Международный ТБ ФОРУМ Технологии и Безопасность

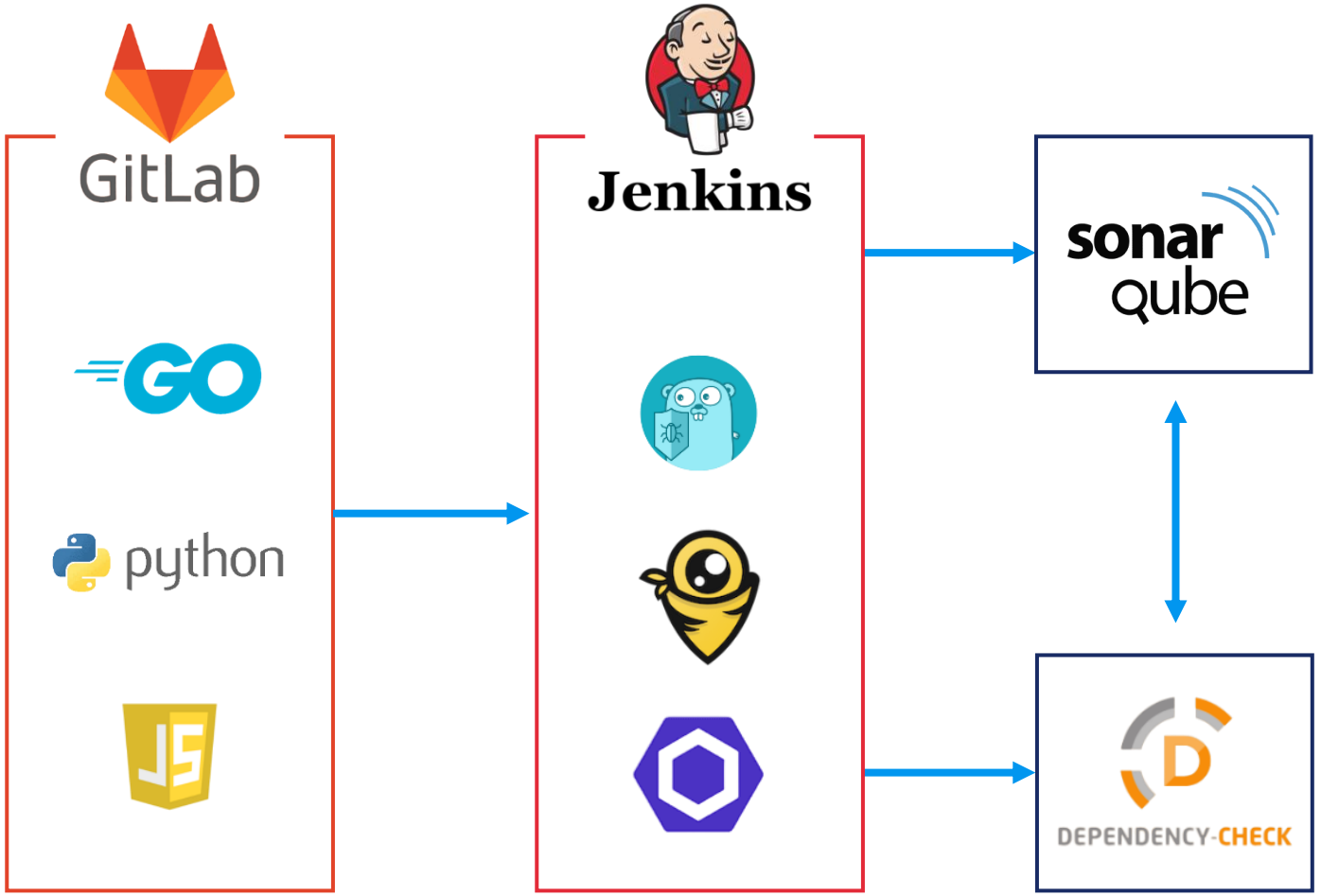
От сертификации СЗИ к сертификации РБПО

BASIS

Как мы пришли к безопасной разработке

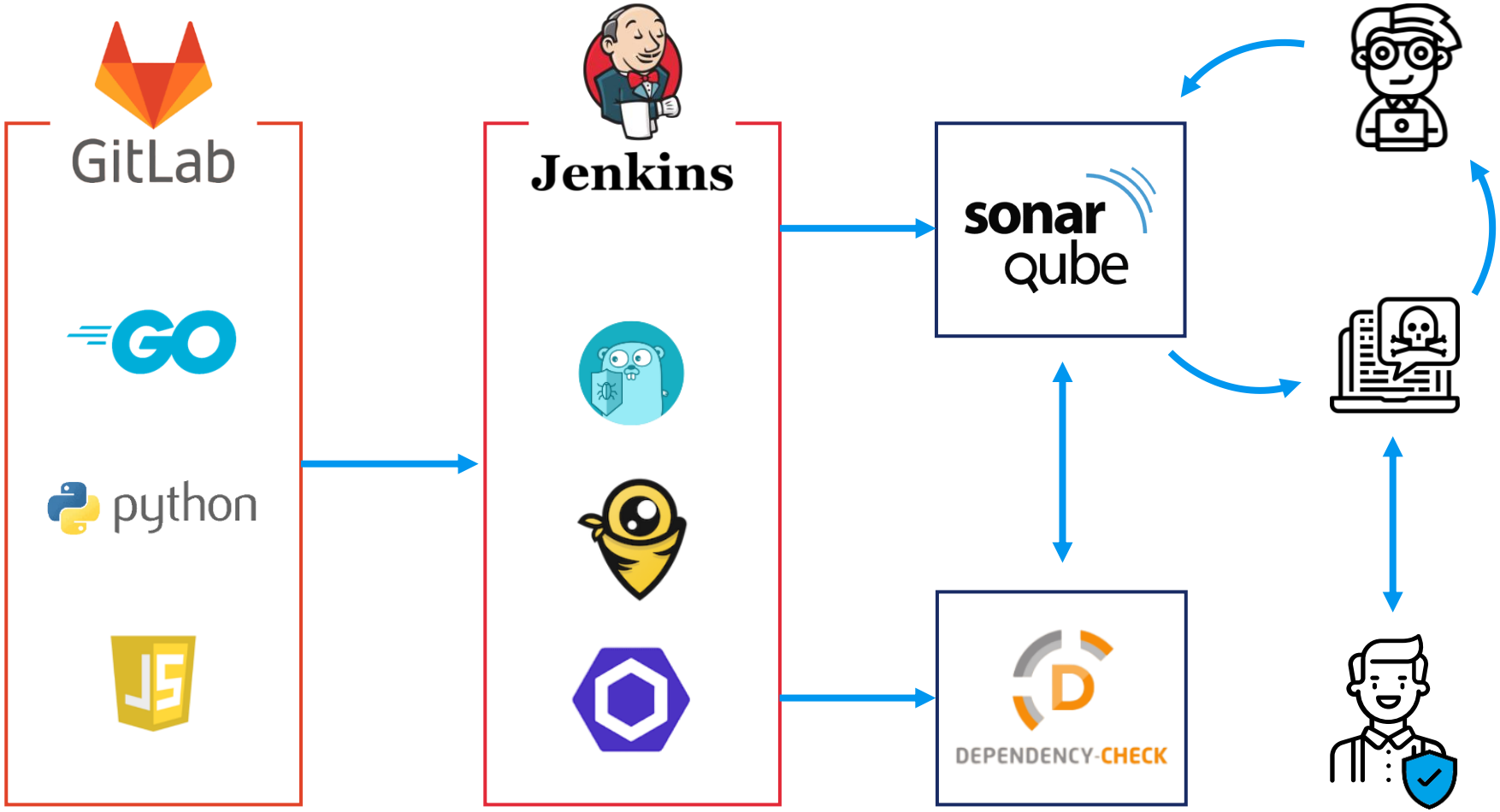
Натали Дуботолкова
Инженер DevSecOps «Базис»

Статический анализ и анализ компонентов



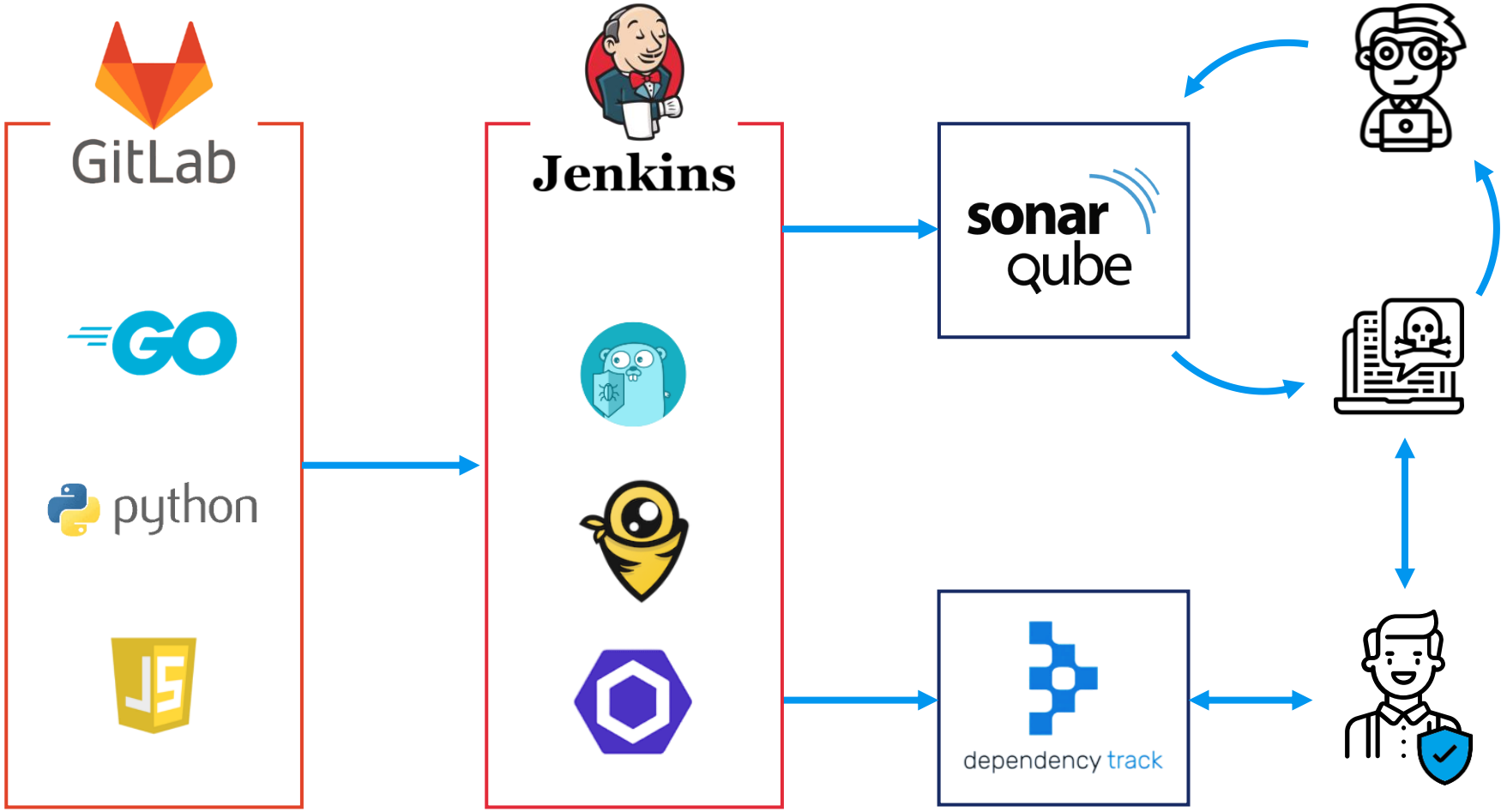
BASIS

Статический анализ и анализ компонентов



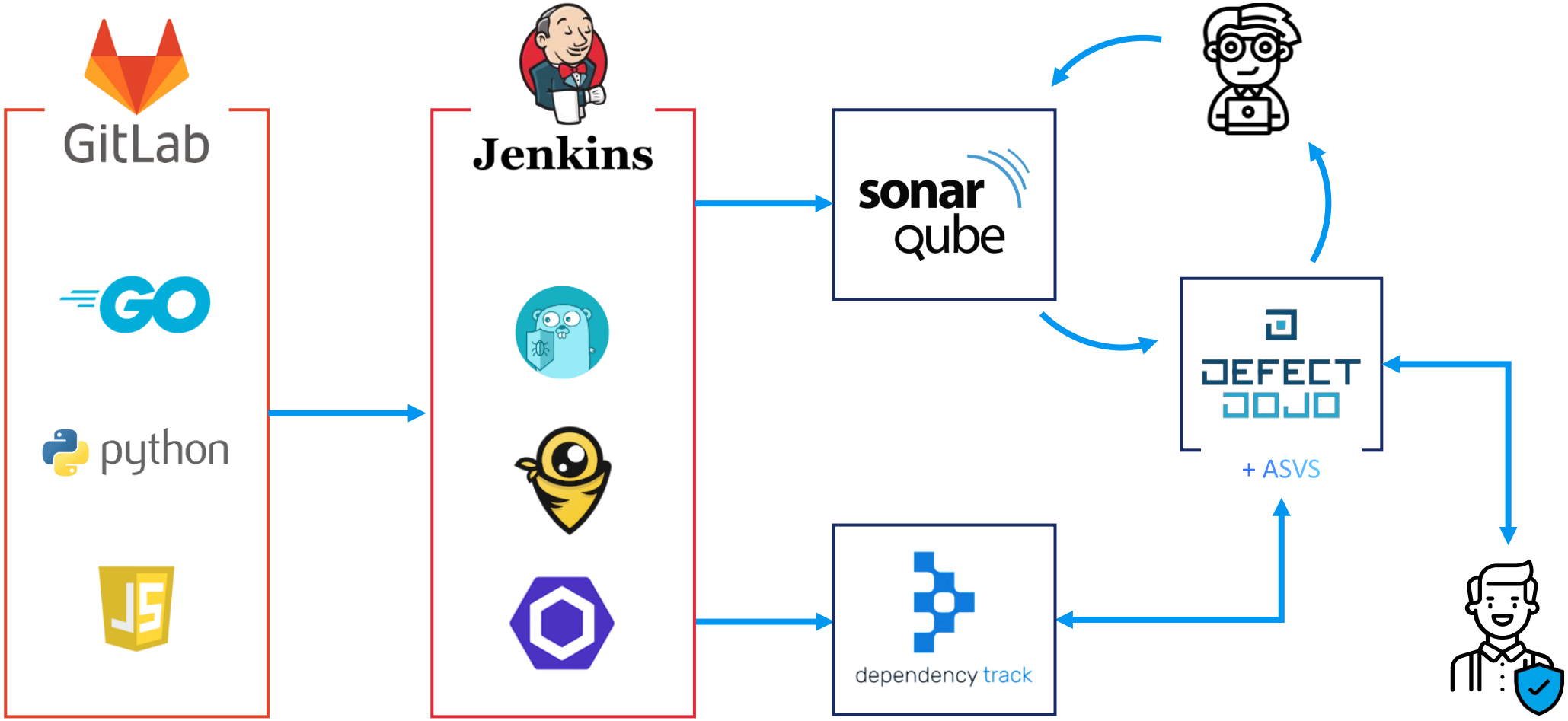
BASIS

Статический анализ и анализ компонентов



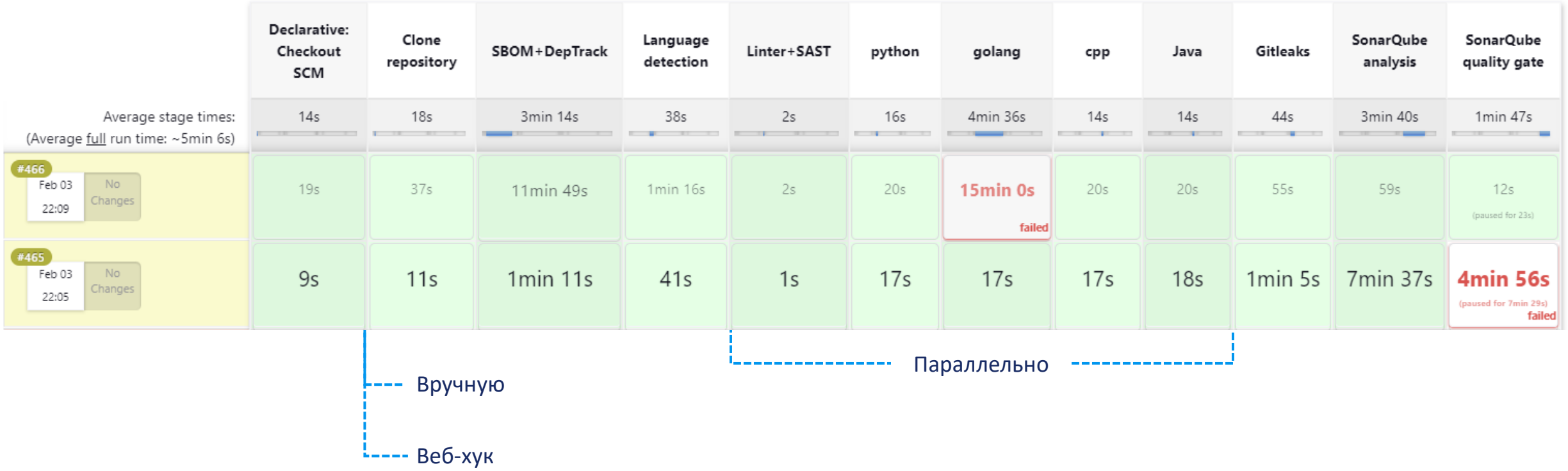
BASIS

Статический анализ и анализ компонентов



BASIS

Jenkins pipeline



Динамический анализ

OWASP
Zed Attack Proxy

BURPSUITE

nessus®
Professional

ИСП РАН

ИСП Crusher
- Sydr

BASIS

Управление уязвимостями

01 Сканирование проектов

02 Выявление уязвимостей

03 Определение приоритетов уязвимостей

04 Рекомендации по устранению

05 Исправление уязвимостей

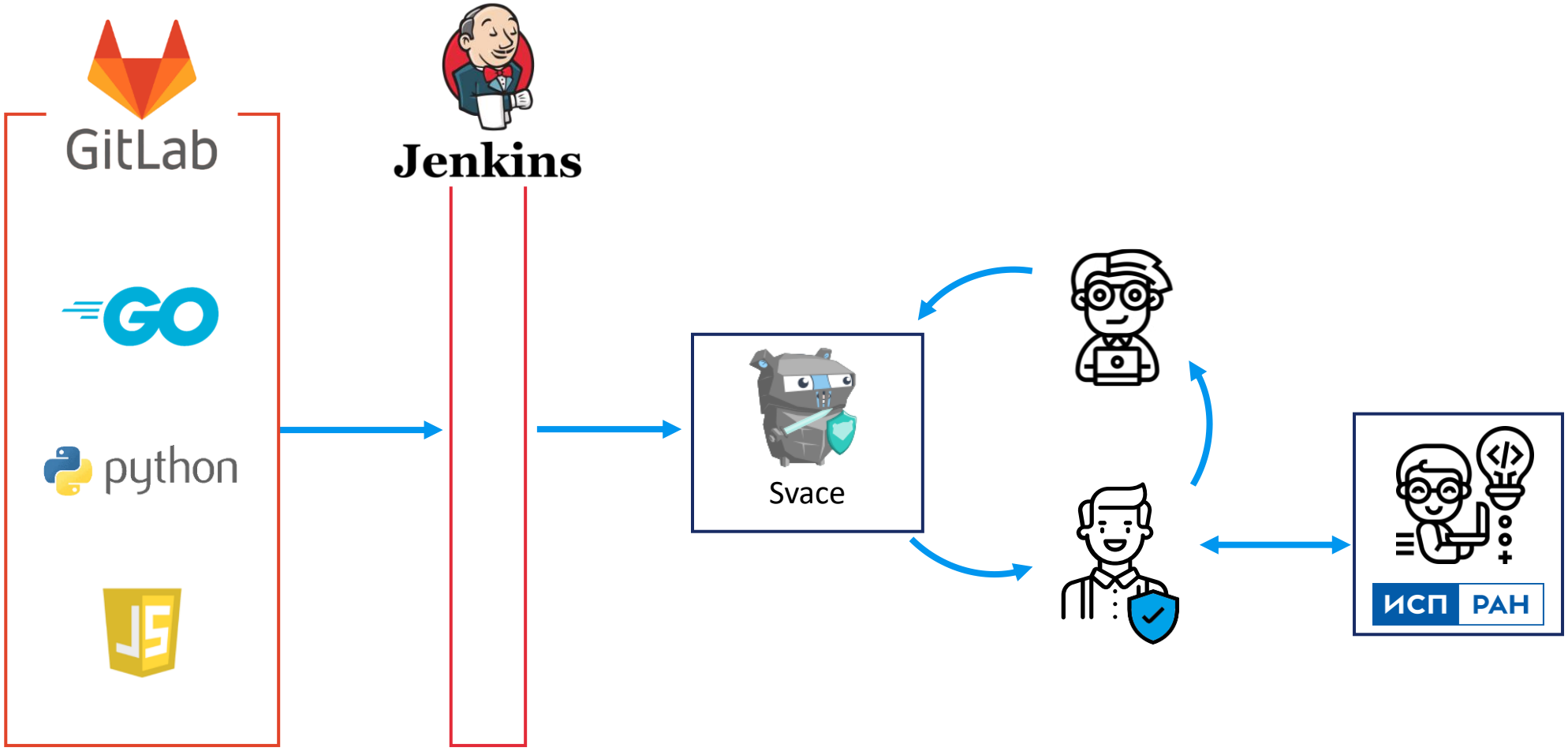
06 Экранирование уязвимостей

BASIS

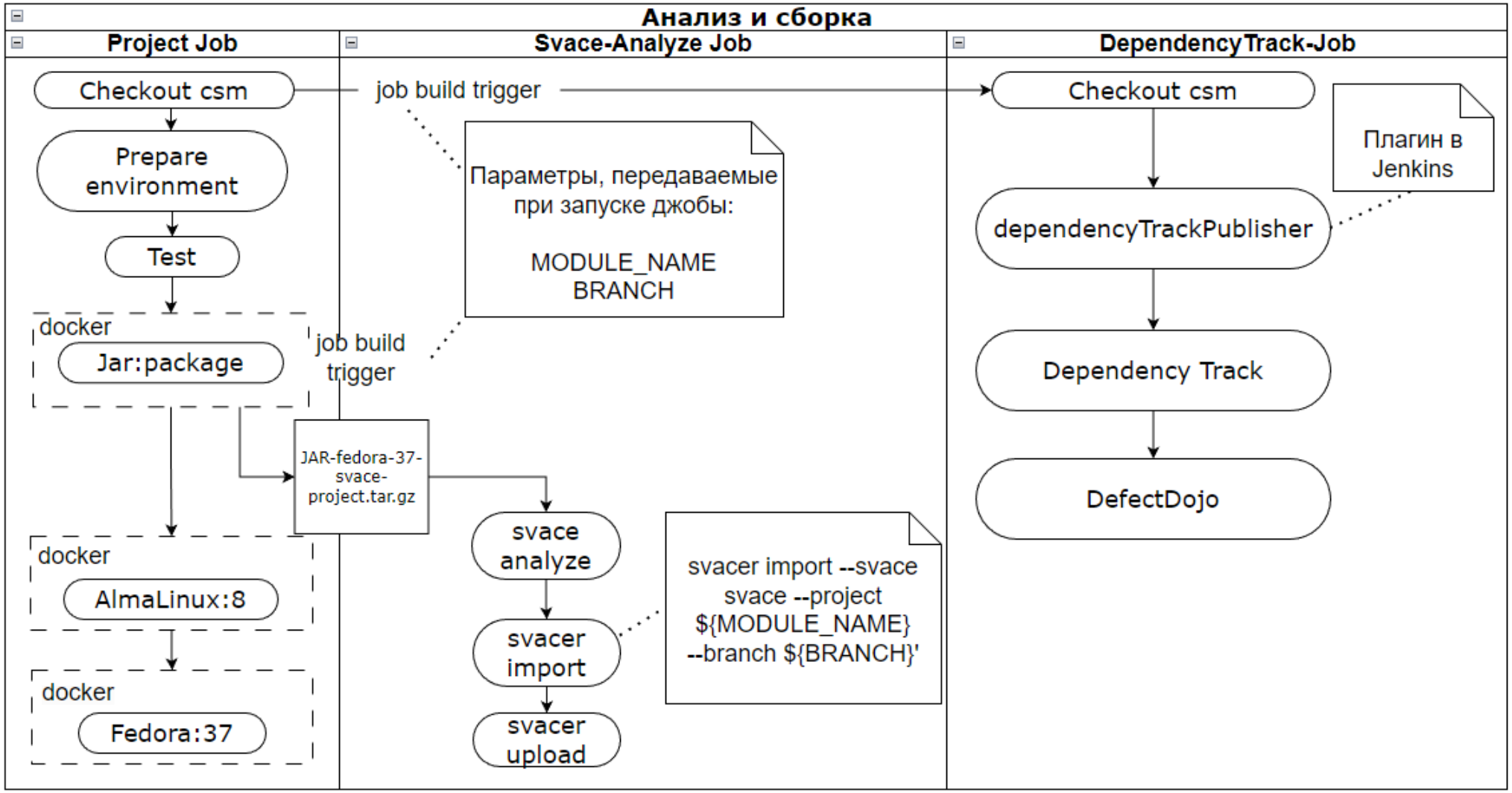
Возникшие проблемы

- Сканеры не находят серьёзных уязвимостей
- Большое количество ложноположительных результатов
- Нет инкрементного анализа
- Нет возможности посмотреть стек вызовов функции

Интеграция Svace в сборочный конвейер



Запуск svace из Jenkins



На данный момент

Улучшилось качество проводимого анализа

Уменьшилось количество ложноположительных результатов

Увеличилась скорость повторного анализа

Отчёты стали понятнее

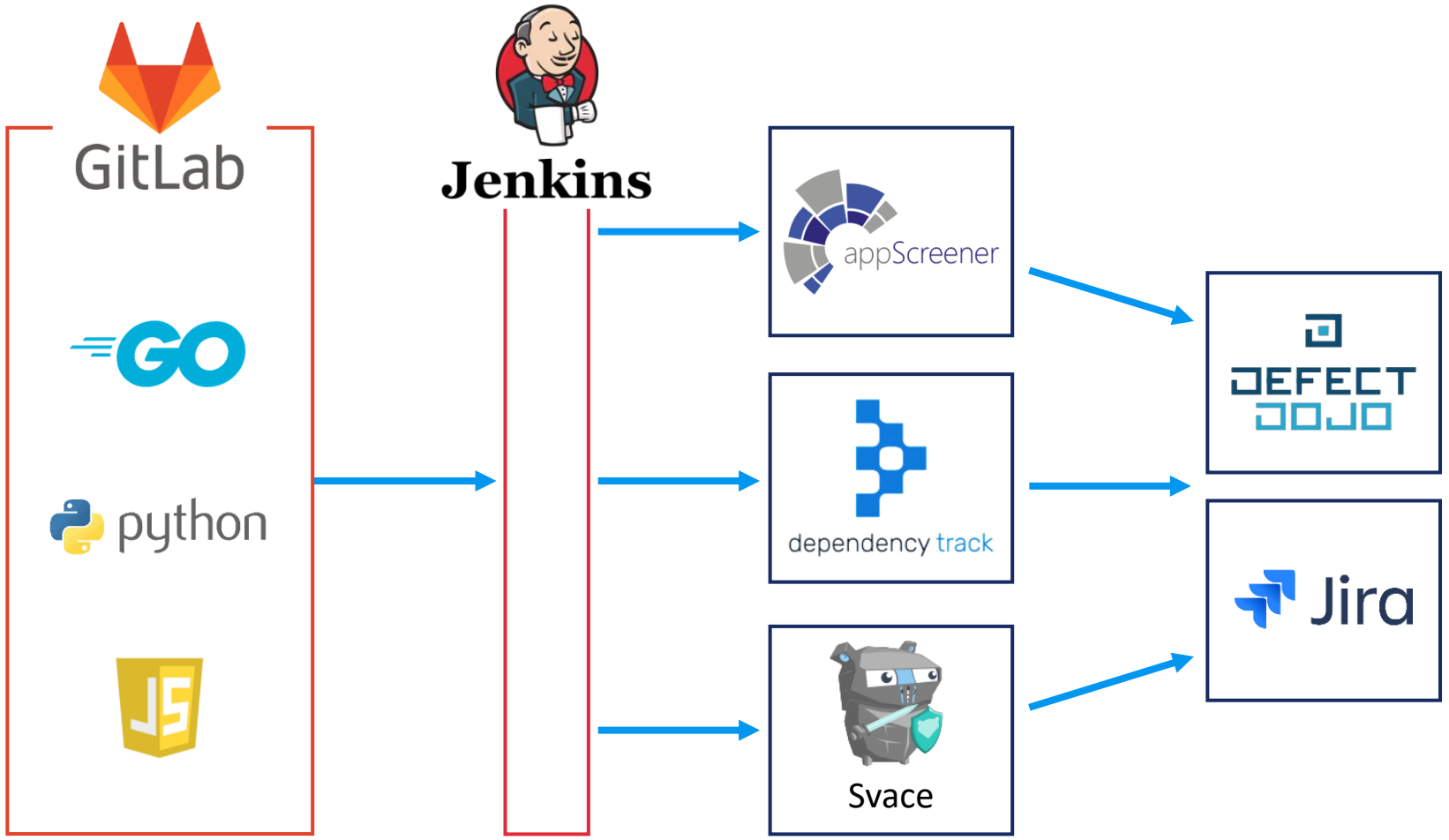
Планы

Внедрение Svace в оставшиеся и новые проекты

Проведение фаззинг-тестирования с использованием Sydr

Оптимизация сборочных конвейеров

Статический анализ и анализ компонентов Svace



BASIS

Уязвимости в контейнерах

01 Уязвимости ОС

02 Зависимости

03 Уязвимости ПО

04 Небезопасные инструкции в Dockerfile

Уязвимости в контейнерах

01 Уязвимости ОС

02 Зависимости

Проведение анализа

При сборке образа

Ежемесячно

aqua trivy

BASIS

Уязвимости в контейнерах

Небезопасные инструкции в Docker

Не монтировался ли docker.sock

Задан ли пользователь

Запрещено взаимодействие между контейнерами

Безопасное подключение к файловой системе из контейнера

Включены встроенные модули безопасности

Linux Security Module

Выделены только нужные права

Capabilities

Использование hadolint → Defect Dojo

Фоновые задачи

Инвентаризация инфраструктуры

Обучение сотрудников

Список доступов к хостам и приложениям

Своевременная блокировка сотрудников после увольнения

Чек-лист на начальном этапе РБПО

Топ-7

- С кем мы будем контактировать
- Как данный проект собирается
- Какие языки используются
- Какой у команды gitflow
- Существует ли регламент выпуска релизов, точные даты
- Кто будет участвовать в исправлении уязвимостей
- Сроки

Спасибо за внимание!

Натали Дуботолкова
nddubotolkova@basistech.ru