SECIRON

SECIRON

Mobile Application Protection Solution

Presented by:
Haekal Aufar Amriel
Technical Consultant Manager Indonesia Region

Overview

- Introduction
- Mobile App Protection Solution
- Benefit & Value Proposition

1.0 Introduction

SECSIRON

SecIron Footprints

SecIron is a leading global provider in the mobile security industry. We are committed to bringing **mobile app security** to everyone and building security guarantees for the Smart World.

EST. 2010

Protected > 10k apps

11 Countries (Asia)
~ 3 R&D Centres ~

Global References

SECIRON

> 60 Satisfied Clients

95% Customer Retention

Gartner Peer Insights™

SecIron named as Top 10 Mobile Application Security Solutions Provider 2023 by CIOutlook

Read more

SecIron

Awarded By CIOutlook

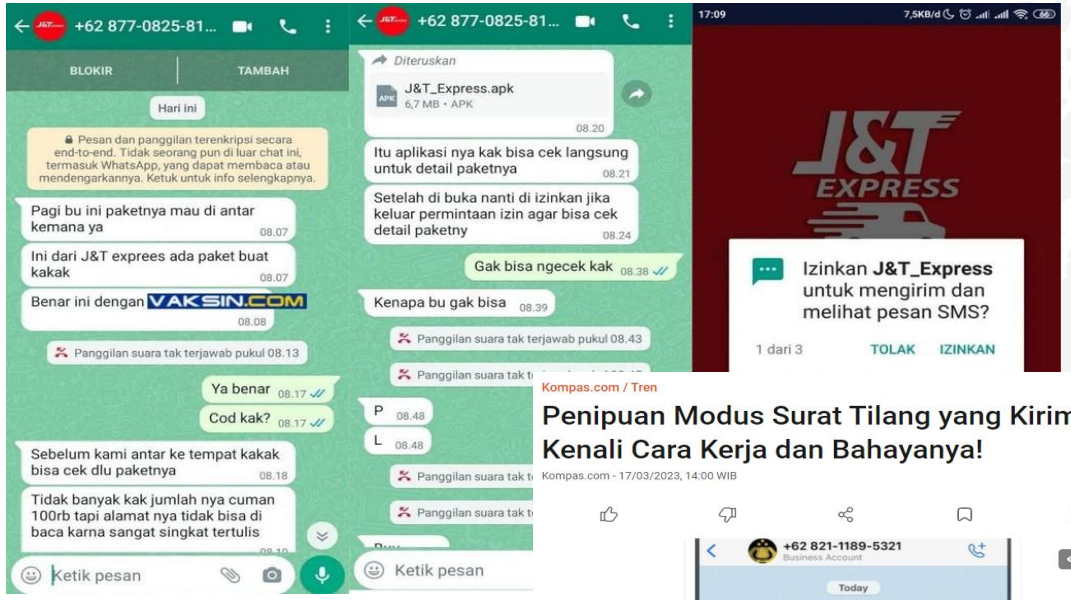
ISO 27001 Certified

COMMON CRITERIA CERTIFIED EAL2

www.seciron.com

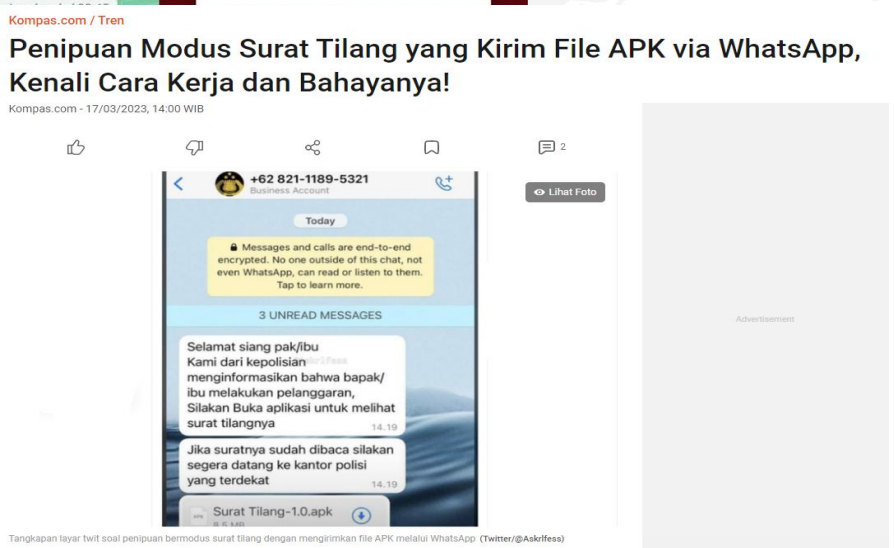
Fake Apps Incident

− How about if your app becomes a Victim?



Source:

https://kumparan.com/kumparantech/waspada-penipuan-kurir-palsu-minta-instal-aplikasi-curi-otp-bobol-m-banking-1zNZuyJbrgE/full/gallery/2



Source:

https://www.kompas.com/tren/read/2023/03/17/140000265/penipuan-modus-surat-tilang-yang-kirim-file-apk-via-whatsapp-kenali-cara

Scam and Social Engineering

Fake Apps that contain Malware

Attack Any Low Security Mobile Apps

Data Theft
Reputation Damage
Financial & Law Impact

Current Practice for Mobile App Security

– Try to think.

SECIRON

Current Practice

VS

Facing Reality

Rely on Developer.

- Security Up-to-date?
- Resource and Effort?
- Time-to-market?

Rely on Source Code Review and Penetration Test.

- False positive?
- Environment risk?
- Scope? Frequency?

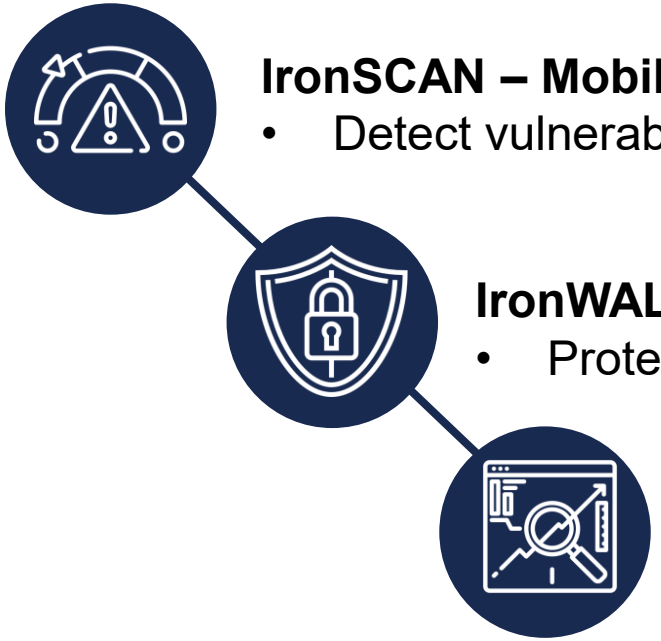
Thinking No Attack is Safe.

- No attack or no visibility?
- Really can control the app?

2.0
Mobile App Protection Solution

SECIRON

SecIron – Mobile Application Security Solution



IronSCAN – Mobile Application Security Testing

- Detect vulnerabilities with recommendations to rectify.

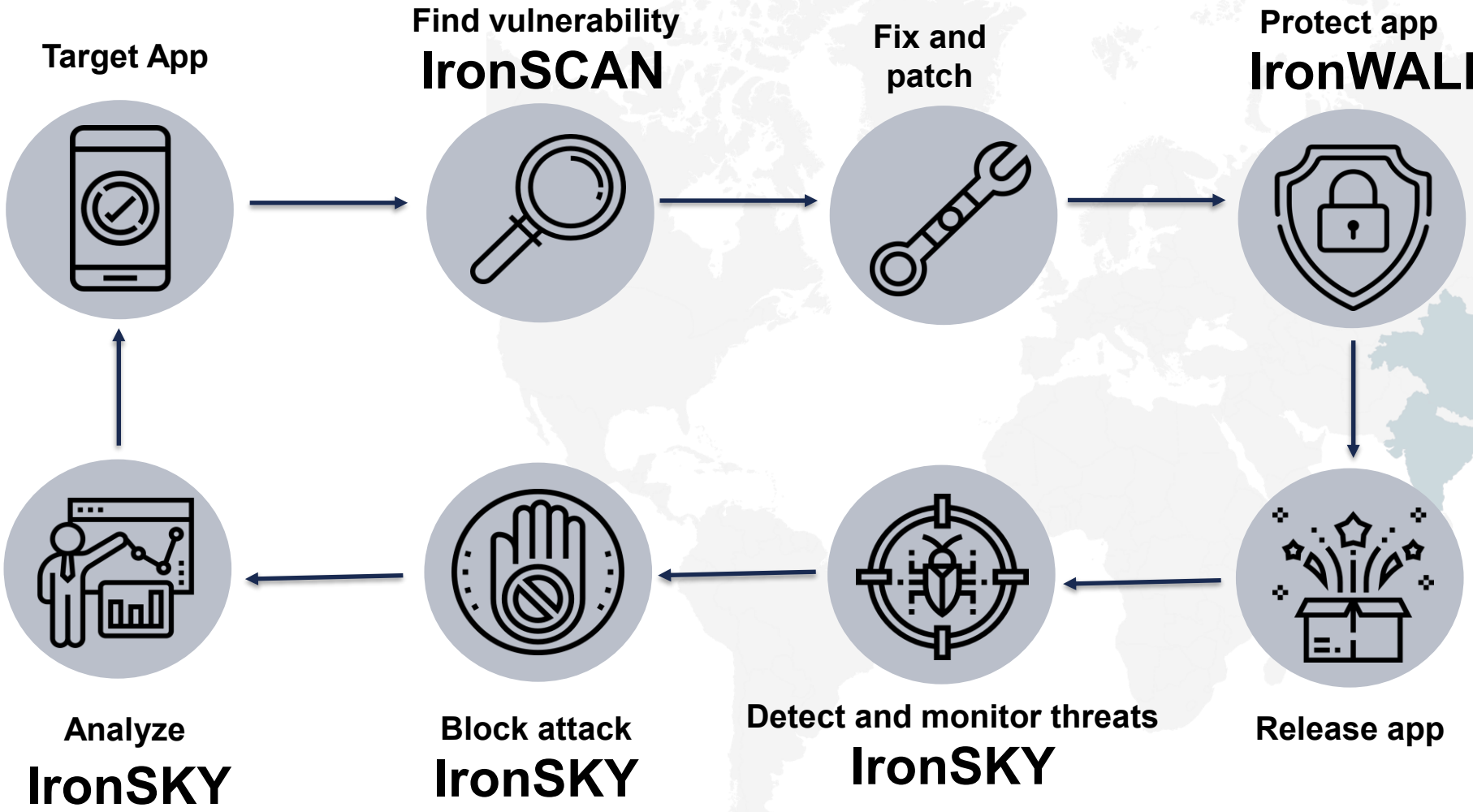
IronWALL – Application Hardening Platform

- Protect application from reverse-engineering and attacks

IronSKY – Real-time Threats Monitoring System

- Real-time monitoring, detection and response to threats.

Mobile App Security Lifecycle

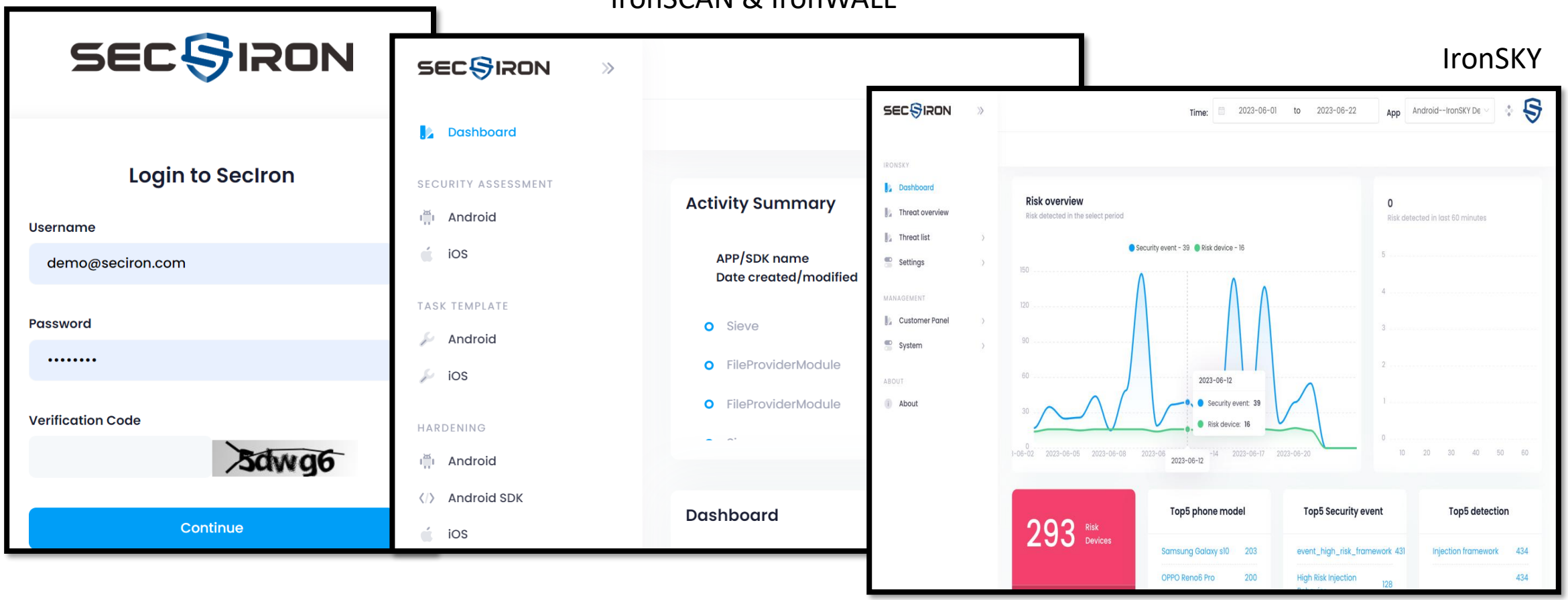


Seciron Platform Preview

Saas or On-Premises

IronSCAN & IronWALL

IronSKY

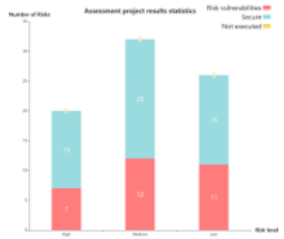


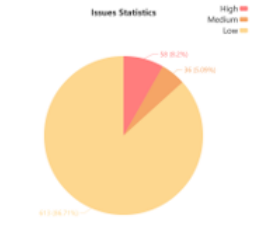
Sample of IronSCAN Reports

SECIRON

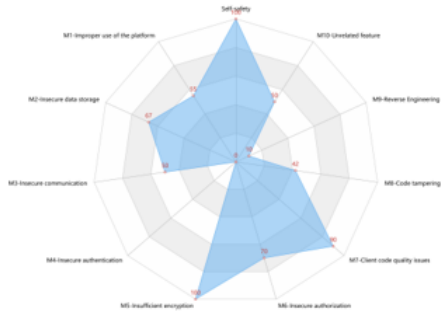
Security Score	61 /100

	TOTAL	HIGH	MEDIUM	LOW
ISSUES CHECKED	78	20	32	26
ISSUES WITH RISKS	30	7	12	11
RISKS OCCURRENCE	707	58	36	613





Security performance



1.3.Issues Summary

	ISSUE	RISK LEVEL	RESULT
Self-safety(4 items)			
1	Permission information	Low	Pop-up message (27 found)
2	Behavior information	Low	Pop-up message (390 found)
3	Virus scanning	High	Secure
4	Apk file in resource file	Low	Secure
M1-Improper use of the platform(10 items)			
5	Janus signature mechanism vulnerability	High	Secure
6	Start hidden service risk	Low	Secure
7	Insecure application signature algorithm risk	Low	Secure
8	Dynamic registration of Receiver risks	Medium	Risk exist(found 5 risks)
9	PendingIntent misuse of Intent risk	Low	Risk exist(found 5 risks)
10	Intent component implicit call risk	Low	Risk exist(found 20 risks)
11	Denial of service attack vulnerability	Medium	Risk exist(found 1 risk)
12	Loading dex risk from sdcard	Medium	Secure
13	Loading so risk from sdcard	Medium	Secure
14	Insecure browser call vulnerability	Medium	Risk exist(found 5 risks)
M2-Insecure data storage(11 items)			
15	Webview plaintext password storage risk	High	Risk exist(found 6 risks)
16	Webview File same origin policy bypass vulnerability	High	Risk exist(found 5 risks)
17	Plaintext digital certificate risk	Medium	Secure
18	Database injection vulnerability	High	Secure

2.3.M2-Insecure data storage

2.3.1.Webview plaintext password storage risk

Purpose of assessment	Check whether the user name and password are saved in plaintext in WebView component of APP.
Risk Level	High
Description	The Android Webview component has the function of prompting the user to save the password by default. If the user chooses to save, the username and password will be stored in plaintext in the application directory databases/webview.db.The user name and password stored in local plaintext will not only be browsed by the application, other malicious programs may also access the webview database of the application through privilege escalation or root to steal user' s login username and password that the user has logged in to.
Assessment result	Risk exist(found 2 risks)
Assessment result description	The WebView component of this app does not set to turn off the function of auto save password , user name and password may be stored in plaintext
Assessment details	1. [file]: com/ipay/IPayIHActivity$2 [method]: public onCreateWindow(Landroid/webkit/WebView;ZZLandroid/os/Message ;)Z 2. [file]: com/ipay/IPayIHActivity$2$1 [method]: public
Solution	Developer self-check:Turn off the save password function of the webview component by setting WebView.getSettings (). SetSavePassword (false).

Highlight IronWALL Features

- Protect mobile application running on an untrusted/compromised environment
- Addressing risk of:
  - Malware attack
  - Fake account opening
  - Data tampering for fraud activities
  - Security defense breached
  - Cloned app for phishing
- No source code changes required
- Quick implementation; available on SaaS and on-premise
- Suitable to use for Consumer apps related to financial or credential data; or enterprise app in BYOD environment

Anti-Reverse Engineering

3 layers (Hide, Encrypt, Transform) to protect source code from reverse engineer.

Anti-Dynamic Attack

Prevent debugging, tampering, injection attack, screen hijacking, rooted and emulators

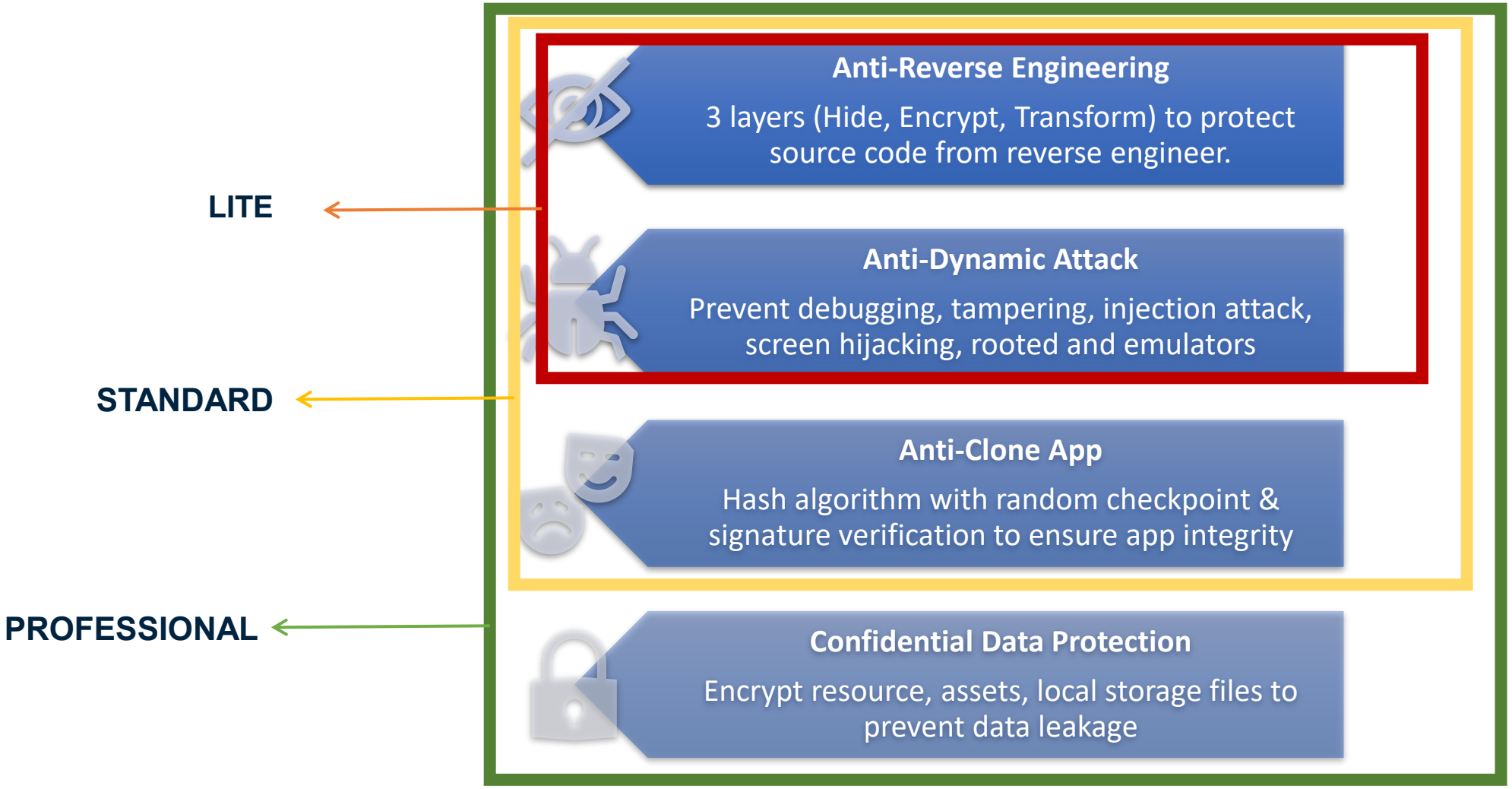
Anti-Clone App

Hash algorithm with random checkpoint & signature verification to ensure app integrity

Confidential Data Protection

Encrypt resource, assets, local storage files to prevent data leakage

Highlight IronWALL Features



Example: Anti-reverse Protection on Android (IronWALL)

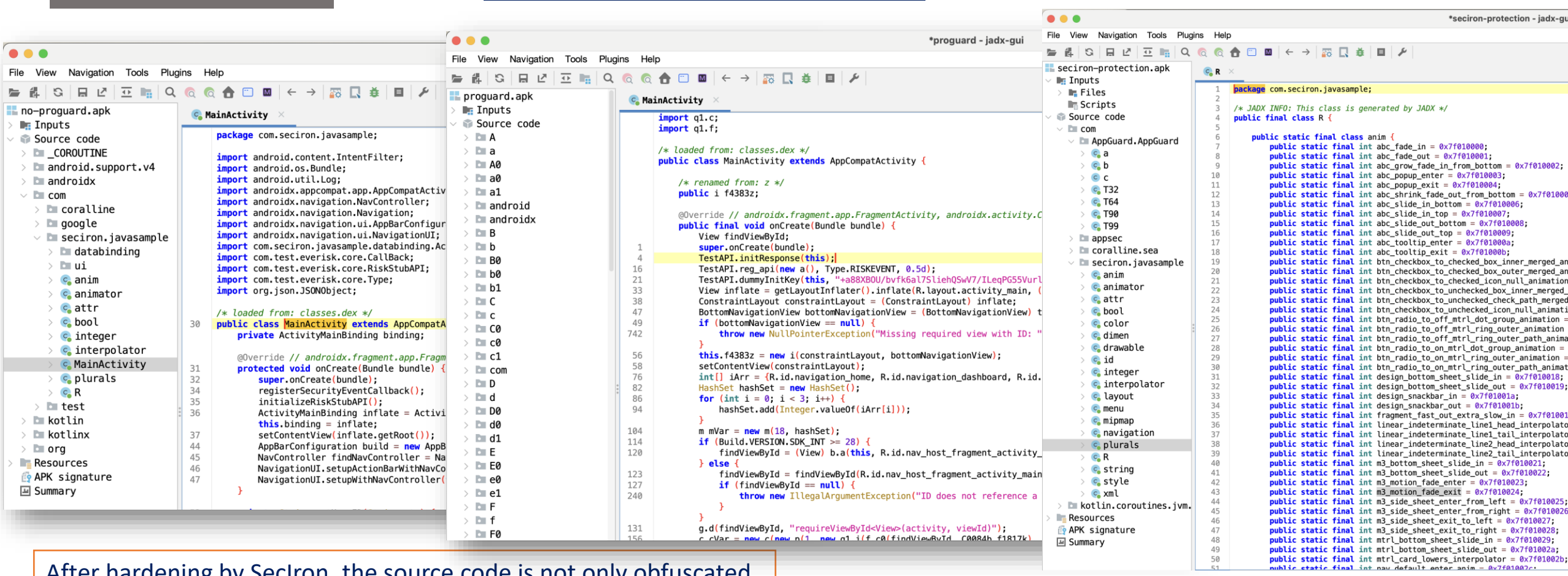
− Already available from IronWALL Lite Version

SECIRON

Original Code

Standard Obfuscation

Next Gen Hardening



After hardening by SecIron, the source code is not only obfuscated but also hidden and the classes are encrypted.

Support CI/CD Integration

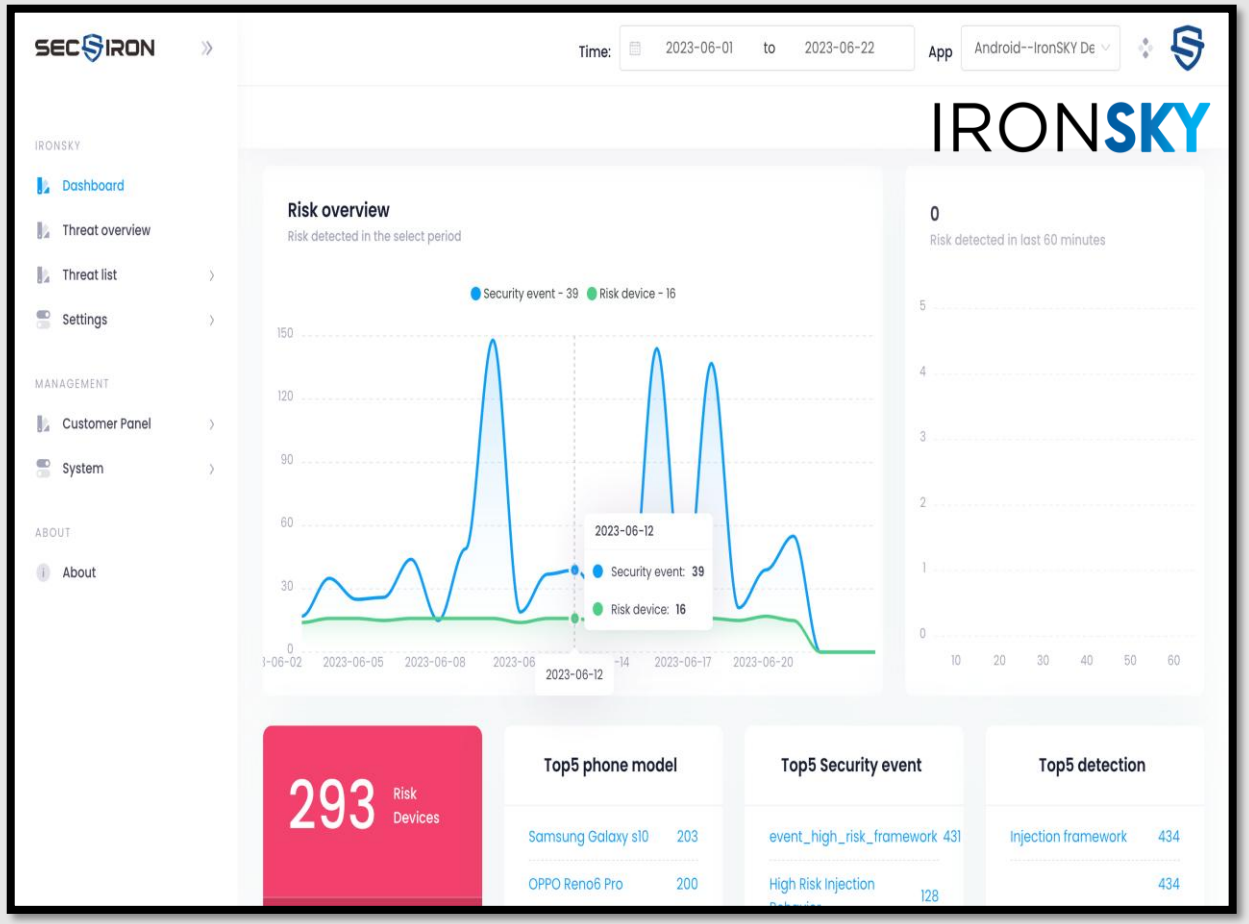
Example:

java -jar *secapi-4.2.5.2.jar* **-i** *http://192.168.0.6:8090* **-u** *lzz* **--password** *1234566* **-a** *98918240-8a85-41a8-8002-c35457255094* **-c** *2ebe1900-ed3b-41d5-8183-5ecd3b1426ba* **-f** *0* **-t** *458* **-p** *D:\app-debug.apk* **-d** *G:* **--action ud –ks** *1824004939987288065* **--ms** *1824004776086470657* **--lp**

Parameter	Description (MANDATORY)
-i	Service IP address which needs to include port number. If it is a domain name, configure it as given - https://portal.seciron.com
-u	Username: created user on the hardening service platform
--password	Password Username of Platform
-a	Api_key: obtained through the hardening service platform or from SecIron
-c	API secret: obtained through the hardening service platform or from SecIron
-f	Hardening product type: • 0: Android app hardening (APK or AAB) • 7: iOS app hardening (iPA or Xcarchieve)
-t	Hardening policy ID
-p	Upload file directory or OR file (required)
-d	Download file directory: Prior to hardening, a folder must exist
--action	• ud: upload and download at the same time • u: upload hardening package • d: download hardening package • l: view logs • s: view status

Parameter	Description (OPTIONAL)
--id	The hardening task ID to be downloaded
--dpre	The prefix of the hardened file name can be set
--dsuf	The suffix of the hardened file name can be set
-q	Timeout time: Exit automatically after timeout, in seconds Optional: The default of downloading process is 7200 seconds by default. When uploading and downloading at the same time, please excluding uploading process.
-D	Specify the information file and download all tasks contained within it, regardless of whether they have previously been downloaded.
--tmp	Script temporary file storage directory
--ks	Keystore id
--ms	SDK id
--lp	Add the queries segment, but do not add it if it's not included. If QUERY_ALL_PACKAGES has already been requested, please ignore it.

IronSKY – Real-time Threats Monitoring System



- Environment Risk
  - Injection framework
  - Emulator
  - VPN Proxy
  - Root certificate error
  - Root/Jailbreak
  - Sensitive settings
  - Accessibility permission
  - Blacklist/whitelist
  - Side-load detection
  - Unofficial Source
  - Risk/Malware App
- Behaviors
  - HTTPS hijacking
  - HTTP Proxy
  - Injection attack
  - Debugging behavior
  - Domain fraud
  - Memory tampering
  - Multi-boxing
  - Location fraud
  - Screen mirroring
  - Remote Access Detection
  - Screen Hijacking Detection
  - Auto Clicker Detection
  - Keylogger Detection

1. False positives and false negatives may occur in single-point detection
2. In order to trace the source, provide a 24-hour query of the number of startups

IronSKY – Easy Integration

SECIRON

HYBRID SDK INTEGRATION

- Static Protection
- Integrity Protection
- Dynamic Protection
- Confidential Data Encryption

1. IronSKY SDK Integration (Manual/Auto - Optional)

2. Harden App with IronWALL & Config Configuration

3. Go Live with End-to-End Hardened Mobile App

Benefit & Value Proposition

SECIRON

Prevent Before It's Late.

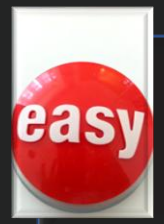
Reference: Mobile Top 10 OWASP

SECIRON

SECIRON

Benefit Implementing SecIron Solution

Flexibility of Deployment



Easy Integration

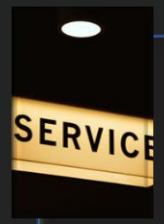
Wide Range of Supported Platforms

3 Layer of Code Protection

Have Complete Features for Static & Dynamic Protection

Less Impact to User Performance

Simplicity on License Scheme



Comprehensive Support in Indonesia

SECIRON

Thank You!

Office: Shibuya1-11-1, COI Nishi-Aoyama Bldg 3F
Shibuya-ku, Tokyo 150-0002

www.seciron.com