NO FF ONE 2022

DevSecOps по-крупному: мифы и легенды на опыте одного банка

Карина Петрова, Никита Тажбенов

DevSecOps-аналитик, DevSecOps-инженер, Сбер

Москва, 26 августа, 2022

Кто мы

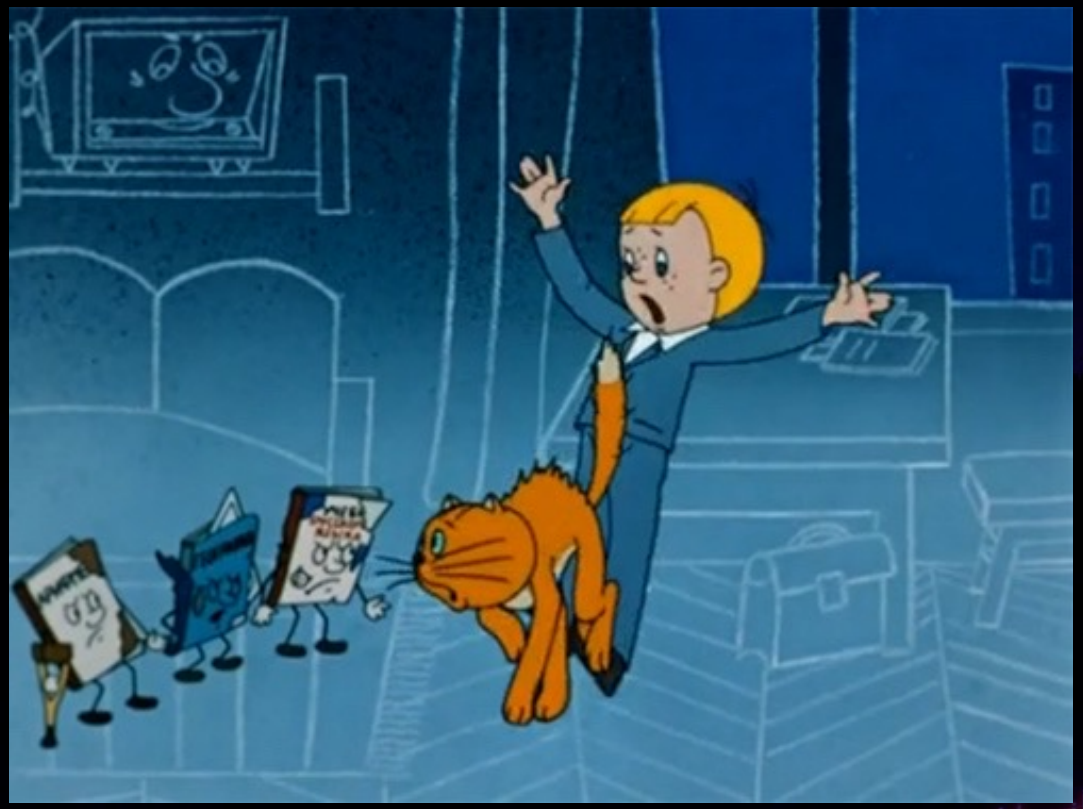
Карина Петрова, DevSecOps-аналитик, Сбер

Окончила АГТУ по направлению «Телекоммуникации», но с 2021 года вошла в мир Application Security, работая аналитиком в команде DevSecOps Сбера.
На текущий момент погружается детальнее в практику OSS.

Никита Тажбенов, DevSecOps-инженер, Сбер

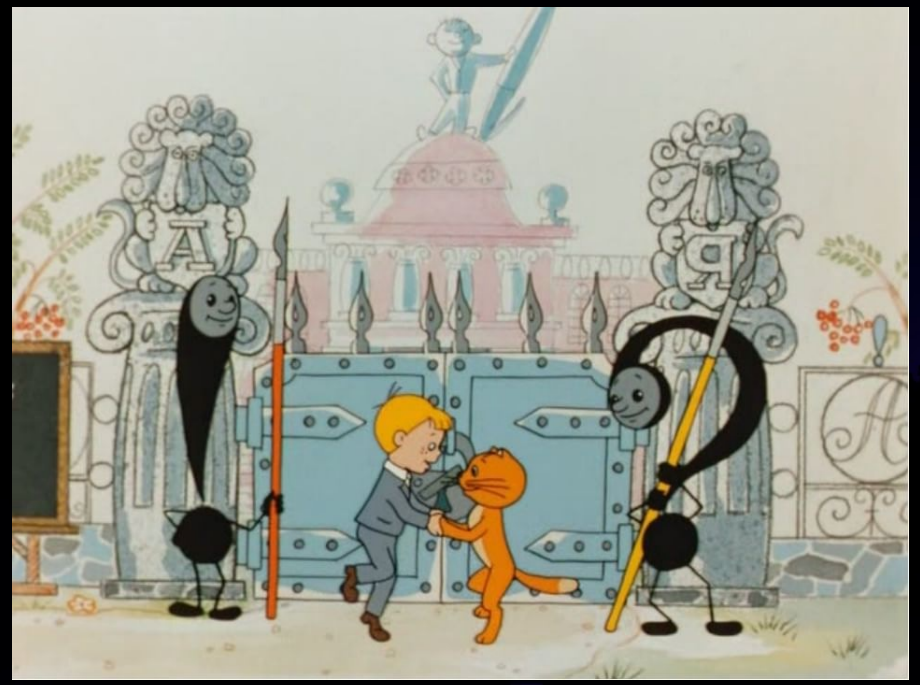
С 2017 года занимается блокчейн-разработкой, в частности безопасностью операций. Является призером и победителем таких хакатонов, как Waves Blockchain Hackathon 2018, DSXT Blockchain Hackathon 2019, TUI Hackathon. В данный момент работает DevSecOps-инженером в Сбербанке.

В стране невыученных уроков DevSecOps



Программист Виктор заключает договор с уязвимостями вне порога QG

Мы в Alpha живем



Разработчики систем, которые сидят в ДМЗ и молятся на WAF

Неспящие хакеры и взломщики внутри сетки

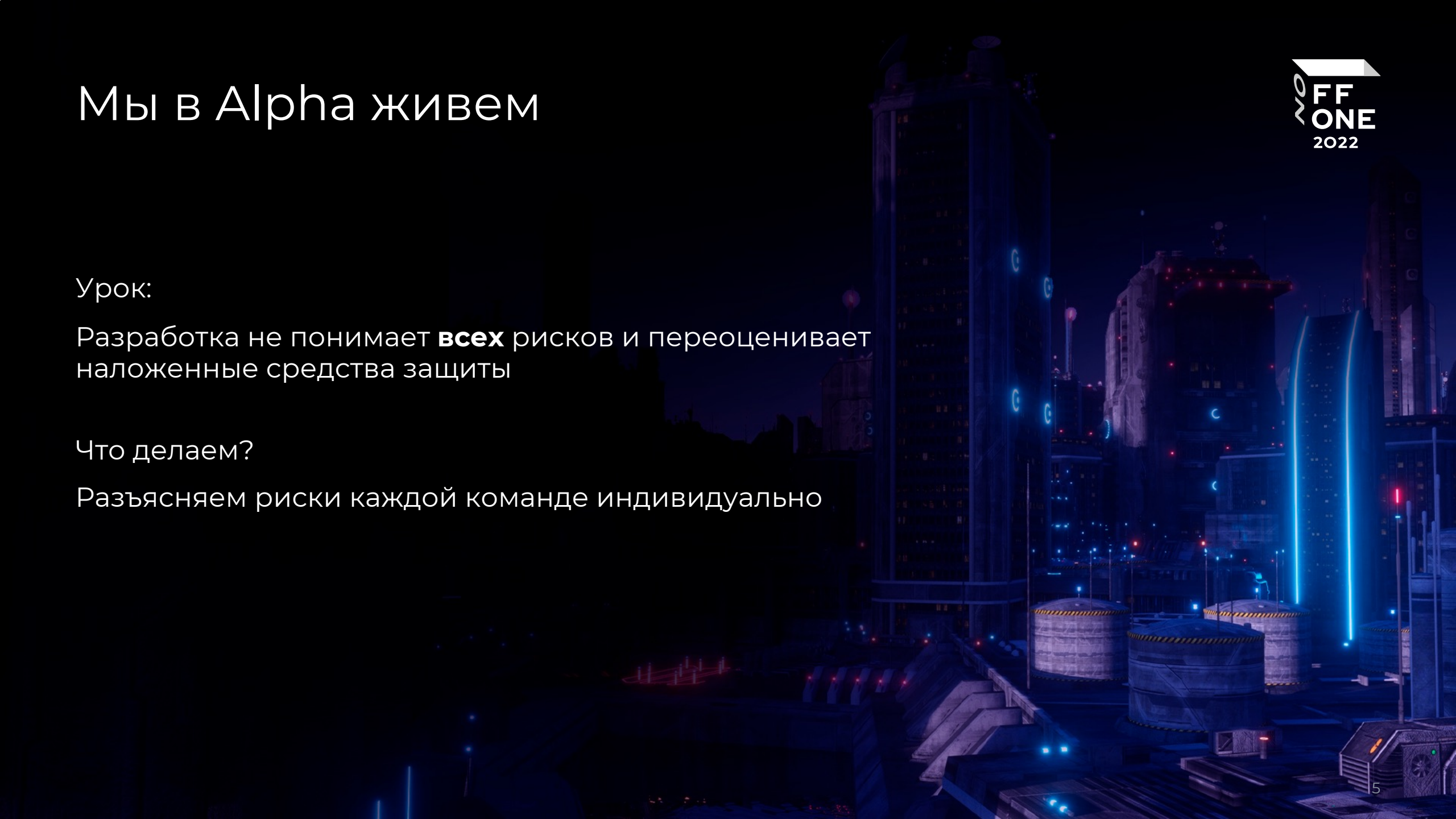
Мы в Alpha живем

Урок:

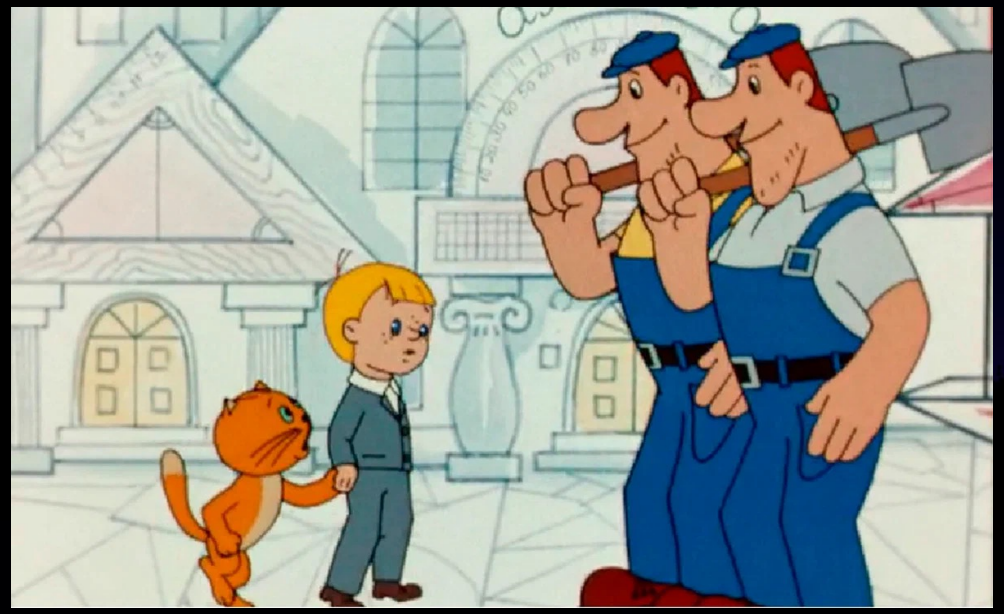
Разработка не понимает **всех** рисков и переоценивает наложенные средства защиты

Что делаем?

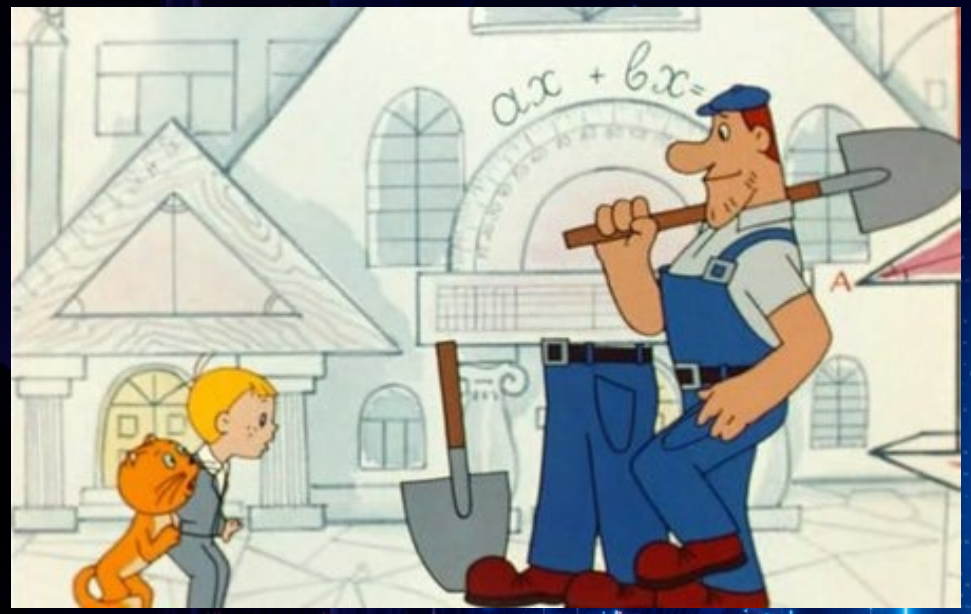
Разъясняем риски каждой команде индивидуально



Два сапога - пара

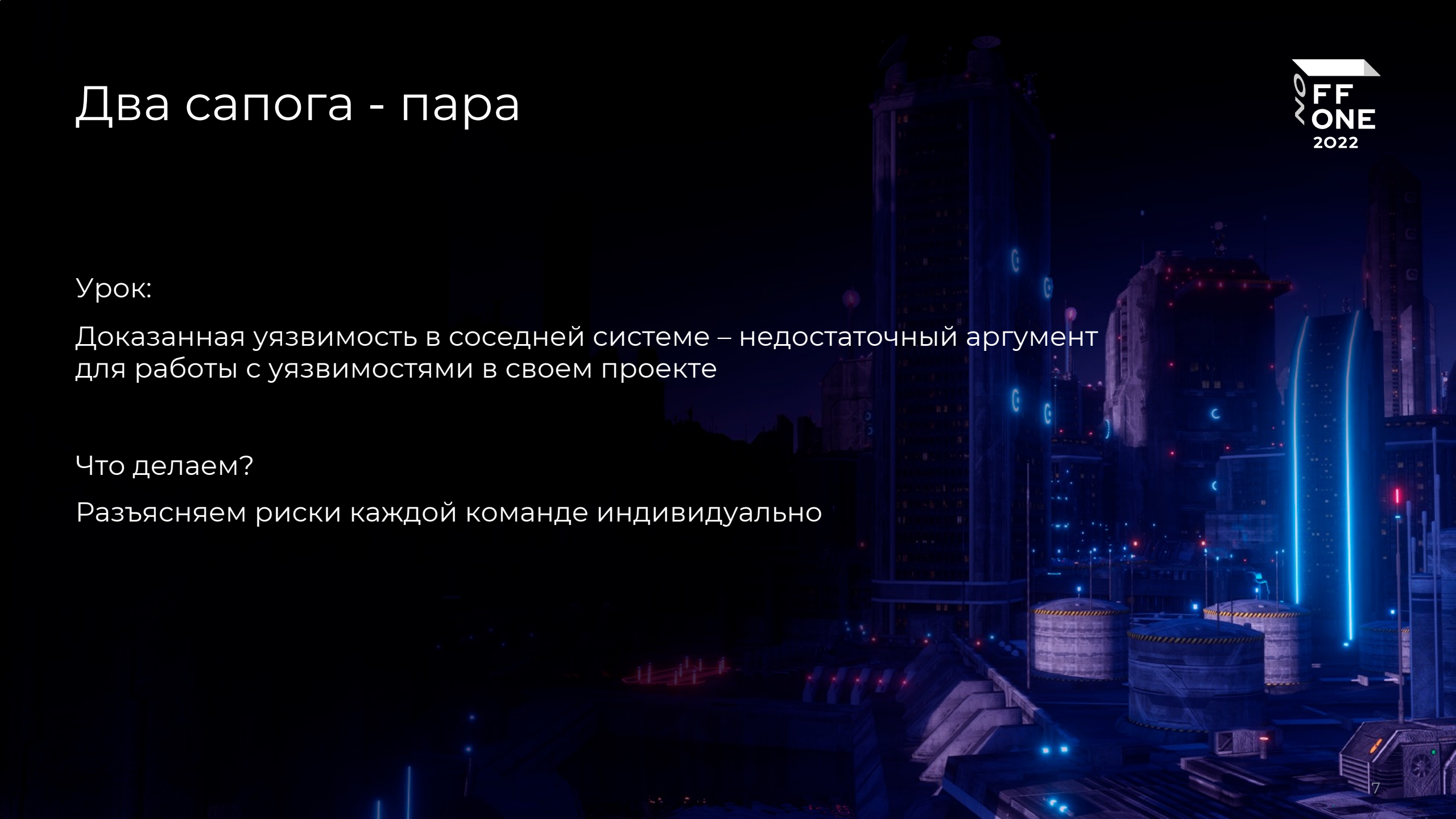


Виктор и его коллега Тимофей Котов обсуждают смежные модули их систем



Система Котова после аудита. Будет ли Виктор триажить сработки в связи с этим?

Два сапога - пара



Урок:

Доказанная уязвимость в соседней системе – недостаточный аргумент для работы с уязвимостями в своем проекте

Что делаем?

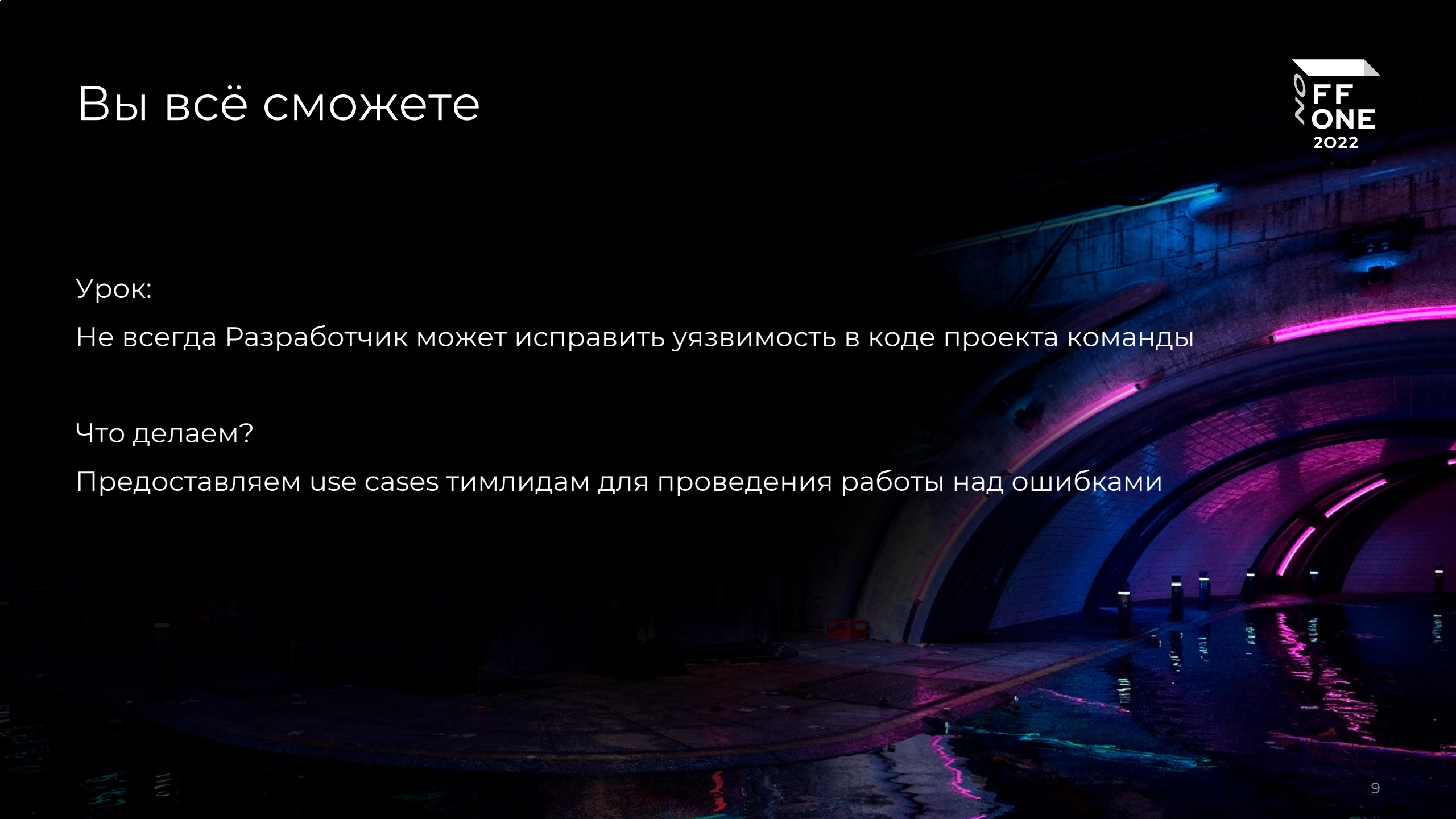
Разъясняем риски каждой команде индивидуально

Вы всё сможете

Разработчик может исправить любую уязвимость в коде проекта команды

- Что ты такое?
- Я скуля в вашем коде!
- Неправда! Я вчера коммитил добавление PreparedStatement! Правда анализатор ругается все равно...Не понимаю...
- Это круто, но Виктор Перестукин решил не валидировать типы...
- Ой...

Вы всё сможете



Урок:

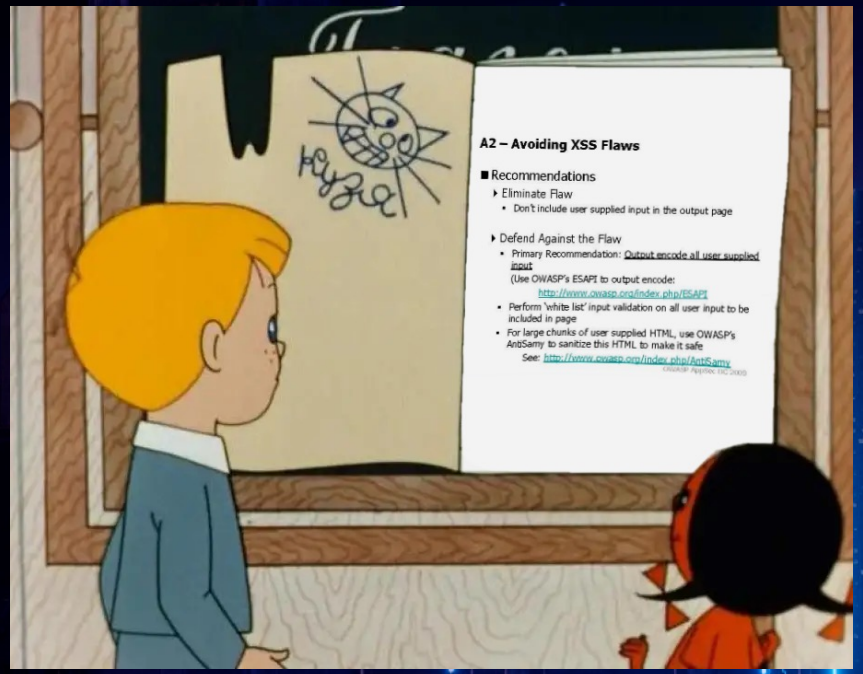
Не всегда Разработчик может исправить уязвимость в коде проекта команды

Что делаем?

Предоставляем use cases тимлидам для проведения работы над ошибками

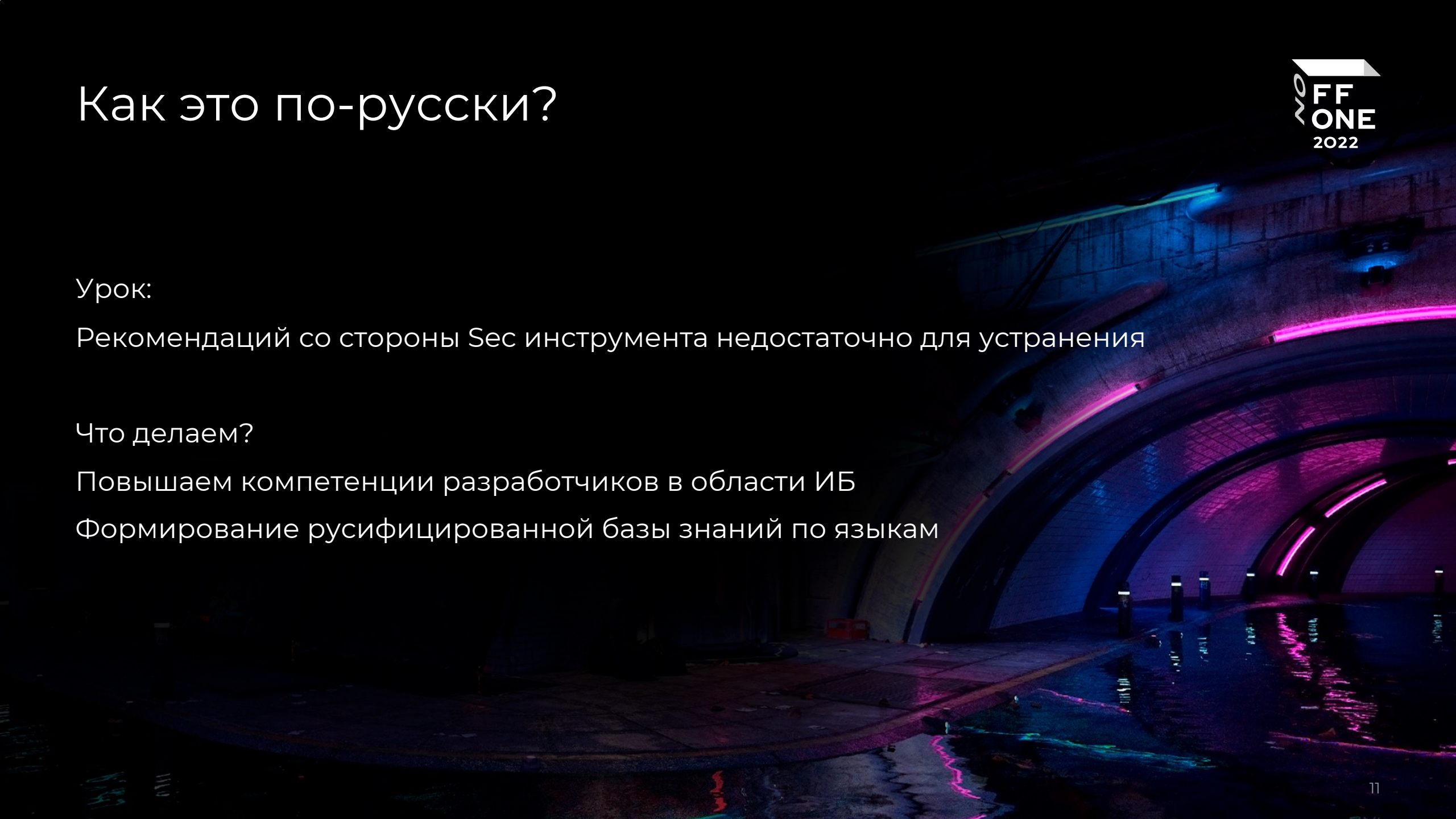
Как это по-русски?

Виктор увидел количество critical сработок в коде и...



пытается понять стандартную рекомендацию на заморском языке

Как это по-русски?



Урок:

Рекомендаций со стороны Sec инструмента недостаточно для устранения

Что делаем?

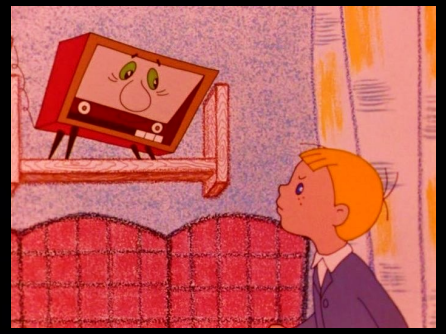
Повышаем компетенции разработчиков в области ИБ

Формирование русифицированной базы знаний по языкам

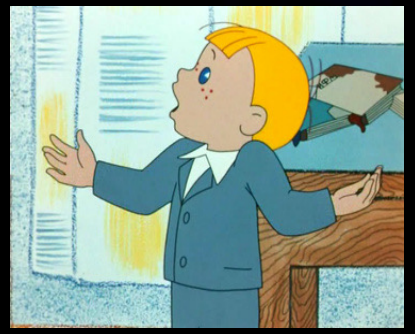
Ты не пройдешь!

Поставьте запятую

Ты не пройдешь!



Гнев



Отрицание

Торг

Депрессия

Принятие

Ты не пройдешь!

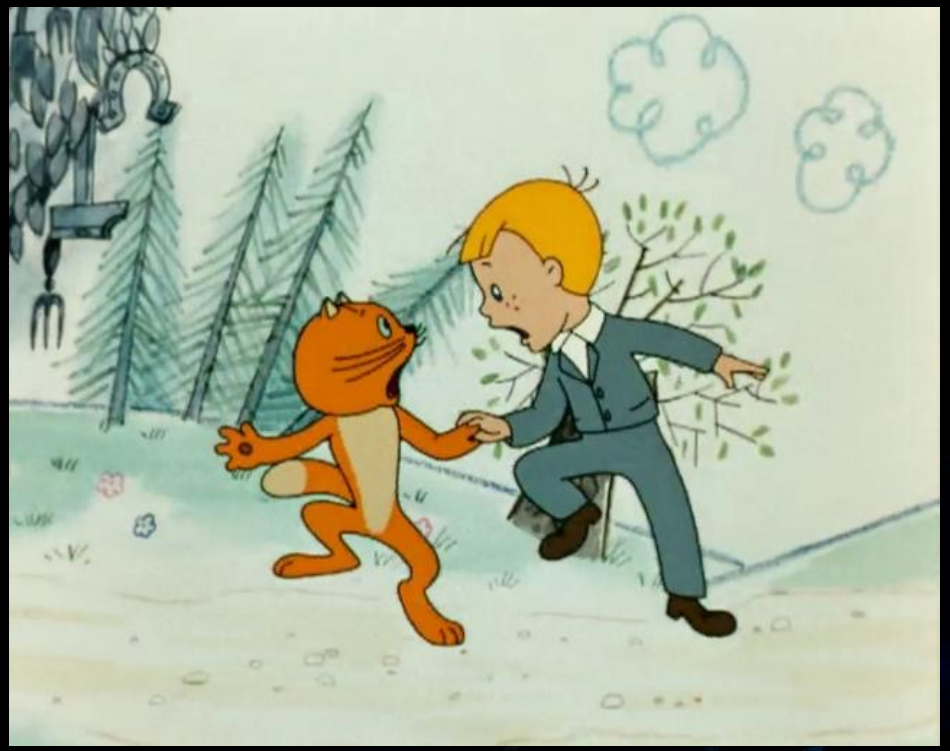
Урок:

Блокировка релиза – недостаточная мотивация для разработчиков по работе с уязвимостями

Что делаем?

Повышаем вовлеченность разработки в Sec проверки

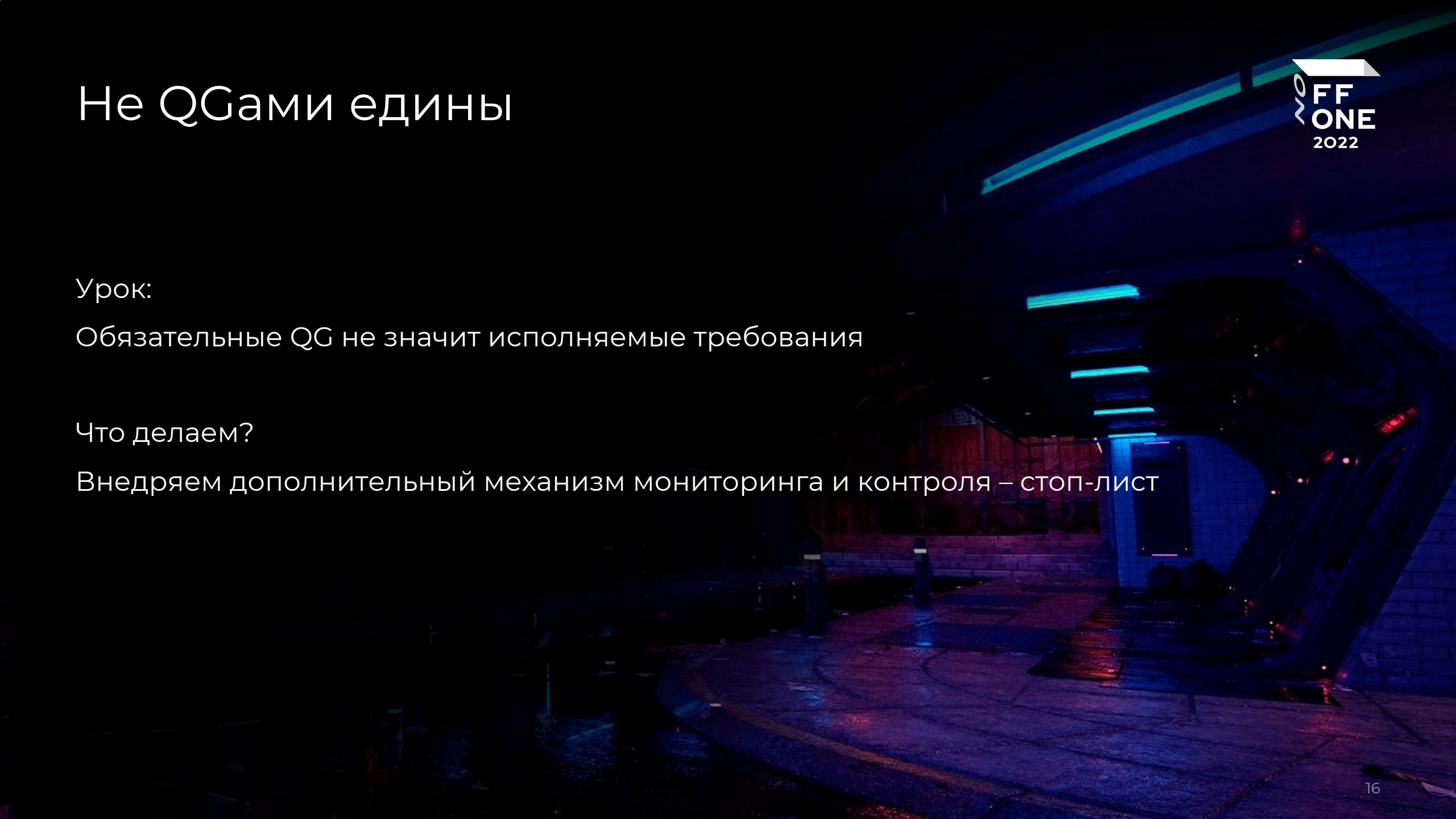
Не QGами едины



Витя с Тимофеем в шоке от блокировки релиза...

И пытаются найти пути обхода

Не QGами едины



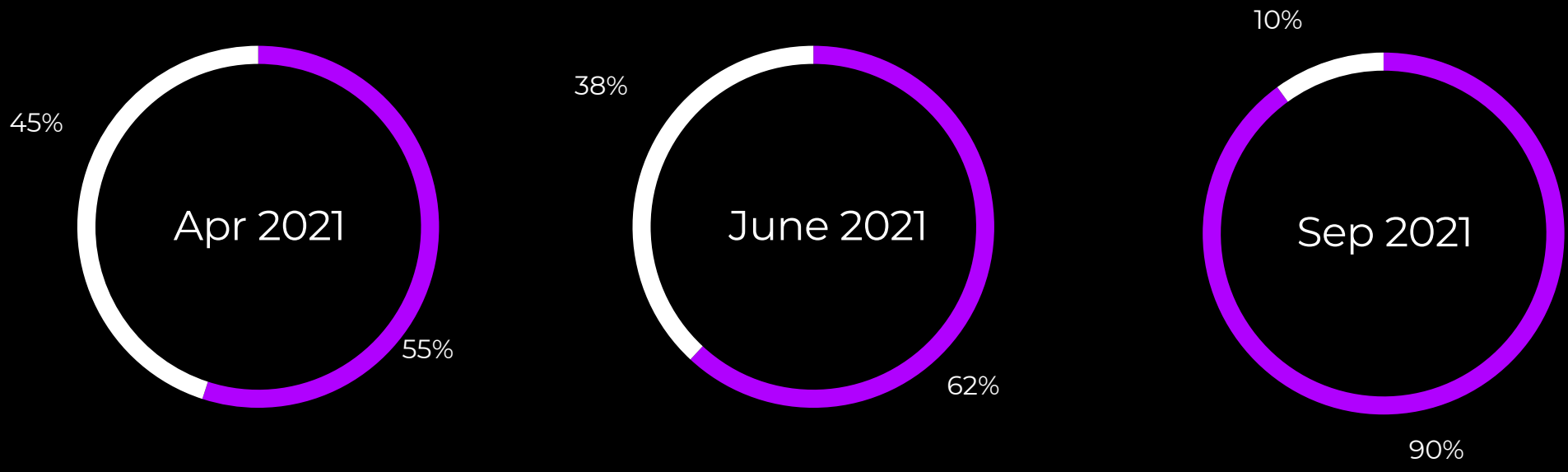
Урок:

Обязательные QG не значит исполняемые требования

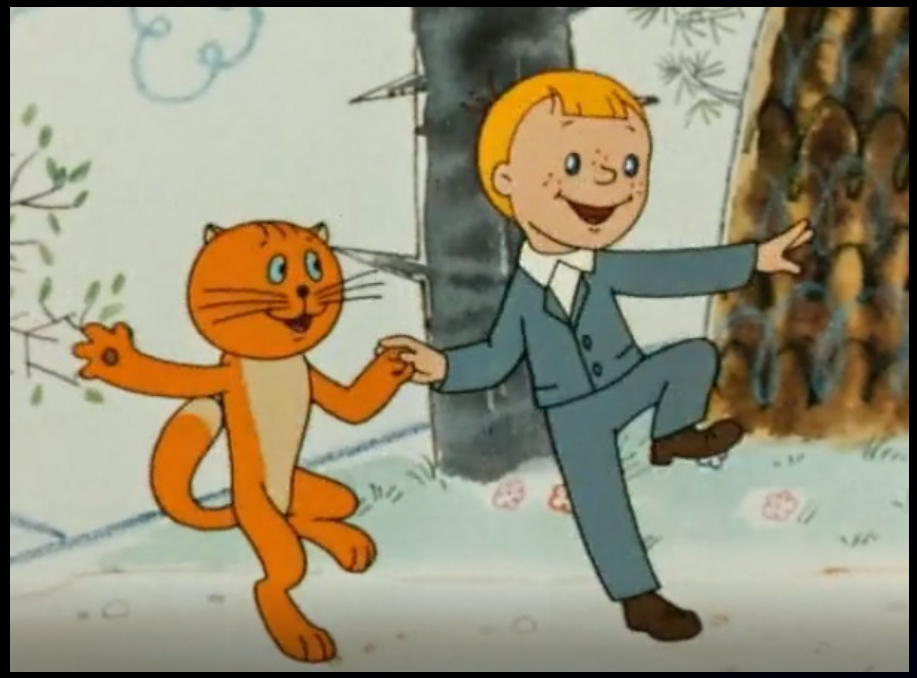
Что делаем?

Внедряем дополнительный механизм мониторинга и контроля – стоп-лист

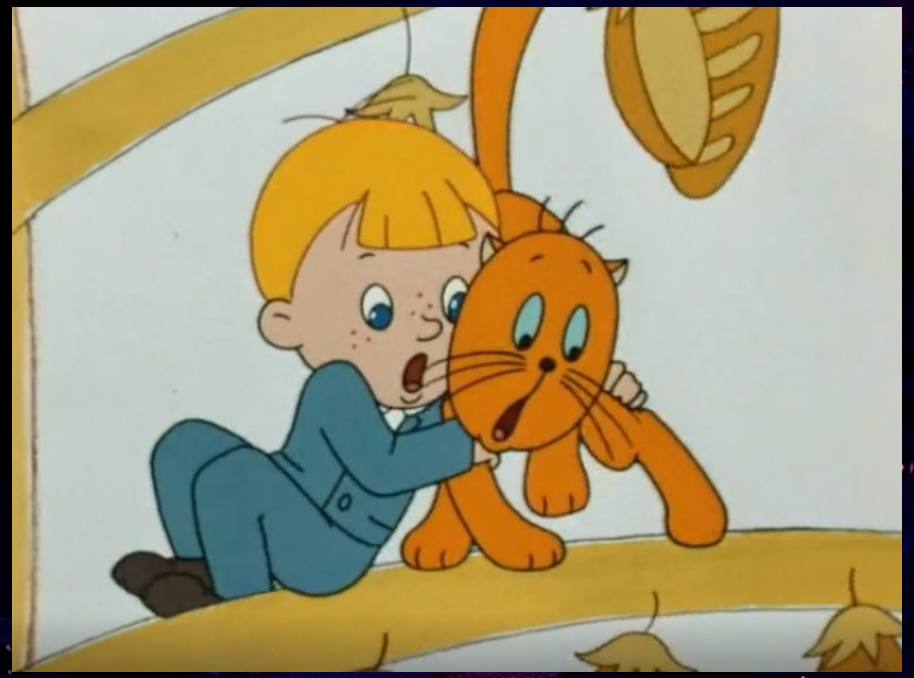
Не QGами едины



Вас много, а я одна

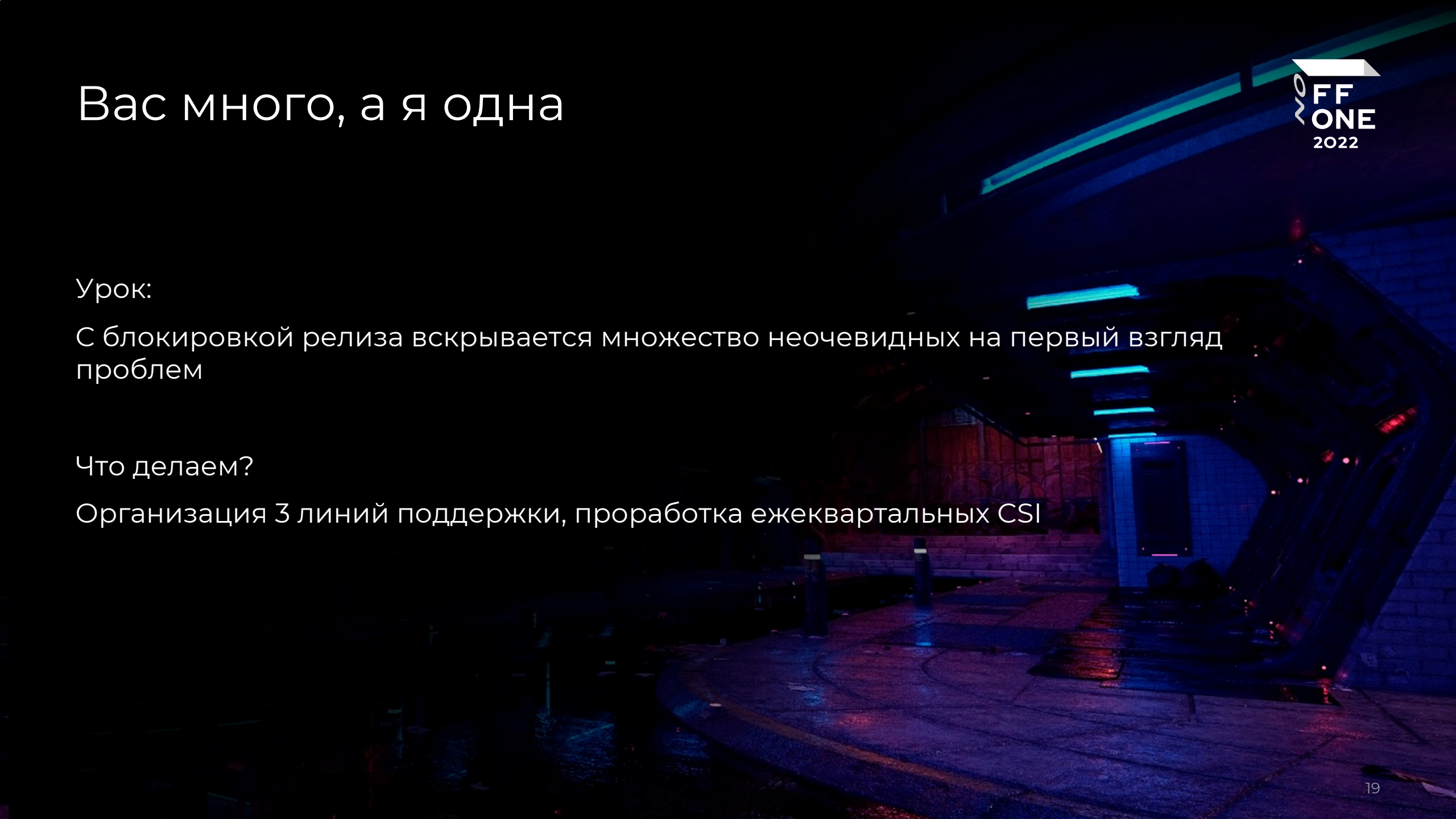


Только вопросы по уязвимостям



+100500 обращений

Вас много, а я одна



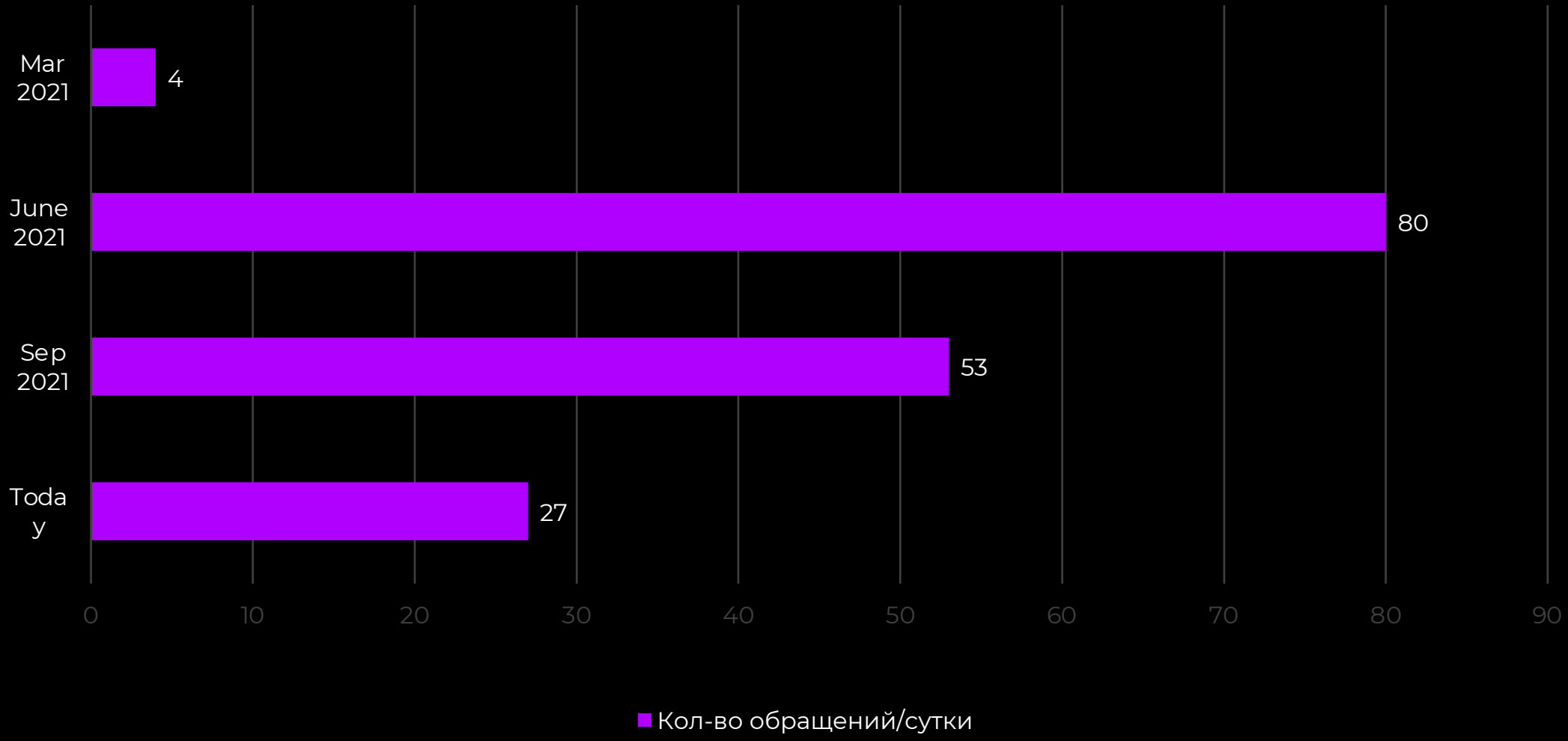
Урок:

С блокировкой релиза вскрывается множество неочевидных на первый взгляд проблем

Что делаем?

Организация 3 линий поддержки, проработка ежеквартальных CSI

Вас много, а я одна



Кто даст DAST?!

Виктор рад, что появился DAST,
будут и PoC, SAST достал фолзить...

Виктор не был готов к DAST...

Кто даст DAST?!

Урок:

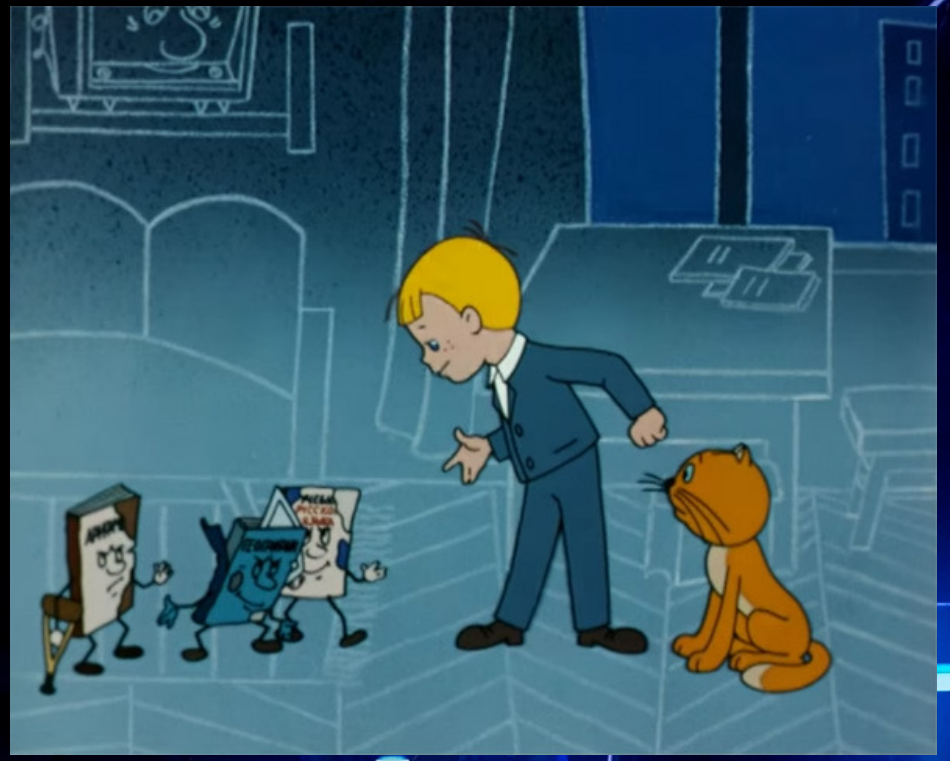
DAST требует другой уровень зрелости разработки и практик DevOps

Что делаем?

Осуществляем поиск других путей для применения инструментов класса DAST

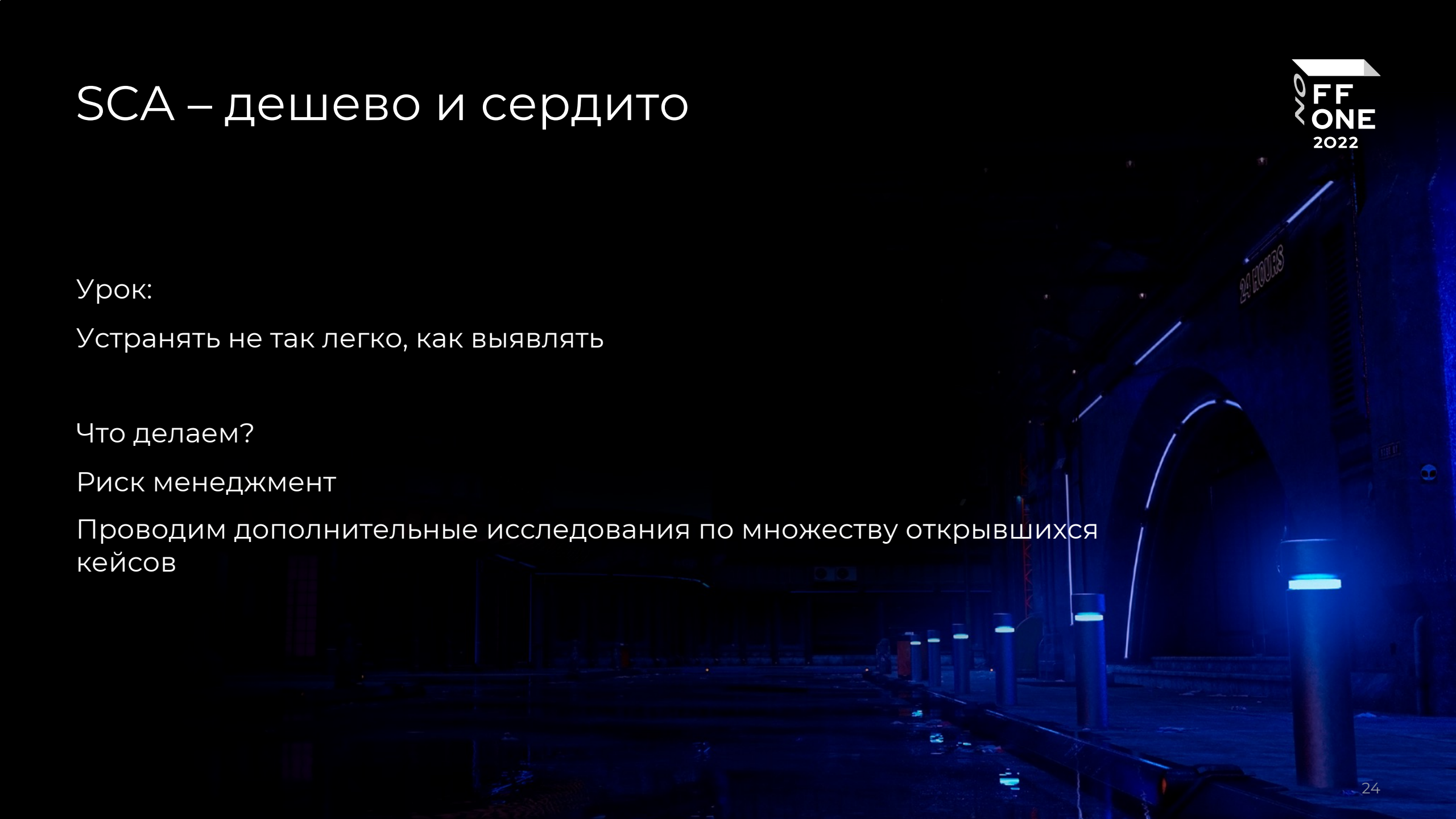
SCA – дешево и сердито

В предвкушении простоты устранения



Методики, принятие рисков, процессы...

SCA – дешево и сердито



Урок:

Устранять не так легко, как выявлять

Что делаем?

Риск менеджмент

Проводим дополнительные исследования по множеству открывшихся кейсов

Можно купить DevSecOps, но не безопасность

Виктор с Тимофеем выучили все уроки по DevSecOps ☺


ON
FF
ONE
2022