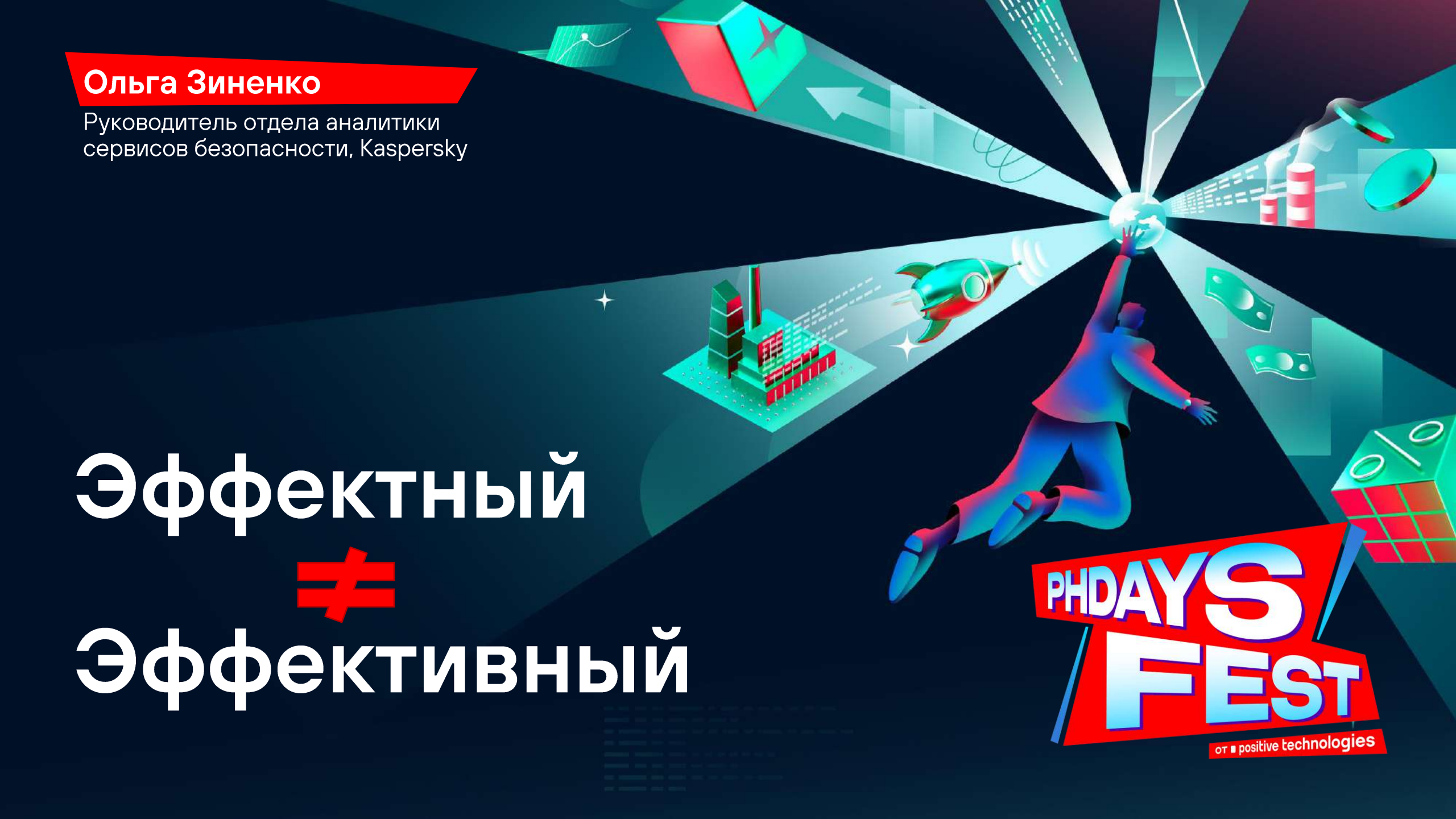
Ольга Зиненко
Руководитель отдела аналитики
сервисов безопасности, Kaspersky



Эффектный ≠ Эффективный

PHDAYS FEST
от positive technologies

Аудиты, Комплаенс, Пентест, Исследования

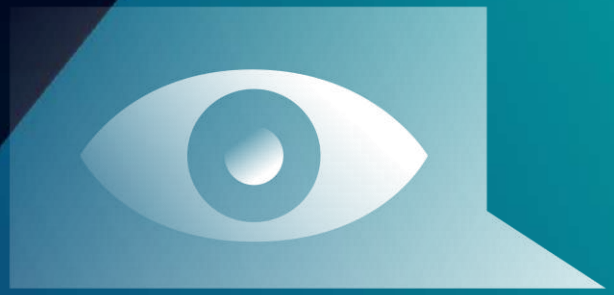
Уже 12 лет отвечаю за результат

Ольга Зиненко

Руководитель отдела аналитики сервисов безопасности, Kaspersky

Эффектность

Целью вашего клиента точно не является получение шокирующих эмоций от продемонстрированных атак



Цели для компании

Зачем вам пентест?

POSITIVE HACK DAYS FEST

от positive technologies

Какие задачи пытаются решить компании

Оценка влияния успешных атак на компанию

Приоритизация бюджета и трат на ИБ

CISO

Выявление и устранение критических уязвимостей в инфраструктуре

Выявление необходимых мер защиты

ИБ Менеджмент

Получение нового видения на используемые системы, приложения, сети и данные

Исполнители

Понимание рисков ИБ

Дирекция

Тренировка и проверка готовности к реагированию на угрозы

Оптимизация и улучшение процесса

SOC Менеджмент

Свободное место для ваших задач

Someone else

Из чего складывается пентест
по мнению Заказчика

Полнота

Экспертность

План действий

Проект можно считать эффективным, если

- **Корректны цели исследования**
- **Качественное исполнение**
- **Эффективное устранение**

по его завершению Заказчик ушел с четким пониманием того, что нужно сделать, чтобы усовершенствовать систему защиты

Чтобы проект прошел хорошо,
Исполнитель должен наладить

- Процессы
- Коммуникации
- Инструменты
- Автоматизация

Эффективные цели

Определение поверхности атаки

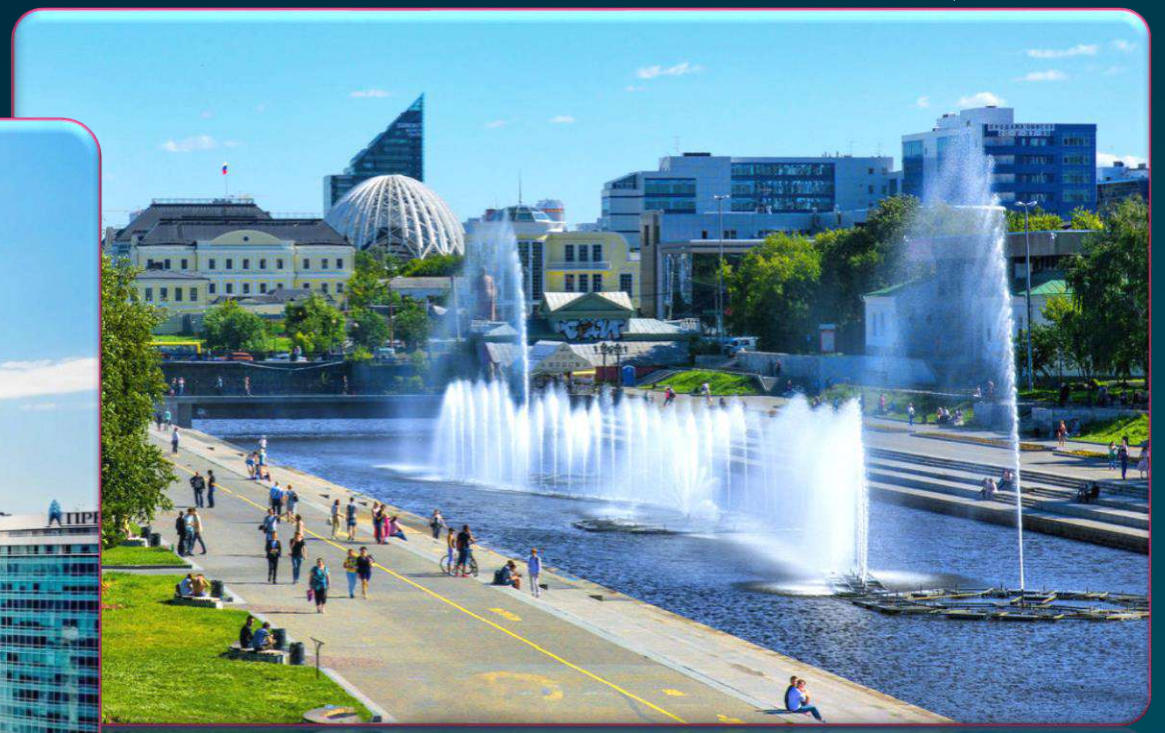
Границы проведения работ напрямую зависят от полноты данных, собранных на этапе разведки

Публичная информация о компании

- **Векторы потенциальных атак**
- **Учетные данные из утечек**
- **Дополнительная информация**

DFI сервис

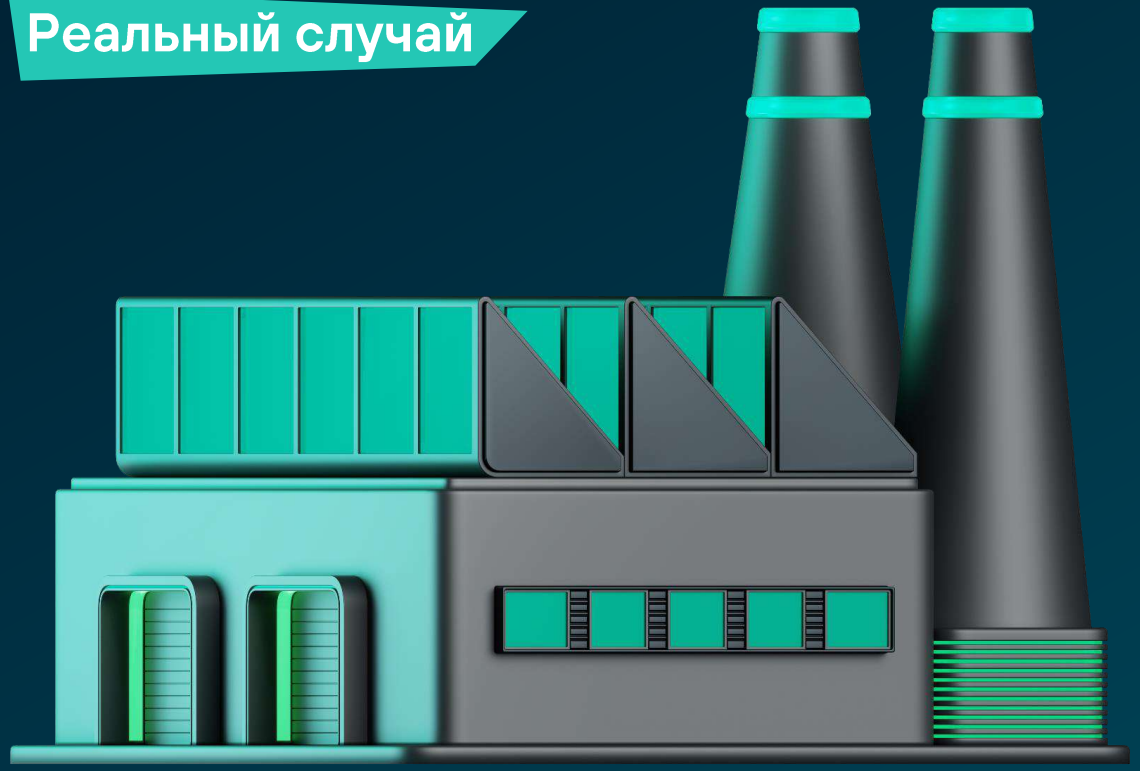
Инфраструктура в глазах Заказчика



Как это видят пентестеры

Выход за границы

Реальный случай



Одной актуальной учетной записи может быть достаточно для компрометации компании

Эффективное исполнение

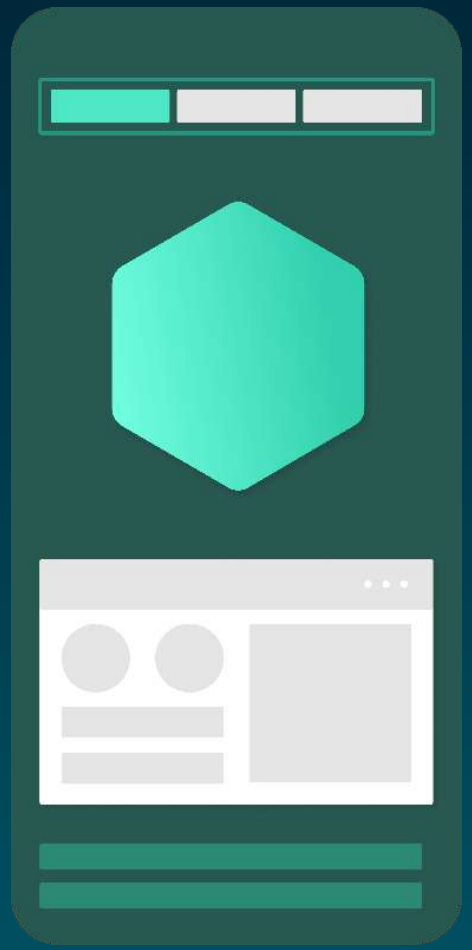
By Kaspersky security assessment

Командная работа

Кейс 1

Доступ во внутреннюю сеть

Был получен через мобильное приложение корпоративного мессенджера. Уязвимая конфигурация сервера позволила организовать SOCKS5-туннель прямо во внутреннюю сеть



Командная работа

Кейс 2

Zero-day

Уязвимости в сервисе для видеоконференцсвязи позволили получить доступ во внутреннюю сеть компании и развить атаку там

Роль аналитика в команде

- ✓ Верификация модели угроз
- ✓ Визуализация данных
- ✓ Составление рекомендаций
- ✓ Взаимодействие с ИБ-специалистами заказчика
- ✓ Презентация результатов

Эффективное устранение

Приоритизация уязвимостей

Какие из уязвимостей следует устранять в первую очередь?

Приоритет

=

Уровень риска

+

Критичность вектора

+

Сложность устранения

План действий

1 месяц

Срочные меры

- То, что надо было сделать вчера

1 год

Среднесрочные меры

- Наиболее важные изменения, требующие значительных усилий

Более 1 года

Долгосрочные меры

- Изменение архитектуры и бизнес-процессов, внедрение или совершенствование процессов и средств контроля безопасности

Эффективность для Заказчика может быть не эффективна для Исполнителя

phd x pt

Реальный случай

Постоянное совершенствование

Оценка удовлетворенности Заказчика после каждого проекта позволяет принимать оперативные меры по корректировке внутренних процессов и улучшению предоставляемых услуг

Спасибо!