OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Меня хорошо видно && слышно?

Ставьте  , если все хорошо

Напишите в чат, если есть проблемы

Проверить, идет ли запись!

Методологии безопасной разработки (SSDL)

Колесников Александр

Правила вебинара

Активно участвуем

Задаем вопросы в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара

SSDL

Методики

Рефлексия

Практика?

Цели

1. Получить представление о SSDL
2. Познакомиться с основными этапами
3. Воспроизвести отдельные этапы

SSDL?
Secondary Standards Dosimetry Laboratories?

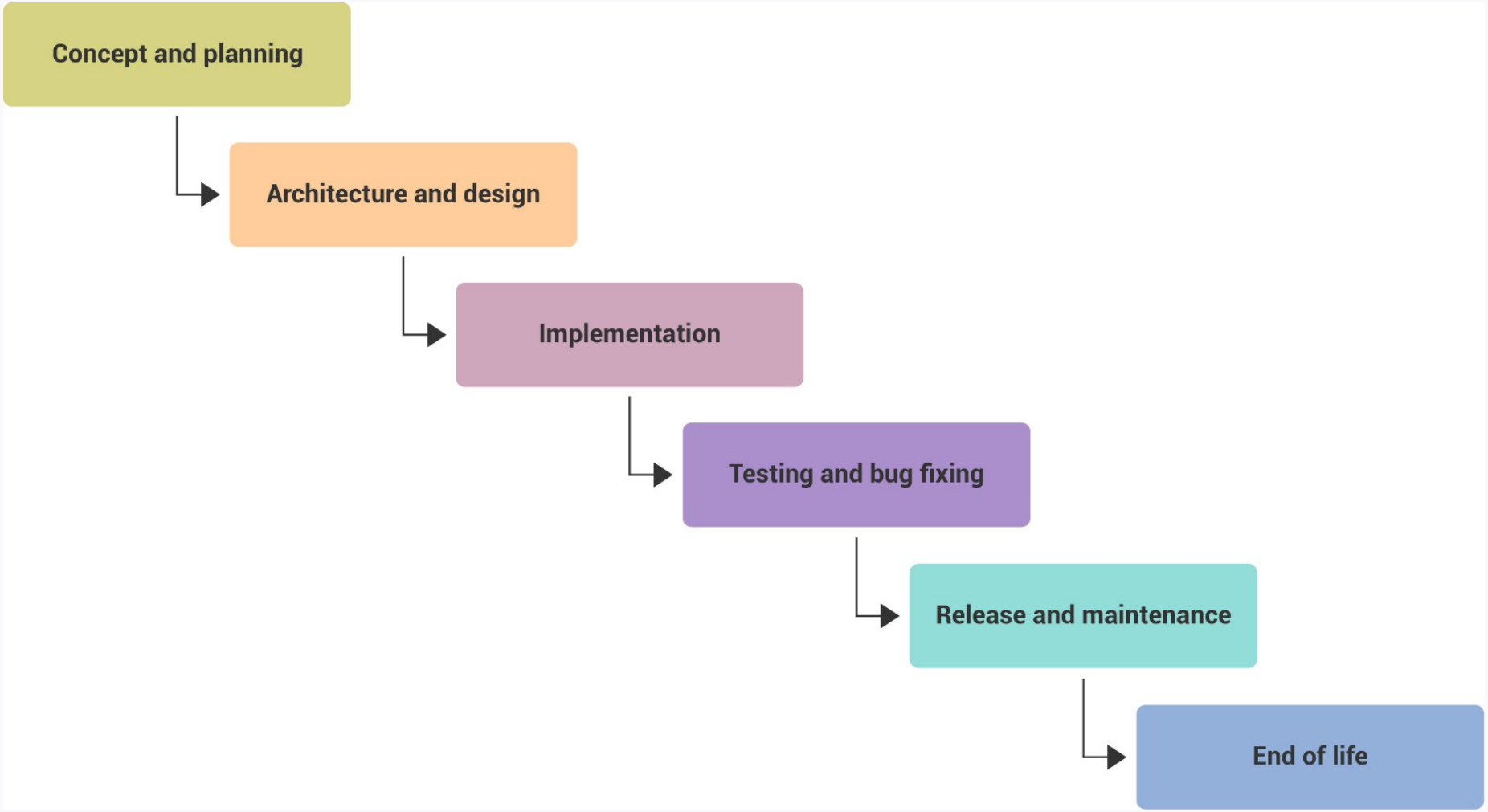
Что такое SSDL?

- **S**ecure **S**oftware **D**evelopment **L**ifecycle - процесс направленный на предотвращение появления уязвимостей

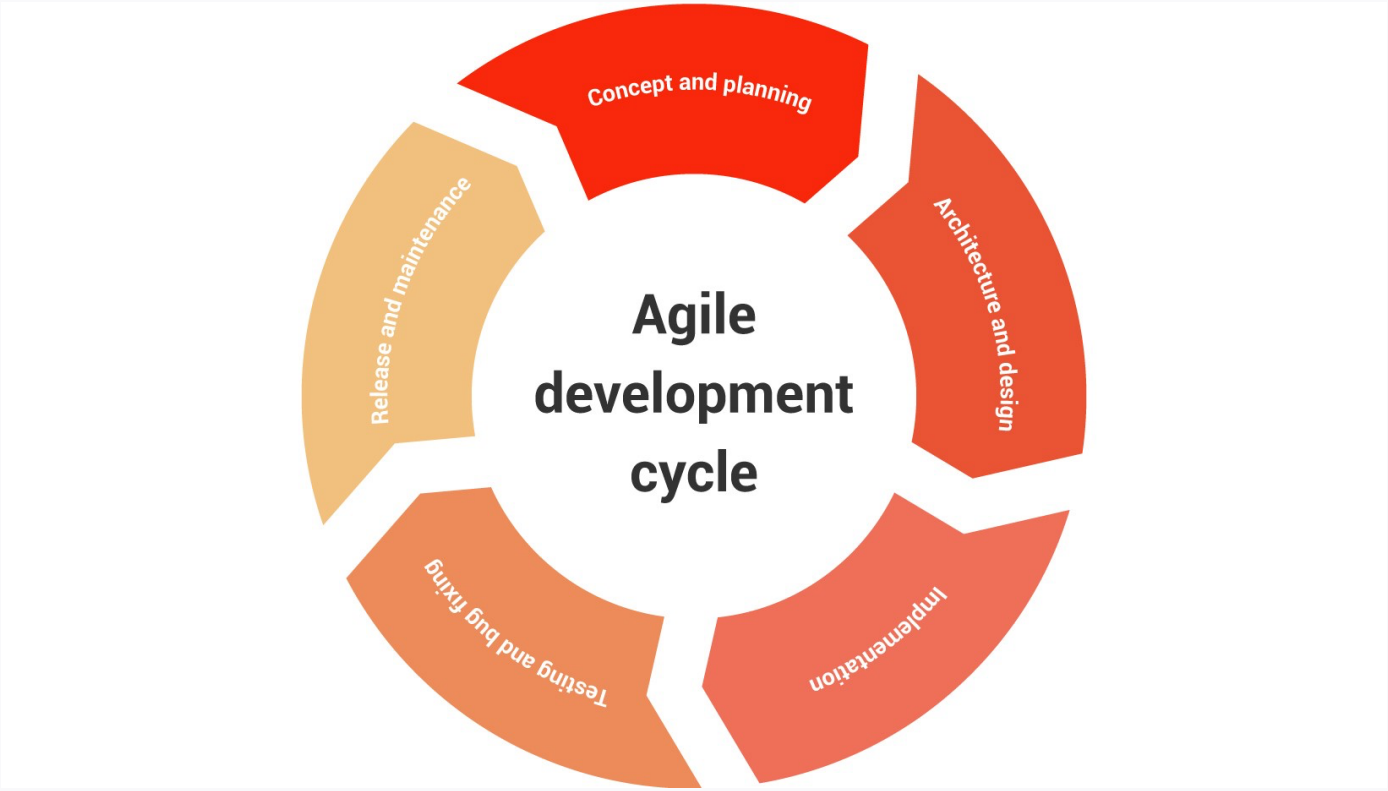
- Свод этапов, правил и соглашений, которые должны присутствовать на каждом этапе разработки.

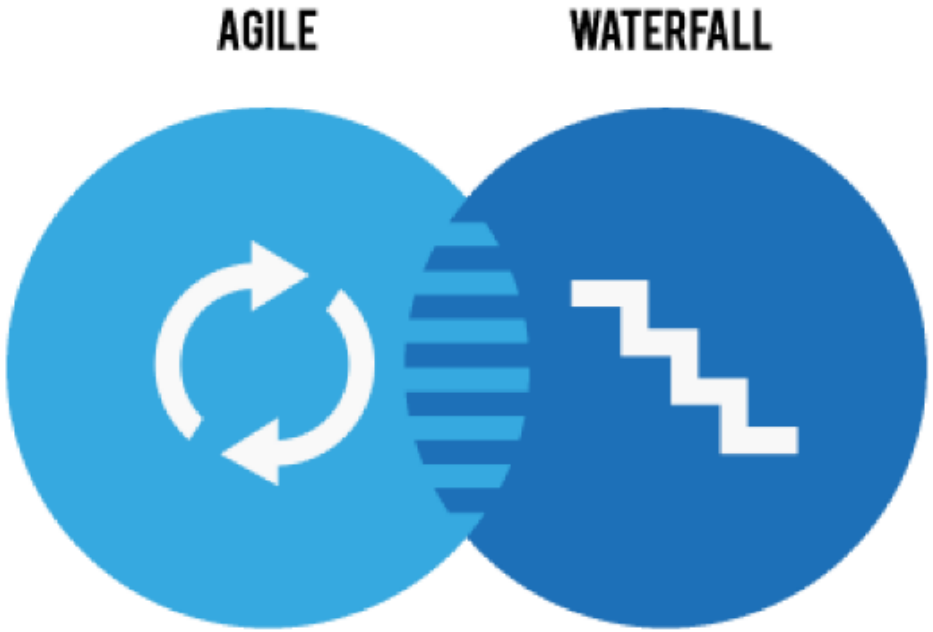
С чего всё началось

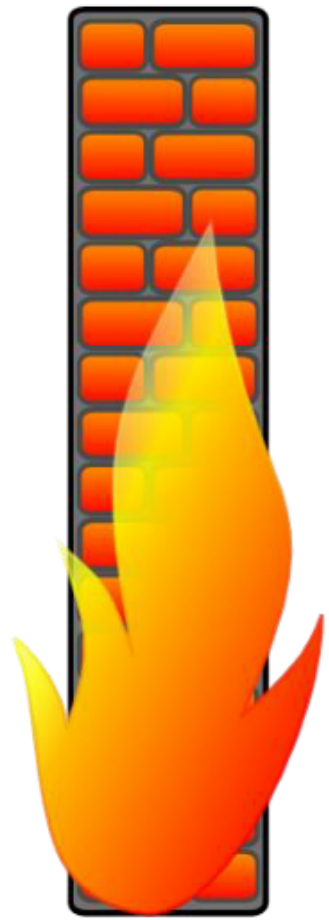
Подходы к разработке



Подходы к разработке



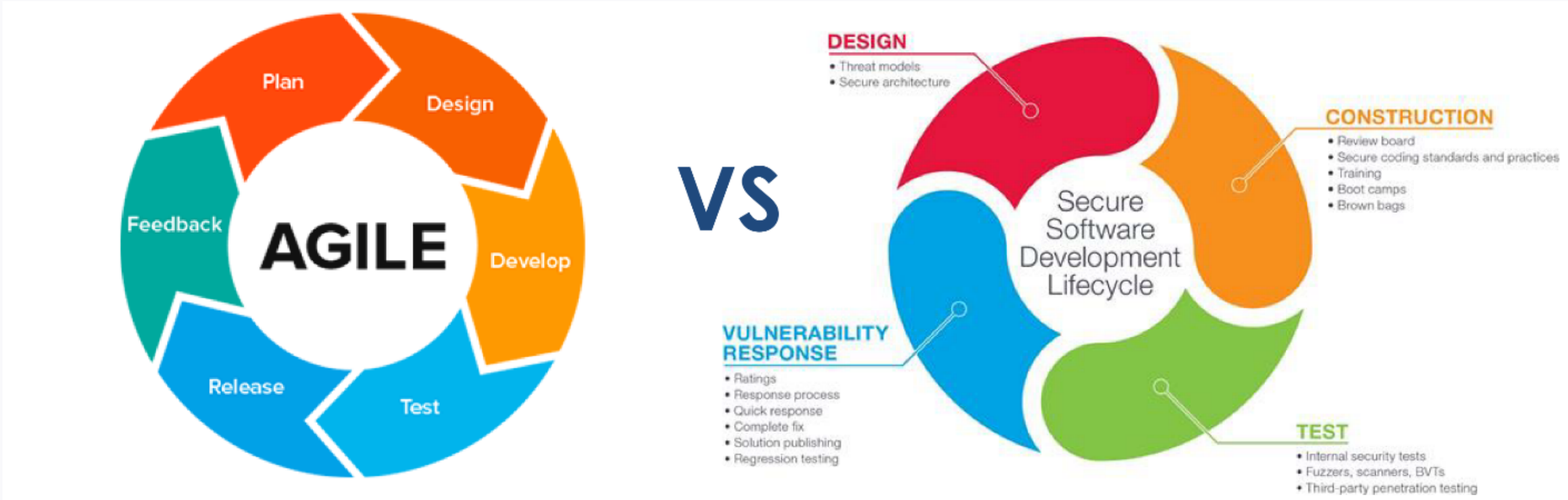




wall

Security

Как сделать безопасно?

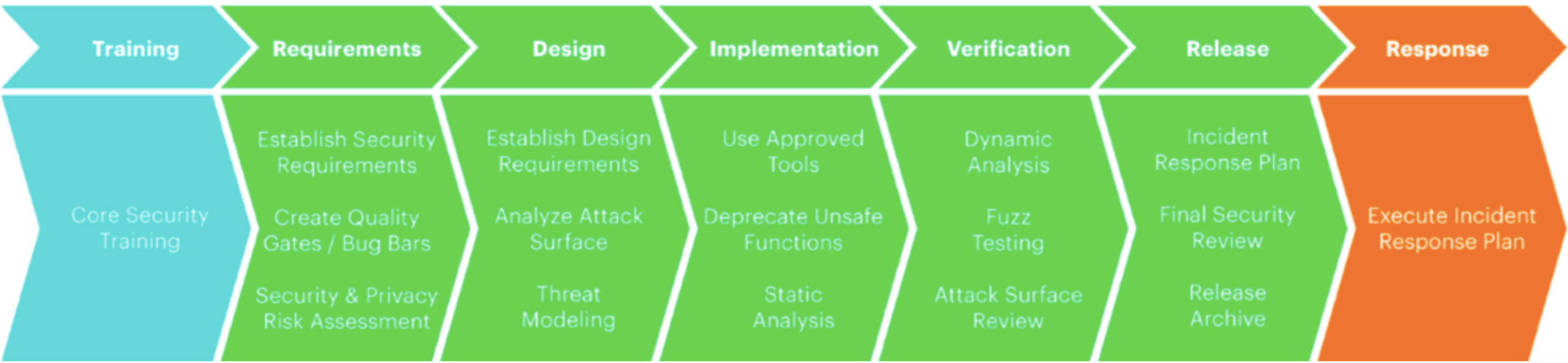


Какие подходы существуют?

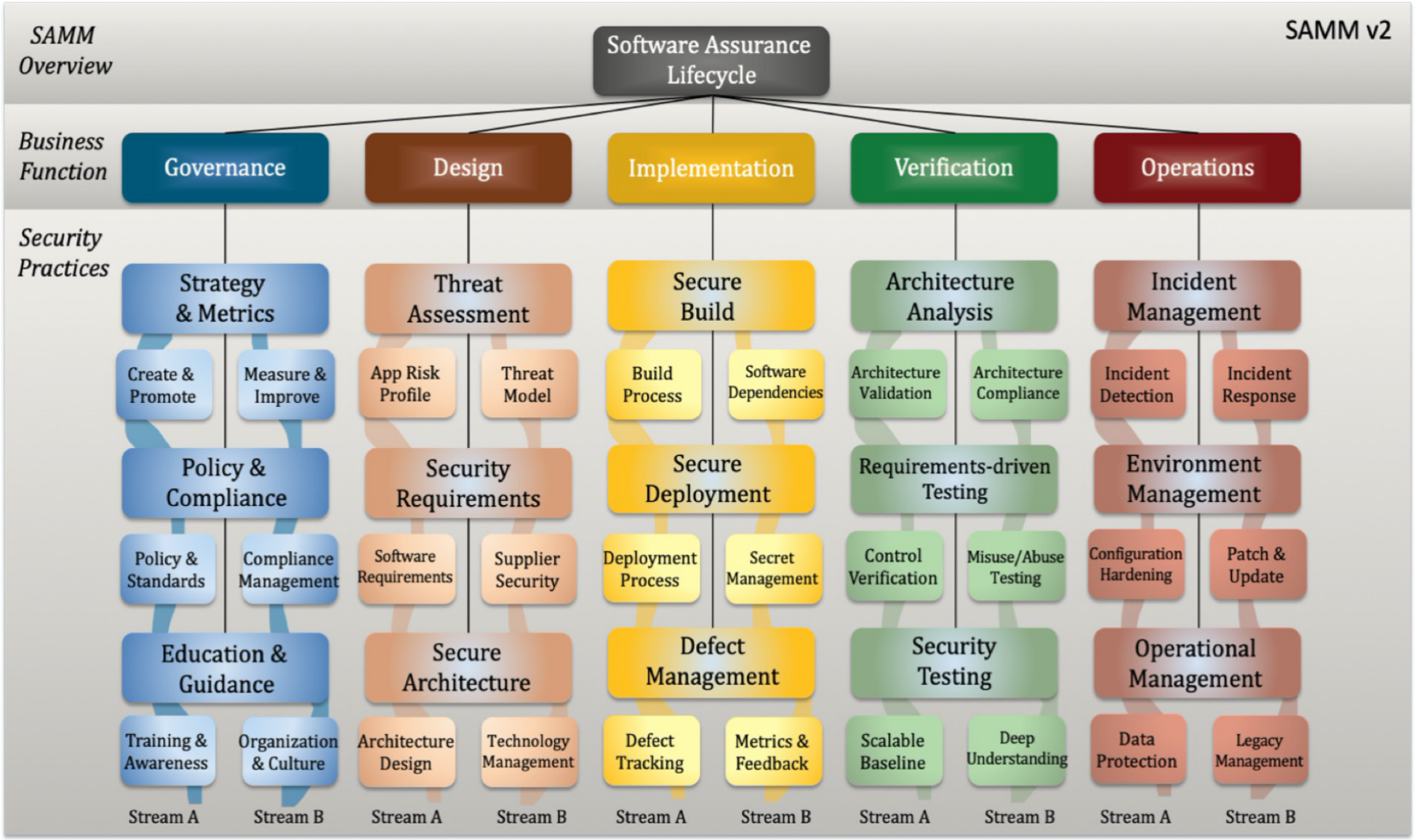
- Microsoft SDL
- SAMM
- BSIMM

1. Выбор подхода базируется на знаниях собственного процесса разработки
2. В любом случае метод это не жесткие требования, а рекомендации
3. Нужно проводить адаптацию для каждого из этапов

Microsoft SDL



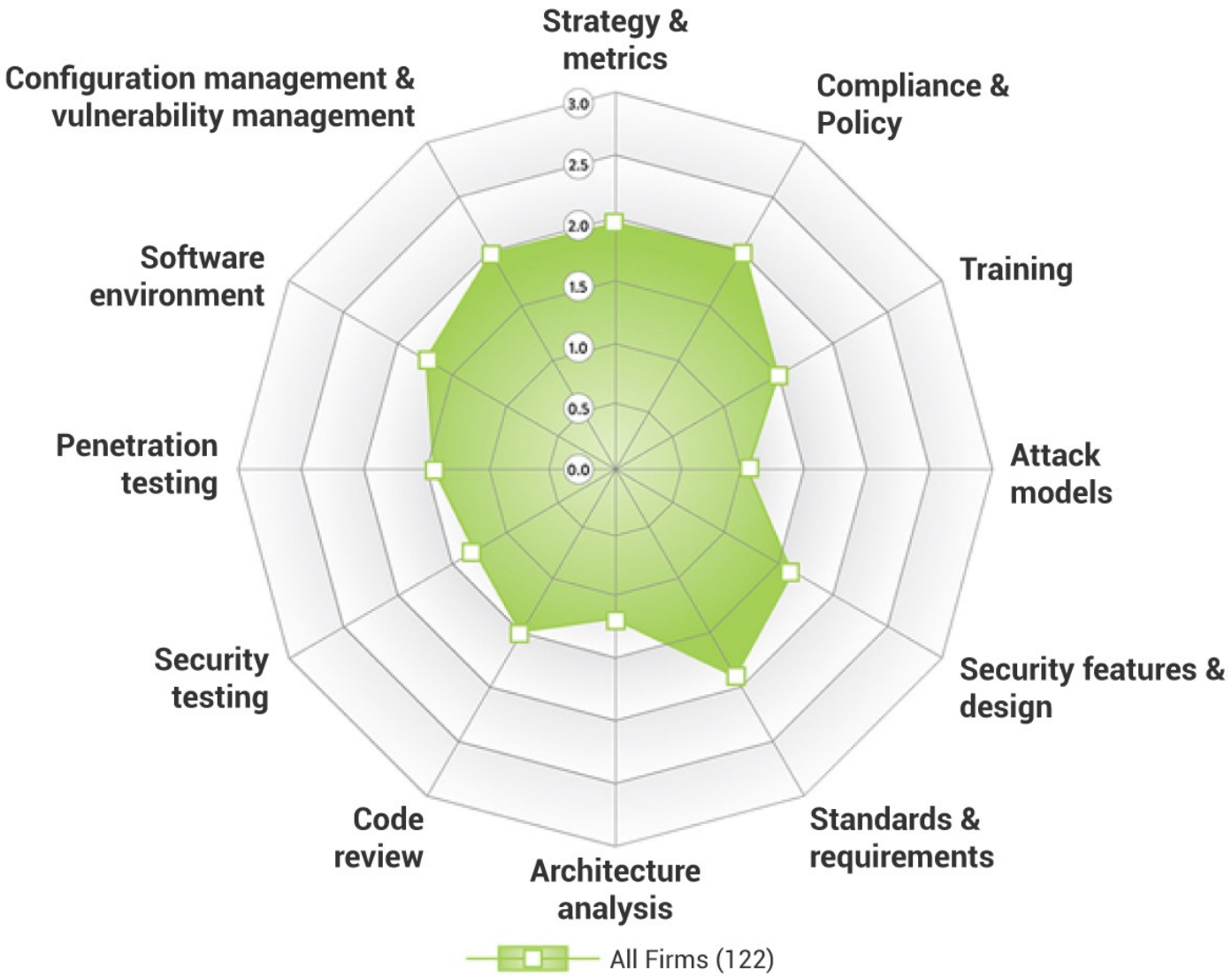
SAMM V2.0


SAMM Overview
SAMM v2
Software Assurance Lifecycle
Business Function
Governance
Design
Implementation
Verification
Operations
Security Practices
Strategy & Metrics
Create & Promote
Measure & Improve
Policy & Compliance
Policy & Standards
Compliance Management
Education & Guidance
Training & Awareness
Organization & Culture
Threat Assessment
App Risk Profile
Threat Model
Security Requirements
Software Requirements
Supplier Security
Secure Architecture
Architecture Design
Technology Management
Secure Build
Build Process
Software Dependencies
Secure Deployment
Deployment Process
Secret Management
Defect Management
Defect Tracking
Metrics & Feedback
Architecture Analysis
Architecture Validation
Architecture Compliance
Requirements-driven Testing
Control Verification
Misuse/Abuse Testing
Security Testing
Scalable Baseline
Deep Understanding
Incident Management
Incident Detection
Incident Response
Environment Management
Configuration Hardening
Patch & Update
Operational Management
Data Protection
Legacy Management
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B

Особенности SAMM v2.0

- Оценка уровня обеспечения информационной безопасности
- После оценки создается программа для внедрения процедур и практик для безопасной разработки
- Необязательно приводить все процессы к идеалу, есть описание того как это делать постепенно
- Разделы для всех активностей можно изучать отдельно и выбирать то, что нужно
- Внутри фреймворка:
  - 5 бизнес-функций
  - 3 практики по информационной безопасности
  - 2 активности по каждой из практик

BSIMM


Strategy & metrics
Compliance & Policy
Training
Attack models
Security features & design
Standards & requirements
Architecture analysis
Code review
Security testing
Penetration testing
Software environment
Configuration management & vulnerability management
3.0
2.5
2.0
1.5
1.0
0.5
0.0
All Firms (122)

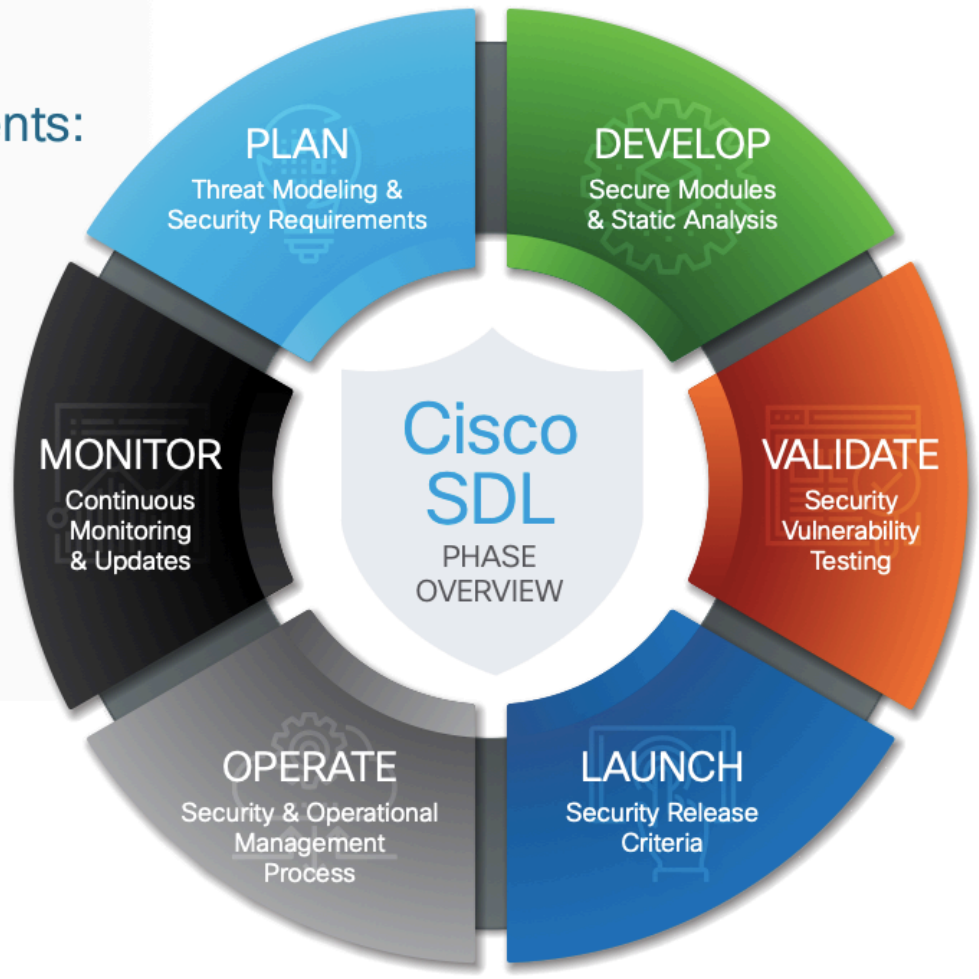
Особенности BSIM 10

- Фреймворк включает в себя:
  - 4 домена
  - Каждый домен включает по 12 практик
  - Всего 112 активностей
  - У каждой из активностей есть уровни зрелости их 3
- Необязательно приводить все процессы к идеалу, есть описание того как это делать постепенно
- Разделы для всех активностей можно изучать отдельно и выбирать то, что нужно

CISCO SDL

Cisco SDL is better described by examining its compositional elements:

- Product Security Requirements
- 3rd Party Security
- Secure Design
- Secure Coding
- Secure Analysis
- Vulnerability Testing



Следующий вебинар

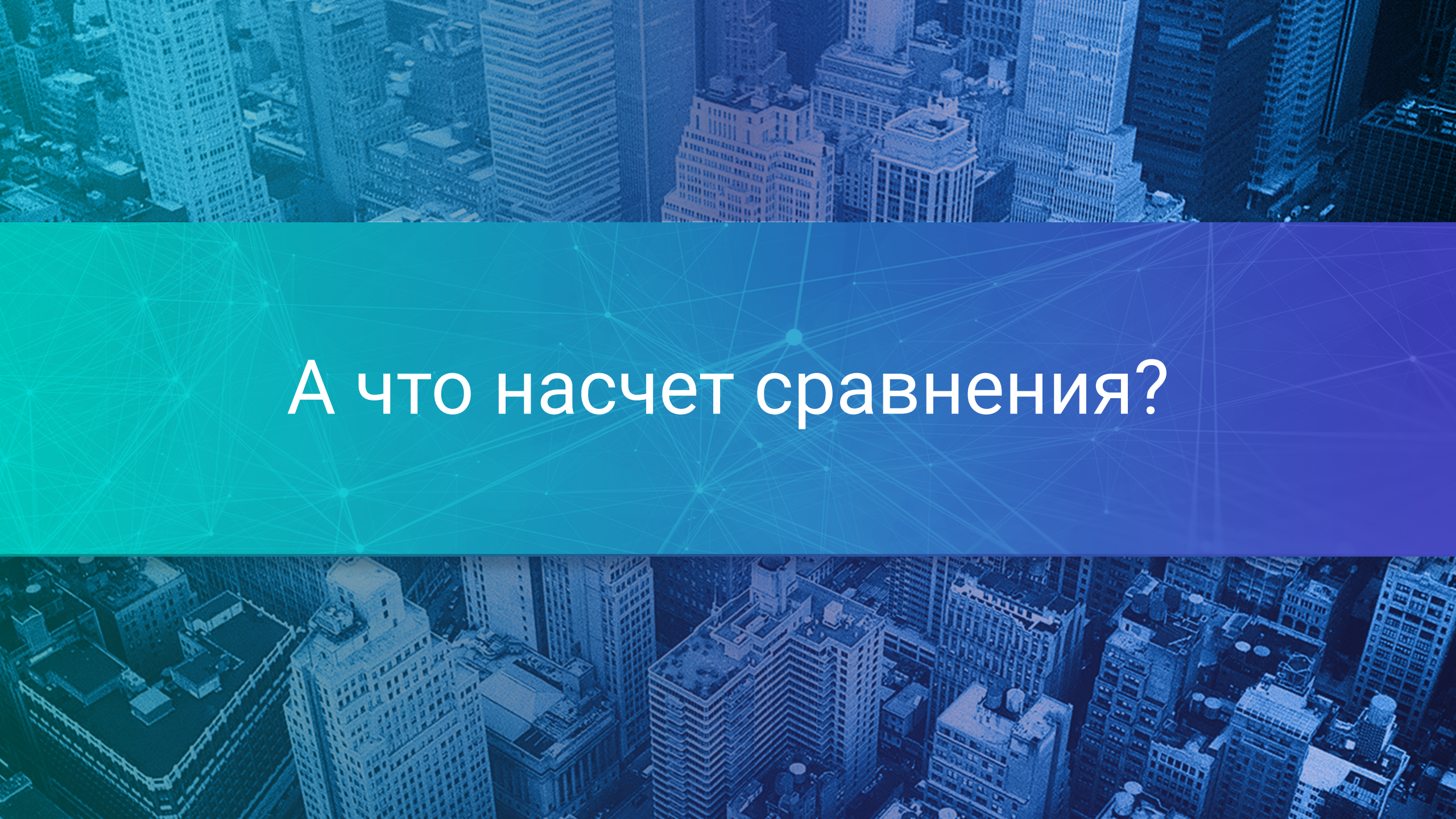
Тема:

Утилиты для статического и динамического анализа защищенности веб-приложений: DAST/SAST/IAST

Ссылка на вебинар будет в ЛК за 15 минут

Материалы к занятию в ЛК — можно изучать

Обязательный материал обозначен красной лентой


А что насчет сравнения?


Заполните, пожалуйста,
опрос о занятии по ссылке в чате

Спасибо за внимание!
Приходите на следующие вебинары

Колесников Александр