Solar appScreener

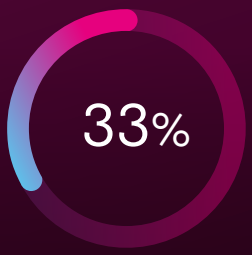
Поиск уязвимостей и недекларированных возможностей в исходном и бинарном кодах

rt-solar.ru
rt.ru

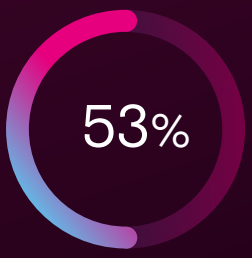
Ростелеком
Солар

Безопасность бизнеса зависит от безопасности приложений

приложений уязвимы



уязвимостей критические



уязвимостей эксплуатируются удаленно

успешных атак используют дыры в коде

Solar appScreener — статический анализатор безопасности приложений (SAST) для поиска уязвимостей и недекларированных возможностей (НДВ), включая прописанные в коде пароли и логические бомбы.

Solar appScreener — единственный анализатор с поддержкой 30+ языков программирования и бинарного статического анализа (9 расширений исполняемых файлов).

Использование Solar appScreener не требует глубоких технических знаний. Заказчик получает детальную информацию о найденных уязвимостях и НДВ и советы по настройке экранов уровня приложений (WAF).

Открытый API и интеграция с основными репозиториями, CI/CD-серверами, SonarQube и Atlassian Jira упрощают встраивание Solar appScreener в цикл безопасной разработки ПО.

Решаемые задачи

- Обнаружение уязвимостей и НДВ в приложениях
- Соответствие требованиям стандартов и регуляторов
- Контроль внешней и внутренней разработки
- Обеспечение цикла безопасной разработки (Secure SDLC)

Возможности

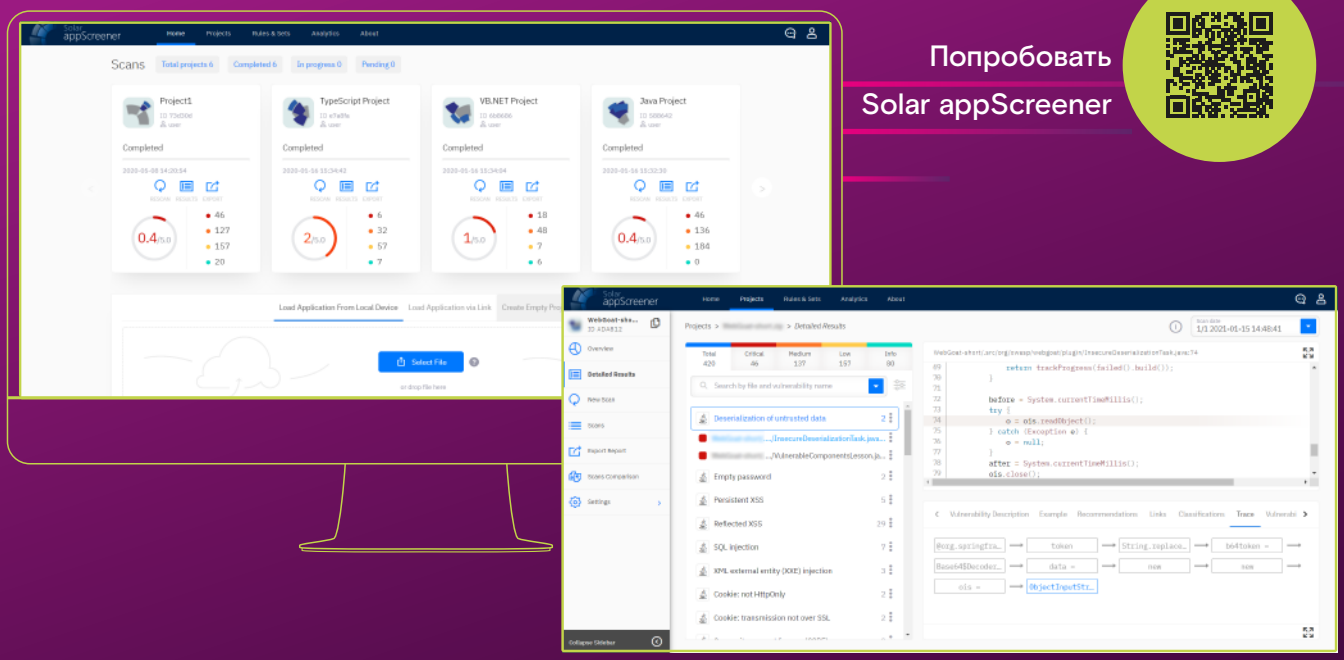
- Анализ исходного кода
- Анализ исполняемых файлов
- Выявление уязвимостей
- Выявление недекларированных возможностей
- Сравнение результатов проверок
- Построение отчетов
- Разграничение прав разработчиков
- Подготовка рекомендаций для разработчиков и офицеров безопасности
- Работа с системами отслеживания ошибок
- Интеграция в процесс разработки

Поддерживаемые языки программирования

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 | PASCAL | LOTUSSCRIPT | DART

*Данные Risk Based Security, Solar JSOC Security Report 2019 и Министерства внутренней безопасности США, 2018

Взаимодействие с Solar appScreener



Попробовать
Solar appScreener

Примеры применения

Оперативная блокировка уязвимостей

Проверка новой системы дистанционного обслуживания в банке выявила критические уязвимости. На их устранение требовалось 3,5 месяца. Банк решил развернуть систему и предотвратить использование уязвимостей с помощью WAF, а Solar appScreener помог с его настройкой.

Контроль разработчиков

Solar appScreener выявил в мобильном приложении уязвимости, отсутствовавшие в исходном коде, предоставленном разработчиками — боясь штрафных санкций, они отдали урезанную и обфусцированную версию кода.

Выявление уязвимостей в сторонних компонентах ПО

В исходном коде бизнес-приложения обнаружили небольшое количество уязвимостей. Повторная проверка с помощью бинарного анализа выявила неизвестные строки кода и сотни уязвимостей — в спешке разработчики использовали сторонние компоненты: готовые коды из интернета, модули и т.д.

Анализ бинарного кода

JAR WAR EXE DLL APK IPA APP AAR EAR

Поддерживаемые стандарты отчетности

PCI Security Standards Council ™ OWASP HIPAA COMPLIANCE SANS CWE ФСТЭК России ОУД4

Преимущества

Умеет работать без исходных кодов

Для анализа достаточно получить файлы у системного администратора или дать ссылку на Google Play или App Store

10+ методов анализа кода

Для выявления максимума уязвимостей и НДВ в коде Solar appScreener использует более 10 методов анализа, в том числе потока выполнения и taint-анализа

On-premise и SaaS

Можно развернуть как на собственных вычислительных мощностях, так и использовать как услугу из облака «Ростелеком-Солар» по модели SaaS

Дает понятные рекомендации

Офицер безопасности получает подробные описания найденных уязвимостей и НДВ, а также рекомендации по настройке WAF

Минимизирует ложные срабатывания

Технология Fuzzy Logic Engine минимизирует процент ложноположительных и ложноотрицательных срабатываний

Управляется в 2 клика

Наглядный и удобный интерфейс. Процесс анализа максимально автоматизирован и не требует постоянного внимания

Рассчитан на службу ИБ и не требует опыта разработки

Solar appScreener обладает интуитивно понятным интерфейсом, для работы с ним не нужно знать программирование и проходить специальное обучение

Легко интегрируется в процесс разработки ПО, обеспечивая Secure SDLC

Интеграция с Git и Subversion, средствами разработки, серверами CI/CD, платформой анализа качества кода и системой отслеживания ошибок

Интеграция

Репозитории: git, Subversion

Отслеживание задач: Atlassian JIRA

Анализ кода: sonarqube

Средства разработки: Visual Studio, eclipse, IntelliJ IDEA

VCS-хостинги: GitLab, GitHub, Bitbucket

Средства сборки: Xcode, Maven, Gradle, sbt, Visual Studio, CMake, GNU (Make, Autotools)

Серверы CI/CD: TeamCity, Jenkins, Azure DevOps Server

Открытый API для дополнительной интеграции и автоматизации, включает JSON API и CLI

Ростелеком Солар

presale@rt-solar.ru rt.ru rt-solar.ru

+7 (499) 755-07-70