론 - ㈜시큐리온의 대응 기술 개발 필요성

1) 과거 전통적인 패턴 기반 악성 앱 탐지

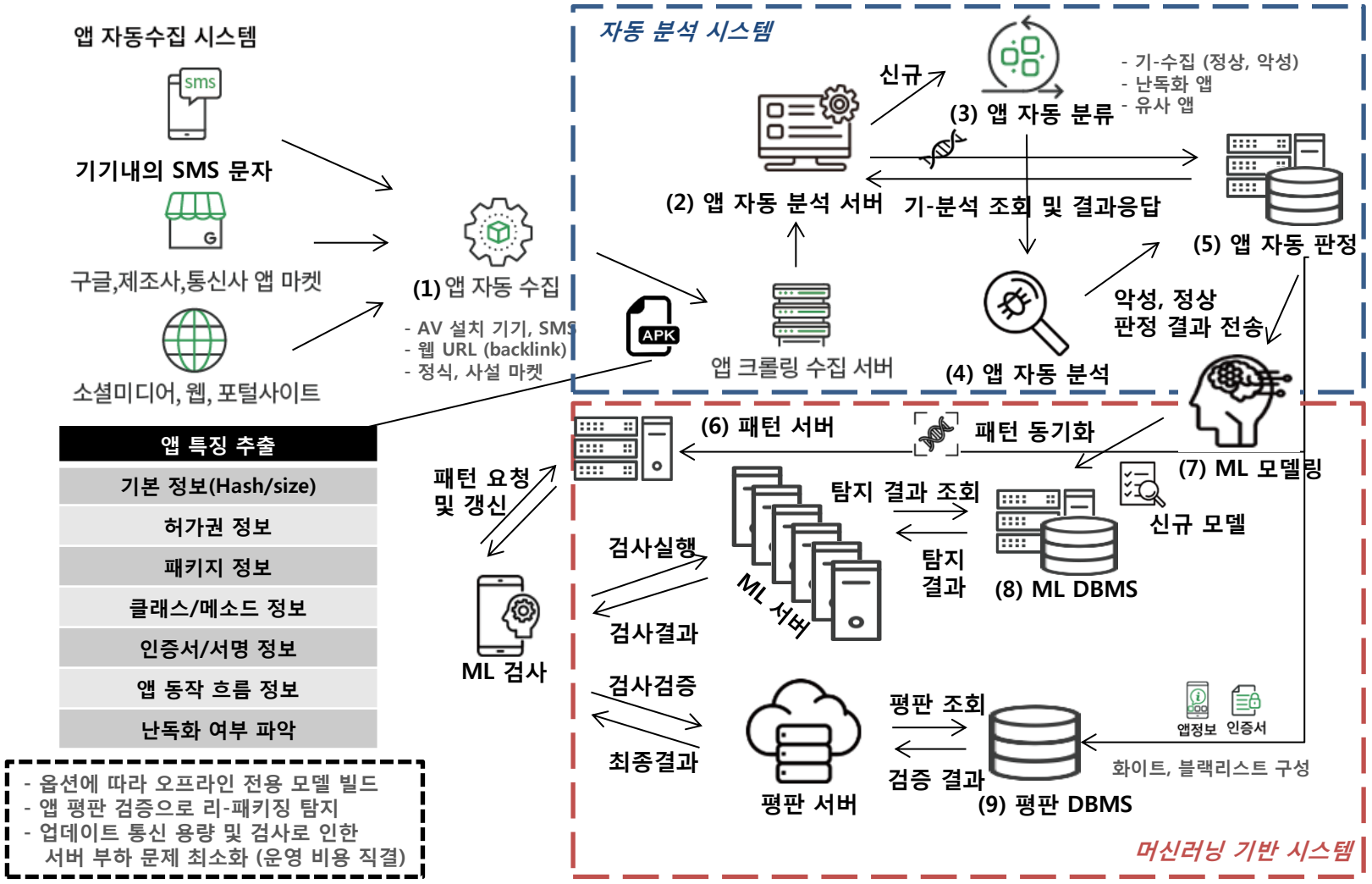


2) 과거 온프레미스 서버 기반 악성 앱 탐지



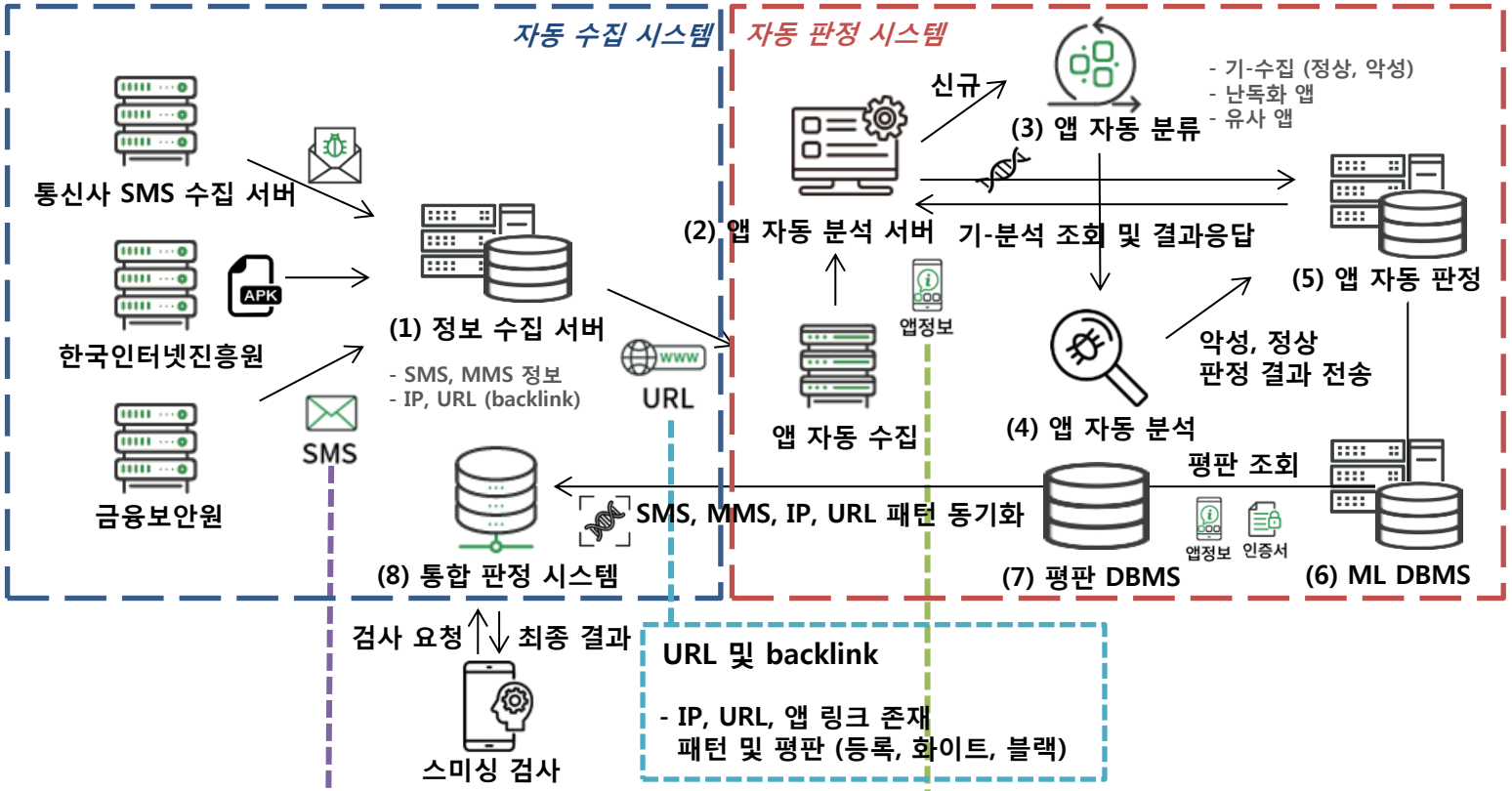
본론 - ㈜시큐리온의 대응 기술 현황

클라우드 서버 머신러닝 기반 악성 앱 탐지



본론 - ㈜시큐리온의 대응 기술 현황

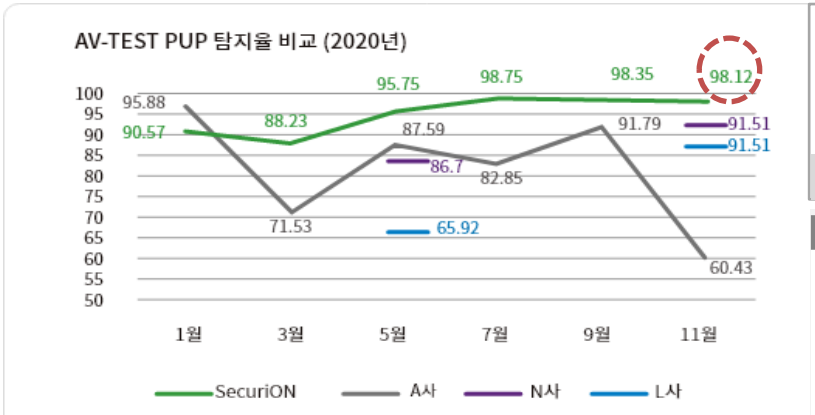
문자메시지 기반 악성 행위 탐지



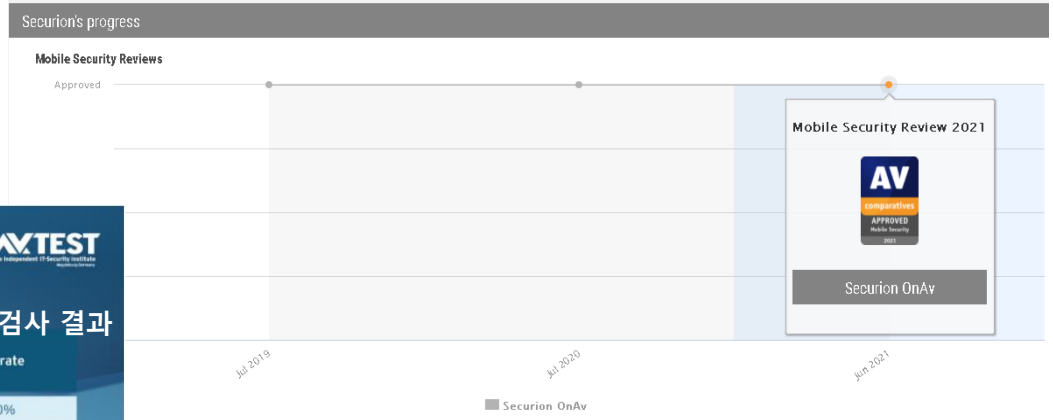
본론 - ㈜시큐리온의 대응 기술 경쟁력

지난 3년간 글로벌 인증 평가 기관 성적

출처: Av-test 2020년 평가점수 평균(총 6회), Av-comparatives 등



독일 18회	오스트리아 3회	영국 2회	중국 4회	중국 1회



출처: Av-test 21년 7월 검사 결과

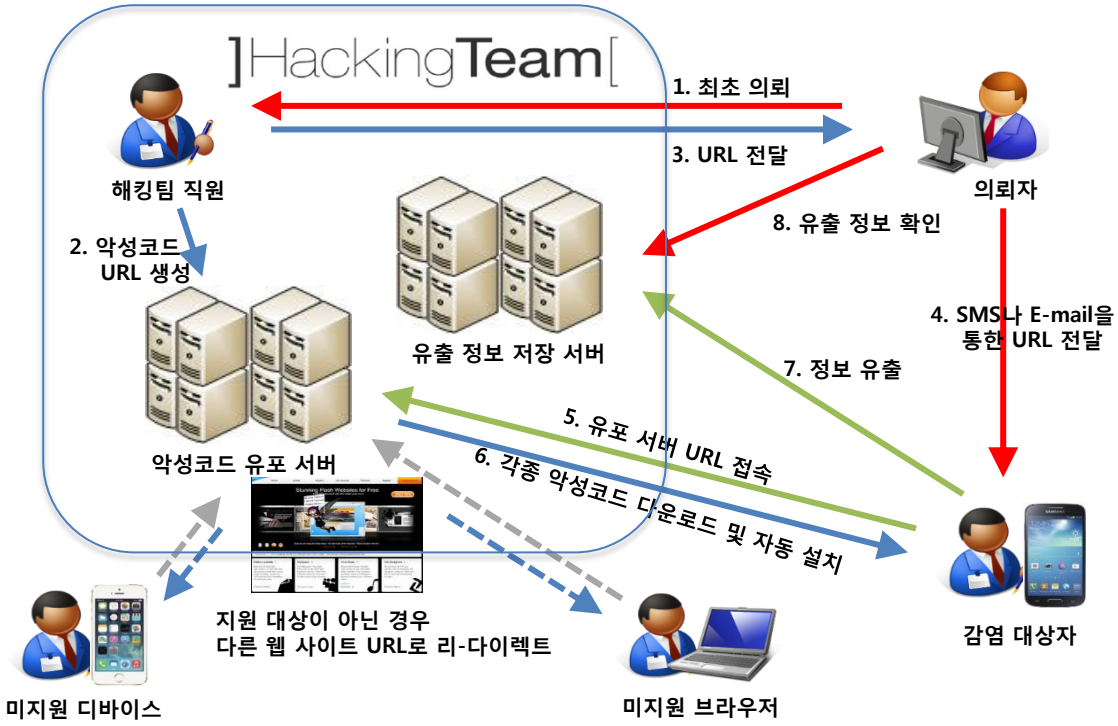
Manufacturer	Product	Detected stalkerware apps	Undetected stalkerware apps	Detection rate
Antiy	AVL	29	0	100%
Bitdefender	Mobile Security	29	0	100%
Trend Micro	Mobile Security	29	0	100%
ESET	Mobile Security	28	1	96.6%
Kaspersky	Internet Security for Android	28	1	96.6%
F-Secure	SAFE	27	2	93.1%
G DATA	Mobile Security	27	2	93.1%
securiON	OnAV	26	3	89.7%
Avast	Mobile Security	24	5	82.8%
AVG	AntiVirus FREE	24	5	82.8%
Avira	Antivirus Security	24	5	82.8%
McAfee	Mobile Security	24	5	82.8%
Protected.Net	Total AV	24	5	82.8%
AhnLab	V3 Mobile Security	23	6	79.3%
Ikarus	mobile.security	23	6	79.3%
LINE	Antivirus	21	8	72.4%
NortonLifeLock	Norton 360	17	12	58.6%
Google	Play Protect	9	20	31.0%

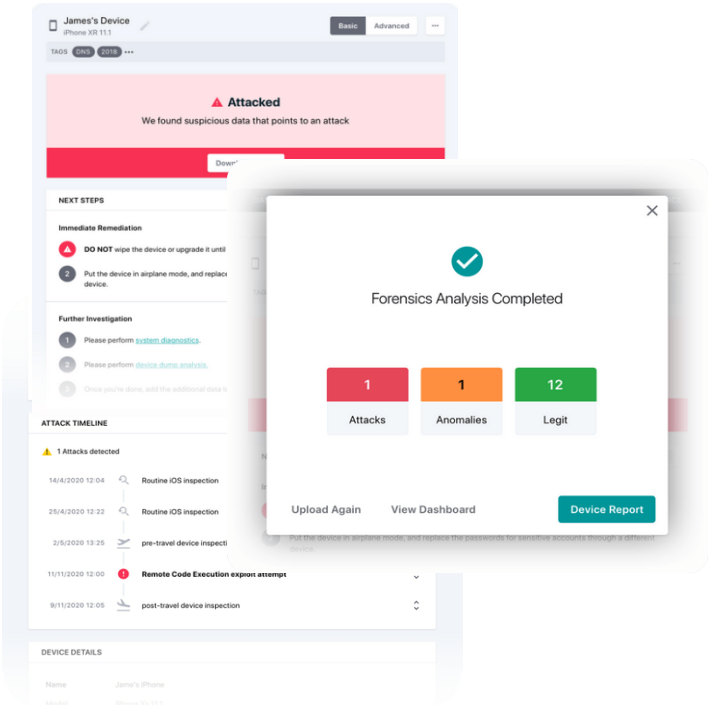
- 잠재적인 악성 앱 (PUA: Potentially Unwanted App), 타사 대비 알려지지 않은 신·변종 악성 앱 높은 탐지율
- ML 기술로 인력 및 비용 투자 규모 대비 우수한 성적
- 최근 스파이 앱(스토커웨어) 탐지 검증 결과
  - 29가지 스파이 앱 대상 글로벌 18개 AV 제품으로 검증 진행
  - 3개사만 전체 탐지 성공, ㈜시큐리온 OnAV 8위 선정

결론 - ㈜시큐리온의 대응 기술 고도화 필요성

HackingTeam과 NSO그룹의 비즈니스 모델

- 이태리 HackingTeam은 Shadowbroker에 의한 정보 유출로 서비스 중지, 이스라엘 NSO 그룹은 건재





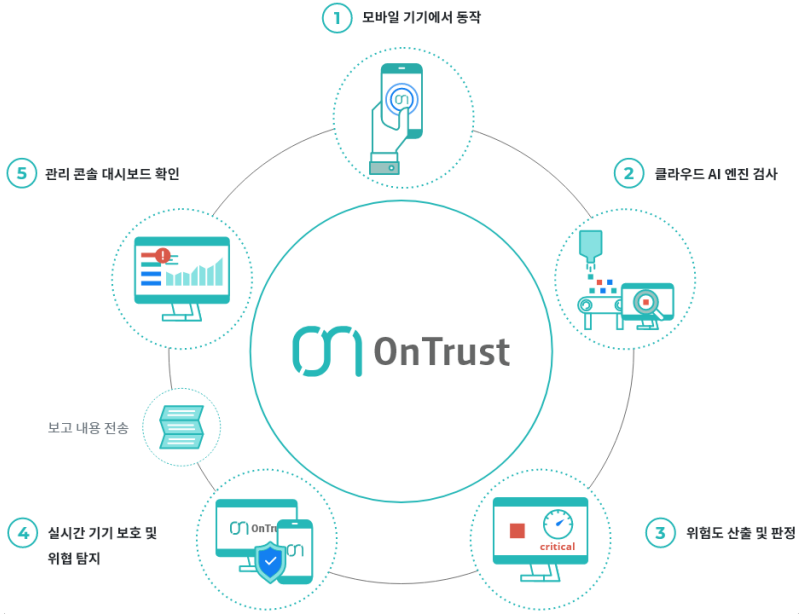
해외 관련 대응 현황: 모바일 EDR 기반 ZecOps 기술 제안

- 의심스러운 이벤트 타임라인을 자동으로 구성하여 침해시기 파악, 앱 샌드박스 기능 및 검색, 장치 로그 자동 분석
  - 기기 정보 수집용 경량 어플리케이션 제공, PC 또는 키오스크 설치 가능

결론 - ㈜시큐리온의 최신 대응 기술

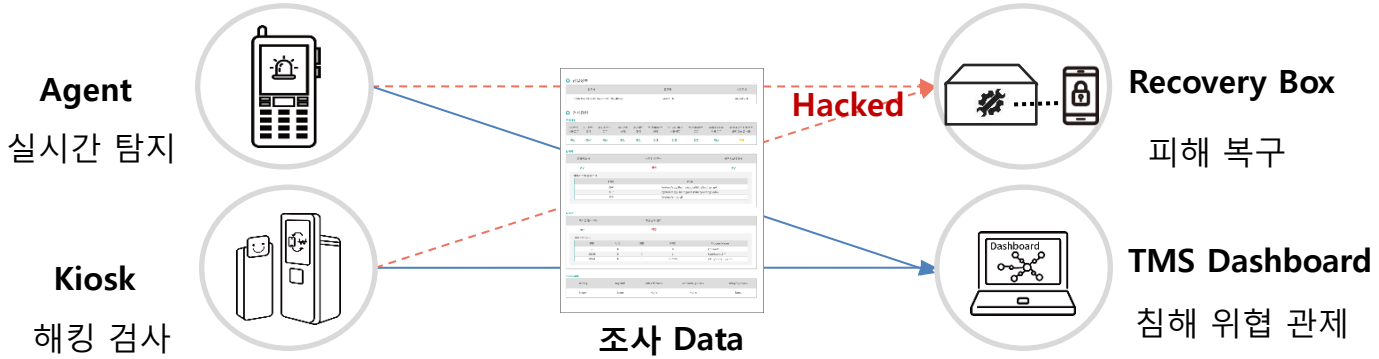
1) OnTrust: 기기 무결 상태 보증, Post-execution 단계의 Anti-exploitation

- 머신러닝 기반 악성 앱 위협 자동 판정 및 평판 검증
  - ML 기반 신-변종 악성 앱 탐지 및 리-패키지 앱 대응
- 기기 잠금 해제, 루팅, 부팅 상태, 기기 무결성 검증
  - 펌웨어, 파티션, 파일 시스템 변조 검사 수행
- 실시간 OS 보안 상태 검사 및 알려지지 않은 취약점 공격 탐지
  - 알려진 1-day 취약점에 대한 CVE 검사
  - 알려지지 않은 0-day 취약점에 대한 공격 행위 실시간 탐지

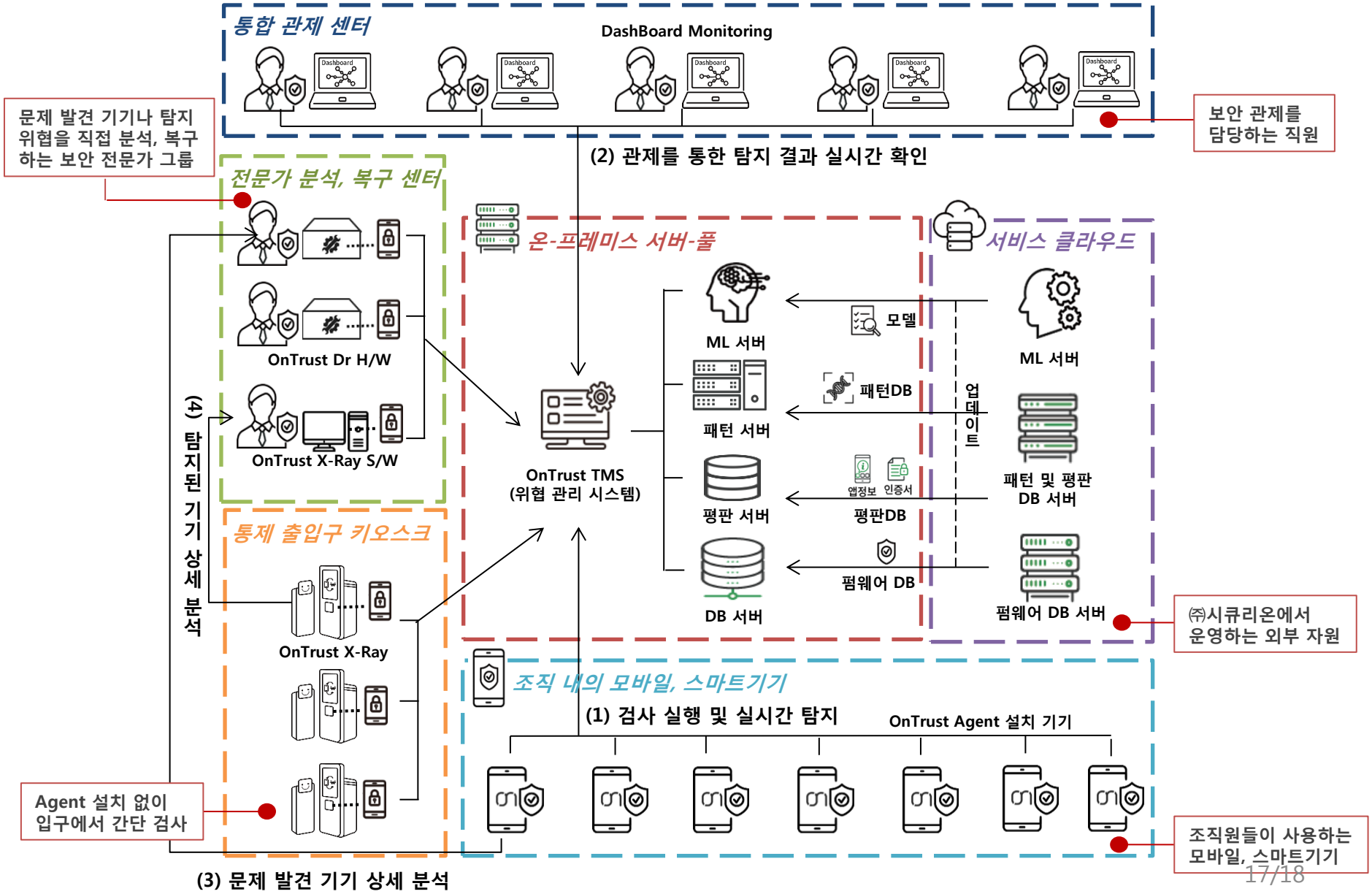


2) 다양한 형태의 제품 및 서비스 제공

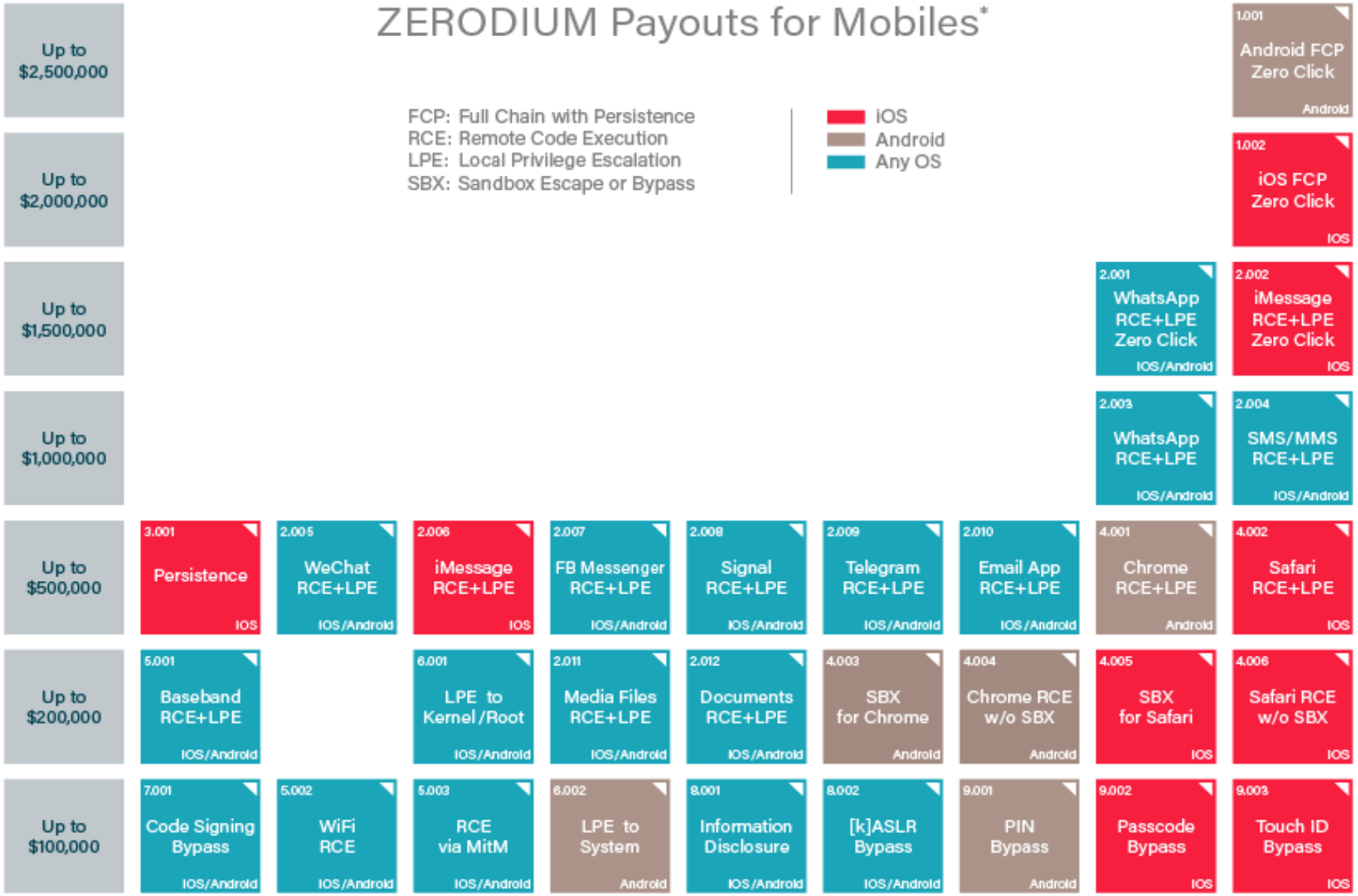
- 기기별 보안 등급, 공격벡터, 위협요인, 기기 변조 사항 및 공격코드 등



결론 - ㈜시큐리온의 최신 대응 기술



결론 - Q & A



** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019/09 © zerodium.com