Безопасность инфраструктуры и защита от фишинг-атак

МегаФон | ПроБизнес

Станислав Погоржельский

Руководитель технологической поддержки

МЕГАФОН | ПроБизнес

Какие темы мы с вами обсудим?

- Применение инструментариев сотрудника ИБ для защиты инфраструктуры из вне
- Угрозы фишинговых атак
- Бонус. Security Awareness от МегаФона: платформа для повышения осведомленности сотрудников

ПроБизнес

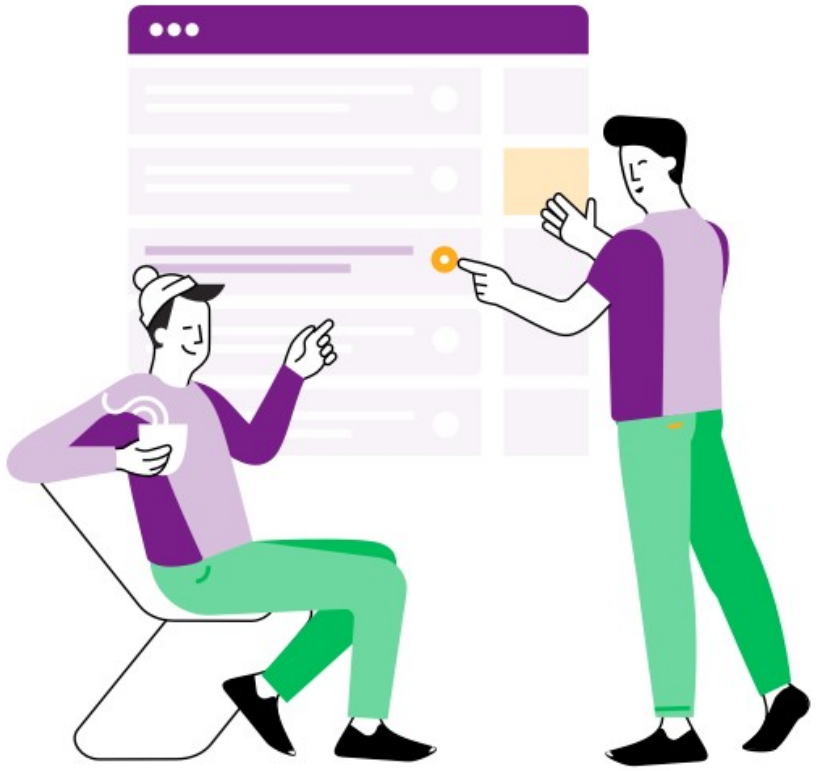
«Требуется 20 лет для того, чтобы построить репутацию компании, и всего 3 минуты инцидента по информационной безопасности для того, чтобы все это разрушить».

Какова цель кибератаки?

- Вывести из строя доступность веб-ресурса или IPv4 адреса
- Кража данных. Например, снятие копии дампа СУБД, где хранится информация о пользователях
- Испортить репутацию. Например, подмена текста на главной WEB странице сайта

ПроБизнес

Кейс.
Услуги КБ от МегаФона как инструментарий защиты активов Заказчика



МЕГАФОН | ПроБизнес

Пример компании, которую мы защитили

Цель проекта:

— Выявить у клиента «проблемные» места в ИТ инфраструктуре
— Предложить инструментарий решения проблем
— Комплексно решить задачи
— Провести обучение для персонала по работе с персональными данными

ПроБизнес

Этап 1. Консалтинг

Анализ инфраструктуры по явным возможным уязвимостям

Применили услуги:

«Сканер уязвимостей» и **«PENTEST»**

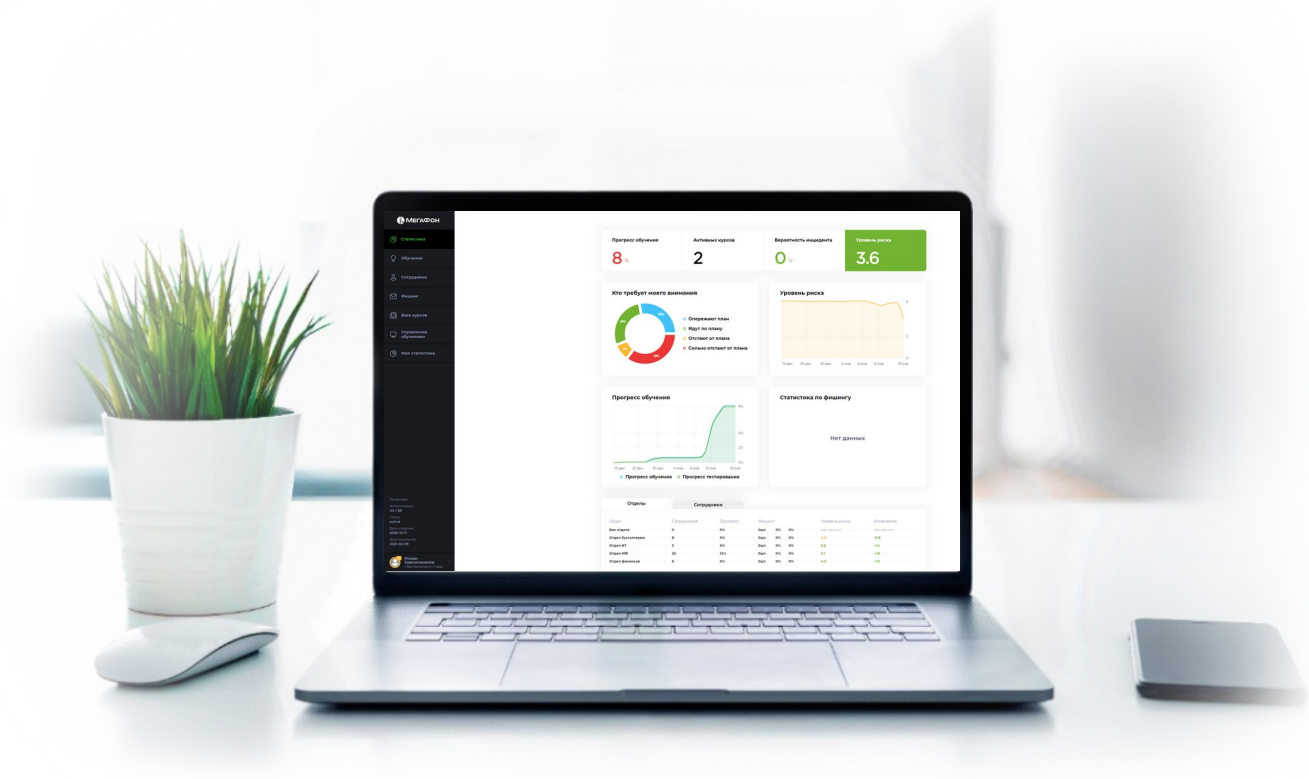
Сформировали отчет, в котором отразили:

- Наличие используемого ПО в периметре Заказчика
- Версии ПО и наличие требуемого обновления, чтобы учесть актуальные сигнатуры
- Изучили сетевую топологию
- Составили основную модель угроз и перечень возможных «нарушителей»
- Проверили наличие выполнения регламентирующих правил (нормативы) на наличие средств применения и оформления документации

ПроБизнес

Этап 2. Выводы

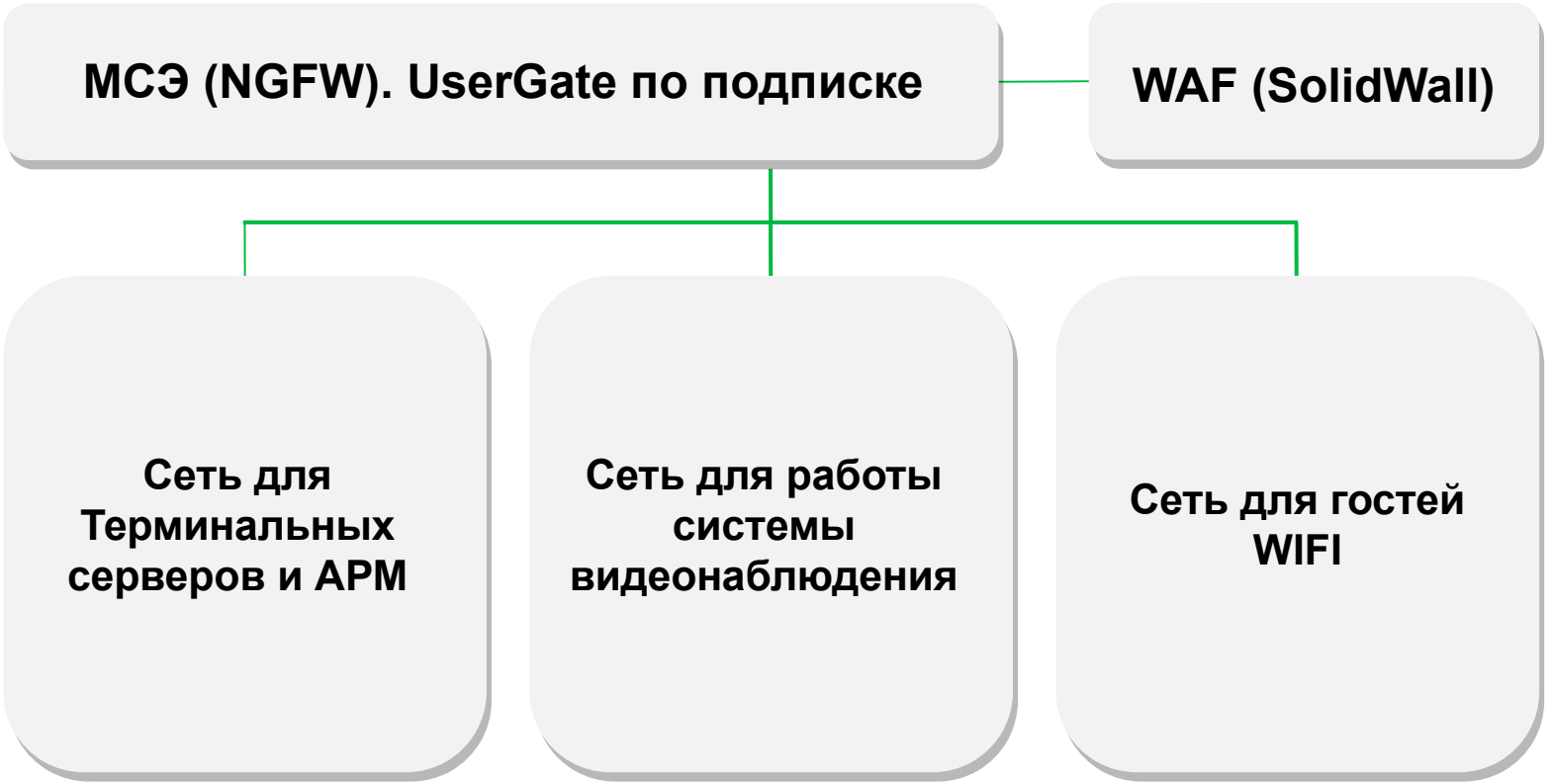
- Заказчик использует ПО, которое не обновлялось уже давно
- Не было защиты из вне (публичный интернет канал)
- Не выполнялись требования нормативной функции или ПО было снято с поддержки от вендора
- Отсутствие разделение сетей, т.е. не было даже DMZ для гостевого WIFI



ПроБизнес

Этап 3. Решение и реализация средств КБ

Разделили сети заказчика на группы и установили новое ПО



Выводы:

- Заменили текущий МСЭ на UserGate, т.к. вендор оборудования не может оказывать услуги
- Новое ПО МСЭ предоставили в аренду, чтобы можно было оперативно наращивать ресурсы и модули ИБ
- Разделили сети, чтобы минимизировать ущерб от злоумышленника при попадании его в корпоративную сеть
- Решили вопрос с регуляторами, т.к. UserGate находится в реестре российского ПО и имеет сертификат ФСТЭК
- Предоставили WAF для сайта

ПроБизнес

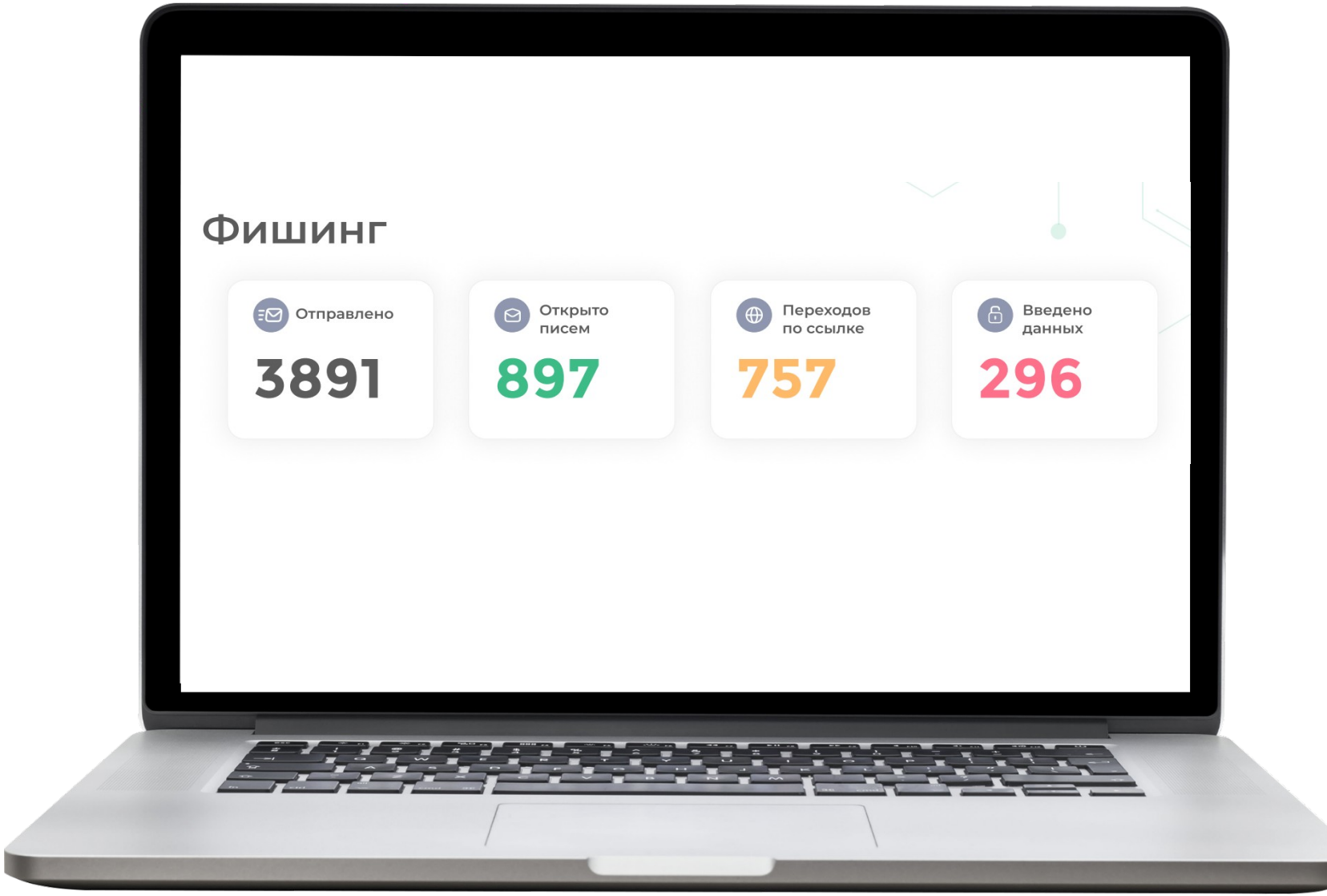
Этап 4. Работа с пользователями

Выявили проблемы:

- Большинство технически неподкованных сотрудников не знают основ цифровой гигиены, поэтому халатно относятся к информационной безопасности при использовании личных и корпоративных устройств
- У руководителей отсутствует возможность контролировать уровень знаний своих сотрудников
- Нельзя проверить действия сотрудников в ситуациях, приближенных к реальной атаке
- У руководителей нет подробной аналитики по уровню подготовки сотрудников и степени их уязвимости к действиям злоумышленника

ПроБизнес

Провели тестовую фишинговую рассылку

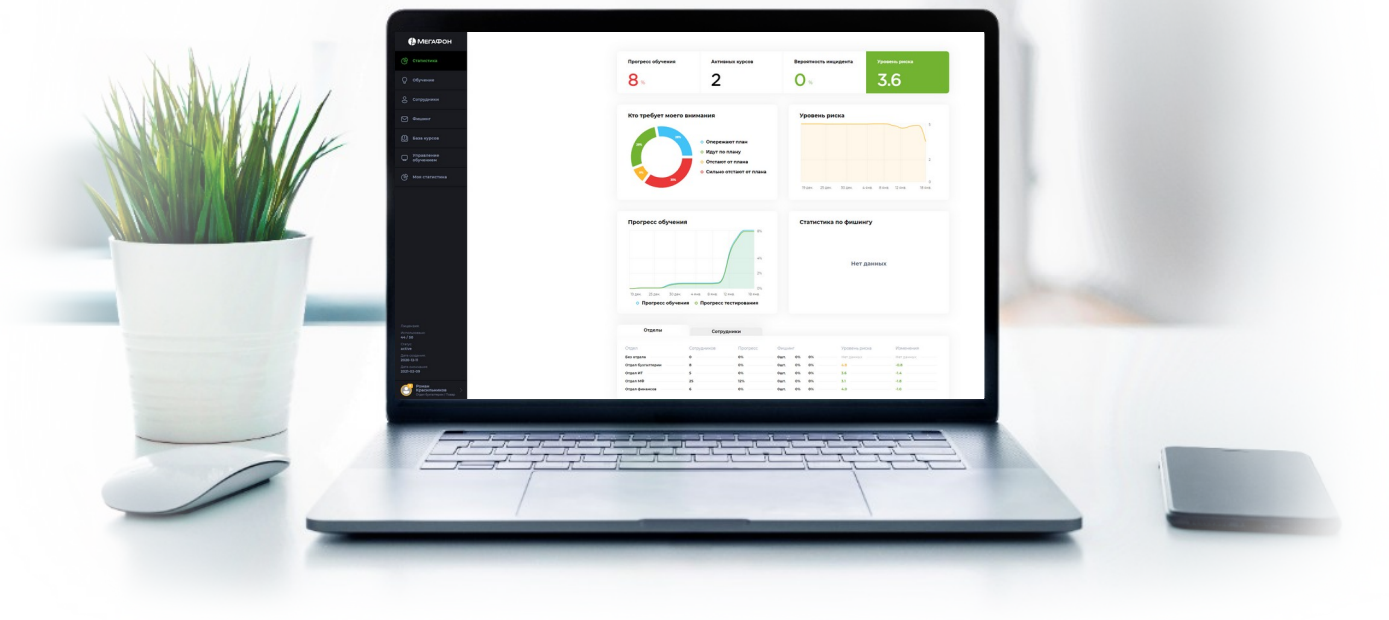


ПроБизнес

Security Awareness от МегаФона: платформа для повышения осведомленности сотрудников

Платформа в лёгкой и понятной форме повышает осведомлённость сотрудников в сфере информационной безопасности и цифровой гигиены.

При помощи имитации фишинговых рассылок у компании есть возможность проверить степень уязвимости сотрудников к действиям злоумышленника.



Теория

- Обучающие курсы
- Имитация фишинга
- Подробная аналитика

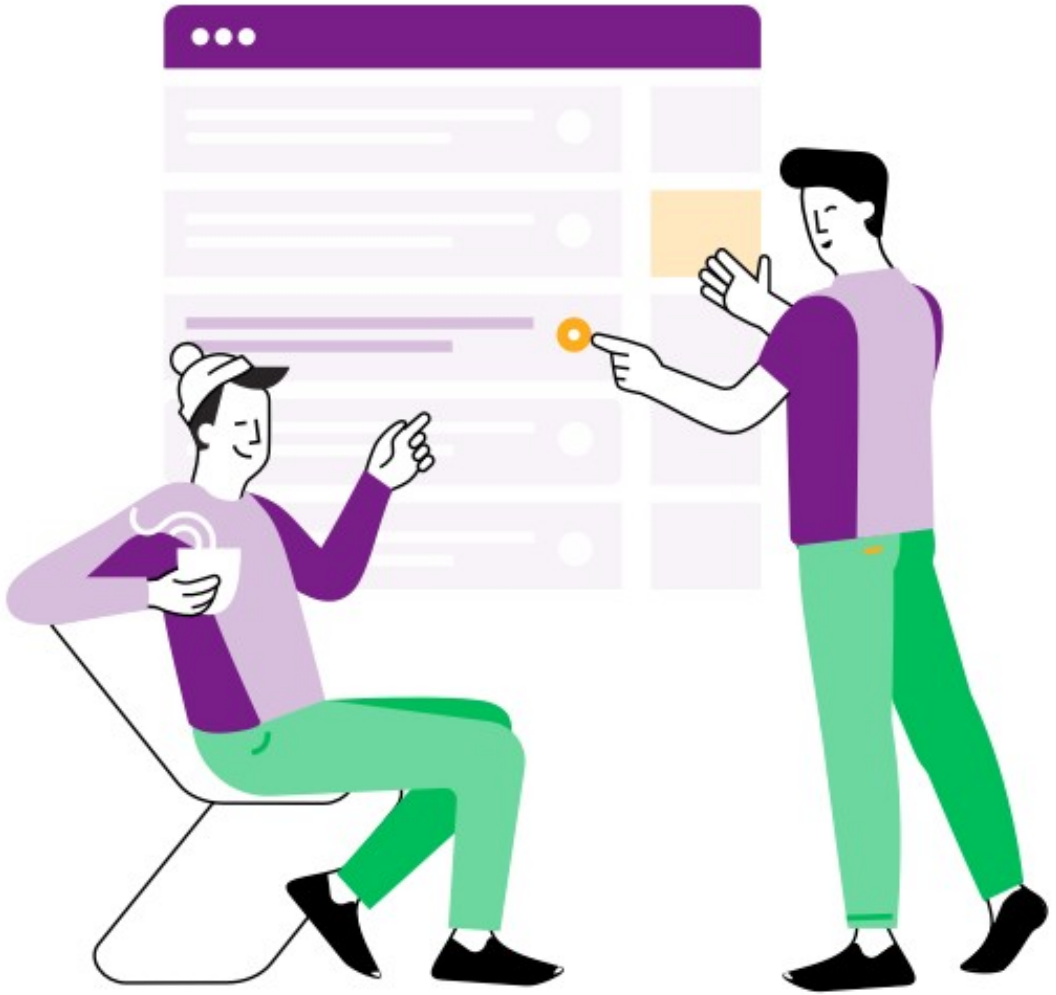
Практика

- Тестовые задания
- Вирусные вложения
- Выявление уязвимых сотрудников

ПроБизнес

Выводы из кейса

- Внедрили логирование на все сетевые события ИТ и ИБ, что помогло оптимизировать работу специалистов Заказчика
- Применяемые ранее средства ИБ не работают в настоящем времени
- Обновление и поддержка от вендора – важная составляющая в любой ИТ инфраструктуре
- Социальный хакинг важный фактор ИБ, который нужно учесть, а также проводить тестовые учебные фишинговые рассылки



ПроБизнес

Предложение от МегаФона

Как понять нужна ли «Security Awareness от МегаФона: платформа для повышения осведомленности сотрудников» в компании?

Предлагаем провести тестовую учебную фишинговую рассылку в вашей компании, до покупки платформы обучения.

ПроБизнес

Технологии включают бизнес

Погоржельский Станислав
Руководитель технической поддержке по облачным и инфраструктурным решениям МегаФона

stanislav.pogorzhels@Megafon.ru

8 800 550 05 55
b2b.megafon.ru

МегаФон | ПроБизнес