ГАЗПРОМБАНК

Новые аспекты в задачах по безопасной разработке

Сергей Горленко

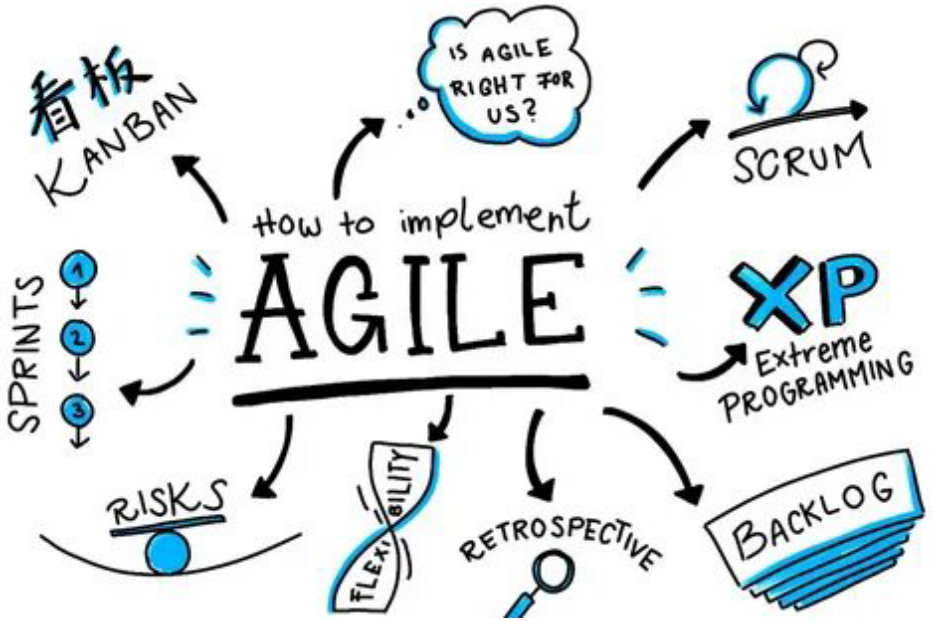
Предпосылки создания SecDevOps

Изменение подхода к предоставлению цифровых продуктов

- Снижение времени Time-to-Market для новых продуктов
- Переход к разработке АС силами работников Банка
- Применение методологии Agile при создании и модернизации цифровых продуктов

Изменение подходов к автоматизации цифровых продуктов в Банке

- Внедрение современных инженерных практик разработки ПО – DevOps
- Внедрение и применение инструментов автоматизации проектного управления
- Увеличение доли автоматизированных тестов для новых версий АС



Развитие практик AppSec

	Было	Стало	Планируется
Анализ исходного кода (SAST)	Проверка предоставленных внешним разработчиков кодов с использованием инструментов банка, ручной запуск	Сборка и проверка кода проводится автоматизировано в рамках DevOps pipeline	Разработка и реализация процессов по выявлению закладок
Контроль внешних Библиотек при скачивании (OSA)	Фрагментарные оповещения при появлении публичных новостей о критичных уязвимостях	Реализован контроль внешних библиотек при разработке, все скачиваемые библиотеки хранятся во внутреннем репозитории	Осуществляется выбор инструментов для обеспечения практики
Компонентный анализ приложений (SCA)	Процесс отсутствовал	Реализован процесс компонентного анализа при сборке приложений	Осуществляется выбор инструментов для обеспечения практики

Развитие практик AppSec

	Было	Стало	Развитие
Динамический анализ Web и мобильных приложений (DAST)	Выполнялся по запросу, не интегрирован с производственным процессом	Интегрирован в производственные процессы при deploy приложений	Производится выбор инструментария для реализации практики IAST
Security Quality Gates (SQG)	Процесс отсутствовал	Разработаны количественные метрики, позволяющие определить допустимое количество уязвимостей для АС. Контроли метрик Security QualityGates(SQG)) выполняются автоматизировано в DevOps pipeline	Разработать критерии, которые в зависимости от критичности АС будут динамически определять SQS.
Автоматизация проведения ПСИ инструментами (BAST)	Процесс отсутствовал	Требования разделены на группы для автоматизации	Автоматизация проверки требований.

Этапы по внедрению инструментария AppSec

Q1,2018

Начало работ, оценка рынка инструментов и подготовка планов внедрения

Q1,2019

Развернуты инструменты по Контролю внешних Библиотек при скачивании. Настроены политики блокировки

Q3,2019

Развернуты инструменты Компонентного анализа приложений, Статического анализа кода, автоматизированы внутри pipelines DevOps практики SAST,SCA. Применяется SQG

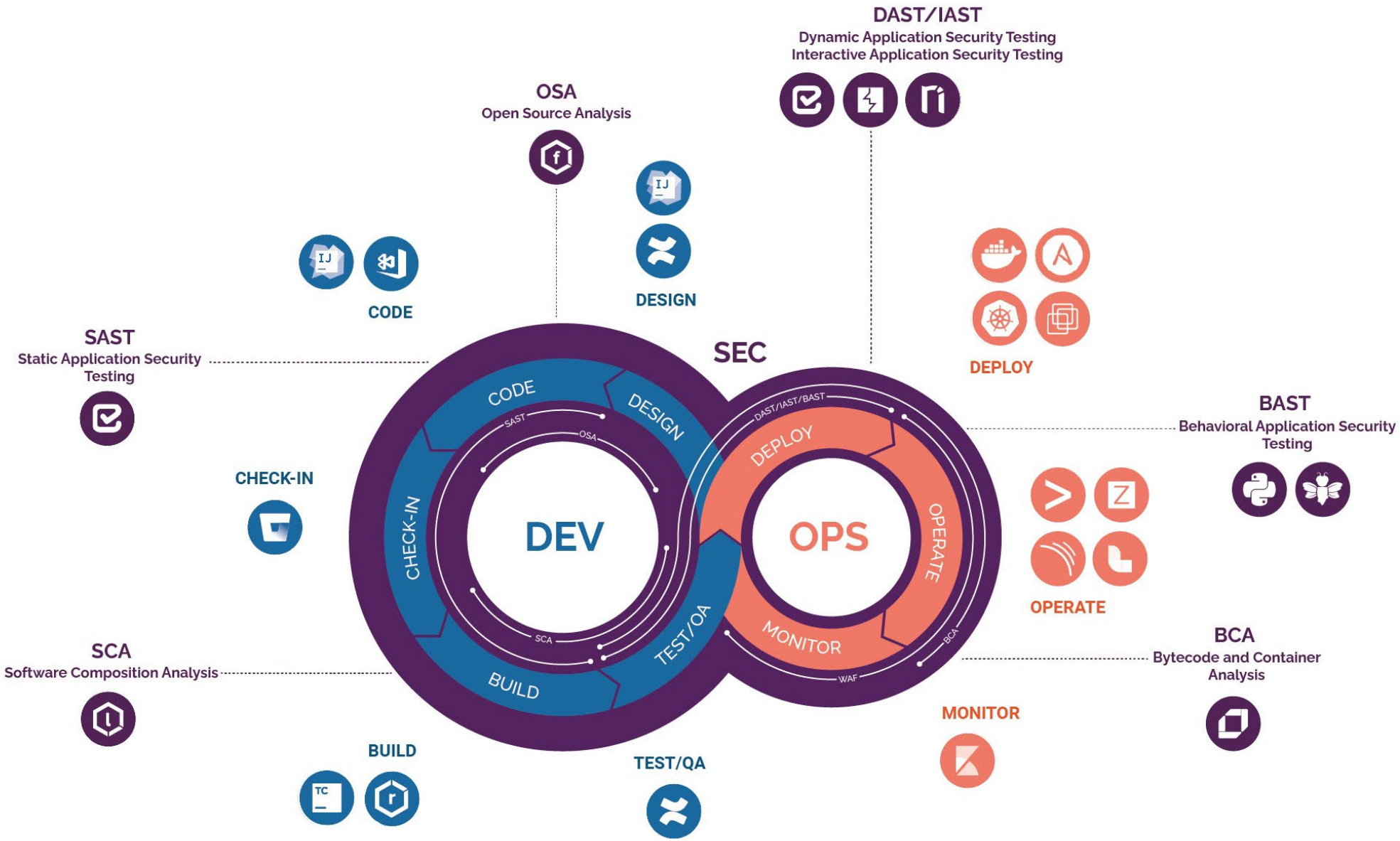
Q1,2020

Формализация практик в процессе разработки ПО. Тиражирование практик на АС Банка и команды разработки.

Q2,2020

Развернут инструмент для Динамического анализа приложений

Взаимодействие практик AppSec с процессами DevOps



Новые задачи после 24.02.22

1. Риски активации программных закладок
2. Целенаправленные действия по внесению закладок для РФ
3. Риски по блокированию репозиториев
4. Санкционные риски
5. Риски использования пикселей и метрик сайтов/мобильных приложений

vuejs / vue-cli Public

Code | Issues 805 | Pull requests 115 | Discussions

!!!!!!!!!! Please do something to warn USERS besides publishing new versions

Mister-Hope commented on 15 Mar • edited

See https://github.com/RIAEvangelist/node-ipc/issues/233#issuecomment-1068182278 the `node-ipc` is doing things far more than ever expected.

If any users are using ip in russia, all their file will be wiped entirely by ❤️, and that's a VERY DANGEROUS BEHAVIOR. This is not just making a joke, but damaging russia people's PC or server

Пути решения новых задач

- Стандартизация стека разработки в части использования внешних библиотек
- Разработка и реализация процессов по выявлению закладок

- Разработка и реализация процессов по выявлению закладок

- Создание внутреннего кэша внешних репозиториев

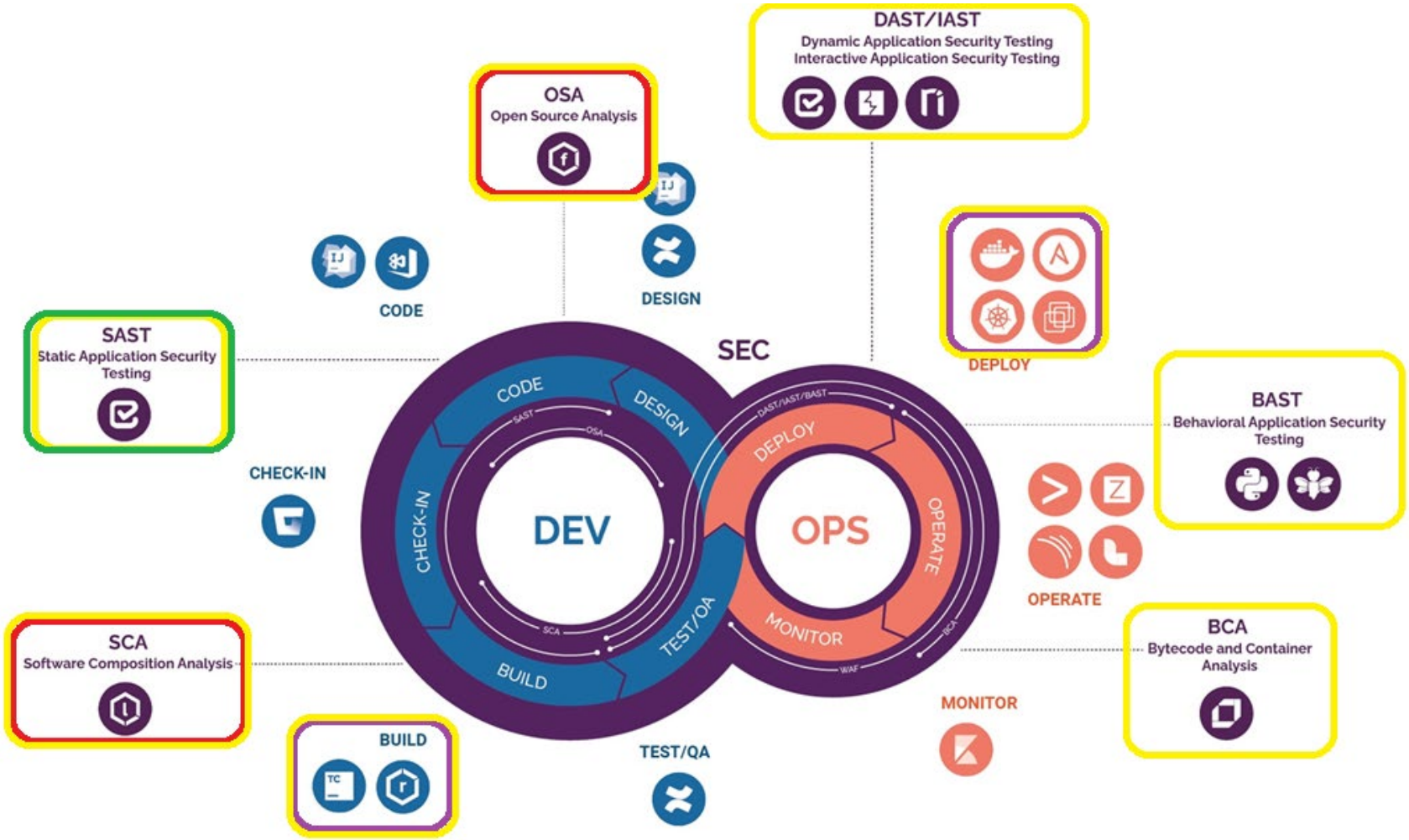
- Замена инструментов AppSec на opensource и российские аналоги

- Переход на российские аналоги метрик Реализация подхода по использованию контролируемого хранилища пикселей
- Контроль применения метрик и пикселей

*пиксель — JavaScript-код, который собирает информацию о пользователях и отслеживает их действия на сайте. Какие страницы посещал пользователь, на какие кнопки нажимал, какие формы заполнял, какие товары сложил в корзину, а какие купил

**метрика — инструмент веб-аналитики, который помогает получать наглядные отчеты, видеозаписи действий посетителей, отслеживать источники трафика и оценивать эффективность онлайн- и офлайн-рекламы

Влияние санкционного риска на архитектуру



OpenSource

Риск реализовался переход на OpenSource

devOps инструменты влияющие на AppSec, запланирован переход на Opensource

Риск не реализовался возможен переход на OpenSource или российское ПО

Спасибо за внимание

Горленко Сергей Александрович
Вице-Президент - начальник Департамента развития технологий защиты информации
email: Sergey.Gorlenko@gazprombank.ru