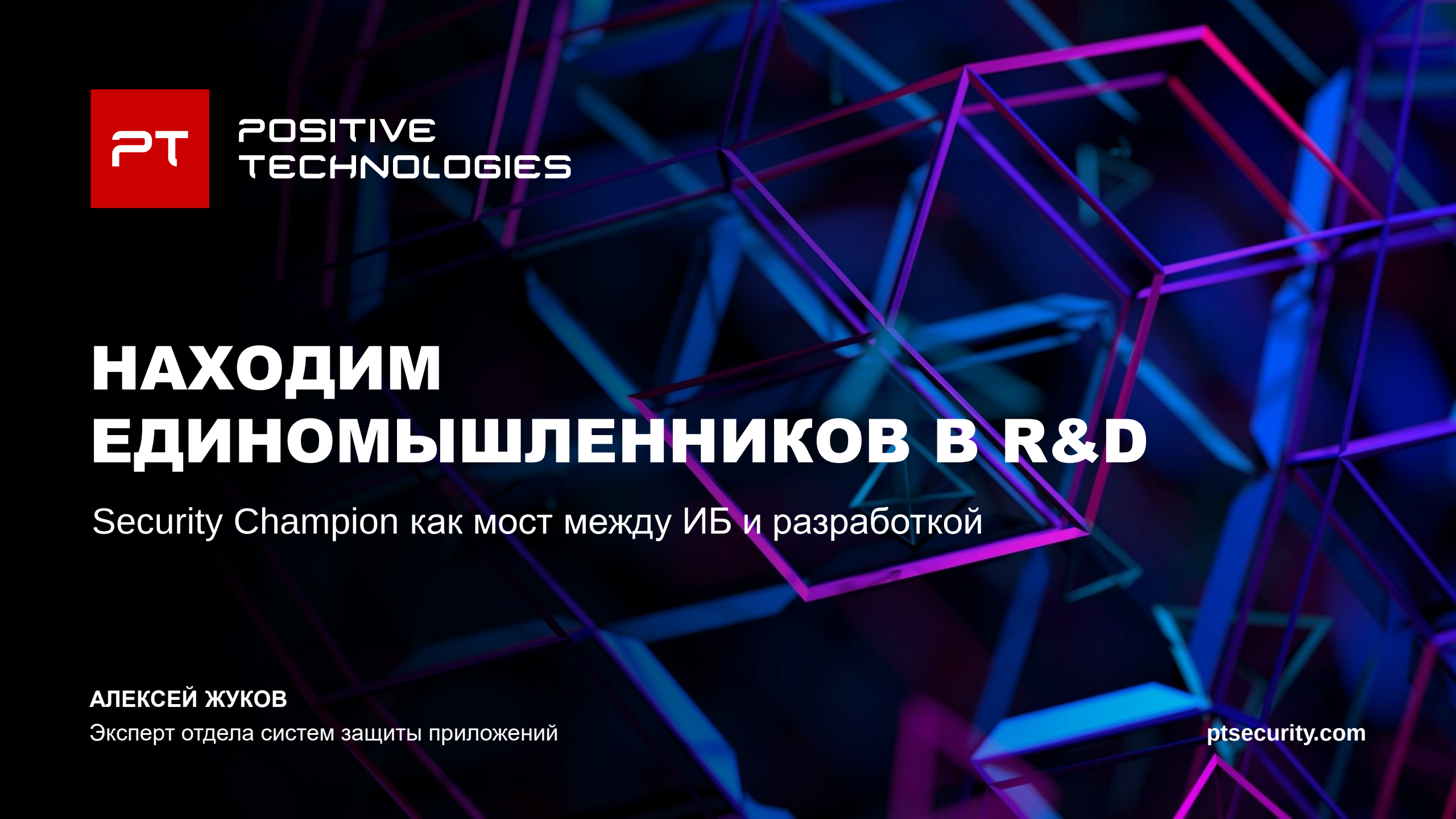


POSITIVE TECHNOLOGIES

НАХОДИМ ЕДИНОМЫШЛЕННИКОВ В R&D

Security Champion как мост между ИБ и разработкой

АЛЕКСЕЙ ЖУКОВ

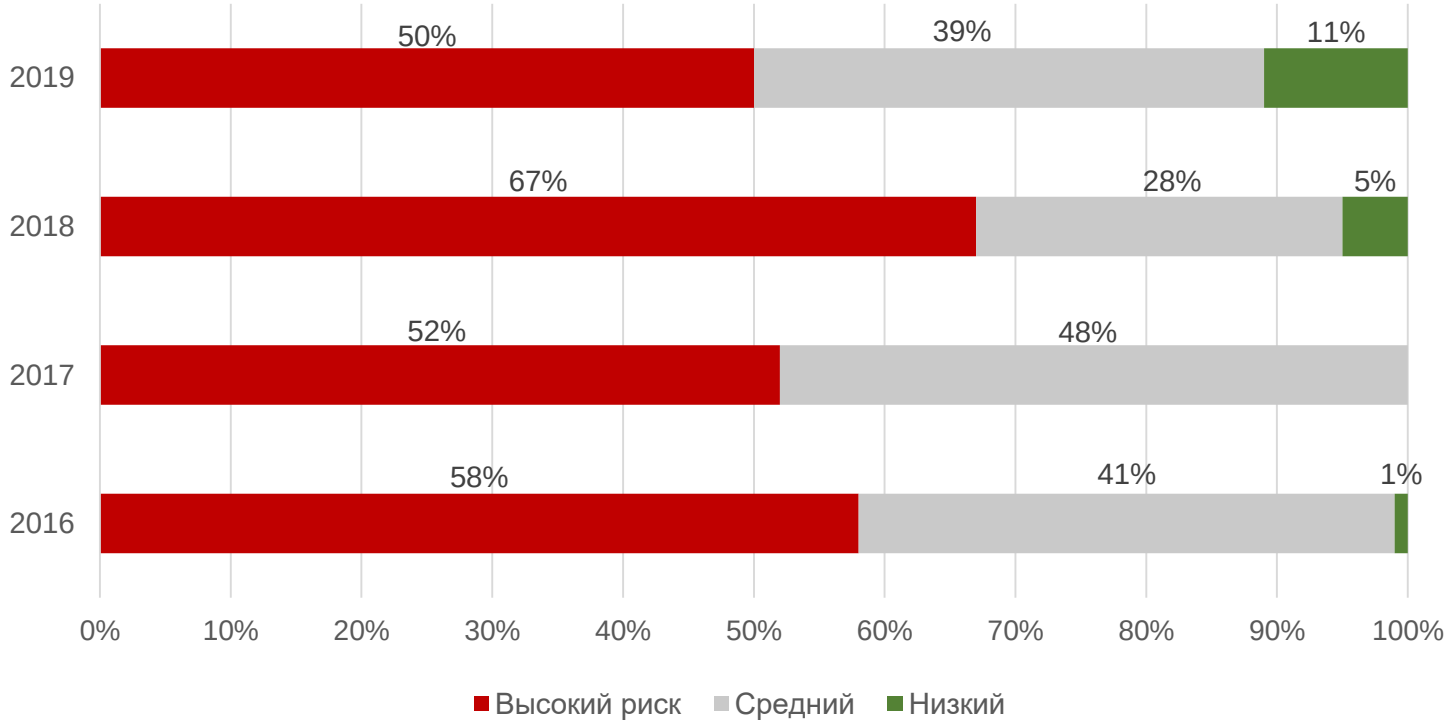
Эксперт отдела систем защиты приложений

ptsecurity.com

Зачем: уязвимости

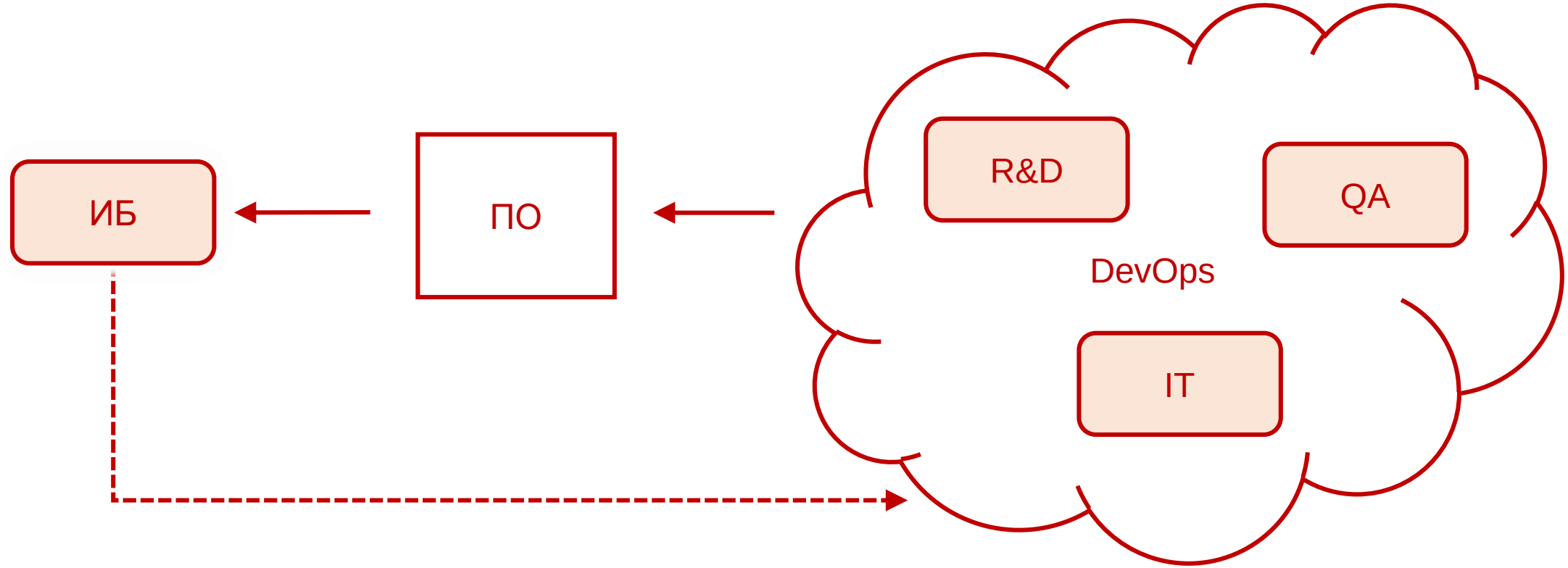
Отношение к уязвимостям в духе **«на скорость не влияет»**

ИБ привлекается лишь на **поздних стадиях** разработки



Отчет «Уязвимости и угрозы веб-приложений в 2019 году», Positive Technologies

Суть проблемы:



Как выглядит **скепсис R&D**

	High	Medium	Low	Information	Total
New Issues	13	141	1,580	0	1,734
Recurrent Issues	0	0	0	0	0
Total	13	141	1,580	0	1,734

Scan Time	00h:05m:34s
Lines Of Code Scanned	21403
Files Scanned	28

PAGE 300 OF 302

Дисклеймер: это сгенерировал не наш анализатор ;)

Почему **R&D** не стремится в **ИБ**

Причины

Нет ресурсов: своих текущих задач более, чем достаточно и проблемы ИБ не вписываются в рабочий график

Воспринимают ИБ как помеху, стоящую на пути развития функциональности продукта

Негативный предыдущий опыт и вызванный им скепсис в отношении ИБ и уязвимостей

С каждой из этих проблем нужно бороться индивидуальными методами

Что делать

Какие инструменты использовать?

Где взять ресурсы R&D?

Как зажечь R&D вопросами ИБ?

Нужен авторитет в среде R&D

Как разделить роли между ИБ и R&D?

Давайте есть слона **по частям**

Боли ИБ

- Как и для чего ломают приложения
- Возможные последствия
- Атаки на цепочки поставок

Роль Security Champion

- По-прежнему разработчик
- Развитие навыков ИБ и управления

Профильные материалы

- «Предсказываем случайные числа»
- «Небезопасная десериализация»
- «Защита Docker в production»

Нужен напарник, с которым идем в PoC

PoC

Обеспечение дальнейшей поддержки руководства

ИБ-шная часть работы Security Champion должна носить официальный характер. Показываем, что в команде разработки появляется свой человек, к которому можно обратиться по вопросам ИБ

Лучше один отличный результат, чем несколько средненьких

По итогам PoC важно показать руководству, что в теме не осталось белых пятен и все ее аспекты детально проработаны. Поэтому правильнее сосредоточиться на одном, максимум, двух проектах

Комплексное видение проблемы

Получаем видение текущих проблем как со стороны ИБ, так и от R&D

Предпосылки для создания автономной DevSecOps-команды

Security Champion понимает свою роль. Он не является исполнитель задач ИБ, их взаимоотношения носят двусторонний характер. Формируем осознание того, что DevSecOps --- в первую очередь сообщество

Поддержка руководства

Необходимость

Явное и однозначное подтверждение ценности для бизнеса

Роль Security Champion – не увлечение, а часть работы R&D с ясными обязанностями и полномочиями

Залог успешного тиражирования опыта PoC на все команды разработки

Тиражируем и стимулируем

Добровольное участие

Нужно сделать так, чтобы команды сами захотели своих Security Champion’ов

Нематериальное поощрение

Важно дать понять, что роль Security Champion --- способ развить в себе навыки, востребованные на рынке и выходящие за грани коридора «Джун-мидл-сеньор-тимлид»

Признание значимости

Security Champion’ы должны понимать востребованность решаемых ими задач

Сувенирка, бонусы, KPI и все такое

Не забываем и о материальной подпитке: на голом энтузиазме далеко не уедешь

Целевая структура

Взаимодействие

- ИБ – SC – R&D
- SC --- не исполнитель задач ИБ
- Тренинги и менторство

Сообщество

- SC — свой человек в R&D с четким перечнем задач
- ИБ как консультант

Митапы

- Командные
- Индивидуальные

Чем планируем заниматься

Отталкиваемся от наших целей. Постепенно, начиная с одной-двух задач. Привлекаем ИБ для консультаций

Обучаемся, играя: доклады с конференций, онлайн-курсы, внутренний CTF

Пушим инициативу Security Champion, даем инструменты для работы

Критерии успешности

Оцениваем тренды, а не абсолютные значения

Анализ динамики изменений как основы для принятия решений

Анализируем причины

Ставим вопросы и корректируем подходы к решению проблем

Рост сообщества

Показатель заинтересованности команд разработки в тематике ИБ

Чек-лист

01

ПОДДЕРЖКА РУКОВОДСТВА

- Убедитесь, что руководство понимает важность внедрения безопасной разработки.
- Пилотирование, постепенное внедрение

02

РОЛЬ SECURITY CHAMPION

- Выделите участника команды разработки, заинтересованного в безопасности продукта (позволяет решить технические, организационные и другие проблемы).

03

ТИРАЖИРОВАНИЕ ПОДХОДА

- Фиксируем значимость темы для компании в целом
- Добровольное участие
- Стимулирование участников команды Security Champion

04

НАЛАЖИВАЕМ СТРУКТУРУ ВЗАИМОДЕЙСТВИЯ

- Определите роли всех участников
- Регулярные митапы
- Развитие сообщества

05

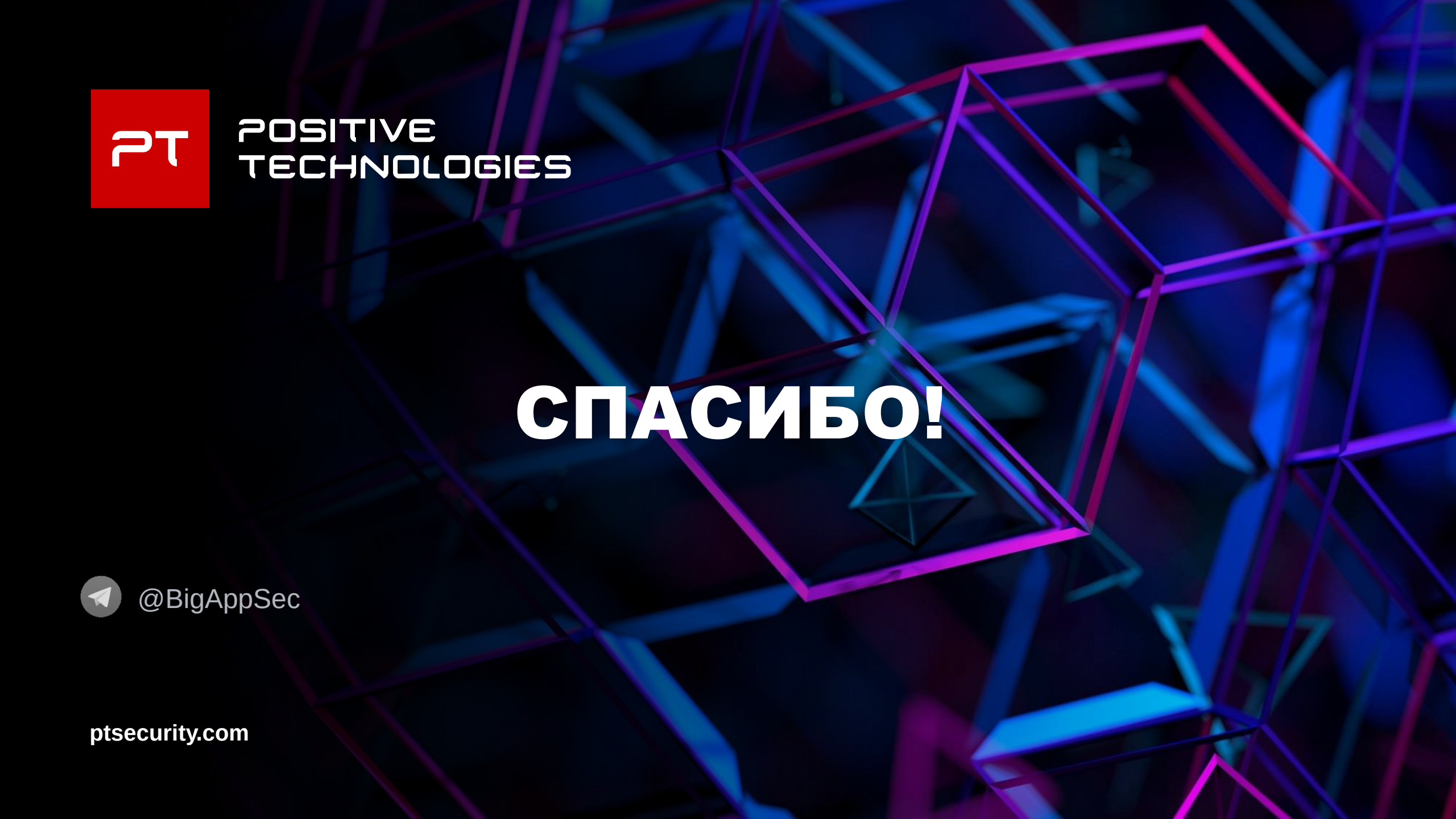
ЧЕМ ЗАНИМАЕМСЯ

- Основываемся на поставленных целях, постепенно решая требуемые задачи
- ИБ – не начальник и не враг, а консультант и наставник
- Обучаемся
- Осваиваем инструменты ИБ

06

ОЦЕНИВАЕМ УСПЕШНОСТЬ

- Работаем с трендами
- Анализируем причины


POSITIVE
TECHNOLOGIES
СПАСИБО!
@BigAppSec
ptsecurity.com