

# Sahdow "Apps"

Chema Alonso

Twitter: @chemaalonso

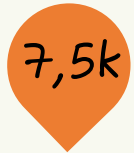


# Rising threats in Mobile Channels



84%

Organizations promoting mobile channels



7,5k

Number of mobile applications published every day



37%

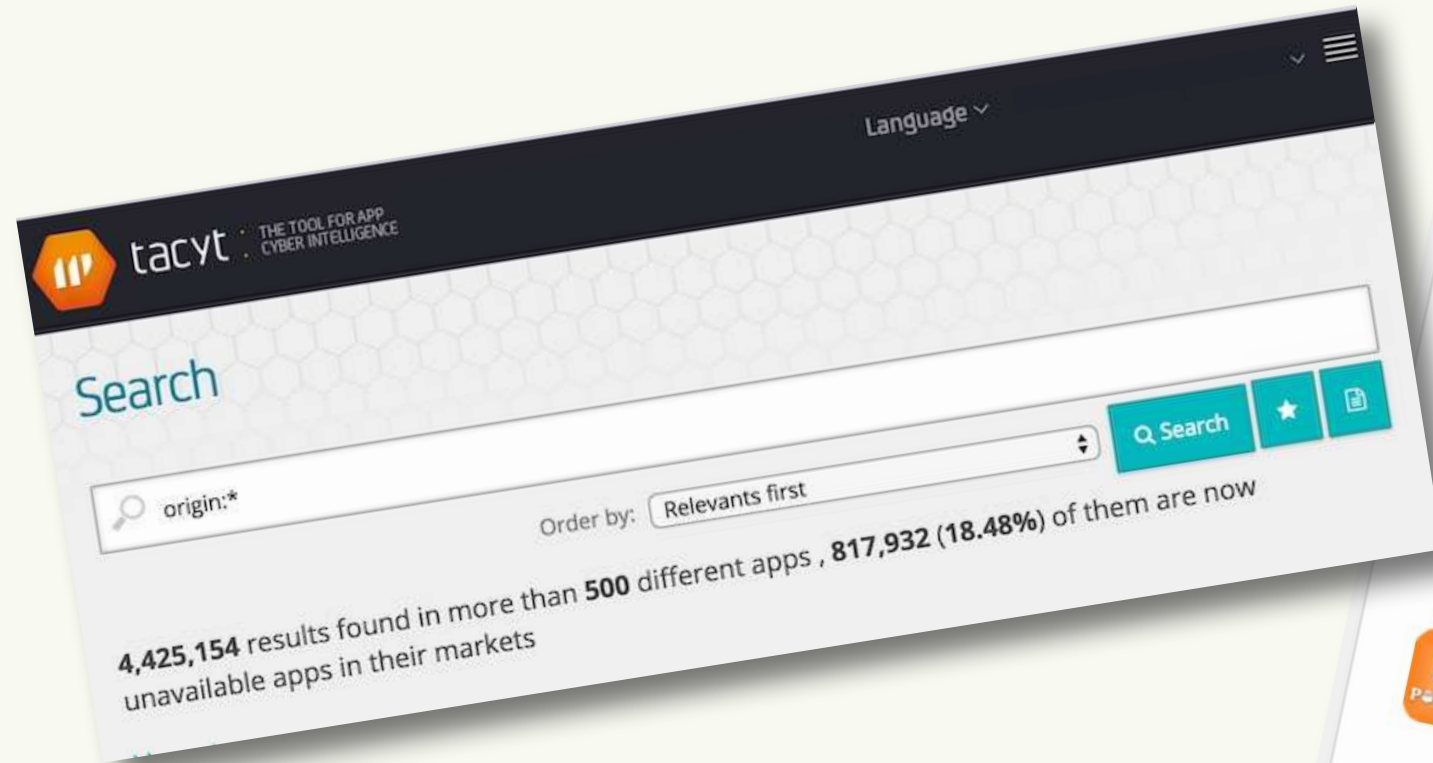
Apps with two or more OWASP Top 10 Mobile Risks



# OWASP TOP 10 Mobility Risks



# Path 5 (Tacyt)



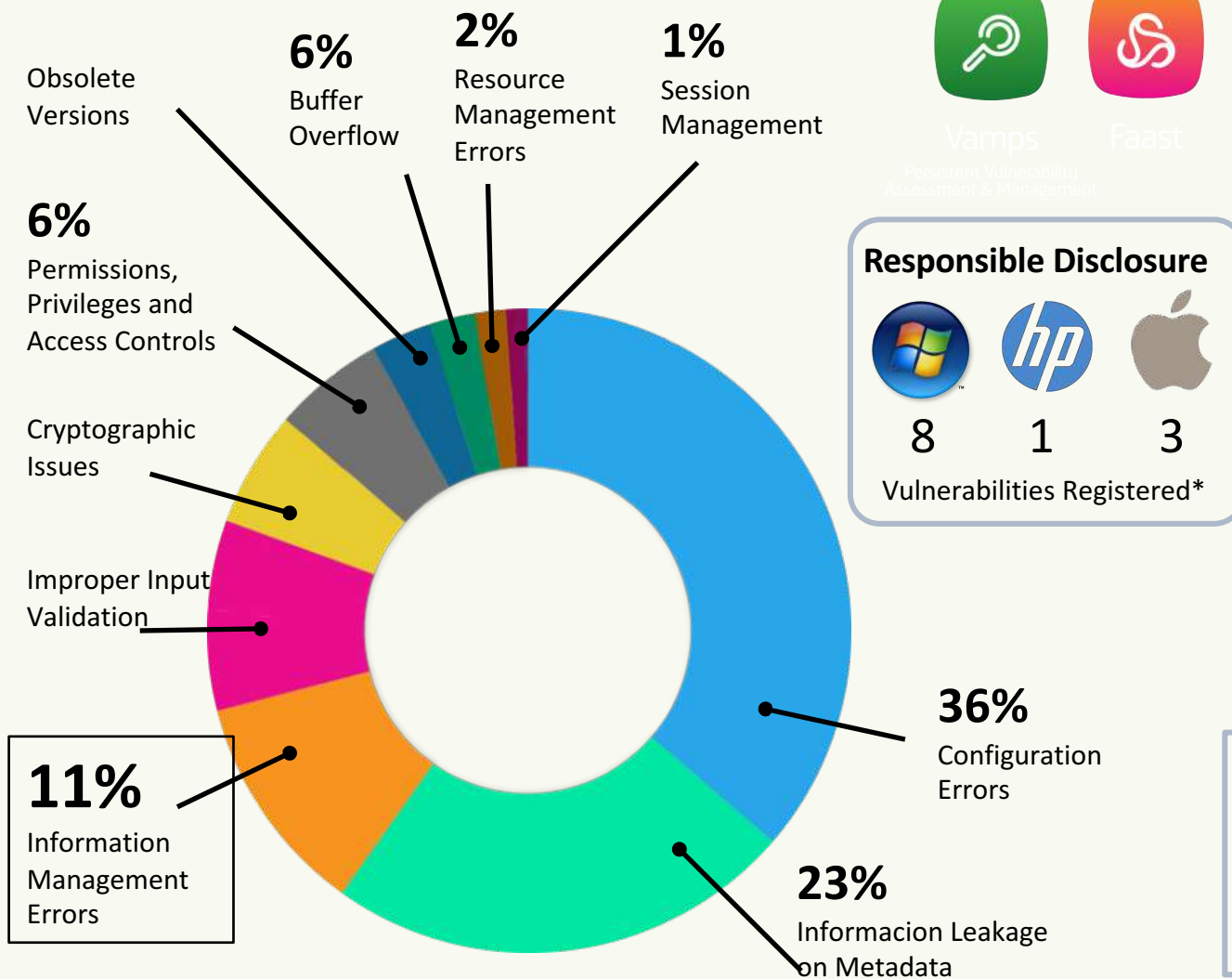
# How an App should be developed

## Secure Development





# Vulnerability Insights\_



**23%** related to Metadata Information Leakage

**11%** related to Incorrect Information Management

**Lack of care** in the management of information which is accessible via the Internet

**82%** related to incorrect systems and apps configuration

Most of the errors can be attributed to **poor practices by system administrators**

\* August 2016



# Faast: Pentesting Persistence

## Results

Summary

Assets Map

Vulnerabilities

Metadata

Network services

Software

IP addresses

IoT

Creation date

07 July · 02:45

about a month ago

Launch date

07 July · 02:45

about a month ago

End date

Not finished

Creation time zone

UTC

Scan evolution

2588032 / 5219523 potential tasks

In process

EDIT

RELAUNCH

Domain

Creator

chema

Workers

20

Mode

Continuous

Automatically include new plugins when they are available

Yes

Day of the week

Mon Tue Wed Thu Fri Sat Sun

Vulnerabilities

12501

Users

12

Network services

3540

IP addresses

2254

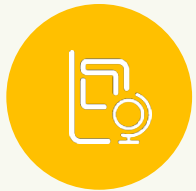


# Are my Apps affected? Certainly YES



**Are you aware of the development of ANY App of your organization?**

It's not possible to manage what you don't know that exists: App for special events or offers, external developments, multiple brands, multiple companies.



**Did you know when ANY App are published?**

Could be multiple developer accounts, Unofficial markets, lack of unpublish.



**How about your QA & Security acceptance test of ANY App?**

Lack of Budget, Lack of expertises, need to release version, risk assumption.



**Do you track ANY detected issues?**

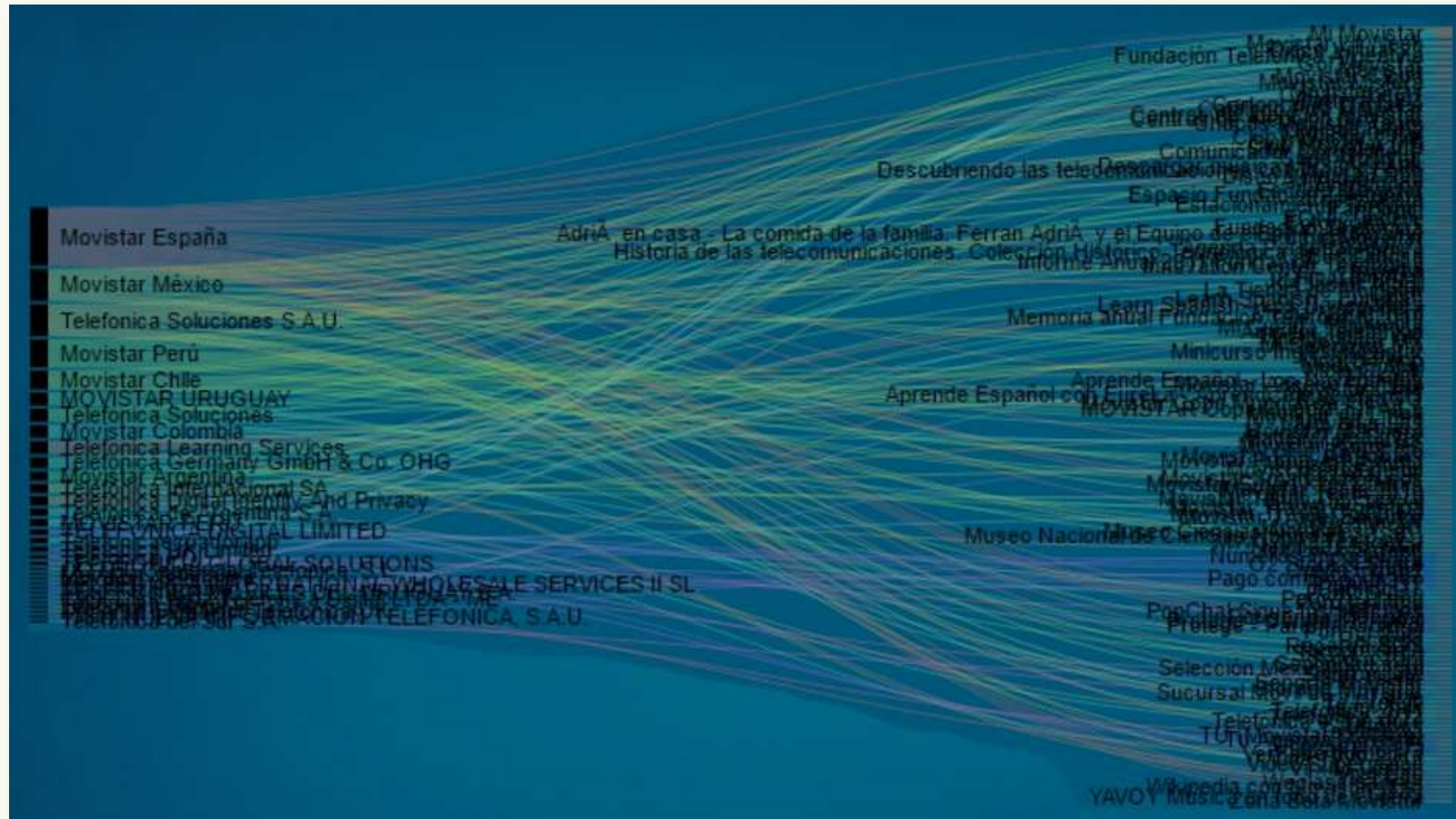
Need of specialized tools which requires expertise: App Discovery, App Analysis, ...








*And the result is...*








## Analysis Platform for Mobile Applications

-  **Handle Shadow Apps**  
Detect vulnerabilities in Mobile Apps even in those you don't know that exist.
-  **Continuous in-depth Analysis**  
Perform fast static & dynamic analysis and backend penetration testing.
-  **Track detected issues**  
Allow manage detected vulnerabilities along time and versions.





Let's play around. Path 6 DEMO

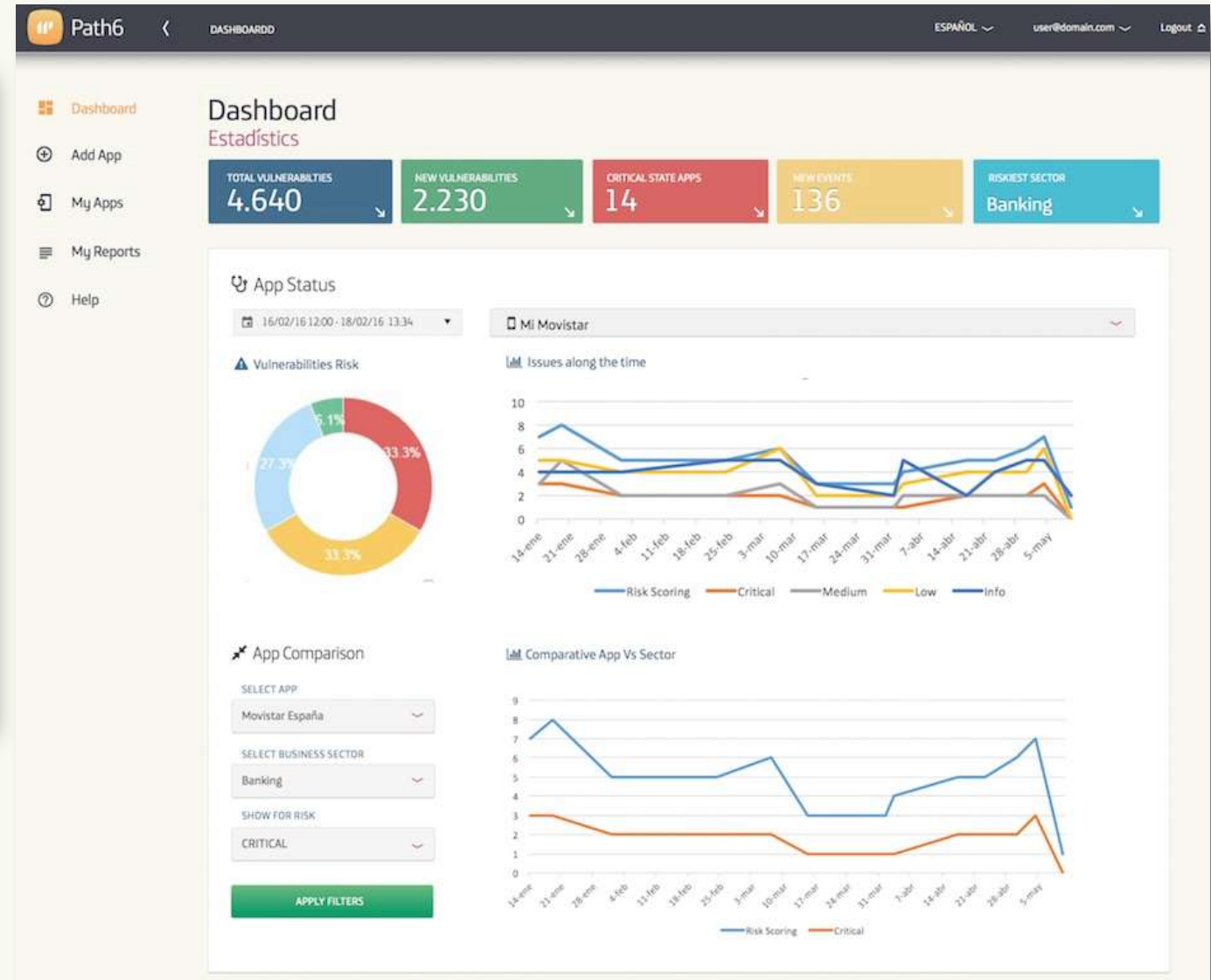
 Path6 Language ▾

## Login to your account

☐ Remember me  
 [Forgot your password?](#)

 **Latch** : PROTECTED ✓  
Is your account protected with Latch?  
[Click here to find out how to do it.](#)

 ElevenPaths 2016 © Telefonía Digital España S.L.U. All rights reserved. Telefonía CYBER SECURITY UNIT





# Shadow Apps & Approved Apps

- If You Can't Measure It, You Can't Manage It
- What's the policy to configure your MDM?
- How evolve security in old approved apps?





# Questions?

- Chema Alonso
- <https://twitter.com/chemaalonso>
- <http://www.elladodelmal.com>
- <https://www.elevenpaths.com>

