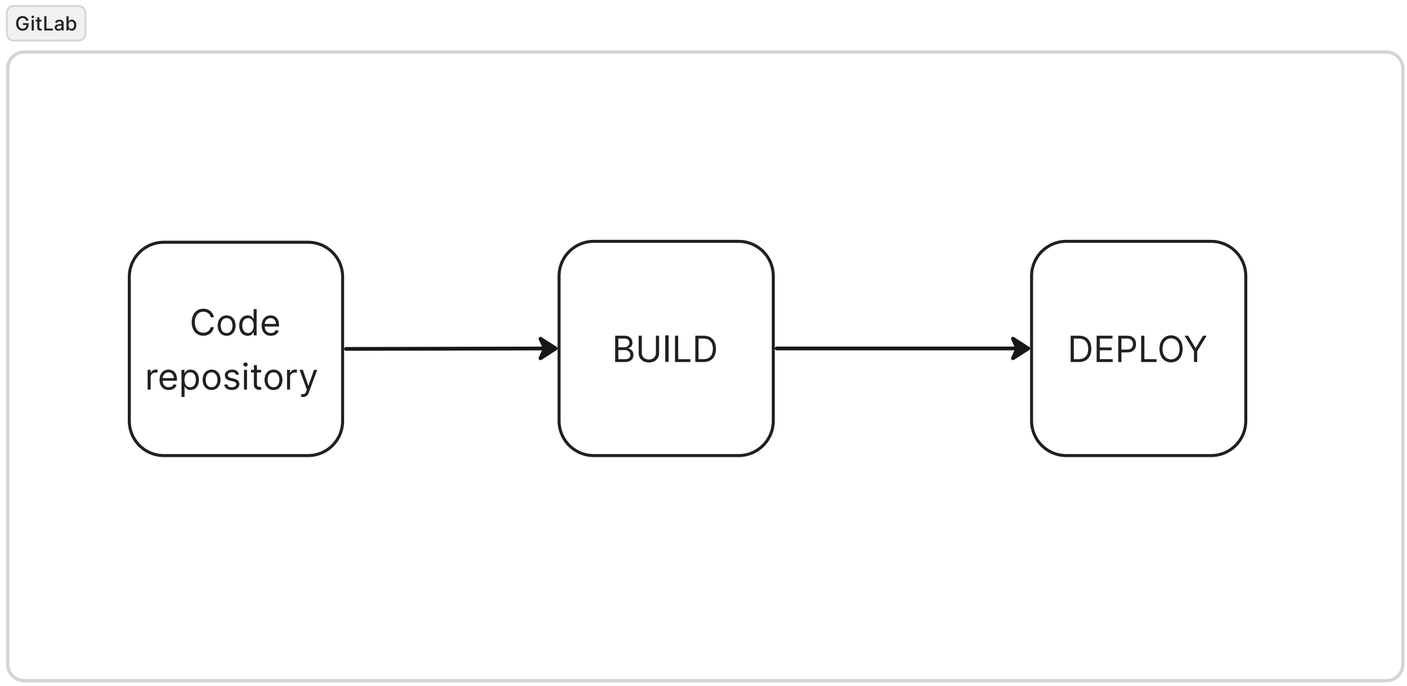
Как происходит процесс CI/CD сейчас

- Отсутсвует проверка исходного кода и артифактов на наличие ошибок и уязвимостей
- Сотрудник ИБ вынужден повторно прорабатывать модель угроз, из за-за того что не участвует в процессе
- Увеличивается стоимость и сроки исправления ошибок и уязвимостей
- Приложения не защищены от кибер-угроз после выпуска



Преимущества при внедрении практик DevSecOps и инструментов анализа

- Своевременное обнаружение проблем
- Сокращение длительности и стоимости исправления ошибок
- Увеличенная ценность продукта и его защищенность
- Минимизация рисков появления и эксплуатации уязвимостей в продукте

Как необходимо доработать процесс CI/CD

- Внедрение практик **DevSecOps** - это важный критерий безопасности
- Необходима интеграция проверок информационной безопасности в существующий процесс
- Практика взаимодействия разработки и ИБ на всех этапах жизненного цикла продукта
- Поэтапное наращивание количества проверок
- Развитие культуры разработки безопасного продукта, развитие кибер-иммунитета

План поэтапного внедрения иструментов анализа

- Интеграция с SCA сканером (OWASP Dependency-Check)
- Интеграция с SAST сканером (SonarQube)
- Добавление Quality Gates для merge requests
- Добавление собственных правил в Gitlab файл свойств (sonar-project.properties)
- Добавление доверенного хранилища с интегрированными проверками (Harbor)