AppScreener is next-generation software for application security testing. AppScreener's convenient interface requires just a couple of clicks, since all the intricate variability of algorithms and settings is automated as much as possible.

If the source code is available, the scanner easily integrates with software repositories. Otherwise, a working copy of the program can be simply uploaded to AppScreener. Mobile software can to be tested by merely copying a link the app in Google Play or Apple Store into the AppScreener menu.

AppScreener provides detailed recommendations and instructions on addressing any vulnerabilities by either (1) amending the source code or (2) using remedies available in SIEM, WAF and Firewall systems.

STATIC CODE ANALYSIS

01
0110
0001
0110 1

AppScreener
Software Security assessment in plain language

AppScreener

APPSCREENER – THE FIRST SOLUTION THAT BLENDS A SCIENTIFIC APPROACH TO DECOMPILATION WITH CODE ANALYSIS TECHNOLOGIES

Product users:

Data Security Departments

Software Developers

Quality Control Departments

6
ADVANTAGES OF APPSCREENER

▎ No need for source code to analyze applications

▎ Test results are generated in the format of specific recommendations on addressing vulnerabilities

▎ Detailed instructions are produced on setup procedures for SIEM, WAF, FW and NGFW security systems`

▎ Several code analysis technologies are employed to detect a greater number of vulnerabilities

▎ A user-friendly interface that enables scanning by just two mouse clicks

▎ The product seamlessly integrates with the process of secure software development

PROBLEMS ADDRESSED BY APPSCREENER

▎ Web and mobile applications are available to external users; the IS department, while having no control over their security, is still held responsible for incidents

▎ Lack of proper communication between the IS department and developers: the source code is not handed over to IS, or, at best, IS gets an archive that is almost impossible to sort out

▎ Web application code errors take too long to fix

▎ Data leaks owing to bugs intentionally built into the code by developers

▎ Lack of control over the security of applications used by the company
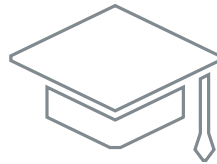
5
FACTS ABOUT APPSCREENER

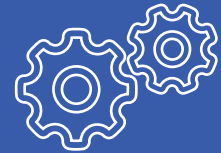**#1** First product that analyzes applications without the source code using the "white box" method

The fuzzy logic engine reduces the number of false positives

A local and a cloud version are available

The development team includes three PhDs specializing in code decompilation

Product based on four code testing technologies, particularly taint analysis

APPSCREENER IS AN INDISPENSABLE TOOL FOR ANY ORGANIZATION THAT

- Provides online services to external users
- Uses critical systems and applications developed in-house or by a third party
- Requires strict control over in-house or third-party development, particularly because source codes are not available

- Has the SDLC methodology in place, so data security officers play a role in code acceptance
- Needs to meet standards and regulations regarding software code analysis

APPSCREENER STRUCTURE

AppScreener consists of three functional elements:

▎ The analytical system

▎ The reporting system

▎ The Fuzzy Logic Engine to process false positives

This structure makes our product a fast and efficient application security-testing tool that requires no lengthy setup or training.

Repository

Source code
Java, Scala, Android,
iOS (Objective-C), PHP,
C#, C/C++, PL/SQL

Binary code
Java, Scala, Android,
iOS (Objective-C), PHP,
C#, C/C++

Download on the
App Store

Google play

Build module

Deobfuscator

Internal representation

Decompiler

Analyzer

Translation of vulnerabilities to the source code

Fuzzy Logic Engine

REPORTING

Recommendations on amending the code

Recommendations on network security systems setup

Bug tracking

wwpass

AppScreener