Международный ТБ ФОРУМ Технологии и Безопасность

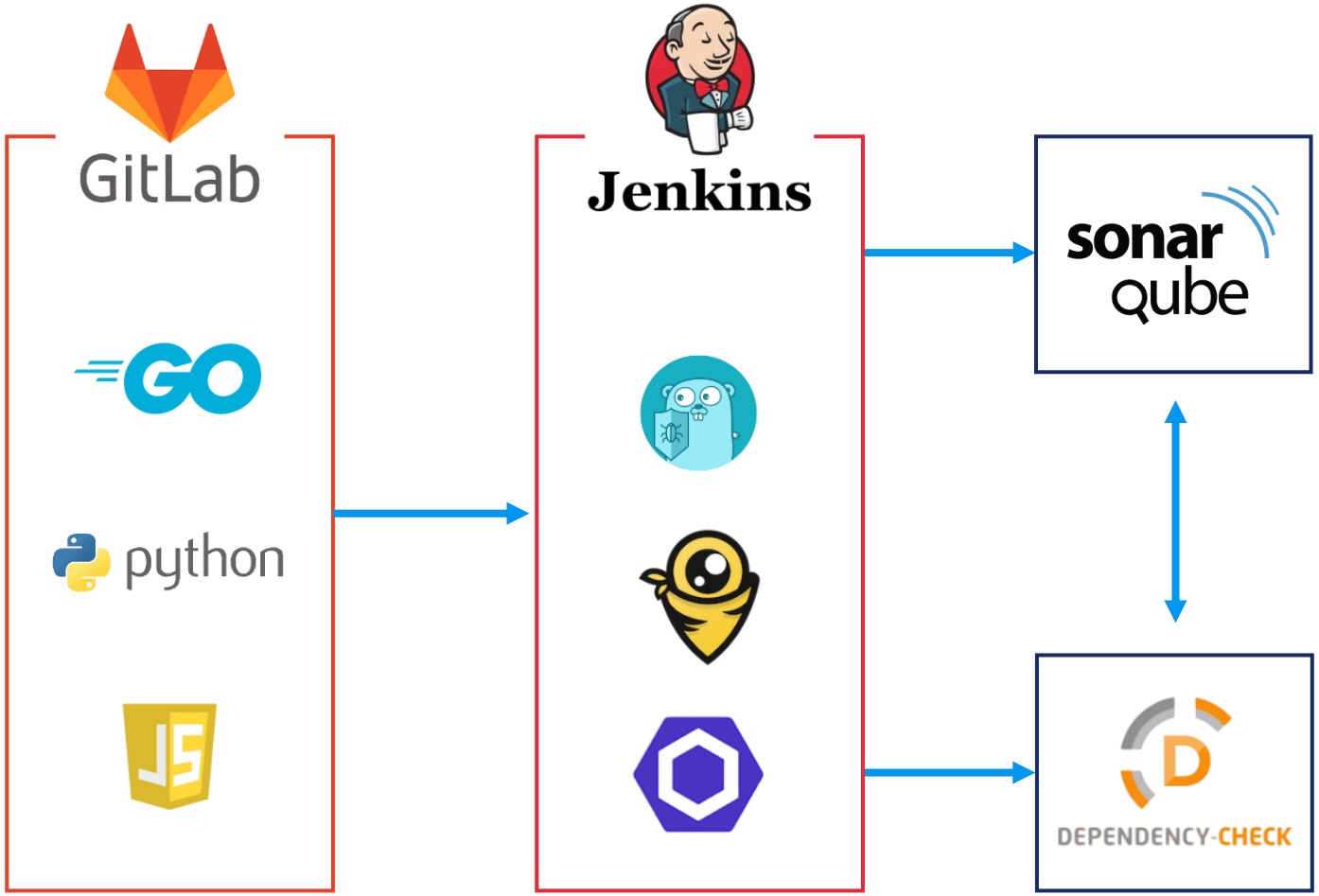
От сертификации СЗИ к сертификации РБПО

BASIS

Как мы пришли к безопасной разработке

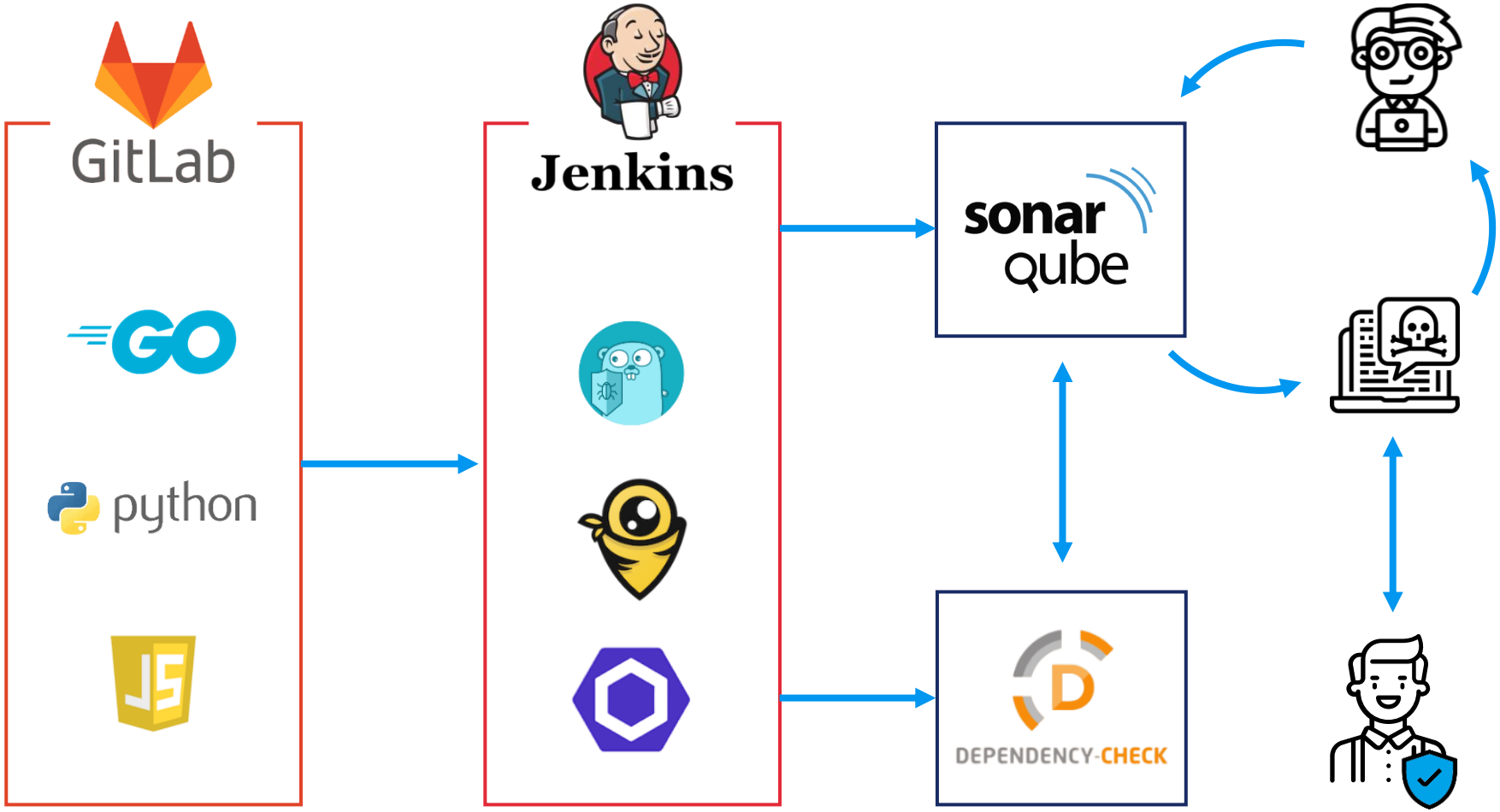
Натали Дуботолкова
Инженер DevSecOps «Базис»

Статический анализ и анализ компонентов



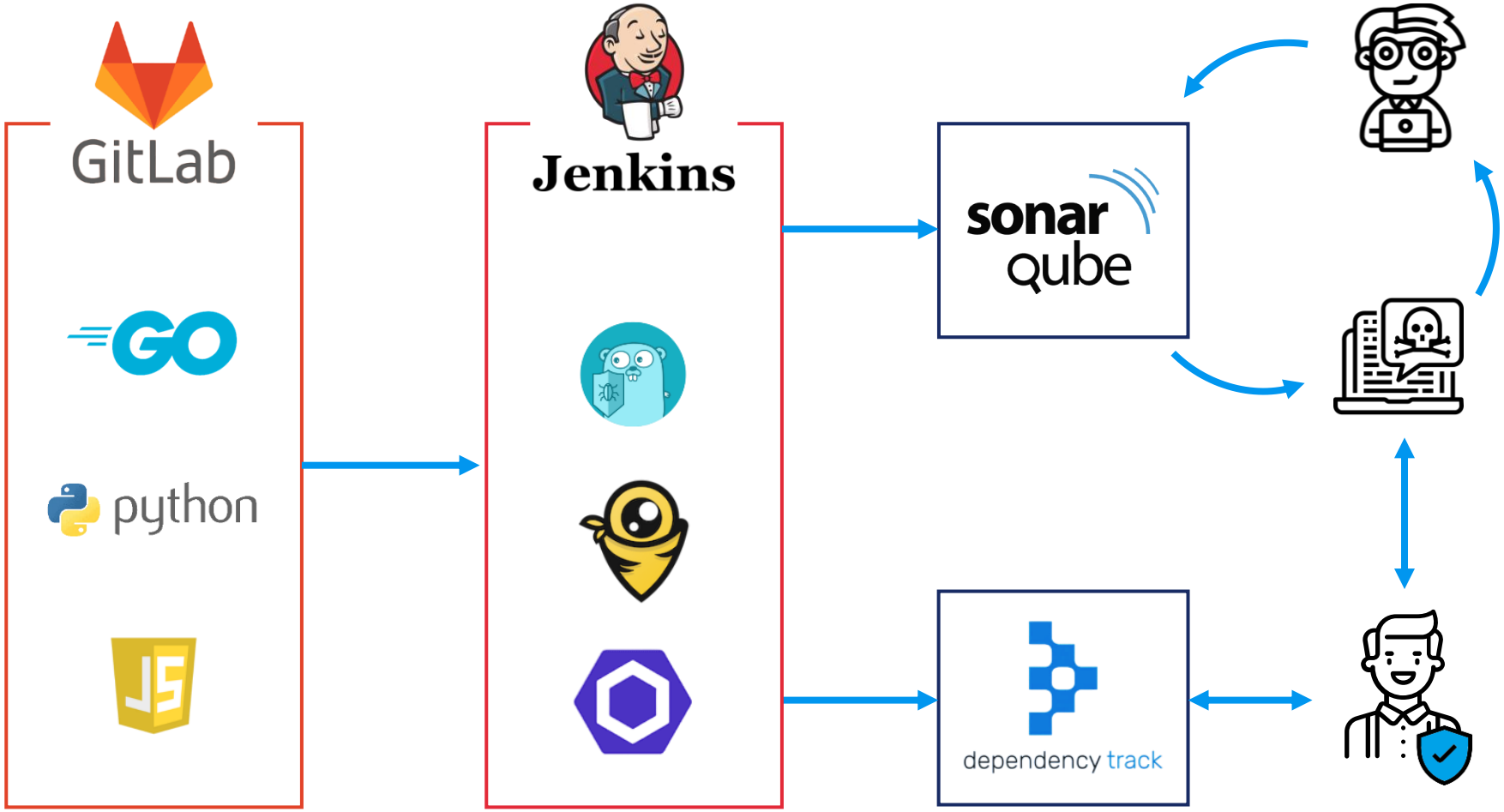
BASIS

Статический анализ и анализ компонентов



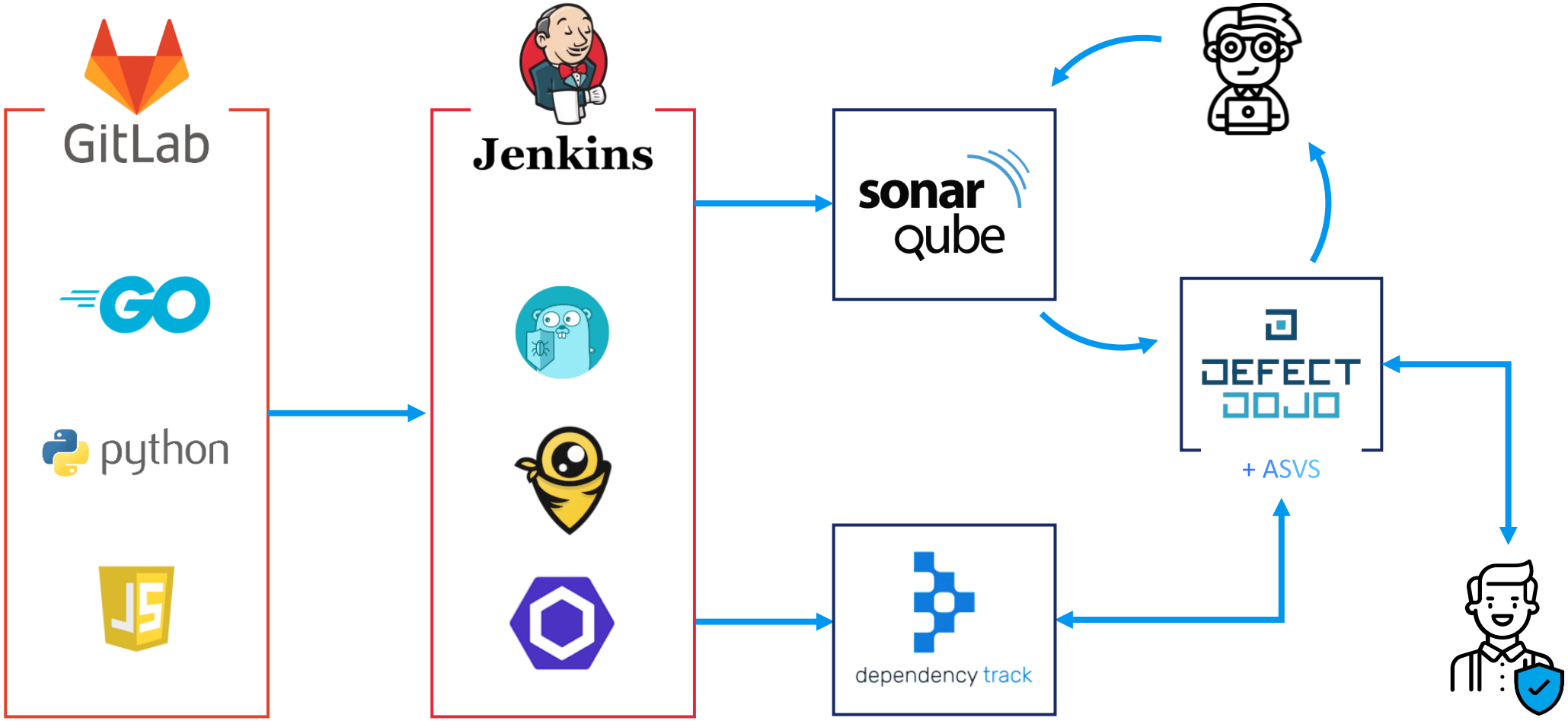
BASIS

Статический анализ и анализ компонентов



BASIS

Статический анализ и анализ компонентов



BASIS

Jenkins pipeline

	Declarative: Checkout SCM	Clone repository	SBOM+DepTrack	Language detection	Linter+SAST	python	golang	cpp	Java	Gitleaks	SonarQube analysis	SonarQube quality gate
Average stage times: (Average full run time: ~5min 6s)	14s	18s	3min 14s	38s	2s	16s	4min 36s	14s	14s	44s	3min 40s	1min 47s
#466 Feb 03 22:09 No Changes	19s	37s	11min 49s	1min 16s	2s	20s	15min 0s failed	20s	20s	55s	59s	12s (paused for 23s)
#465 Feb 03 22:05 No Changes	9s	11s	1min 11s	41s	1s	17s	17s	17s	18s	1min 5s	7min 37s	4min 56s (paused for 7min 29s) failed

Параллельно

Вручную

Веб-хук

BASIS

Динамический анализ

OWASP
Zed Attack Proxy

BURPSUITE

ИСП Crusher

- Sydr

BASIS

Управление уязвимостями

01 Сканирование проектов

02 Выявление уязвимостей

03 Определение приоритетов уязвимостей

04 Рекомендации по устранению

05 Исправление уязвимостей

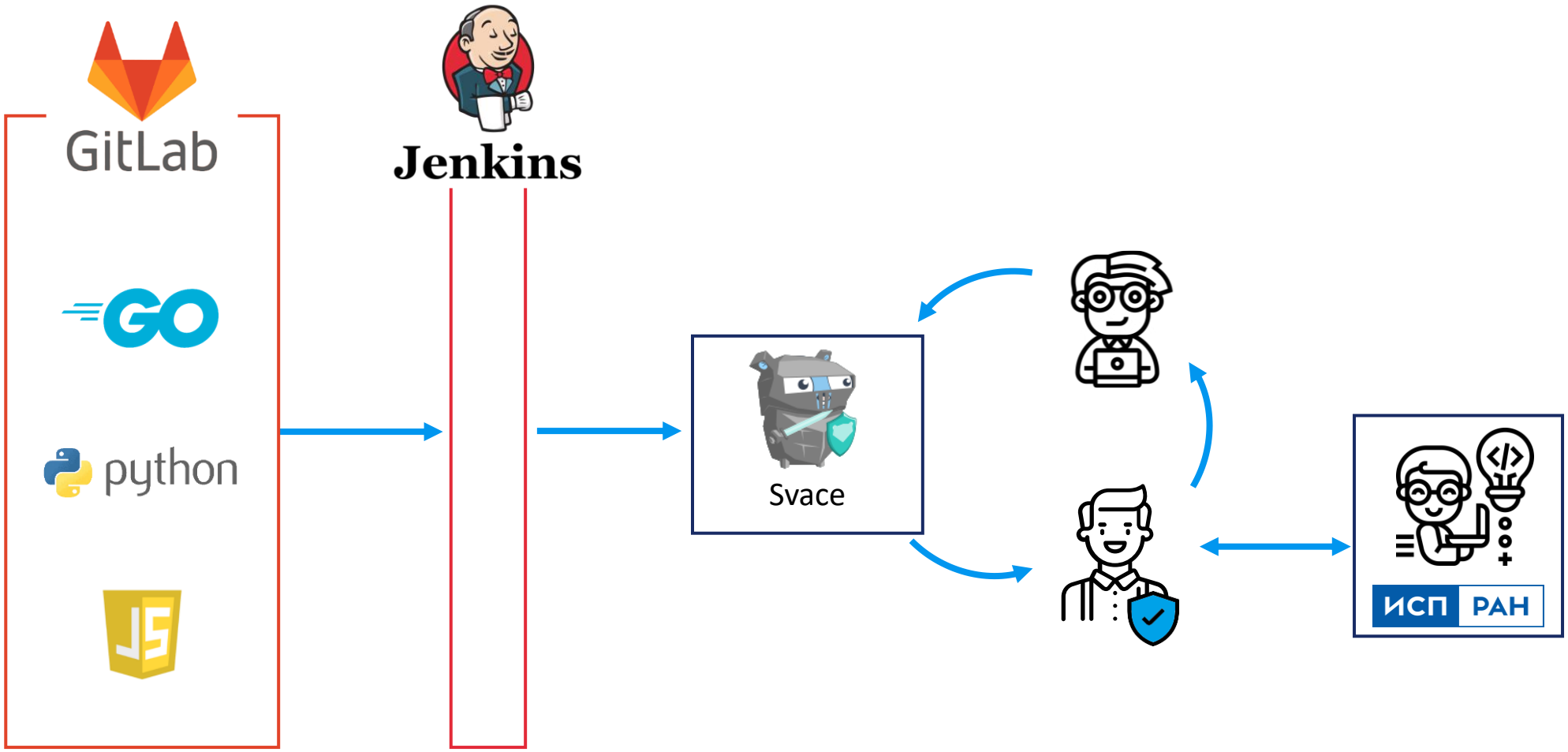
06 Экранирование уязвимостей

BASIS

Возникшие проблемы

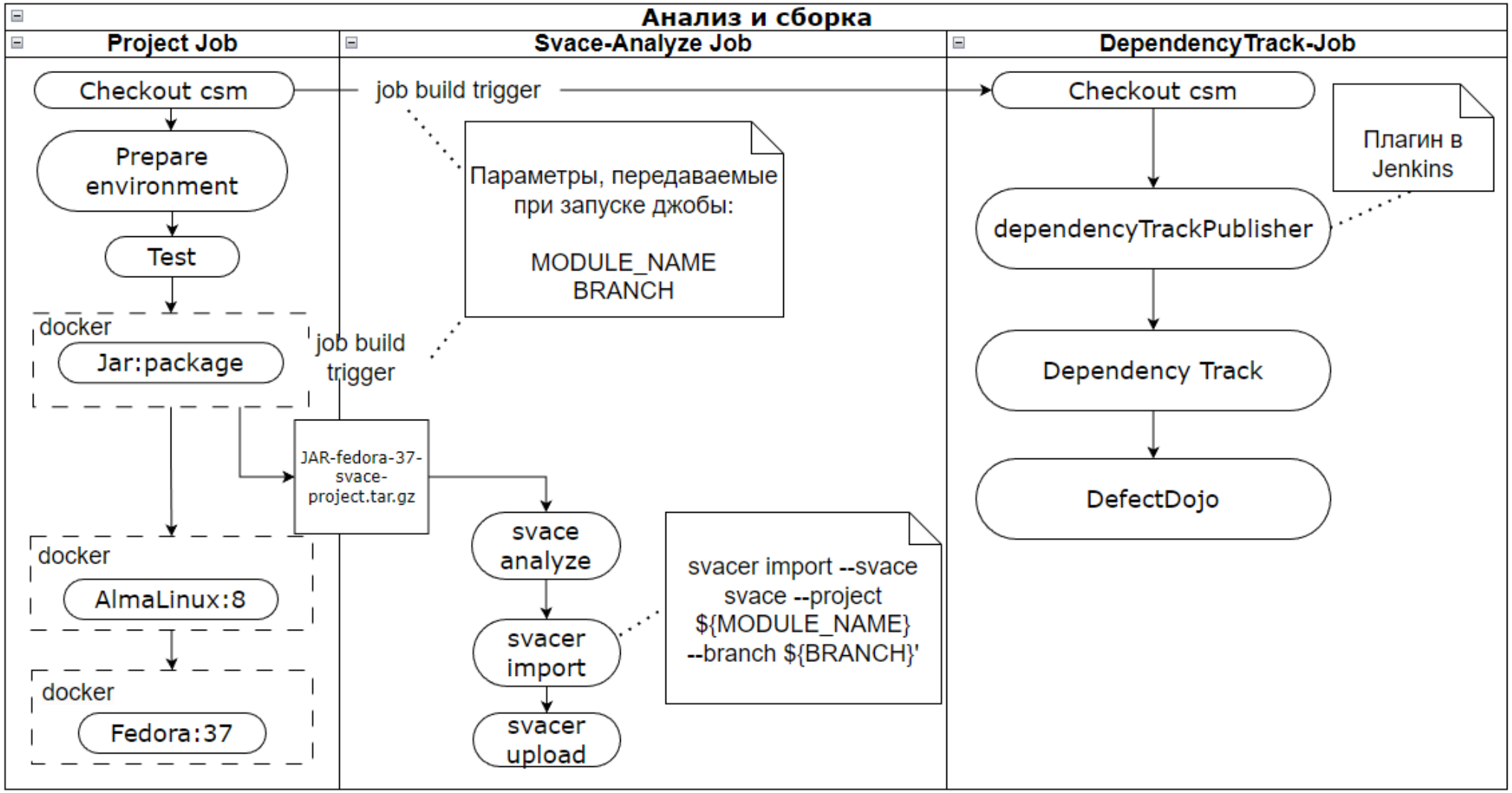
- Сканеры не находят серьёзных уязвимостей
- Большое количество ложноположительных результатов
- Нет инкрементного анализа
- Нет возможности посмотреть стек вызовов функции

Интеграция Svace в сборочный конвейер



BASIS

Запуск svace из Jenkins



На данный момент

Улучшилось качество проводимого анализа

Уменьшилось количество ложноположительных результатов

Увеличилась скорость повторного анализа

Отчёты стали понятнее

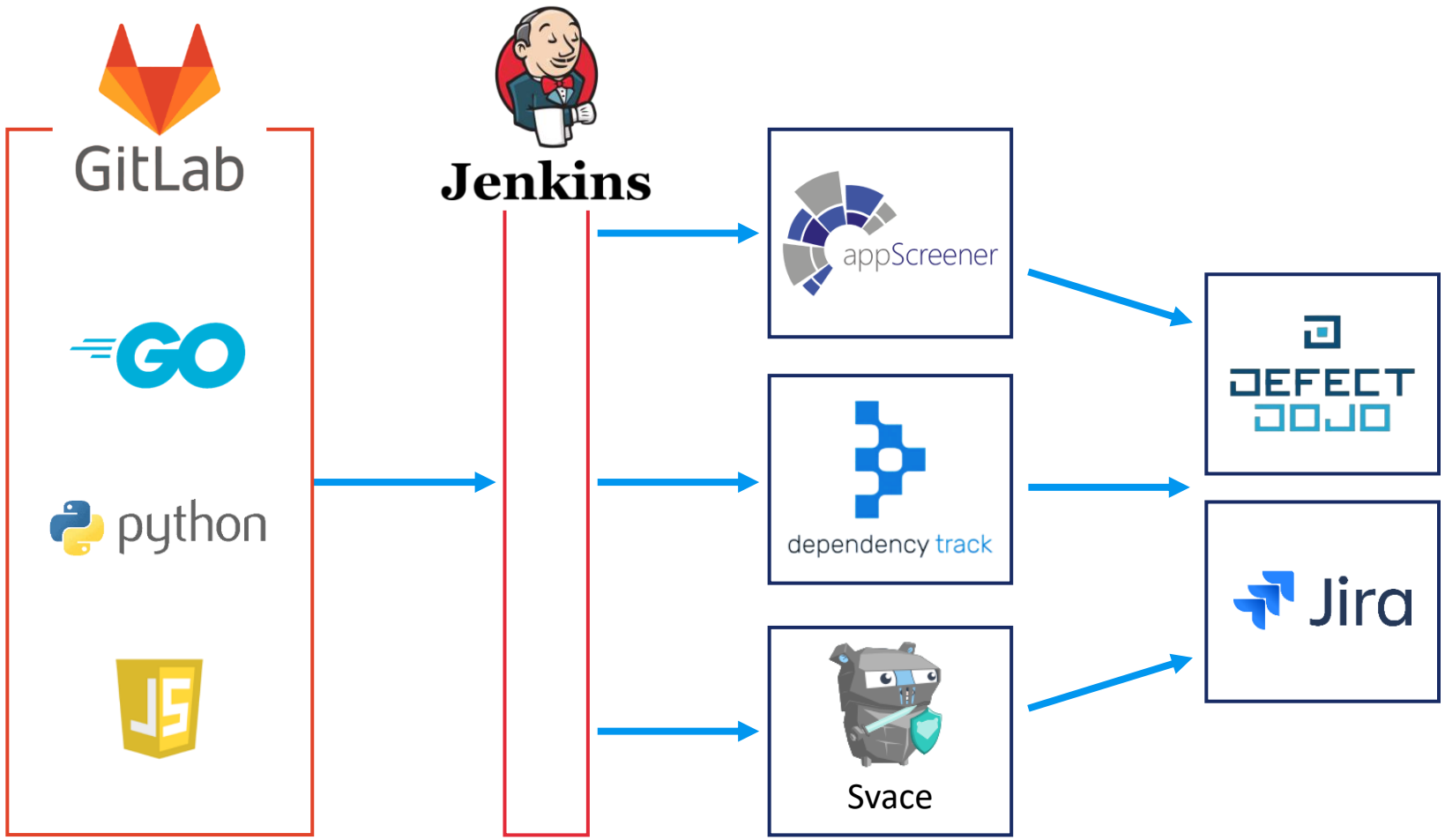
Планы

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

03 Уязвимости ПО

02 Зависимости

04 Небезопасные инструкции в Dockerfile

BASIS

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