



# Zyroroid iOS

iOS Application Analyzer

(주)라온시큐리티

# Table of contents

## I. 회사 소개

1. 일반 현황 및 사업 분야	4
2. 특징점	5

## III. Zyroid iOS 상세 기능

1. 편리한 원격 입력	14
2. 실시간 데이터 분석 및 조작	15
3. 편리한 자동 점검	16
4. 컴플라이언스	17
5. 악성 앱 점검 기능	18
6. 사용자 입력 자동화	19

## II. Zyroid iOS 소개

1. 개발 배경	7
2. Zyroid iOS란?	8
3. Zyroid iOS 특징점	9
4. 제품 구성	10
5. 기능 구성도	11
6. 산업군별 적용 대상	12

## IV. 취약점 점검 항목

1. 점검 항목 리스트	21
--------------	----

# I. 회사 소개

- ▶ 1. 일반현황 및 사업분야
- ▶ 2. 특징점

# 1. 일반 현황 및 사업분야

(주)라운시큐리티는 해킹 기법 연구를 통해 획득한 기술을 바탕으로 보안 솔루션 개발 및 모의 해킹 컨설팅 서비스를 제공하고 있는 보안 솔루션 개발 및 컨설팅 회사입니다.

## [일반정보]

회 사 명	주식회사 라운시큐리티
대 표 이 사	양정규
사 업 분 야	모의해킹 보안 제품 연구/개발
주 소	서울시 금천구 가산동 543-1 대성D-POLIS B동 1108호
연 락 처	02-861-9890 010-4177-1156
회 사 설 립 도	2012년 3월 14일
해 당 부 문 간 사 업 기 간	2012년 3월 ~ 현재

## 솔루션 ▶

## [사업분야 및 주요성과]

- Android Application 점검도구 (Zyroid SE/DE)
  - SKT, SKP, KB손해보험, CJ올리브네트웍스 납품
- Android 악성행위 모니터링 시스템 (Zyroid Enterprise)
  - 삼성전자, KT 납품
- KISA Android 악성행위 모니터링 시스템 개발

## 컨설팅 ▶

- SK Planet 모의해킹
- 삼성전자 갤럭시S4 모의해킹 (2회 수행, NDA체결)
- 온라인게임 모의해킹 (다수)
- EBAY(옥션, 지마켓) 모의해킹
- LG U+ Fuzzing
- 대검찰청 모의해킹
- 카카오 앱 모의해킹
- 삼성SDS 화이트해커 해킹대회 문제출제 및 운영
- KISA 해킹방어대회 문제출제 및 운영  
(2006년 3회 ~ 2013년 10회) 총 8번 운영

## 연구 ▶

- Google Android 취약점 발견 (2013)
- Android 악성행위 모니터링 시스템 구축
  - Hooking 기법 연구
- iPhone Hooking 기법 연구
  - Kernel Hooking, Library Hooking, Application Hooking 기법 연구

## 2. 특징점

(주)라운시큐리티는 기술과 고객과의 신뢰를 최우선으로 생각하며 운영하고 있는 회사입니다. 기존의 많은 모의 해킹 수행 이력과 연구 성과, 해킹대회 입상 경력 등 최고의 기술력을 확보하기 위해 최선을 다하고 있습니다.

### 다수의 모의 해킹 수행 경험 보유

- 다수 모의 해킹 수행 인력 보유
- 일반/금융/기관 등 다양한 환경에서 모의해킹 수행
- 웹/데이터베이스/단말 등 다양한 대상에 대한 모의해킹 수행

### 세계해킹대회 입상 경력자 보유

- KISA 해킹방어대회 8년 연속 출제 / 운영
- 세계 최고 수준의 DEFCON 본선 진출 4위
- 국내에서 주최한 국제해킹대회 우승



RaonSecurity

### 최신 해킹기법 보유

- 금융권 메모리 해킹 최초 발견 및 보유
- Mobile 해킹 기법 보유
- APT 공격 해킹 기법 보유
- 취약점 Exploit 제작 기술 보유
- Mobile Zero Day 보유 (구글에 보고/버그 채택)

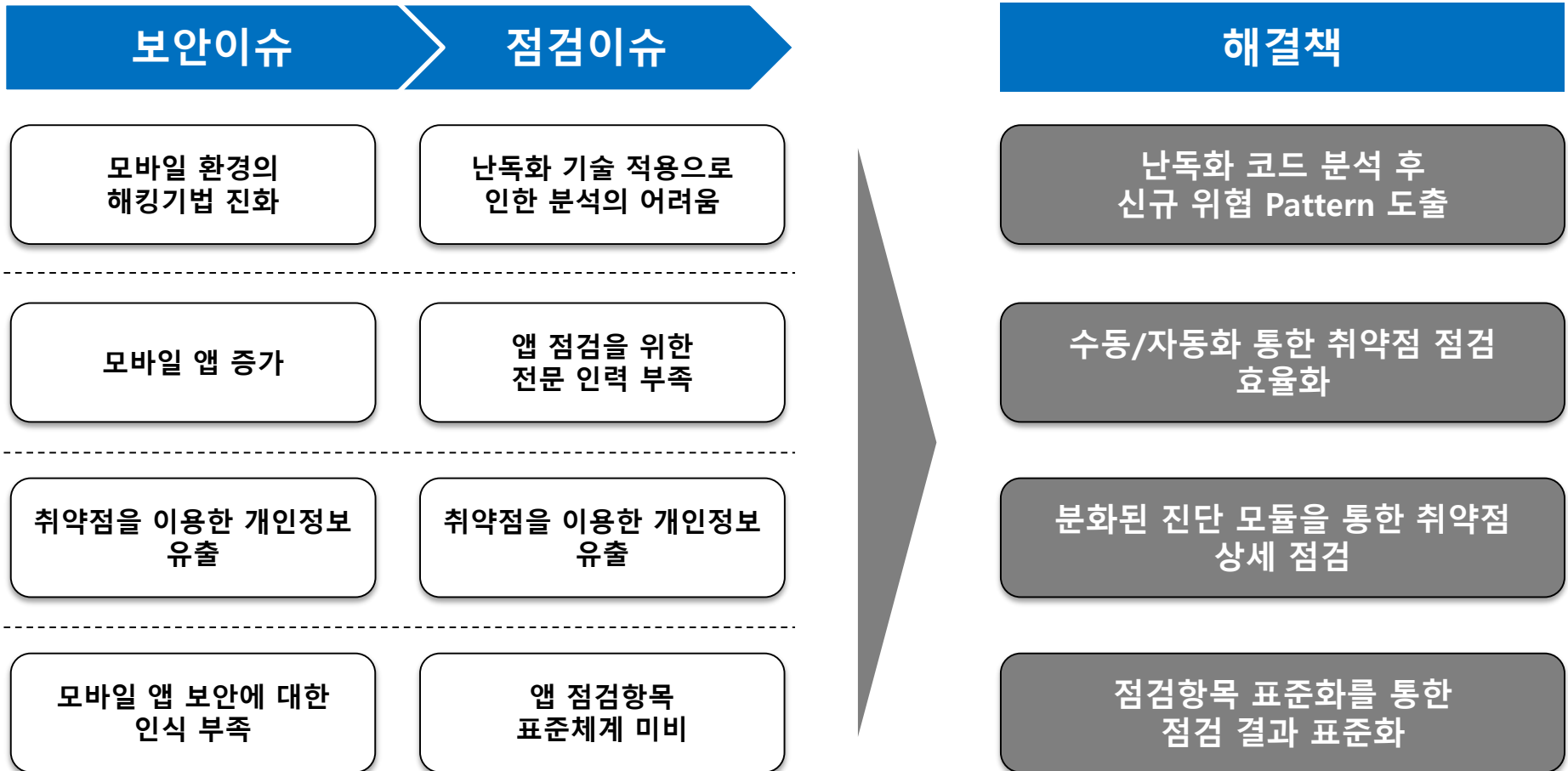
### 보안 솔루션 개발 기술 보유

- 웹 애플리케이션 취약점 점검 솔루션 개발기술 보유
- Smart Phone Monitoring 시스템 개발
- 모의해킹 시 필요 도구 개발 기술 보유
- 다양한 개발 언어 숙련

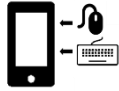
## II. Zyroid iOS 소개

- ▶ 1. 개발 배경
- ▶ 2. Zyroid iOS란?
- ▶ 3. Zyroid iOS 특징점
- ▶ 4. 제품 구성
- ▶ 5. 기능 구성도
- ▶ 6. 산업군별 적용 대상

모바일 환경에서의 해킹 기술은 진화하고 있으나 인적(전문가), 물적 자원의 부족으로 인한 대응 능력의 한계와 다양한 보안 요구사항의 수용능력의 제한 등은 점검 기준 및 절차의 표준화가 요구되고 있으며 Zyroid iOS는 기술적, 관리적(컴플라이언스) 측면에서 향상된 보안 점검을 수행합니다.



## 2. Zyroid iOS란?



### 쉬운 사용자 입력

스마트폰과 PC 동기화 후  
키보드와 마우스로 스마트폰 조작



### 컴플라이언스 충족

개인정보보호법  
정보통신망법  
전자거래기본법 등



### 실시간 데이터분석

점검자 PC에서 APP 패키지의  
실시간 분석 및 조작



### 수준 높은 점검환경

정밀분석을 위한 다양한 정보  
제공  
시스템이 판단하기 힘든 항목  
점검 가능



### 편리한 자동점검

점검을 위한 기본 정보 입력 후  
원클릭 자동점검



### 악성 앱 탐지 가능

행위기반 판단을 통해 악성 앱  
검증 가능



### 실제 단말기 사용

- ▶ iOS 가상 에뮬레이터가 아닌 실제 단말기를 사용
- ▶ 실제 단말기로 인증이 필요한 금융 APP의 동적분석 지원

### 동적 Hooking 사용

- ▶ iOS Version 및 단말기에 독립적
- ▶ iOS 플랫폼 소스 및 바이너리를 수정 없이 분석 가능

### Proxy / Debugger 기능

- ▶ 호출되는 API의 입/출력 값 실시간 분석/수정 가능
- ▶ 진단 APP의 전반적인 API 호출 흐름 파악 가능

### 표준화된 점검 가능

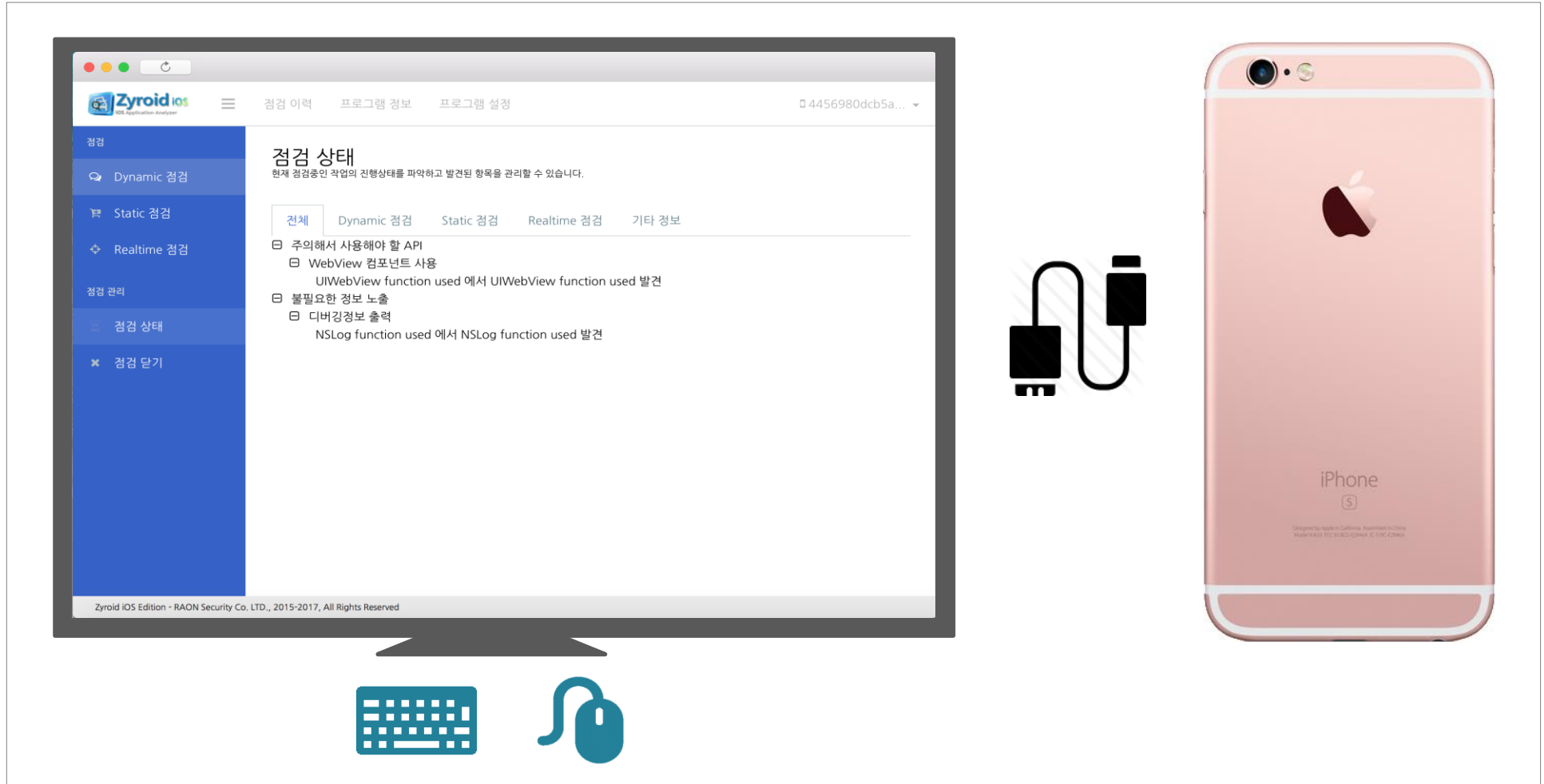
- ▶ 표준화된 점검 기준 적용을 통한 분석 결과의 신뢰성 향상

### 악성 앱 분석 기능

- ▶ 사용자 정보 유출 및 권한 상승 등 악의적인 행동을 하는 악성 앱 분석 가능

# 4. 제품 구성

제품의 구성은 점검용 노트북, Zyroid iOS, 아이폰, USB Cable로 구성되어 있습니다.



# 5. 기능 구성도

Zyroid iOS의 주요 구성은 정적 코드 분석과 동적 분석 그리고 두 기능을 합친 자동 분석기능을 통해 점검 시간 및 점검 수준을 높일 수 있습니다.



# 6. 산업군별 적용 대상

Zyroid iOS는 대부분의 산업분야에서 개발되는 iOS 기반 앱을 대상으로 점검이 가능합니다.

## 산업 분야

 금융	 제조	 게임	 전자상거래
 이동통신	 건설	 자동차	 공공

## 법적 요건 충족

## 주요 법률

정보통신망 이용촉진 및 정보보호 등에 관한 법률  
위치정보의 보호 및 이용 등에 관한 법률  
신용정보의 이용 및 보호에 관한 법률  
개인정보보호법  
전자금융거래법

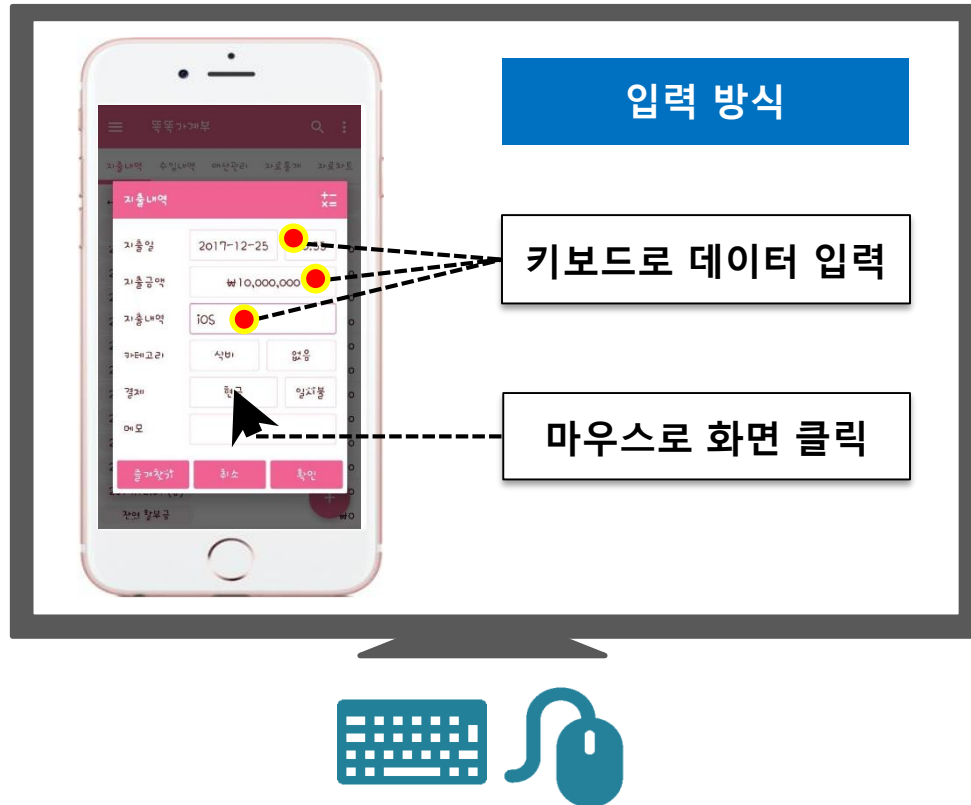
# III. Zyroid iOS 상세 기능

- ▶ 1. 편리한 원격 입력
- ▶ 2. 실시간 데이터 분석 및 조작
- ▶ 3. 편리한 자동 점검
- ▶ 4. 컴플라이언스
- ▶ 5. 악성 앱 점검 지원
- ▶ 6. 사용자 입력 자동화 제공
- ▶ 7. 편리하고 수준 높은 점검 환경 제공

# 1. 편리한 원격 입력

- ▶ PC와 동기화 후 PC 스크린 상에서 키보드와 마우스로 아이폰을 조작 가능
- ▶ PC의 키보드와 마우스로 모든 데이터를 입력하여 입력 시간 단축 가능

### 점검자 PC



### PC와 아이폰 Sync

실시간 화면 동기화



마우스로 잠금 해제

### 아이폰



## 2. 실시간 데이터 분석 및 조작

- ▶ Zyroid iOS를 통해 입력 데이터를 가로챈 뒤 실시간 데이터 조작이 가능
- ▶ 통신구간의 SSL 사용 여부와 상관없이 모든 데이터의 평문 확인 가능

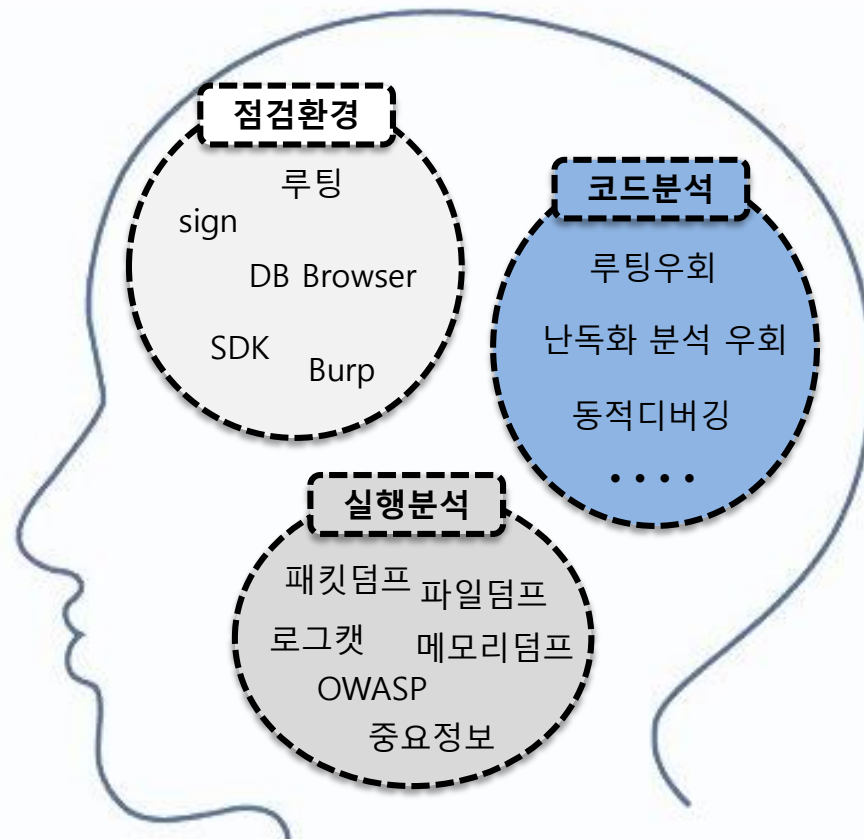


### 3. 편리한 자동 점검

- ▶ 기존의 복잡한 점검 환경구성 및 분석 업무가 간단한 정보 입력만으로 iOS 앱 자동 점검이 가능하도록 구현되어 있습니다.

#### 기존 점검자

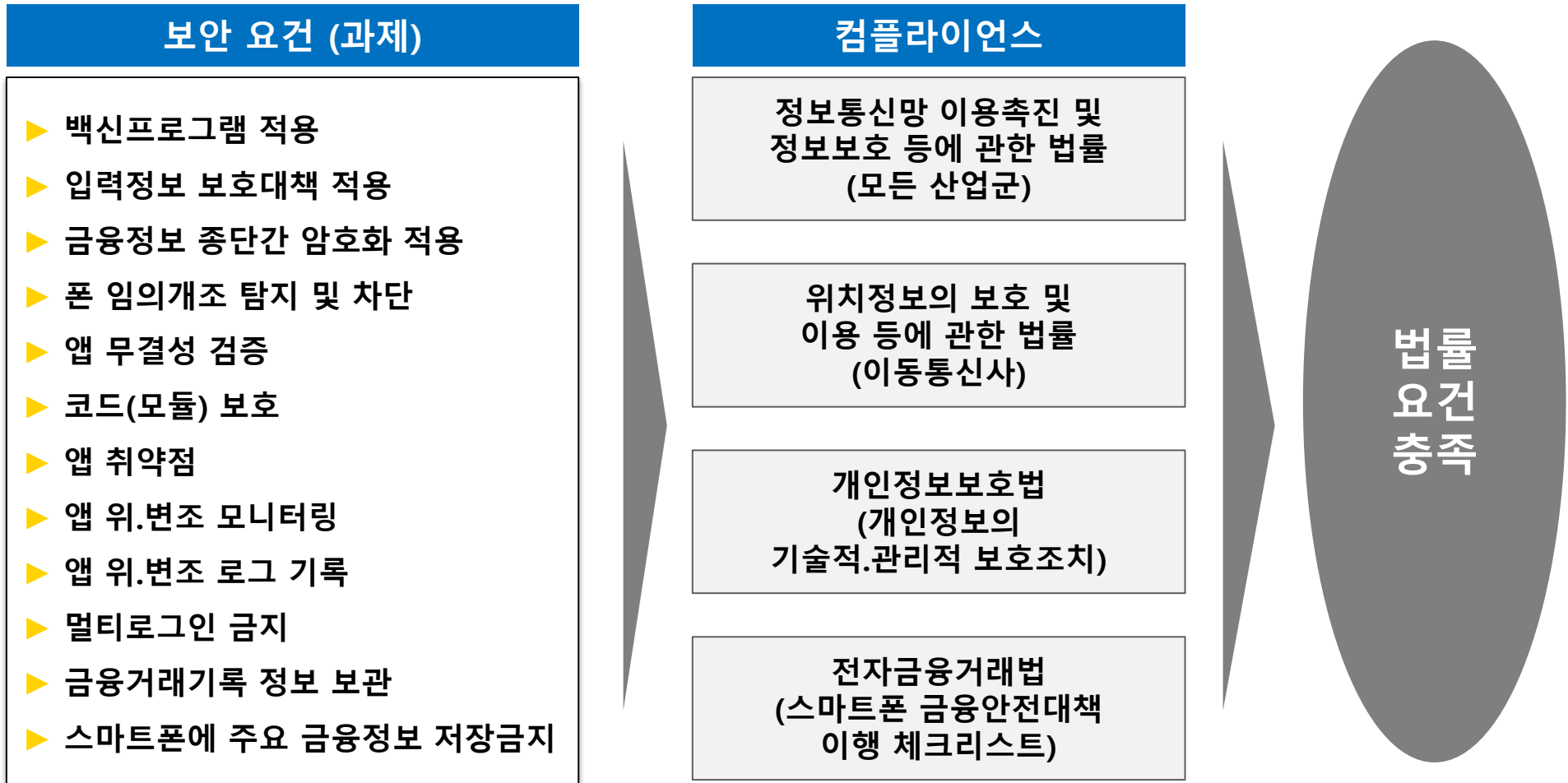
#### Zyroid iOS 점검자



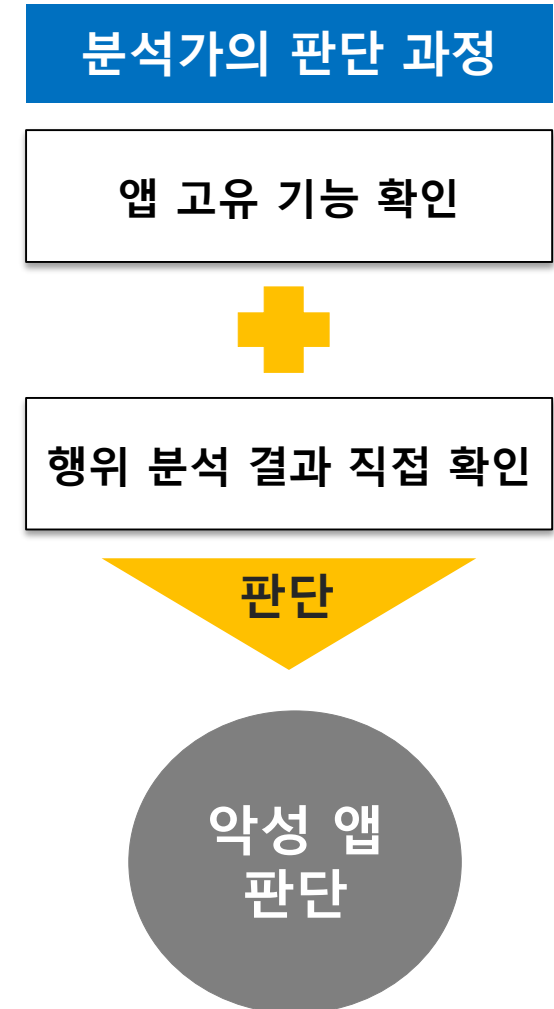


# 4. 컴플라이언스

- ▶ 금융위 금융안전대책 이행 체크리스트 기준의 표준화된 점검 가능
- ▶ 산업군(공공, 금융, 통신, 제조 등)별 보안 요건을 충족한 점검 가능



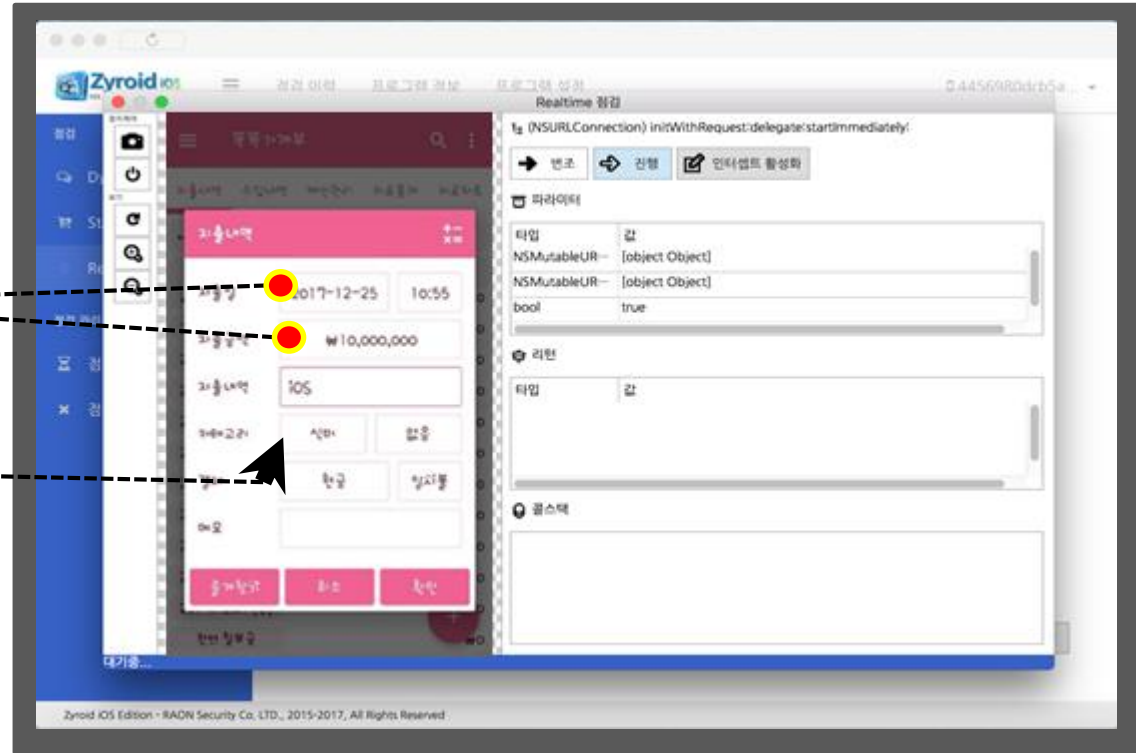
### ▶ 행위 분석을 통한 악성 앱 점검 지원



# 6. 사용자 입력 자동화

- ▶ 동적 분석에서 사용자 입력 시퀀스를 저장하여 재사용
- ▶ 동일 앱에 대한 분석에서 단순 반복작업을 최소화

- 사용자 입력
- 키보드로 데이터 입력
- 마우스로 화면 클릭
- UI 출력 변경 탐지



## IV. **취약점 점검 항목**

### ▶ 1. 점검 항목 리스트

# 1. 점검 항목 리스트

Zyroid iOS는 취약점을 11개로 분류하여 42개의 취약점 항목에 대해 점검이 가능합니다. 취약점 점검 기준은 OWASP MOBILE TOP 10 과 금융위의 금융앱 점검 항목과 더불어 라온시큐리티의 취약점 점검 노하우를 통해 점검 항목을 개발하였습니다.

순번	분류	점검 항목
1	중요정보노출 (앱,설치파일,화면,로그 등 중요정보가 저장되는 모든 곳 점검)	12개
2	불필요한 정보노출 (앱 내 불필요한 정보 및 로그 확인)	2개
3	악용 가능성 (앱 의도와 다른 악용 가능여부 확인)	2개
4	악성코드 및 프로그램 위/변조 대응 (보안솔루션 적용여부)	4개
5	중요정보 암호화 통신 미흡 (SSL 취약점 및 적용여부)	2개
6	권한 상승 / 권한 도용 (명령 실행 등 권한 상승 가능 취약점 확인)	10개

순번	분류	점검 항목
7	취약한 암호화 방식 사용/ 키 노출	1개
8	Server Side Injection (SQL injection 등 server 취약점)	2개
9	서비스 거부	1개
10	기타 정보 (취약점 분석을 위한 활용 정보)	5개
11	수동 점검기능 (함수 입력값 조작)	1개

11개 취약점 분류 , 42개 점검항목

고객의 정보보호를 위한  
최고의 파트너가 되겠습니다.



(주)라온시큐리티

[TEL] 02-861-9890

[FAX] 02-861-9891

[URL] <http://www.raonsecurity.com>

서울 금천구 가산동 543-1 대성D-POLIS B동 1108호