МТС Hello, Conference!_

Архитектур@ програм*ных систем

Научно-техническая конференция №8 / 7 февраля 2020

Андрей Пьянков
Денис Шефановский

- главный архитектор, центр корпоративной архитектуры
- директор по ИБ
- ПАО “МТС”, ООО “МТС ИТ”

Поговорим о DevSecOps

- Практики DevSecOps, что они могут дать компании и продуктовой команде
- Чем управляет информационная безопасность и чем она занимается
- Какие модели организации взаимодействия ИБ и команд

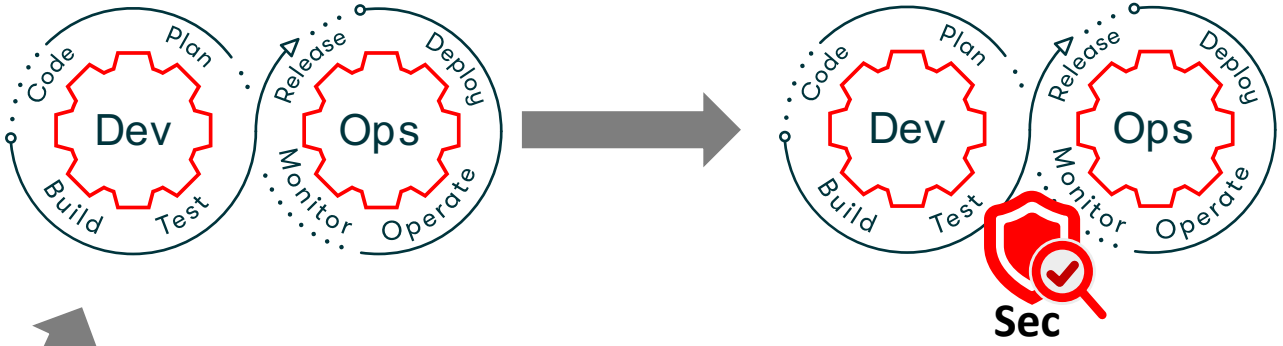
Собственно, а почему безопасность?

- От вопросов безопасности никуда не деться.
- Забота о безопасности потребителя всё больше ложиться на компании разрабатывающие информационные продукты.
- По мнению Национального института стандартов и технологий США (NIST), устранения уязвимостей при проектировании в десятки раз менее затратны, чем после выпуска продукта.

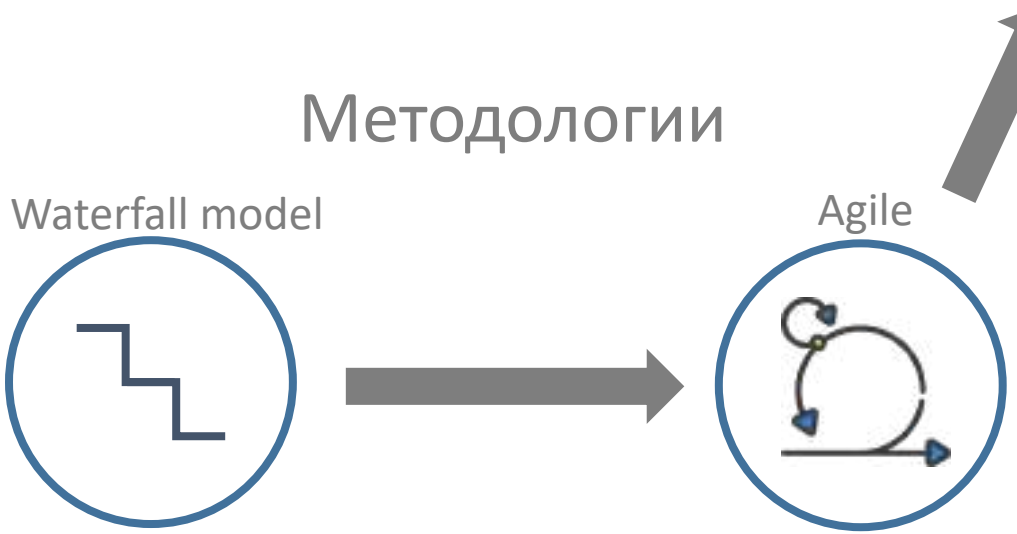
Экскурс в историю

Развитие методологий разработки ПО обусловлено потребностями бизнеса

Практики

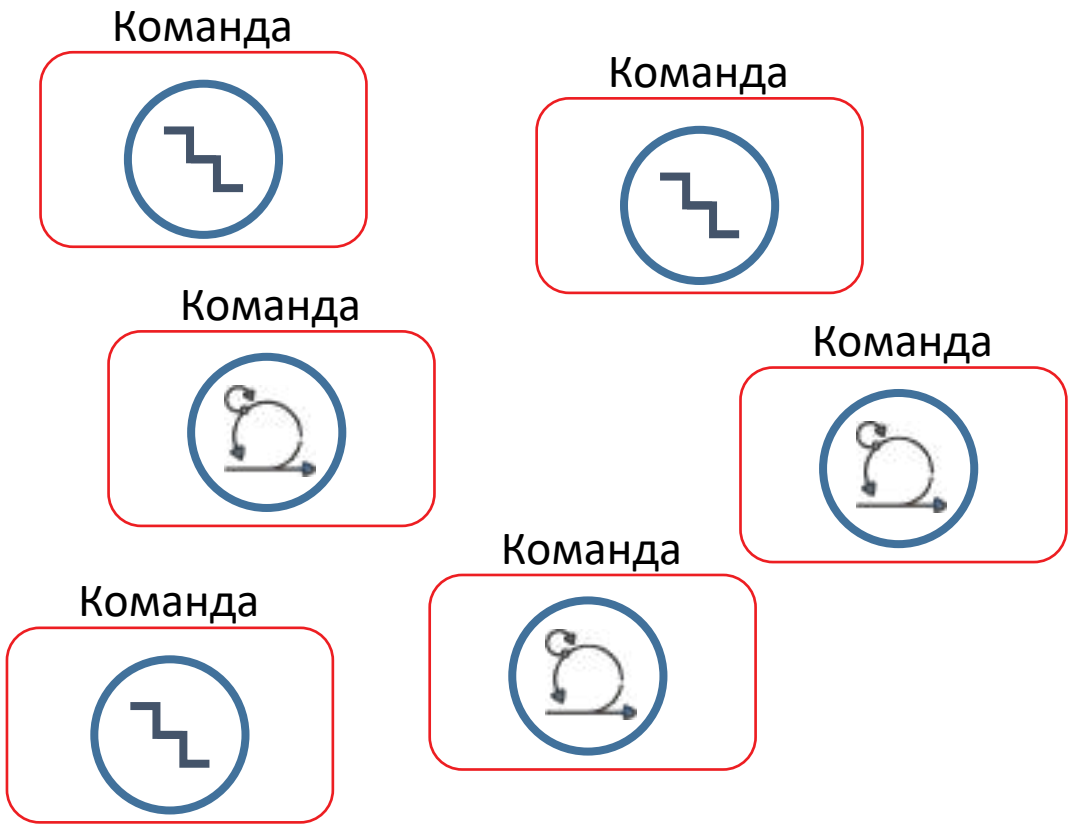


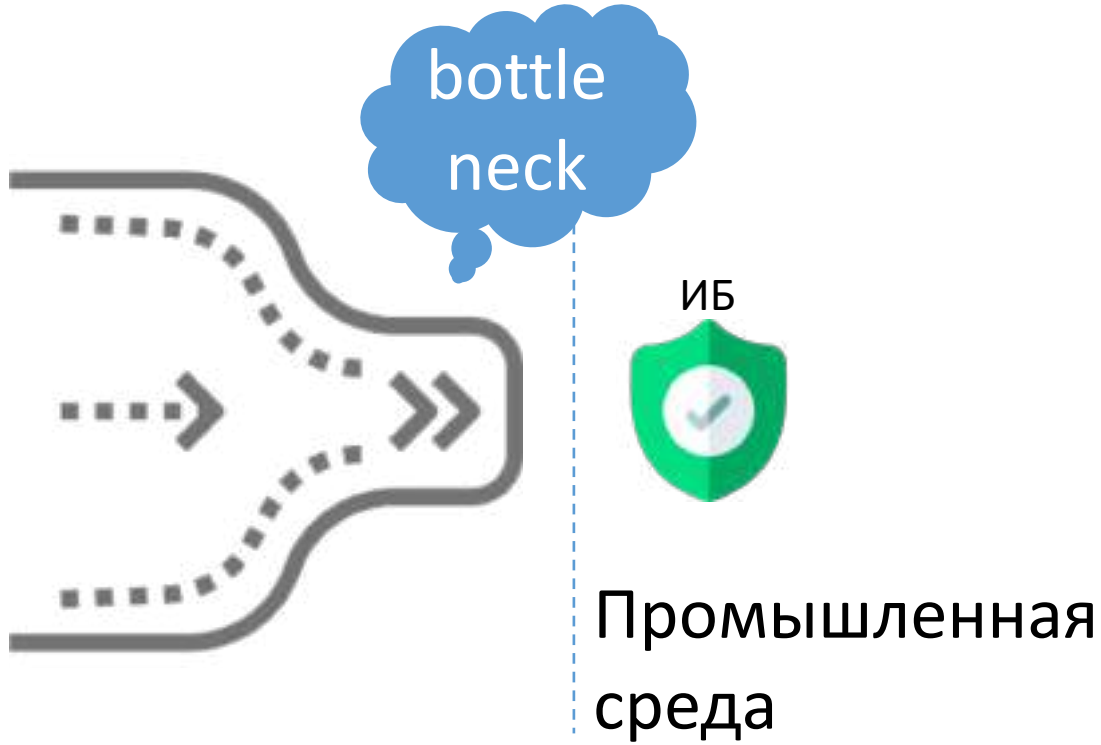
Методологии



DevSecOps это тесное взаимодействие команды с информационной безопасностью

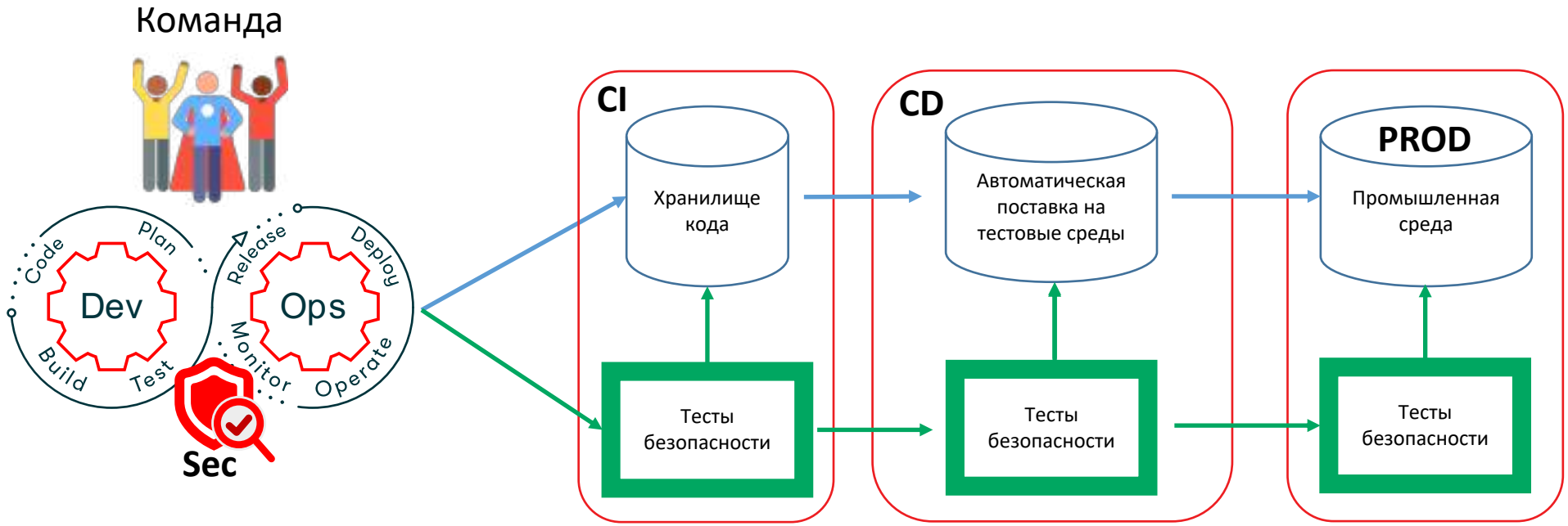
Классическая модель взаимодействия с ИБ



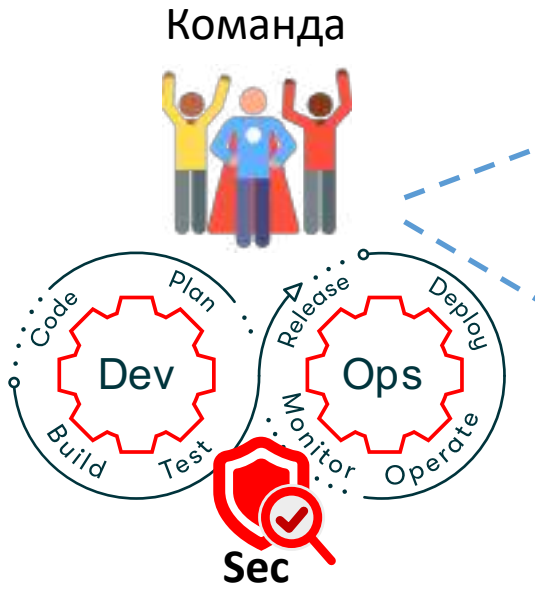


Модель DevSecOps

ПО начинается с написания тестов безопасности



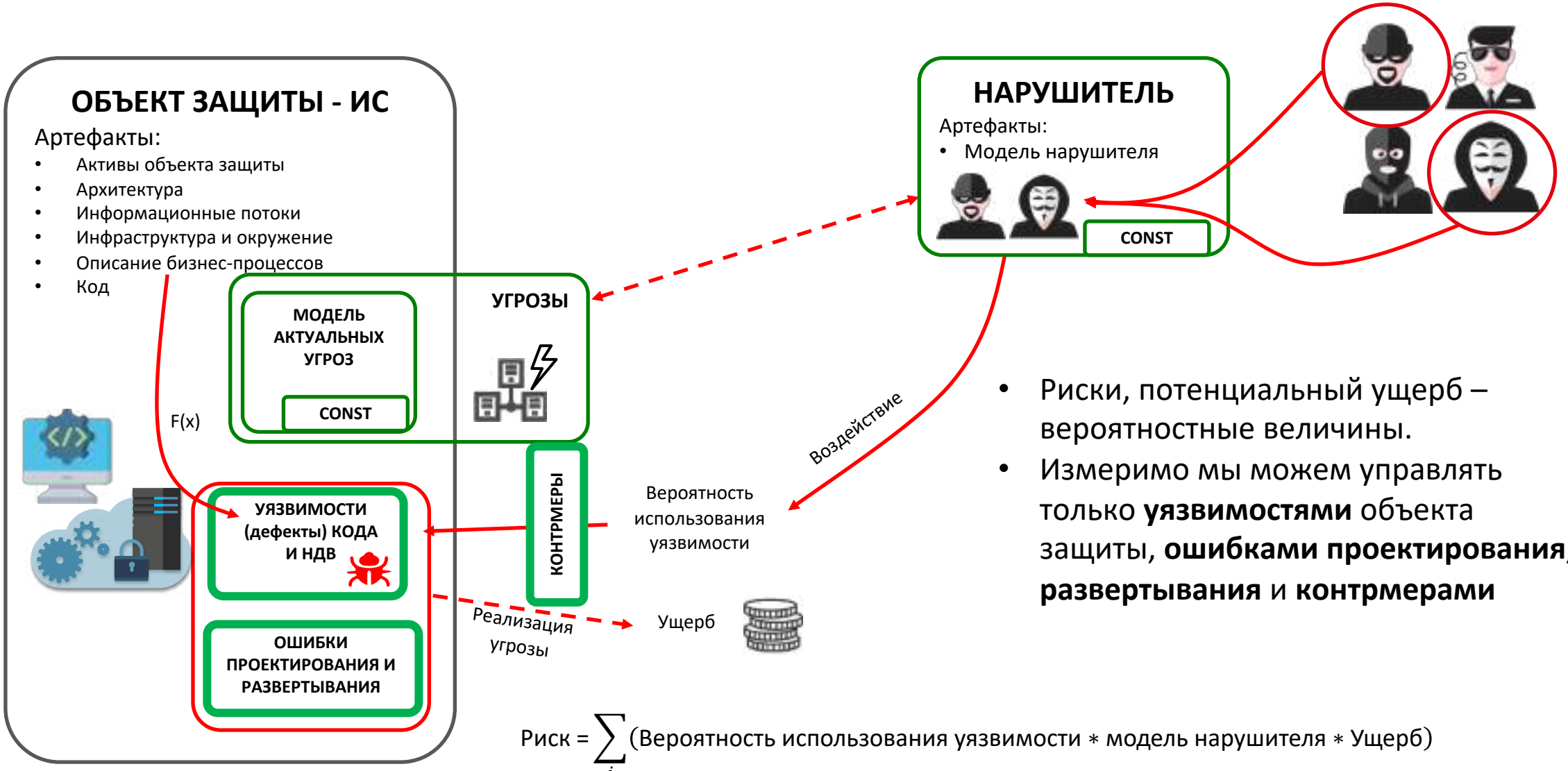
DevSecOps – непрерывная безопасность



Набор практик, нацеленных на взаимодействие разработчиков ПО с экспертами по безопасности

Предотвращение появления уязвимостей на всех этапах процесса производства а не их поиск и устранение перед выходом на Prod

Защищенный код: чем управляем?

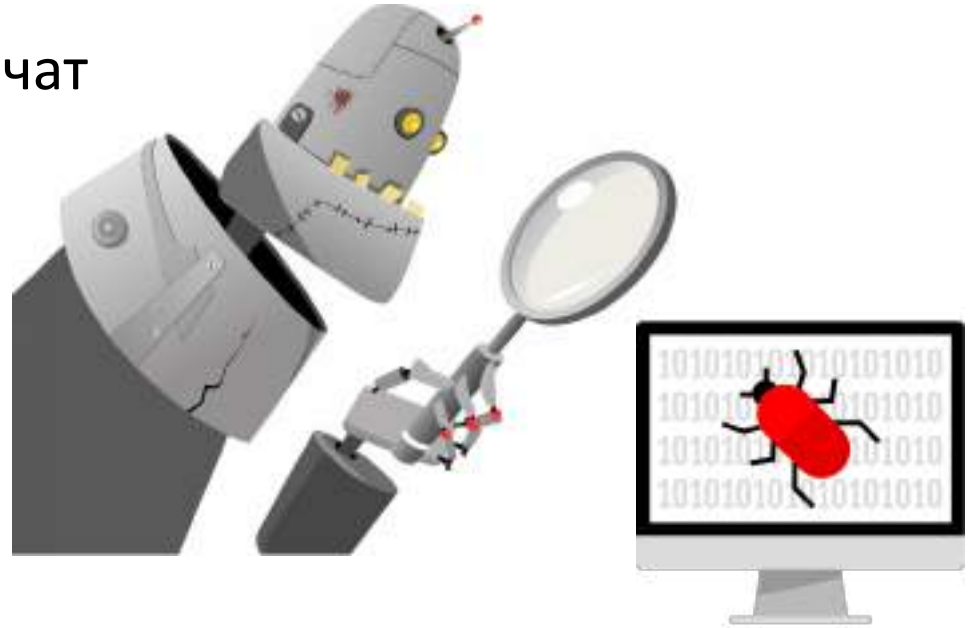


- Риски, потенциальный ущерб – вероятностные величины.
- Измеримо мы можем управлять только **уязвимостями** объекта защиты, **ошибками проектирования, развертывания** и **контрмерами**

$$\text{Риск} = \sum_i (\text{Вероятность использования уязвимости} * \text{модель нарушителя} * \text{Ущерб})$$

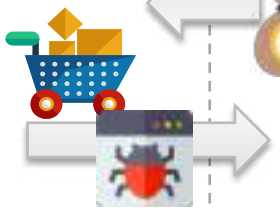
До попадания в базы уязвимостей еще нужно дорасти

- Баз уязвимостей много, но информация об уязвимостях ваших продуктов туда не попадает
- Даже если уязвимость обнаружат, ее не включат в общедоступную базу данных уязвимостей:
  - https://nvd.nist.gov/
  - https://cve.mitre.org/
  - https://www.kb.cert.org/vuls/
  - https://cxsecurity.com/
  - …

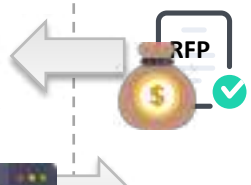


Защищенный код: а зачем?

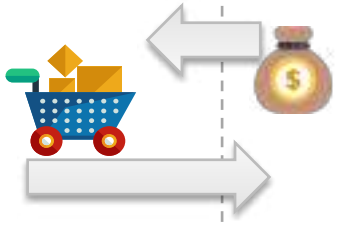
РАЗРАБОТЧИК



ЗАКАЗЧИК



Эксплуатация / сервисы



ПОТРЕБИТЕЛЬ

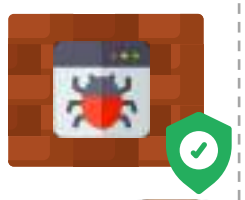
ЗАЧЕМ НАМ БЕЗОПАСНОСТЬ?!
НАДО БЫСТРЕЕ ВЫЙТИ НА PROD
И ПОЛУЧИТЬ ДЕНЬГИ!

Затраты:
- Исправление дефектов в готовом продукте
- Задержки при сдаче в эксплуатацию

Разработчик несет мах затраты на исправление дефектов в готовом продукте.
Потери из-за задержки T2D

ЗАЧЕМ МНЕ ТАКИЕ ПРОДУКТЫ И РАЗРАБОТЧИК?!

Затраты:
- накладные средства защиты информации
- эксплуатация средств защиты информации
- проведение аудита защищённости
  - при приемке
  - периодические и внеплановые
- интеграция со средствами защиты информации,
- защита процессов тех поддержки,
- мониторинг и обработка инцидентов безопасности,
- системы антифрода (использование уязвимостей)



Заказчик несет максимальные затраты на создание и поддержание защищенности, так как ему нужно компенсировать незащищенность разработанного продукта + потери дохода из-за незащищенных продуктов

ЗАЧЕМ МНЕ ТАКОЙ СЕРВИС И ПРОДУКТЫ?!

ВНЕДРЕНИЕ ЗАКЛАДОК, УЯЗВИМОСТЕЙ

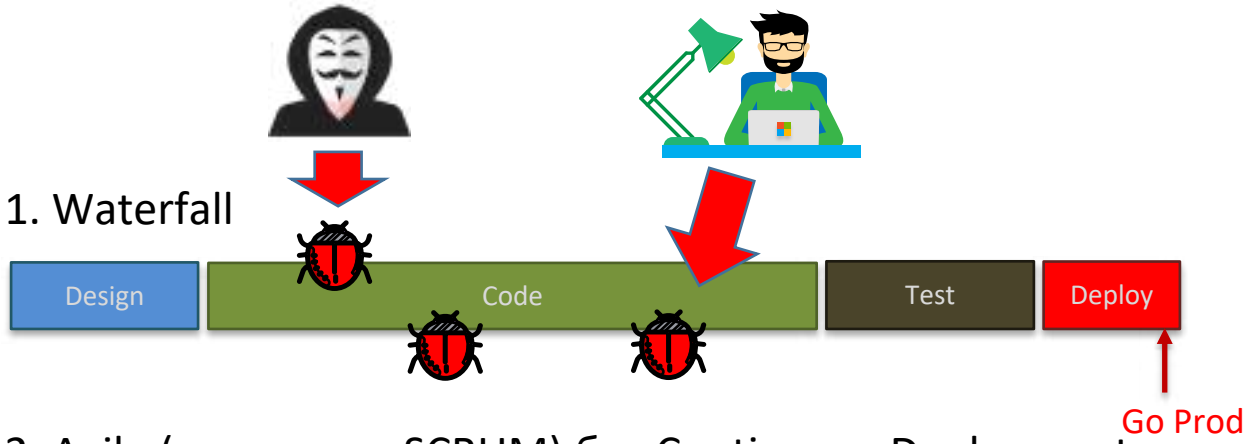
АТАКИ НА ИНФРАСТРУКТУРУ, ДАННЫЕ, СЕРВИСЫ.
ФРОДОВАЯ АКТИВНОСТЬ

НАРУШЕНИЕ ТАЙНЫ СВЯЗИ, ЛИЧНОЙ ЖИЗНИ
ФИНАНСОВЫЙ УЩЕРБ, ОТСУТСТВИЕ СЕРВИСОВ

НАРУШИТЕЛИ

Защищенный код: почем уязвимости?

Разработка защищенного кода



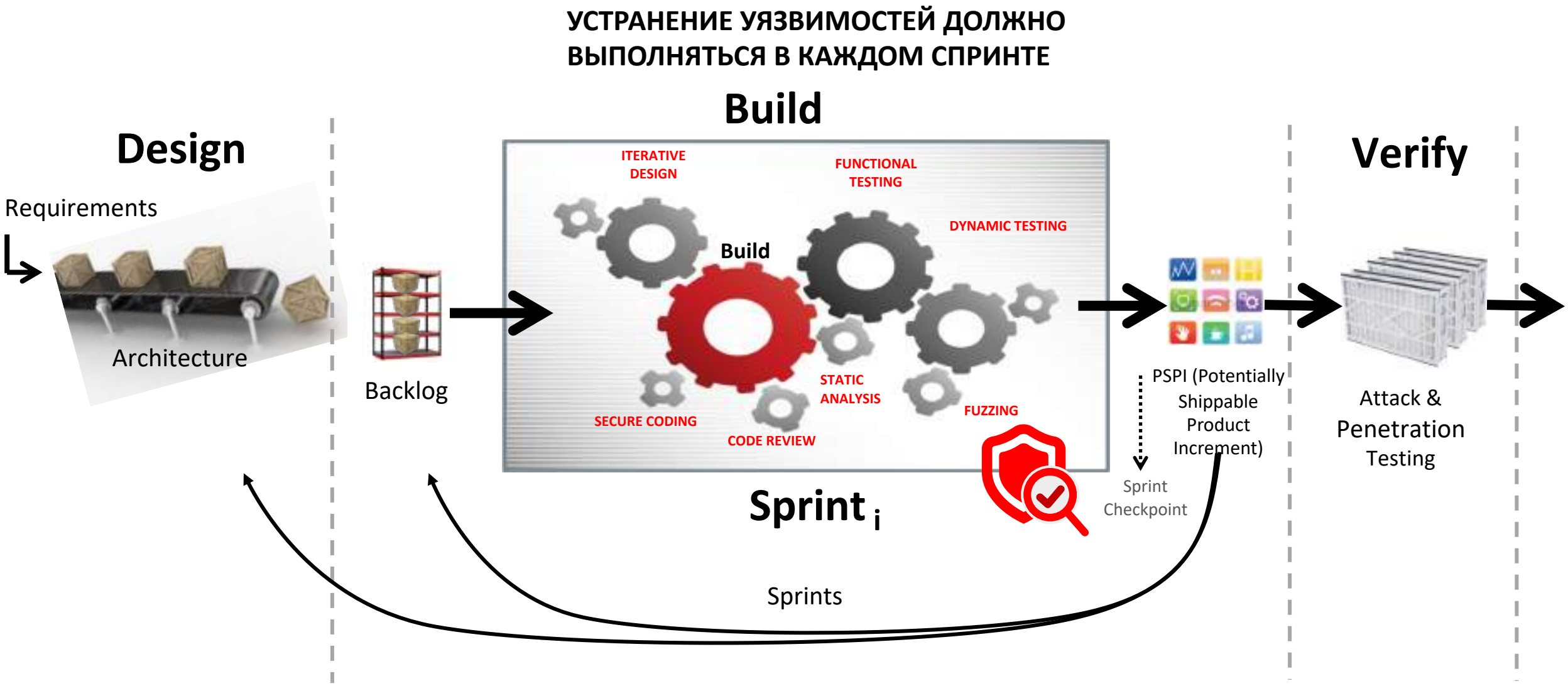
НЕ ЗАБЫВАЕМ ОБ УЯЗВИМОСТЯХ И НСД КОТОРЫЕ ПРЕВНОСЯТ СБОРЩИКИ И КОМПИЛЯТОРЫ

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ В КОДЕ

ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ ЗАКЛАДОК В КОДЕ И СТОРОННИХ КОМПОНЕНТАХ

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ В СТОРОННИХ КОМПОНЕНТАХ (УЯЗВИМЫЕ БИБЛИОТЕКИ И ТД).

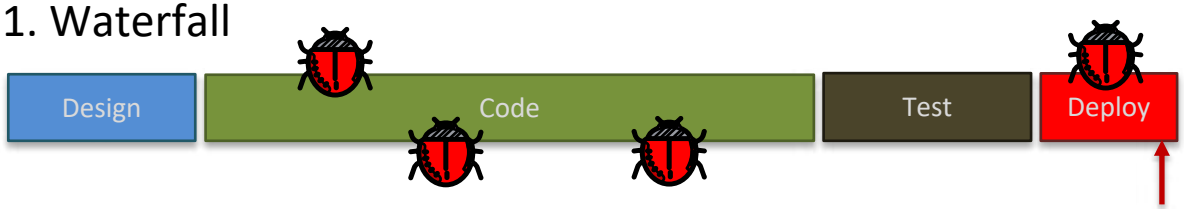
Разработка защищенного кода



Скупка уязвимостей

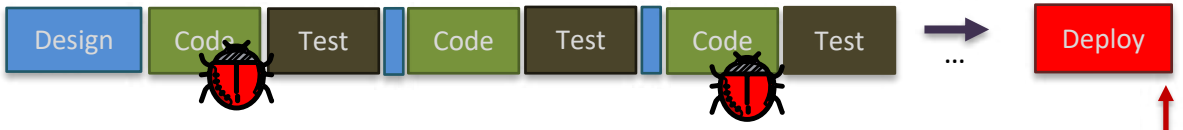
ЕСЛИ ВАШ ПРОДУКТ ШИРОКО ИСПОЛЬЗУЕТСЯ И / ИЛИ СВЯЗАН С КРИТИЧЕСКИМИ АКТИВАМИ ПОЛЬЗОВАТЕЛЕЙ, ТО ЗАПУСТИТЕ ПРОГРАММУ BUG BOUNTY

1. Waterfall



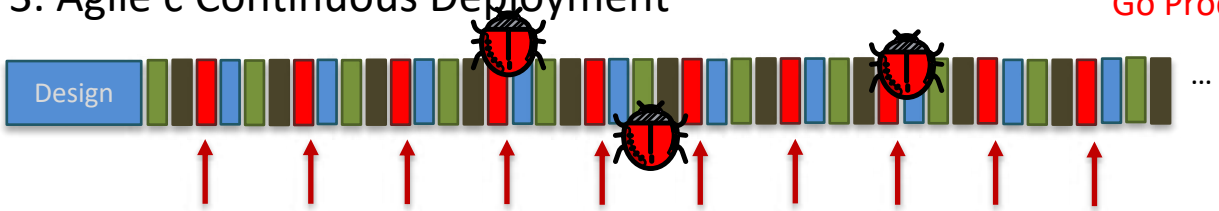
Go Prod

2. Agile (например, SCRUM) без Continuous Deployment

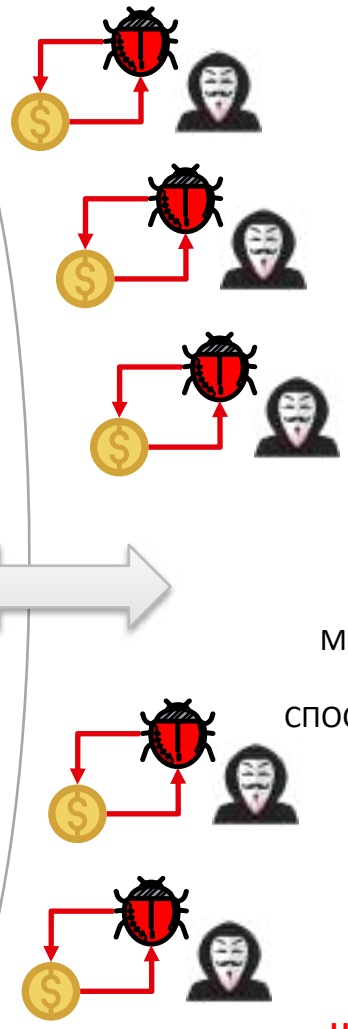


Go Prod

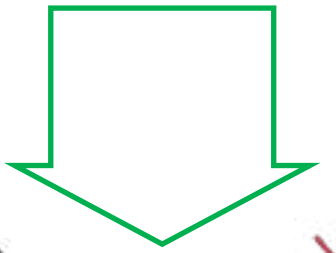
3. Agile с Continuous Deployment



Go Prod Go Prod Go Prod Go Prod Go Prod Go Prod Go Prod



УСТРАНЕНИЕ ИНЦИДЕНТОВ СВЯЗАННЫХ С ЭКСПЛУАТАЦИЕЙ УЯЗВИМОСТЕЙ



МОТИВИРОВАННЫЕ НА РЕЗУЛЬТАТ ХАКЕРЫ СПОСОБНЫ НАЙТИ БОЛЬШЕ УЯЗВИМОСТЕЙ.

СТОИМОСТЬ НАХОЖДЕНИЯ ОДНОЙ УЯЗВИМОСТИ БУДЕТ МАКСИМАЛЬНО НИЗКОЙ.

ЗАЧЕМ БОРОТЬСЯ С ХАКЕРАМИ? ИСПРОЛЬЗУЕМ ИХ ПОТЕНЦИАЛ!

НО, УГРОЗА ЦЕЛЕНАПРАВЛЕННЫХ АТАК ОСТАЕТСЯ!

Защищенный процесс доставки

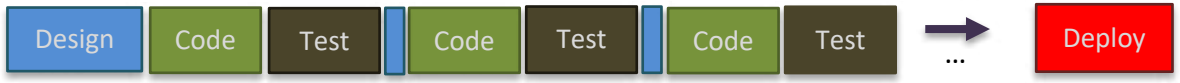
ИСПОЛЬЗУЙТЕ DEPLOY DMZ ДЛЯ ДОСТАВКИ ПРОГРАММ КОНЕЧНОМУ ПОЛЬЗОВАТЕЛЮ

ПРОВОДИТЕ РАЗВЕРТЫВАНИЕ БЕЗ УЯЗВИМОСТЕЙ В ОКРУЖЕНИИ И КОНФИГУРАЦИИ

1. Waterfall

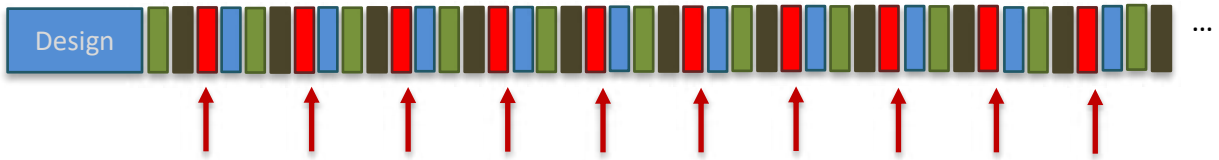
Go Prod

2. Agile (например, SCRUM) без Continuous Deployment

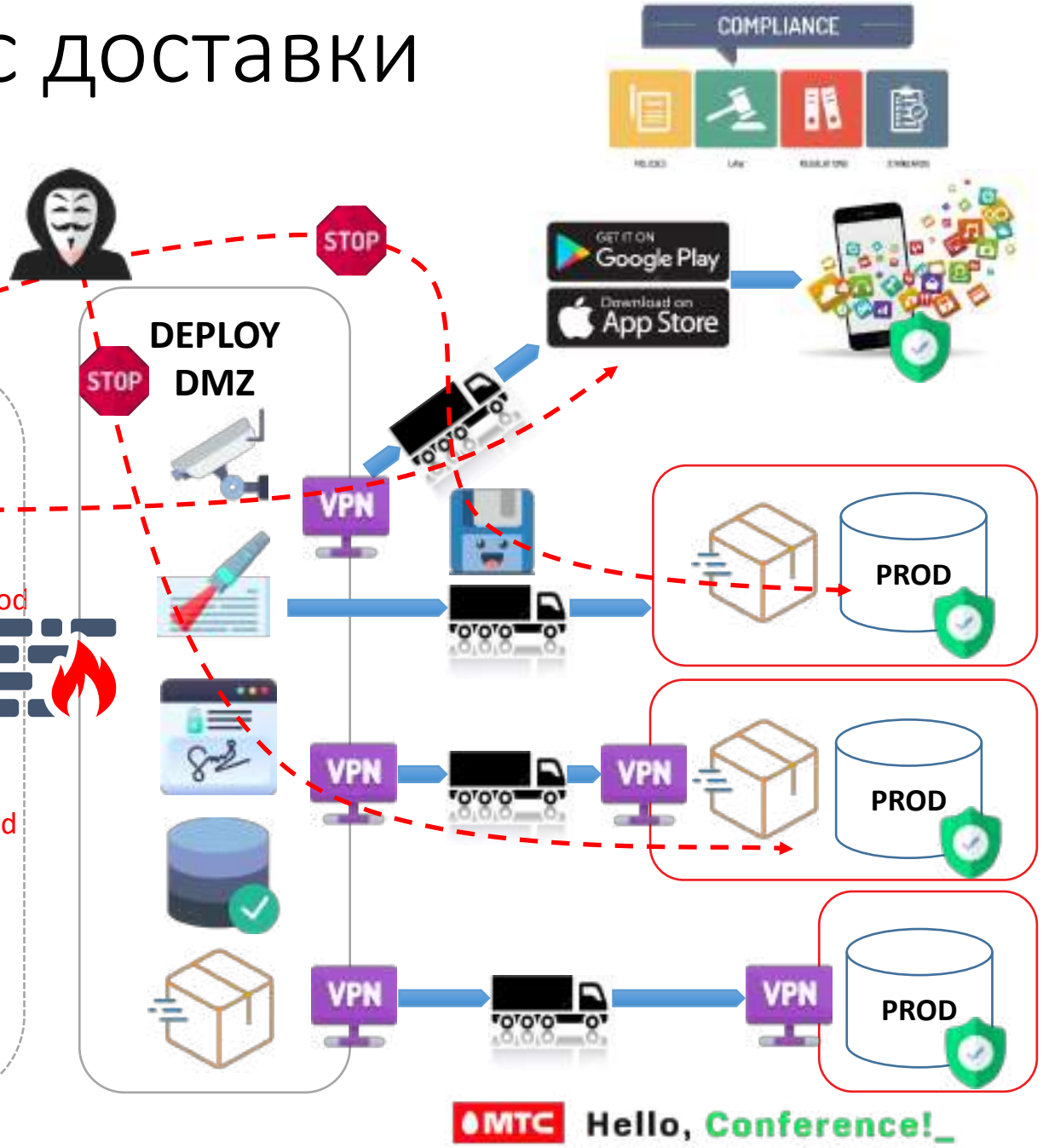


Go Prod

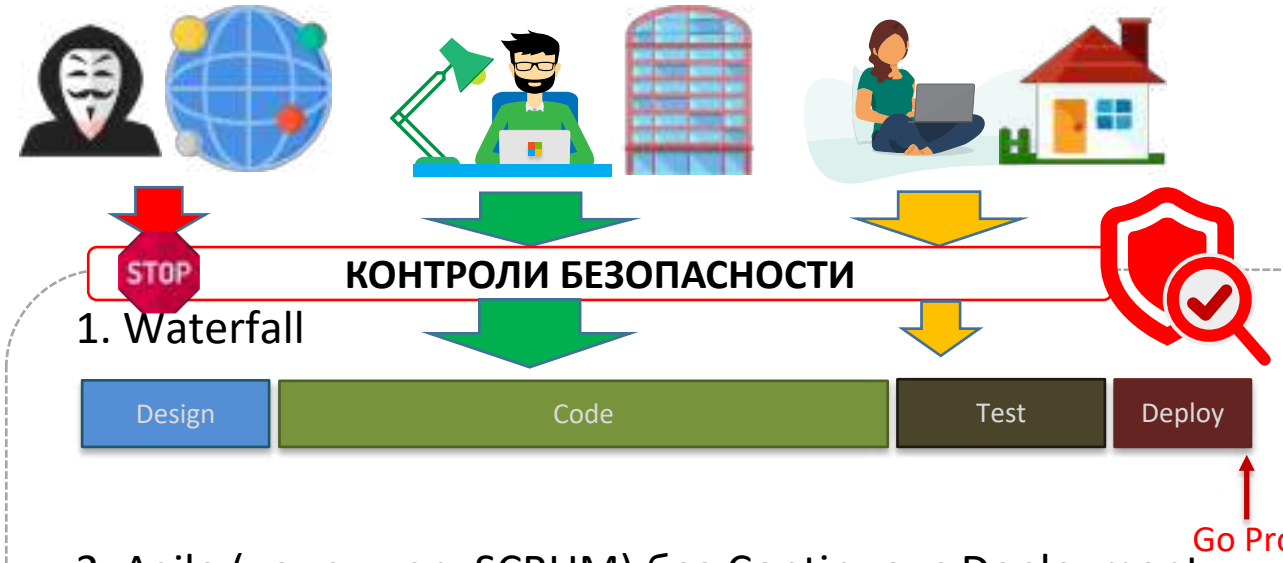
3. Agile с Continuous Deployment



Go Prod Go Prod Go Prod Go Prod Go Prod Go Prod Go Prod

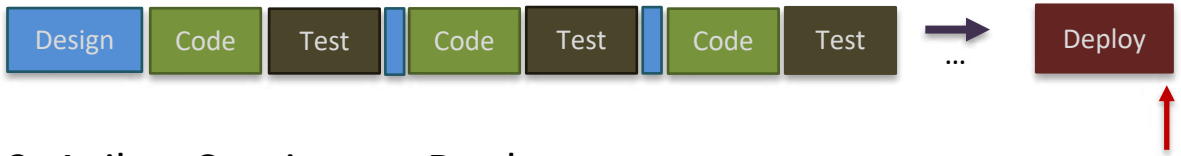


Защита процесса производства

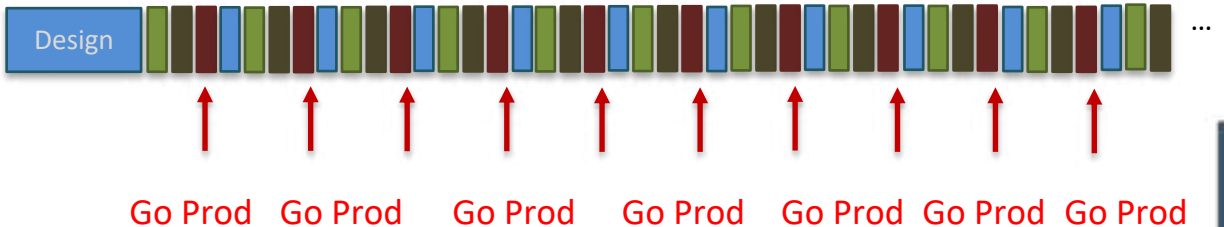


1. Waterfall

2. Agile (например, SCRUM) без Continuous Deployment



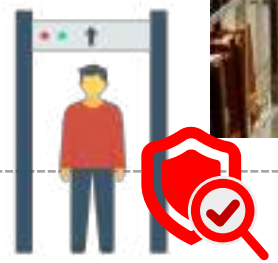
3. Agile с Continuous Deployment



НУЖНО РАЗДЕЛЯТЬ ПРОИЗВОДСТВЕННЫЙ СЕГМЕНТ И WORKSPACE СОТРУДНИКОВ, А НА ГРАНИЦЕ ВВОДИТЬ КОНТРОЛИ БЕЗОПАСНОСТИ

Например:

- Проверка кода поступившего от сотрудников работающих вне компании;
- Защита ресурсов pipeline от атак и НСД

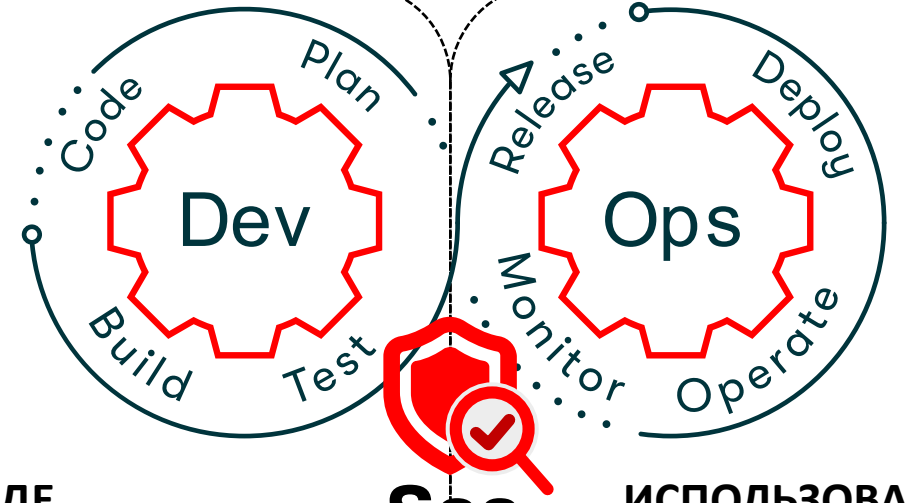


..а инструментарий?

SAST	DAST	В КОНФИГУРАЦИИ	В ОБРАЗЕ КОНТЕЙНЕРА	СЕТЕВЫЕ УЯЗВИМОСТИ
PVS-Studio	acunetix	Sysdig	Sysdig	POSITIVE TECHNOLOGIES
MICRO FOCUS	Qualys.	cavirin	anchore	tenable
SYNOPSYS	Ростелеком Солар	CIS-CAT Pro	Twistlock	OpenVAS
sonarqube	arachni	OWASP Open Web Application Security Project	aqua MicroScanner	GFI Software
lgtm.com	ZAPROXY	Docker Bench Security	Dagda	BeyondTrust
CHECKMARX				

Собираем все вместе

Инструментарий и обученный персонал



Инструментарий и обученный персонал

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ В КОДЕ

ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ ЗАКЛАДОК В КОДЕ И СТОРОННИХ КОМПОНЕНТАХ

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ В СТОРОННИХ КОМПОНЕНТАХ (УЯЗВИМЫЕ БИБЛИОТЕКИ И ТД)

СКУПКА УЯЗВИМОСТЕЙ

ИСПОЛЬЗОВАНИЕ DEPLOY DMZ ДЛЯ ДОСТАВКИ ПРОГРАММ КОНЕЧНОМУ ПОЛЬЗОВАТЕЛЮ

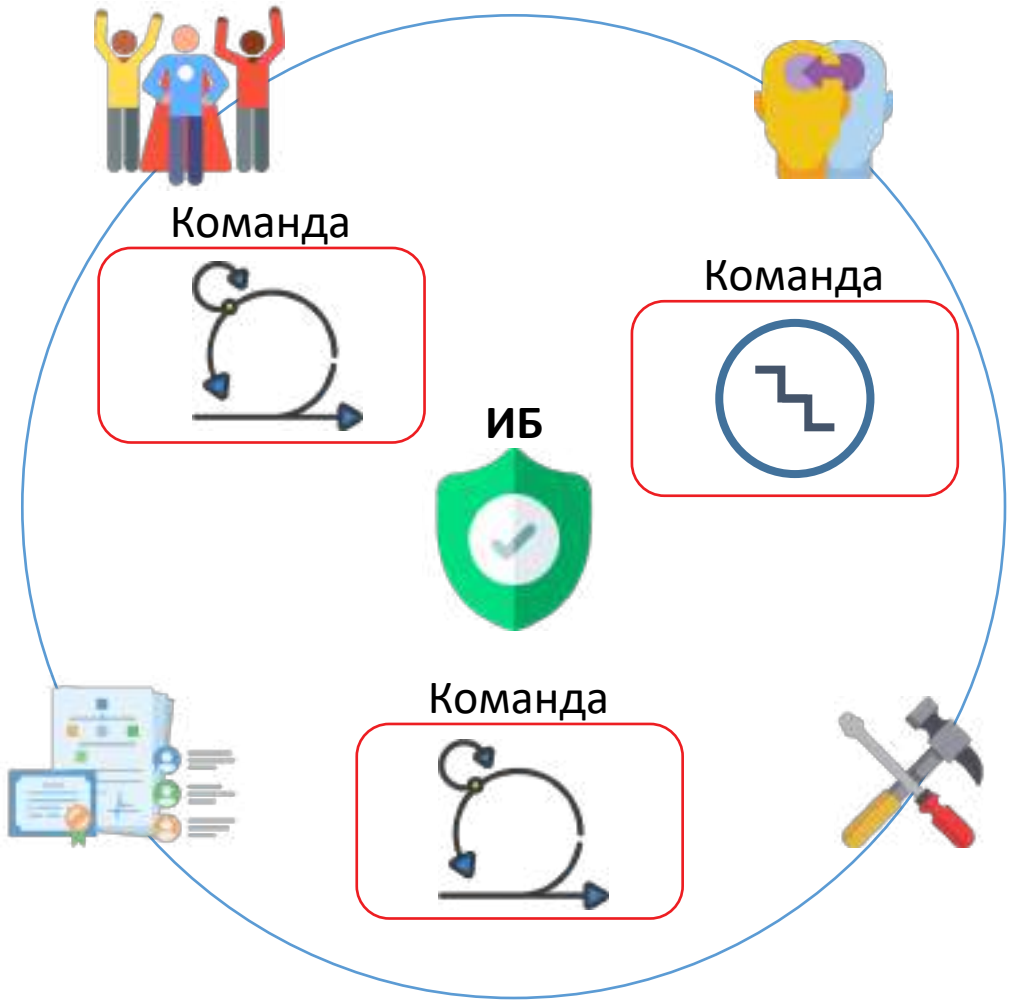
РАЗВЕРТЫВАНИЕ В PROD БЕЗ УЯЗВИМОСТЕЙ В ОКРУЖЕНИИ И КОНФИГУРАЦИИ

ЗАЩИТА ПРОЦЕССА ПРОИЗВОДСТВА

НЕПРЕРЫВНО С BENCHMARKS И KPI СОГЛАСНО ПОЛИТИК И COMPLIANCE

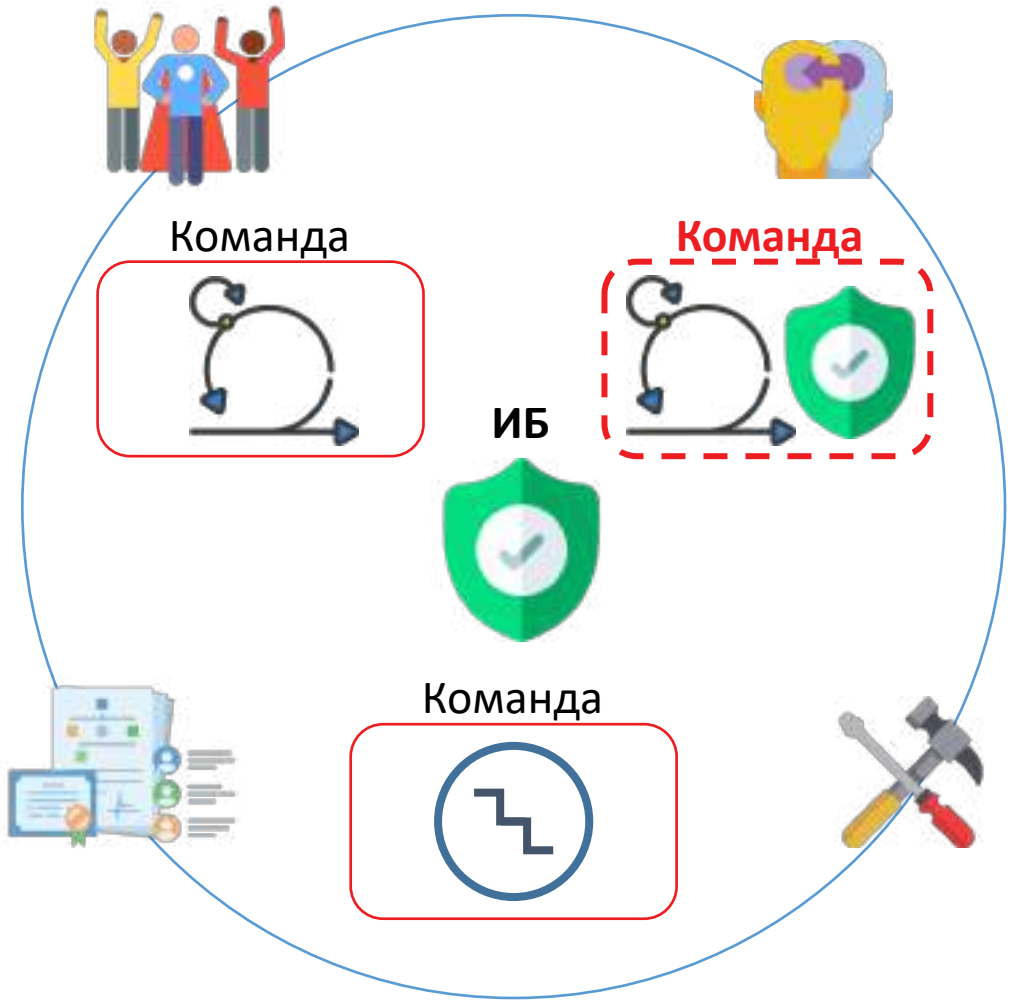
DevSecOps как общекомандный сервис

- ЗА
  - Высокий уровень экспертизы централизованной команды
  - Широкое использование гильдий у разработчика
  - Наличие интегрированного в pipeline инструментария и его сопровождение централизованной командой
- ПРОТИВ
  - Централизованная команда может быть bottleneck для процессов команд => требуется введение Security champion
  - Нет погружения в продукт => требуется введение Security champion



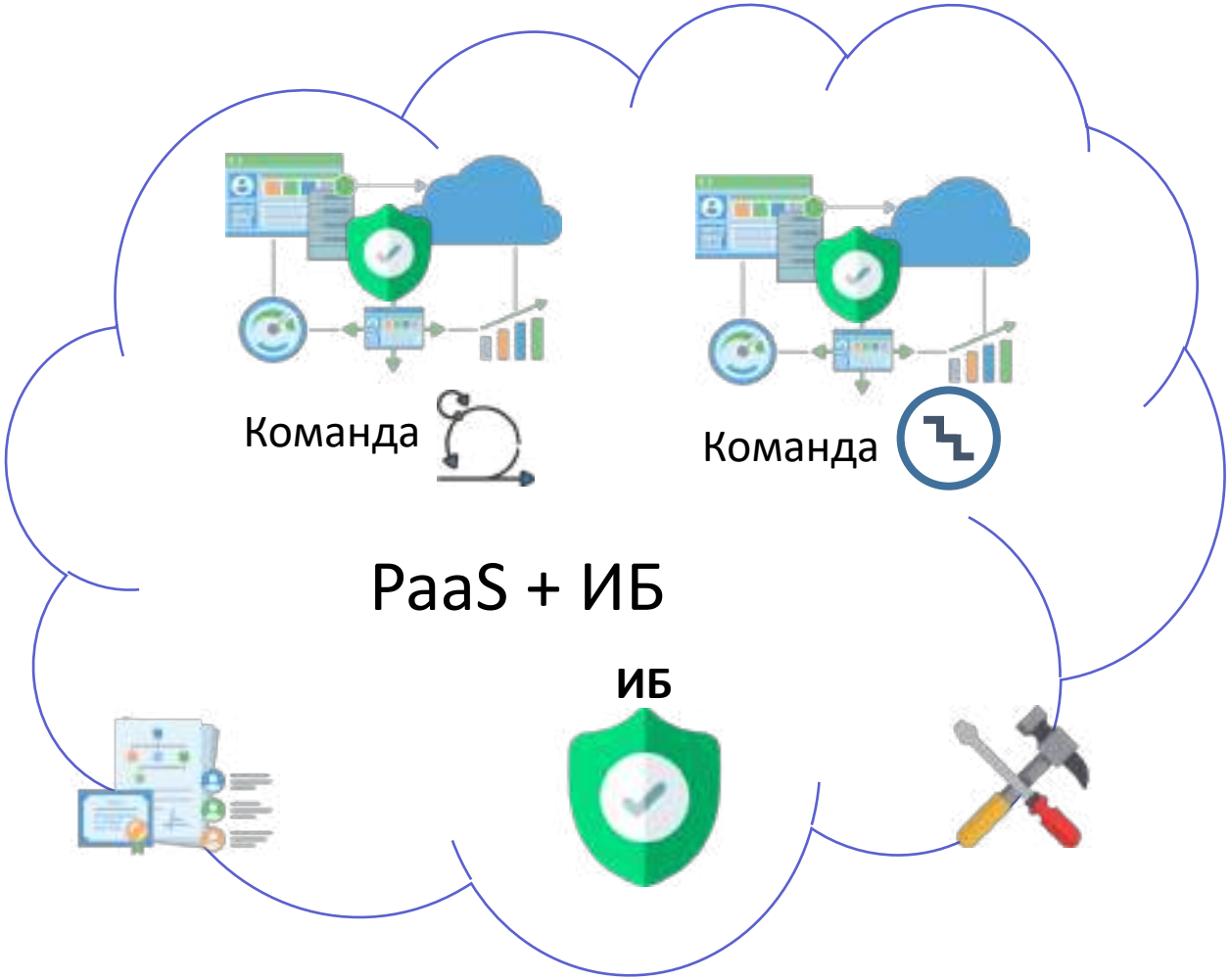
DevSecOps внутри команды разработки

- ЗА
  - Для больших продуктов
  - Специфические технологии разработки (встроенные системы, ПЛИС)
  - Глубокое погружение в продукт, но лучше Security champion
- ПРОТИВ
  - Большое число специалистов и затраты на них при большом числе команд
  - Отдельная закупка и интеграция специализированного инструментария DevSecOps
  - Долгий вход специалистов в процесс для созданных продуктов



DevSecOps: сервис для PaaS

- ЗА
  - Для маленьких внешних команд потребителей PaaS
  - Продажа безопасности как сервиса
- ПРОТИВ
  - Непонимание модели угроз для продуктов на PaaS => требуется введение Security champion
  - Все технологии разработки не охватить



Security Champions

Где взять столько сотрудников безопасности?
Роль Security Champion – интерфейс в продуктовую команду по ИБ!

Обязанности:
- Работа с ИБ, консультирование команды
- Работа с инструментальным стеком ИБ
- Проведение тренингов и код-ревью

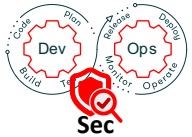
Мотивация:
- Расширение знаний в области ИБ
- Повышение рыночной стоимости

Итого, о чём поговорили

1. Виды уязвимостей и контрмеры как основной объект ИБ

2. Разработка защищённого кода и скупка уязвимостей

3. Защита процесса производства



4. Подходы к созданию процесса DevSecOps

5. Роль Security Champion