Mobile Channel Risks

Regain control of your Mobile Channel

Gone are the times when apps were an area limited specifically to promotional offers and games. Now, mobile apps are a key tool within organizations' channel strategies to maintain contact with their clients.

Unfortunately, this tendency has given way to the apparition of critical vulnerabilities in the companies' official apps. Threats to users are exponentially evolving through apps developed by malicious actors, representing a risk to the security and privacy of users and organisations.

Mobile Channel Risks offers a complete view of the risks in your mobile channel, identifying vulnerabilities in your apps and detecting mobile threats against your company.

Complete control

Autonomous discovery of the entire pool of apps belonging to the company, giving a complete account of their evolution and status.

Continuous analysis

Continuous security analysis of the organisation's official apps to detect vulnerabilities and help to fight them.

Proactive detection

Ongoing monitoring of official and unofficial markets, detecting third-party apps that aim to impersonate the company.

Analysis & Response

Threat contextualization and proactive withdrawal of suspicious third-party apps from markets.

Benefits

- Centralised view of the security status of your mobile apps, facilitating the identification, management and correction of any vulnerabilities or security risks.
- Complete control of your mobile channel through an autonomous discovery system that allows you to have an updated view of your entire pool of apps.
- Visibility and anticipation against mobile threats aimed at users of your organisation, gaining insights into the campaigns, techniques and actors involved.
- Outsource the withdrawal of suspicious and/or malicious apps from mobile markets (official and unofficial) that are harbouring them.

Target audience

- Entities that use mobile channels to communicate with their clients and employees, and that need to regularly know the security risks related to their apps.
- Organizations with a digital presence that need to obtain a comprehensive view of mobile threats (brand imitation, fraud, mobile malware, etc.) against their companies.
- Entities that implement MDM systems to manage their mobile devices and that need to regularly monitor the security level of apps installed by their employees

Mobile Channel Risks

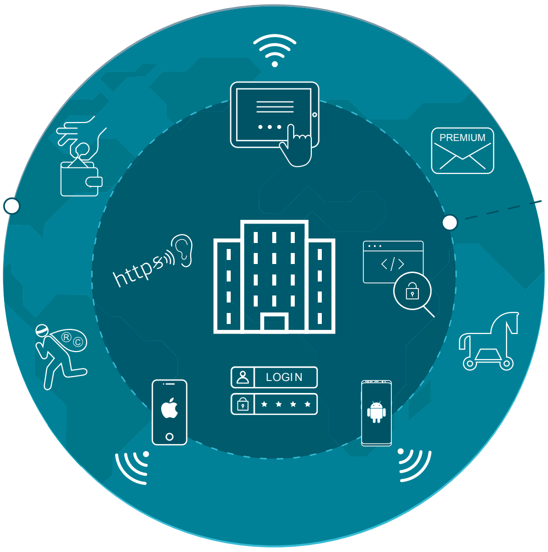
Risks covered under our offer

Our services offer full coverage against risks in the mobile channel, that is "Risks Inside" (arising from vulnerabilities in the organization's official apps) and "Risks Outside" (from suspicious third-party apps targeting the company's users).

Risks Outside

(Suspicious Third-Party Apps)

- Brand spoofing
- Counterfeiting & tampering
- Spyware & intrusive adware
- Mobile malware



Risks Inside

(Official Customer App)

- Information leakages
- Critical vulnerabilities
- Lack of vision & control
- Vulnerable services & libraries

Technology used

Get to know the proprietary technologies used by the Mobile Channel Risks service:

mASAPP

A technology designed to help organisations proactively discover and analyse their mobile apps, making it possible to continuously identify new vulnerabilities in their apps.

Tacyt

A cyber-intelligence tool that monitors, analyses and correlates main markets for mobile apps, thereby facilitating the process of detecting and investigating mobile threats and reducing their impact on organisations.

Technical features

- **Continuous, in-depth analysis:** Uninterrupted analysis to identify vulnerabilities stemming from attributes, libraries or services, based on a complete set of security tests encompassing static analysis, dynamic runtime analysis, evaluation of third-party frameworks and back-end services.
- **Actionable information:** The results of the analysis are presented as structured information on the vulnerabilities that were identified (description, related impact, detailed evidence and path of the vulnerable attribute, etc.), in addition to a series of recommendations to remediate those vulnerabilities.
- **Autonomous discovery:** Proprietary system capable of automatically inferring new search rules based on settings from configured apps. The organisation's apps and versions that are published in different markets are thus autonomously discovered.
- **Mobile threat detection system** based on patterns (contextual, technical, circumstantial, etc.) and supported by our big data applications (> 9M apps) and a powerful metadata correlation engine.