Сообщество FinDevSecOps: как мы помогаем финансовым организациям выстраивать процесс безопасной разработки

Карапет Манасян
идеолог и сооснователь FDSO, CPO MOEX
Татьяна Билык
лидер FDSO, директор технологических проектов АФТ

Карапет Манасян

- Глава платформы производства, MOEX Group
- Создаю внешние/внутренние сообщества, лидер FinDevSecOps
- Спикер ИТ-конференций, DevOpsConf, AgileDays и др.
- Участник Russia State of DevOps 23-24 (T1)
- Вечный студент, ВШЭ IT, РАНХиГС MBA ИБДА

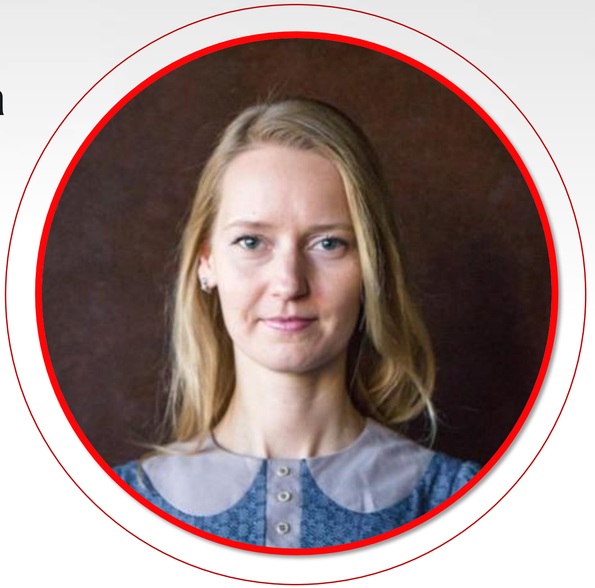
Татьяна Билык

Директор технологических проектов, Ассоциация ФинТех

Помогаю находить ценность во взаимодействии участников фин. рынка

Спикер финтех-конференций (Davos-2019, др.)

ВШЭ (InfoSec), MBA (Стратегический менеджмент; IT)



Сообщество FinDevSecOps

ССЫЛКА НА МАНИФЕСТ

Миссия Достижение синергетического эффекта от объединения усилий сторон, заинтересованных в развитии безопасной разработки программного обеспечения и opensource-решений для финансовой и смежных секторов.

2023 Дата основания

20+ Организаций, присоединившихся к Манифесту Сообщества

50+ Участников Сообщества

Банк России, Альфа Банк, Газпромбанк, base alt, Т Банк, ВСК страховой дом, Совкомбанк, MOEX GROUP, НСПК, РоссельхозБанк, ДОМ РФ, Капитал Life страхование жизни, Русский Стандарт банк, Альфа Страхование, ART искусство прибыли, росбанк, синара банк

FIN DEV SEC OPS

Вопросы, с которыми мы можем помочь

Где найти best practices для российского финансового рынка?

FIN DEV SEC OPS

Вопросы, с которыми мы можем помочь

Как быстро найти нужных вам людей?

FIN DEV SEC OPS

Вопросы, с которыми мы можем помочь

Как выбрать инструментарий, чтобы быстро и не ошибиться?

FIN DEV SEC OPS

Вопросы, с которыми мы можем помочь

Как повлиять на роадмэп развития вендорского ПО, если вам чего-то не хватает?

FIN DEV SEC OPS

Вопросы, с которыми мы можем помочь

Как повлиять на разрабатываемое нормативное регулирование?

FIN DEV SEC OPS

ТИПОВОЙ ПРОЦЕСС DEVSECOPS

1. Одинаковая интерпретация регуляторных документов
2. Применение лучших практик
3. Переиспользование практик и инструментов
4. Проекция документов/методологий на инструменты
5. Создание фреймворка для инженеров и разработчиков

FIN DEV SEC OPS

ДЛЯ КОГО?

1. Команды разработки цифровых продуктов
2. Инфраструктурные и платформенные команды
3. AppSec команды

FIN DEV SEC OPS

СЛОИ ТИПОВОГО ПРОЦЕССА

Входные артефакты

Бизнес-требования

Нормативные документы

Внутренние требования

Перечень рисков и меры их снижения

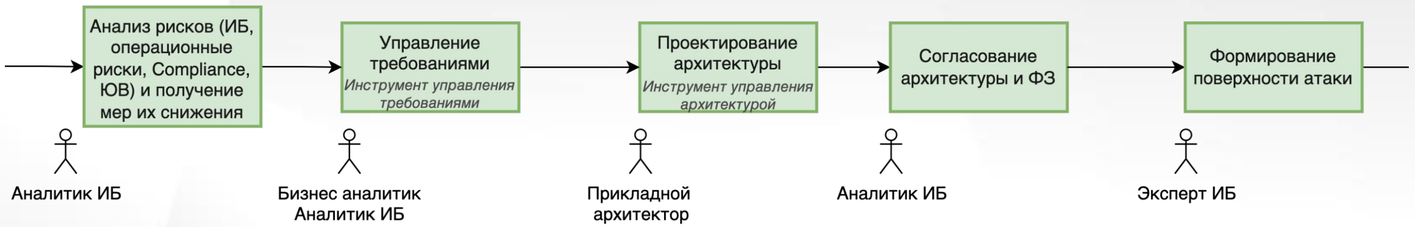
Требования к ИС

Требования к ИС

Архитектура

Процесс безопасной разработки

Security gates (SGs)



Выходные артефакты

Перечень рисков и меры их снижения

Требование к ИС (функциональные, нефункциональные, ИБ)

Архитектура

Согласованная архитектура

Согласованные требования к ИС

Список критических для ИБ объектов (в т.ч. список точек входов в систему)

Список защищаемой информации

Регуляторные документы

ГОСТ Р 56939-202X

5.1 Планирование процессов разработки
5.2 Обучение сотрудников

ГОСТ Р 56939-202X

5.3 Формирование и предъявление требований безопасности к программному обеспечению

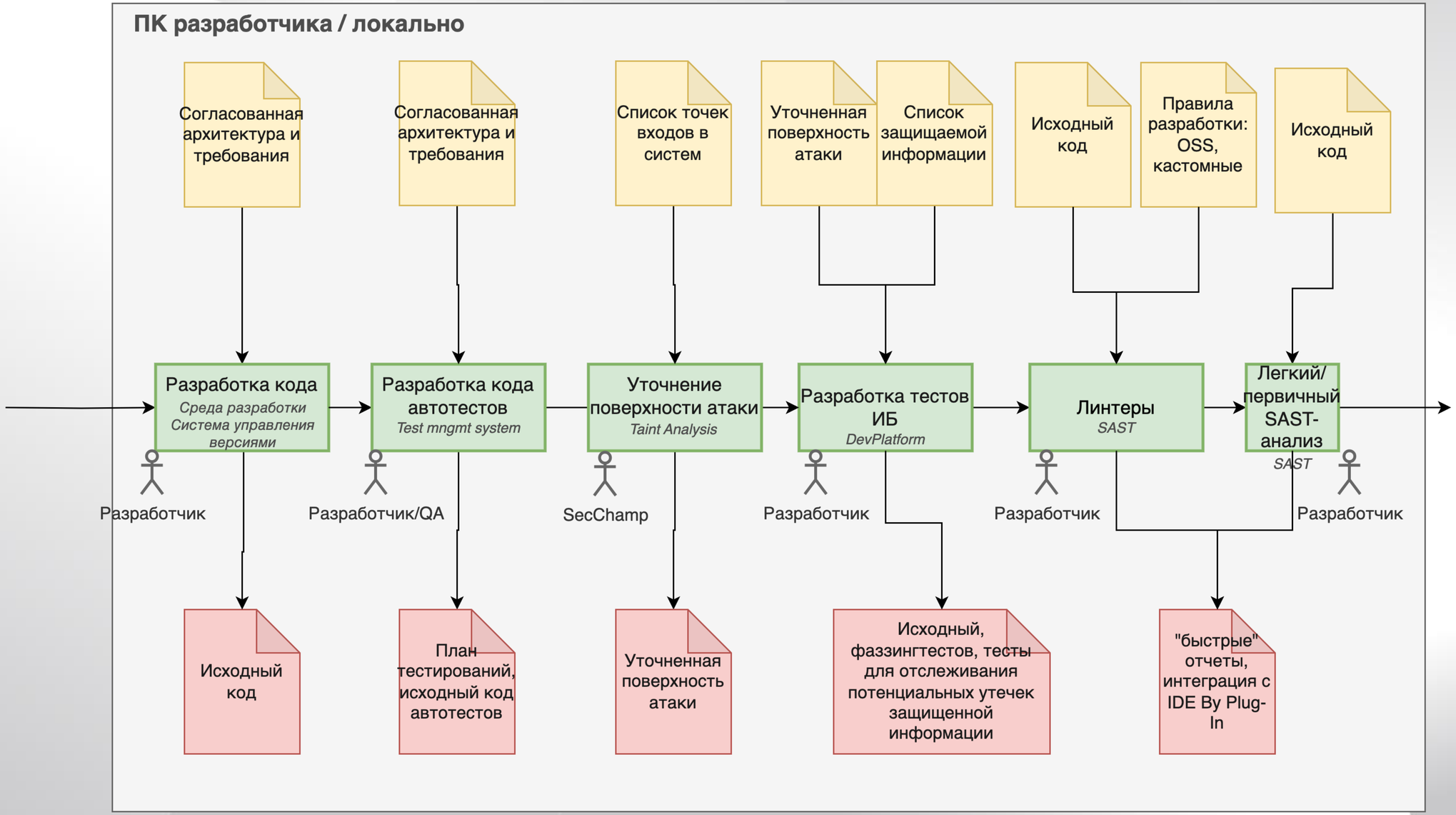
ГОСТ Р 56939-202X

5.4 Управление конфигурацией программного обеспечения
5.6 Разработка, уточнение и анализ архитектуры программного обеспечения

Инструменты

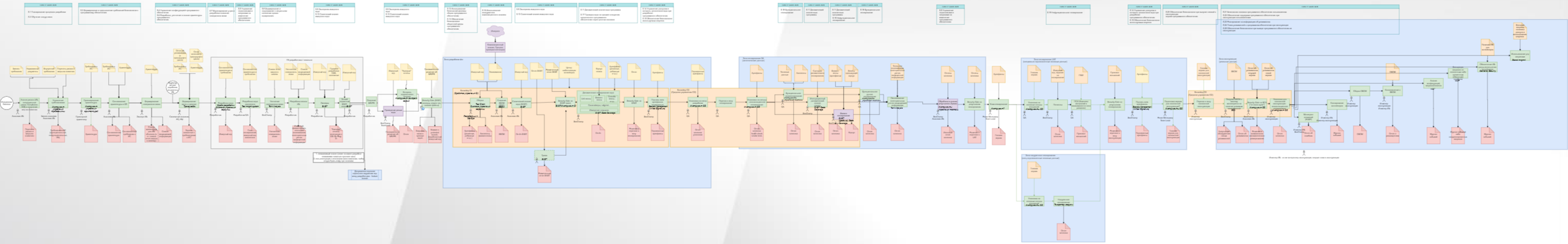
FIN DEV SEC OPS

ЧАСТЬ ПРОЦЕССА (пример)



FIN DEV SEC OPS

СТРАШНО… МЫ НЕ ЗНАЕМ ЧТО ЭТО ТАКОЕ



Инициатива

Локальное окружение инженера/разработчика

Dev окружения

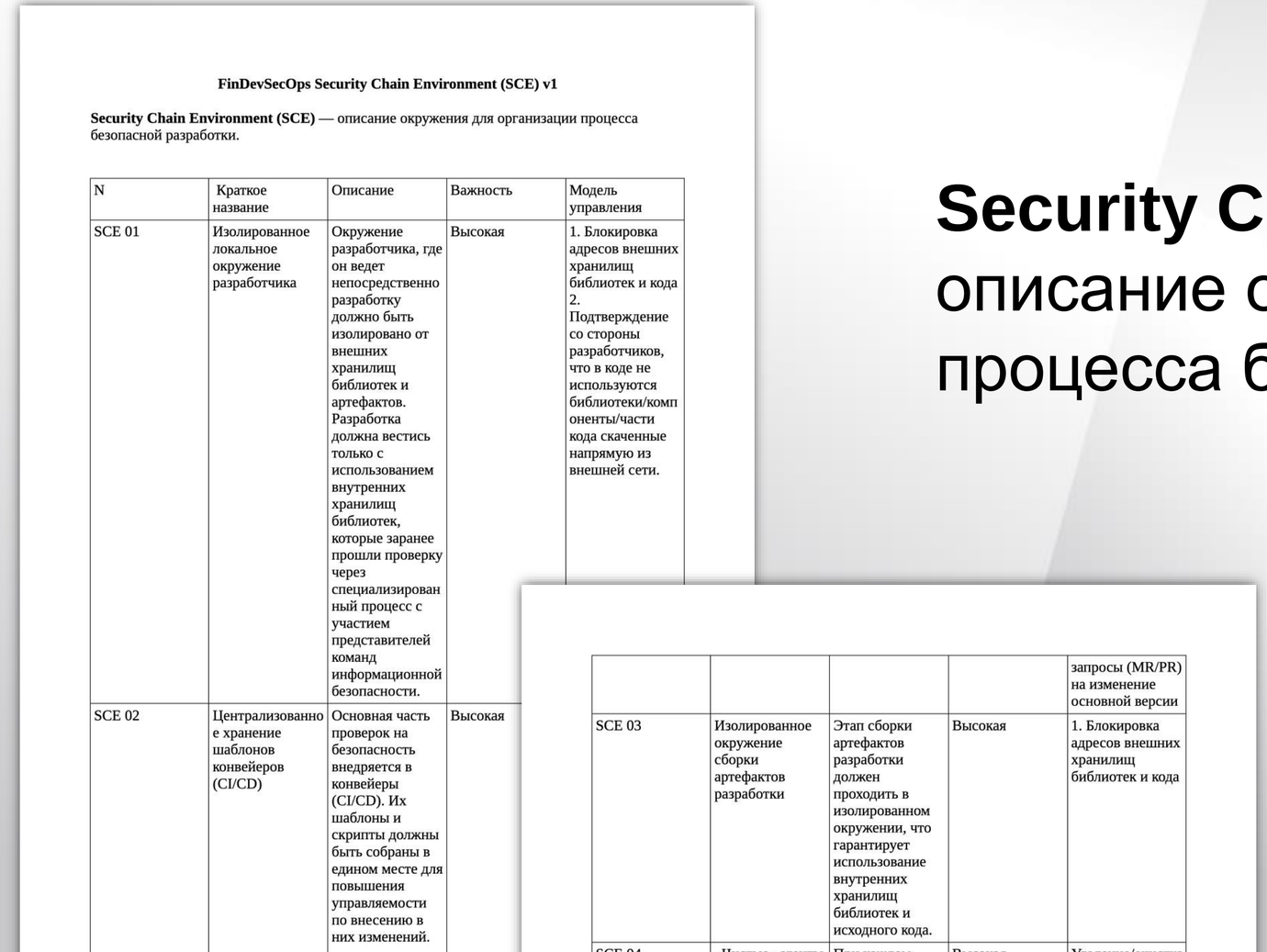
TEST/QA окружения

INT/LOAD/ PreProd окружения

PROD окружение

FIN DEV SEC OPS

Security chain env (SCE)



FinDevSecOps Security Chain Environment (SCE) v1

Security Chain Environment (SCE) — описание окружения для организации процесса безопасной разработки.

N	Краткое название	Описание	Важность	Модель управления
SCE 01	Изолированное локальное окружение разработчика	Окружение разработчика, где он ведет непосредственно разработку должно быть изолировано от внешних хранилищ библиотек и артефактов. Разработка должна вестись только с использованием внутренних хранилищ библиотек, которые заранее прошли проверку через специализированный процесс с участием представителей команд информационной безопасности.	Высокая	1. Блокировка адресов внешних хранилищ библиотек и кода 2. Подтверждение со стороны разработчиков, что в коде не используются библиотеки/компоненты/части кода скаченные напрямую из внешней сети.
SCE 02	Централизованное хранение шаблонов конвейеров (CI/CD)	Основная часть проверок на безопасность внедряется в конвейеры (CI/CD). Их шаблоны и скрипты должны быть собраны в едином месте для повышения управляемости по внесению в них изменений.	Высокая	
				запросы (MR/PR) на изменение основной версии
SCE 03	Изолированное окружение сборки артефактов разработки	Этап сборки артефактов разработки должен проходить в изолированном окружении, что гарантирует использование внутренних хранилищ библиотек и исходного кода.	Высокая	1. Блокировка адресов внешних хранилищ библиотек и кода

Security Chain Environment (SCE) — описание окружения для организации процесса безопасной разработки.

Инструменты DevSecOps

№	Направление	Разделение	Тип	Класс	Вендорское ПО	Open Source
1	**Инструменты DevSecOps**	**AppSec**	**SAST**	**Статический анализатор**	SVACE Solar AppScreener (SAST) PVS Studio Application Inspector GitLab SAST CheckMarx Coverity Klockwork Fortify Sonar Qube	Bandit Terrascan CodeQL Chechov Weggli Joern MATE Semgrep tfsec kics bearer njsscan clj-holmes Dagda Blackduck Osquery PMD Retire.js
2			**Taint Analysis**	**Анализ поверхности атаки**	PVSStudio ИСП РАН Natch Qodana	pyre-check psalm Triton find-sec-bugs pyt airbus-seclab (bincat) polytracker FlowDroid Ponce
3			**IAST**	**Интерактивный анализатор**	AppInspector Synopsys Seeker Veracode Interactive Analysis Microfocus Fortify WebInspect Checkmarx CxIAST Contrast Assess Hdiv Detection (IAST) CAST Codename SCNR (Arachni)	DongTai Contrast
4			**SCA**	**Анализатор**	Solar AppScreener (SCA) Code Scoring Сканер уязвимостей Ya Cloud AppSecTrack Spectral Snyk Azul qwiet Black Duck	Dependancy Track Dependency Check Grype Speed OpenSCAP Trivy

Сообщество создало перечень инструментов безопасной разработки: **OSS и вендорские**

FIN DEV SEC OPS

КЕЙСЫ FDSO

Реализация процесса проверки внешних инфраструктурных артефактов и библиотек разработки

Ускорение пилотирования инструментов безопасной разработки

Переиспользование готовых решений по безопасной разработке

FIN DEV SEC OPS

Активности FinDevSecOps на 2024

Осень 2024

Проведение воркшопов по продуктам:

- SwordFish Security
- ИСП РАН
- Positive Technologies
- Solar

18-21 ноября 2024

DevSecOps-хакатон

4 кв. 2024

Открытые обсуждения типового DevSecOps-процесса для фин. отрасли и карты DevSecOps-инструментов

БЛИЖАЙШИЕ ЗАДАЧИ

1. Создать базу знаний сообщества
2. Создать методологию безопасной разработки в финтехе на базе типового процесса
3. Запустить курсы по безопасной разработке
4. Бенчмаркинг по инструментам и практикам

FIN DEV SEC OPS

DEVSECOPS НАЧИНАЕТСЯ ЗДЕСЬ

FinDevSecOps@fintechru.org