

# Business Drive AppSec

Дмитрий Куколев



## О себе



Дмитрий Куколев



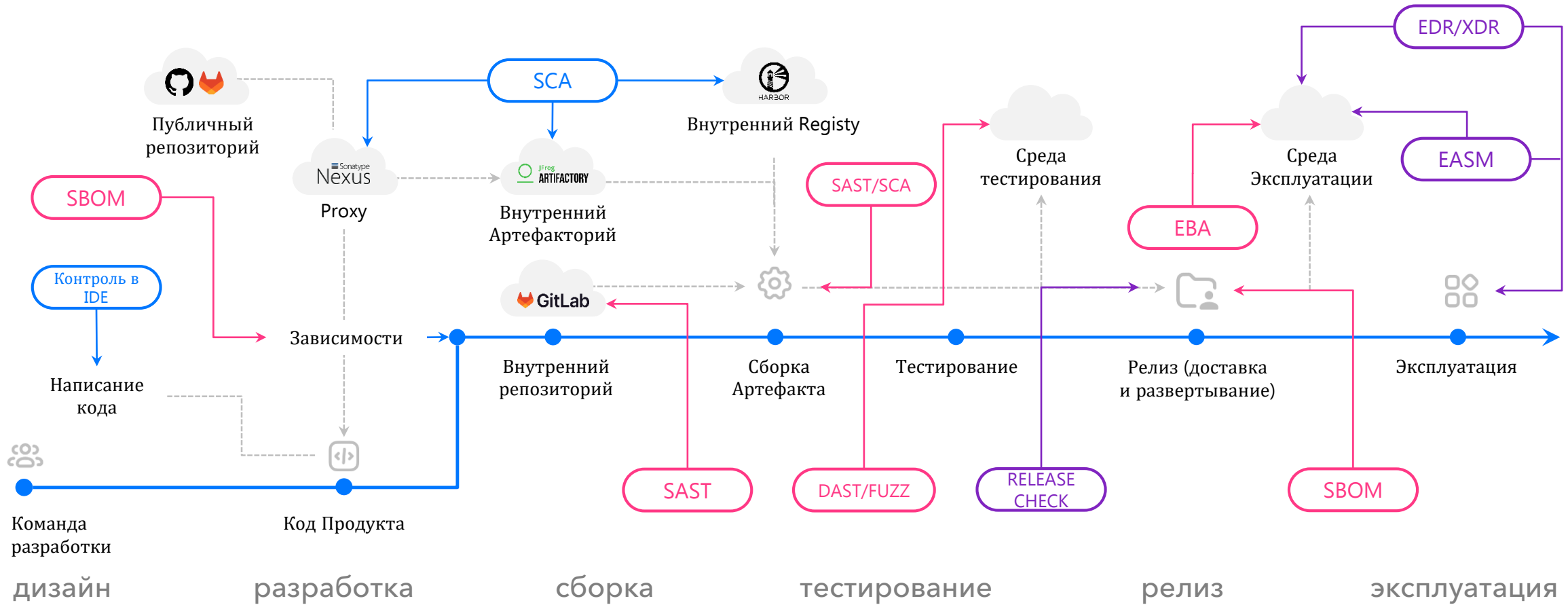
Директор департамента  
мониторинга и реагирования на  
инциденты ИБ



@dmitriykukolev

Опыт построения  
процессов безопасного  
производства 12+ лет

# Типовой процесс Производства и DSO



# Подход Business Driven AppSec

**Business Drive AppSec** — фокус на реальную защищенность продукта основанный на потребностях бизнеса



AppSec должен строиться исходя из наиболее актуальных угроз для Бизнеса в рамках их ИТ продукта

## Основные принципы Business Driven AppSec

- Фокус на угрозах
- Ранее «внедрение»
- Взаимодействие ИТ и ИБ

# Точки приложения усилий

1

Определить сценарии продукта

2

Определить угрозы и понять как мы можем найти уязвимости, критичные для бизнеса

3

Прозрачная интеграция в существующий процесс разработки

4

Постоянное взаимодействие с командами в роли Архитектора ИБ

5

Моделирование векторов атак и динамические тестирование на безопасность

# Этапы внедрения Business Driven AppSec

Процессы AppSec сильно отличаются от компании к компании и от продукта к продукту, но всегда можно выделить наиболее эффективные точки приложения усилий на первых этапах внедрения:

- Архитектура ИБ
- Secrets + SCA
- Динамическое тестирование

 Что надо сделать:

- Анализ бизнес-процессов и приоритизация критичных компонентов
- Установка метрик безопасности и требований к приложениям
- Внедрение инструментов

# Выводы

Подход построение AppSec, основанный на оценке реальных бизнес потребностей позволяет снизить трения между ИБ и ИТ, учитывая потребности бизнеса.

Внедрение практик AppSec на основе реальных потребностей бизнеса позволяет снизить затраты на внедрение инструментов и процессов ИБ и повысить продуктивность практической безопасности