ZIMPERIUM®

Where's the "Sec" in Mobile DevOps?

8th October 2024

Simon Scaife | Mobile AppSec

Agenda

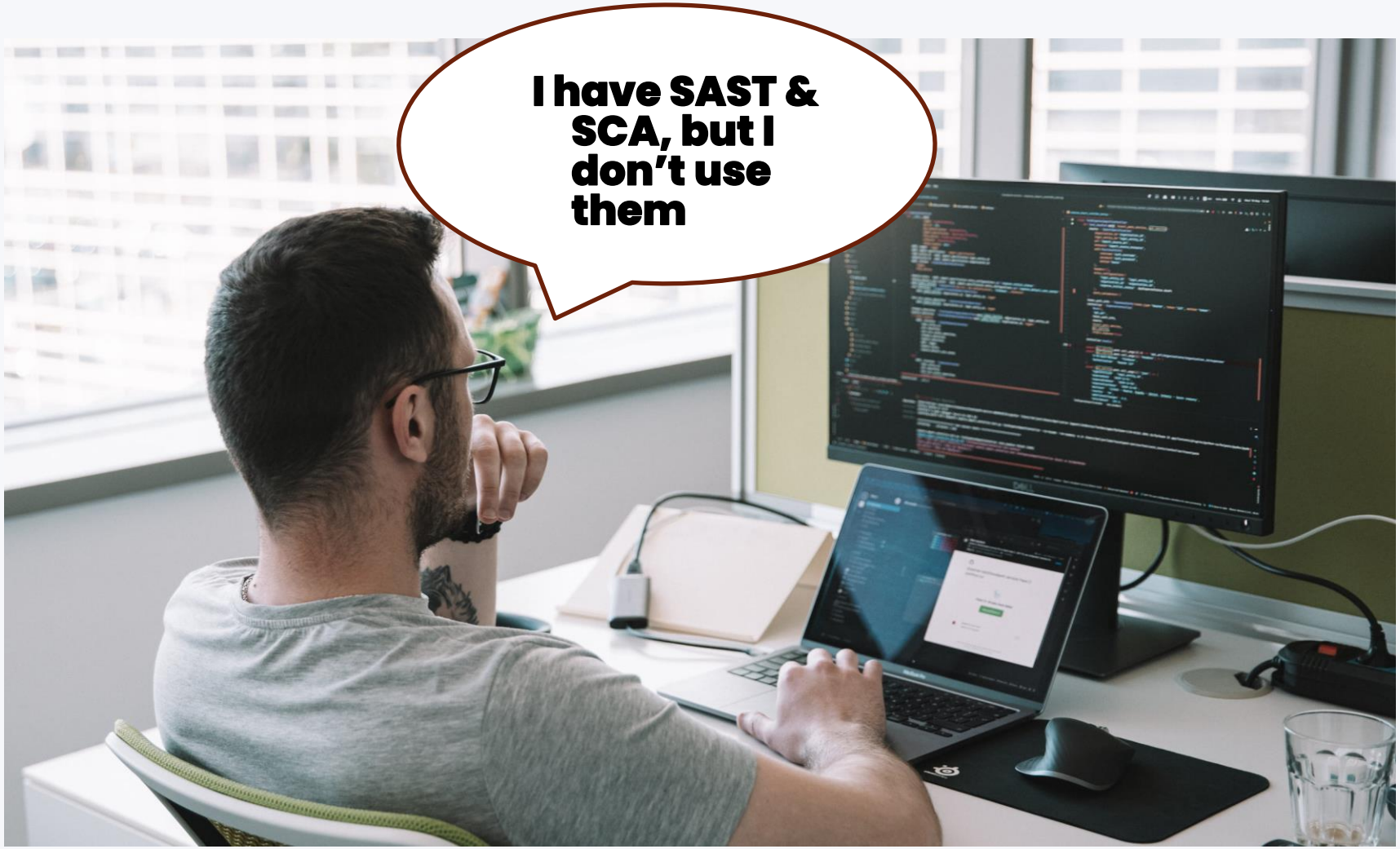
- Today's Enterprise Mobile App Footprint
- How secure are today's mobile Apps?
- Why Mobile is Different & why traditional perimeter-based security does not Work
- Where do risks arise?
- A better approach

ZIMPERIUM.

About the Presenter

Simon Scaife – Mobile AppSec Sales Leader

Typical conversation I have…



ZIMPERIUM.

Today’s Mobile App footprint

Mobile App usage continues to grow

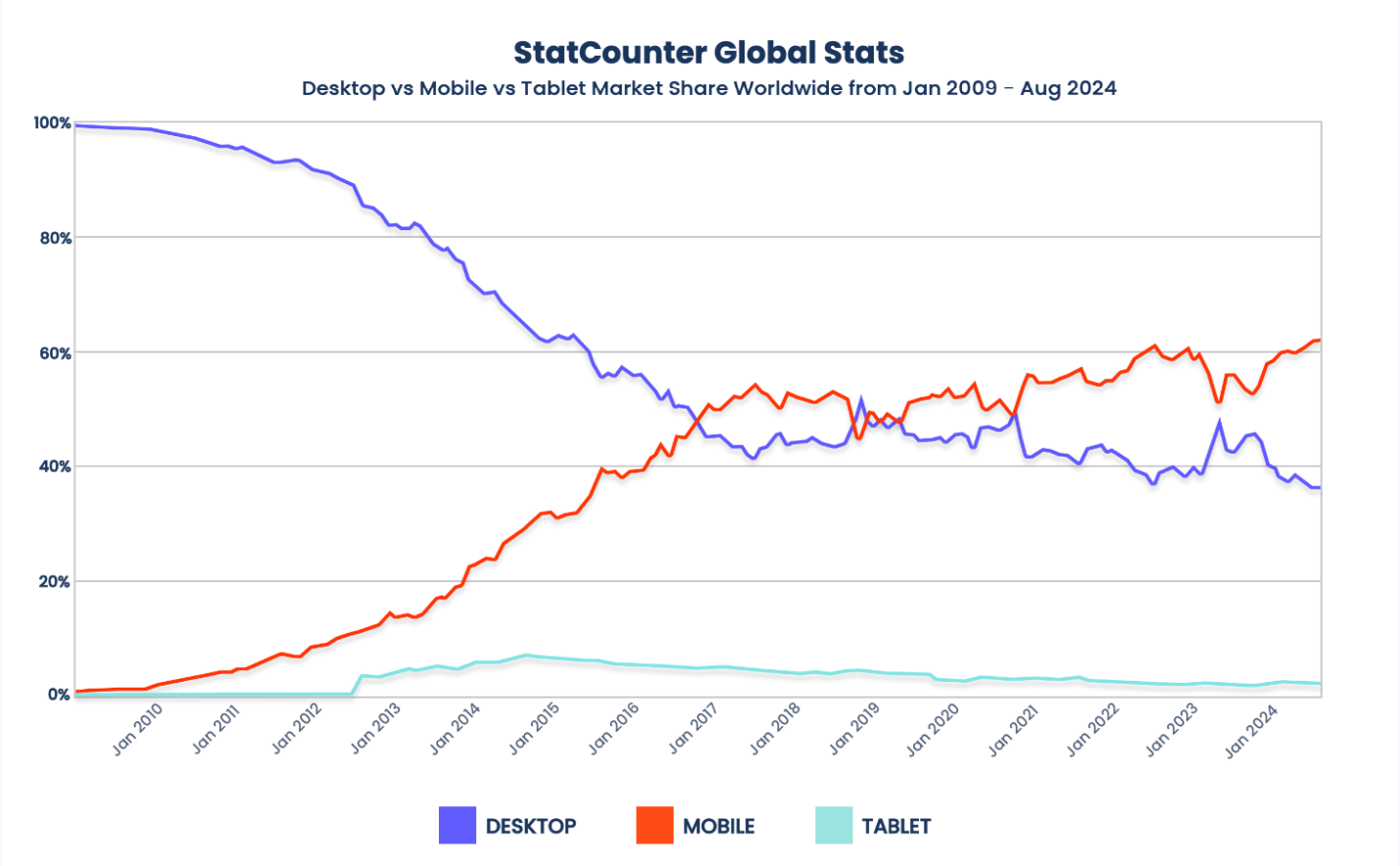
- **90%** of mobile internet usage is spent in apps
- **100 billion hours** logged in mobile apps each year
- **60%** of all web traffic worldwide is from mobile devices
- **71%** of employees leverage smartphones for work tasks

ZIMPERIUM.

Source: https://www.mobiloud.com/blog/mobile-apps-vs-mobile-websites

Mobile is eating the world...

Desktop vs Mobile vs Tablet market share



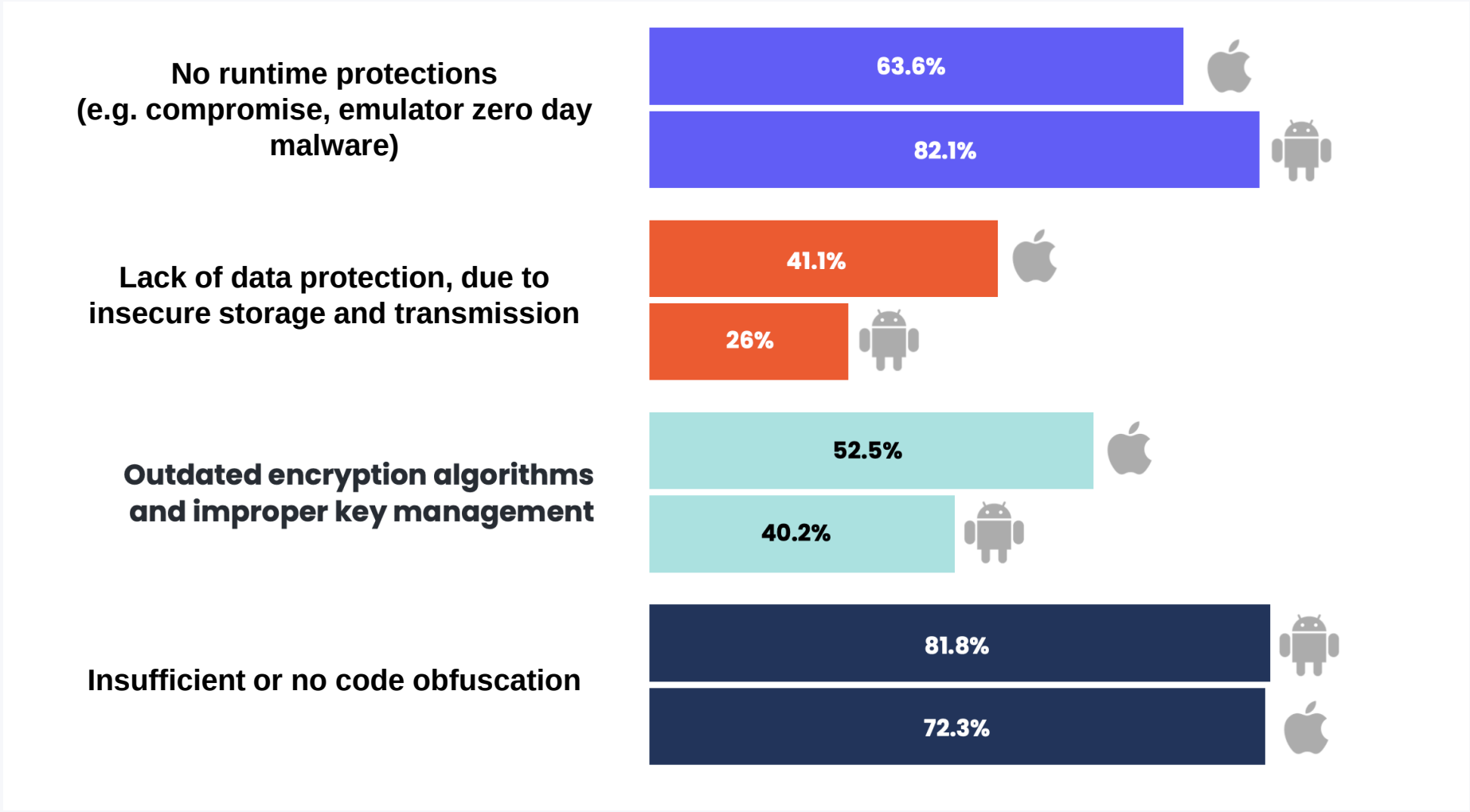
How Secure are today's Mobile Apps?

Why is mobile such an easy target?

- Lack of Security on Mobile Devices & Mobile Apps
- Advanced attacker tools are readily available
- Lack of Industry regulation specific to mobile Apps
- Security patches are not applied, missing or delayed
- Lack of Knowledge or low priority for many Businesses
- Sideloading Apps from 3rd Party App Stores

ZIMPERIUM.

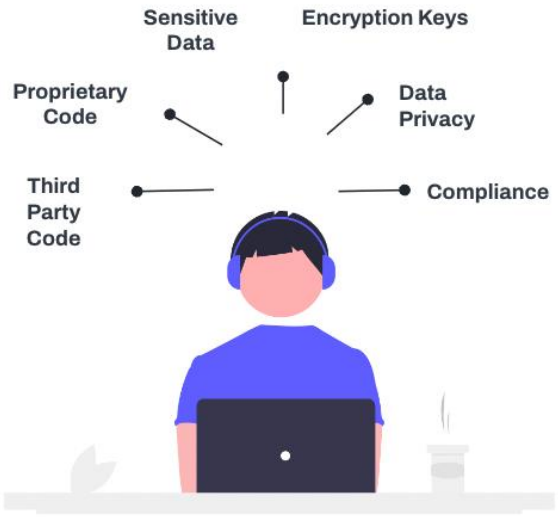
We did our homework, a few million times...
Focusing on apps that contain corporate data



Where exactly are the risks?

During development

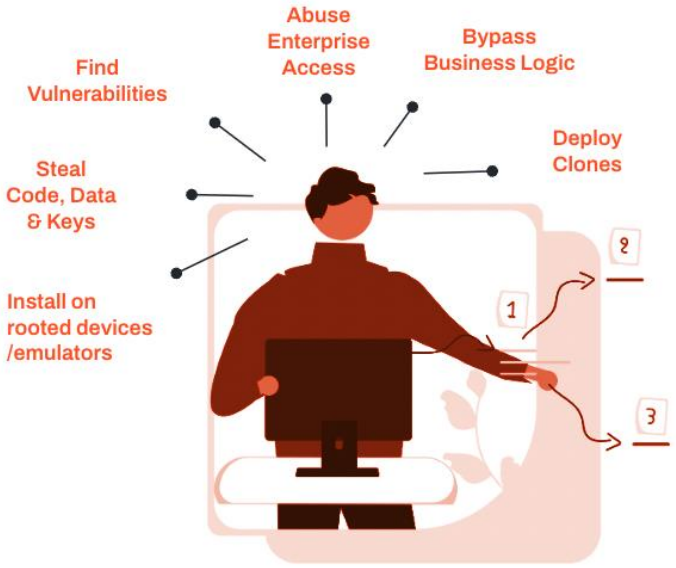
Enterprises building multi-functional apps



Supply chain risk. Third party SDKs.

Once published to stores

Attackers trying to reverse engineer the app



IP Theft.

Repackage Apps. Bypass paywall.

On an end-user's device

Attackers deploying on-device attacks via various vectors

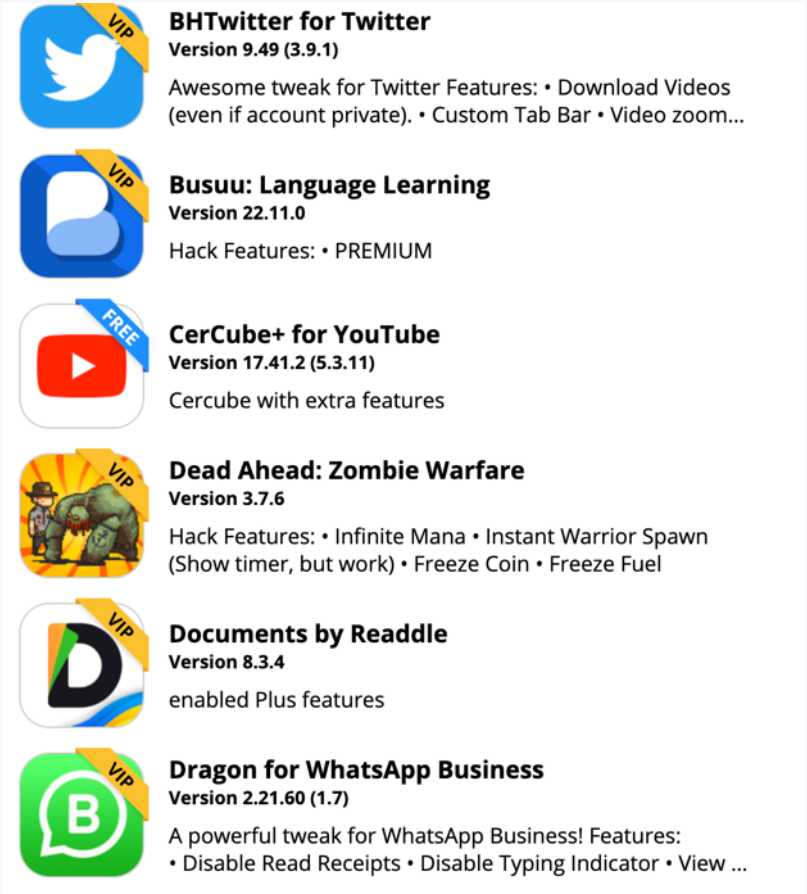
Theft of credentials. Financial fraud.

ZIMPERIUM.

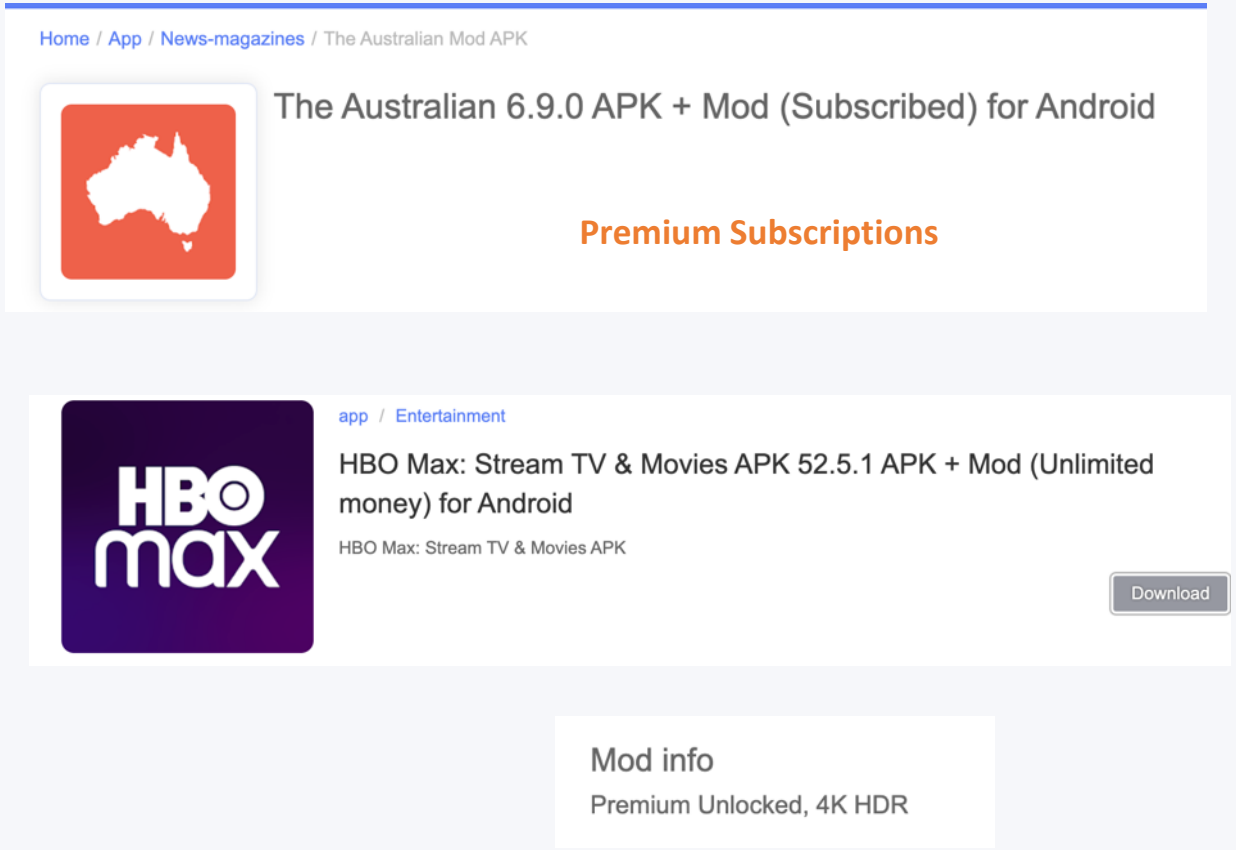
So what, who cares?

This can happen to your app!

iOS



Android



ZIMPERIUM.

And it’s happening to mobile banking apps too!

Queensland woman loses $57k in phone hack scam

An Aussie woman has issued a warning after a scammer stole her life savings through what appears to be no fault of her own.

Staff writers

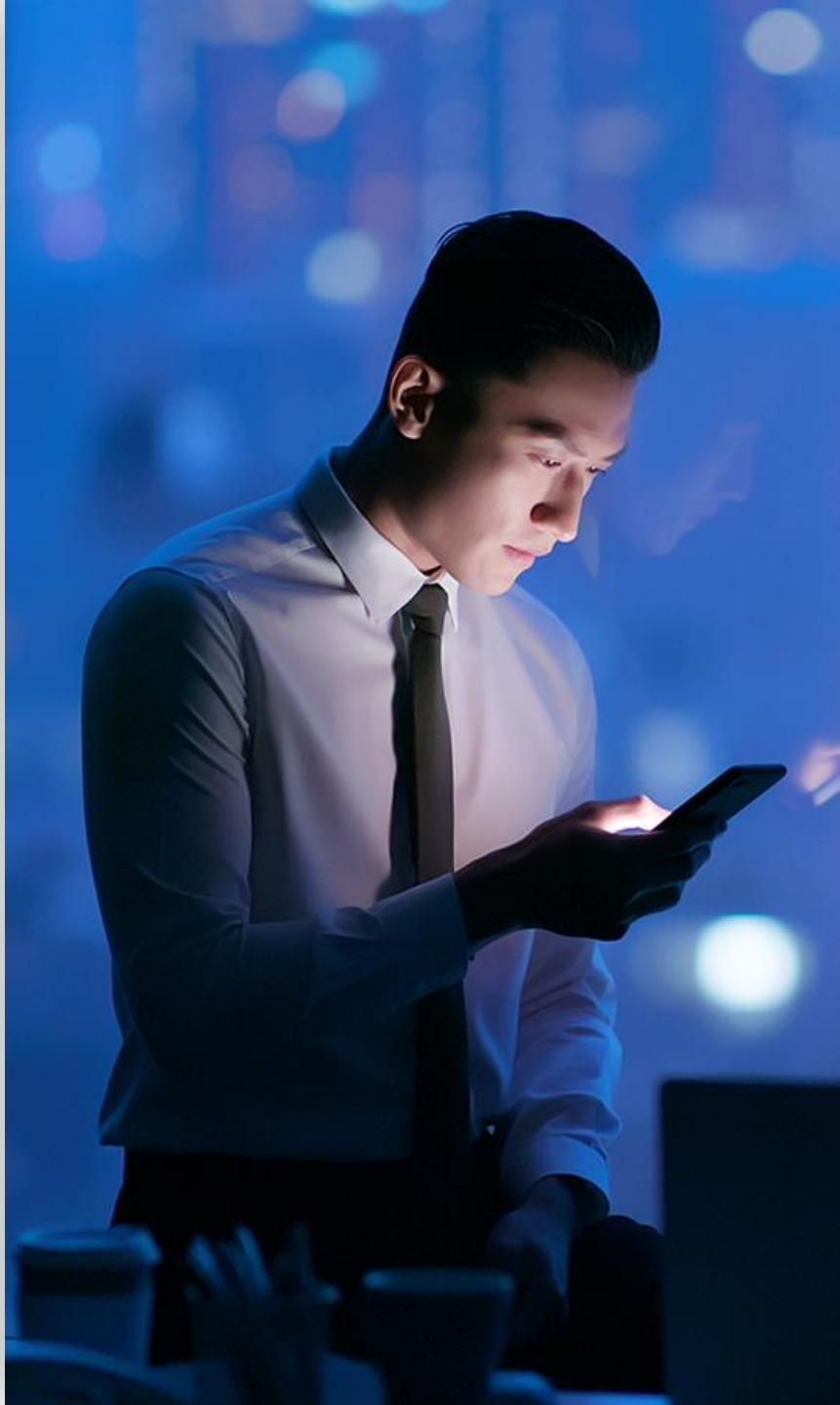
2 min read August 28, 2024 - 3:47PM news.com.au

An Aussie woman has issued a warning after a scammer stole her life savings through what appears to be no fault of her own.

Deslie Harvey, a 79-year-old grandmother from Queensland, recounted her horror at sitting in hospital with her sick husband when, in the space of less than 30 minutes, she watched on as her bank account was wiped clean.

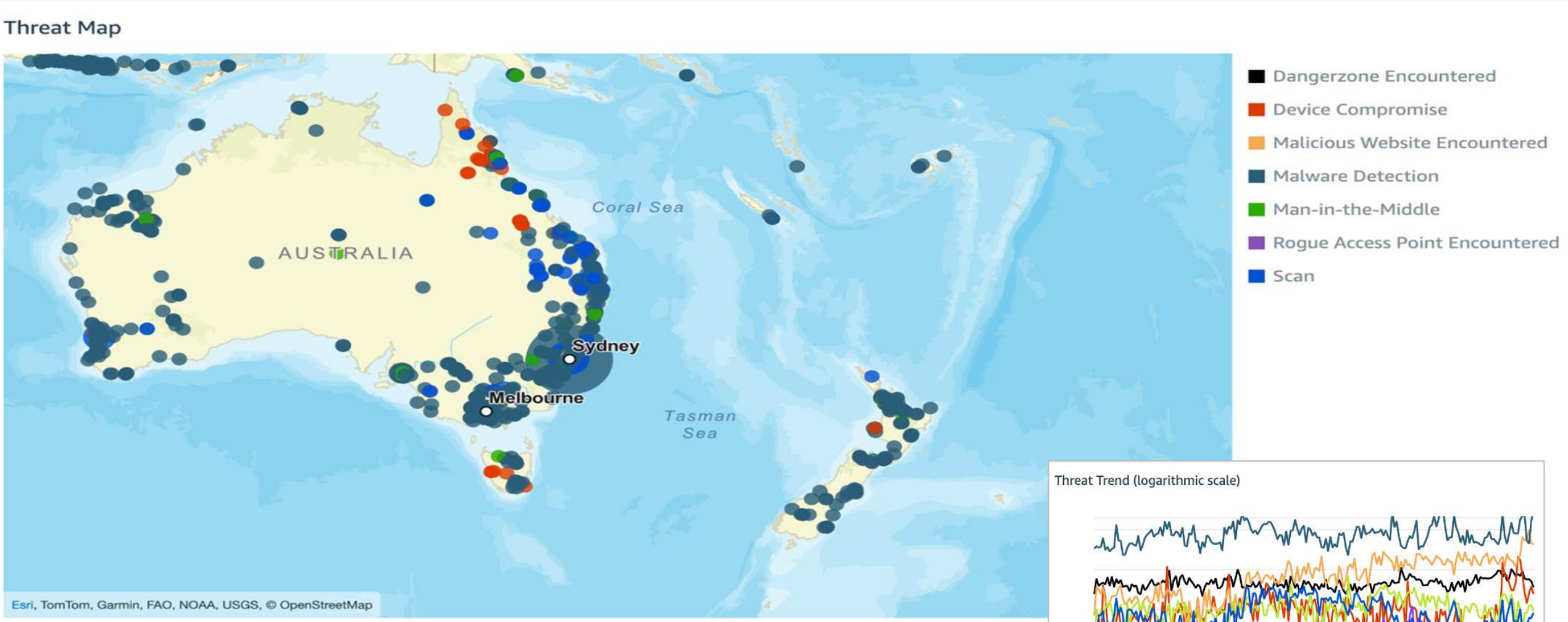
A hacker had somehow gained control of her phone remotely and successfully put through seven transactions.

They were able to bypass security measures when an authorisation code was sent to her mobile – as they already had access.



ZIMPERIUM.

The threats facing your Mobile Apps and users



ZIMPERIUM.

A better approach

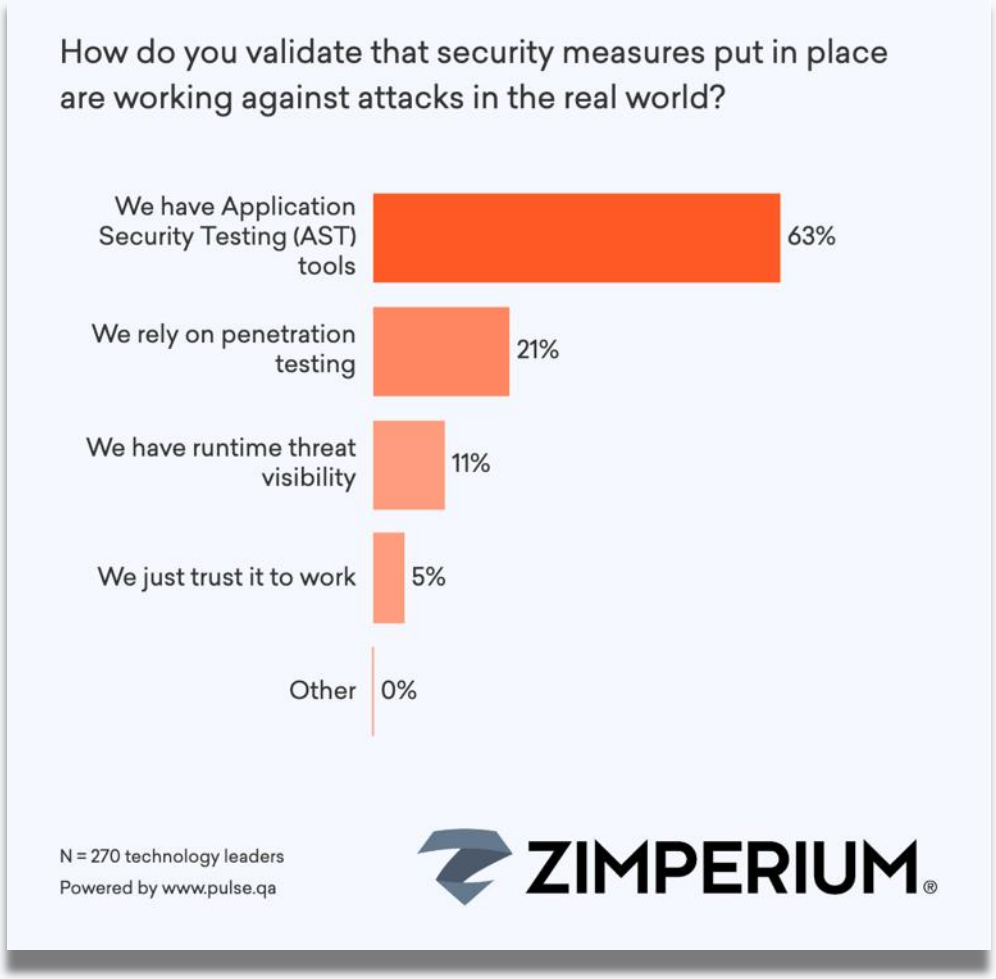
Mobile Application Security Testing (MAST)

- Do you test your app binary before releasing to production, in addition to testing the source code?
- Do you rely on Pen Testing at the end of the development cycle before go live?

SAST, SCA

Pen Testing

Binary analysis
(while cooking)



What does a MAST scan look for?

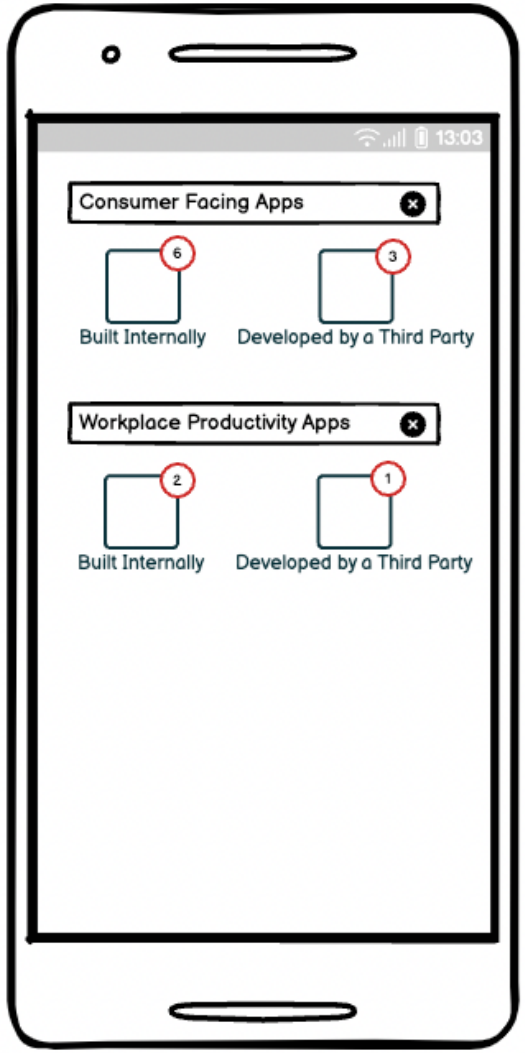
Is there sufficient protection against reversing, tampering with, and repackaging malware?

Can the app protect itself from attacks on the end-user's device?

Is the app exposing sensitive functionality and data when using the underlying platform capabilities?

Have third-party components the mobile app uses, such as libraries and frameworks, checked for known vulnerabilities?

Is sensitive data being leaked on compromised devices & networks?



Is sensitive data being exposed to other apps or leaked to cloud storage, backups, or the keyboard cache?

Are you using proven cryptographic schemes, and will it be sufficient when the attacker controls the devices?

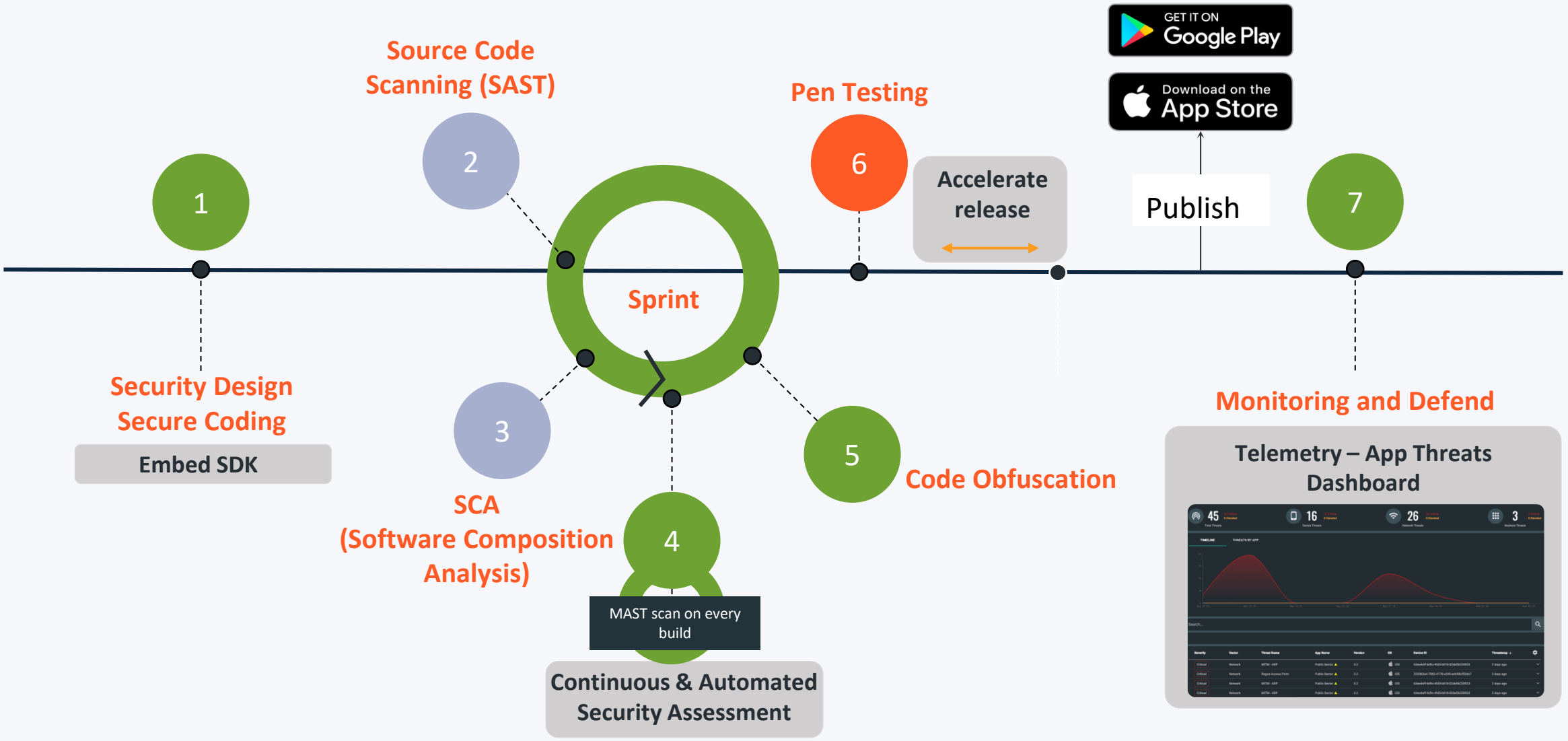
Are you handling authentication securely when giving access to remote services via the app?

Are you ensuring the confidentiality and integrity of information exchanged between the mobile app and remote endpoints?

Does the app comply with industry best practices and regulatory requirements? (MASVS ; OWASP ; PCI ; NIAP ; GDPR ; HIPAA)

ZIMPERIUM.

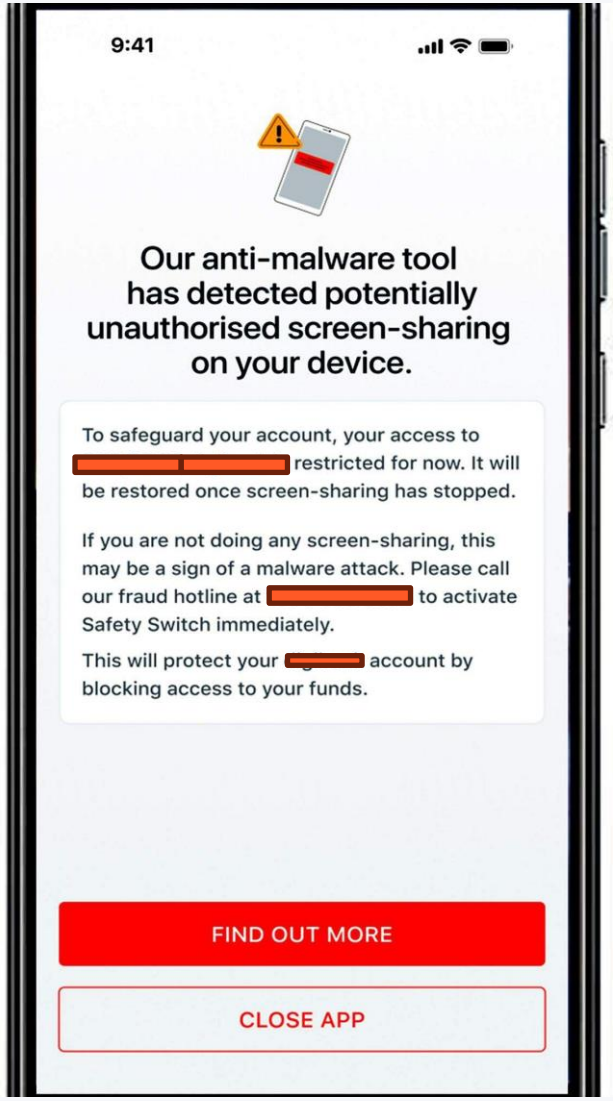
Mobile DevOps Workflow



ZIMPERIUM.

Wouldn’t this be better?

Mobile AppSec in action



ZIMPERIUM.

Key Takeaways

1. **Mobile Apps are exposed to different threats when compared to Web Apps. So you need to take a different approach to Secure DevOps.**

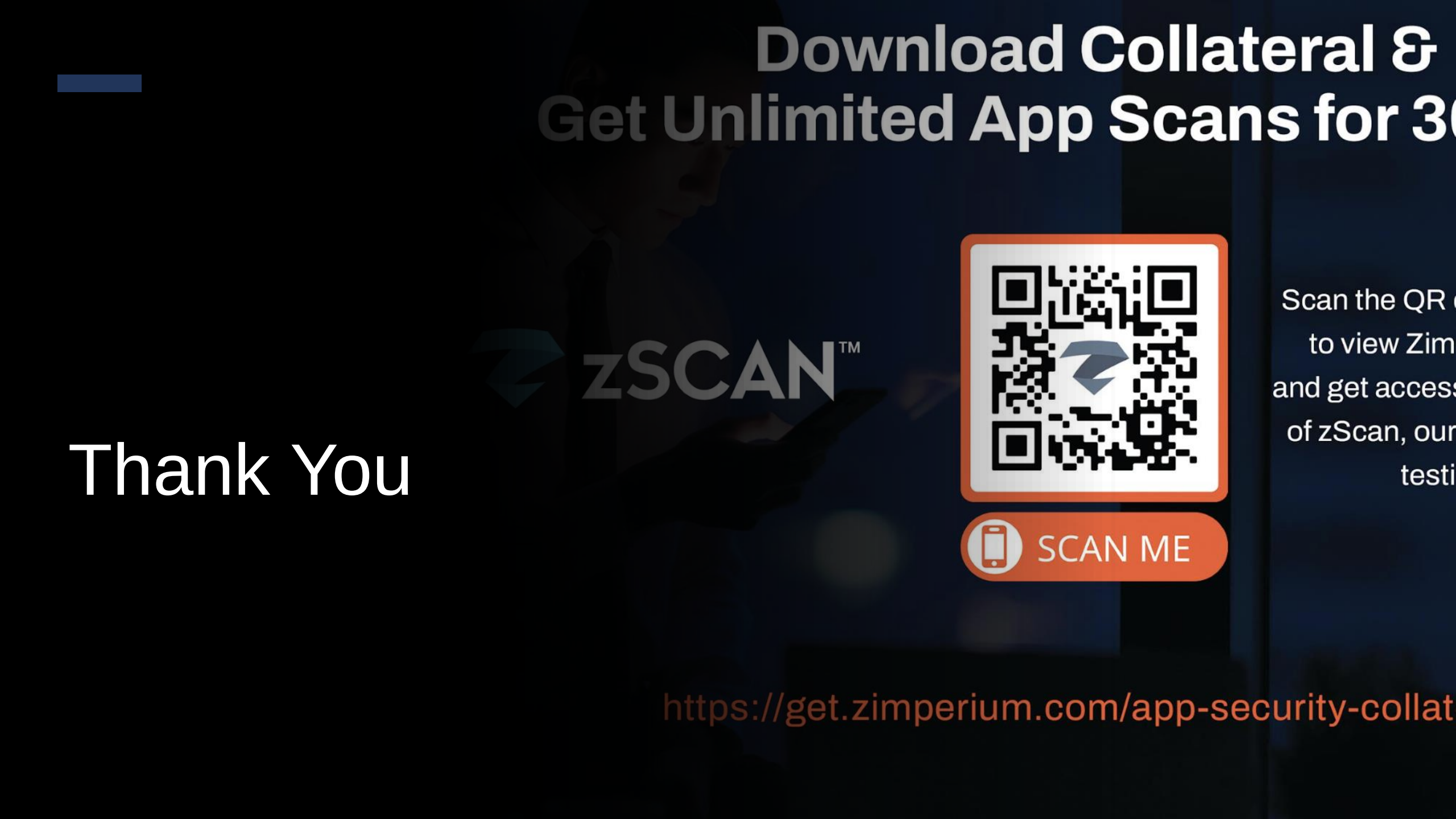
2. **Consider MAST for mobile Apps, to bridge the gap between source code testing and pen testing.**

3. **Have a plan for protecting your mobile App when it's "out there in the wild".**

ZIMPERIUM.

Source: Zimperium 2024 Global Mobile Threat Report

Thank You


Download Collateral &
Get Unlimited App Scans for 3
zSCAN™
SCAN ME
Scan the QR
to view Zim
and get access
of zScan, our
testi
https://get.zimperium.com/app-security-collat