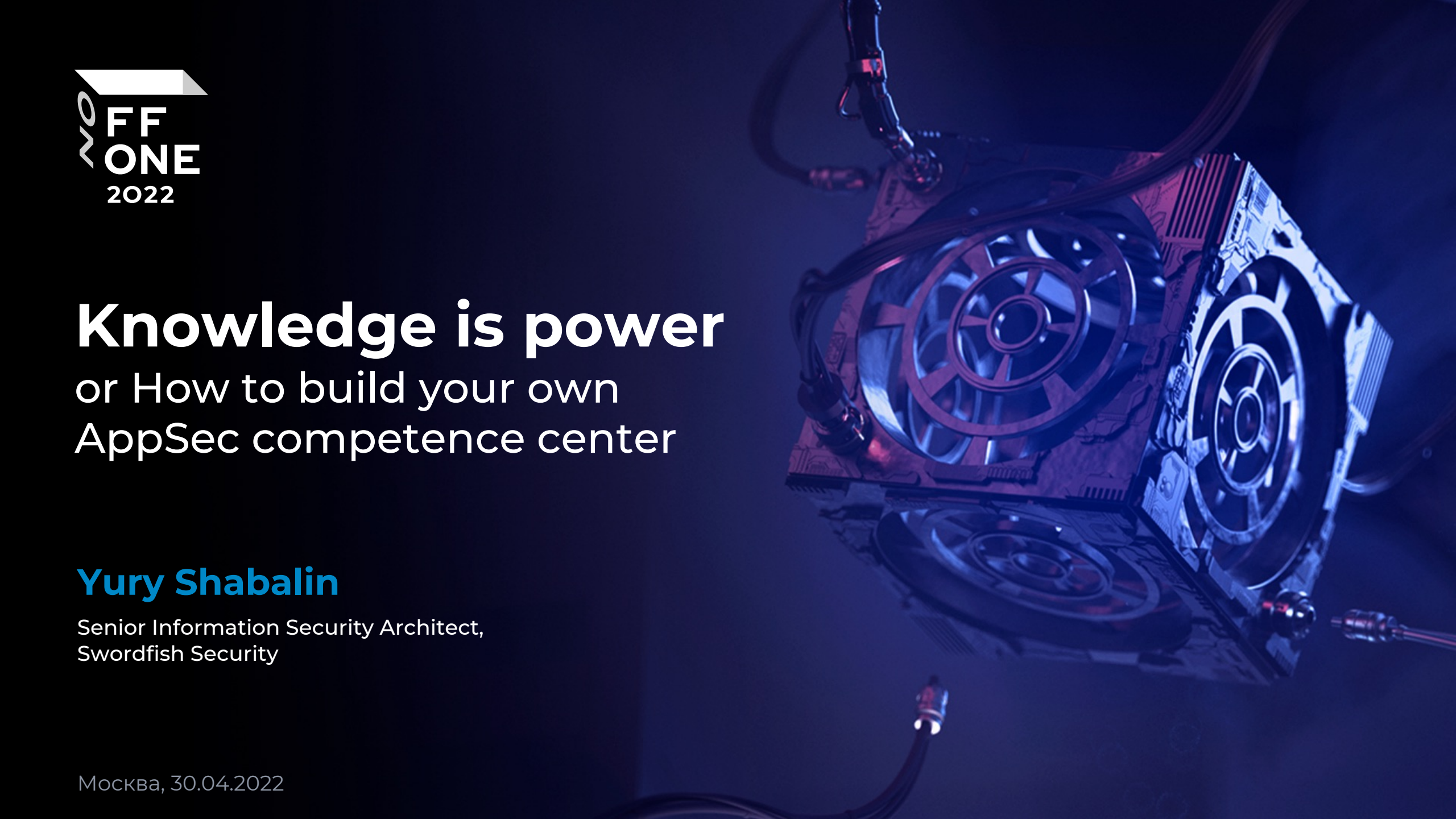


ON FF ONE 2022

Knowledge is power

or How to build your own AppSec competence center

Yury Shabalin

Senior Information Security Architect,
Swordfish Security

Москва, 30.04.2022

Whoami

Yury Shabalin

Chief Security Architect at Swordfish Security

- Ex - Positive Technologies, Alfa-Bank, Sberbank
- Developer
- SSDL integrator
- Source code analyst
- Mobile application security analyst
- Security Researcher
- Android Bughunter

Speaker at conferences

Zer0Nights, PhDays, RISSPA, OWASP, OFFZONE

Для кого это выступление

- Вы только планируете или начинаете выстраивать процесс безопасной разработки (DevSecOps)
- Вы в активной фазе развития процесса DevSecOps
- У вас всё работает и вы счастливы

Какие проблемы пытаемся решить

Коммуникационные / процессные

1. Безопасность живет в своем замкнутом мире
2. Разработка не знает о существовании безопасности
3. Разработка и безопасность конфликтуют
4. Безопасность — карательный орган

Какие проблемы пытаемся решить

Проблемы с инструментами

1. Нет инструментов под используемые технологии
2. Нет денег на инструменты
3. Инструменты адски фолзят
4. Некому разбирать срабатывания
5. Никто не устраняет уязвимости

Awareness – главная часть DevSecOps

OFF ONE 2022

Чего мы добиваемся?

1. Выстраивание отношений между безопасностью и разработкой
2. Поиск разработчиков, заинтересованных в безопасности (потенциальные Sec Champ)
3. Узнаваемость «бренда» отдела безопасности
4. Формирование / развитие компетенций у разработки
5. Улучшение качества / безопасности приложения

С чего начать?

С того что уже есть

1. Соберите все свои наработки в едином месте
   - Требования к ПО
   - Архитектурные требования
   - Требования к OpenSource
   - Библиотеки / шаблоны безопасного кода
   - Рекомендации по безопасности
2. Пересмотрите / переработайте эти материалы в нормальный (человеческий) вид

Создайте портал AppSec

- У всех должен быть доступ
- Внутри понятная и четкая структура
- Развернуть можно где угодно
  - Confluence
  - Wiki
  - Wordpress
  - SharePoint
  - Что угодно, что уже есть в компании
- Все материалы, что есть – выкладываем туда (см. предыдущий слайд)
- Анонсы всех мероприятий или отчеты с них – также на портале
- Все дефекты, что заводим в дефект-трекер, ссылаются на этот портал

Развитие портала – примеры безопасного кода

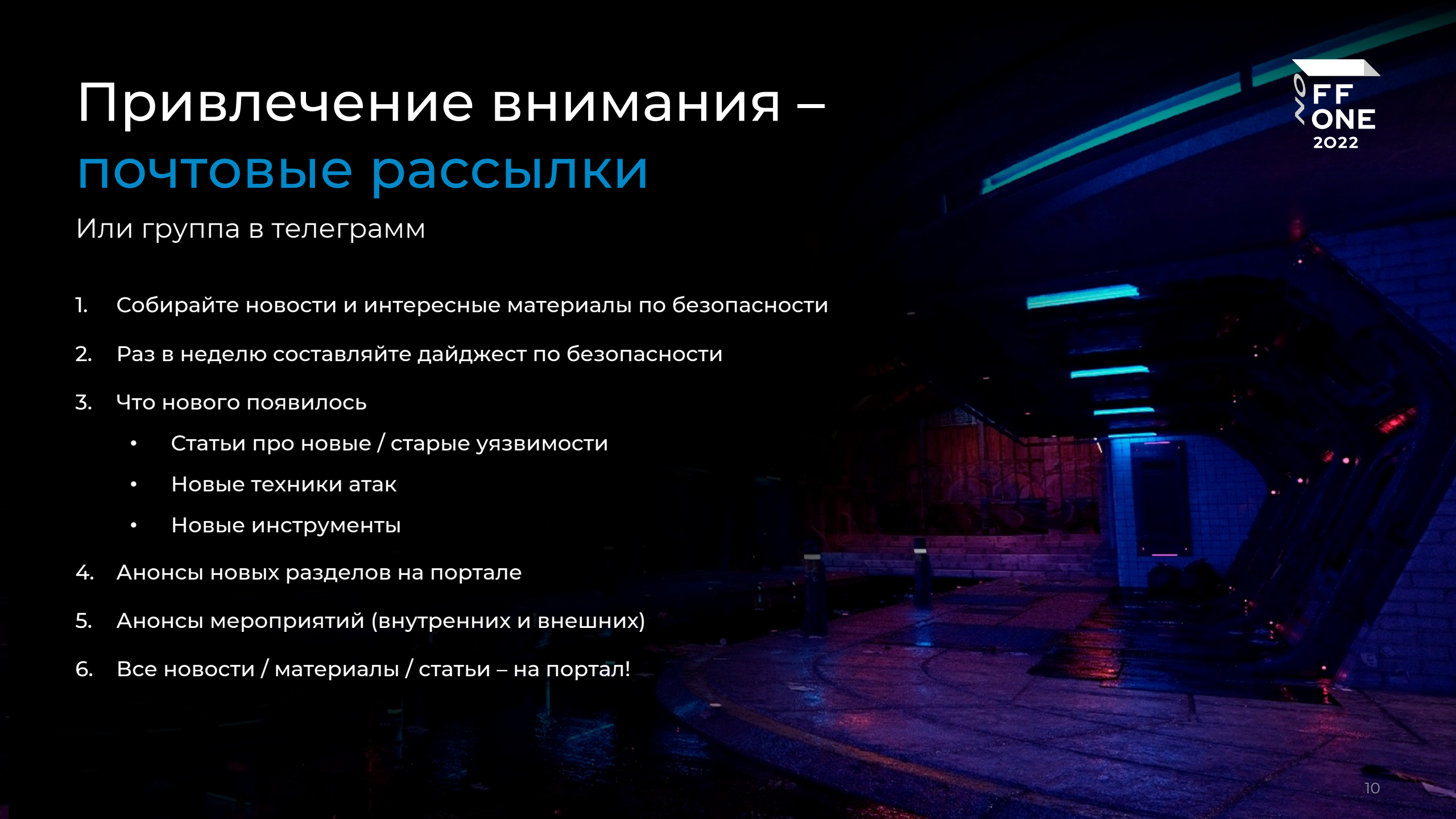
Или примеры небезопасного

1. Пройдите по уязвимостям, которые ранее были обнаружены
2. Посмотрите, какие ошибки были допущены в коде
3. Как их исправили
4. Создайте несколько страниц с описанием того, как правильно делать
5. Если таких примеров нет внутри, посмотрите на общепринятые стандарты разработки и нужное перенесите себе
6. Все материалы – на портал!

Привлечение внимания – почтовые рассылки

Или группа в телеграмм

1. Собирайте новости и интересные материалы по безопасности
2. Раз в неделю составляйте дайджест по безопасности
3. Что нового появилось
   - Статьи про новые / старые уязвимости
   - Новые техники атак
   - Новые инструменты
4. Анонсы новых разделов на портале
5. Анонсы мероприятий (внутренних и внешних)
6. Все новости / материалы / статьи – на портал!



Проводим обучение (1/3)

OFF ON ONE 2022

Интерактивные курсы

1. Быстрые и легкие тренинги
2. Понятная подача материала
3. Можно вернуться к ним в любой момент
4. Находятся в корпоративной системе обучения
5. Назначаются всем, кто принимает участие в разработке при выходе на работу
   - Тестировщики
   - Разработчики
   - Аналитики
   - Архитекторы
   - Бизнес (да-да)
6. Знакомят коллег с азами безопасности и главное, знакомят с отделом ИБ и внутренним порталом
7. После прохождения курса – welcome-письмо от отдела ИБ со всеми ссылками
8. Все ссылки на курсы – на портал! И в курсе – ссылки на портал)

Проводим обучение (2/3)

Онлайн / видео тренинги

1. Намного более технические и информативные, чем интерактивные
2. Разбиты по смыслу и главам. Можно проходить по частям
3. Факультативно – домашние задания
4. Как один из вариантов – собирать группу и между видео делать сессии ответов на вопросы и разбор заданий, но это сложнее
5. В курсе – только ваши технологии и инструменты
6. Тренинги или ссылки на них – на портал!

Проводим обучение (3/3)

Проведение митапов

1. Митапы внутренние от внутренней команды ИБ на конкретную тему

   Тема выбирается или голосованием разработки, или по наиболее часто встречающимся уязвимостям

2. Митапы внешние, где можно приглашать коллег из соседних компаний поделиться опытом.

   А можно и не из ИБ, а из разработки

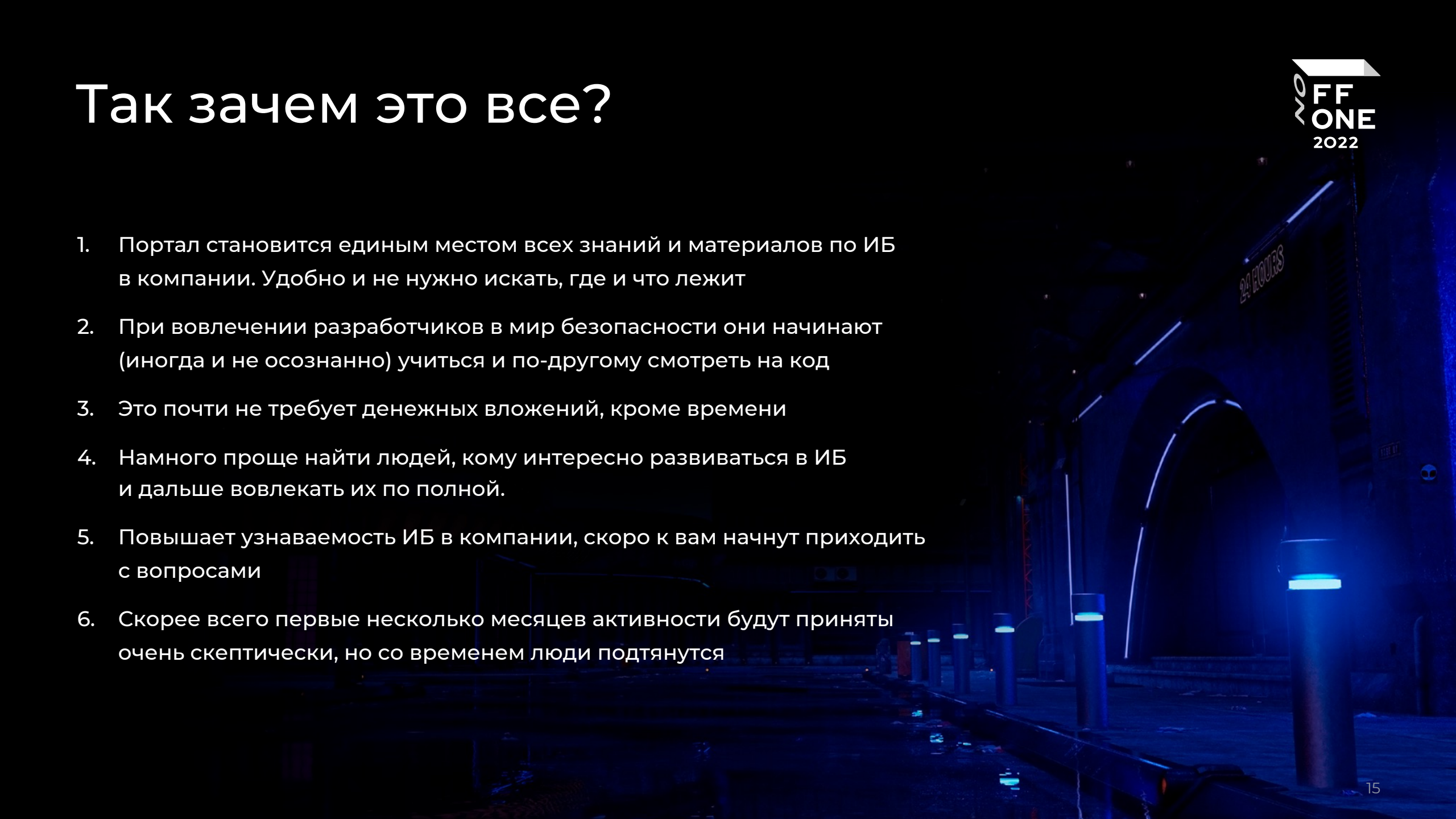
3. Устраивать совместные митапы с разработчиками из нескольких компаний

4. Записи митапов – на портал и в рассылку

Проводим CTF

- Не обязательно разрабатывать свои, можно взять уже имеющиеся
- Как вариант – развернуть внутри площадку и добавлять туда задания
- Из плюшек победителям – дополнительные выходные, мерч компании, всеобщее одобрение и слава
- К победителям – более пристальный взгляд в плане их роли, как Security Champions
- После проведения – встреча с разбором заданий и запись на портал!

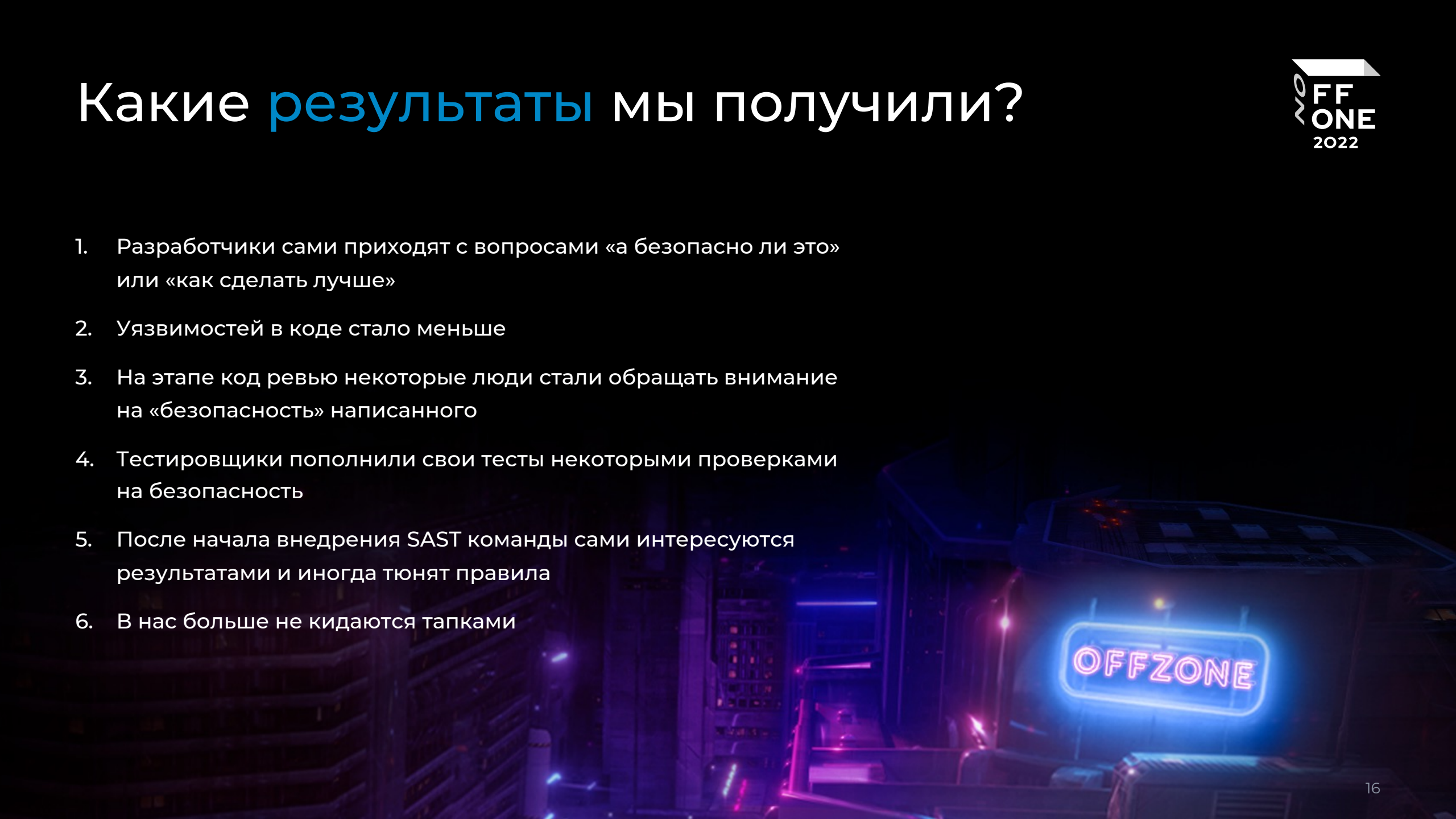
Так зачем это все?



1. Портал становится единым местом всех знаний и материалов по ИБ в компании. Удобно и не нужно искать, где и что лежит
2. При вовлечении разработчиков в мир безопасности они начинают (иногда и не осознанно) учиться и по-другому смотреть на код
3. Это почти не требует денежных вложений, кроме времени
4. Намного проще найти людей, кому интересно развиваться в ИБ и дальше вовлекать их по полной.
5. Повышает узнаваемость ИБ в компании, скоро к вам начнут приходить с вопросами
6. Скорее всего первые несколько месяцев активности будут приняты очень скептически, но со временем люди подтянутся

Какие результаты мы получили?

1. Разработчики сами приходят с вопросами «а безопасно ли это» или «как сделать лучше»
2. Уязвимостей в коде стало меньше
3. На этапе код ревью некоторые люди стали обращать внимание на «безопасность» написанного
4. Тестировщики пополнили свои тесты некоторыми проверками на безопасность
5. После начала внедрения SAST команды сами интересуются результатами и иногда тюнят правила
6. В нас больше не кидаются тапками



Что делать еще?

1. Security Day / Внутренние конференции (день с докладами ИБ)
2. Очное приглашение на ИБ конференции / митапы
3. Соревнования между командами разработки
4. Лекции / тренинги для бизнеса
5. Телеграмм-бот / чат / канал с вопросами / ссылками
6. Общий чат, где можно задать любой вопрос
7. Полноценные руководства по безопасному программированию
8. Настольная игра по безопасности
9. И многое многое другое, что вы сможете придумать и вам самим было бы интересно

Спасибо
за внимание!

Вопросы?

yshabalin@swordfishsecurity.com
@Mr_R1p


OFF
ONE
2022