It's Never Too Late For Static Application Security Testing

SolaredAPPscreener provides a comprehensive approach to fighting vulnerabilities in your critical applications, mixed with a combo of industry-wide accepted practices as well as unique proprietary technologies.

Secure Software Development

Decrease the number of vulnerabilities and remediation time

Legacy Software Security Assessment

Find security breaches in legacy apps that are not actively developed.

Open Source Security

Verify security of open source components used in your software.

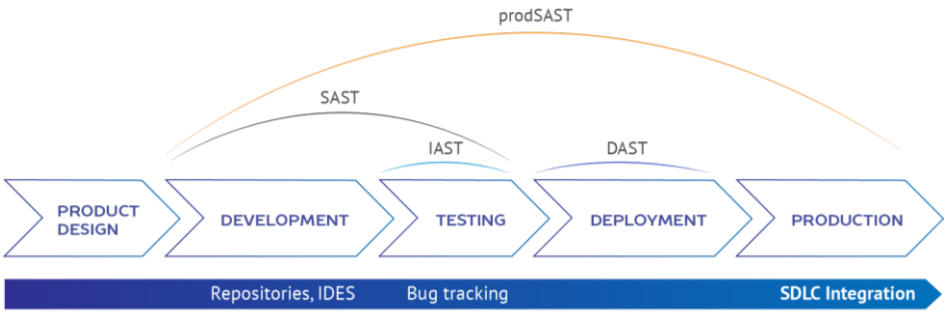
Commercial Software Security Assurance

Test purchased or custom-made applications for vulnerabilities or back doors*

SDLC integration = SAST adoption

To make full use of SAST, companies should consider deep integration with the existing software development environment. Even if the security assessment software supports all required programming languages, the necessity of adding a separate step for devs to run application security testing may be a burden.

SolaredAPPscreener seamlessly plugs into each stage of the software development lifecycle (SDLC), thus allowing your developers to easily run security scans and focus on building applications.



Solared APPscreener SDLC integration

Technology Armory of SolaredAPPscreener

Static Application Security Testing (SAST)

Catch and remediate potential vulnerabilities as early as possible while the testing process is integrated with the existing development life cycle.

Production SAST (prodSAST)

Run SAST even if development is completed. No matter whether you have the source code, binaries or executables, it's always a good time for prodSAST by SolaredAPPscreener.

Dynamic Application Security Testing (DAST)

Apply dynamic scanning to learn how vulnerable your applications are. The black-box approach is perfectly tailored to running application testing.

Interactive Application Security Testing (IAST)

Combine best practices of SAST and DAST approaches to get new vulnerability insights.

Mobile Application Security Testing (mAST)

Easily check that your mobile applications are secure.

* With the consent of the app owner

Production SAST

The DAST approach allows users to better address the security testing requirements of waterfall-oriented teams, with dynamic analysis commonly being applied once a runtime version of the software is available. At this stage, it is sometimes difficult, or even impossible, to obtain the source code from the development. Moreover, DAST scanning results can rarely provide the same level of vulnerability coverage as SAST. Therefore, black box testing is the only method available when your application is running.

But what if it is not?
SolaredAPPscreener makes it possible to use Static Analysis, even when development is completed. Using Production SAST allows binary and executable files to be assessed for vulnerabilities, with the unique technology reconstructing the original source code and mapping any detected vulnerabilities.

Secure Open Source Usage

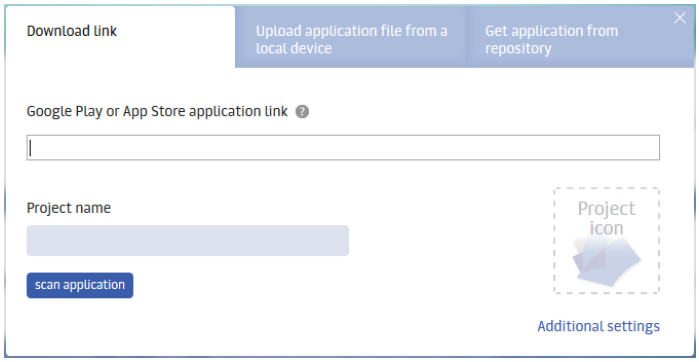
It is not surprising that developers often rely on open source components while developing commercial software. Indeed, one can find almost any functionality source code or ready to deploy library on popular online repositories. However, while this approach helps to save time and prevent the need to write code, it also puts application security at risk.

SAST can be of great value to run application security testing in the case that the source code is available. However, what if the developer had implemented a ready to use library as part of the project? How can you know whether it exposes your business to cyber-attacks?

SolaredAPPscreener Open Source Scan allows for the scanning of any formats of open-source components for vulnerabilities and back doors. No matter whether you have source code, binaries or executables, just upload them to SolaredAPPscreener and get a full report on potential risks associated with third party code usage within the applications you develop or purchase.

Mobile Application Security Testing

Running security testing for mobile apps has never been easier. All you have to do is paste an app link on GooglePlay or AppStore, with SolaredAPPscreener then obtaining the source code from the package and applying static analysis for full vulnerability coverage.



Mobile app import

With Compliance in Mind

SolaredAPPscreener is a great choice for companies seeking to support compliance with security standards, with users being able to easily generate scan reports formatted according to PCI DSS, OWASP or HIPAA vulnerability classification.

Polyglot Programming Compatible

SolaredAPPscreener easily detects coding language and has no problems understanding polyglot programs written in multiple languages. Just upload the source code and press Scan.

Current language support

Static Analysis

Java, Scala, PHP, Android, iOS, C#, PHP, PL/SQL, Python, Ruby, C/C++, VB 6.0, T/SQL

Binary Analysis

Android, iOS, jar, war, exe, dll

Contacts

Headquarters

Email: info@solaredsecurity.com
Adress: 3rd floor, Ulysses house,
Foley street, Dublin 1

USA
Sales: sales@solaredsecurity.com
Support: support@solaredsecurity.com
Phone: +1 (415) 848 2330
Adress: 795 Folsom Street, 1st Floor,
San Francisco, California, 94107