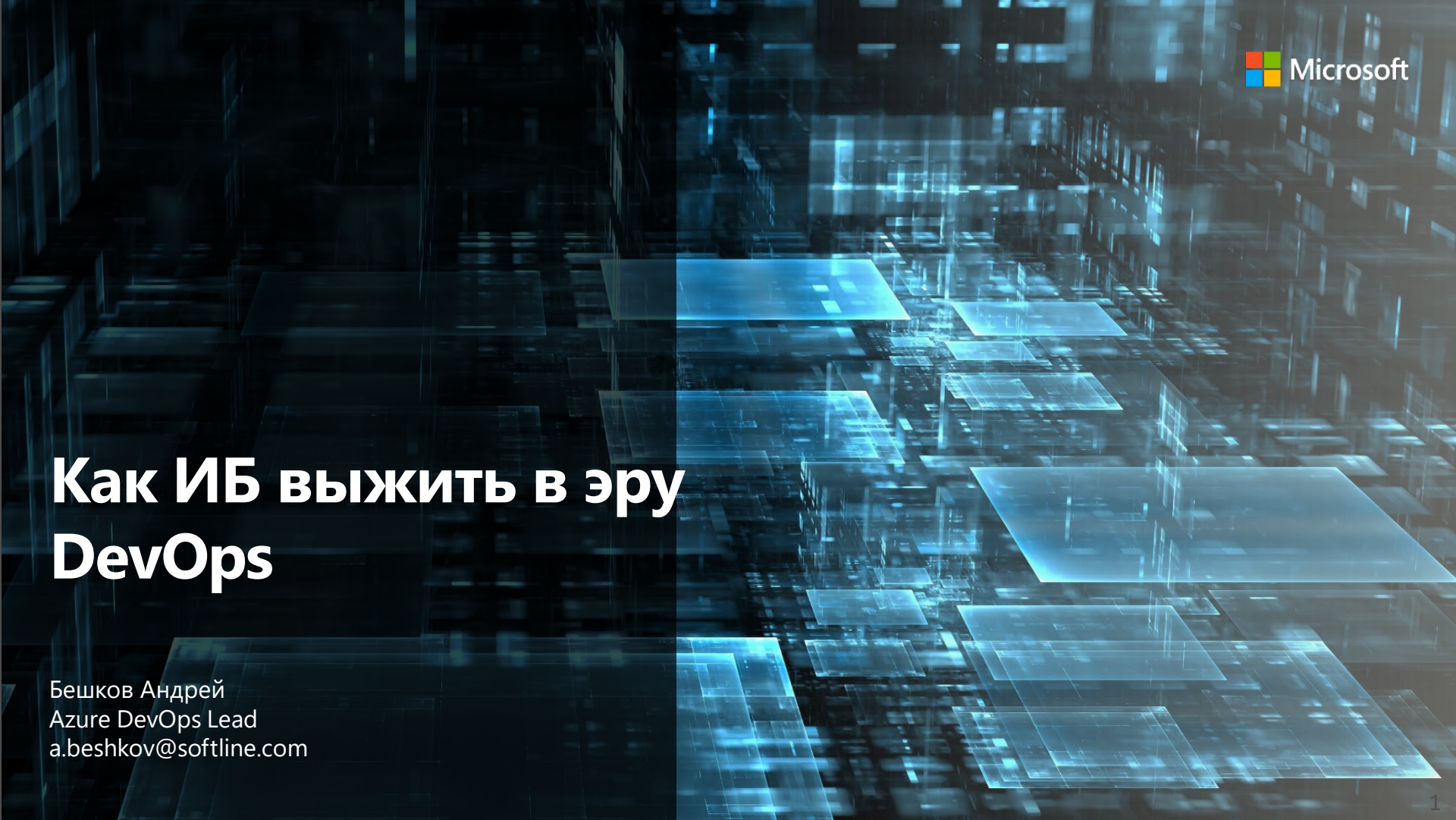


Как ИБ выжить в эру DevOps

Бешков Андрей
Azure DevOps Lead
a.beshkov@softline.com

3/4

КОМАНД “ВЕРЯТ В AGILE”

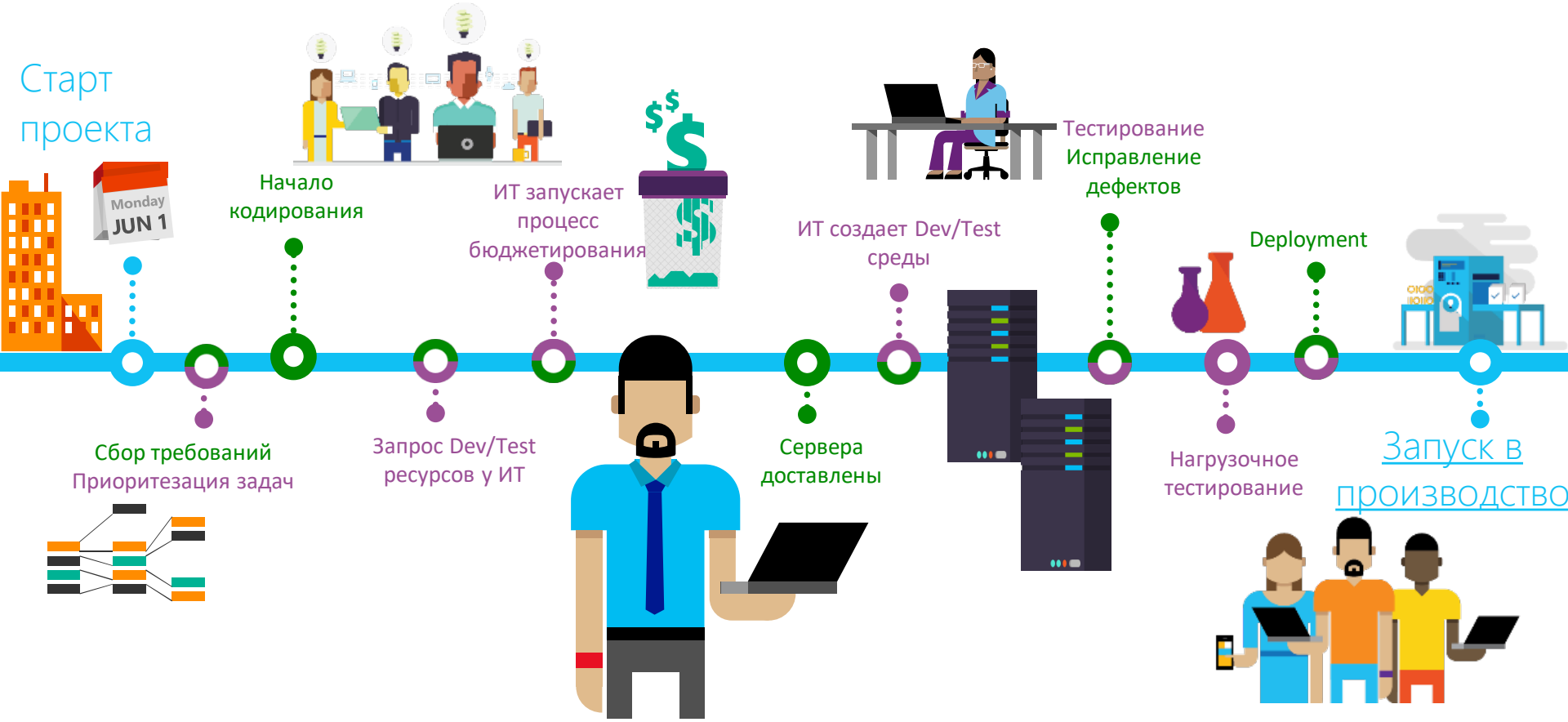
НО В БОЛЬШИНСТВЕ ОРГАНИЗАЦИЙ ДО СИХ ПОР ТРЕБУЮТСЯ НЕДЕЛИ И МЕСЯЦЫ НА ПОСТАВКУ НОВОЙ ФУНКЦИОНАЛЬНОСТИ

41%

ИТ БЮДЖЕТОВ НА РАЗРАБОТКУ ТРАТЯТСЯ ВПУСТУЮ

ВКЛЮЧАЯ БЮДЖЕТЫ НА РАЗРАБОТКУ, ОПЛАТУ ВНУТРЕННИХ ИЛИ НАЕМНЫХ СПЕЦИАЛИСТОВ

Цикл разработки приложения. Где же тут ИБ?



Agile — методология, определяющие следующие базовые ценности и принципы:

- люди и взаимодействие важнее инструментов и процессов
- общение с бизнес-заказчиком важнее согласования условий
- работающий продукт важнее исчерпывающего документирования
- своевременная реакция на изменения важнее следования первоначальному плану

DevOps (акроним от англ. development и operations) — это набор современных практик и подходов, направленных на сокращение time-to-market и повышение эффективности взаимодействия блоков развития и сопровождения ИТ.

Continuous Integration — практика DevOps, направленная на автоматизацию процесса сборки решения и запуска сборки всякий раз при внесении изменения в код.

Continuous Deployment — практика DevOps, подразумевающая, что каждое изменение после успешного прохождения автоматизированных тестов отправляется в продуктив в автоматическом режиме.

DEVOPS ПРЕИМУЩЕСТВА

СИЛЬНЫЙ ИТ БЛОК ЭТО КОНКУРЕНТНОЕ ПРЕИМУЩЕСТВО

Компании с высоко-производительным ИТ с 2х большей вероятностью достигают своих бизнес целей, финансовых показателей и доли рынка

ПОСТАВКА КОДА 30X БЫСТРЕЕ

… в сравнении с низкопроизводительными командами

ПРАКТИКИ ДЕВОПС ПОВЫШАЮТ ПРОИЗВОДИТЕЛЬНОСТЬ ИТ ДЕПАРТАМЕНТА

В 60 РАЗ МЕНЬШЕ СБОЕВ

… и восстановление после сбоев 168X быстрее в сравнении с низко-производительными командами

Agile — методология, определяющие следующие базовые ценности и принципы:

- люди и взаимодействие важнее инструментов и процессов
- общение с бизнес-заказчиком важнее согласования условий
- работающий продукт важнее исчерпывающего документирования
- своевременная реакция на изменения важнее следования первоначальному плану

DevOps (акроним от англ. development и operations) — это набор современных практик и подходов, направленных на сокращение time-to-market и повышение эффективности взаимодействия блоков развития и сопровождения ИТ.

Continuous Integration — практика DevOps, направленная на автоматизацию процесса сборки решения и запуска сборки всякий раз при внесении изменения в код.

Continuous Deployment — практика DevOps, подразумевающая, что каждое изменение после успешного прохождения автоматизированных тестов отправляется в продуктив в автоматическом режиме.

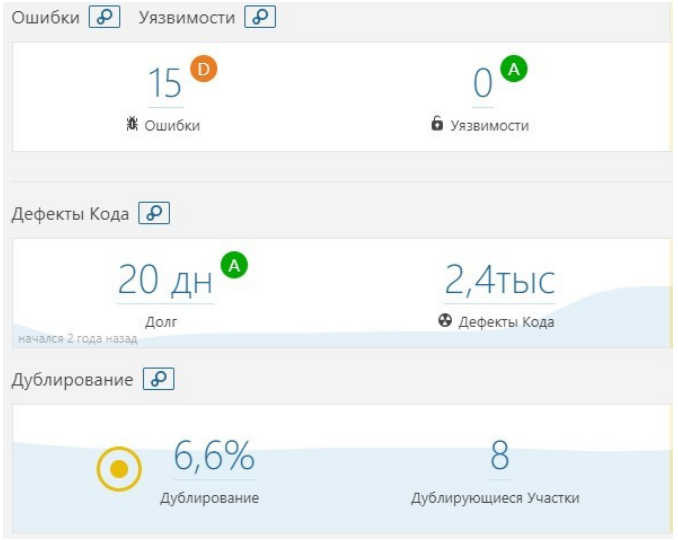
Как быстро это происходит?

- Переход на более детальные и короткие этапы планирования (спринты длительностью в 2 недели);
- Разбиение каждой большой задачи на более мелкие и предварительная временная оценка выполнения каждой небольшой задачи;
- Фиксированная емкость каждого спринта в человеко-днях, что позволяет взять в работу на 2 недели только определенный объем задач и успешно их выполнить;
- Исходя из предварительной оценки задачи и ограничения по емкости спринтов в человеко-днях можно с высокой точностью спрогнозировать время выполнения каждой задачи на 2 месяца вперёд

Azure DevOps и Appcenter.ms как пример DevOps

Технический долг -35%

Внедрение практик CodeReview и сервиса автоматической проверки кода SonarQube позволило сократить технический долг на 35%.



Поиск устаревшего опенсорса

Продукты > Black Duck by Synopsys

ПОЛУЧИТЬ

Сведения о ценах
Стоимость развернутых компонентов шаблона

Категории
Безопасность
Средства для разработчиков

Black Duck by Synopsys

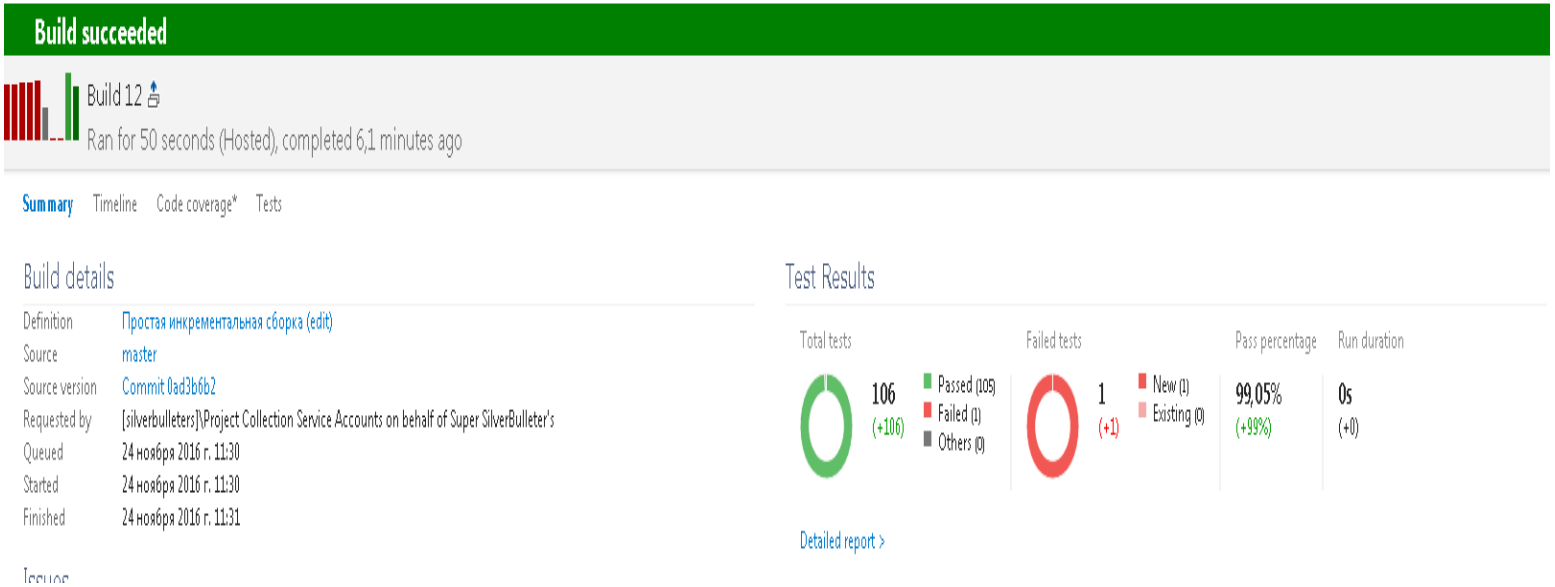
Synopsys

Обзор Планы Reviews

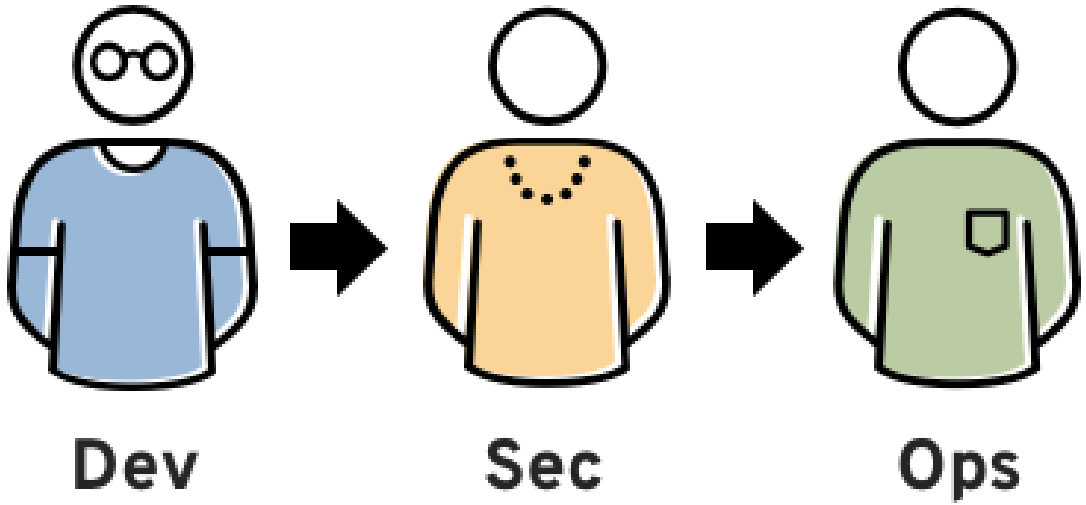
Secure and Manage Open Source Software

Black Duck by Synopsys helps security and development teams identify and mitigate open source related risks across their applications and containers. With Black Duck Hub, organizations can identify open source, map known vulnerabilities, and triage and track remediation. Black Duck provides the most comprehensive language coverage, the industry's largest open source software KnowledgeBase, and extensive integration with third-party development tools.

Автотесты для поиска дефектов и уязвимостей



Shift Left или DevSecOps



Баг Баунти? Не райский остров!

Для начала в приватном режиме.

Сначала сам пентести, а потом зови других

Запускать только если умеете отработать вал заявок. Ответ в жестко фиксированные сроки.

Платить по максимальному влиянию.

Своя инфраструктура или Hackerone?

https://www.hackerone.com/blog/the-bug-bounty-field-manual
https://www.owasp.org/index.php/OWASP_Best_Practices_in_Vulnerability_Disclosure_and_Bug_Bounty_Programs

Security as a Code!