

MobileAppDriller

Mobile App Security:
le app italiane sotto la lente e
come automatizzare il processo di
verifica delle vulnerabilità con una
nuova piattaforma "made in Italy"

Agenda

1 Introduzione

MOBILE APP SECURITY

2 Survey

LA SICUREZZA DELLE MOBILE APP ITALIANE

3 MAD e DevSecOps

AUTOMAZIONE DELL'ANALISI

4 Case study

LA PIATTAFORMA ALL'OPERA

5 Demo

Relatori

Edoardo Montrasi

- IT/OT Senior Security Consultant
- Technical Pre-sales & Delivery
- PCI QSA – ISO 27001 LA

Luca Capacci

- Senior Security Engineer
- Network, webapp & mobile app Pentester
- R&D



COMPLIANCE



CONSULENZA



OFFENSIVE SECURITY



DEFENSIVE SECURITY

www.cryptonetlabs.it

Agenda

1 Introduzione

MOBILE APP SECURITY

2 Survey

LA SICUREZZA DELLE MOBILE APP ITALIANE

3 MAD e DevSecOps

AUTOMAZIONE DELL'ANALISI

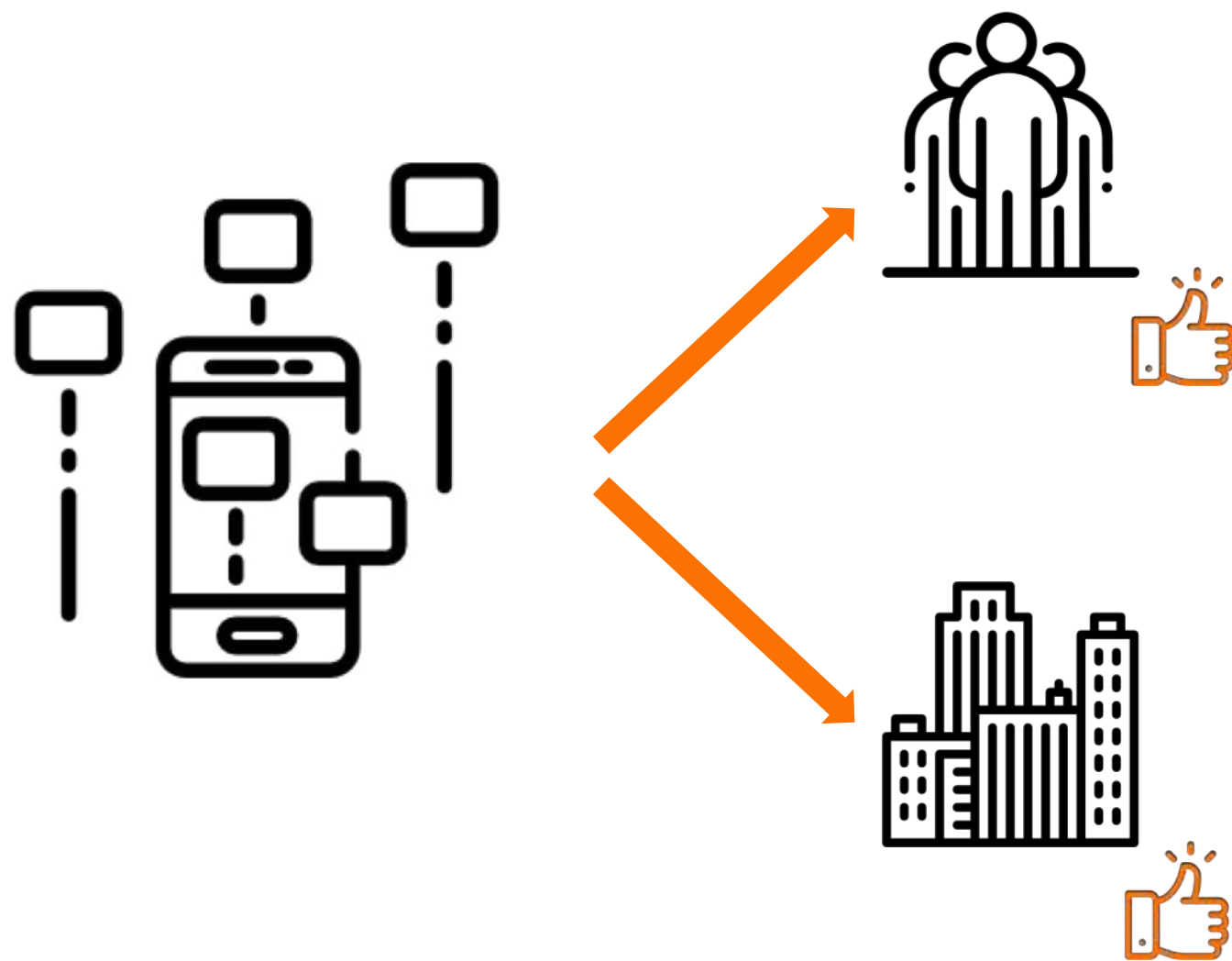
4 Case study

LA PIATTAFORMA ALL'OPERA

5 Demo

La rivoluzione delle Mobile App

Un dato di fatto: gli store propongono circa 6 milioni di app ideate per i più svariati usi.



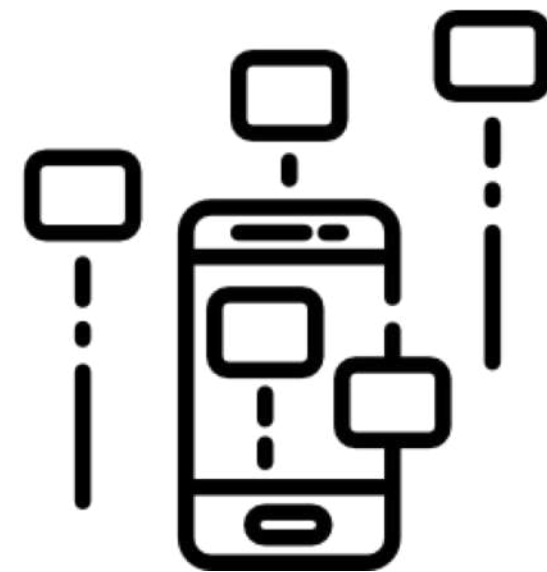
- Maggior confidenza con i dispositivi mobili
 - User experience immediata
 - Personalizzabili
 - Disponibili sempre e ovunque
 - Utilizzabili anche offline
-
- Fidelizzazione cliente (rafforzamento brand, «azienda in tasca», geolocalizzazione, servizi personalizzati, contatto h24)
 - Funzionalità evolute

Punti di attenzione

Le Mobile App utilizzano e gestiscono i dati dell'utente

Cosa sa uno smartphone di noi?

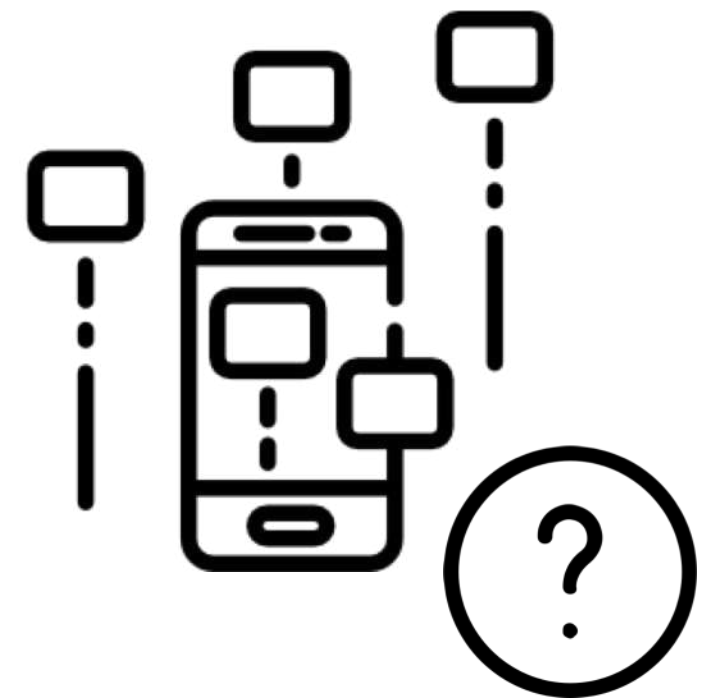
- credenziali
- dati personali
- dati di localizzazione
- informazioni bancarie e finanziarie
- carte di credito
- preferenze degli acquisti
- informazioni sanitarie
- interessi e hobby
- ecc.



Punti di attenzione

Le Mobile App sono in esecuzione su un dispositivo **untrusted**

Spesso non controllato o difficilmente controllabile dall'IT aziendale



La realtà dei fatti

CORCOM Digital Economy Telco Industria 4.0 PA Digitale Finance VideoInterviste Privacy Le Guide di CorCom

Data breach per 5 milioni di europei, Dublino apre dossier su Facebook

Home > Cyber Security

Condividi questo articolo

Nel mirino della Data Protection Commission le misure messe in atto dall'azienda Usa per l'adeguamento al Gdpr. Rischio multa da 1,63 miliardi di dollari

04 Ott 2018



L'attacco hacker a Facebook è stato reso possibile, ha spiegato la società, dallo sfruttamento da parte di "attori esterni" di tre vulnerabilità che riguardano la funzione 'Visualizza come' e la nuova versione del caricamento video introdotta a luglio 2017, che a sua volta ha generato in modo errato un token di accesso all'app mobile di Facebook. L'azienda ha già provveduto a rimediare i bug.

cybersecurity AI CYBERDIFESA DARK WEB DATA BREACH IOT LEGALE MALW

VULNERABILITÀ

Data breach per Air Canada, rubati dati sui passaporti

Di Luca Sambucci - 30 August 2018 - 19:45



Departing Toronto Pearson

Fra il 22 e il 24 agosto i tecnici di Air Canada hanno notato delle attività di login sospette e hanno quindi bloccato tutti gli account degli utenti che usano l'app mobile (circa 1,7 milioni di persone).

I dati di almeno 20.000 passeggeri inseriti all'interno dell'app sono stati oggetto di furto, inclusi i dettagli sui passaporti. In particolare, BBC riporta che i dati coinvolti sono: nome, indirizzo e-mail, numero di telefono e tutti i dati relativi al passaporto che gli utenti hanno inserito, che normalmente includono numero del passaporto, paese e data di emissione, scadenza, nazionalità, paese di residenza e data di nascita.

Quindi?

Emerge la necessità di garantire:

Confidenzialità



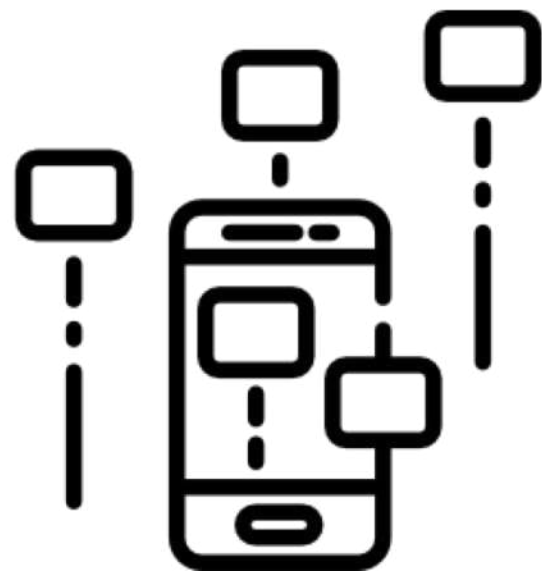
Integrità



Disponibilità



Regole per il trattamento dei dati



Prevenzione per **personal data** loss, breach e disclosure



Protezione dei **dati finanziari** legati ai pagamenti con **carte di credito**



Protezione dei **dati finanziari**

Best practices

OWASP Mobile Top 10 (2016)

M1 – Improper
Platform Usage

M2 – Insecure
Data Storage

M3 – Insecure
Communication

M4 – Insecure
Authentication

M5 – Insufficient
Cryptography

M6 – Insecure
Authorization

M7 – Client
Code Quality

M8 – Code
Tampering

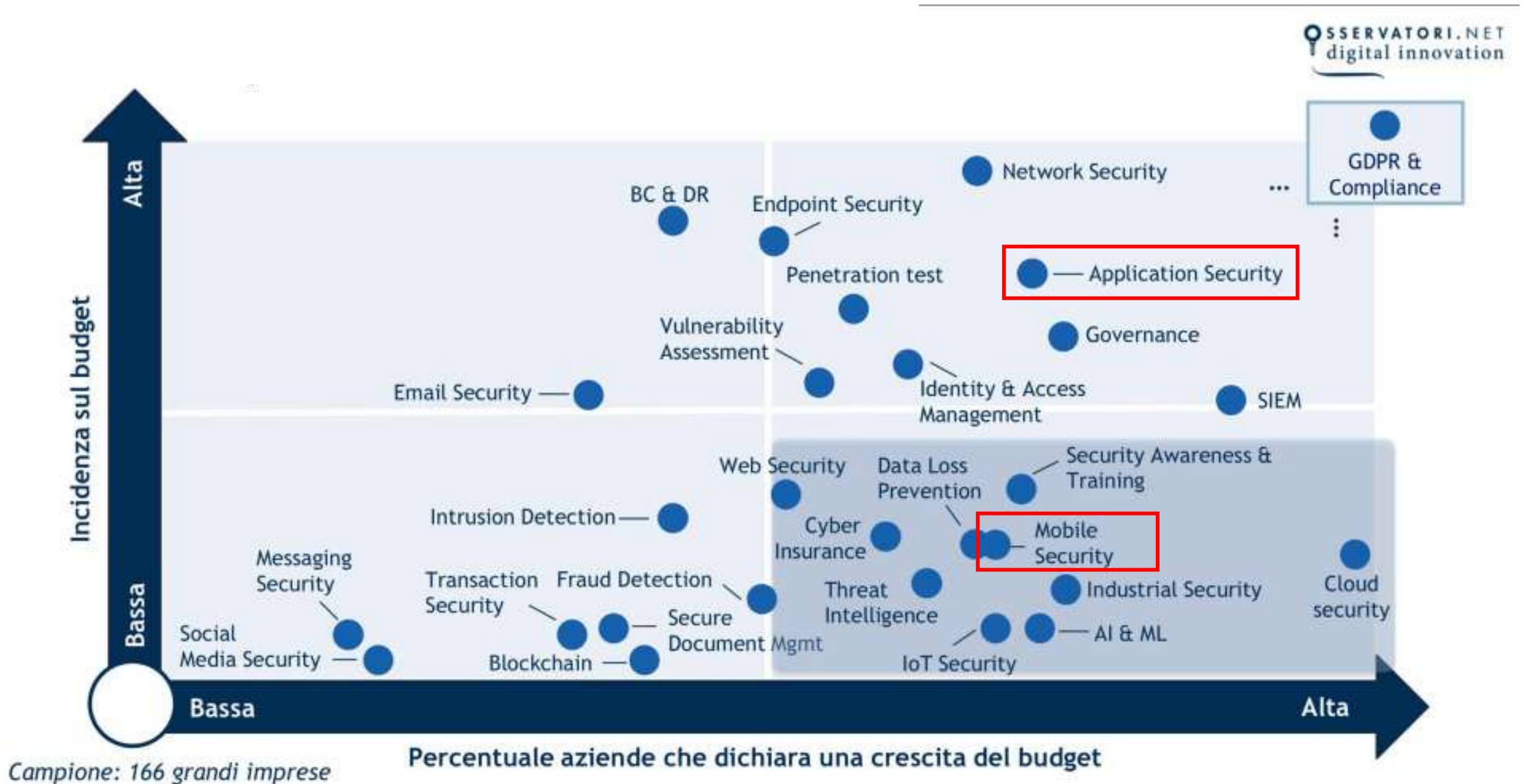
M9 – Reverse
Engineering

M10 –
Extraneous
Functionality



Fonte: OWASP Mobile Top 10 2016

Maturità del mercato



Fonte: Osservatorio Information Security & Privacy - Winter is coming: adapt to react! (5/2/2019)

Vulnerability: Assessment vs Management

ASSESSMENT
Conoscenza



Attività episodica, per **acquisire consapevolezza** delle problematiche di sicurezza



Gestire l'analisi delle vulnerabilità come «**continuous compliance**»

Agenda

1 Introduzione

MOBILE APP SECURITY

2 Survey

LA SICUREZZA DELLE MOBILE APP ITALIANE

3 MAD e DevSecOps

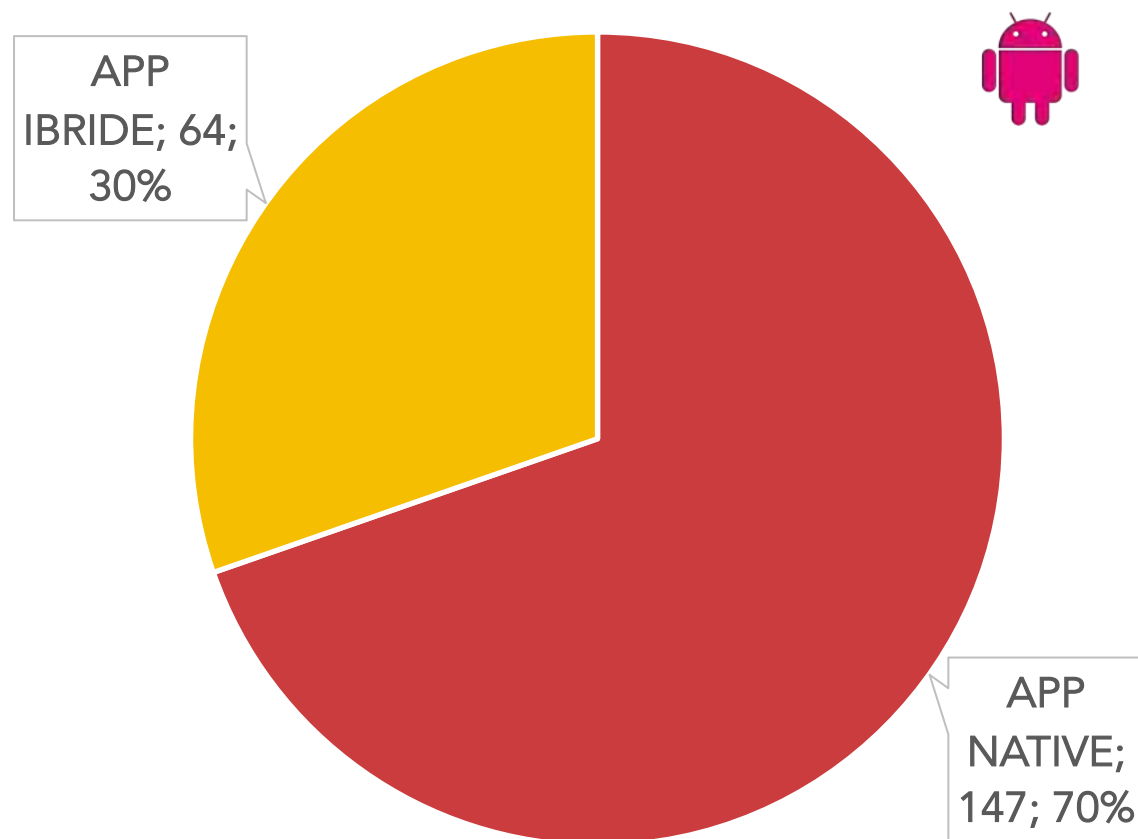
AUTOMAZIONE DELL'ANALISI

4 Case study

LA PIATTAFORMA ALL'OPERA

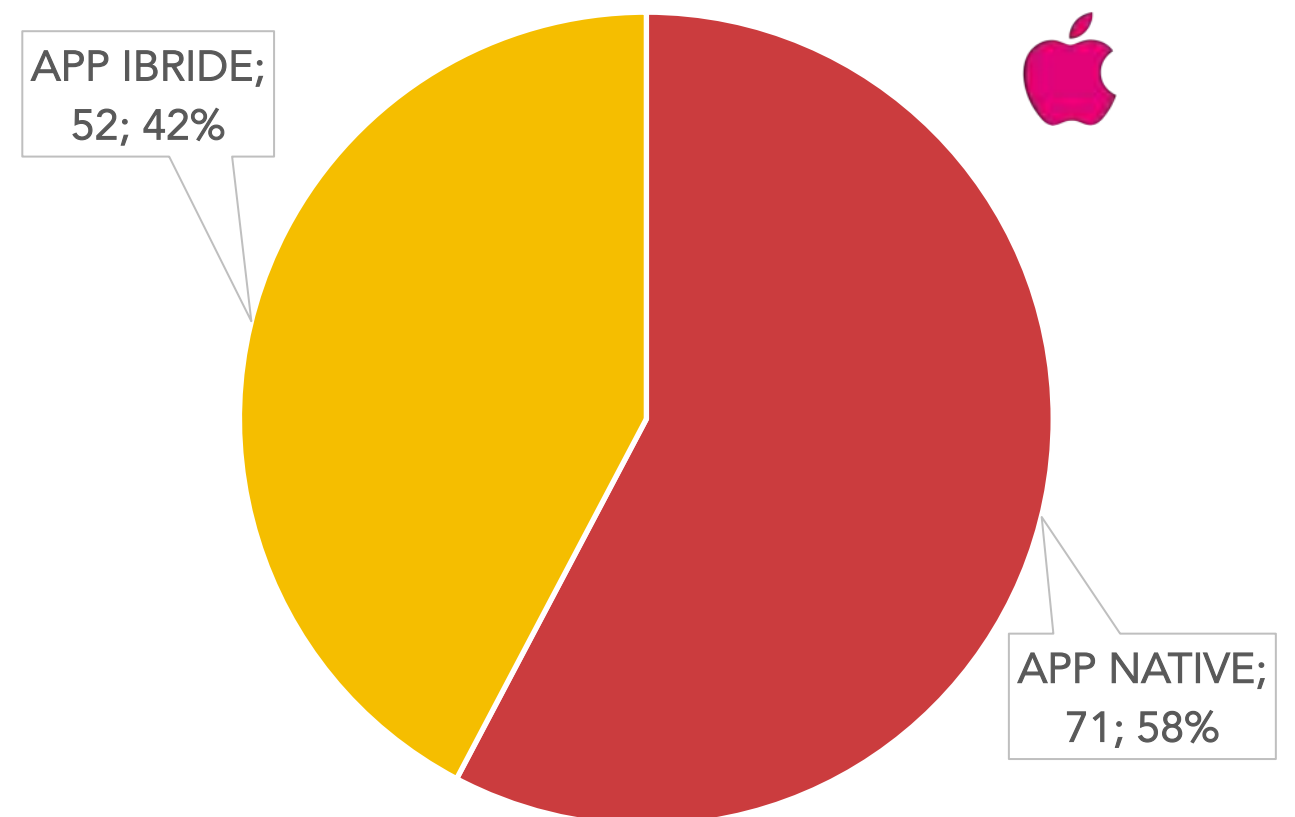
5 Demo

Survey: composizione del campione



TOTALE

211



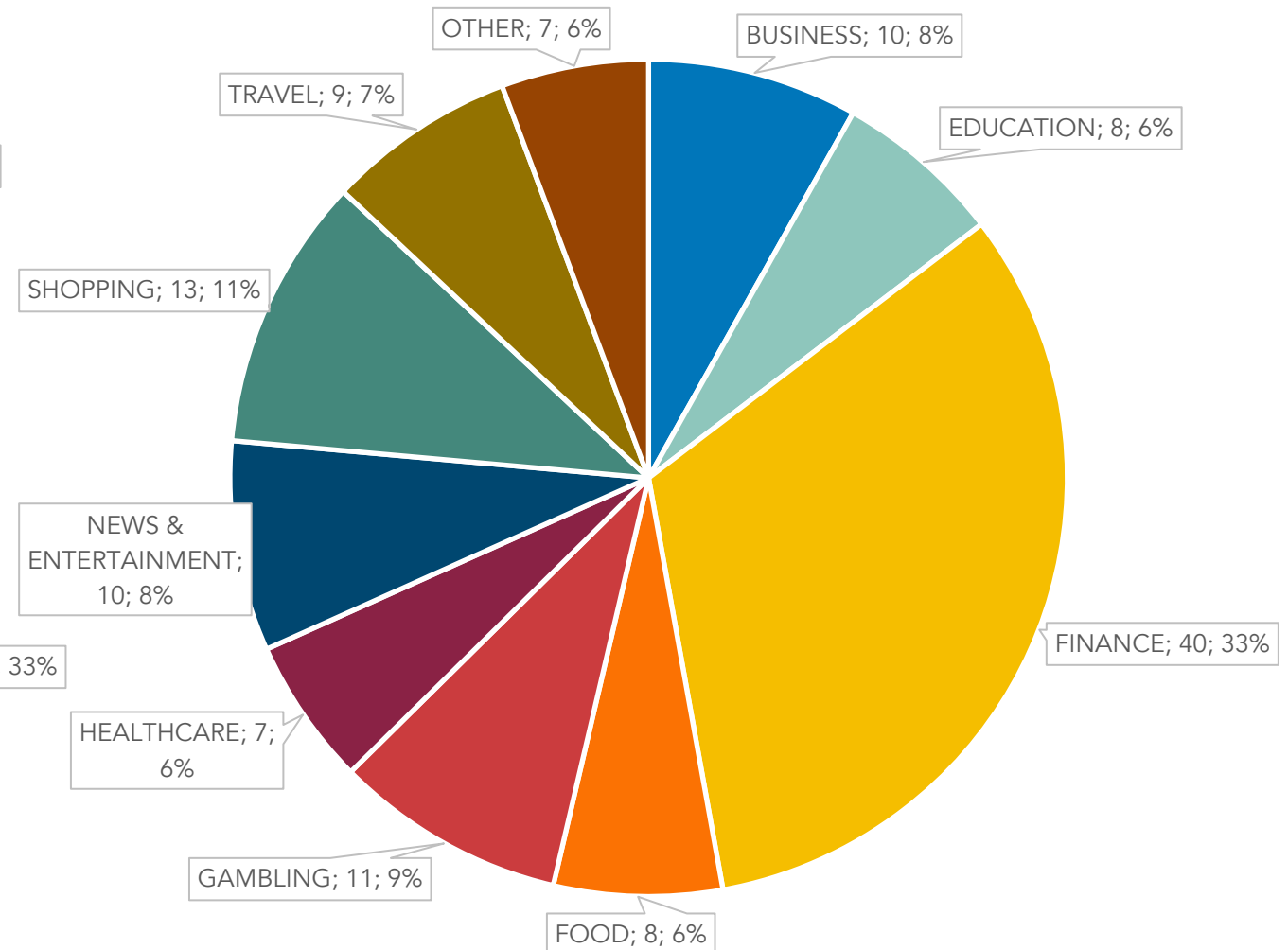
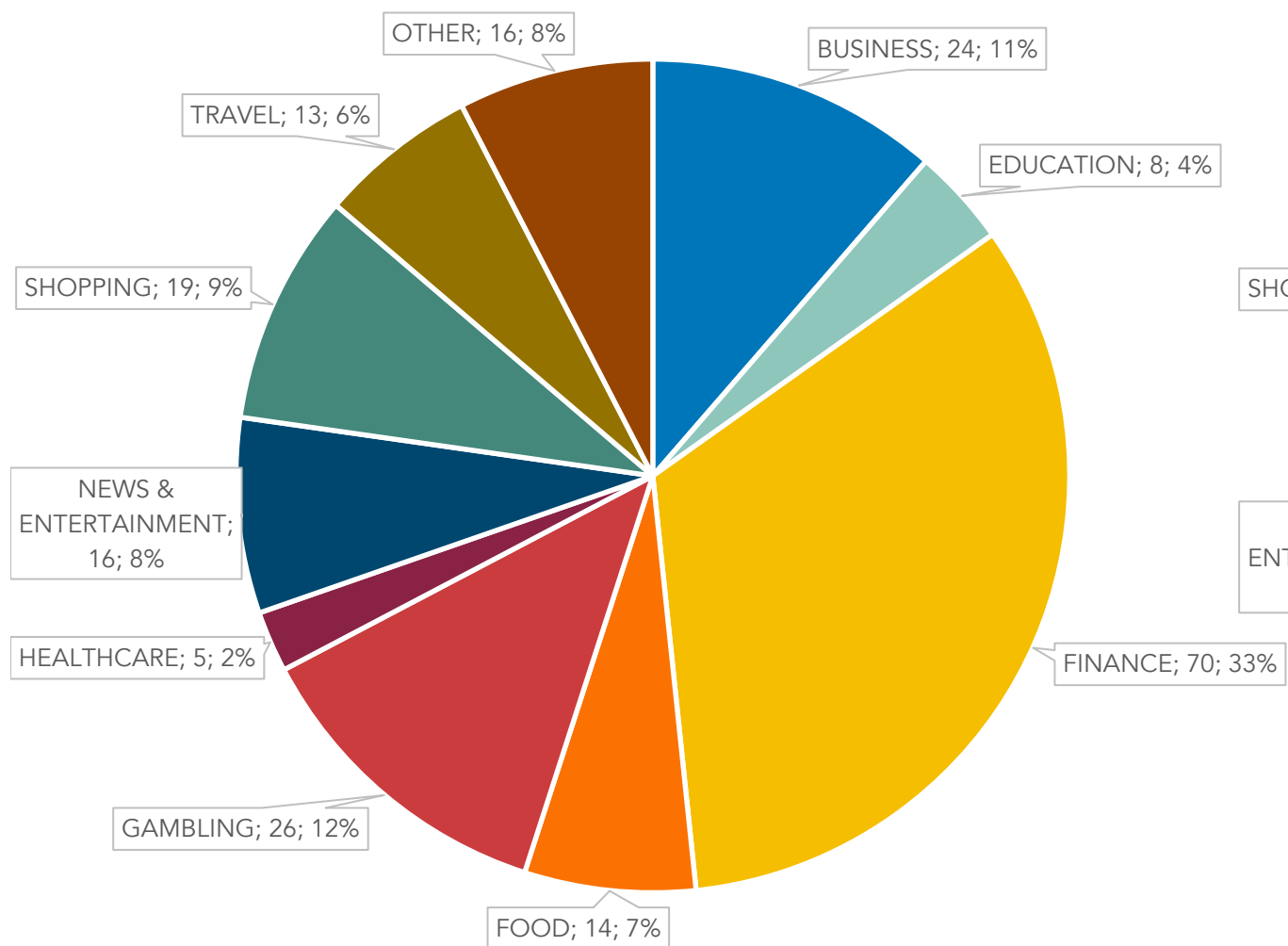
TOTALE

123

Note:

- app ibride = sviluppate con Cordova/Phonegap o Xamarin
- selezionate app **affendenti solo organizzazioni italiane** più popolari su Google Play e su Apple App Store
- le applicazioni sono state analizzate esclusivamente in modalità **statica**

Survey: settori commerciali



Survey: aggregazione vulnerabilità

Categorie

Vulnerabilità

Data leakage

- Sensitive data stored in the private folder of the mobile app:
 - Username
 - Password
 - Token
- Token disclosed via SharedPreferences
- AllowBackup flag is not false or UIFileSharingEnabled flag set to True
- Internal IP address leakage
- External data storage
- Apache Cordova CVE-2016-6799, CVE-2014-3502, CVE-2014-1881, CVE-2014-1882
- World readable files
- Public Shared Preferences
- iOS storage protection level mis-configured

Reverse engineering

- Lack of obfuscation

Tampering

- Lack of root / jailbreak detection
- Unused requested permissions
- Android APK certificate signed with key shorter than 2048 bits
- Stack Smashing Protection (SSP) not enabled
- Automatic Reference Counting (ARC) not enabled
- Apache Cordova CVE-2017-3160, CVE-2015-1835, CVE-2014-3500

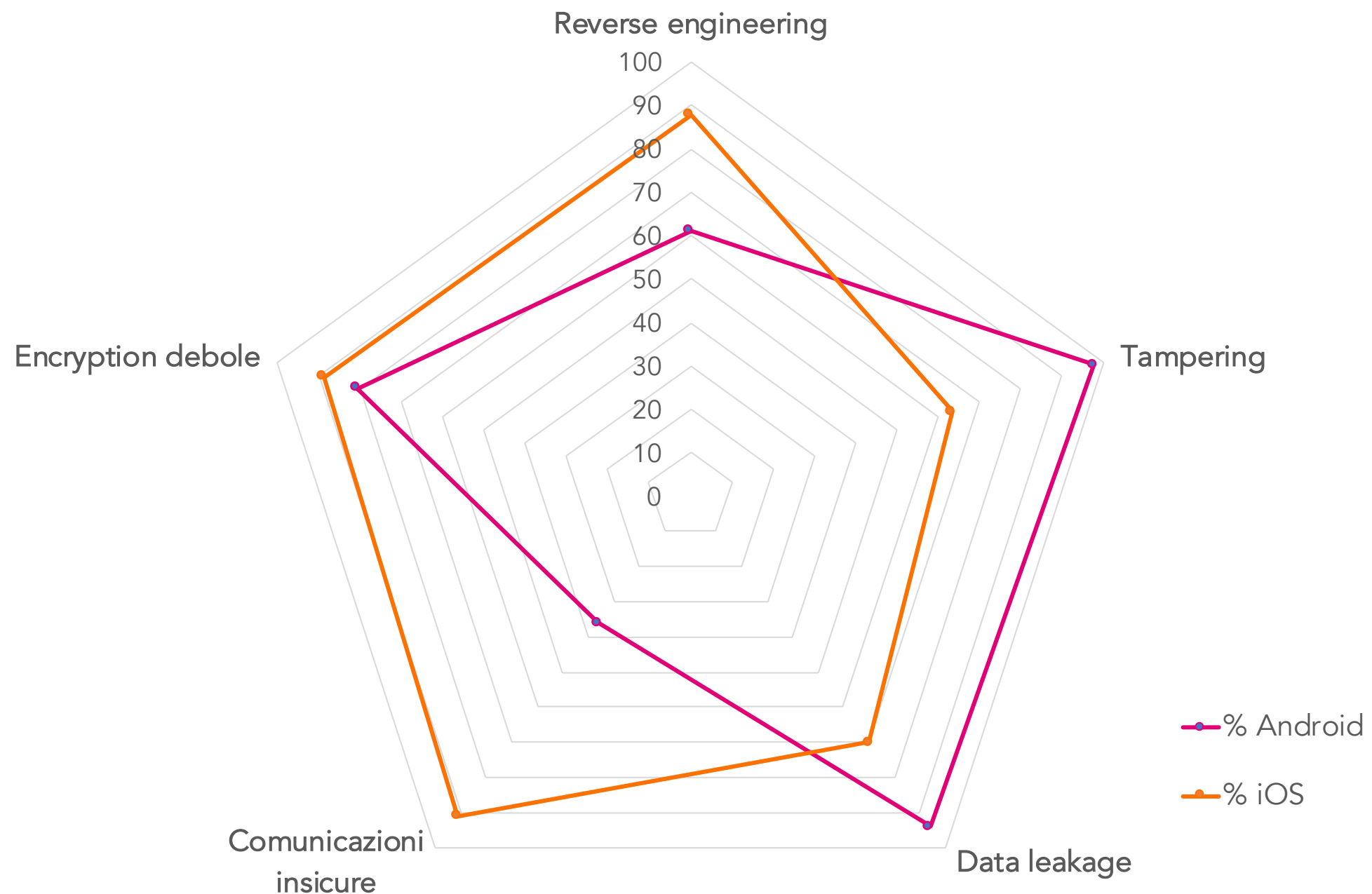
Comunicazioni insicure

- Insecure HTTP URLs detected
- Insecure HostnameVerifier
- Insecure TrustManager
- App Transport Security mis-configured
- ATS allows TLS 1.0 or 1.1
- Ciphers not supporting Perfect Forward Secrecy (PFS) allowed
- Apache Cordova CVE-2015-5256, CVE-2014-3501, CVE-2015-5207, CVE-2015-5208, CVE-2012-6637

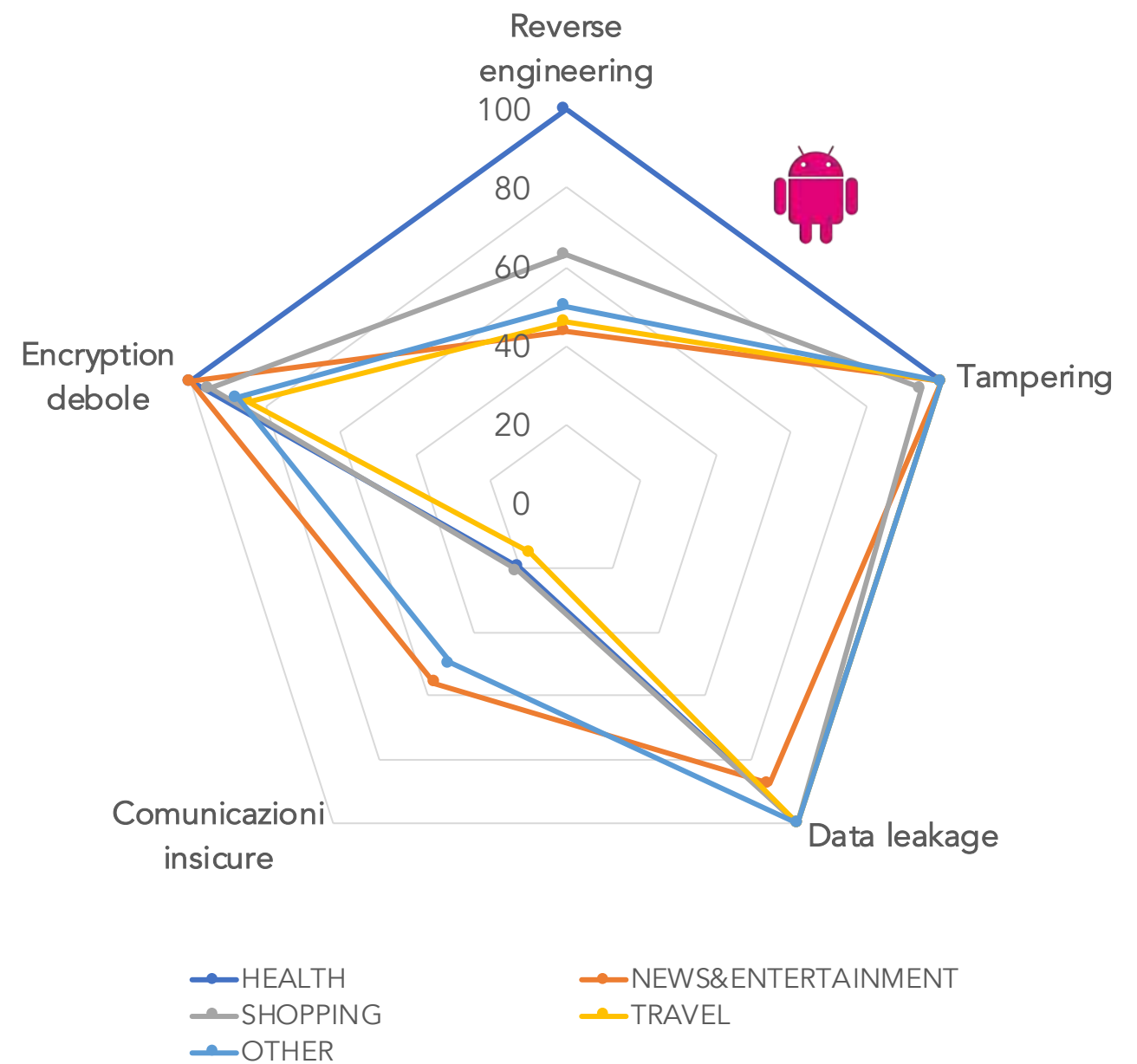
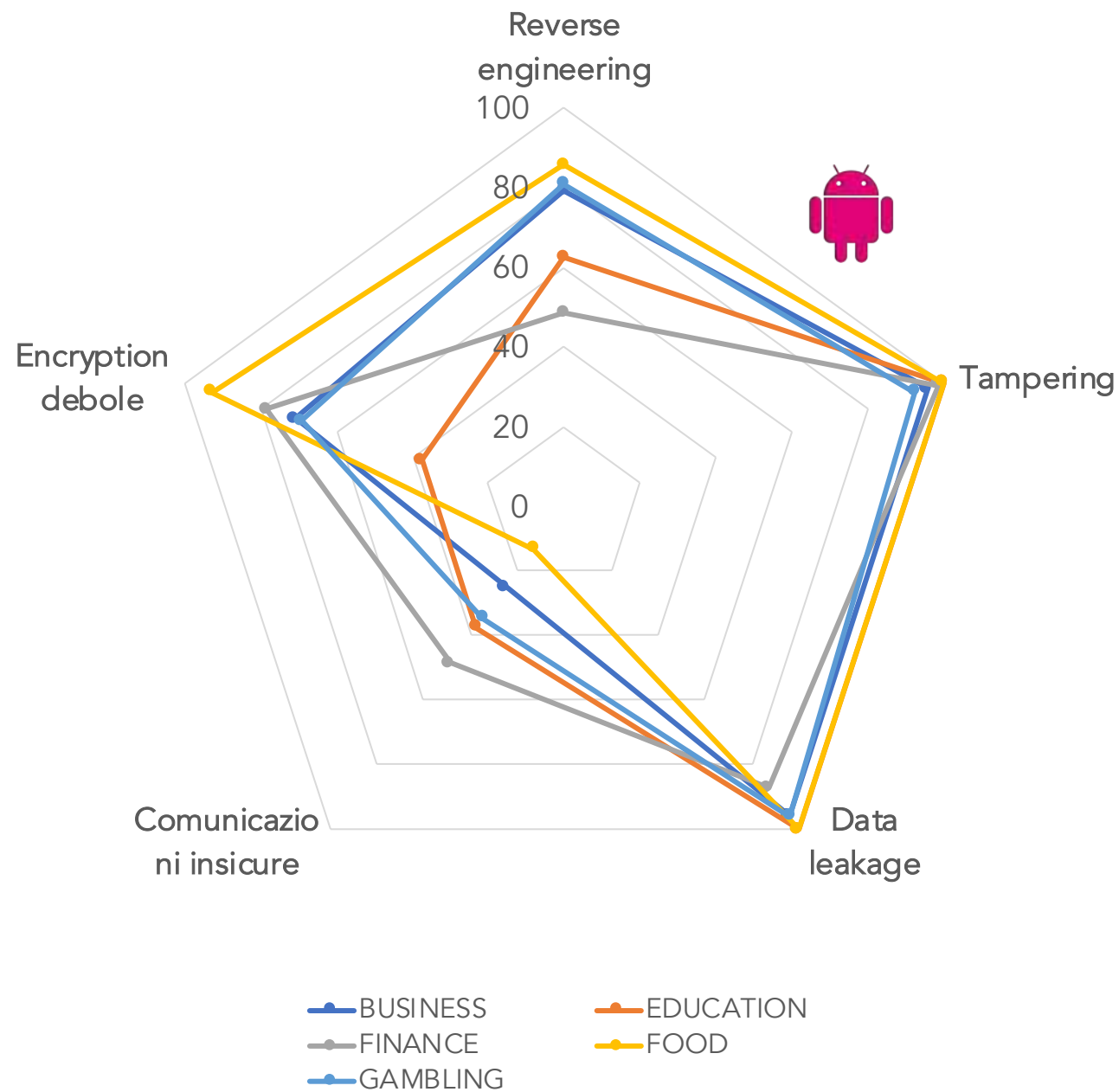
Encryption debole

- Insecure DES cipher
- Insecure MD2, MD4, MD5 hash algorithm
- Insecure SHA-1 hash algorithm
- Insecure ECB encryption mode
- Insecure RC4 cipher
- Predictable random data generation
- Apache Cordova CVE-2015-8320

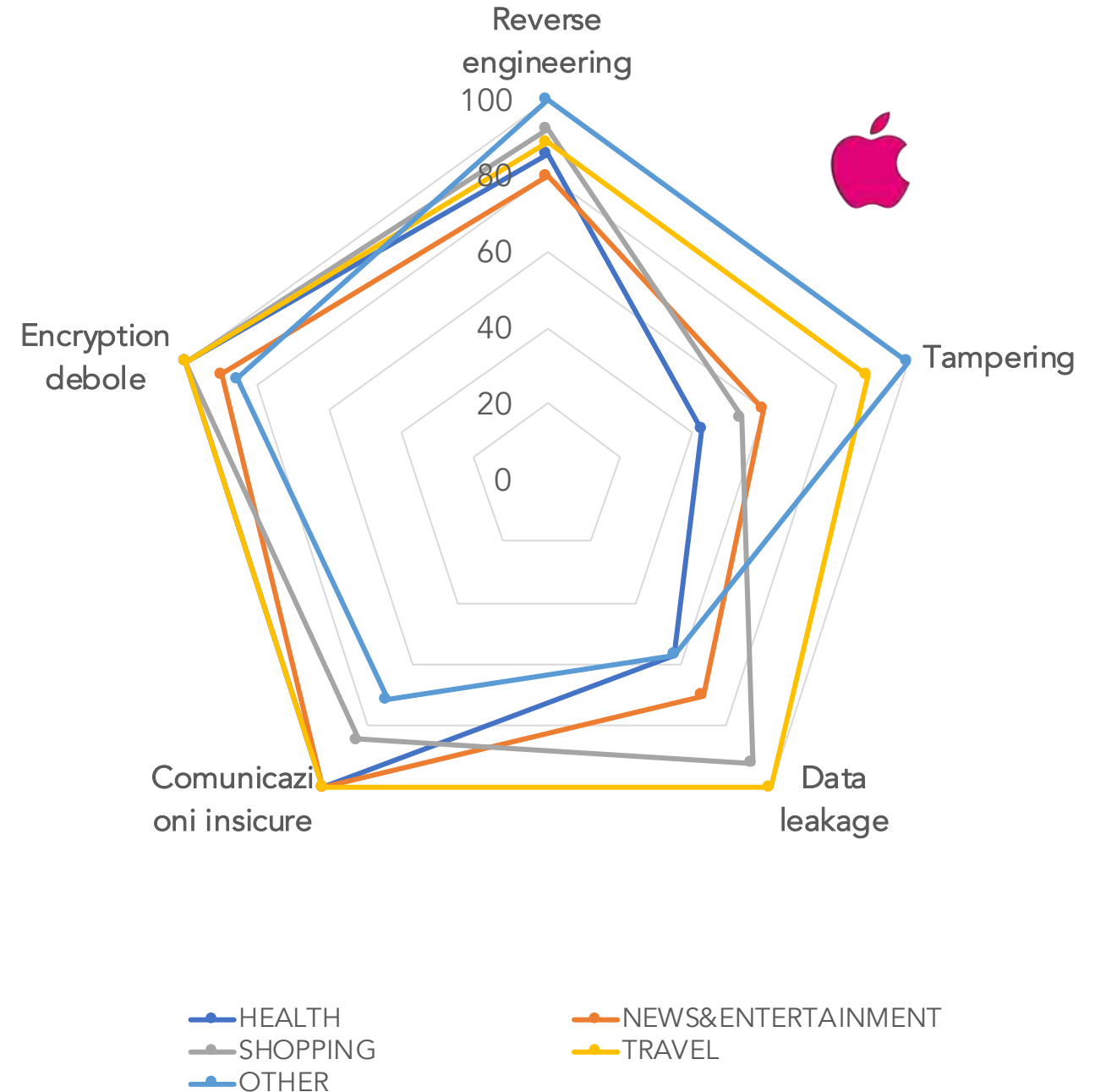
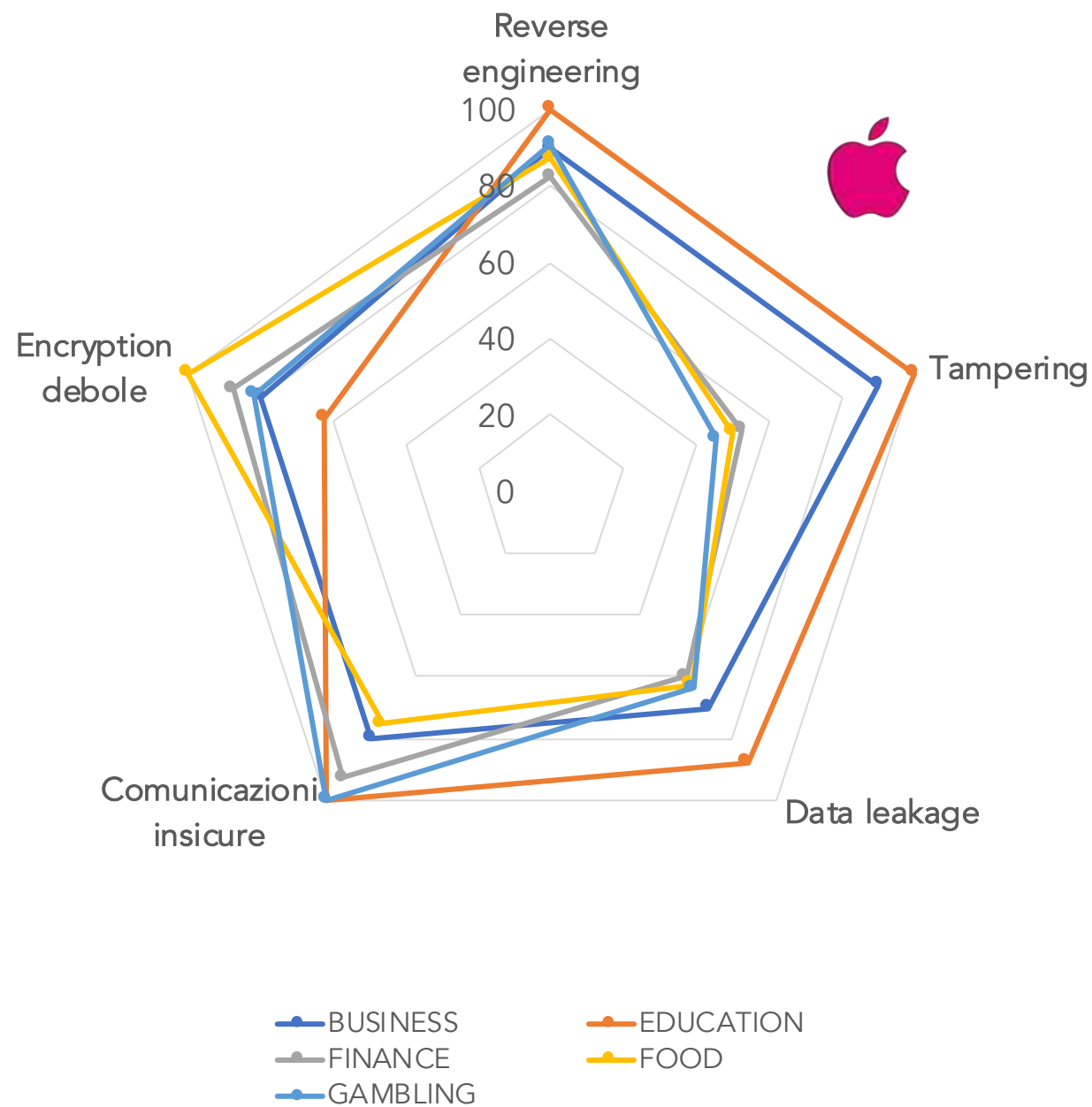
Diffusione vulnerabilità per tipologia



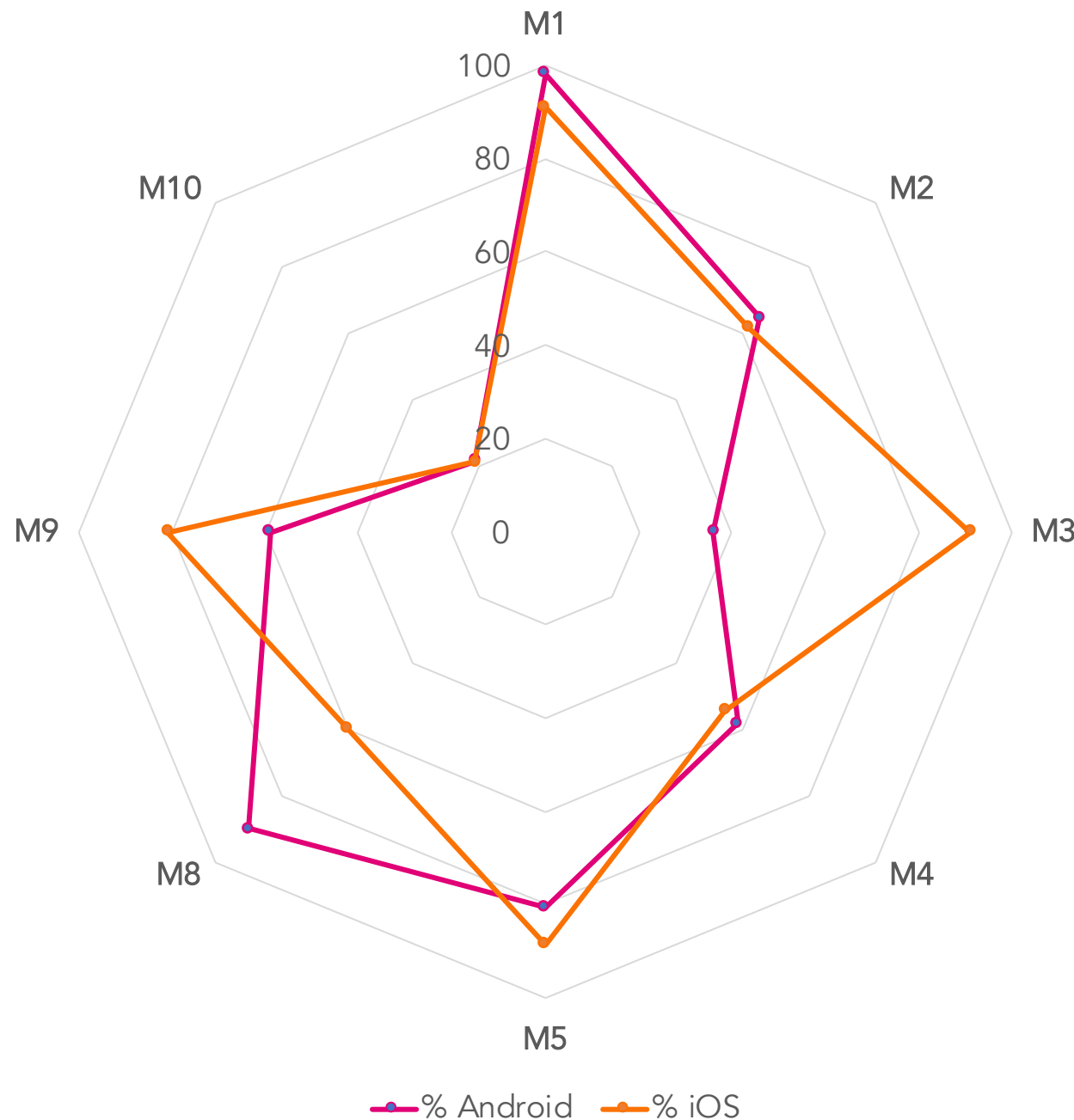
Diffusione per tipologia e settore



Diffusione per tipologia e settore



Diffusione per categorie OWASP Top10



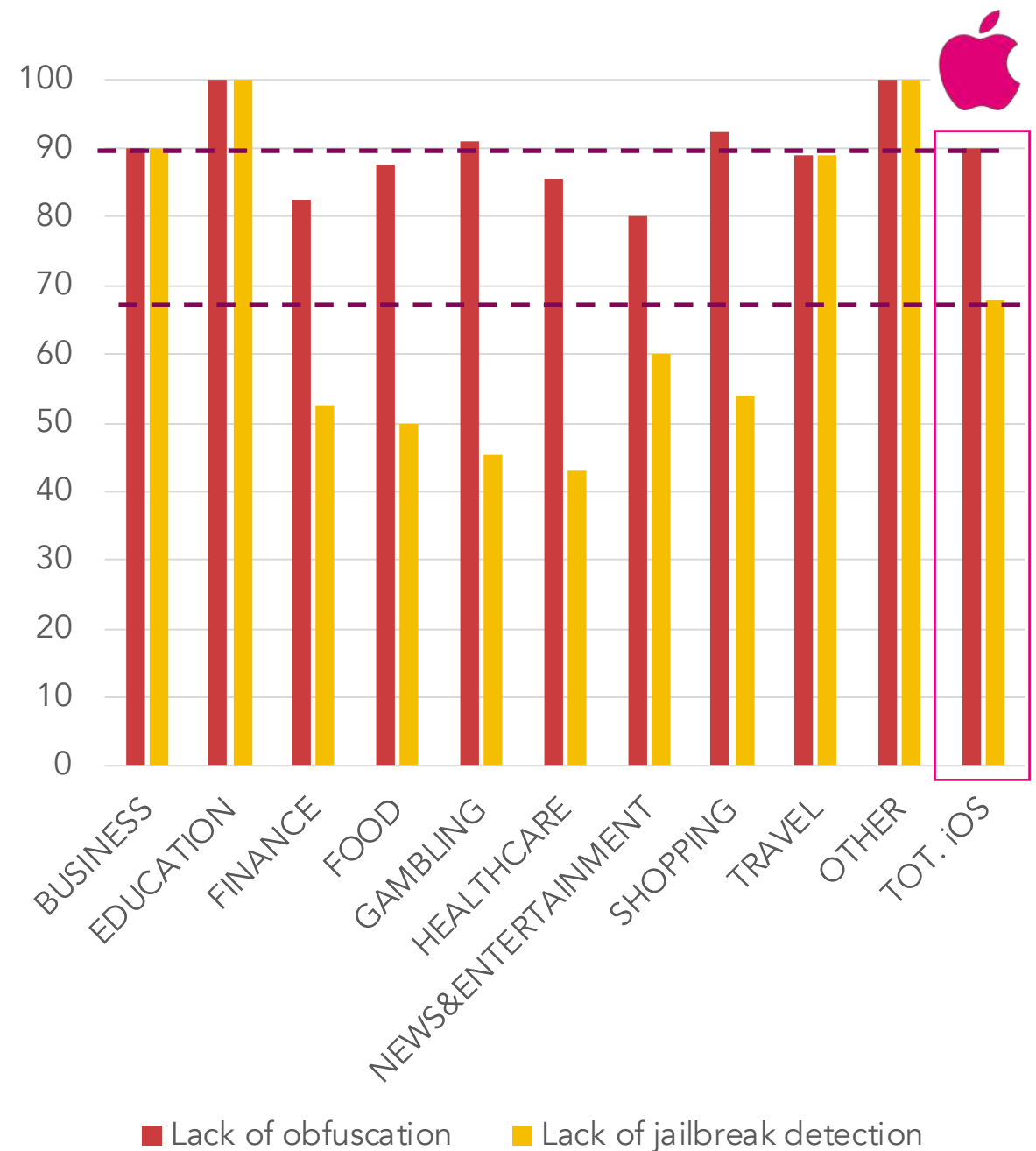
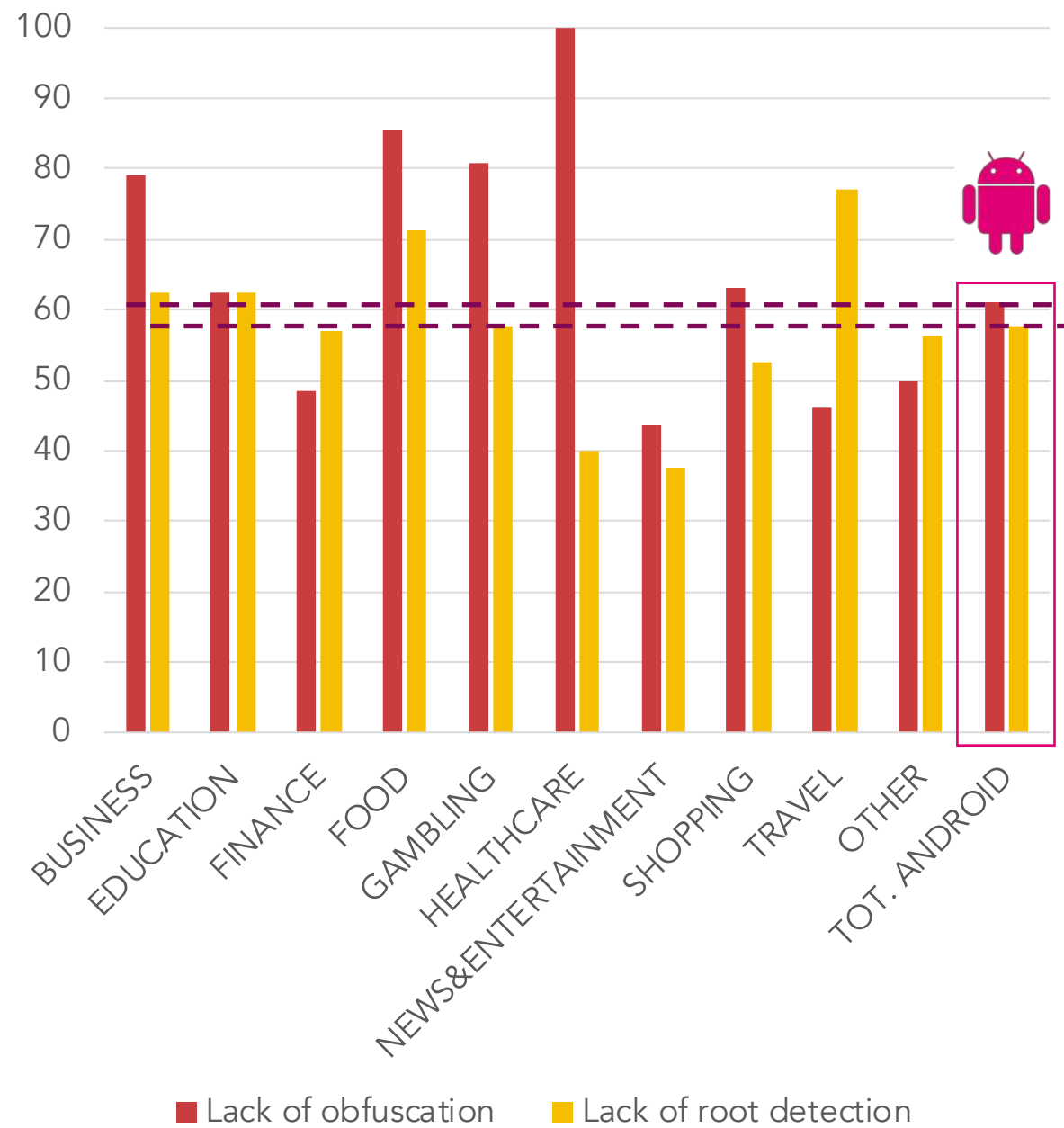
OWASP Mobile Top Ten 2016

- M1 - Improper Platform Usage
- M2 - Insecure Data Storage
- M3 - Insecure Communication
- M4 - Insecure Authentication
- M5 - Insufficient Cryptography
- M6 - Insecure Authorization
- M7 - Client Code Quality
- M8 - Code Tampering
- M9 - Reverse Engineering
- M10 - Extraneous Functionality

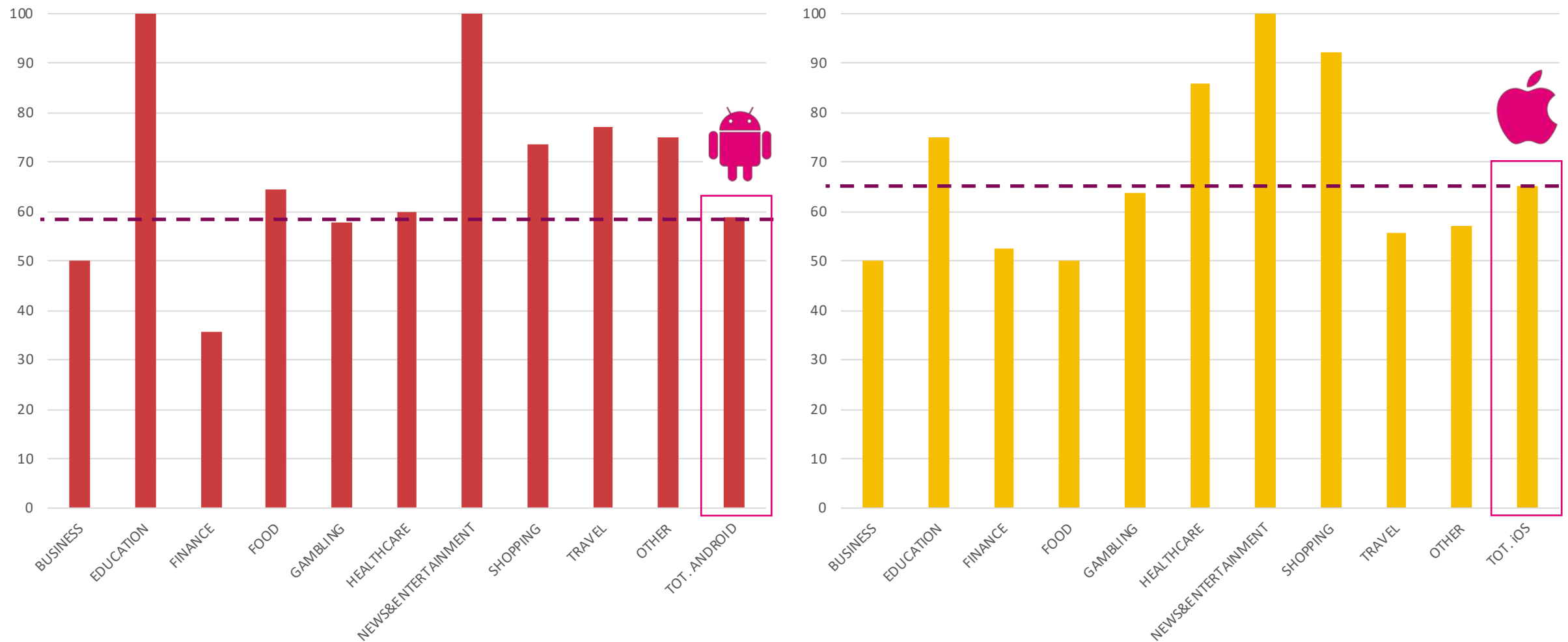
Nota:

Le categorie M6 e M7 sono verificabili solo con analisi dinamiche (cioè con app in esecuzione) e i test conducono a risultati significativi se si dispone di opportune credenziali di accesso

Drill-down su obfuscation e root detection



Approfondimento: http vs https



Presenza di URL del backend della mobile app
potenzialmente contattati in HTTP

Survey: considerazioni conclusive

Dove viene lasciato allo sviluppatore più arbitrio nelle scelte sulle configurazioni dei meccanismi di sicurezza, il rischio che siano presenti vulnerabilità è più alto

Questo ha due implicazioni:

- È necessario **formare** gli sviluppatori per scrivere mobile app sicure e usare le funzioni di sicurezza dell'OS mobile secondo le linee guida del vendor
- È necessario introdurre uno o più **gateway di validazione** nel ciclo di sviluppo software al fine di individuare e indirizzare queste problematiche

Agenda

1 Introduzione

MOBILE APP SECURITY

2 Survey

LA SICUREZZA DELLE MOBILE APP ITALIANE

3 MAD e DevSecOps

AUTOMAZIONE DELL'ANALISI

4 Case study

LA PIATTAFORMA ALL'OPERA

5 Demo

Strumento utilizzato

CryptoNet Labs utilizza la piattaforma proprietaria di Vulnerability Assessment e Management specifica per l'analisi della sicurezza delle Mobile App



Security Governance

- Governo della sicurezza delle app mobili attraverso un processo automatico di verifica prima della distribuzione
- Controlli atomici, riproducibili e misurabili nel tempo
- Validazione di app mobili prodotte da fornitori esterni
- Security Awareness

Sviluppo Software

- Piattaforma integrabile nel ciclo di sviluppo SW
- Supporto per lo sviluppo di codice sicuro
- Efficacia e consistenza all'attività di security testing
- Supporto alla remediation delle vulnerabilità



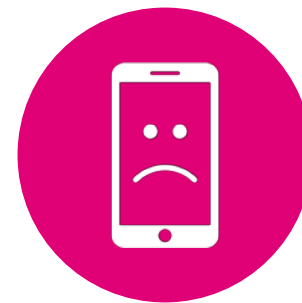
Caratteristiche: In-Depth Security



Controllo completo di una mobile app
MAD effettua più di 100 tipologie di controlli per Android e iOS al fine di identificare tutte le possibili vulnerabilità



Librerie di 3e parti/SDK
MAD effettua l'analisi di librerie di terze parti, nel caso l'app le utilizzi



Falsi positivi
La tecnologia di MAD riduce la segnalazione di falsi positivi: in ogni caso l'utente può marcare le vulnerabilità non esistenti per affinare le analisi successive



API backend analysis
MAD esegue un'analisi completa del backend dell'app, valutando le API proprietarie e di terze parti

Caratteristiche: Analisi statica e metadati

“Early build”: Può essere applicata anche alle prime build dell'app, quando non è ancora funzionalmente completa



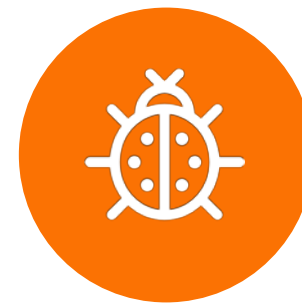
Analisi statica del codice

Caricato il pacchetto IPA o APK (non sono necessari sorgenti), MAD lo decompila e analizza in profondità il codice, in modo indipendente dal linguaggio di sviluppo Java, ObjectiveC o Swift



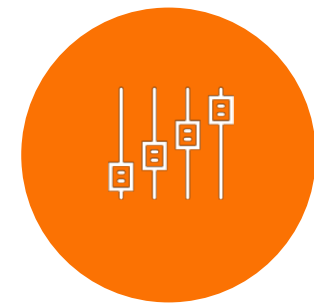
Informazioni sensibili e Forensics

MAD identifica valori codificati all'interno dell'app che per loro natura possono essere sensibili.
Es: API Key, IP, URL, password...



Controllo delle WebViews

MAD è in grado di effettuare la scansione di app che usano Webview per identificare possibili vulnerabilità nel loro utilizzo



Esame di metadati e configurazioni locali

MAD rileva problematiche di:

- Android – manifest, permessi, flag, ecc.
- iOS – info.plist, ATS, entitlement, ecc.
- più in generale – versione vulnerabili Cordova / PhoneGap, la presenza di obfuscation o altre segnalazioni

Caratteristiche: Analisi dinamica e network



Analisi dinamica

MAD effettua un'analisi a runtime completa eseguendo l'app su dispositivi reali attrezzati e registrando il comportamento (MAD è jailbreak-independent)



Insecure data storage

MAD individua tutti i file creati e segnala eventuali informazioni sensibili registrate all'interno



Network traffic analysis

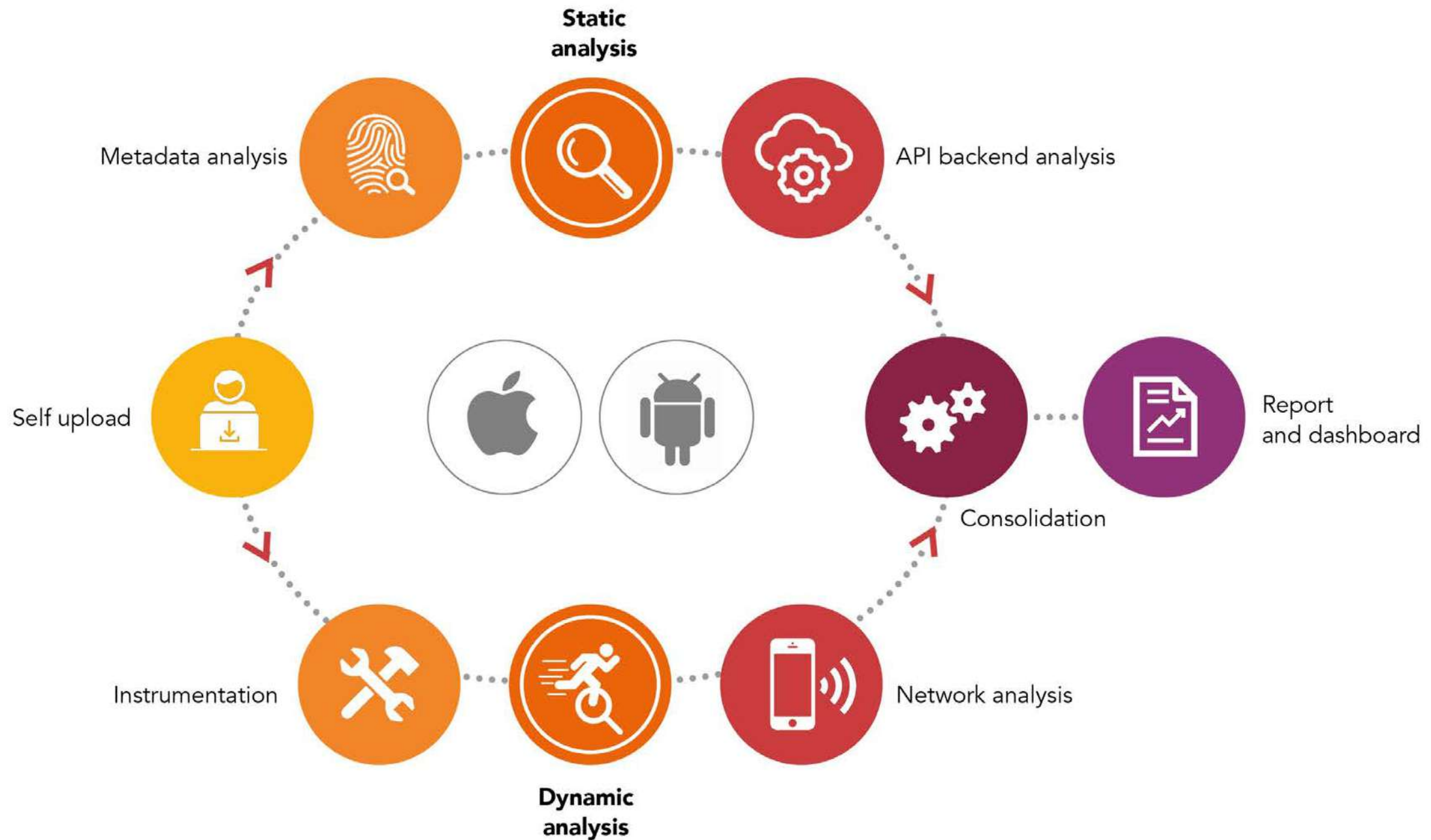
L'app è eseguita in un ambiente "man-in-the-middle" con cui MAD traccia di tutte le attività a livello di rete e rileva comunicazioni insicure



Insecure Android / iOS IPC

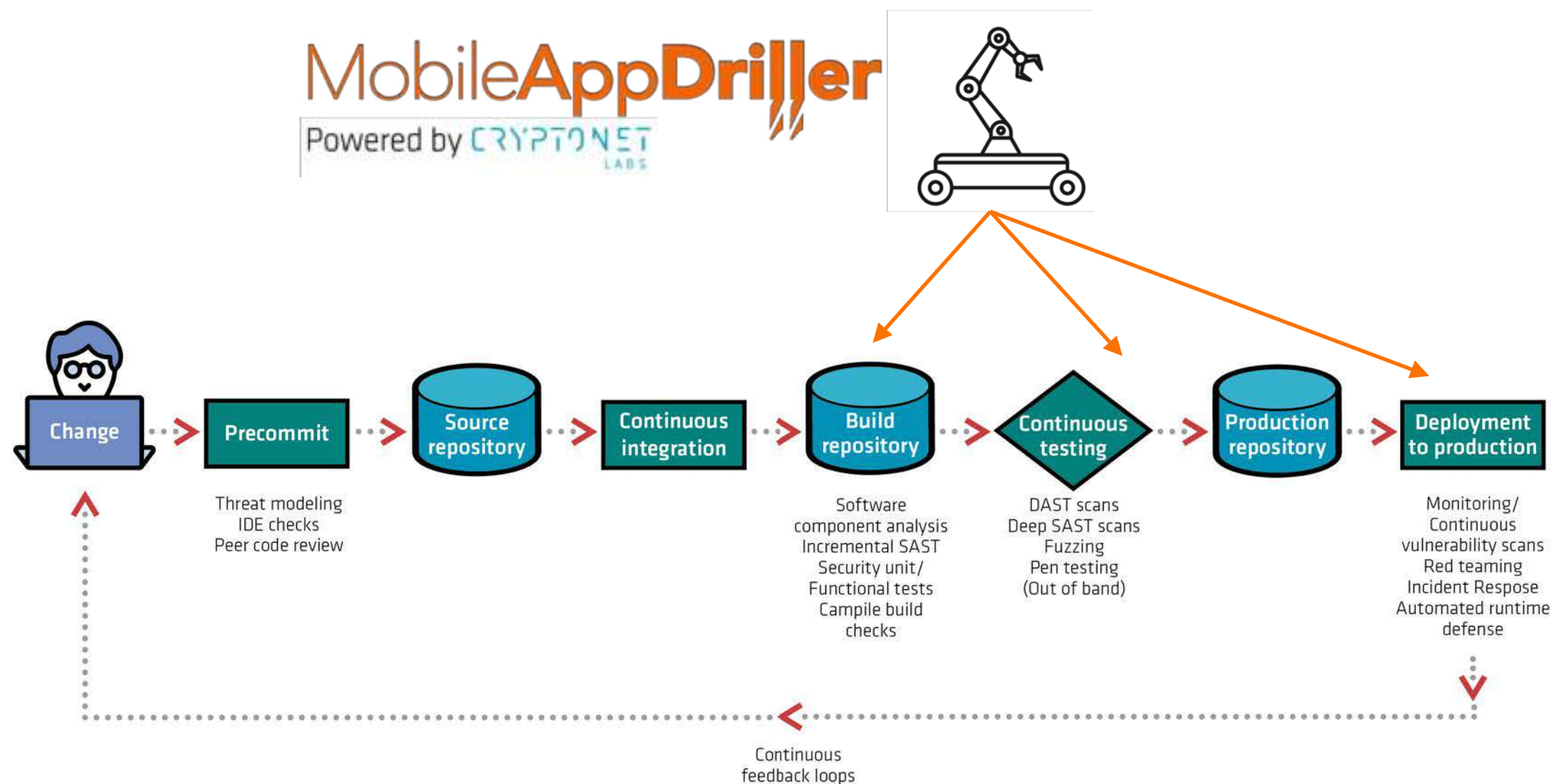
MAD identifica le vulnerabilità nelle varie componenti IPC come Activities, Content provider, clipboard, URL scheme, ecc.

MAD: funzionamento



DevSecOps

MAD può essere **integrato** nella toolchain automatizzata DevOps, supportando il cliente nella transizione del SDLC delle Mobile App verso Dev**Sec**Ops



Agenda

- 1 Introduzione
MOBILE APP SECURITY
- 2 Survey
LA SICUREZZA DELLE MOBILE APP ITALIANE
- 3 MAD e DevSecOps
AUTOMAZIONE DELL'ANALISI
- 4 Case study
LA PIATTAFORMA ALL'OPERA
- 5 Demo

Case study: il cliente e le sue esigenze

Cliente

- Società italiana leader nel settore Finance
- Eroga servizi ai propri clienti tramite **mobile app** sviluppate internamente

Contesto

Attenzione alle problematiche di sicurezza

- per la criticità dei dati trattati
- per il rispetto di leggi e standard
- prevenzione del danno di immagine

Superamento del concetto di vulnerability assessment a favore di un processo di **vulnerability management** per tutta la durata del suo ciclo di vita.

Esigenze

- soluzione **automatizzata**
- per eseguire **test ripetibili**
- basati su **best practices riconosciute**
- con **risultati misurabili e comparabili** nel tempo
- e diversi **livelli di analisi** (executive + tecnico)



Case study: il progetto proposto

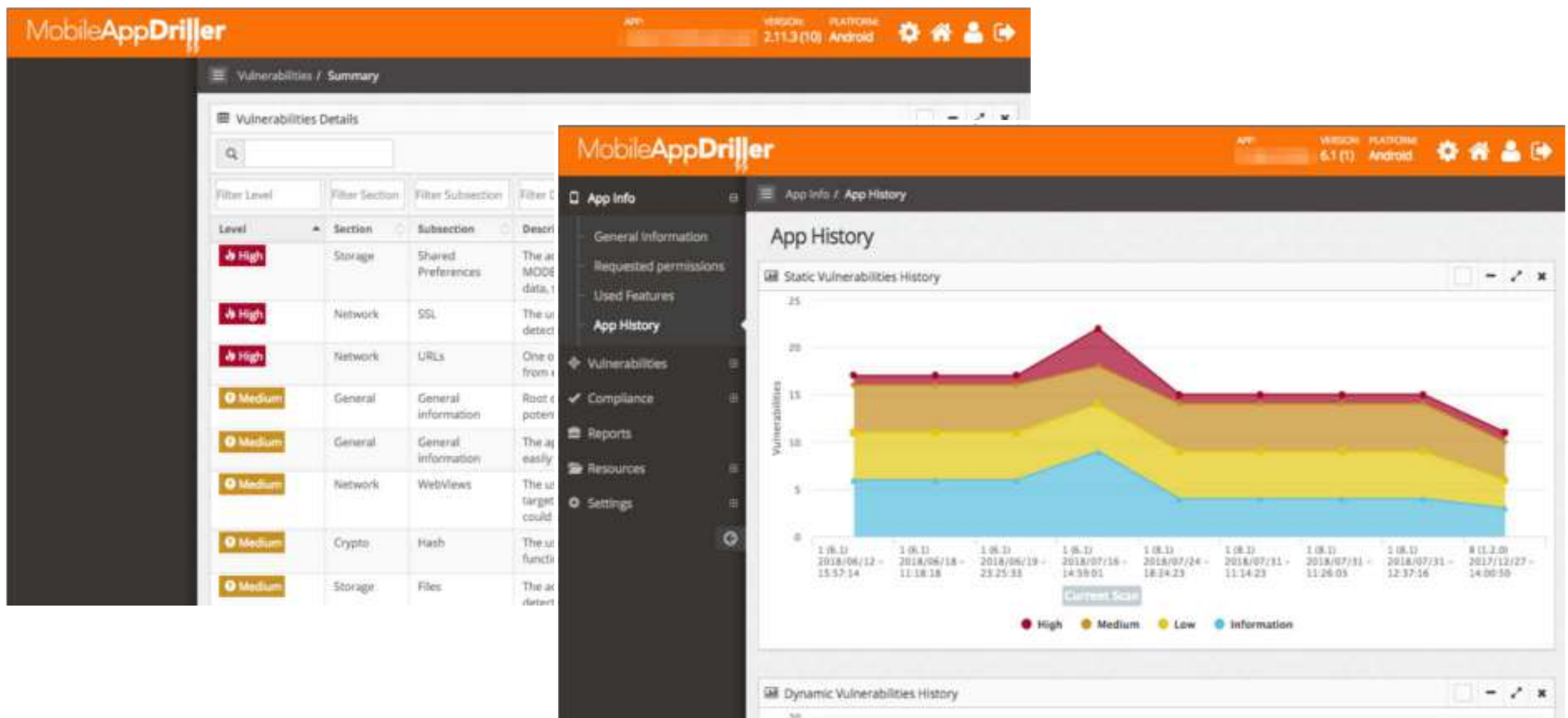
CryptoNet Labs:

- Ha **integrato** nel ciclo di sviluppo software l'uso di **Mobile App Driller**
 - piattaforma per **automatizzare** i controlli di sicurezza secondo lo standard OWASP
 - tramite **analisi statica** e **dinamica** del pacchetto binario (senza necessità di codice sorgente)
- Ha inoltre **implementato i controlli presenti nelle linee guida interne** del cliente per lo sviluppo di codice sicuro, personalizzando MAD sulle sue specifiche esigenze
- Fornisce **supporto specialistico**
 - a sviluppatori, application owner e IT security analyst
 - per la revisione dei risultati e la definizione delle azioni di remediation

MobileAppDriller

Case study: fattori di successo

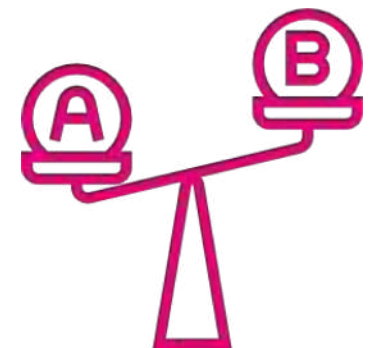
La nostra **esperienza** pluriennale nei pentest di Mobile App è confluita in **MAD**, progettato per dare **completezza** di analisi, **riproducibilità** dei test ed **efficacia** nella fruizione dei risultati



Benefici per il cliente

Grazie all'uso di MAD il cliente:

- Rende **efficace la gestione delle misure di sicurezza** all'interno del proprio ciclo di sviluppo di software introducendo diversi punti di controllo automatizzato, adattandosi alla propria metodologia Agile (in particolare, prima della conclusione di ogni «sprint»)
- **Determina le priorità** di intervento, grazie alla fruibilità della piattaforma MAD e alla completezza delle informazioni presentate
- **Riduce i tempi di verifica della remediation**, potendo eseguire in totale autonomia un numero illimitato di scansioni secondo le proprie necessità
- Dispone di uno strumento per il **monitoring** della sicurezza nel processo di sviluppo, grazie alla riproducibilità dei controlli, con la possibilità di evidenziare trend di miglioramento (KPI)
- È conforme agli standard **GDPR, PCI, PSD2 e OWASP**



Agenda

- 1 Introduzione
MOBILE APP SECURITY
- 2 Survey
LA SICUREZZA DELLE MOBILE APP ITALIANE
- 3 MAD e DevSecOps
AUTOMAZIONE DELL'ANALISI
- 4 Case study
LA PIATTAFORMA ALL'OPERA
- 5 Demo

Demo





Grazie per l'attenzione

MobileAppDriller

sales@cryptonetslabs.it

MAD: in sintesi

Descrizione	Soluzione che automatizza la ricerca e l'analisi di vulnerabilità di sicurezza per mobile app, integrandosi nel SDLC del cliente
Tipologie di analisi	Statica (reverse engineering) Dinamica + Network (MITM)
Piattaforme supportate	Android (statica+dinamica) iOS (statica+dinamica)
Elementi di differenziazione	- controlli ripetibili e misurabili "app portfolio" management - timeline e trend - scan history e comparison - customizzazione: controllo completo della soluzione
Licensing	Per app / anno (test illimitati)

Deployment	Cloud (SaaS) o on-premises – nessuna differenza funzionale
Fruizione	In autonomia o (se cloud) in full outsourcing
Destinatari	Sviluppatori, Security analyst, Auditor, IT manager
Quando utilizzarla?	Dopo ogni build, in collaudo, in fase di validazione di una fornitura
Grado di copertura	Individua automaticamente vulnerabilità o fornisce al tester elementi di indagine, nonché la possibilità di test su device reali
Aree di controllo	Codice, app configuration, network traffic, encryption, storage, log, IPC, ecc.

Appendice

GDPR e mobile app



- Art. 5 - Principi applicabili al trattamento
I dati personali sono trattati in maniera da **garantire un'adeguata sicurezza**, compresa la protezione, mediante misure tecniche e organizzative adeguate, **da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o danno accidentali**
- Art. 32 – Sicurezza del Trattamento
Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamenti, come anche del rischio [...] mettono in atto misure tecniche e organizzative [...] che comprendono [...] **una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento**

PCI DSS e mobile app

- FAQ #1283

L'ambiente in cui il consumatore utilizza l'app (il suo dispositivo) è fuori dal perimetro PCI, ma **l'app deve essere sviluppata seguendo le best practice di settore e tutti i requisiti dello standard PCI-DSS applicabili**



- Requisito 6.5 standard PCI-DSS

Non devono essere introdotte vulnerabilità applicative durante le diverse fasi del ciclo di sviluppo software, in particolare l'implementazione

- PCI Mobile Payment Acceptance Security Guideline 2.0 (09/2017)

Gli sviluppatori devono prevenire gli accessi non autorizzati e la compromissione dei dati, testare le app e i sistemi di back-end che ne costituiscono l'ambiente, attuare misure protettive contro le vulnerabilità, utilizzare tecniche di hardening

PSD2 e mobile app



- Utilizzare un **doppio fattore di autenticazione** per identificare l'utente e per autorizzare i pagamenti
- **Proteggere la confidenzialità e l'integrità** delle credenziali utilizzate
- Generare un **codice di autenticazione** secondo **specifici requisiti**
- Garantire **comunicazioni sicure** tra l'app di pagamento e i sistemi di back-end della banca
- **Separare gli ambienti** di esecuzione
- Assicurare che **il software** (o il dispositivo) **non sia stato alterato**