Tacyt

The tool for
app cyber intelligence

Monitoring and analysis of mobile threats

Tacyt is an innovative cyberintelligence tool that provides professionals and security experts with big data technology to investigate mobile app environments.

Security threats within the mobile world are growing incessantly: specific attacks, aggressive adware, fake applications performing like genuine applications only to steal information and consume services on a second level, etc. These threats continue actively available on the markets long enough to affect thousands of users.

Tacyt enables the quick detection, discovery and analysis of these threats to reduce their potential impact on organizations.

Tacyt monitors, stores, analyzes, correlates and classifies millions of mobile apps while adding thousands of new apps every day

Innovation
New tool at the service of security analysts and experts.

Intelligence
Patented technology for correlation and applicable intelligence.

Freshness
(New apps quick catching) in different Android and iOS app markets.

Global vision
Evaluation of the application and its circumstances: when, who, what and where.

Versatility
Versatile and high-performance tool that can be accessed by companies and experts

Benefits

- Access to all the information associated with an application: metadata, permissions, developer, files, accessed urls, etc.
- Query, comparison and linking of applications that share any datum indexed on the platform.
- Detection and prevention of fraud against clients or employees (malware, adware, credential theft, breach of policies, etc.).
- Detection of threats against a company trademark.
- Identification of suspected patterns such as: developers with a record of fraud, applications that share certificates, etc.
- Identification of the operating method to determine who is behind the app, other associated campaigns and applications, to ascertain their full history and anticipate upcoming attacks.

Target group

Tacyt has been created for companies who:

- Want to reduce their risk against app-related threats.
- Seek to proactively monitor the emergence of "fake" apps.
- Offer security and cyberintelligence services.
- Are security researchers and analysts.
- Are managed security service providers (MSSP).
- Are law enforcement agencies (LEA).

Tacyt

Mobile cyberintelligence ecosystem

Tacyt provides a full range of features for improving the analysis and research to provide a solution to any fraudulent action in which some mobile component could have been used. Tacyt lets analysts track the activities of these mobile component developers and anticipate other possible actions that they have done.

Tacyt has also been designed for establishing alerts that detect activities of developers with malicious intentions, thereby turning them into a comprehensive solution for security, legal or marketing teams, or for mobile app trend analysts.

Technical features

Powerful cross-market and cross-platform search engine (Android and iOS) that allows to analyze and filter on the basis of different parameters: dates, size, images, relationships between apps, circumstantial data, developers, digital certificates, etc.

Filters that are easily created, with real-time and shareable alerts. Backed by different correlation methodologies for classifying information and simplifying research and analysis.

Immediate update of the applications and their circumstances as they change on the markets. Possibility to subscribe to official, public and advanced filters that are constantly upgraded.

Its API enables programmatic interaction with the information and communication with other software. The external APK analysis can be automated for integration with any other tool.

Tacyt can be acquired as a stand-alone product or as a CyberThreats service module, fully managed and operated by Telefónica

Tacyt

Providing with a quick detection, uncovering and analysis of mobile threats. *Stand-alone* access to the tool through:

- Comprehensive Web console focused on analyst and infosec professionals.
- API, enabling programmatic interaction with the information and communication with other software.

CyberThreats

Providing with ongoing monitoring, detection and answer to posible mobile threats under three models:

- Model 1: Apps analysis.
- Model 2: Detection & app analysis.
- Model 3: Detection, app analysis & reaction (take down).

If you want to be a part of our Value Added Partners ecosystem (VAP), please contact us.