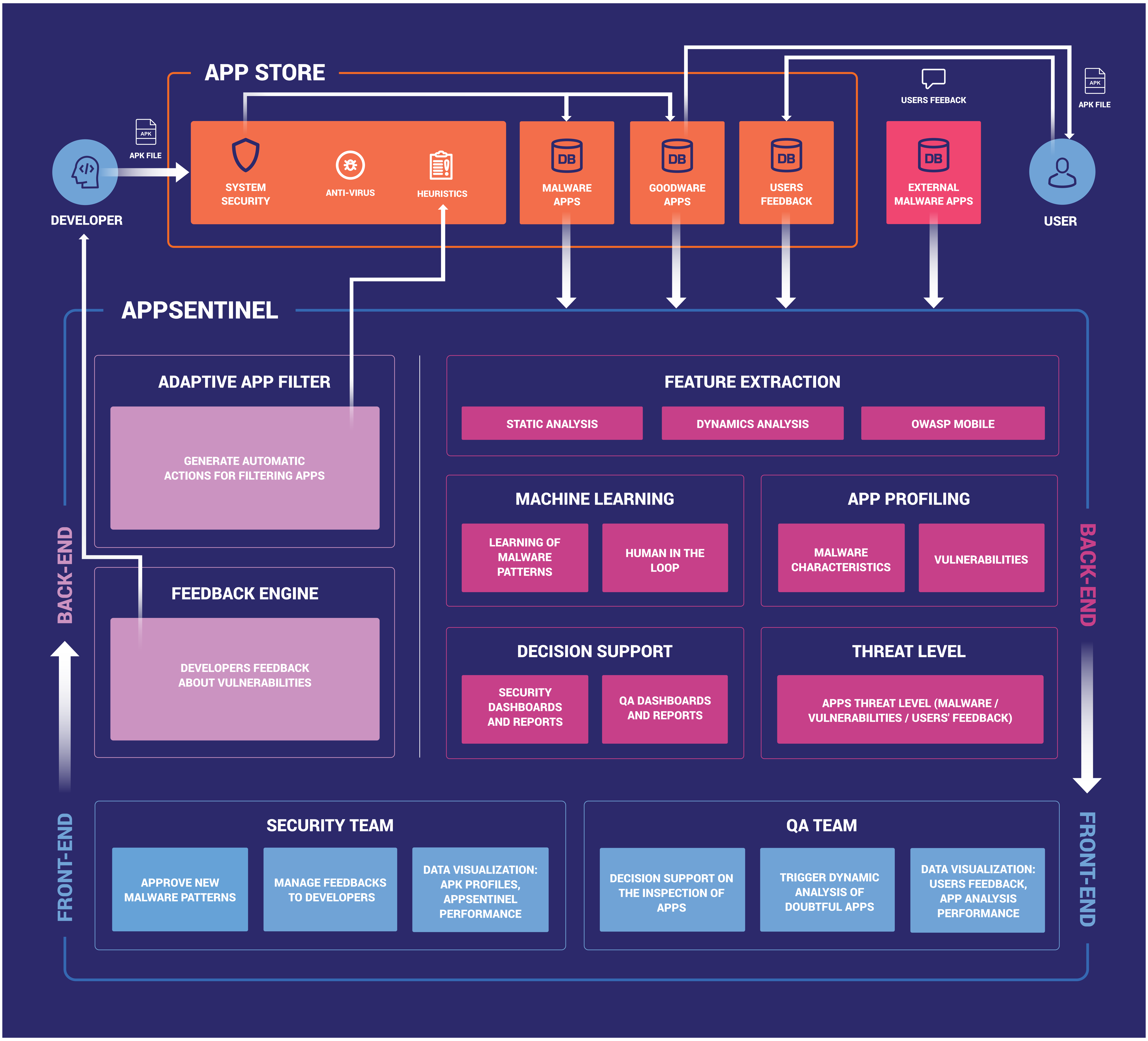
AppSentinel

Intelligent Cloud Based Anti-Malware Technology for Android App Stores

The penetration of mobile devices in people lives is such that in 2016 alone occurred 149.3 billion app downloads, number that is expected to more than double by 2020. This growth is accompanied by an unprecedent increase in malware applications submitted to app stores. In 150 000 apps tested by MacAfee on users' devices in 2016, 37 000 were malware. Moreover, in this context of a high level of threats to app consumers, the lack of good app development practices leads to vulnerabilities that can be exploit by malware practitioners to gain access to private and confidential data.

Aptoide, being a marketplace between app developers and users, is well positioned to face these problems, as it is the first entity to receive new apps. Therefore, it has the possibility of discovering new threats faster than other players (like antivirus companies) and act before it affects a large number of users. To take advantage of such position, Aptoide and ISCTE-IUL are researching and developing an intelligent cloud based anti-malware technology for Android app stores: AppSentinel.

AppSentinel will be integrated in the already existing security system of Aptoide. When a new app enters in the marketplace it is also sent to the AppSentinel module, where static and dynamic analysis are used to obtain the app characteristics, which feed machine learning algorithms. Those algorithms, trained with considerable and updated internal (from Aptoide) and external datasets of malware and goodware, have the goal of inferring new malware patterns. Furthermore, the static and dynamic analysis will also support the understanding of the app vulnerabilities, based on OSWAP mobile rules. Using the malware patterns and the app vulnerabilities, the system will create the profile of each app related to these 2 vectors. Joining users' feedback to the app profiles, will be determined the threat level for each app. The system is thought to support 2 teams: security and quality assurance (QA). The security team will analyse and approve new malware patterns and manage feedbacks to developers about their apps' vulnerabilities. The QA team will have an optimized support on the inspection of apps with results of static and dynamic analysis. New malware patterns detected by AppSentinel and approved by the human operators will enter in the app store heuristics tool in order to automatically filter apps that show those malicious behaviours.


APP STORE
APK FILE
DEVELOPER
SYSTEM SECURITY
ANTI-VIRUS
HEURISTICS
DB
MALWARE APPS
DB
GOODWARE APPS
DB
USERS FEEDBACK
USERS FEEBACK
DB
EXTERNAL MALWARE APPS
APK FILE
USER
APPSENTINEL
ADAPTIVE APP FILTER
GENERATE AUTOMATIC ACTIONS FOR FILTERING APPS
FEEDBACK ENGINE
DEVELOPERS FEEDBACK ABOUT VULNERABILITIES
FEATURE EXTRACTION
STATIC ANALYSIS
DYNAMICS ANALYSIS
OWASP MOBILE
MACHINE LEARNING
LEARNING OF MALWARE PATTERNS
HUMAN IN THE LOOP
APP PROFILING
MALWARE CHARACTERISTICS
VULNERABILITIES
DECISION SUPPORT
SECURITY DASHBOARDS AND REPORTS
QA DASHBOARDS AND REPORTS
THREAT LEVEL
APPS THREAT LEVEL (MALWARE / VULNERABILITIES / USERS' FEEDBACK)
BACK-END
BACK-END
FRONT-END
FRONT-END
SECURITY TEAM
APPROVE NEW MALWARE PATTERNS
MANAGE FEEDBACKS TO DEVELOPERS
DATA VISUALIZATION: APK PROFILES, APPSENTINEL PERFORMANCE
QA TEAM
DECISION SUPPORT ON THE INSPECTION OF APPS
TRIGGER DYNAMIC ANALYSIS OF DOUBTFUL APPS
DATA VISUALIZATION: USERS FEEDBACK, APP ANALYSIS PERFORMANCE

Aptoide
Your Android App Store

ISCTE IUL
Instituto Universitário de Lisboa

Lisb@20 20

PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Social Europeu