Трансформация процессов безопасной разработки в МТС RED с учетом рекомендаций ФСТЭК России

Денис Шефановский
руководитель Центра платформ кибербезопасности MTC RED

Сергей Деев
старший менеджер по продукту MTC RED

МТС RED — сервис-провайдер и разработчик решений для кибербезопасности

- Опыт работы с компаниями из разных сфер российской экономики, понимание отраслевой специфики
- Филиалы во всех крупных городах и часовых поясах РФ
- В ядре сервисов — разработки отечественных вендоров, не подлежащие санкционным рискам

Известные специалисты со всего рынка – одна из самых больших экспертиз

400+
Команда экспертов

10+
Лет опыта защиты лидирующего оператора связи

10+
Готовых продуктов и сервисов

20+
Продуктов и сервисов до конца 2025 года

2005
Запуск корпоративного МТС SOC

2017
Выход МТС SOC на коммерческий рынок

2022
Создание МТС RED – «дочки» МТС со специализацией в ИБ

2023
Запуск новых сервисов и продуктов МТС RED

2024
Расширение портфеля за счет собственных новых разработок

МТС RED

Как развивались практики безопасной разработки в ПАО МТС и МТС RED

До 2020

Каждая команда разработки в МТС определяет свои требования к безопасной разработке

2020

Департамент ИБ МТС централизованно управляет практиками безопасной разработки в продуктах

2022

Создается дочерняя компания МТС, с профилем ИБ – МТС RED. Развиваются собственные продукты ASOC и CCS

2023

Департамент управления технологиями МТС развивает безопасную разработку, основываясь на «лучших мировых практиках» и масштабирует их на все разрабатываемое ПО

2024

МТС RED ведет подготовку к приведению соответствия процессов РБПО к требованиям проекта ГОСТ 56939-XX Разработка безопасного ПО

РБПО?! РБПО!

Снижение вероятности возникновения уязвимостей в разрабатываемом ПО

Снижение ущерба от потенциальных уязвимостей ПО

Снижение количества и критичности потенциальных уязвимостей ПО

Оперативное устранение возникающих уязвимостей в ПО

RED

РБПО: Ключевые отличия

01

Обязательный внешний аудит (лаборатория и орган сертификации)

02

Доверенные инструменты анализа, сборки и другие

03

Функциональное и специализированное тестирование

04

Разное отношение к рискам, связанным с уязвимостями

05

Управление уязвимостями на всех этапах ЖЦ ПО

06

Определение поверхности атаки и работа с ней

07

Формирование документированных свидетельств

РБПО: кто реализует

1

Команда AppSec

Инструментарий, процессы, качество и поддержание сертификации. Поверхность атаки

2

Security Champions

Один энтузиаст ИБ на 10 - 30 разработчиков. Работа с уязвимостями

3

Архитекторы ИБ

Модель угроз. Реализация подхода Security by Design

4

Консультанты

Помощь в сертификации. Обучение. Построение процессов

MTC RED

Наш путь к РБПО: Ключевые изменения

«Лучшие практики»:

- Оценка зрелости (BSIMM\OWASP SAM)
- Модель угроз для ПО
- SAST
- DAST
- OSA\SCA
- Bug bounty
- Тестирование на проникновение
- Security Champions

РБПО: дополнительные меры

- Анализ безопасности архитектуры ПО (поверхность атаки)
- Безопасность систем и сред разработки
- Использование доверенных инструментов анализа
- Фаззинг
- Модульное и функциональное тестирование
- Выявление побочных взаимодействий со средой функционирования
- Обучение экспертов ключевым аспектам РБПО и владения инструментами анализа
- Анализ утечек чувствительных данных
- Разработка и актуализация документации

ASOC
(платформа управления процессом безопасной разработки)

SAST
статические анализаторы

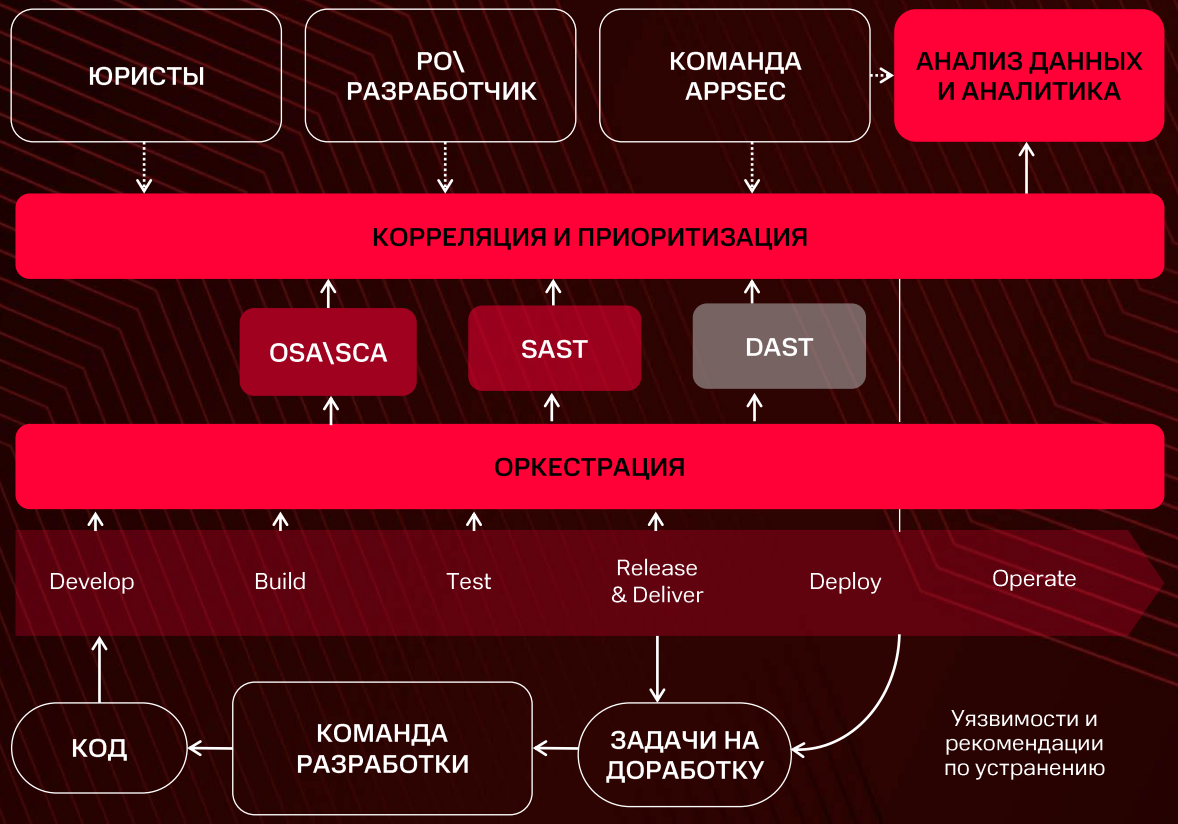
DAST
динамические анализаторы

SCA
анализ сторонних компонентов

OSA
анализ Open Source

RED

Безопасность на всех жизненных циклах разработки



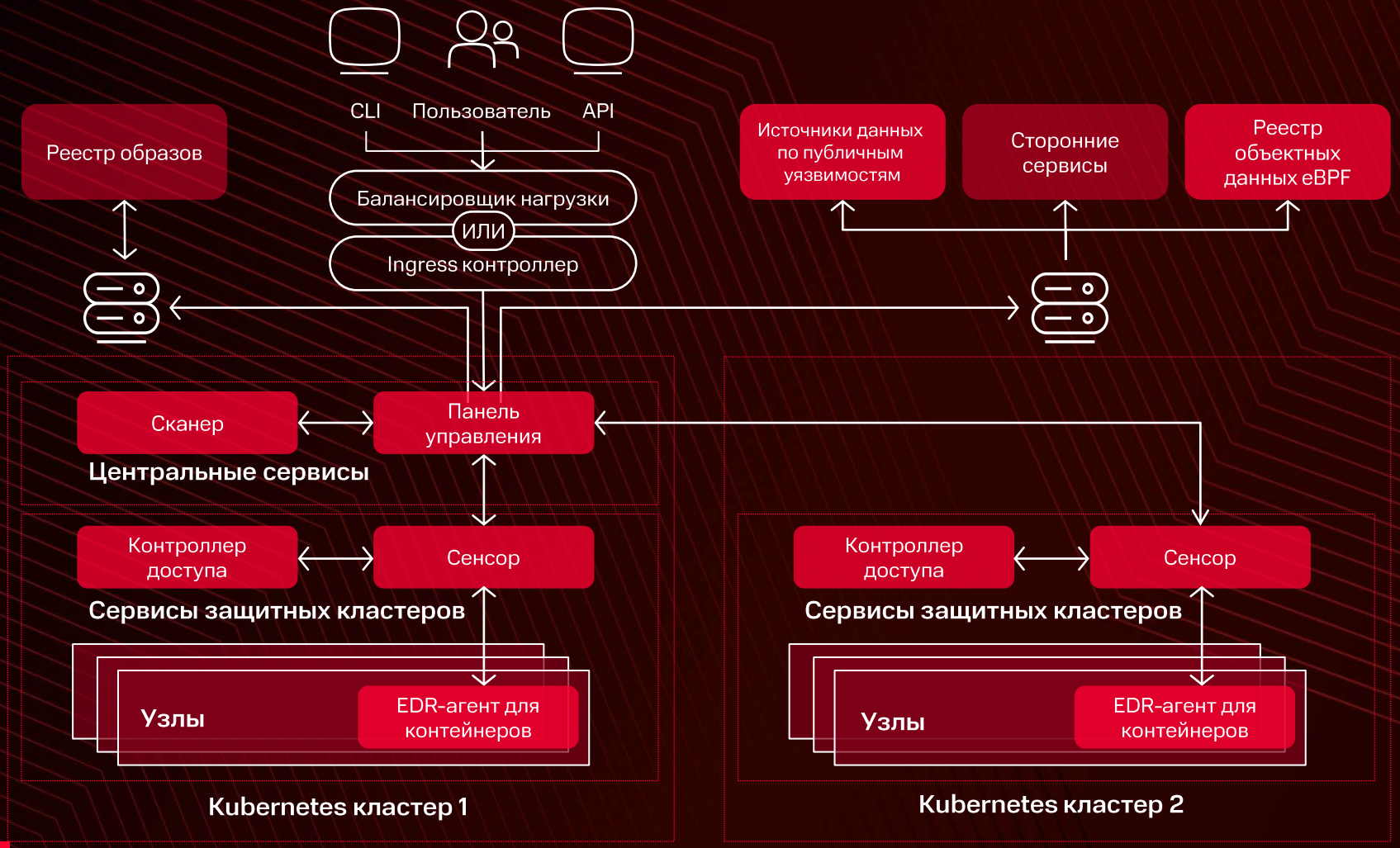
Аналитика
Основанная на метриках для оценки уровня безопасности ПО

Приоритизация
Отображение уязвимостей по уровню критичным

Корреляция
Объединение информации об уязвимостях из разных источников, позволяя повысить эффективность их обработки

Оркестрация
Гибкое и автоматизированное управление инструментами анализа защищенности ПО на разных этапах жизненного цикла разработки

Cloud and Container Security
(платформа обеспечения безопасности облачных и локальных сред контейнеризации)



5 компонент продукта:

- Панель управления
- Сканер
- Сенсор
- Контроллер доступа
- EDR-агент для контейнеров

Объект поставки – образы контейнеров, соответствующие спецификации стандарта Open Container Initiative (OCI)

РБПО: за кадром

Участие в ТК для подготовки и оценки готовящихся стандартов по безопасной разработке

Работа в консорциуме Технологического центра исследования безопасности ядра Linux

Работа по верификации дефектов в компонентах с открытым исходным кодом

РБПО: открытые вопросы

01 Стандарты РБПО в стадии разработки

02 Какие требования к изготовителю? Кто будет сертифицировать?

03 Какой набор доверенных инструментов?

04 Насколько сложно сертифицировать процесс РБПО?

05 Чему соответствуют уровни реализации мер РБПО?

06 РБПО для ИТ = Роскачество?

07 Преимущества для ИТ отрасли (не ИБ)?


M
T
Вопросы?
RED
C

M T

Интересно узнать про наши технические решения?

[cybersecurity@mts.ru]

RED C