Solar appScreener

Search for vulnerabilities and undocumented features in source and binary codes

Secure apps for your customers

Pre-approved Grant available for Singapore SMEs

Mobile: +65 84311778 or +65 91370722
*E-Mail: bd@**athenadynamics.com***

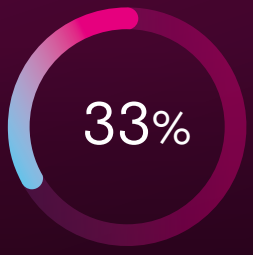
SG:D | SMEs GO DIGITAL
PRE-APPROVED

Rostelecom Solar | athena dynamics
A Member of BH GLOBAL CORPORATION LTD

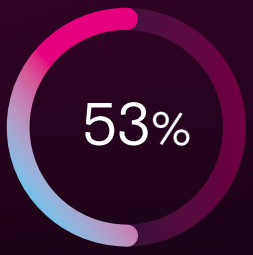
athenadynamics.com
solarappscreener.com

App security drives business security

of apps are vulnerable



of vulnerabilities are critical



of dangerous vulnerabilities can be exploited remotely

of successful attacks exploit code flaws

Solar appScreener is a static application security testing (SAST) tool capable of detecting vulnerabilities and undocumented features, including hardcoded passwords and logic bombs.

Solar appScreener is the only analyzer that supports 30+ programming languages and binary static analysis (9 extensions of executable files).

Solar appScreener does not require any profound technical skills. A user receives detailed descriptions of revealed vulnerabilities and undocumented features, as well as recommendations on how to configure web application firewalls (WAF).

Open API, integration with the main repositories, CI/CD servers, SonarQube and Atlassian Jira allows Solar appScreener to be easily embedded in secure software development lifecycle (SDLC).

Tasks addressed

- Secure SDLC
- Detection of vulnerabilities and undocumented features in apps
- Standard and regulatory compliance
- Control over in-house and outsourced development efforts

Features

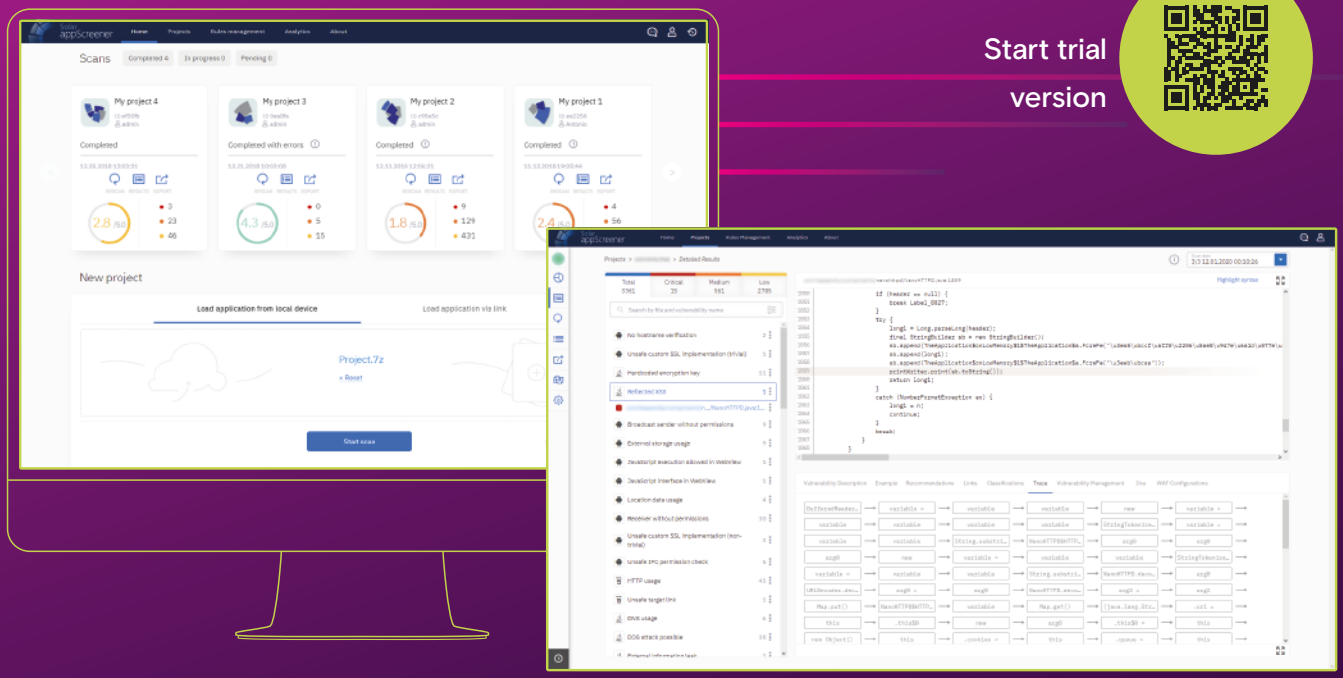
- Source code analysis
- Executable file analysis
- Vulnerability detection
- Undocumented feature detection
- Scan results comparison
- Customizable reports
- Developer access control
- Recommendations for developers and security officers
- Interoperability with issue tracking systems and Atlassian Jira
- Integration into development process

Supported programming languages

JAVA | JAVA FOR ANDROID | JAVASCRIPT | SOLIDITY | RUBY | VBSCRIPT | PERL | SCALA | HTML5 | APEX | PYTHON | PL/SQL | T/SQL | C/C++ | JSP | KOTLIN | VISUAL BASIC 6.0 | VBA | PHP | DELPHI | ASP.NET | 1C | TYPESCRIPT | COBOL | GROOVY | SWIFT | C# | VYPER | VB.NET | GO | ABAP | OBJECTIVE-C | RUST

*According to Risk Based Security, Solar JSOC Security Report 2019, and U.S. Department of Homeland Security, 2018

User interface



Use cases

Prompt vulnerability blocking

The testing of a new remote banking system revealed critical vulnerabilities, which required 3.5 months to be addressed. The bank decided to block vulnerabilities by deploying WAF, with Solar appScreener providing detailed configuration recommendations.

Control over developers

Solar appScreener tested a mobile app and detected vulnerabilities that were absent from the source code provided by developers. To avoid sanctions, the developers submitted an abridged and obfuscated code for analysis.

Detecting vulnerabilities in third-party software components

While the testing of business app source code revealed few vulnerabilities, a repeat check via binary analysis identified earlier unknown code lines and hundreds of vulnerabilities. To save time, developers actively employed third-party components, ready-to-use codes from the internet, modules, etc.

Binary code analysis

JAR WAR EXE DLL APK IPA APP AAR EAR

Regulatory compliance

PCI Security Standards Council™ OWASP HIPAA COMPLIANCE SANS CWE

Benefits

No source code required

Just download executable files or simply specify a Google Play or App Store link

Launch in a few clicks

User-friendly and intuitive interface and highly automated analysis

No development skills needed

Solar appScreener designed for security officers rather than developers and doesn't require software development skills

Detailed recommendations

Recommendations on how to address vulnerabilities and undocumented features, and how to configure WAF

Fewer false positives

False positives and false negatives (with regard to both vulnerabilities and undocumented features) are minimized via Solar appScreener`s Fuzzy Logic Engine

10+ code analysis methods

To analyze apps, Solar appScreener can combine 10+ methods maximizing the detection of code vulnerabilities and undocumented features

On-premise and SaaS

Can be either deployed at a customer's site or provided as a cloud-based service, thus enabling the security team to select the optimal solution

Easy integration with SDLC

Integration with the CI/CD, development environments, platform for continuous inspection of code quality and issue tracking system

Integration capabilities

Repositories git SUBVERSION Issue tracking Atlassian JIRA Code analysis sonarqube

IDE eclipse Visual Studio Xcode

CI/CD Servers TeamCity Jenkins Azure DevOps Server

Open API (including JSON API and CLI) provides powerful integration and automation capabilities

Rostelecom Solar | athena dynamics A Member of BH GLOBAL CORPORATION LTD

dan@solarappscreener.com contact@athenadynamics.com