СБЕРБАНК ТЕХНОЛОГИИ

Практика Software Security в СБТ

ЮРИЙ СЕРГЕЕВ

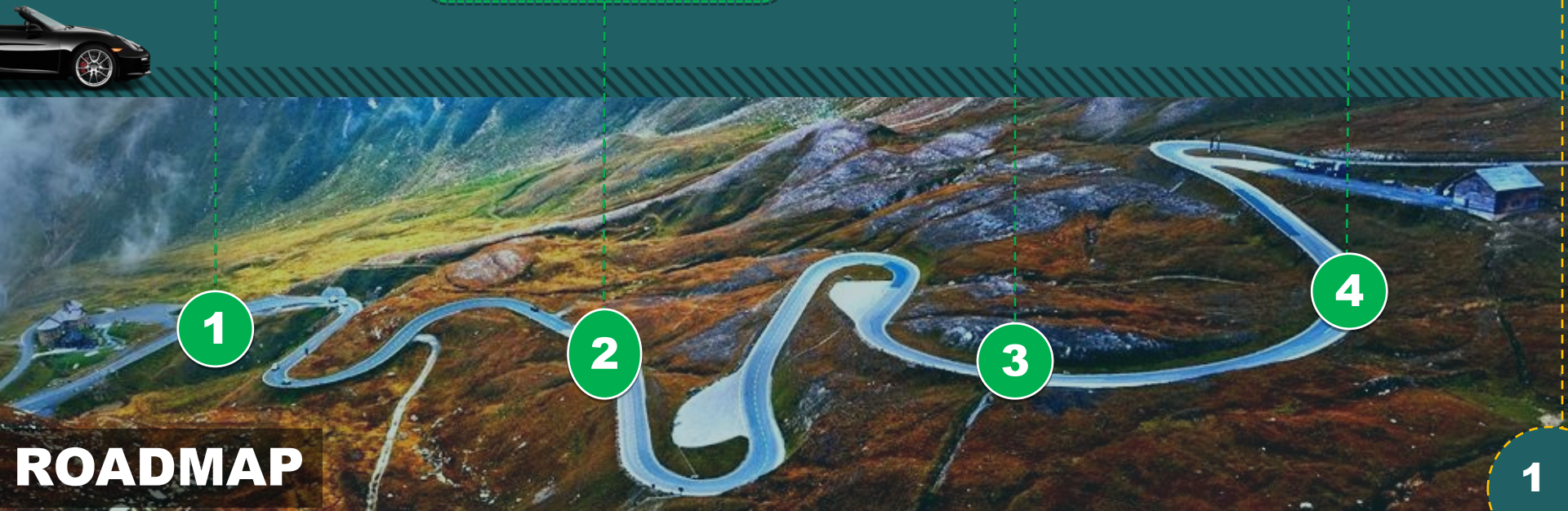
- **Общий контекст**
- **Вызовы индустрии**

Изменение процесса

- Базовые подходы и методики
- Развитие компетенций
- Стратегия тиражирования

Инфраструктура

Целевая модель



ROADMAP

ЗАДАЧИ

Комплексно интегрировать практики защиты ПО в жизненный цикл разработки (SDLC) для крупнейшего Банка России и Восточной Европы.

СЛОЖНОСТИ & ОПАСЕНИЯ

- Позиционирование сервиса внутри и взаимодействие с производственными подразделениями
- Несовершенный инструментарий
- Минимальная экспертиза на рынке
- Масштабирование

МИФЫ vs. РЕАЛЬНОСТЬ

Защищенность разрабатываемого продукта может быть достигнута с помощью тестирования (security testing) перед выпуском и последующим исправлением найденных дефектов.

Реактивный подход > Непрактично

- Позднее обнаружение
- Дорогое исправление
- Минимум активностей

Устранение уязвимостей только изменением дизайна / требований:

- Эффективнее на этапе проектирования
- Дорого, если уязвимости упущены на ранних стадиях

Необходим end-to-end процесс на ВСЕХ стадиях жизненного цикла ПО

МИФЫ vs РЕАЛЬНОСТЬ

Разработка защищенных приложений – крайне дорогая инициатива, которая осуществляется только для достижения формального соответствия стандартам и требованиям регуляторов. Этот процесс зачастую сдвигает сроки поставки продуктов и не приносит осязаемой пользы.

Стоимость незначительна

- vs. Стоимость разработки
- vs. Стоимость (прямой и косвенной) устранения последствий инцидентов

Защита корпоративных активов и клиентских данных

- Соответствие стандартам – вторичная цель

Следование стандартному процессу

- Не влияет на сроки
- Негативное влияние – несистемные, фрагментарные активности прямо перед релизом продукта

БАЗОВЫЕ ПОДХОДЫ

СТРАТЕГИЯ

- Интеграция в проекты на начальных стадиях жизненного цикла разработки

МАСШТАБИРУЕМОСТЬ

- Развитие внутренних ключевых компетенций
- Автоматизация процесса

ПРИОРИТЕТЫ

- Приложения и сервисы с высоким уровнем риска
- Фокус на базовые практики Software Security
  20% усилий vs. 80% эффекта
- Реалистичные угрозы и уязвимости

РАЗРАБОТКА ЗАЩИЩЕННОГО ПО

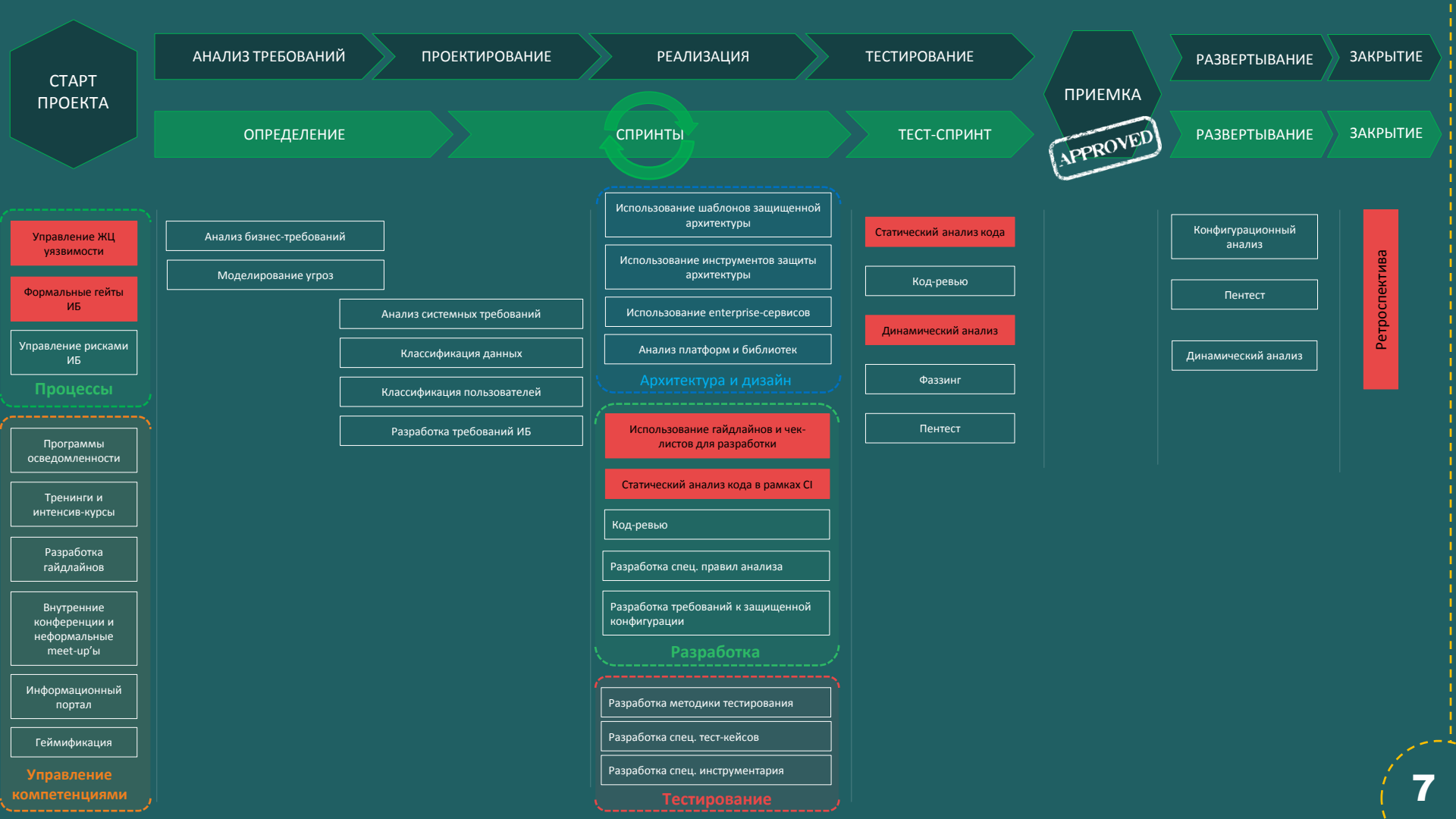
OWASP

BSIMM

OpenSAMM

СТО БР ИББС

СТАНДАРТЫ БЕЗОПАСНОСТИ vs ПРОЦЕСС РАЗРАБОТКИ


СТАРТ ПРОЕКТА
АНАЛИЗ ТРЕБОВАНИЙ
ПРОЕКТИРОВАНИЕ
РЕАЛИЗАЦИЯ
ТЕСТИРОВАНИЕ
ПРИЕМКА
РАЗВЕРТЫВАНИЕ
ЗАКРЫТИЕ
ОПРЕДЕЛЕНИЕ
СПРИНТЫ
ТЕСТ-СПРИНТ
APPROVED
РАЗВЕРТЫВАНИЕ
ЗАКРЫТИЕ
Управление ЖЦ уязвимости
Формальные гейты ИБ
Управление рисками ИБ
Процессы
Анализ бизнес-требований
Моделирование угроз
Анализ системных требований
Классификация данных
Классификация пользователей
Разработка требований ИБ
Использование шаблонов защищенной архитектуры
Использование инструментов защиты архитектуры
Использование enterprise-сервисов
Анализ платформ и библиотек
Архитектура и дизайн
Использование гайдлайнов и чек-листов для разработки
Статический анализ кода в рамках CI
Код-ревью
Разработка спец. правил анализа
Разработка требований к защищенной конфигурации
Разработка
Разработка методики тестирования
Разработка спец. тест-кейсов
Разработка спец. инструментария
Тестирование
Статический анализ кода
Код-ревью
Динамический анализ
Фаззинг
Пентест
Конфигурационный анализ
Пентест
Динамический анализ
Ретроспектива
Программы осведомленности
Тренинги и интенсив-курсы
Разработка гайдлайнов
Внутренние конференции и неформальные meet-up'ы
Информационный портал
Геймификация
Управление компетенциями

БАЗОВЫЕ МЕТОДИКИ

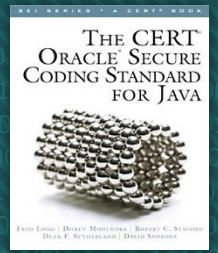
OWASP Testing Guide v.4

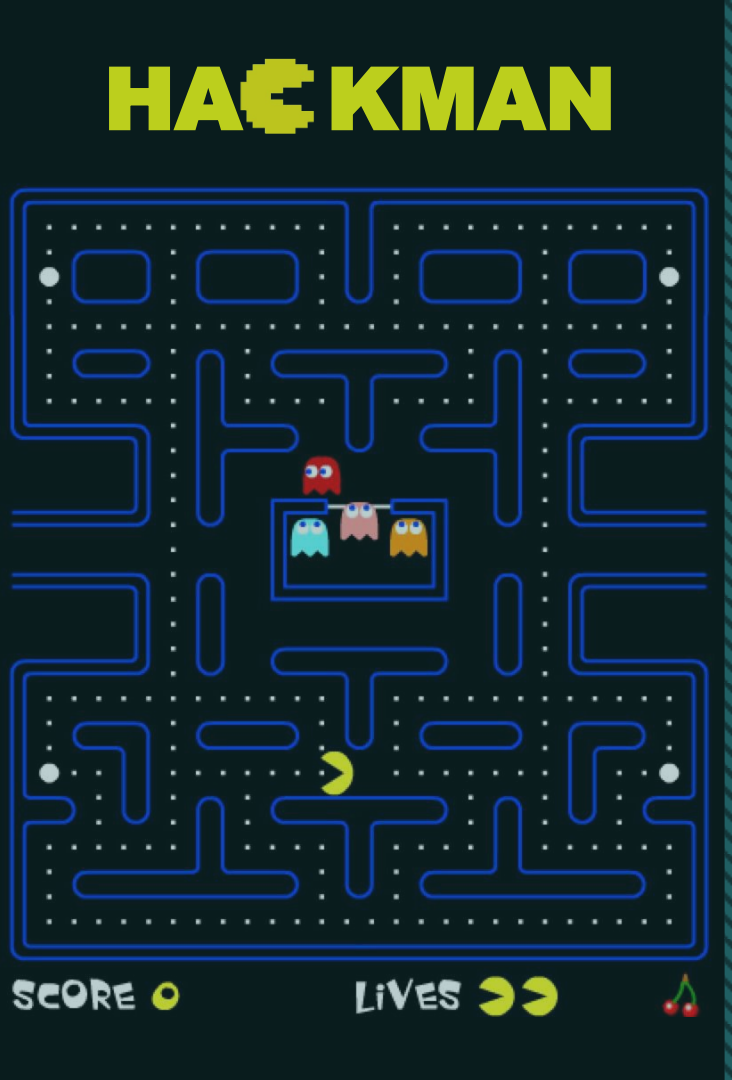
OWASP Application Security Verification Standard v.3

CERT Oracle Coding Standard for Java

Рекомендации ЦБ: Обеспечение ИБ на стадиях жизненного цикла АБС

Собственный план проведения тестирования



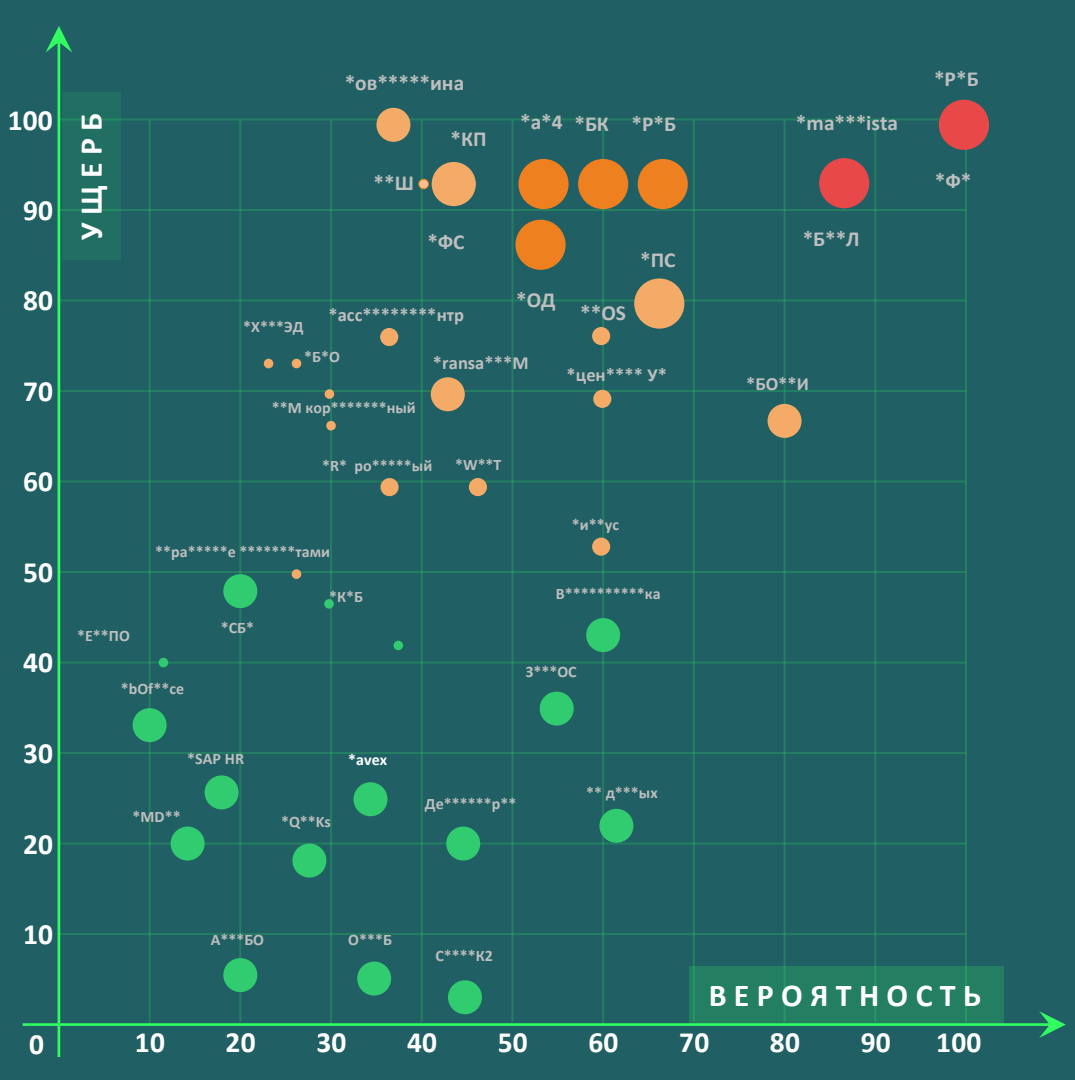


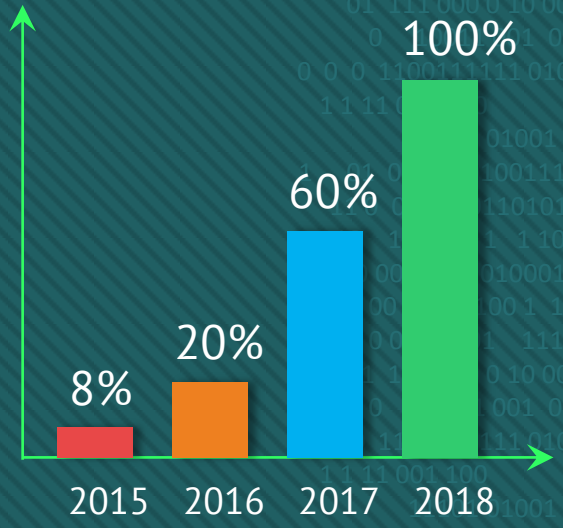
РАЗВИТИЕ КОМПЕТЕНЦИЙ

- Базовые интенсив-курсы
- Внутренние конференции
- Неформальные meet-up’ы
- Геймификация (соревнования в формате CTF)

Exploit
Threat
CWE
SAST
Data
Security
CTF
Education
SDLC
Testing
PCI
Authentication
CSRF
Awareness
Black-box
XSS
BSIMM
NVD
Vulnerability
OWASP
Misconfiguration
Architecture
Injection
DAST
XXE
Exposure
Hack
Deliverable
White-box
Risk
SAST

СТРАТЕГИЯ ТИРАЖИРОВАНИЯ ПРАКТИК ЗАЩИЩЕННЫХ ПРИЛОЖЕНИЙ





ЦЕННОСТЬ

ИССЛЕДОВАНИЕ

РЕАГИРОВАНИЕ

Анализ и исправление кода

Требования

Архитектура

Исходный код

Стенды

Интервью с командой

УСКОРЕНИЕ

ПРОАКТИВНЫЙ ПОДХОД

Тиражирование лучших практик

Выделение в проектной команде роли Security Champion

Передача практик в проектную команду

Наращивание экспертизы

Повторяемый процесс

Экспертная поддержка

Тренинги

Контроль результатов

Понимание реальной ситуации
Снижение рисков ИБ
Индивидуальные требования
Честный Compliance (PCI DSS)
Сервисный подход

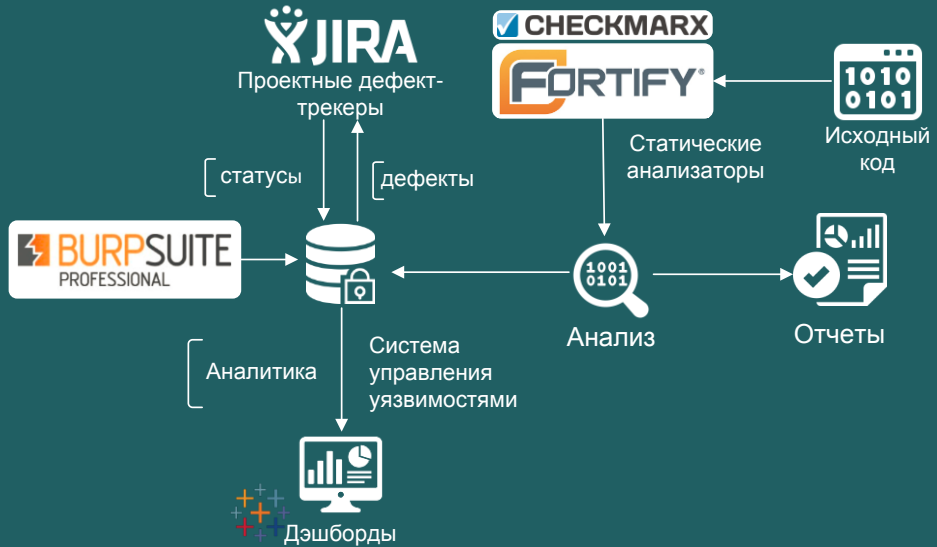
ВРЕМЯ

Безопасность ПОСТФАКТУМ

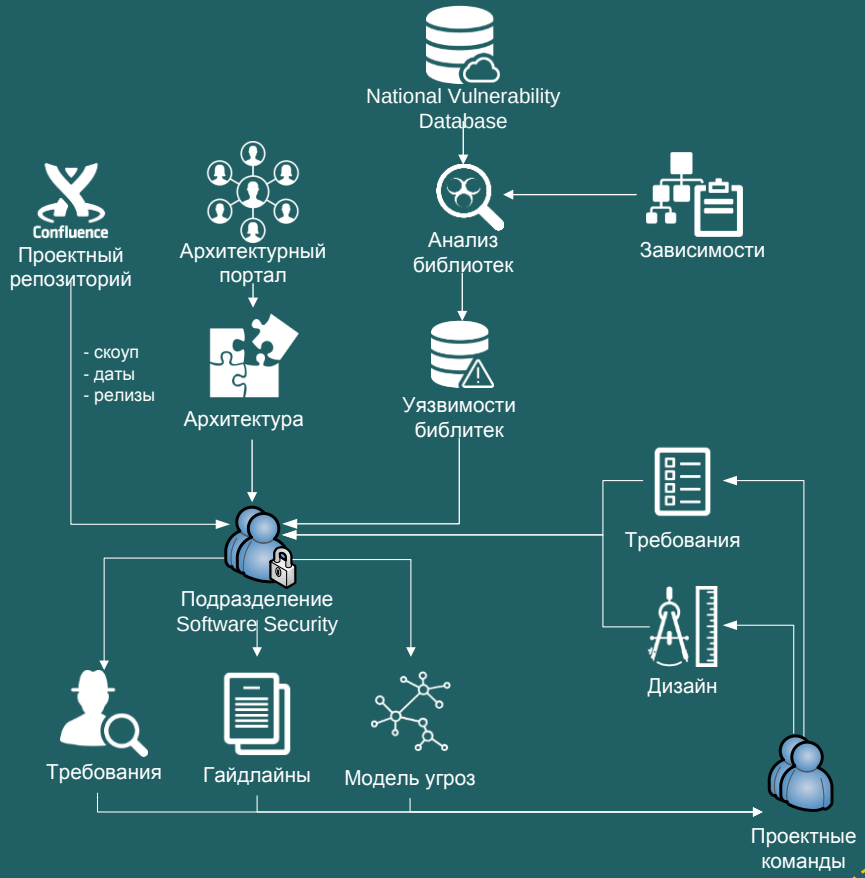
Безопасность В ПРОЦЕССЕ разработки

ЭВОЛЮЦИЯ ПРОЦЕССА

Схема интеграции инструментов



Процесс взаимодействия с проектными командами



ЦЕЛЕВАЯ МОДЕЛЬ

ЦЕЛЕВАЯ МОДЕЛЬ

ЦЕЛЕВАЯ МОДЕЛЬ

Разработана единая система метрик для отслеживания эффективности как подразделения ИБ, так и производственных команд.

ЦЕЛЕВАЯ МОДЕЛЬ

Экосистема управления процессами обеспечения ИБ разрабатываемых приложений и сервисов.

ЦЕЛЕВАЯ МОДЕЛЬ

- ✓ Для каждого типа проекта сформированы индивидуальные требования
- ✓ Контроль в рамках проектных гейтов

ЦЕЛЕВАЯ МОДЕЛЬ

ЦЕЛЕВАЯ МОДЕЛЬ

ВРЕМЯ ПРОКАЧАТЬСЯ !

Юрий Сергеев

Руководитель направления
Software Security @ СберТех

YASergeev.sbt@sberbank.ru

СПАСИБО ЗА ВНИМАНИЕ !