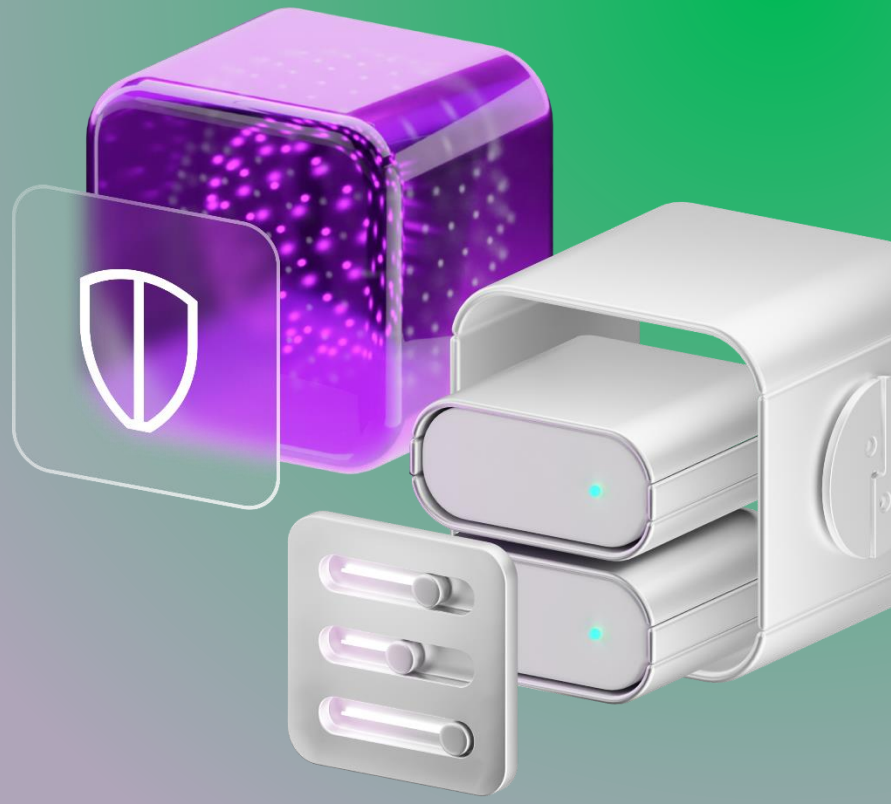
МЕГАФОН | ПроБизнес

Как построить безопасную ИТ-инфраструктуру?



Этап 1. Аудит

Анализ инфраструктуры по явным и возможным уязвимостям с последующим формированием отчета

01 Проверили наличие используемого ПО в периметре организации

02 Изучили версии ПО и наличие требуемого обновления, чтобы учесть актуальные сигнатуры

03 Изучили сетевую топологию

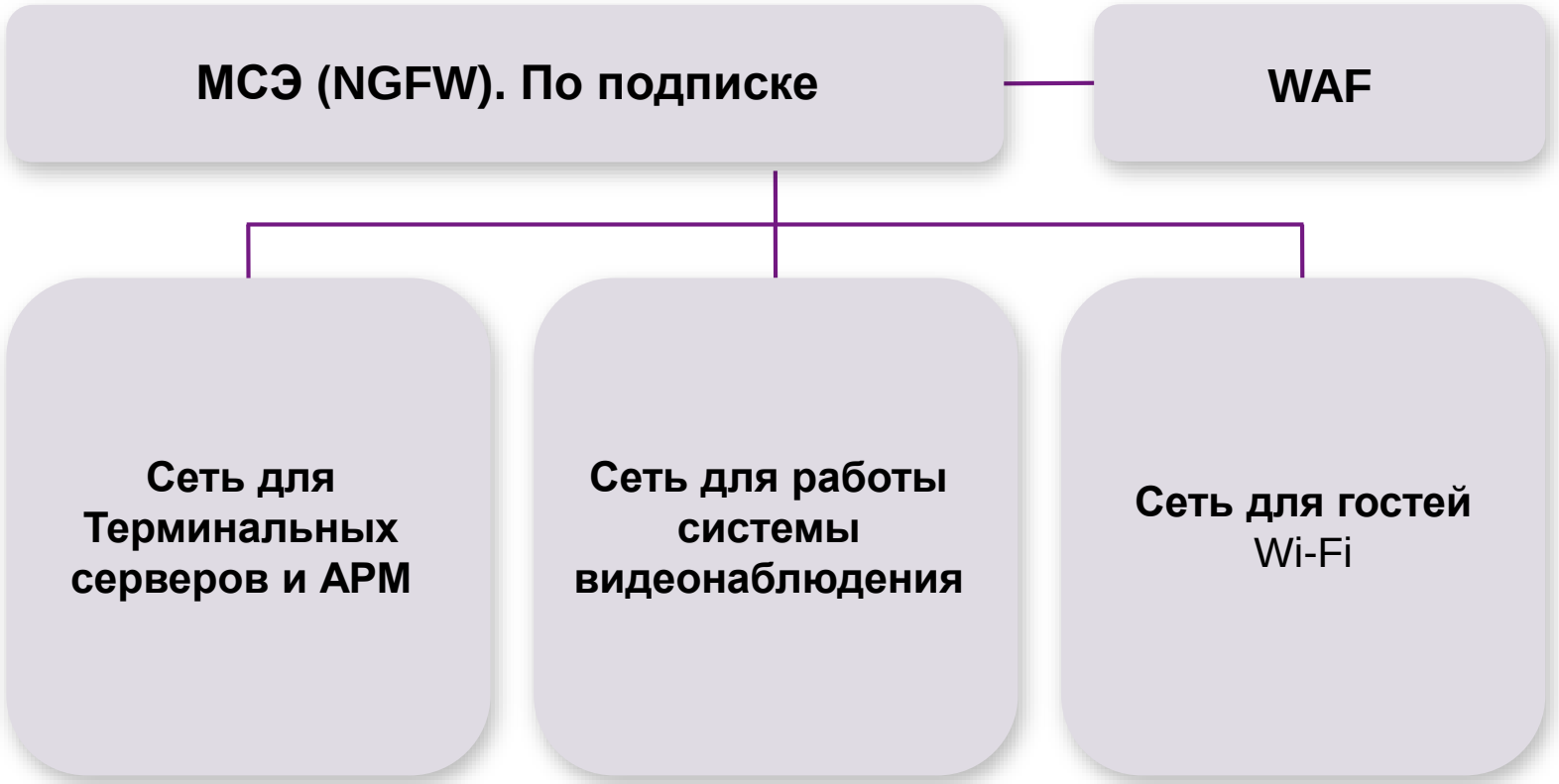
04 Составили основную модель угроз и перечень возможных «нарушителей»

05 Проверили выполнение регламентирующих правил на наличие средств применения и оформления документации

Этап 2. Решение и реализация средств кибербезопасности

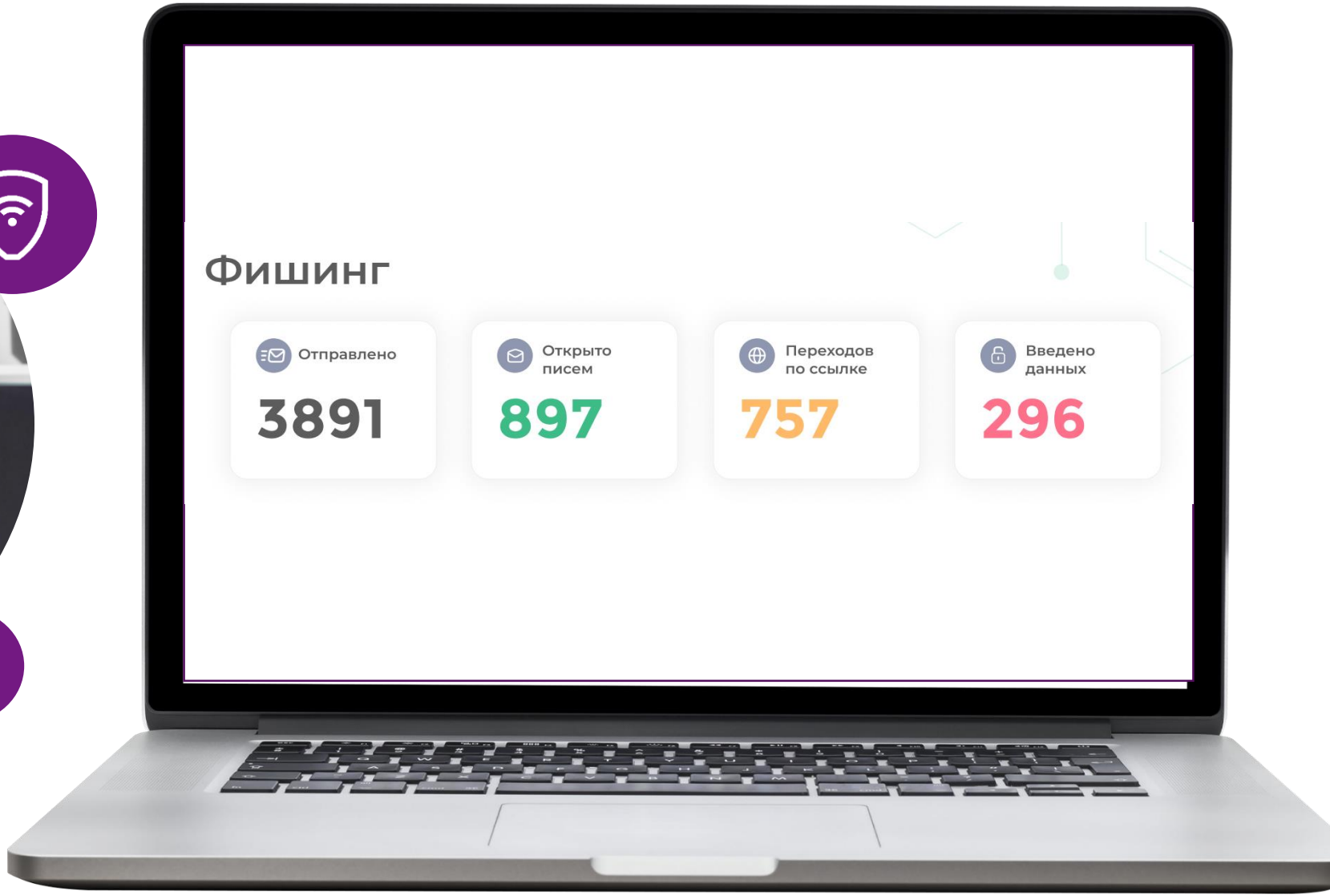
МЕГАФОН | ПроБизнес

Разделили сети заказчика на зоны. Обновили и установили новое ПО



Этап 3. Работа с сотрудниками компании

МЕГАФОН | ПроБизнес



Security Awareness от МегаФона: платформа для повышения осведомленности сотрудников

МЕГАФОН | ПроБизнес

Теория

- Обучающие курсы
- Имитация фишинга
- Подробная аналитика

Практика

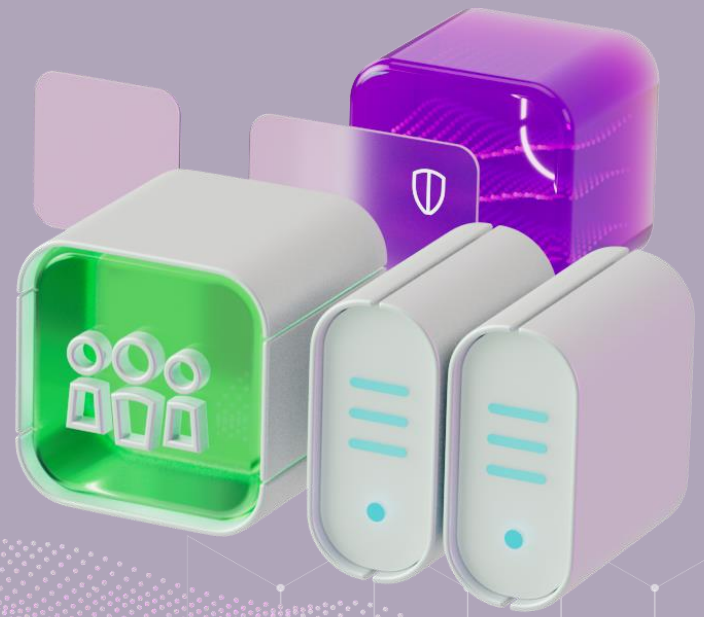
- Тестовые задания
- Вирусные вложения
- Выявление уязвимых сотрудников

Выводы из кейса

- Внедрили логирование на все сетевые события ИТ и ИБ. Это помогло оптимизировать работу специалистов заказчика
- Применяемые ранее средства ИБ не работают в настоящее время
- 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

МегаФон | ПроБизнес

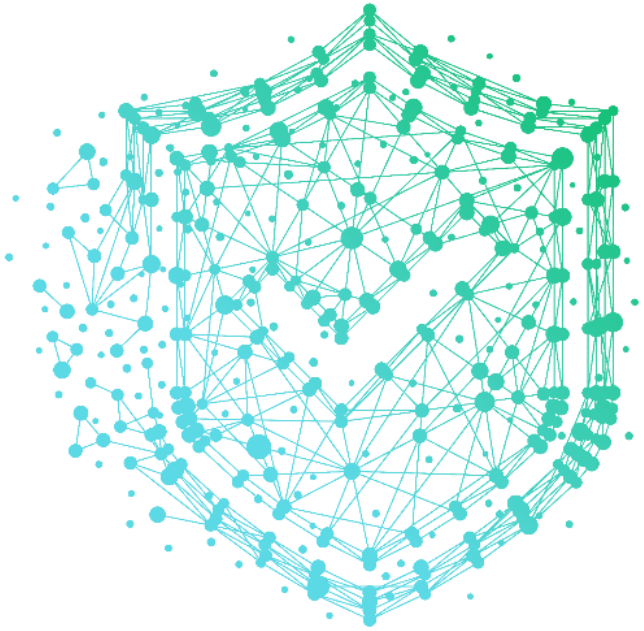
Защита внешнего периметра ИТ инфраструктуры от киберугроз



Инструменты безопасности внешнего периметра

МегаФон | ПроБизнес

- Межсетевые экраны (firewalls)
- Системы предотвращения вторжений (Intrusion Prevention Systems, IPS)
- Системы обнаружения вторжений (Intrusion Detection Systems, IDS)
- Виртуальные частные сети (Virtual Private Networks, VPN)
- DDOS-защита (Distributed Denial of Service protection)
- Системы авторизации и аутентификации
- Системы мониторинга безопасности



МегаФон | ПроБизнес

Как приблизиться к идеальной защите?

Защита внешнего периметра МСЭ

МегаФон | ПроБизнес

Межсетевой экран — контроль и фильтрация проходящего сетевого трафика в соответствии с заданными правилами

Внешний периметр

Межсетевой экран Firewall

Основные функции:

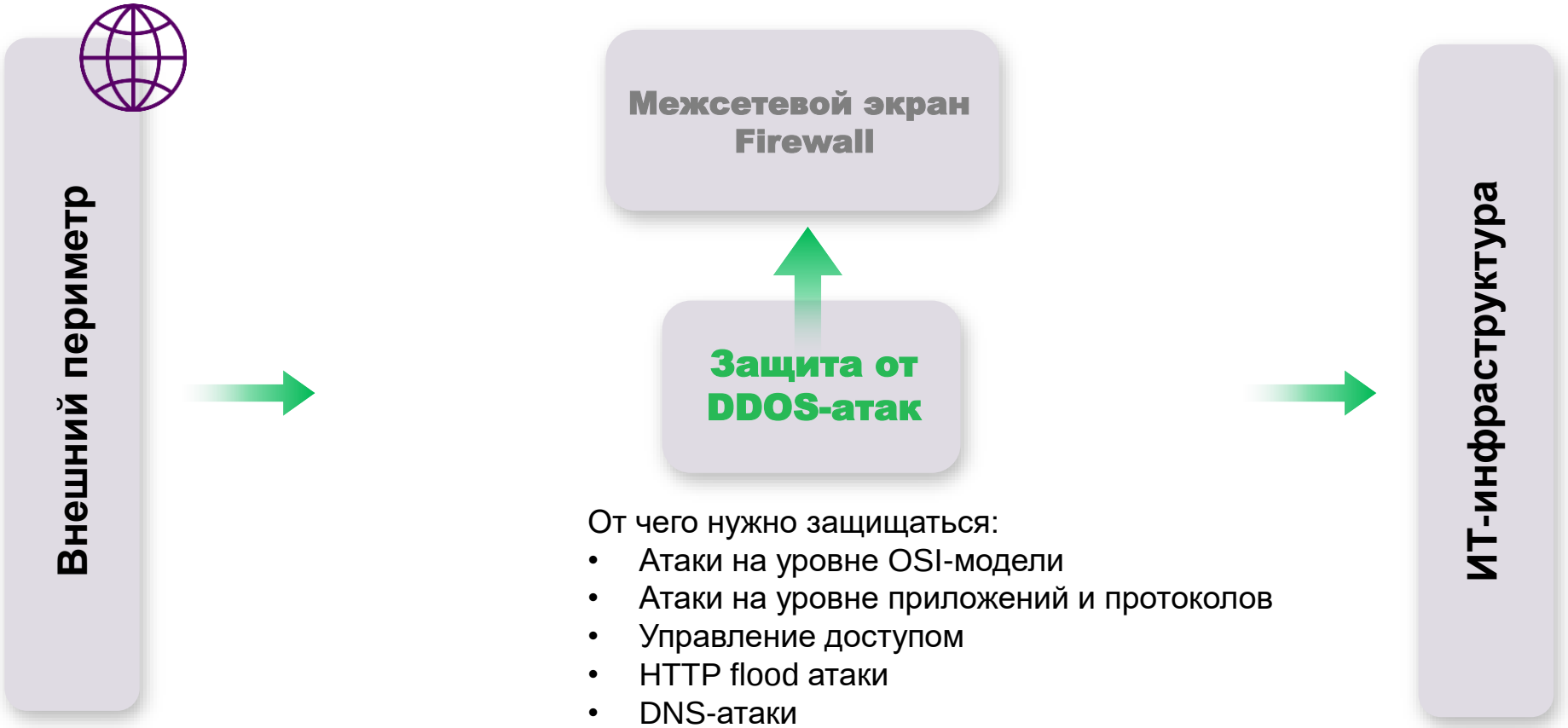
- Фильтрация трафика
- Мониторинг сетевой активности
- Управление доступами
- VPN-шифрование
- Управление портами
- Управление доступа к сайтам

ИТ-инфраструктура

Защита от DDOS-атак

МЕГАФОН | ПроБизнес

DDoS-атака - тип кибератаки, при которой злоумышленник перегружает целевую систему или сеть путем отправки потоков данных с множества источников одновременно. Цель атаки - отказ в обслуживании, что приводит к недоступности ресурса для пользователей.



От чего нужно защищаться:

- Атаки на уровне OSI-модели
- Атаки на уровне приложений и протоколов
- Управление доступом
- HTTP flood атаки
- DNS-атаки
- SNMP-атаки
- Slowloris-атаки
- И т.д

Защита с помощью WAF

МЕГАФОН | ПроБизнес

WAF - совокупность мониторов и фильтров, предназначенных для обнаружения и блокирования сетевых атак на web-приложение

От чего нужно защищаться:

- Атаки на уязвимости веб-приложений
- Атаки на слабые пароли и попытки перебора пароля
- Атаки на управление сессией
- Атаки ZERO DAY и OWASP TOP10
- SQL-инъекции
- XSS-атаки
- CSRF

Защита с помощью NGFW

МЕГАФОН | ПроБизнес

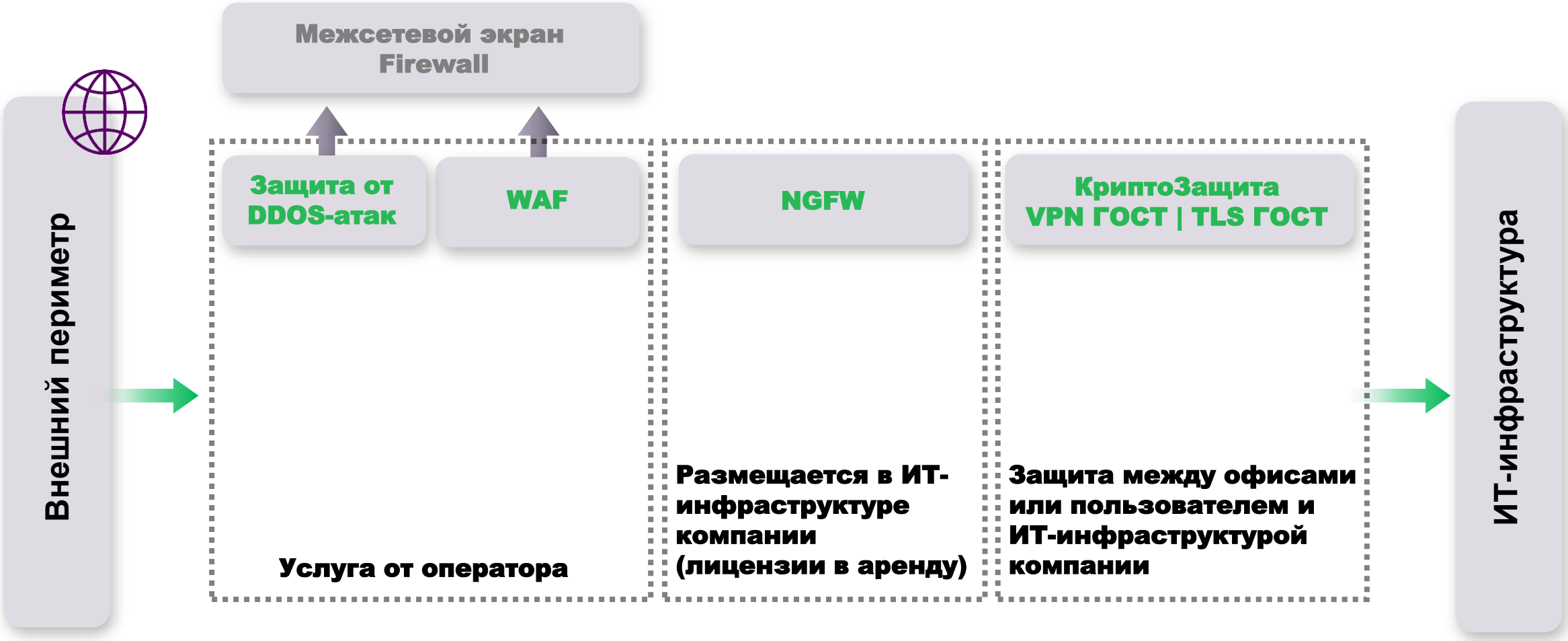
NGFW - межсетевой экран для глубокой фильтрации трафика, интегрированный с IDS (система обнаружения вторжений) или IPS (система предотвращения вторжений) и обладающий возможностью контролировать и блокировать трафик на уровне приложений.

Основные функции NGFW:

- Обеспечивает функционал МСЭ
- Имеется модуль защиты от DDOS-атак
- Может защитить приложения по сигнатурам
- Имеет модуль IPS IDS

Выводы

МегаФон | ПроБизнес



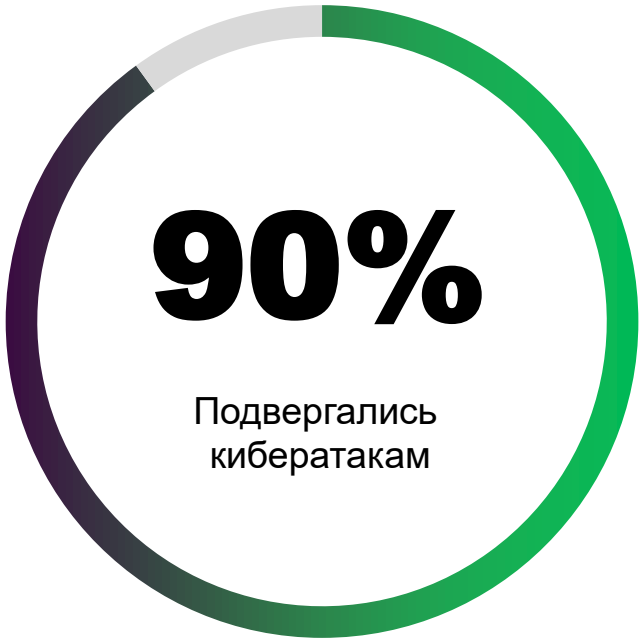
МЕГАФОН | ПроБизнес

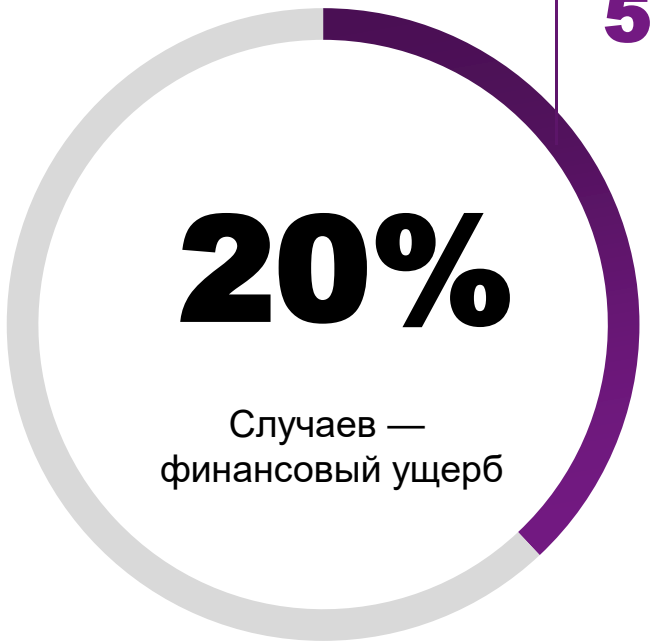
Индекс кибербезопасности

Кибератаки-2021-2023

МЕГАФОН | ПроБизнес

Статистика российского рынка





Из них каждая пятая компания оценила свой ущерб в более чем

5 млн ₽

*По данным исследования МегаФона «Индекс Кибербезопасности»

Оценка ущерба

Оценку ущерба можно грубо провести по следующей формуле, достаточно владеть этими составляющими:

01 Годовая выручка организации, **S**

02 Количество дней простоя для запуска резервной копии и запуск резервных серверов при их наличии или замена на ЗИП, при наличии, **N**

03 Формула:

$$x = \frac{S}{365} * N$$

04 Данные:
Выручка = 1 млрд руб.
Дней простоя = 4 дня

05

$$x = \frac{1\ \text{МЛРД}}{365} * 4 = 10\ 958\ 904\ \text{руб.}$$

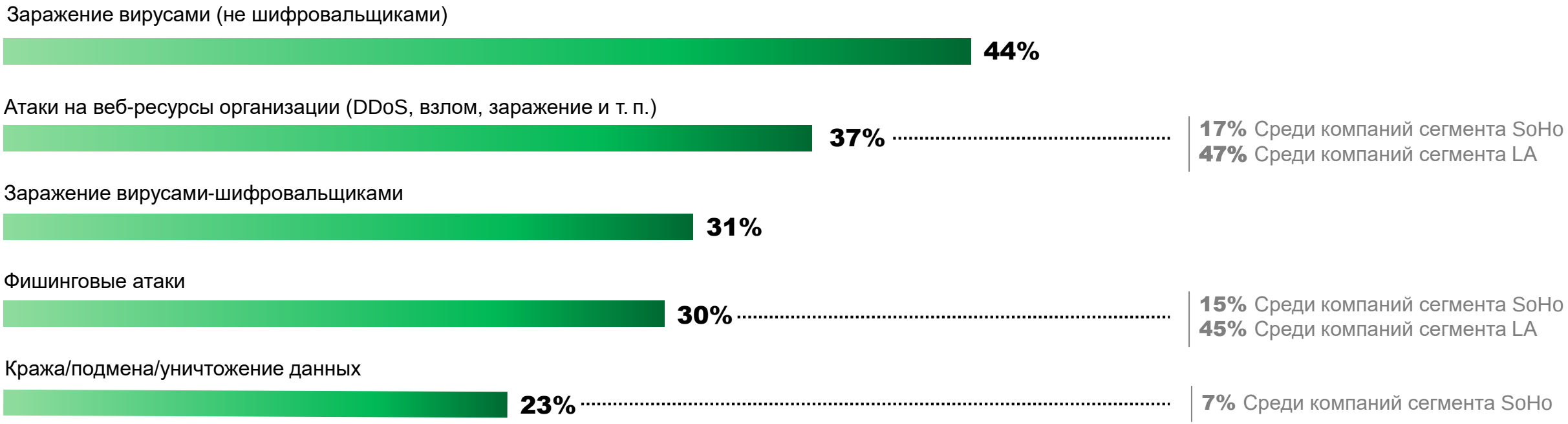
1 день простоя = 2 739 726 руб.

Киберугрозы, с которыми столкнулись компании за год

МегаФон | ПроБизнес

Чаще всего угрозы выражены в заражениях вирусами. В более крупных компаниях с большим количеством инфраструктуры угрозы в целом возникают чаще, особенно часто встречаются атаки на веб-ресурсы (DDoS, взлом, заражение и т. д.).

Угрозы/атаки, с которыми столкнулись за год



*По данным исследования МегаФона «Индекс Кибербезопасности»

Практика от МегаФона

МегаФон | ПроБизнес

1

Реестр операторов, осуществляющих обработку персональных данных

Практика от МегаФона

МегаФон | ПроБизнес

2

Уведомление об использовании файлов Cookies

Практика от МегаФона

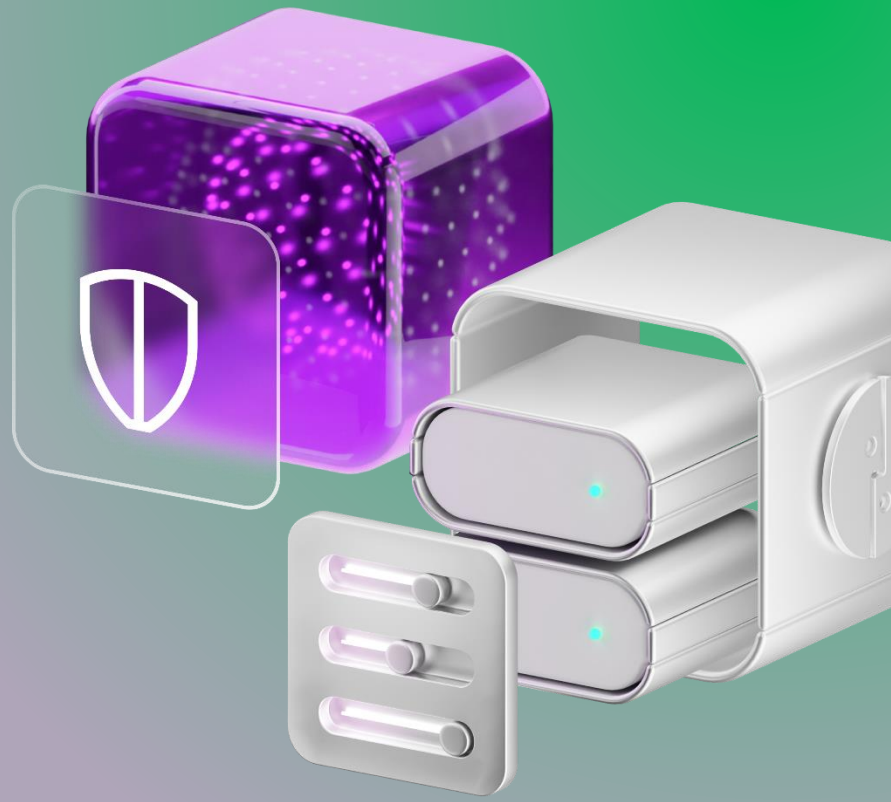
МегаФон | ПроБизнес

3

Список организаций для плановой проверки регистрации как оператора ПНд от РКН на год

МЕГАФОН | ПроБизнес

Целевая модель коммерческого SOC



SOC

МегаФон | ПроБизнес

Security Operation Center — центр мониторинга и реагирования на инциденты информационной безопасности в режиме 24/7

Анализ событий
и инцидентов

Реагирование
на инциденты

Агрегация событий
ИБ из разных источников

Отчетность
и визуализация данных

Команда экспертов 24/7

МегаФон | ПроБизнес

1-я линия

Мониторинг и аналитика событий и инцидентов ИБ — работа по одному готовому сценарию действий: проверка ложноположительных инцидентов ИБ, обогащение инцидента данными, необходимыми для дальнейшего расследования

2-я линия

Техническое реагирование и расследование инцидентов ИБ — работа по нескольким готовым сценариям действий: сдерживание и/или ликвидация последствий инцидента ИБ, выявление первопричины инцидента (например, поиск злоумышленника)

3-я линия

Работа без готовых сценариев действий. Кроме участия в аналитике, реагировании и расследовании, эта линия занимается внедрением (подключением) новых заказчиков к SOC, а также разработкой новых сценариев, правил корреляции, «парсеров» и «коннекторов»

Методолог

Оформление разработанных сценариев в унифицированный вид для дальнейшего использования линиями при помощи инструментов платформы SOAR — Security Orchestration, Automation and Response (в SOC возможны тысячи сценариев)

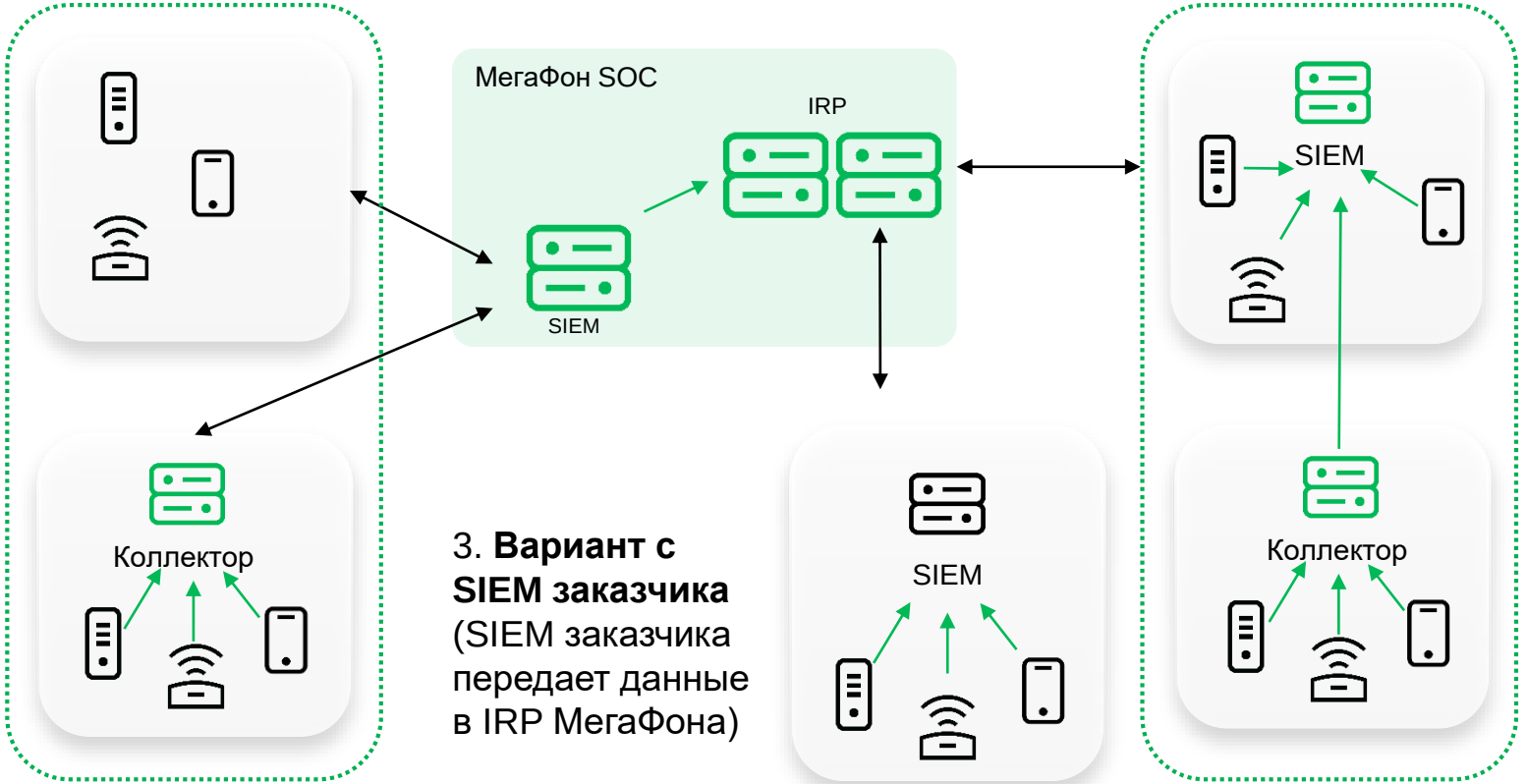
Сервис-менеджер

Менеджер, ответственный за проект на этапе эксплуатации

Варианты реализации на примере МегаФон SOC

МегаФон | ПроБизнес

1. **Облачный вариант** (передача данных от устройств напрямую в облако МегаФона или через коллектор)



3. **Вариант с SIEM заказчика** (SIEM заказчика передает данные в IRP МегаФона)

2. **Вариант в инфраструктуре заказчика** (SIEM МегаФона в инфраструктуре заказчика передает данные в IRP МегаФона)

4. **Сложный гибридный вариант**

МЕГАФОН | ПроБизнес

Технологии включают бизнес

к.т.н. Кокшаров Дмитрий

Менеджер по внедрению цифровых систем