SASTAV

Российское решение для статического анализа кода

Запись в реестре отечественного ПО:
№23718 от 29.08.2024

SASTAV

Проблематика:

Разработчики в первую очередь ориентируются на выполнение технического задания на функционал продукта и не всегда учитывают стандарты безопасности.

Часто это связано с отсутствием компетенций и квалифицированных специалистов по безопасной разработке в штате.

Код ревью - это трудозатратно, и даже секрьюрити чемпионы не всегда в состоянии определить, что уязвимый вектор может проходить через несколько файлов. Такие вычисления доступны только автоматизированным средствам.

Решение:

SASTAV – это статический анализатор, который используется на самых ранних этапах разработки и встраивается в цикл для оптимизации и автоматизации процесса безопасной разработки.

SASTAV поможет точно обнаружить уязвимости и подсветит наилучшие точки для их устранения, чтобы сократить трудозатраты на исправления.

Поддерживаемые языки:

- ASP
- C / C++
- C#
- Go
- Groovy
- Java
- JavaScript
- Kotlin
- Lua
- Objective-C
- PHP
- PLSQL
- Perl
- Python
- Ruby
- Scala
- Swift
- VB6
- VbNet
- VbScript

Преимущества:

Точность поиска результатов

При установке сразу же есть большой набор пресетов с широким выбором правил сканирования, а также возможна более точная кастомизация и анализ бизнес-логики.

Построение графа векторов атак

Помогает визуально ориентироваться в коде и быстро принимать решение, где и на какой именно строчке было бы проще устранить уязвимость.

Высокая скорость сканирования

Позволяет проводить сканирования даже очень больших проектов за небольшое время. Скорость проверки достигает 2 млн. строк кода в час.

Сканирование кода без сборки

SASTAV работает именно с raw-кодом, который не обязательно должен быть компилируемым. Таким образом можно встраиваться в процесс на самых ранних этапах.

Группировка векторов по типу уязвимости и указание на оптимальную точку для устранения дефекта

Помогает максимально эффективно построить процесс исправления с минимизацией трудозатрат разработчиков в десятки раз. Точка может указываться даже для групп разных типов уязвимостей, чтобы закрыть не только 1 тип уязвимости, а сразу несколько.

Сохранение результатов триажа

Если один раз результат уже был помечен определенным статусом, то при дальнейших сканированиях он уже будет отмечен и можно сфокусироваться только на новых векторах уязвимости. При однотипных векторах – будет предложено проставить тот же статус, что уже был и поставить такой же комментарий.

Репозитории группируются в проекты для лучшей навигации по ним

Также в каждом репозитории выделены ветки и можно быстро определить, что сканировалось и когда.

Для каждой сработки предоставляется описание уязвимости и рекомендации по ее устранению.

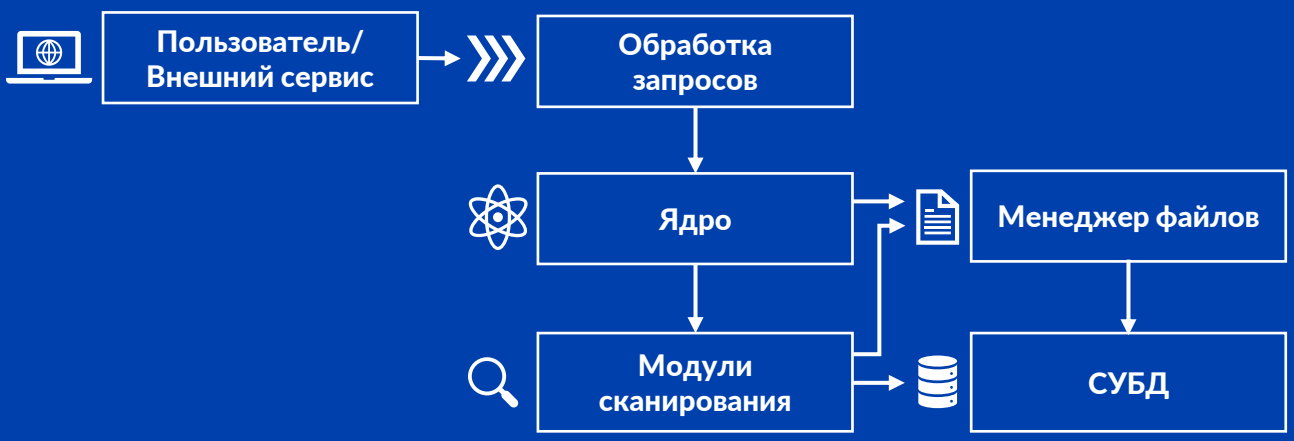
Масштабируемость

Можно подключать любое количество ядер сканирования для распараллеливания процесса при больших нагрузках.

Установка решения за 20 минут

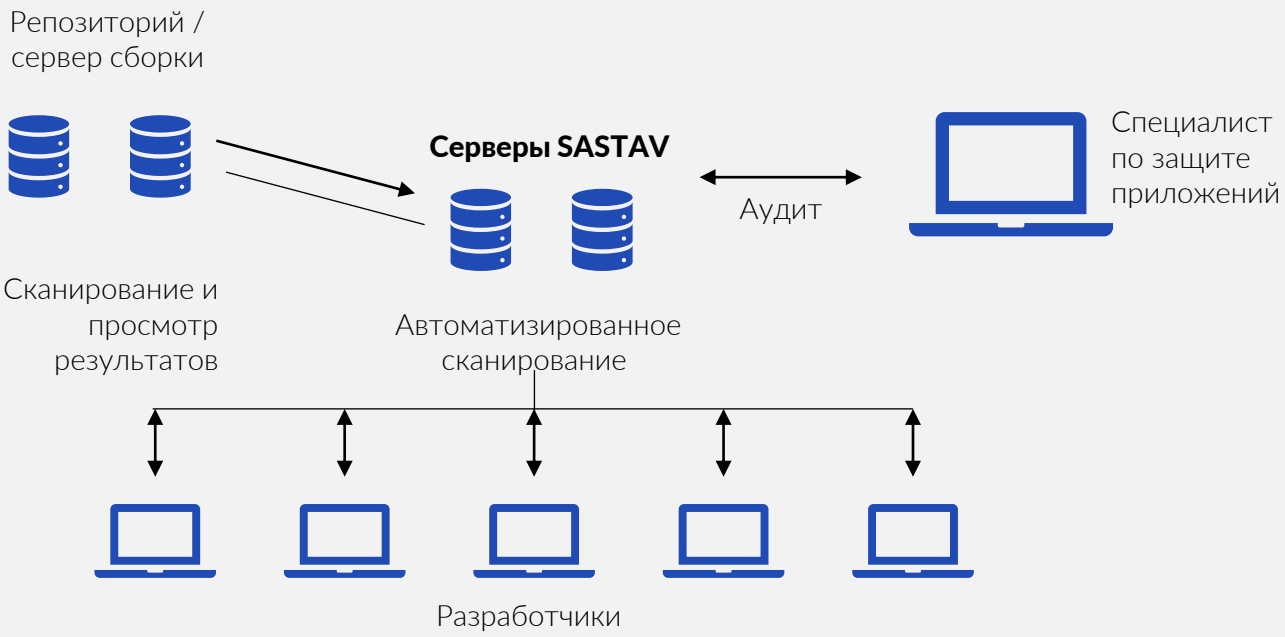
Быстрый старт и минимальные требования к обслуживанию.

Архитектура и стек технологий:



Микросервисы ПО «SASTAV» реализованы на Java и React
Поставка в виде докер-образа или helm-чарта для K8s
Устанавливается на Linux-системы, включая требуемые российскими регуляторами
БД – PostgreSQL
Интеграции посредством API

Запуск сканирований:



SASTAV

Москва, ул Дербеневская, д. 15Б, помещ. 2/1

+7 499 502 1375
support@sastav.ru