



DASA DevOps.

Принципы Agile и роль метрик в построении ценности Secure SDLC.

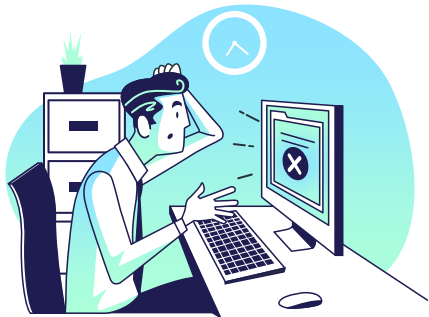
Подготовил: Шмаков Илья, CISO, AppSec 2021, материал для ITSec

Аннотация

- **DevOps Agile Skills Association** обозначает модель компетенций **T**-профильных команд ориентированный на предикаторы потока ценности.
- **Scaled Agile Framework** формализует план действий посредством **Agile Release Train** для **SDLS** от **TDD, BDD** до **CI/CD**, включая **features toggle**.
- Целью презентации является принцип **Kaizen** (радикал **Kaikaku**) для **DMAIC**, структурированного решения проблем.
- Важнее люди, а не инструменты.
- **Lean** как неотъемлемая часть **Shift-Left** подхода в реализации **DevSecOps**.
- **Security** как предикатор **DASA DevOps**.



Проблема DevSecOps и решение



Проблема

- 1 – Интеграция принципов **Security** в построении **SDLC**.
- 2 – Зрелость продукта в ориентации **DevSecOps** для бизнеса, – «костыльность».
- 3 – Применение практик не относящихся к **Agile-Lean**.
- 4 – Ориентация на контракт.
- 5 – Принцип **legging** метрик.



Решение

- 1 – Ориентация на метрики предикторов ценности.
- 2 – Снижение числа метрик выживаемости (компоненты, заказчики, команды).
- 3 – Ввод метрик (**SAFe, Nexus, Less**) производительности.
- 4 – Приоритезация на ведущие метрики, нивелирование **legging**.

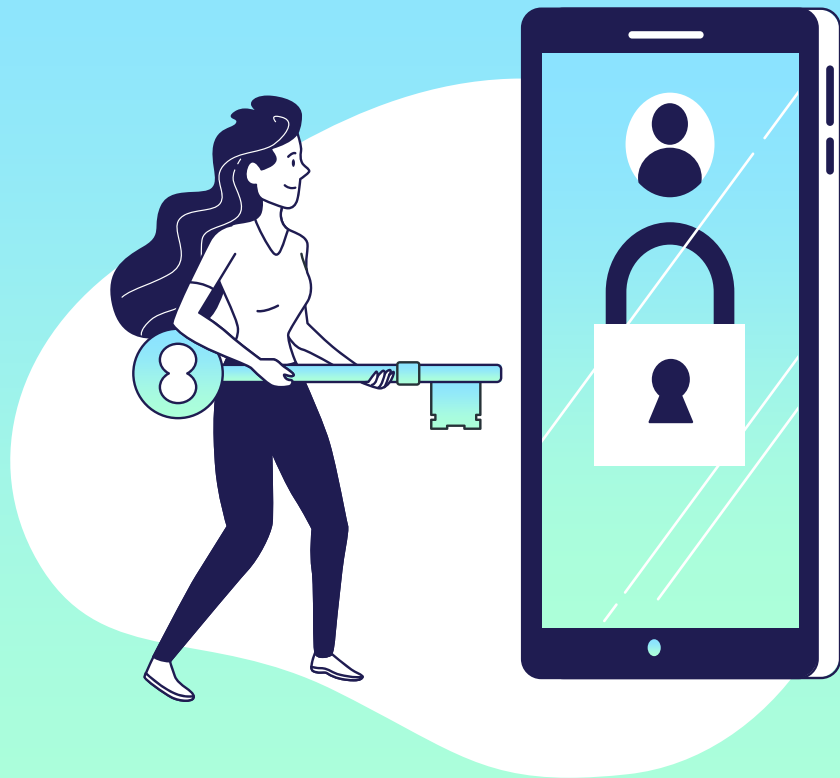


DevOps – это совместная работа менеджмента и разработки ориентированная на непрерывное предоставление, безопасность, создание бизнес ценности.

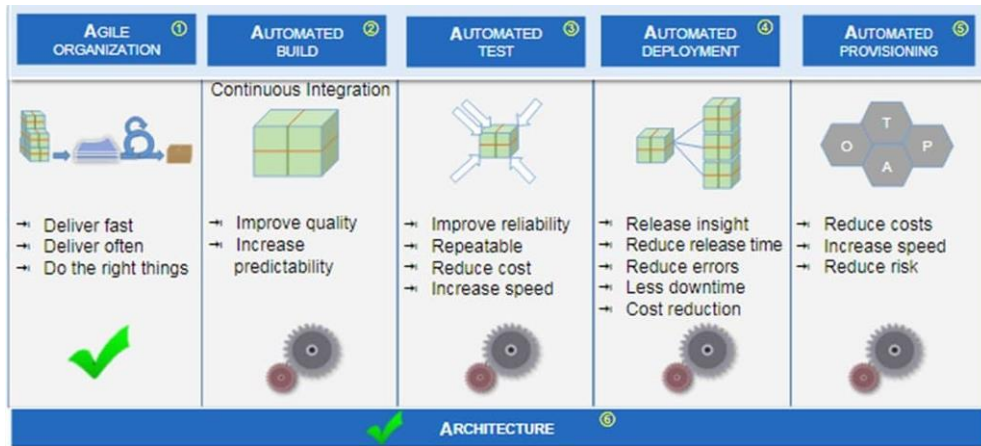
Security – обеспечение контроля.

01 Управление процессами в DevSecOps

DASA DevOps Core
DMAIC
Kaizen
Security Champion
Lencioni

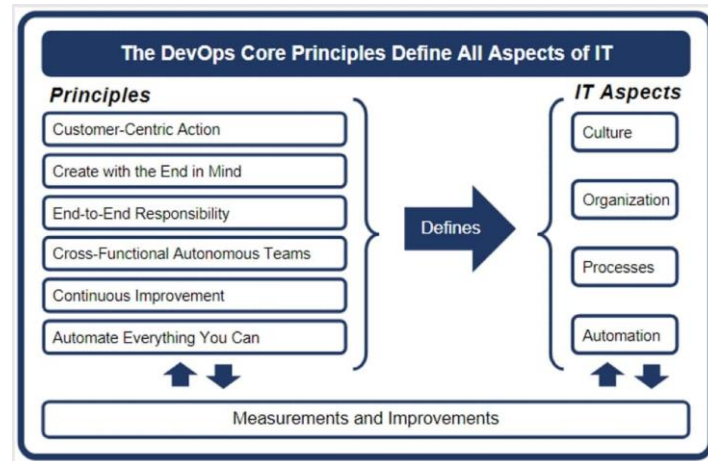


Архитектура процесса DevOps



- Принципы **micro-services**:
 - Производительность;
 - Capabilities бизнес способности;
 - Независимое развертывание;
 - Smart-endpoints через брокеры;
 - Децентрализованное руководство, данные;
 - Инфраструктурная автоматизация;
 - Прототипирование;
 - Эластичность.

- Мотивация по **Даниэлю Пинку** для **DT**:
 - Цель;
 - Автономность;
 - Мастерство.
- Вытекающая градация по принципам **DASA DevOps**:
 - **DT** полностью ответственна за услугу;
 - Уменьшение размера услуги;
 - Быстро изменяемая услуга, – минимальность как принцип применения **features toggle** триггера.

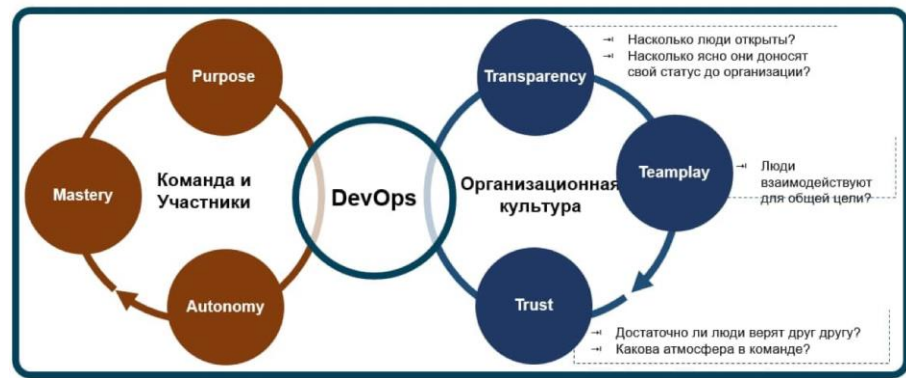


DMAIC и Kaizen событие в плоскости Security



DASA DevOps Main Core через Kaizen

- Применение принципа **Kaizen** через определение проблематики и ее решения для последующей стандартизации, – дает формализацию **Service Relationship Management**.
- Это основной аспект внедрения **Security Champions** в **DevOps** потоке ценности.



- Принципы **Kaizen**:
 - Улучшать можно все и всегда;
 - Не критикуйте – предлагайте;
 - Делайте допущения;
 - Сначала добейтесь качества;
 - Ищите как улучшить, а не «почему невозможно (**принцип 10**)»;
 - Начинайте с того, что недостает в наибольшей степени.
- Ориентация фокуса **Secure** на ценности, итеративном движении, прозрачности, – основа **Security Champions** практики в **DT**.

Security Champion

- **Security Champion** — точка входа в **DT** и евангелист безопасности в одном лице, который в этом заинтересован.
- Если вместо «безопасника» на ошибку в коде или процессе, и последствия укажет **Security Champion**, то его слово будет иметь больше веса в **DT**.
- **Security Champions** знают свой продукт: что с чем взаимодействует и на что смотреть в первую очередь — они эффективнее, в том числе при **Secure Code Review**.
- Это некоторый элемент социальной инженерии, ваши «глаза» в **DT**.
- Чем занимается **Security Champion**:
 - является единой точкой входа в команду разработки по вопросам безопасности;
 - отвечает за использование ИБ-инструментов на всех этапах разработки и сопровождения приложений, откуда и идет градация специалистов в **AppSec**;
 - проводит **security code review** и консультирует команду по вопросам защиты информации;
 - проводит аналитику конвейера потока ценности в продукте и статистических метрик **health**;
 - категоризирует **product/sprint backlog** совместно с **PO/SM/DT**, исходя из рисков для бизнеса.



Ленциони в плоскости Security Champions



Ирония модели Ленциони:
Вы должны начать работать над «мягкими» результатами, как общие человеческие ценности, вместо «жестких» (ценности компании), чтобы состояться как команда.

Модель Ленциони (Lencioni)

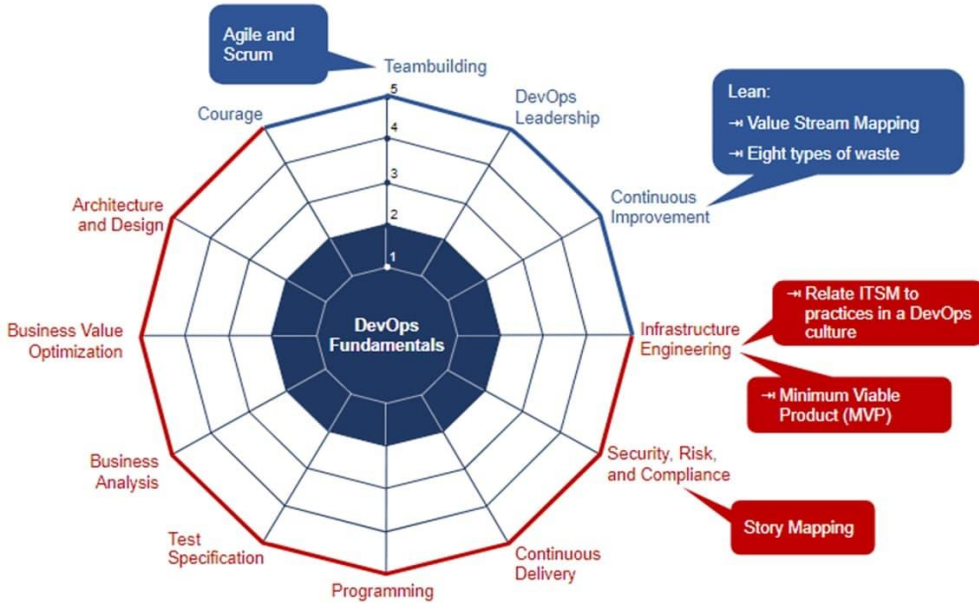




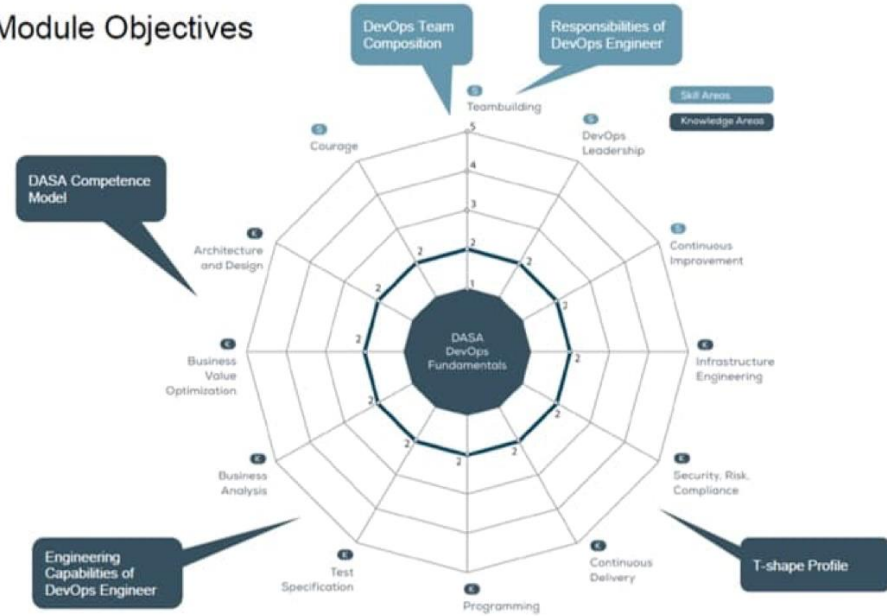
02 Метрики DevSecOps в Secure SDLC

Радар здоровья DASA DevOps
SAFe Essential
Shift-Left by TDD & BDD
PI by ART
Architectural Runway
Story Mapping by Security Default

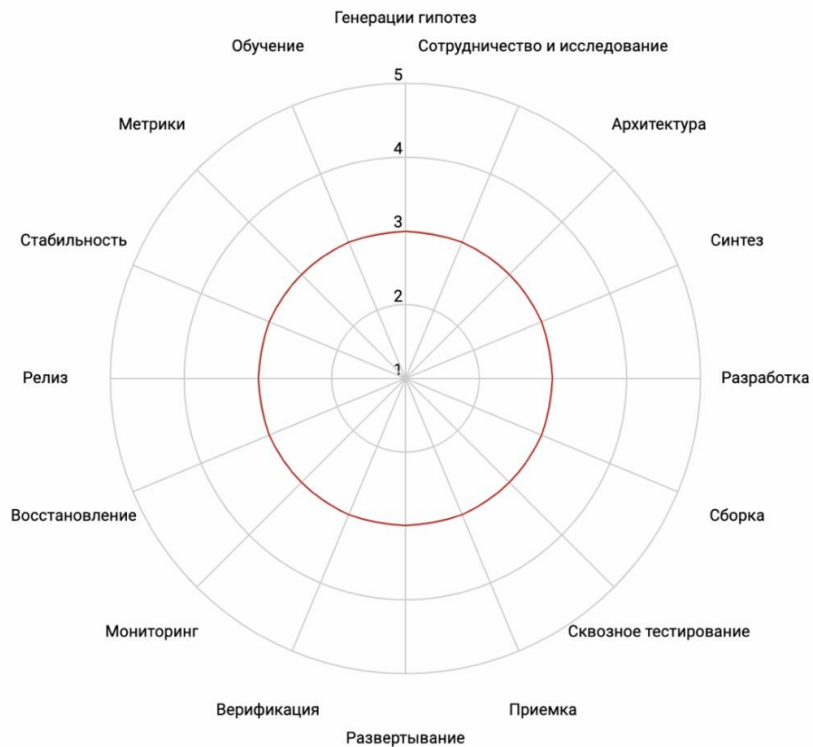
Радар DASA DevOps Fundamentals



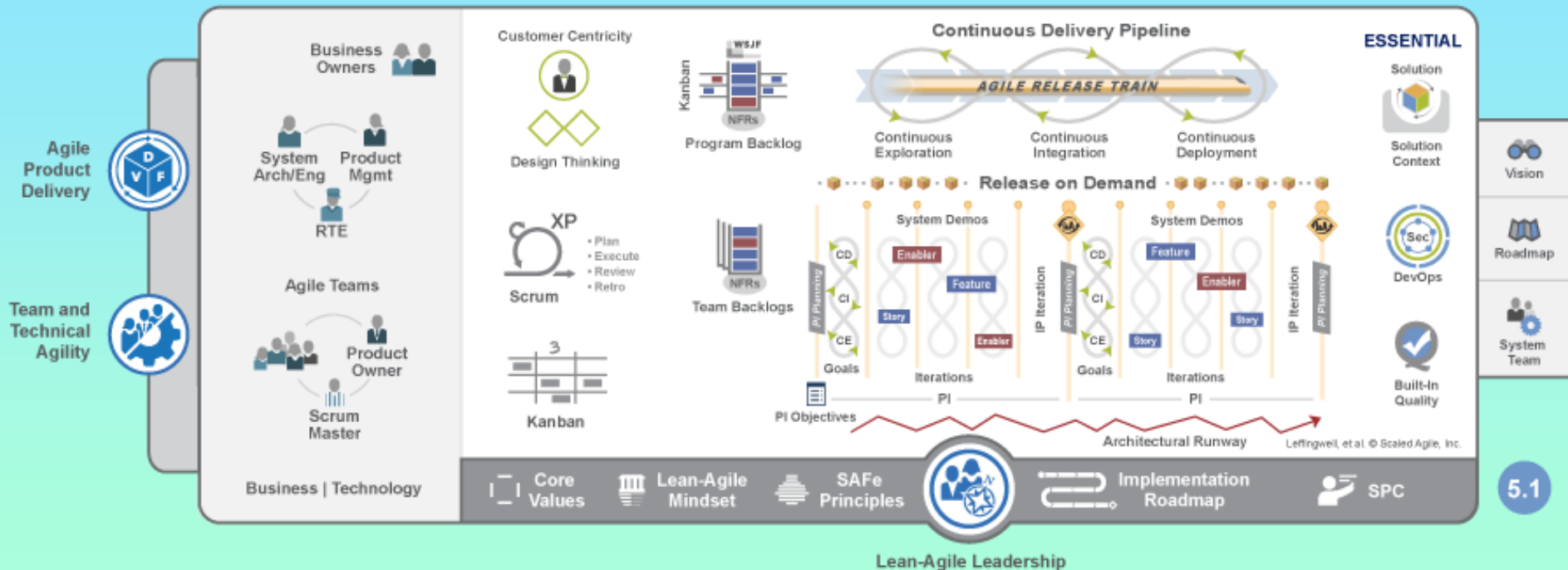
Module Objectives



Радар здоровья DASA DevOps

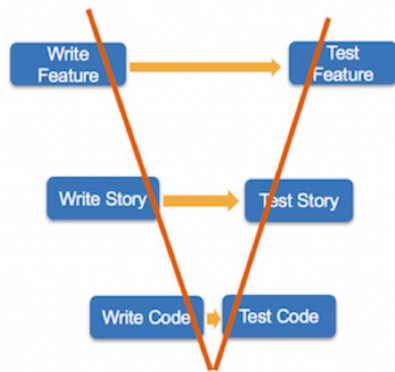


SAFe Essential

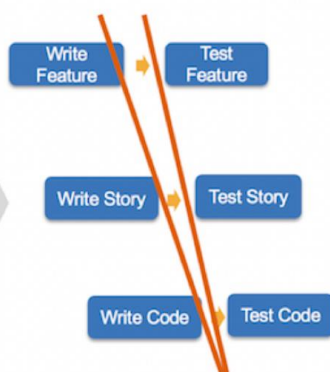


Shift-Left в проекции Secure SDLC (TDD, BDD, PipeLine)

Tradition "V" Model delays feedback

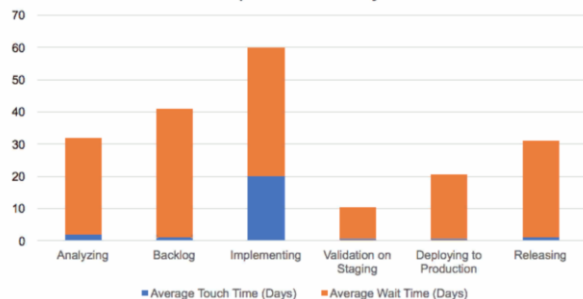


Shift left for fast feedback



Примечание: время реальной работы (touch time) — это время, когда команды добавляет ценность к своему продукту или услуге. Обычно это время составляет небольшой процент (10-20%) от общего времени производства (cycle time), потому что большая часть времени теряется в очередях (ожиданиях) и тратится на перемещения работы из одного состояния в другое.

Pipeline Efficiency



Инкрементальная и итеративная разработка

Инкрементальный: Разработка по частям, имея в виду конечный результат



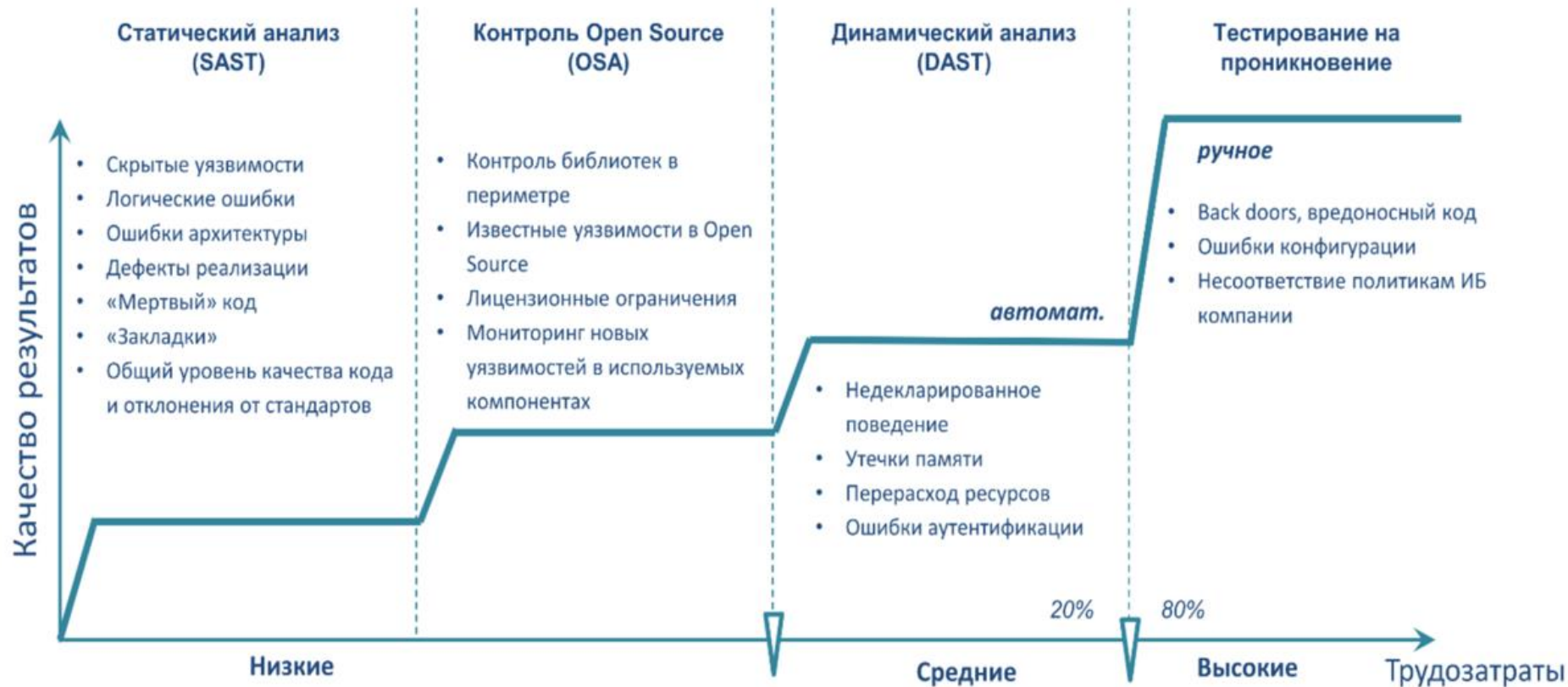
Итеративный: Разработка сырой версии продукта, проверка, затем дальнейшее построение с наращиванием качества и функционала.



© Scaled Agile, Inc



Этапы тестирования Shift-Left



Метрики здоровья продукта по инкременту продукта

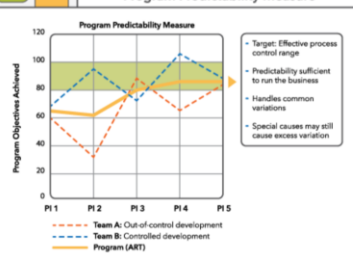
Functionality	PI 1	PI 2	PI 3
Program velocity			
Predictability measure			
# Features planned			
# Features accepted			
# Enabler features planned			
# Enabler features accepted			
# Stories planned			
# Stories accepted			
Quality			
Unit test coverage %			
Defects			
Total tests			
% automated			
# NFR tests			

© Scaled Agile, Inc.

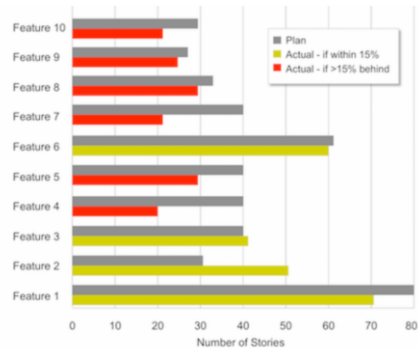
Team PI Performance Reports

Objectives for PI 3	Plan	Actual
Structured locations and validation of locations	7	7
Build and demonstrate a proof of concept for context images	8	8
Implement negative triangulation by: tags, companies and people	8	6
Speed up indexing by 50%	10	5
Index 1.2 billion more web pages	10	8
Extract and build URL abstracts	7	7
Stretch Objectives		
Fuzzy search by full name		
Improve tag quality to 80% relevance		
Totals		
% Achievement: 90%		

Program Predictability Measure

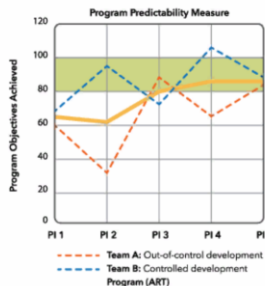


© Scaled Agile, Inc.

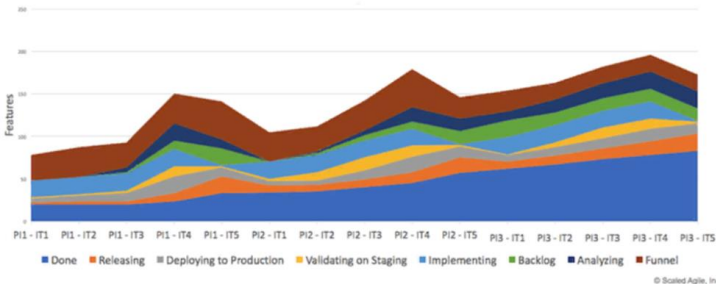


© Scaled Agile, Inc.

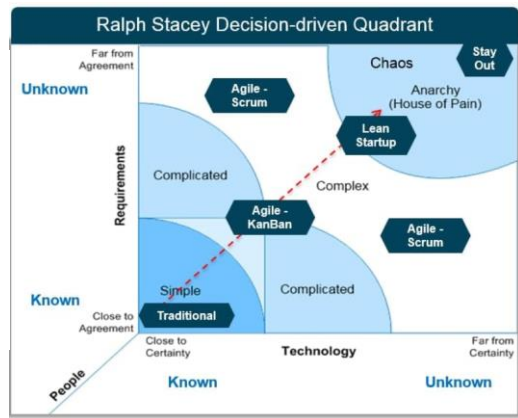
Objectives for PI 3	Plan	Actual
Structured locations and validation of locations	7	7
Build and demonstrate a proof of concept for context images	8	8
Implement negative triangulation by: tags, companies and people	8	6
Speed up indexing by 50%	10	5
Index 1.2 billion more web pages	10	8
Extract and build URL abstracts	7	7
Stretch Objectives		
Fuzzy search by full name	7	0
Improve tag quality to 80% relevance	4	4
Totals	50	45
% Achievement: 90%		



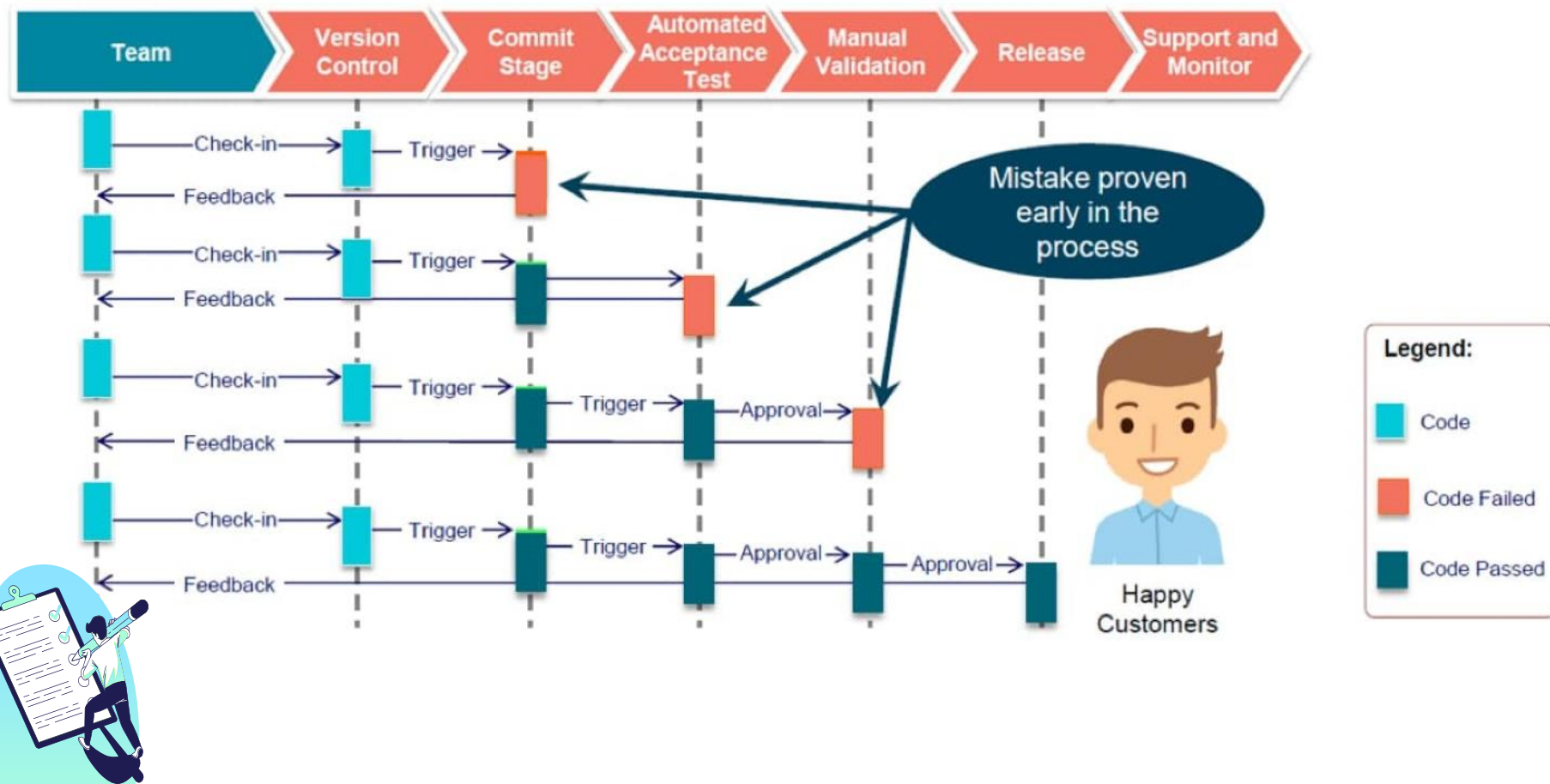
© Scaled Agile, Inc.



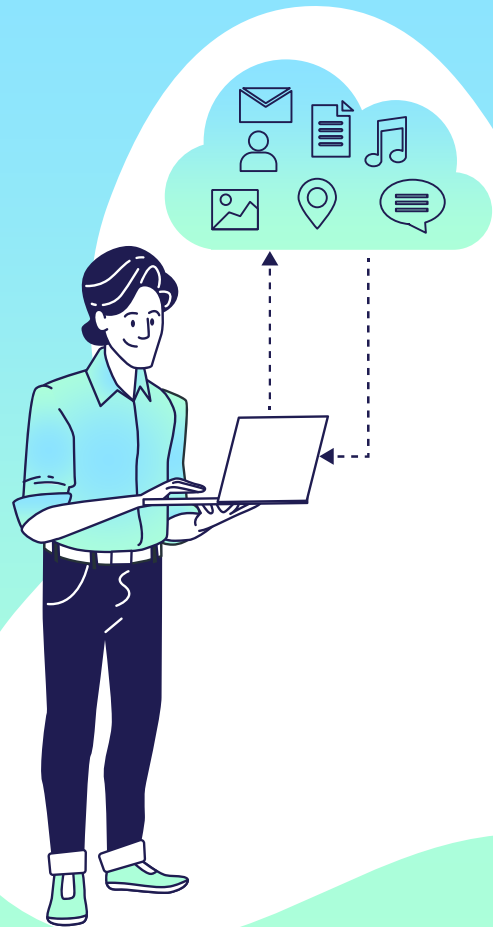
© Scaled Agile, Inc.



Architectural Runway минимизации потерь



03 DevSecOps: процесс построения Secure SDLC



Рекомендации DevSecOps при управлении



- Правильно выстроенный процесс важнее инструментов.
- Не внедряйте всё и сразу. Начните с того, что у вас уже есть, и двигайтесь итерационно.
- Функциональные дефекты и дефекты **ЗИ** - равны.



- Выращивайте в своих командах **Security Champions** и задействуйте в процессе разработки – это повысит поток ценности **Secure SDLC**.
- Помните, что качество продукта — это общая цель.
- Важнее люди, а не процесс.
- Разделяйте влияние **DT Stacks**.



- Автоматизируйте по максимуму – **Infrastructure-as-a-Code** to **Everything-as-a-Code**.
- Выбирайте процессы и инструменты, подходящие именно для вашего продукта.
- Делайте упор на метрики здоровья и зрелости продукта, что бы нивелировать **legging**.

Рекомендации построения по SOLID

Принцип одной ответственности

Разделение на выполнение одной функции – **micro-services**.

Принцип открытости/закрытости

Открыты для расширения, закрыты для изменений. Отсутствие модификаций при масштабируемости.

Принцип подстановки Барбары Лисков

Не должно быть зависимости от способа реализации.

Принцип разделения интерфейса

Разделение прототипирования на взаимосвязи.

Принцип инверсии зависимостей

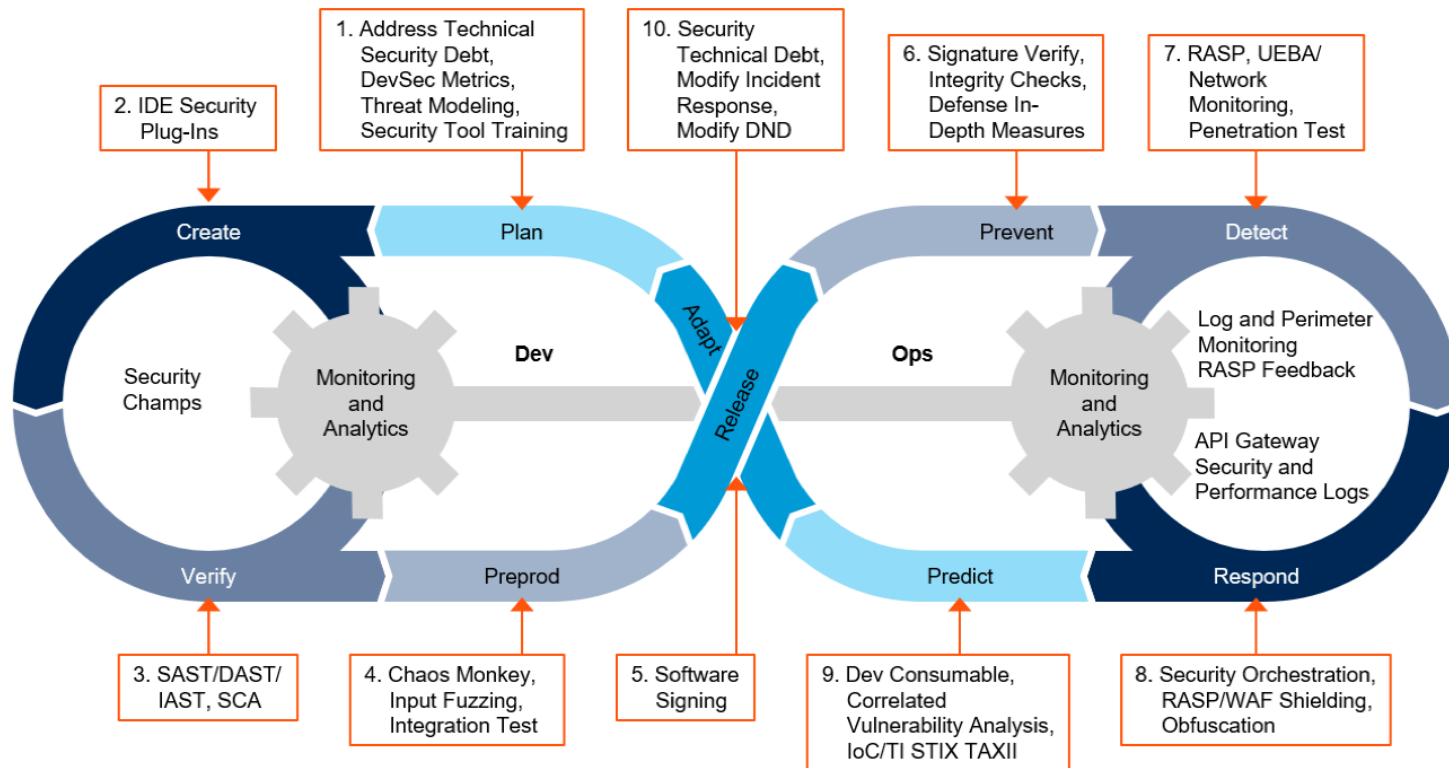
Высокоуровневые модули не должны зависеть от низкоуровневых.

Health Check

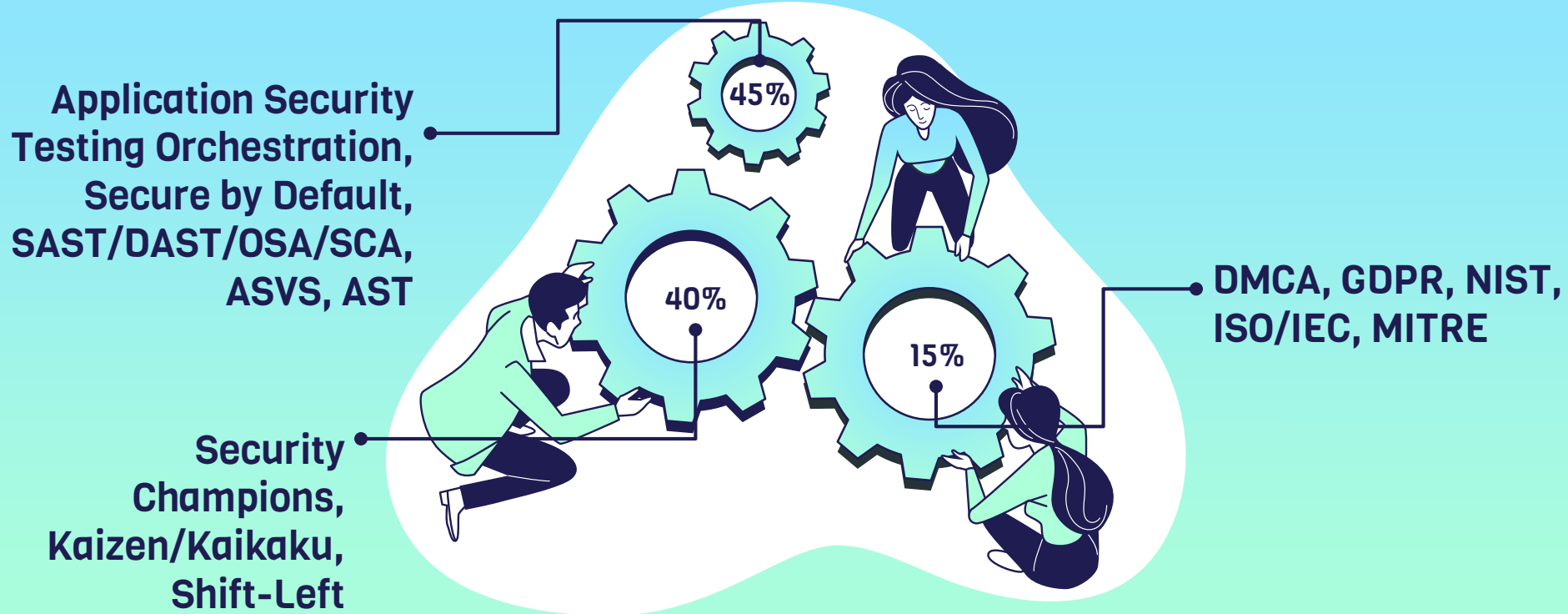
Контроль и адаптации здоровья метрик.

Процесс построения Secure SDLC

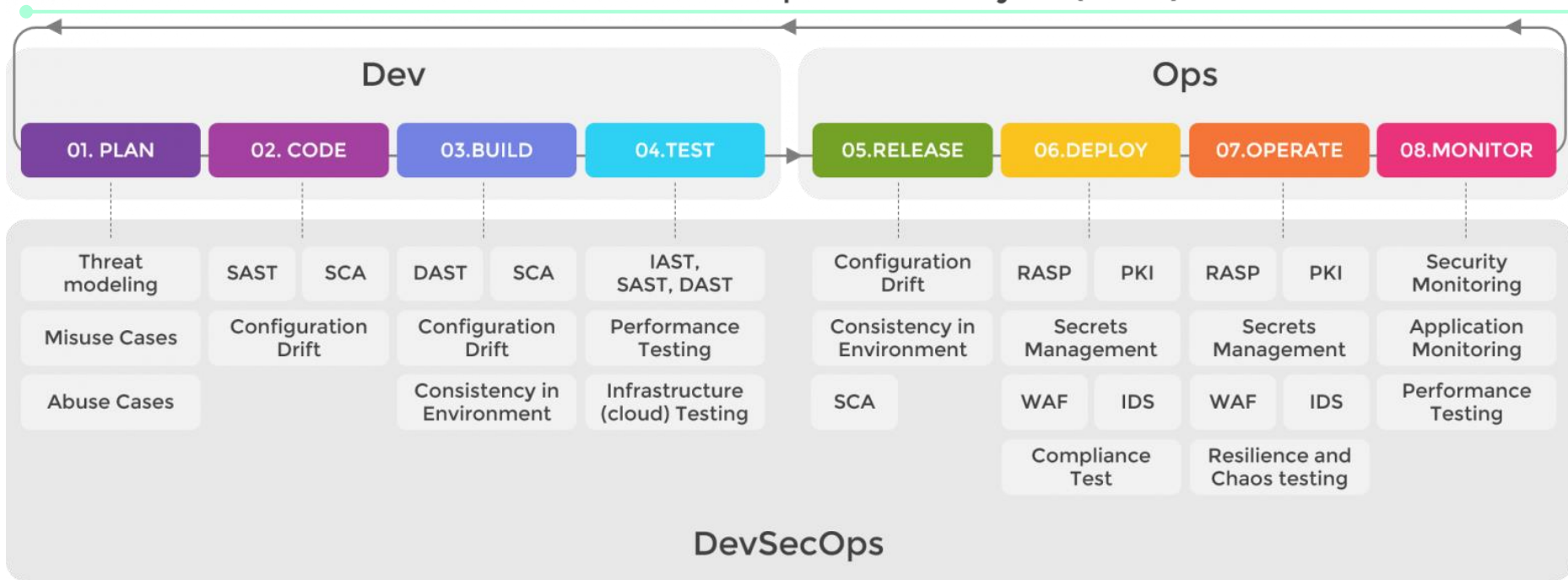
The DevSecOps Toolchain



Эффективность построения метрик в DevSecOps



Secure Software Development Life Cycle (SSDL)



Минимально необходимое для реализации **DevSecOps**:

- Контроль компонент с открытым исходным кодом при попадании в периметр разработки (Open Source Analysis, **OSA**);
- Статический анализ кода (Static Application Security Testing, **SAST**);
- Контроль состава компонент ПО (Software Composition Analysis, **SCA**);
- Все виды динамического анализа (Dynamic Application Security Testing, **DAST** / Interactive Application Security Testing, **IAST** / Behavioral Application Security Testing, **BAST**);
- Анализ бинарного кода и контроль состава контейнеров (Bytecode and Container Analysis, **BCA**);
- Реализация **WAF** (Web Application Firewall).

Lead Time

Снижение времени поставки ценности продукта.

01

Health Check

- Гарантированное время восстановления.
- %A/C -> 98% (accuracy/complete): DoR, DoD.

04

Production Time

Снижение времени на выполнение работ.

02

Время реализации изменений

- Доля автоматического тестирования.
- Контроль масштабируемости.
- Ретроспектива.

05

Частота развертывания

- Количество релизов в единицу времени.
- Контроль версионности.
- Доля отказов.

03

Security Check

- Аудит.
- Контроль артефактов.
- Обеспечение Паркеровской гексады.
- Burn down chart.
- Impediment chart.

06

Спасибо!

Есть ли у вас какие-то вопросы?

shmakovis@inbox.ru

+7 982 348-10-98

@shmakovis



CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik** and illustrations by Stories

Please keep this slide for attribution.

