Какие процессы приводят к результату?

Газизова Светлана
Swordfish Security

SWORDFISH
SECURITY

В современном мире часто говорят: либо процессы, либо результаты.

А что если, есть деятельность, в которой невозможно достичь результата без процесса?...

SWORDFISH
SECURITY

Почему есть смысл меня слушать?

#ктоя

руководитель направления аудита безопасной разработки: выстраиваю процессы, занимаюсь стратегией AppSec и всея, что около☺
автор и тренер курсов DevSecOps

#ктомы

архитекторы, консультанты, инженеры процессов безопасной разработки внедряли DevSecOps/Appsec в финтех, банки, ИТ-компании, здравоохранение, гос.сектор

SWORDFISH SECURITY

Агенда

1. Откуда к нам пришел DevSecOps?
2. Точно ли мы понимаем, границы безопасной разработки?
3. Что происходит после внедрения безопасной разработки?

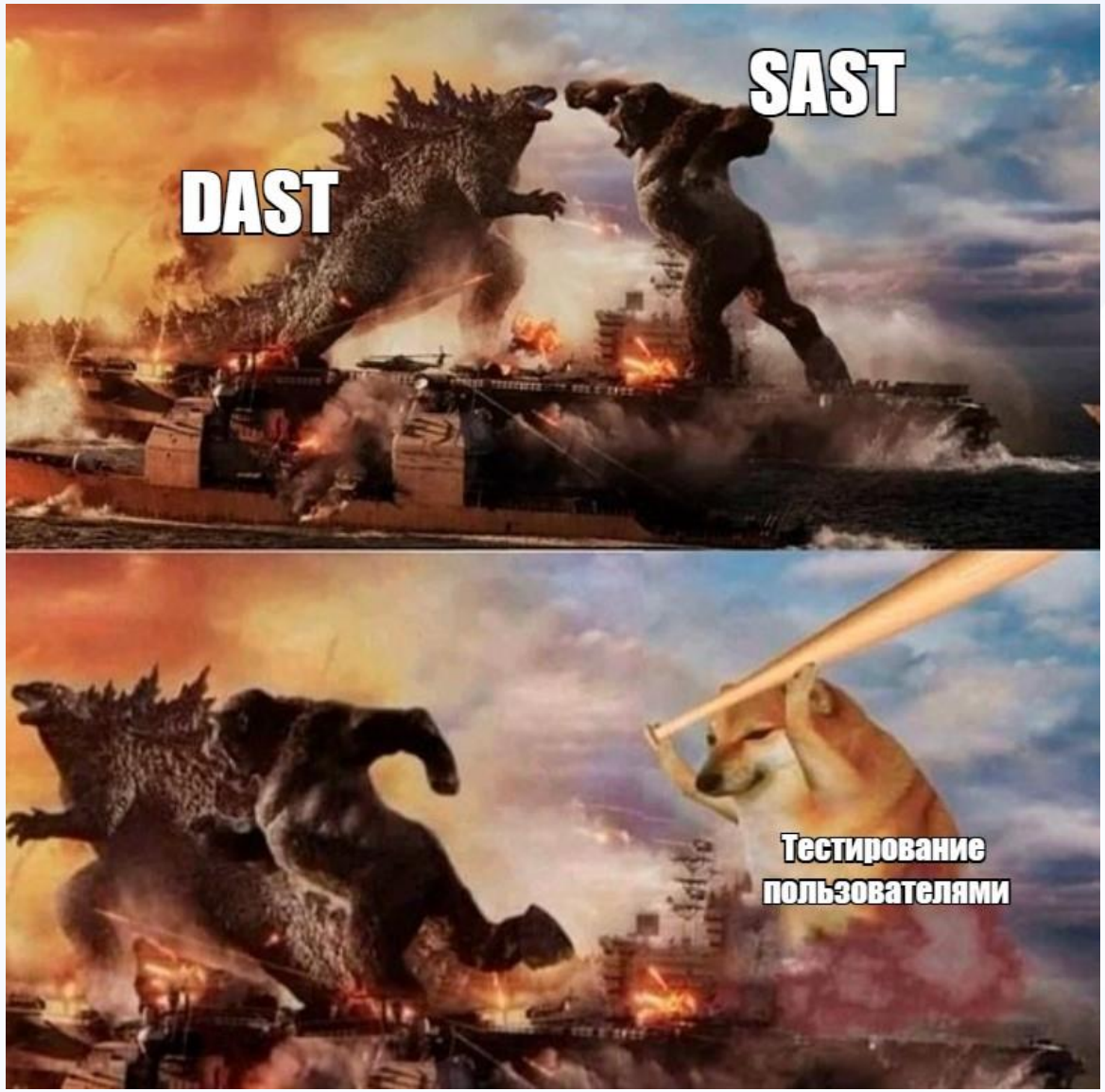
Что ты такое, DevSecOps?

Инструменты безопасной разработки **– есть**!

Инструменты безопасной разработки **– работают**!

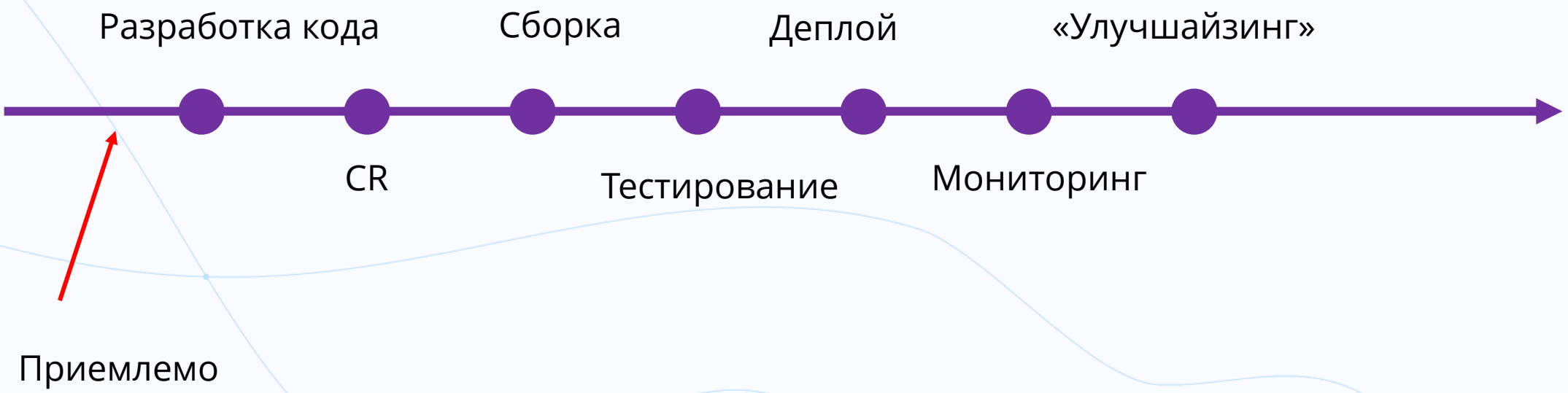
Люди **знают,** как работают инструменты и что с этим делать!

SWORDFISH SECURITY

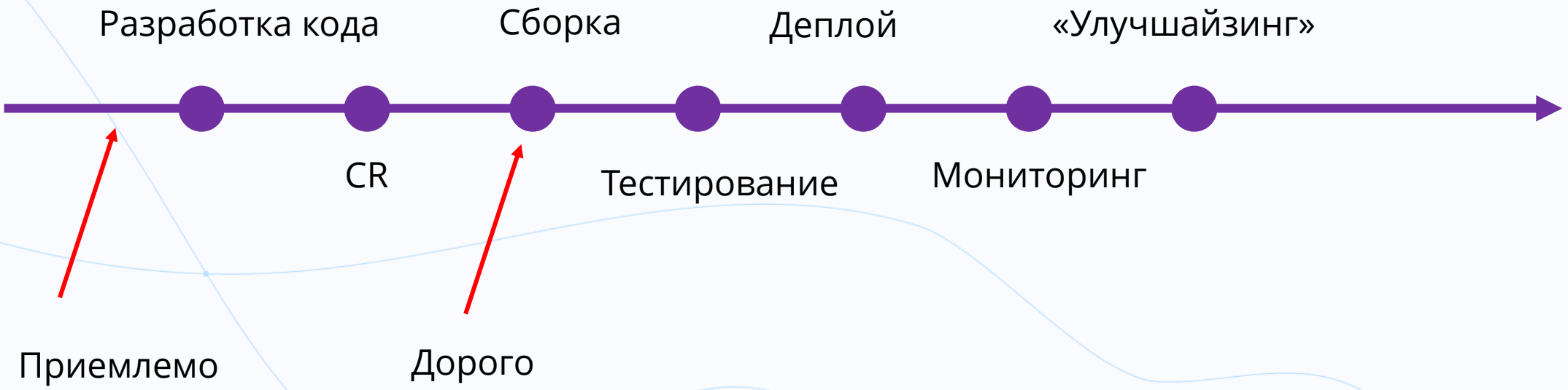


SWORDFISH
SECURITY

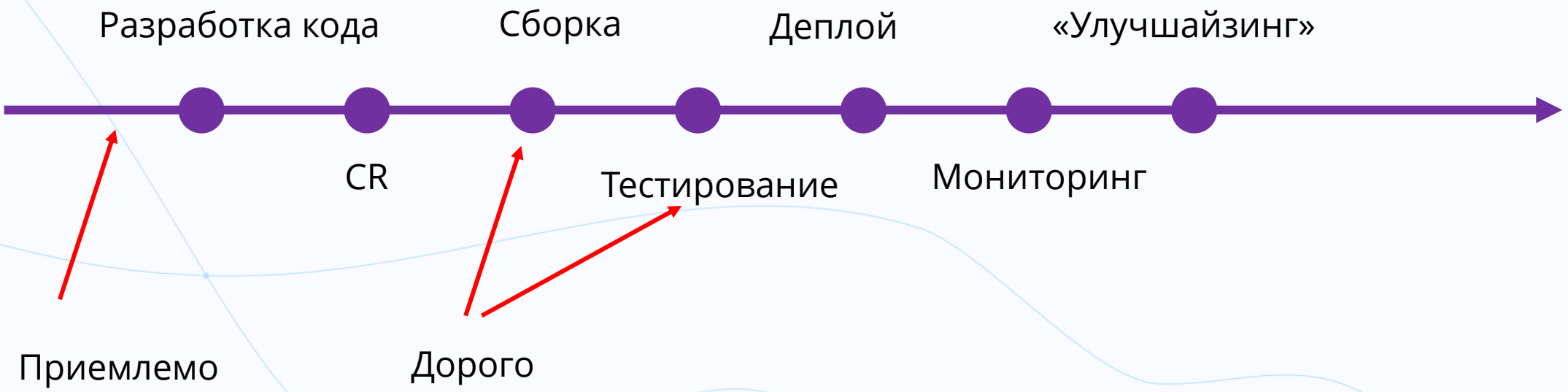
Shift left?



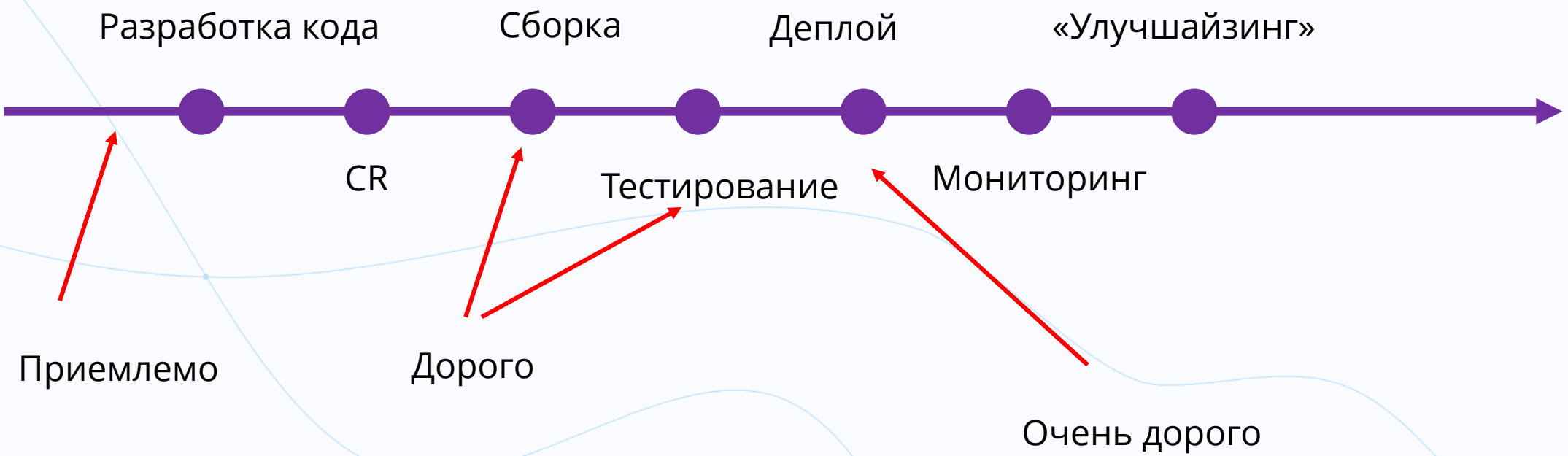
Shift left?



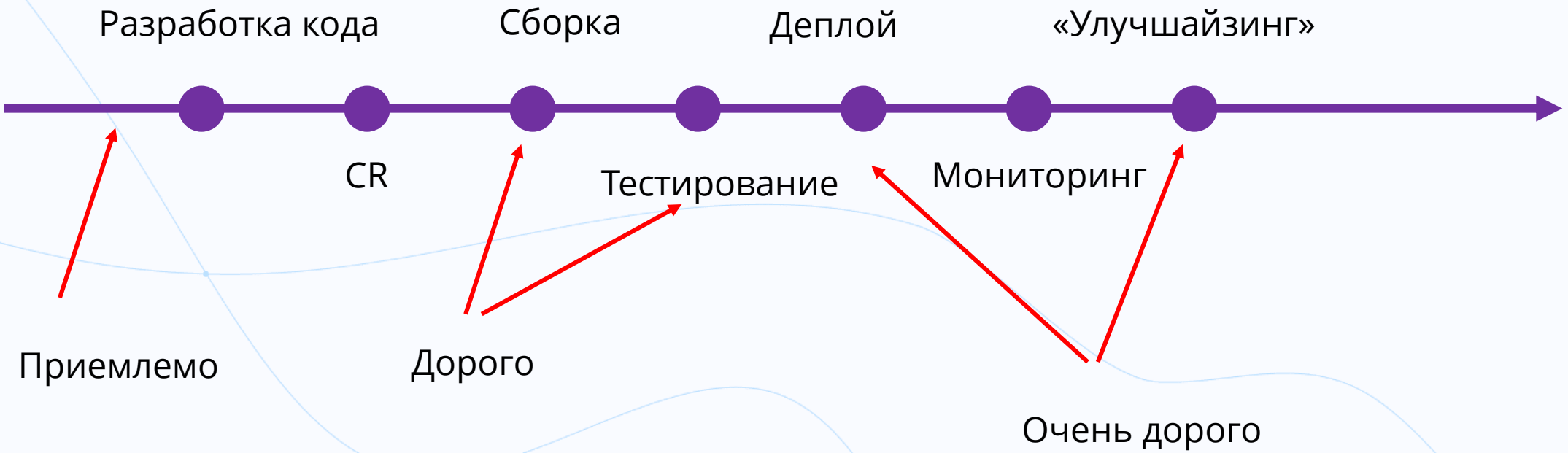
Shift left?



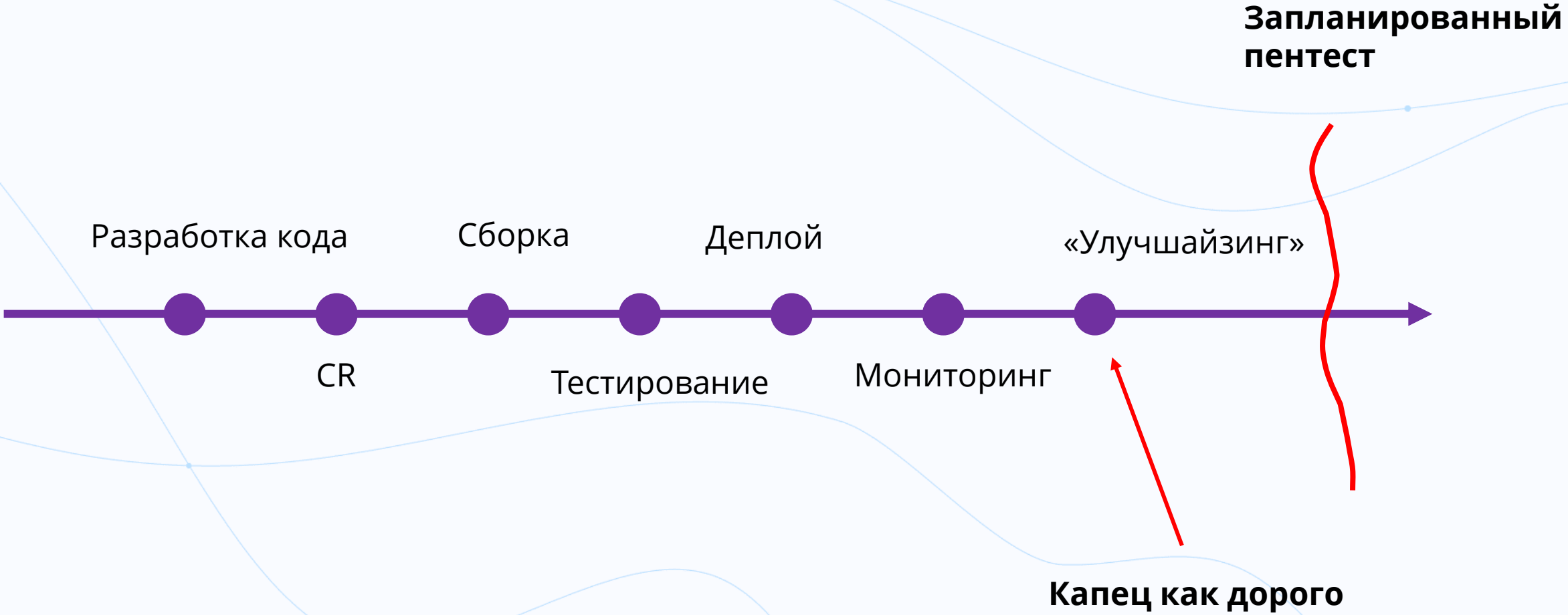
Shift left?



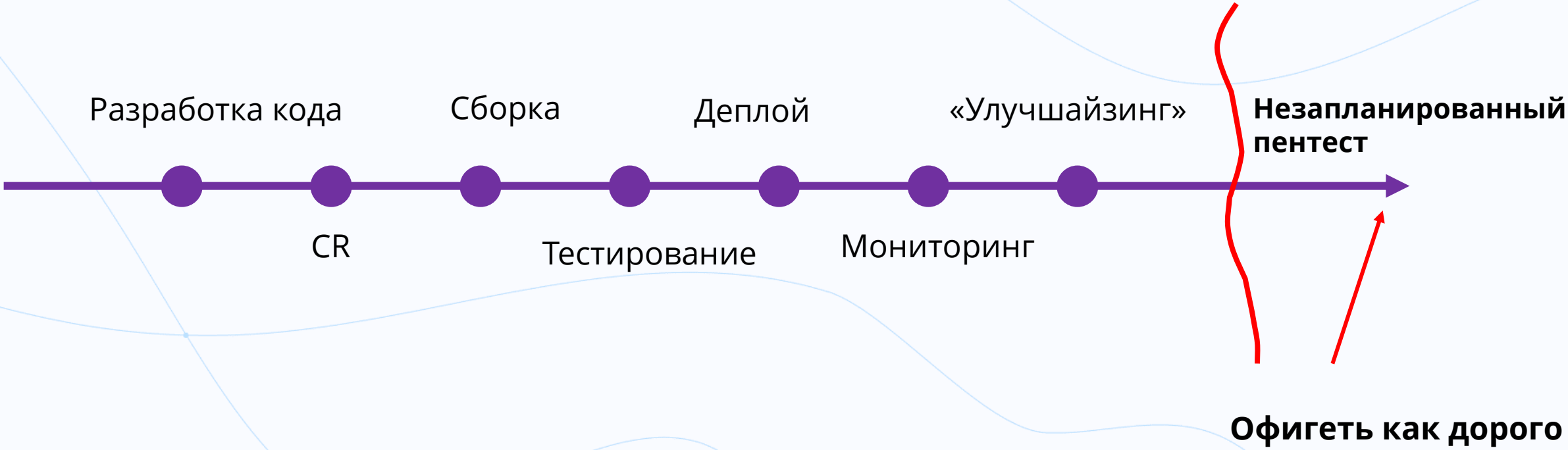
Shift left?



Shift right?

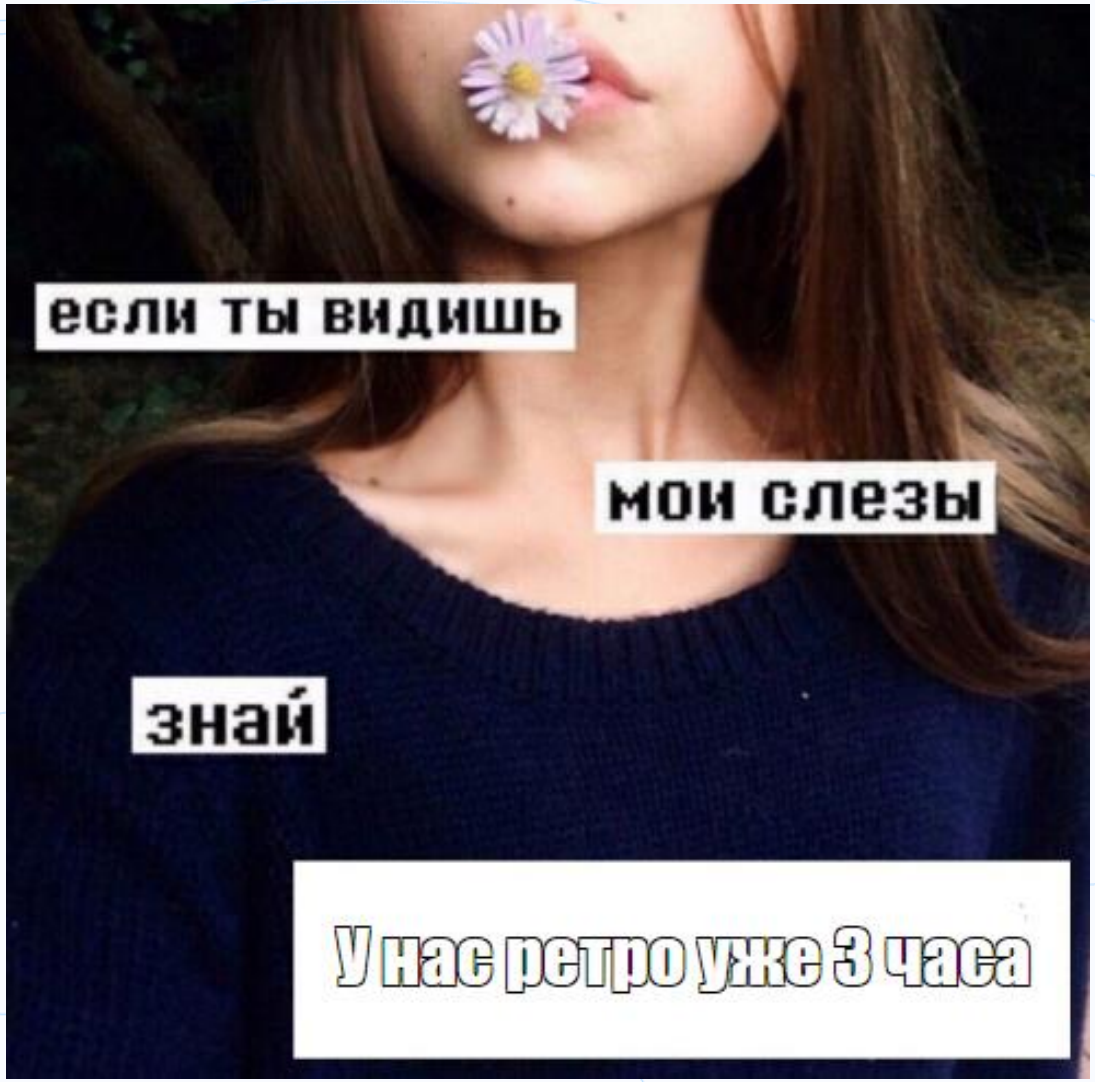


Shift right?



Угадай ~~мелодию~~ методологию

Угадай ~~мелодию~~ методологию

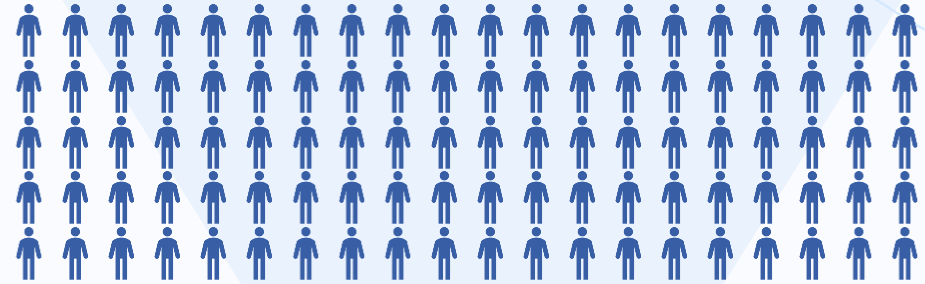


SWORDFISH SECURITY

Нас не хватает!

Соотношение

100:10:1



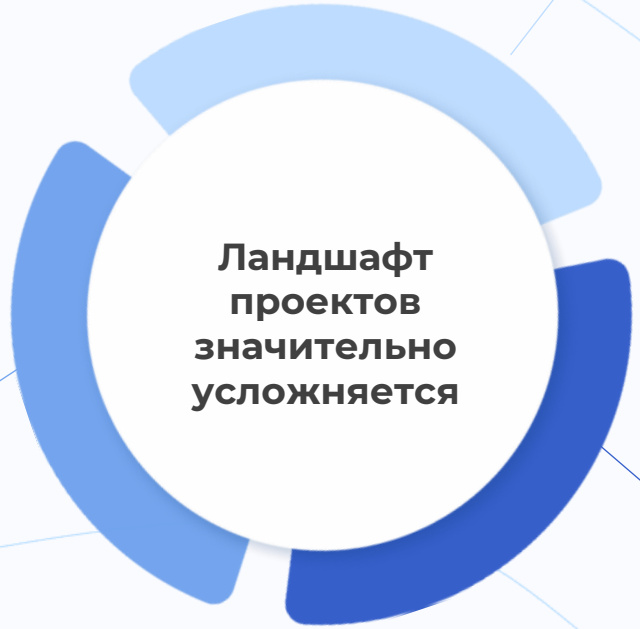
Разработчики ПО(Development)

Инженеры сопровождения (Operations)

Эксперт ИБ (Security)

SWORDFISH SECURITY

Посмотрим со стороны...



Бизнес

- Непрерывный рост количества программных продуктов, цифровых сервисов и приложений
- Рост количества вовлеченных сторон – Бизнес, Разработка ПО, Безопасность
- Скорость выпуска версий: непрерывность и безопасность функционирования цифровых сервисов становятся ключевыми критериями успеха в бизнесе

Кибербезопасность

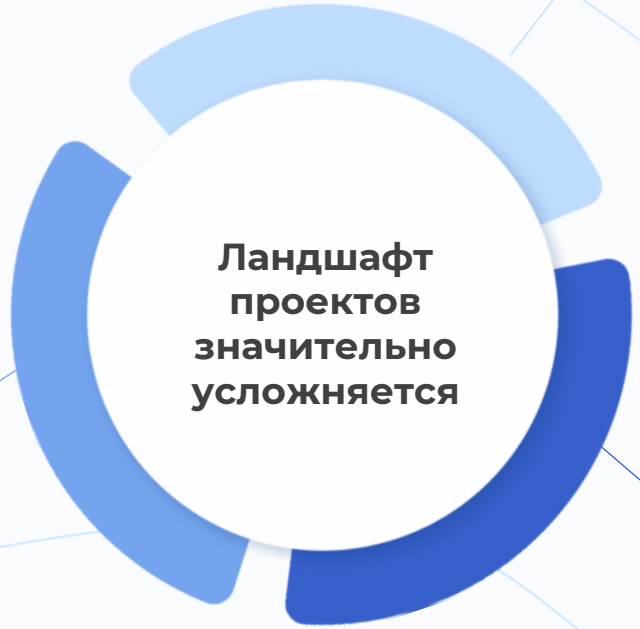
- Рост технического долга дефектов ИБ
- Большое количество ложных уязвимостей
- Нехватка квалифицированных кадров
- Невозможность управления средствами ИБ вручную

Разработка ПО

- Сокращение циклов разработки ПО
- Увеличение количества релизов
- Превращение архитектуры приложений в микросервисную, рост общего количества артефактов ПО
- Появление распределенных команд разработки

SWORDFISH SECURITY

Посмотрим со стороны...



Кибербезопасность

- Рост технического долга дефектов ИБ
- Большое количество ложных уязвимостей
- Нехватка квалифицированных кадров
- Невозможность управления средствами ИБ вручную

Бизнес

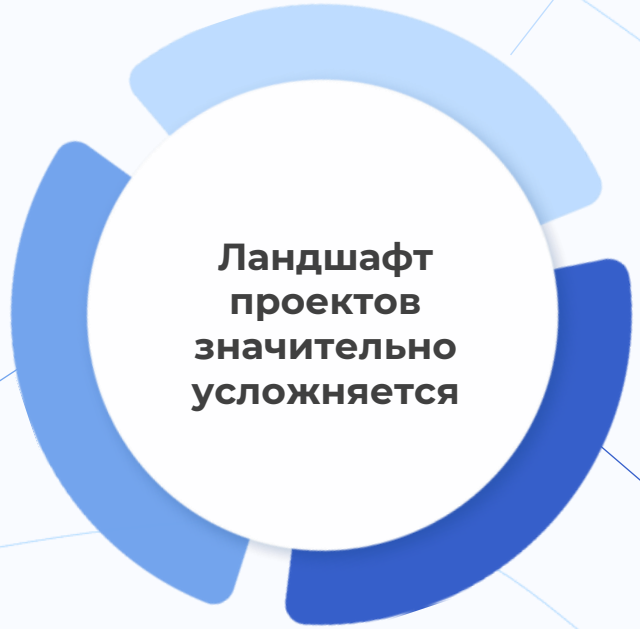
- Непрерывный рост количества программных продуктов, цифровых сервисов и приложений
- Рост количества вовлеченных сторон – Бизнес, Разработка ПО, Безопасность
- Скорость выпуска версий: непрерывность и безопасность функционирования цифровых сервисов становятся ключевыми критериями успеха в бизнесе

Разработка ПО

- Сокращение циклов разработки ПО
- Увеличение количества релизов
- Превращение архитектуры приложений в микросервисную, рост общего количества артефактов ПО
- Появление распределенных команд разработки

SWORDFISH SECURITY

Посмотрим со стороны...



Кибербезопасность

- Рост технического долга дефектов ИБ
- Большое количество ложных уязвимостей
- Нехватка квалифицированных кадров
- Невозможность управления средствами ИБ вручную

Бизнес

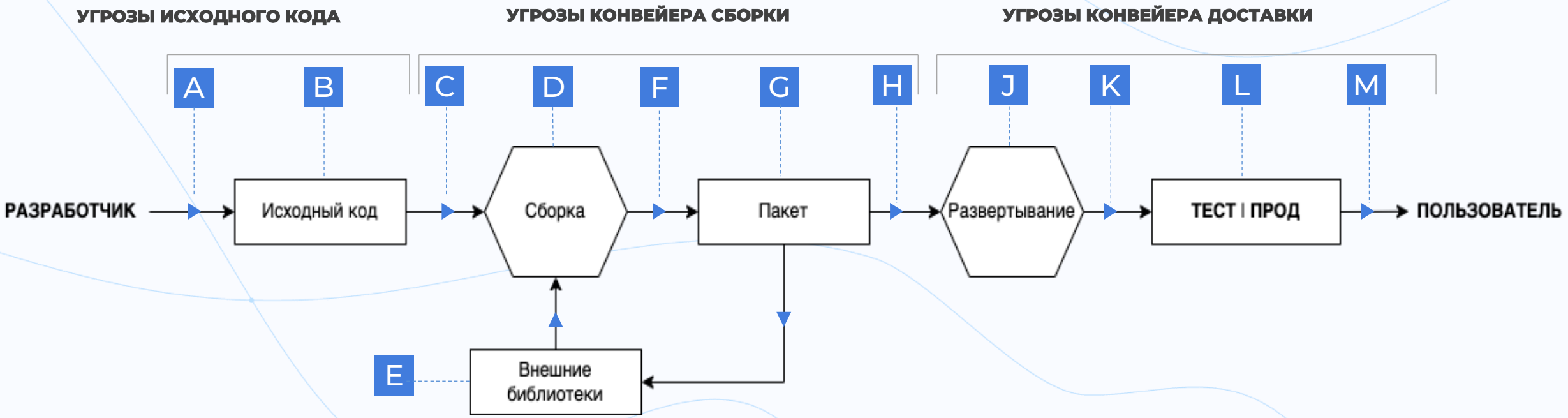
- Непрерывный рост количества программных продуктов, цифровых сервисов и приложений
- Рост количества вовлеченных сторон – Бизнес, Разработка ПО, Безопасность
- Скорость выпуска версий: непрерывность и безопасность функционирования цифровых сервисов становятся ключевыми критериями успеха в бизнесе

Разработка ПО

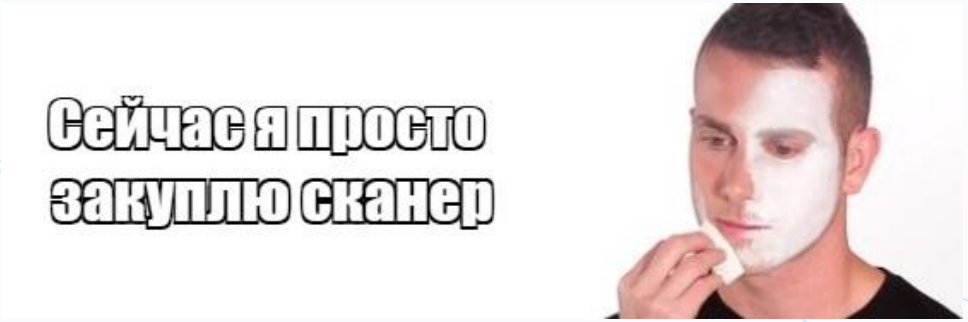
- Сокращение циклов разработки ПО
- Увеличение количества релизов
- Превращение архитектуры приложений в микросервисную, рост общего количества артефактов ПО
- Появление распределенных команд разработки

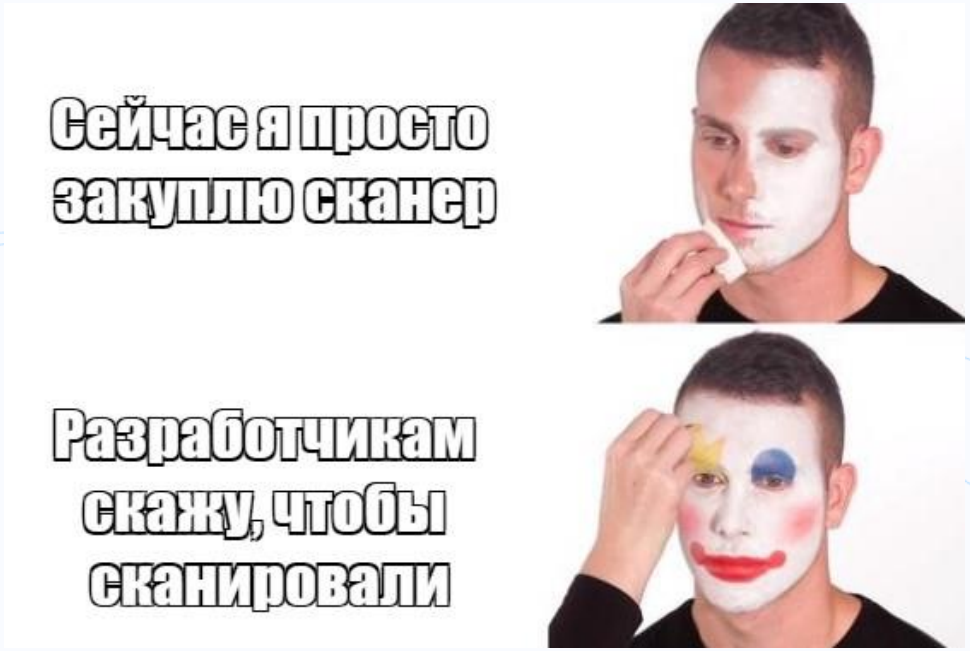
SWORDFISH SECURITY

Восстание машин



SWORDFISH SECURITY

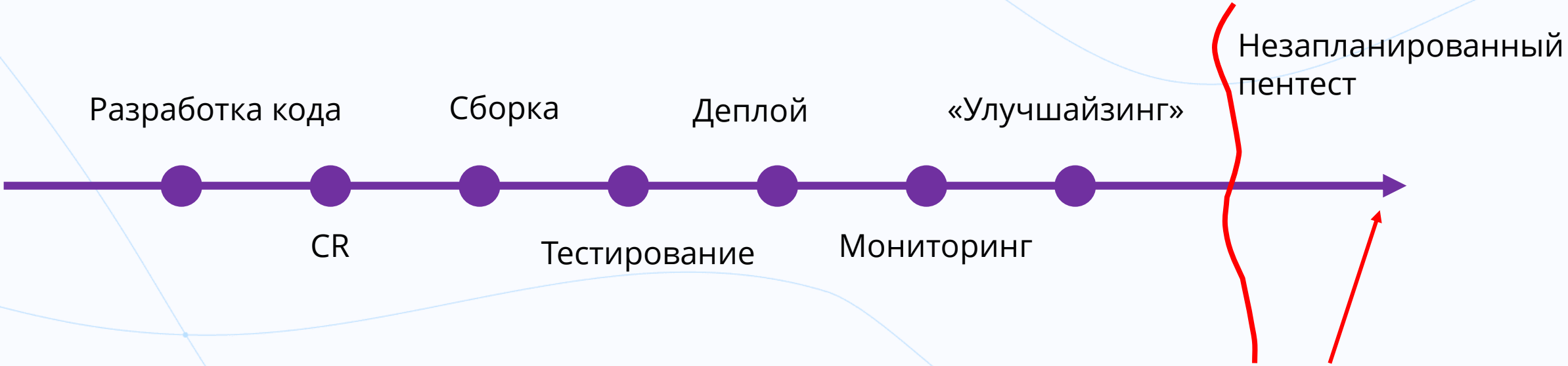

Сейчас я просто
закуплю сканер


Сейчас я просто закуплю сканер
Разработчикам скажу, чтобы сканировали


Сейчас я просто закуплю сканер
Разработчикам скажу, чтобы сканировали
Скажу, что соблюдаем все требования

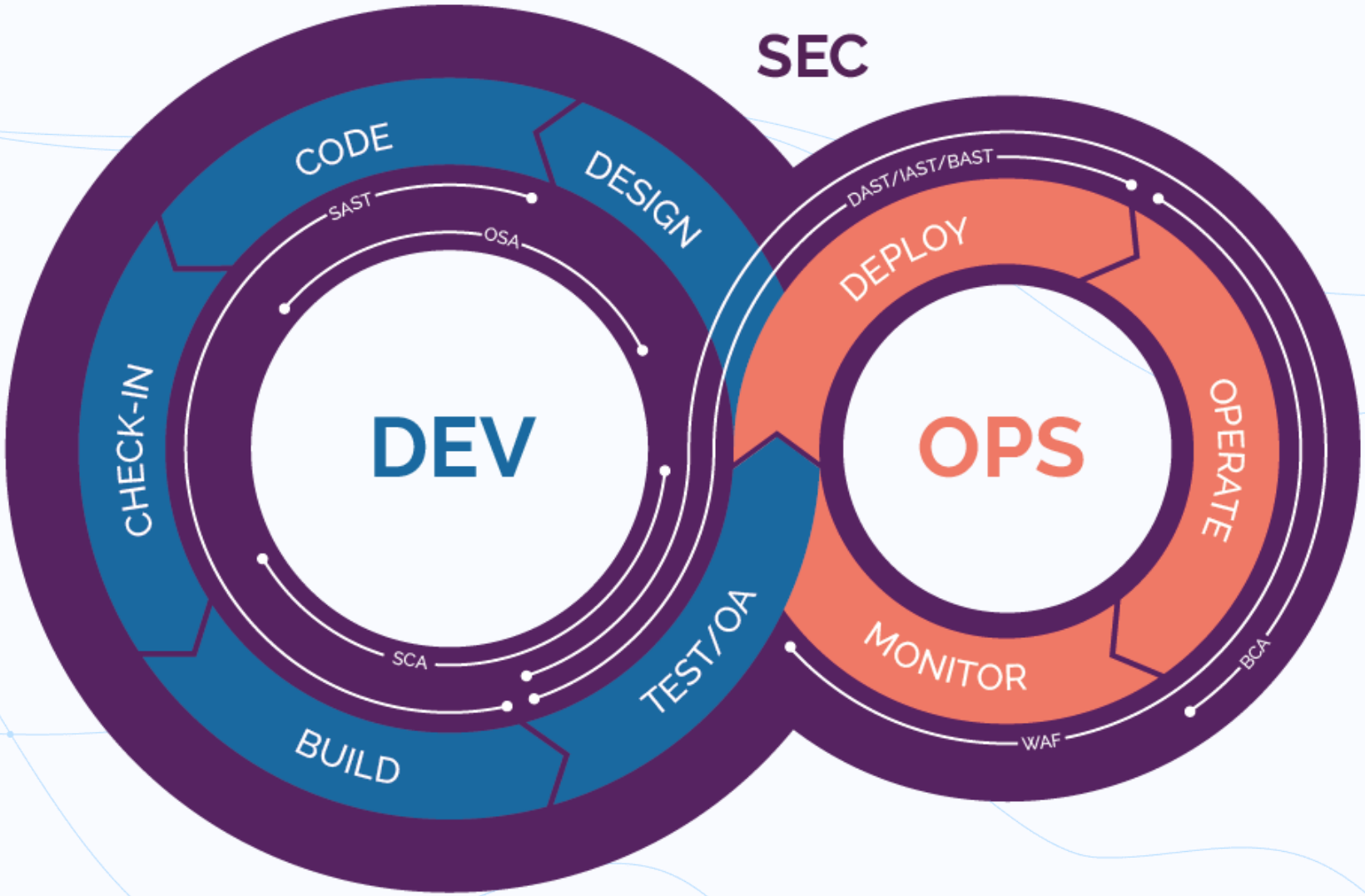

Сейчас я просто закуплю сканер
Разработчикам скажу, чтобы сканировали
Скажу, что соблюдаем все требования
Вау, AppSec это так легко

Кажется, мы это уже где-то видели...



Колоссально дорого

SWORDFISH SECURITY

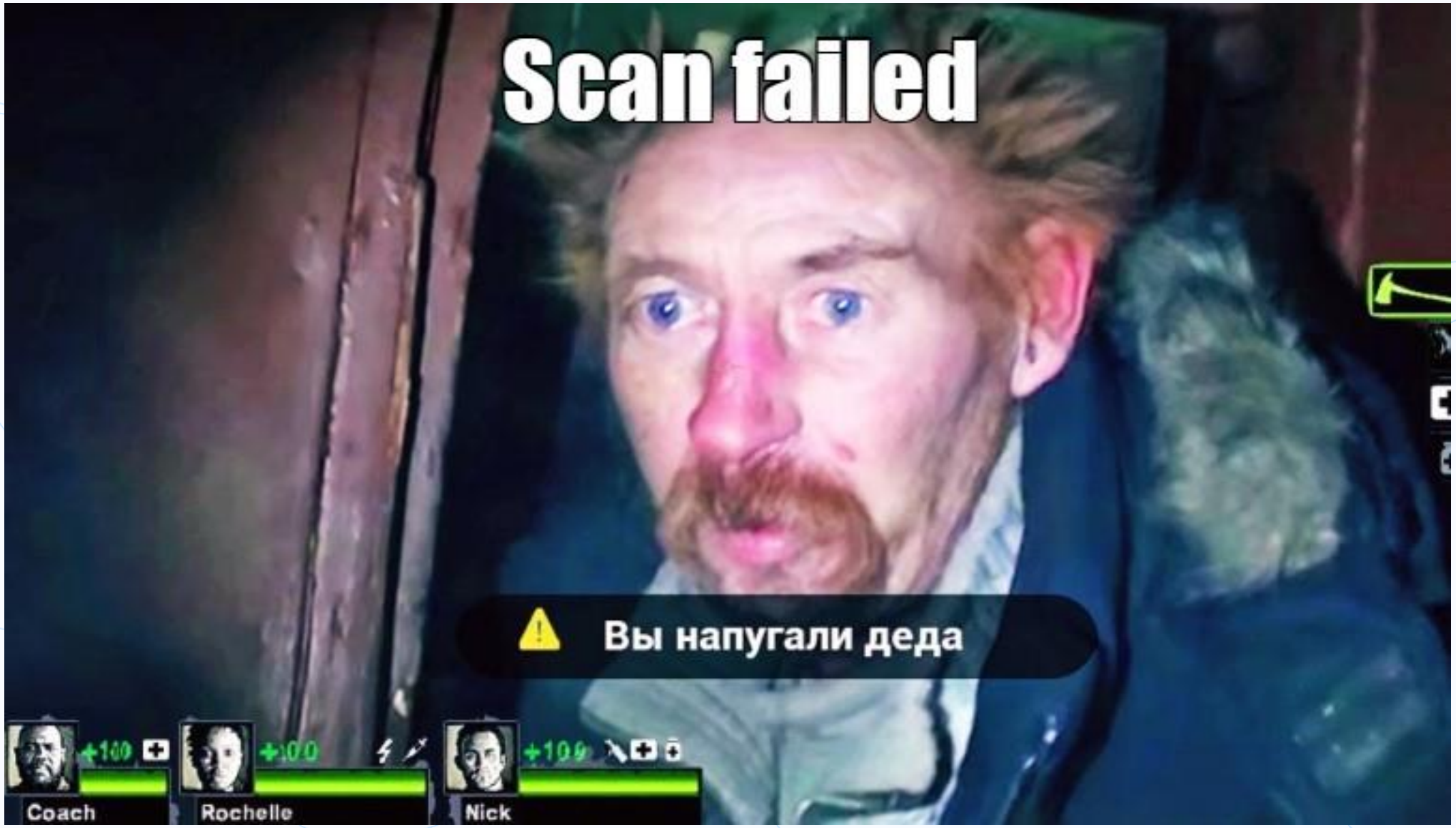


SWORDFISH
SECURITY

SWORDFISH
SECURITY

А какой он, этот ваш DevSecOps?...


Я вам
ЗАПРЕЩАЮ
ДЕПЛОИТЬ



SWORDFISH SECURITY

СЛАБАЯ АУРА

Сканирование завершено успешно

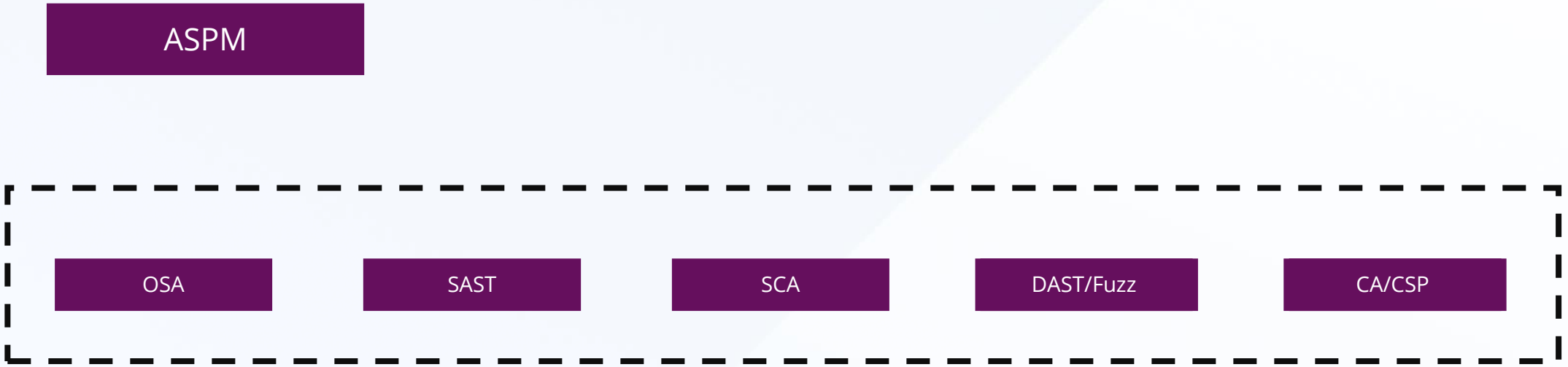
СИЛЬНАЯ АУРА

2880
CRITICAL

2234
HIGH

Что нужно для обеспечения процесса?

Чем меньше ресурсов, тем правильнее надо делать сначала.



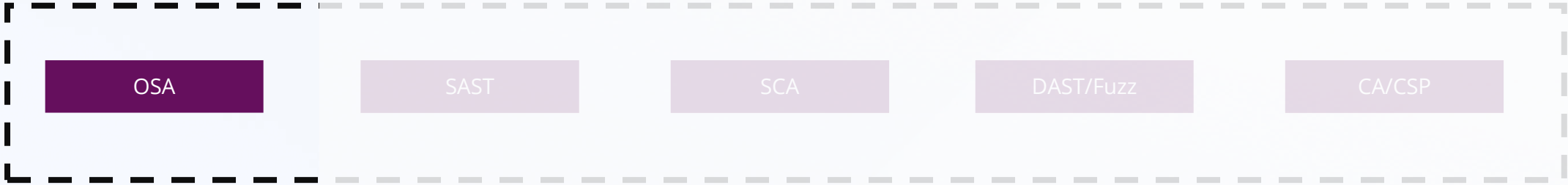
SWORDFISH SECURITY

ASPM

Практика построения полностью автоматизированного, сквозного процесса оркестрации всех инструментальных средств DevSecOps и управления технологическими конвейерами проверок ИБ. В рамках данной практики формируется технологический контур, позволяющий управлять практиками ИБ для всего портфеля разрабатываемых приложений, обеспечивается корреляция уязвимостей ПО и реализуются механизмы сбора и консолидации данных для автоматизированного формирования метрик защищенности ПО.

SWORDFISH SECURITY

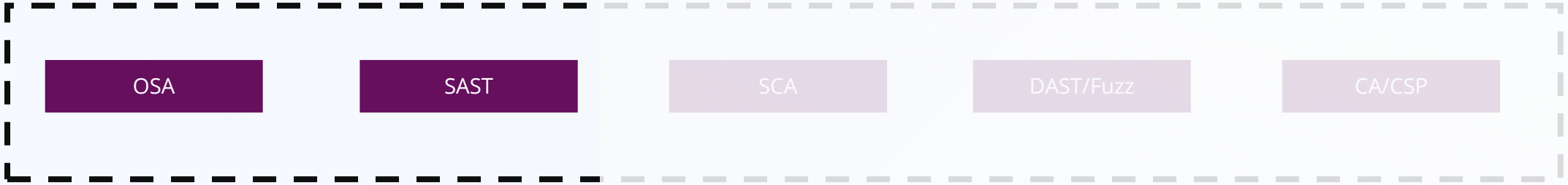
ASPM



Практика анализа библиотек и компонент с открытым исходным кодом, попадающих в контур разработки ПО как на наличие задекларированных уязвимостей так и на лицензионную чистоту.

SWORDFISH SECURITY

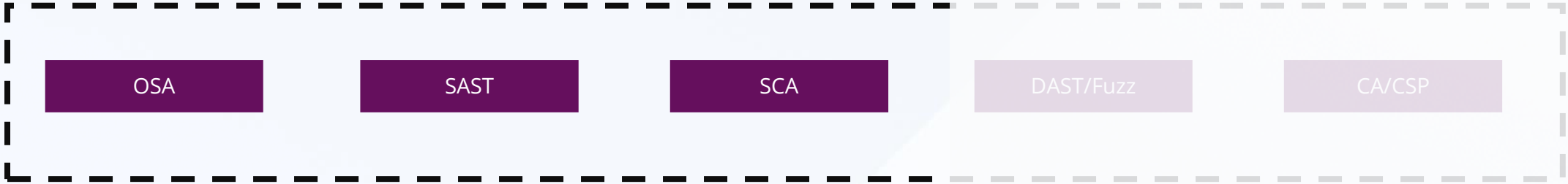
ASPM



Практика анализа исходного кода приложений для обнаружения уязвимостей на фазе непосредственного кодинга в производственном цикле разработки ПО.

SWORDFISH SECURITY

ASPM

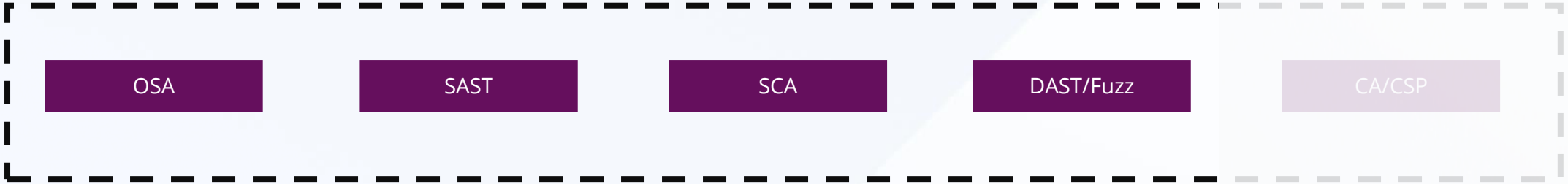


Позволяет контролировать артефакты сборки в процессе всего цикла разработки ПО.

Обеспечивает непрерывный мониторинг появления новых уязвимостей в сторонних компонентах и библиотеках в среде промышленной эксплуатации

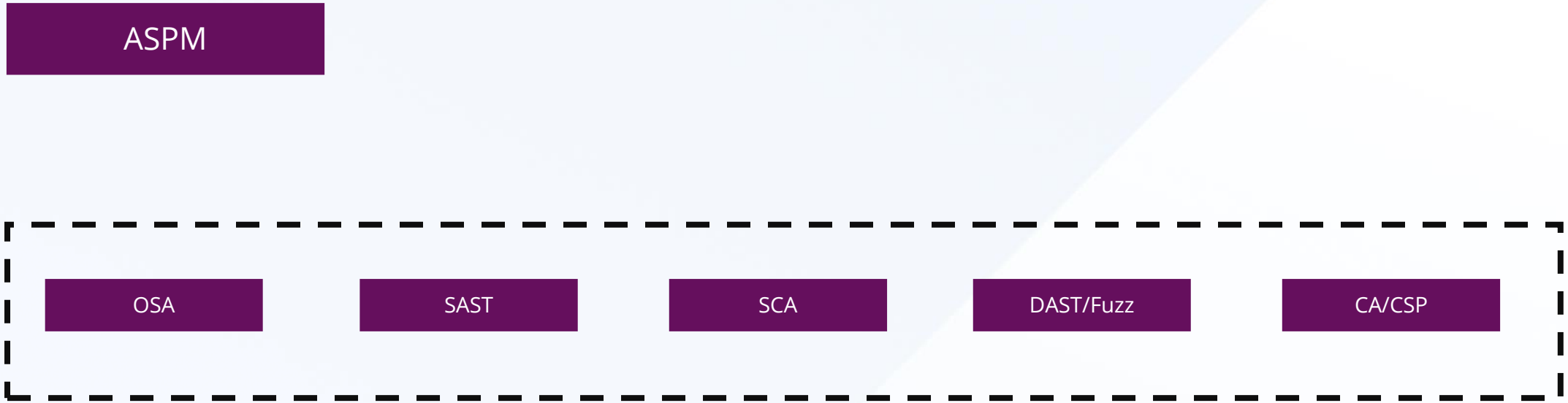
SWORDFISH SECURITY

ASPM



Практика динамического анализа и оценки защищенности уже собранных мобильных и веб-приложений без доступа к исходному коду

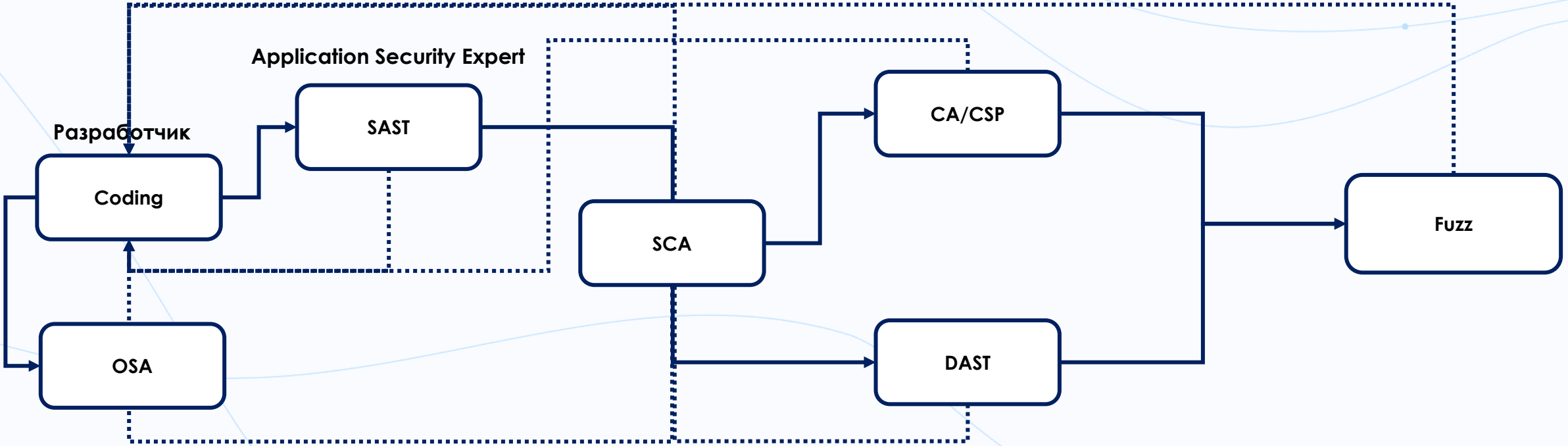
SWORDFISH SECURITY



Практика автоматизированного анализа контейнеров, применяемая для уже собранных дистрибутивов, скомпилированных приложений и docker-образов, в том числе и при недоступности исходного кода для проверок ИБ на поздних этапах цикла разработки ПО

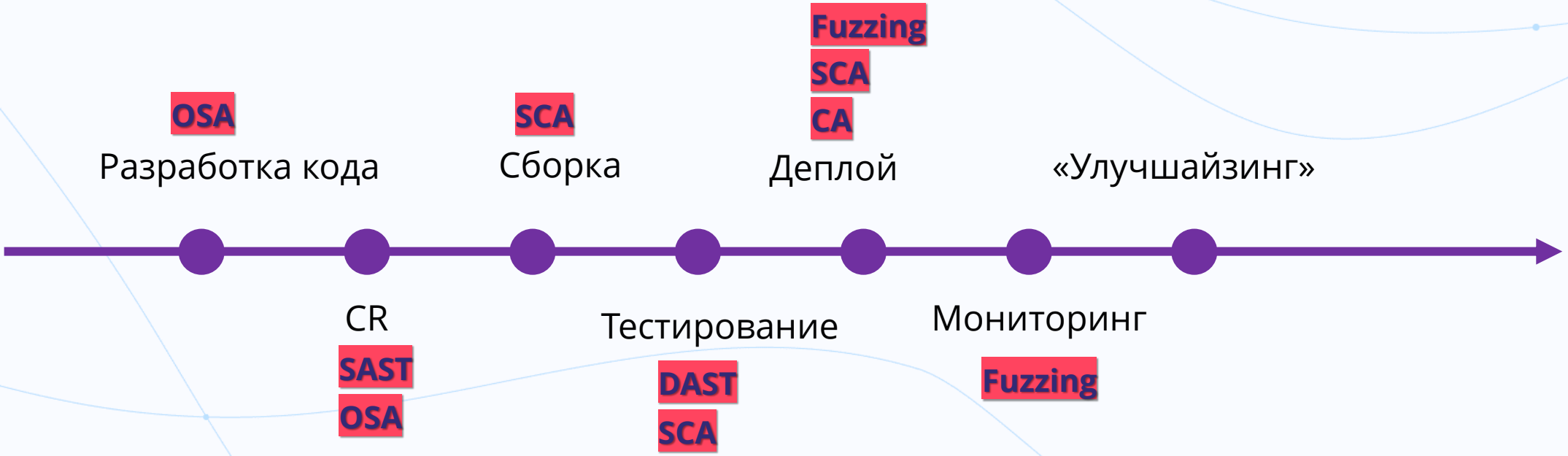
SWORDFISH SECURITY

S-SDL процесс

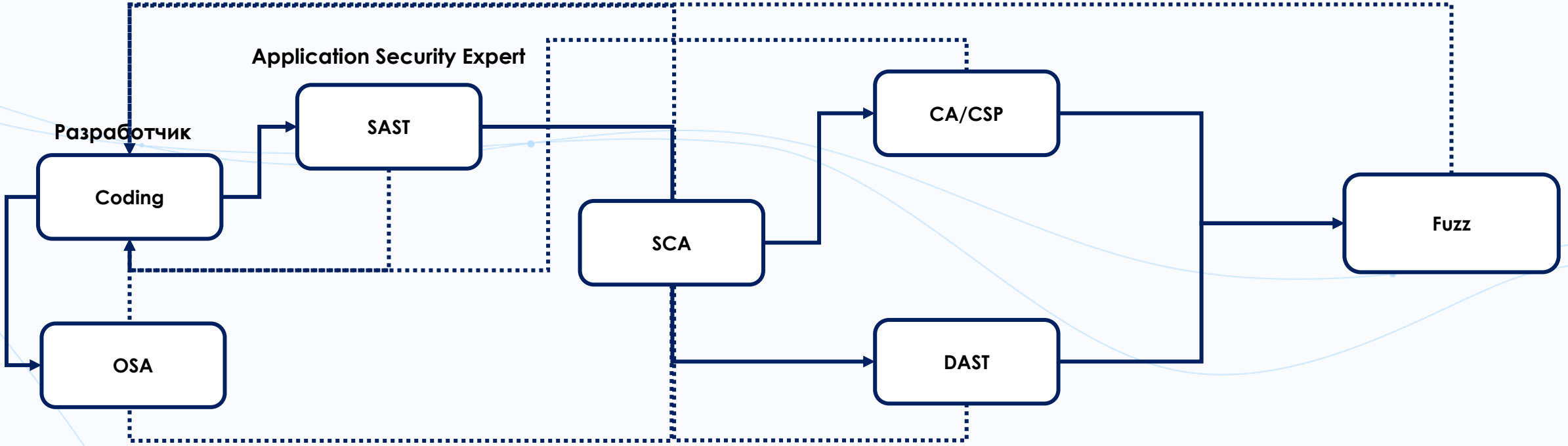


SWORDFISH SECURITY

Как «лежат» инструменты



SWORDFISH SECURITY



Fuzzing
SCA
CA

OSA

SCA

Разработка кода — Сборка — Деплой — «Улучшайзинг»

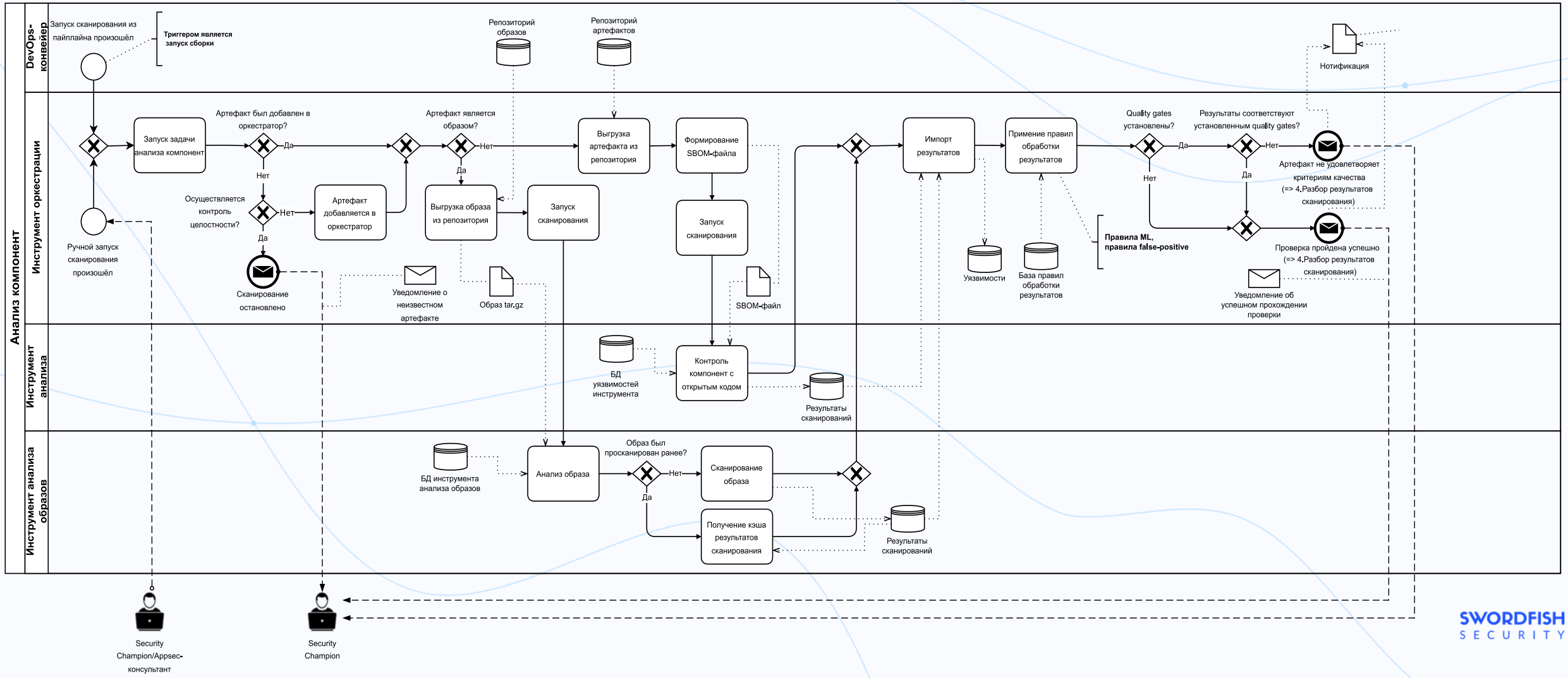
CR
SAST
OSA

Тестирование
DAST
SCA

Мониторинг
Fuzzing

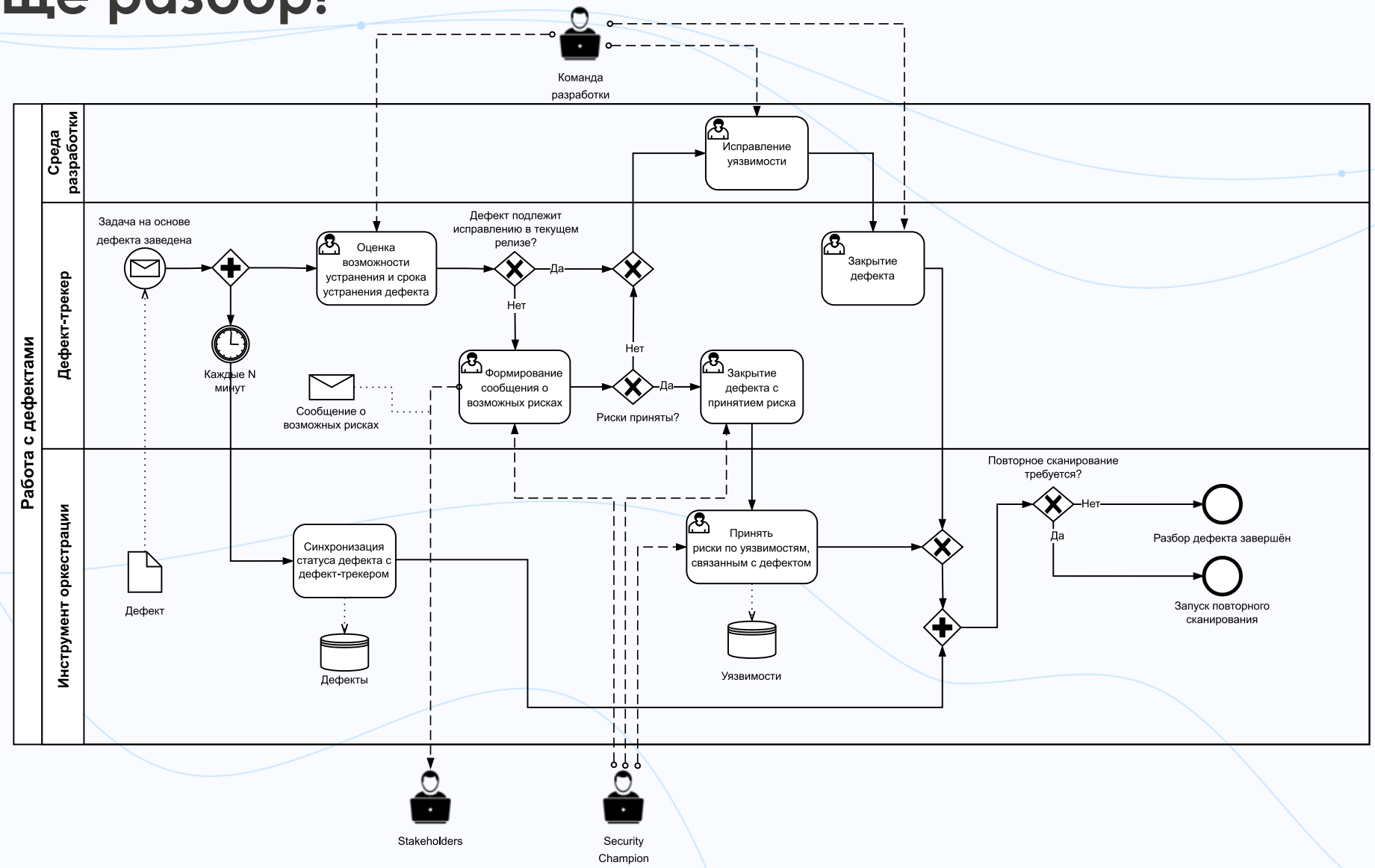
SWORDFISH SECURITY

А ведь внутри кое-что еще...

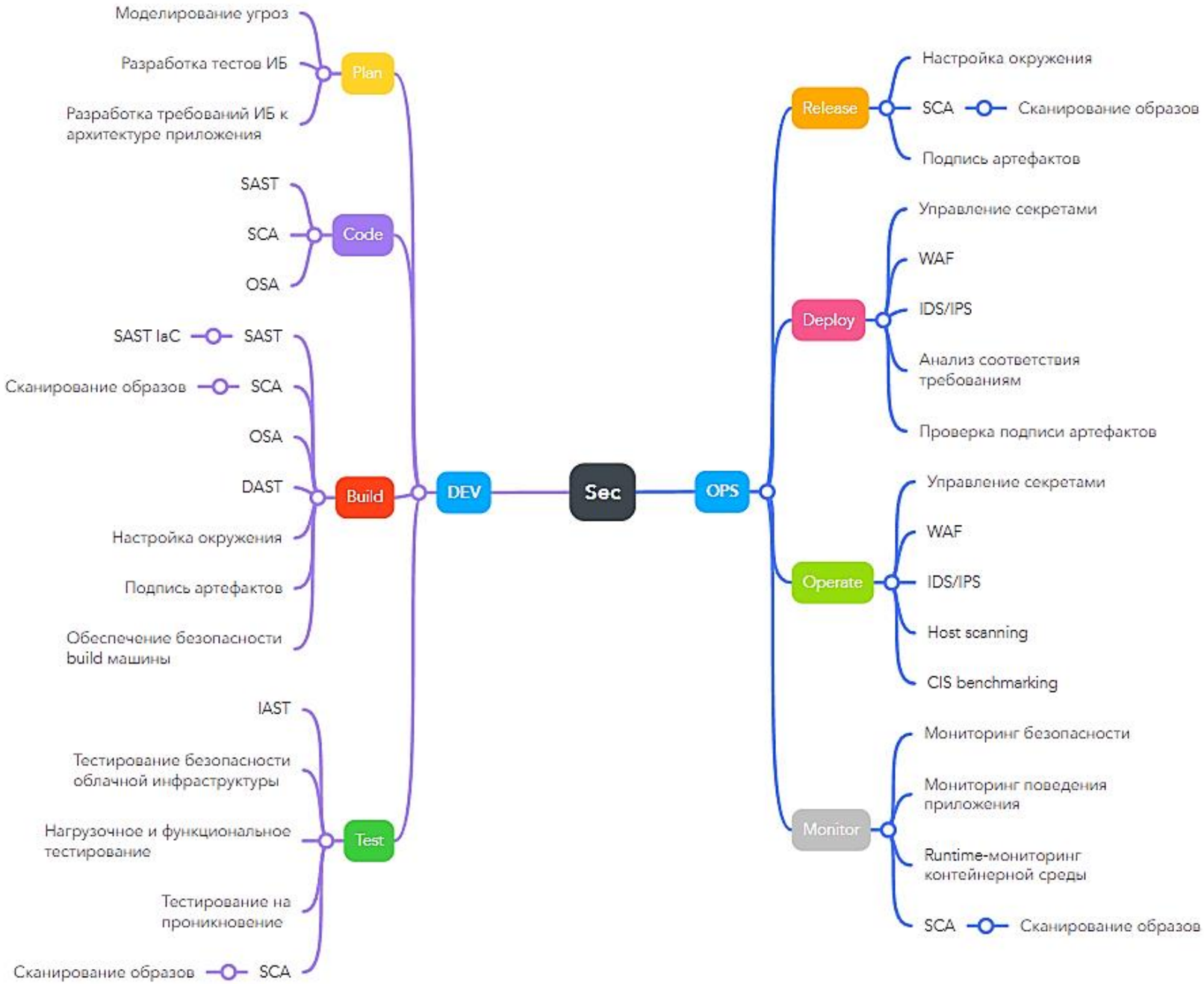


SWORDFISH SECURITY

И есть еще разбор!



SWORDFISH SECURITY


Sec
DEV
Plan
Моделирование угроз
Разработка тестов ИБ
Разработка требований ИБ к архитектуре приложения
Code
SAST
SCA
OSA
Build
SAST IaC
SAST
Сканирование образов
SCA
OSA
DAST
Настройка окружения
Подпись артефактов
Обеспечение безопасности build машины
Test
IAST
Тестирование безопасности облачной инфраструктуры
Нагрузочное и функциональное тестирование
Тестирование на проникновение
Сканирование образов
SCA
OPS
Release
Настройка окружения
SCA
Сканирование образов
Подпись артефактов
Deploy
Управление секретами
WAF
IDS/IPS
Анализ соответствия требованиям
Проверка подписи артефактов
Operate
Управление секретами
WAF
IDS/IPS
Host scanning
CIS benchmarking
Monitor
Мониторинг безопасности
Мониторинг поведения приложения
Runtime-мониторинг контейнерной среды
SCA
Сканирование образов

И есть еще разбор!

Да-да, я знаю, что ничего не видно!

А есть ли релизы после внедрения?...


Аппсек
Заблокировать пайп
Выпустить релиз с критами


Когда пытаешься понять, где FP
А где уязвимость


Ну что, уже все инструменты внедрил?

Но это все, конечно, не правда;-)

Спасибо, что вы здесь!

Визитка

Кое-что невошедшее

@APPSECJOURNEY

За шаблоны для мемов спасибо: https://www.meme-arsenal.com

SWORDFISH SECURITY