

Статический анализ

- Поиск уязвимостей и НДВ без выполнения программы
 - Максимальное покрытие кода – максимальные результаты
 - Необходим статический анализ любого кода
- Инструмент статического анализа
 - Сложные алгоритмы в простой оболочке
 - Внедрение в процессы разработки кода
 - Сертифицирован ФСТЭК
 - Выдает классификацию по БДУ ФСТЭК

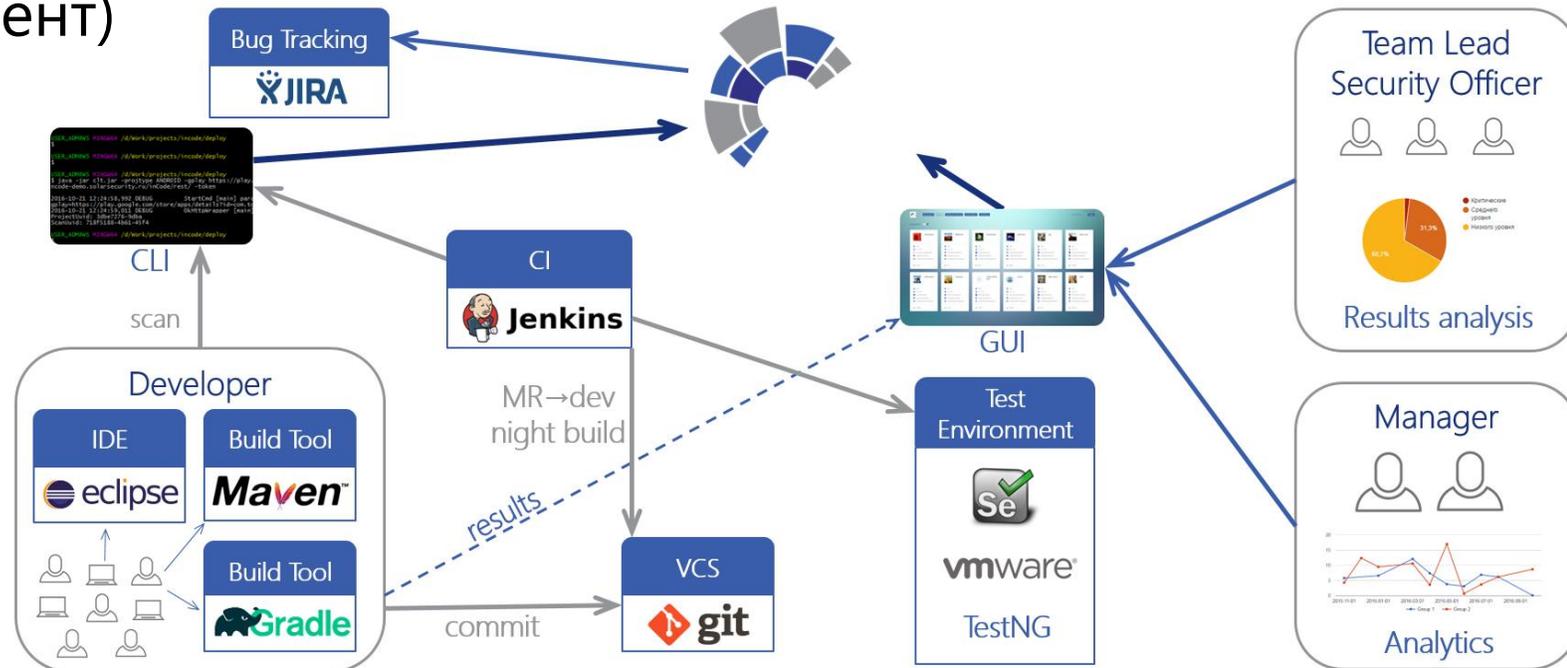


Нормативные документы

- *Требуют статического анализа кода с построением процесса безопасной разработки*
- Распоряжение «Требования к ВСЗИ АСТУ» №282р от 30.06.2017 г. для всех компаний холдинга РОССЕТИ
- Новая редакция приказа №239 - Приказ №60 от 26 марта 2019 г. ФСТЭК РОССИИ
- Приказ МИНЭНЕРГО №1015 от 06.11.2018 о системах мониторинга
- Приказ ФСТЭК РОССИИ №55 от 03.04.2018 года – положение о сертификации
- ГОСТ 56939-2016 о процессе безопасной разработки

Этапы внедрения процесса

- Выбор инструмента
- Выбор команды, проводящей внедрение
- Описание процесса (регламент)
 - Частота проверок
 - Коммуникации между участниками
 - Влияние на релизы
 - Автоматизация, интеграции
- Спецификация технических решений
- Проведение работ по внедрению
- Опытная эксплуатация



Технические аспекты

- Запуск сканирования (формат кода)
- Время и ресурсы на сканирование
- Многостраничный отчет
- Ложно-положительные срабатывания
- Интеграция с помощью плагинов и API

Все сложности решаются на этапе внедрения

Организационные аспекты (1)

- Провести инвентаризацию процессов и анализируемых систем
- Согласовать регламент процесса
- Выделить дополнительные ресурсы на исправление уязвимостей
- Заложить перерасчет мощностей в процессе внедрения
- Учесть изменение условий (технических или организационных)

Организационные аспекты (2)

- Регламентировать проверку кода подрядчиков
- Передать в поддержку компоненты интеграции
- Внедрять постепенно
 - Усиливать влияние на релизы
 - Расширять список подключенных систем и сотрудников
 - Для начала устранять только новые уязвимости
 - Начать устранение с наиболее критических



Спасибо за внимание!

Ярослав Александров

Руководитель отдела разработки

Solar appScreener

y.alexandrov@rt-solar.ru