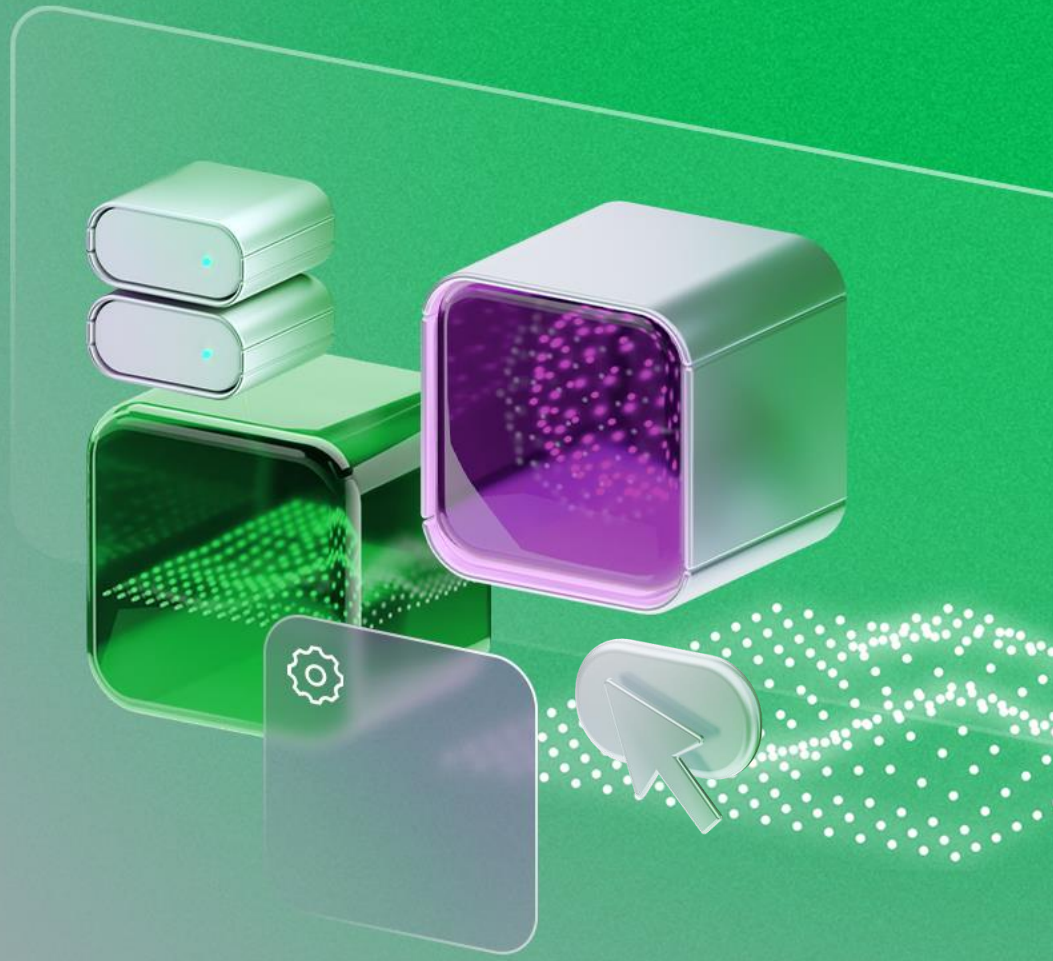
МЕГАФОН | ПроБизнес

МЕГАФОН — НАДЕЖНЫЙ ПАРТНЕР ДЛЯ ВАШЕГО БИЗНЕСА



Причины роста внешних и внутренних угроз

Автоматизация криминального бизнеса

Технологии искусственного интеллекта

Партнерские программы

Доступность мошеннических технологий
Атаки по подписке

Жажда легкого заработка инсайдеры

Рост конкуренции

Рост интереса к направлению ИТ и ИБ молодого поколения

Указ 250 Президента РФ от 1 мая 2022 года

- Обнаруживать инциденты
- Предупреждать об инциденте
- Ликвидировать последствия компьютерных атак
- Реагировать на компьютерные инциденты
- Создать специальные структурные подразделения ИБ или возложить обязанности на существующие

ФСТЭК. Итоги конференции

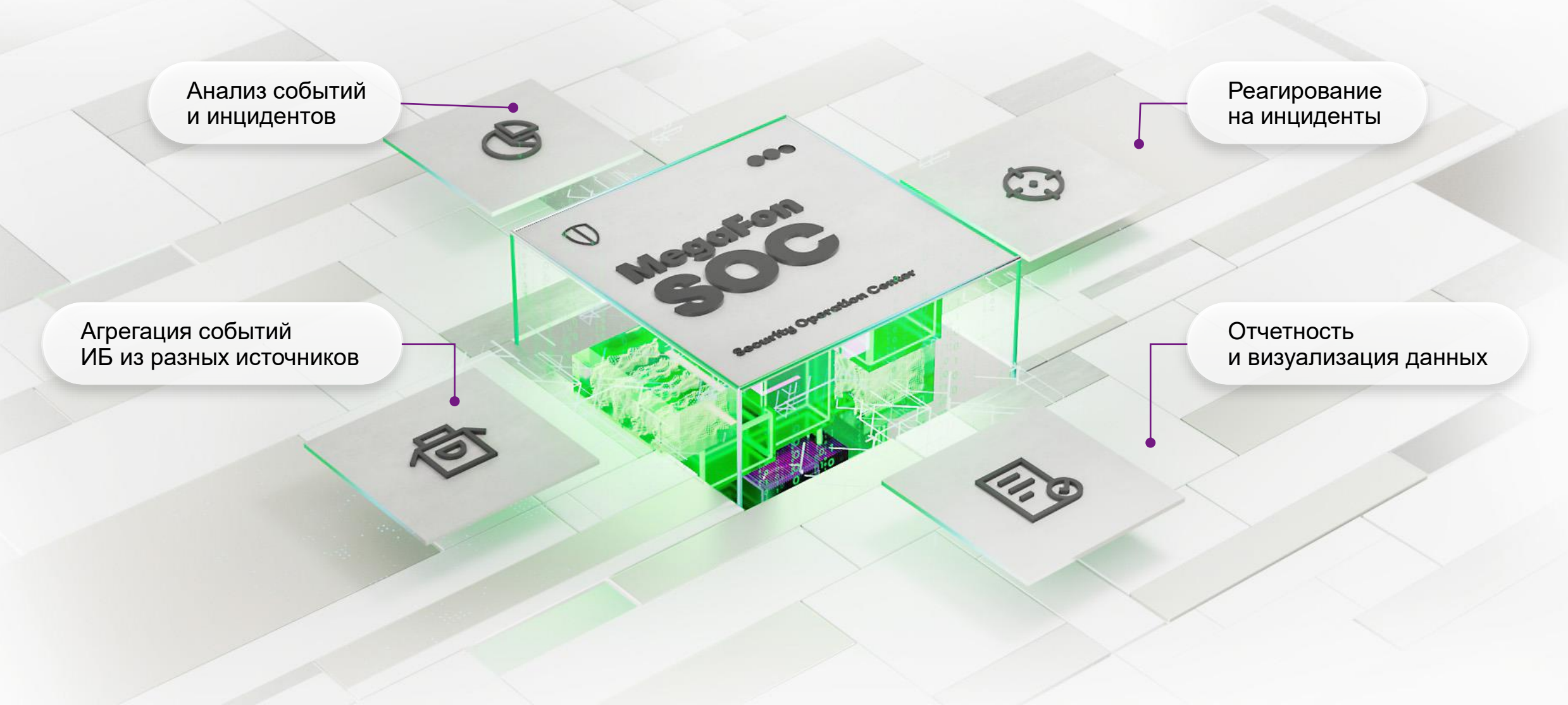
- Слабые пароли пользователей, администраторов
- Использование паролей, установленных по умолчанию
- Однофакторная идентификация
- Уязвимости ПО, используемого на объектах КИИ
- Активные учетные записи уволенных сотрудников
- Использование для доступа к информационной инфраструктуре личных устройств работников
- Использование на РМ личных мессенджеров, социальных сетей.

МЕГАФОН | ПроБизнес

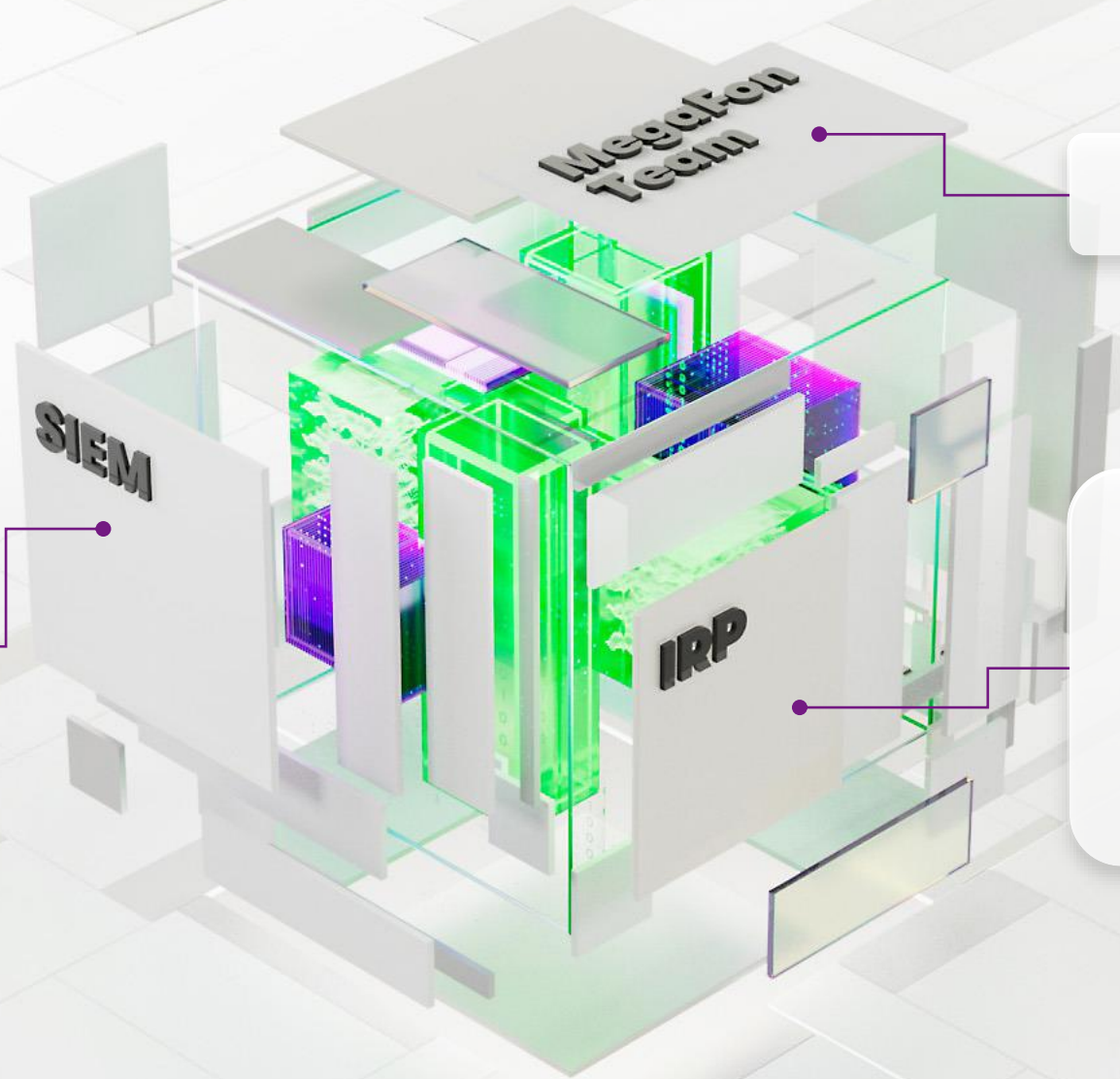
Сервисы информационной безопасности

SOC

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



Из чего состоит SOC



Команда экспертов

SIEM

Security Information and Event Management

Платформа для сбора и анализа информации о событиях ИБ

IRP

Incident Response Platform

Платформа для автоматизации реагирования на киберинциденты

МегаФон

Наши партнеры

SIEM

IRP

positive technologies

kaspersky

Security Vision

SIEM МегаФона

Security Information and Event Management

— Более 150 настроенных источников событий (сетевое оборудование, серверные и пользовательские ОС, средства защиты информации, специализированное ПО)

— Более 20 типов транспортных протоколов передачи событий

— Возможность построения распределенных по филиалам систем сбора событий с учетом баланса нагрузки на сеть и с использованием коннекторов (сборщиков событий с элементов инфраструктуры)

— Подключение нетиповых источников

— Возможность отправки предупреждений на основе предопределенных настроек

— Возможность просмотра данных на разных уровнях детализации

IRP МегаФона

Incident Response Platform

— Автоматизирует ряд рутинных операций по сбору дополнительной информации

— Осуществляет неотложные действия по сдерживанию и устранению угрозы

— Восстанавливает атакованную систему

— Оповещает заинтересованных лиц

— Собирает и структурирует данные о расследованных инцидентах информационной безопасности

— Позволяет роботизировать и автоматизировать действия оператора-специалиста ИБ, которые он производит при реагировании на инциденты информационной безопасности

Команда экспертов 24/7

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

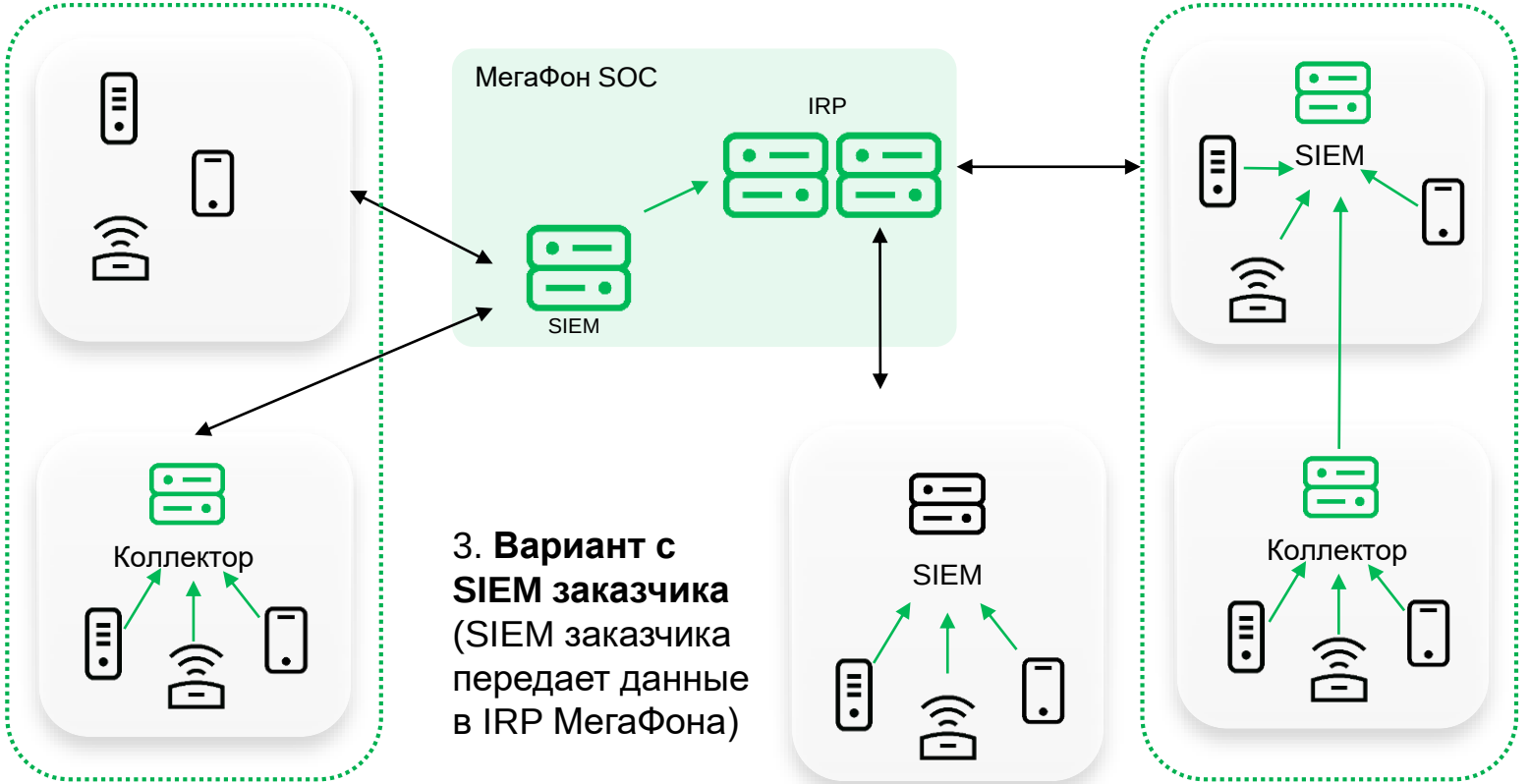
Оформление разработанных сценариев в унифицированный вид для дальнейшего использования линиями при помощи инструментов платформы SOAR — Security Orchestration, Automation and Response (в SOC возможны тысячи сценариев)

Сервис-менеджер

Менеджер, ответственный за проект на этапе эксплуатации

Варианты реализации МегаФон SOC

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



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

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

4. **Сложный гибридный вариант**

Дополнительные услуги

Взаимодействие
с ГосСОПКА

Техническое реагирование
на инцидент

Адаптация СЗИ к
выявленным угрозам

Поиск уязвимостей
в ИТ-инфраструктуре

Предоставление
СЗИ по подписке

Разработка внутренней
документации
и процессов по ИБ

Форензика / Кибер-
криминалистика

Раскрытие
киберпреступлений

Кибербразведка

Поиск и анализ
потенциальных угроз

Консалтинг ИБ

Аудит, пентесты,
разработка документации
и прочее

МегаФон | ПроБизнес

Анализ защищенности IT-инфраструктуры

Поможем оценить реальный уровень защищенности ваших информационных систем и соблюсти требования регуляторов

Security Assessment

- Анализ защищенности
- Red Teaming
- AS IS – TO BE
- Аудит и построение процессов SSDLS
- Тестирование на проникновение
- Реагирование на инциденты
- Социотехническое тестирование

Compliance

- Безопасность КИИ
- Защита персональных данных
- Защита ГИС

МегаФон | ПроБизнес

Анализ защищенности

Выявление максимального количества уязвимостей в инфраструктуре

Цели

- Наиболее широко оценить общий уровень защищенности ИТ-инфраструктуры или системы с целью разработки мер по его повышению
- Найти максимальное количество уязвимостей в инфраструктуре, при этом продвижение в глубину не производится
- Проверить соответствие стандартам безопасности, требующих регулярной проверки защищенности

Результат

- Отчет с описанием найденных уязвимостей, их влияния на бизнес-процессы и оценкой общего уровня защищенности
- Подробные рекомендации по устранению найденных уязвимостей и повышению уровня защищенности инфраструктуры

Объекты тестирования

Внешний периметр | Внутренний периметр | Мобильные приложения | Сети Wi-Fi | Сотрудники | Бизнес приложения (ERP, CRM) | ДБО

МегаФон | ПроБизнес

Тестирование на проникновение

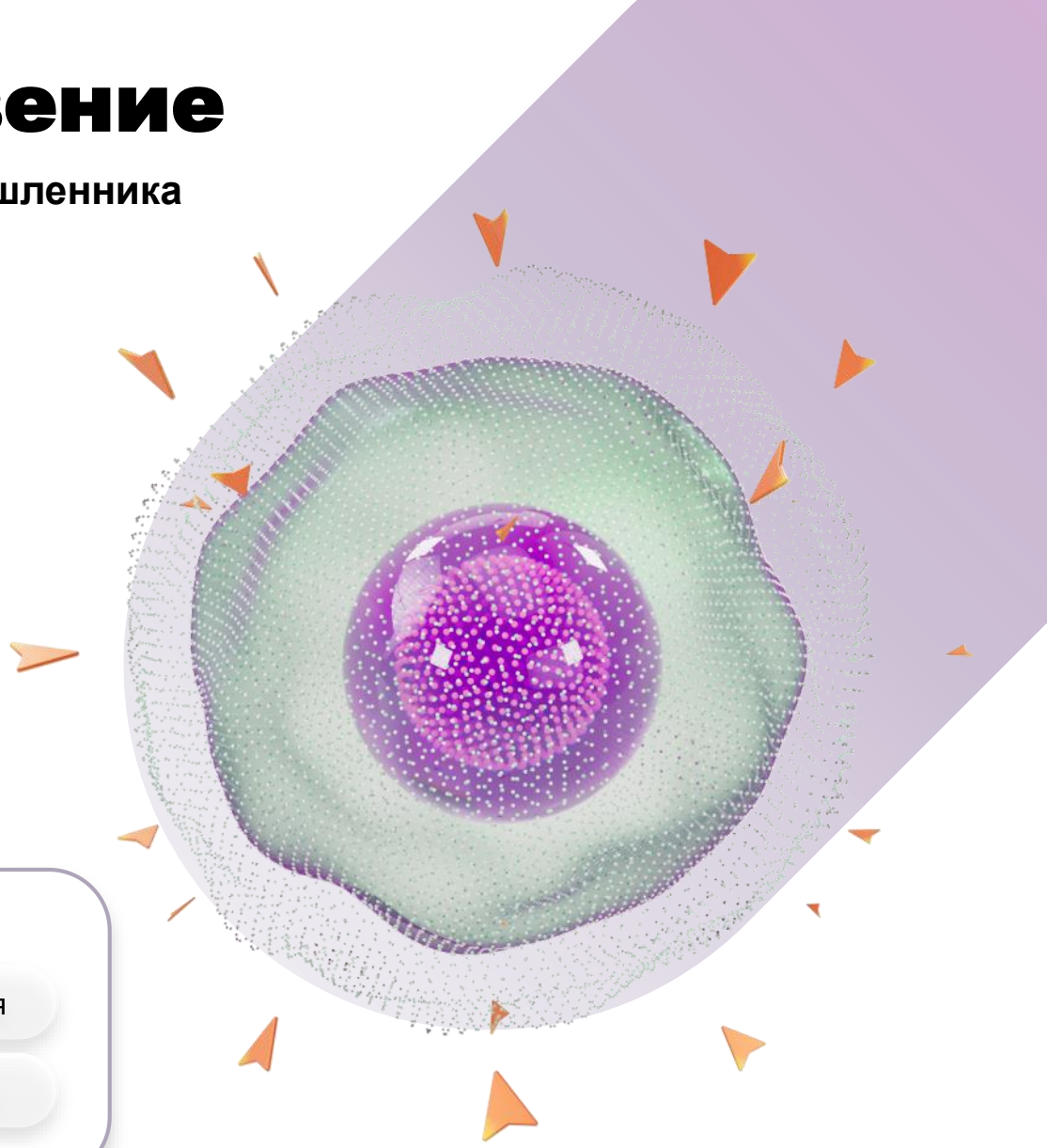
Поиск критических уязвимостей и оценка возможности злоумышленника продвижения в глубь инфраструктуры

Цели

- Определить, может ли текущий уровень защищенности выдержать попытку вторжения потенциального злоумышленника
- Выявить критичные уязвимости в инфраструктуре и определить, насколько «глубоко» злоумышленник может проникнуть в системы
- Проверить соответствие стандартам безопасности, требующих регулярного анализа защищенности

Результат

- Демонстрация возможности фактического проникновения и получения контроля над системой или получения доступа к критической информации
- Отчет с описанием выявленных уязвимостей, причастных к векторам атак и рекомендациями по повышению уровня защищенности



Объекты тестирования

Внешний периметр | Внутренний периметр | Мобильные приложения | Сети Wi-Fi | Сотрудники | Бизнес приложения (ERP, CRM) | ДБО

МегаФон | ПроБизнес

Red Teaming

Имитация реальных кибератак с целью тренировки и оценки эффективности людей, процессов и технологий защиты

Цели

- Незаметно проникнуть в систему, закрепиться в ней и получить доступ к ИТ-инфраструктуре
- Проверить не только работу технической защиты, но и работу службы безопасности, оценить скорость и эффективность реагирования на различные виды угроз

Результат

- Оценка действий службы информационной безопасности и рекомендации по улучшению ИБ компании
- Детальный отчет с результатами тестирования и информацией, собранной в результате проверки
- Список выявленных уязвимостей и недостатков системы безопасности компании
- Перечень отработанных сценариев атаки с подробным описанием

Объекты тестирования

Вся ИТ-инфраструктура компании

МегаФон | ПроБизнес

Аудит безопасности инфраструктуры

Комплексный аудит ИТ/ИБ-инфраструктуры (As Is) и разработкой целевого состояния (To Be)

Цели

Целью аудита является определение текущего уровня зрелости ИТ/ИБ-инфраструктуры с дальнейшим формированием перечня инициатив по трансформации ИТ/ИБ заказчика

Результат

- Отчет о текущем состоянии
- Отчет о целевом состоянии
- Презентация: ключевые результаты, дорожные карты построения ИТ/ИБ, перечни и паспорта инициатив

Этапы проекта

Этап 1	Структура бизнес-процессов заказчика	Анализ документации заказчика, регламентирующей ИБ и ИТ	Анализ ИТ-инфраструктуры	Анализ ИБ-инфраструктуры	Отчет о текущем состоянии
Этап 2	Рекомендации по формированию организационных мер обеспечения ИБ/ИТ	Рекомендации по реализации технических мер обеспечения ИБ/ИТ	Разработка дорожкой карты построения целевого состояния	Оценка бюджета на реализацию инициатив	Отчет о целевом состоянии и результирующая презентация

Безопасность КИИ

Полный комплекс услуг по обеспечению безопасности объектов КИИ

Этапы проведения

1. Первичный сбор данных — результатом является вывод о необходимости выполнения организацией требований 187-ФЗ
2. Проведение категорирования: создание комиссии, определение объектов категорирования, определение категорий значимости
3. Согласование сведений и присвоенных категорий с регулятором
4. Проектировка системы защиты ЗОКИИ
5. Внедрение организационных и технических мер
6. При необходимости — проведение аттестации
7. Построение непрерывного и циклического процесса

Предпосылки

- Очень большое внимание со стороны регуляторов
- Требования предоставить отчет о проведенных в отношении защиты КИИ мероприятий
- Штрафы и уголовная ответственность

Сферы детальности

- **Здравоохранение**
- **Наука**
- **Связь**
- **Финансы**
- **Транспорт**
- **Энергетика**
- **Промышленность:** атомная, оборонная, химическая, металлургическая, горнодобывающая, ракетно-космическая, топливно-энергетическая

Защита персональных данных

Законодательная база

ФЗ-152 с поправками от 1.09.2022, ПП-1119, Приказ ФСТЭК России №21

Краткий обзор состава работ

1. Аудит (с отчетом или без)
2. Акт классификации, модель угроз и нарушителя
3. Техническое задание на систему защиты, технический проект на систему защиты
4. Организационно-распорядительная документация по приказу ФСТЭК России №21
5. Юридическая документация
6. Оценка соответствия
7. Помощь в уведомлении РКН

Кому это нужно, кому обязательно

1. Любая организация малого, среднего и крупного бизнеса независимо от отрасли, на сайте которой есть форма заявки или обратной связи, личный кабинет или система сбора статистики о посещаемости сайта и т.д.
2. Государственные учреждения, особенно работающие с населением
3. Компании, исполняющие требования контрагентов

Риски, последствия утечек

1. Репутационный ущерб и проверки
2. Приостановка работы и штрафы

МегаФон | ПроБизнес

Аттестация ГИС

Защита государственных информационных Систем

Законодательная база

Приказ ФСТЭК России №17, Постановление правительства №676

Краткий обзор состава работ

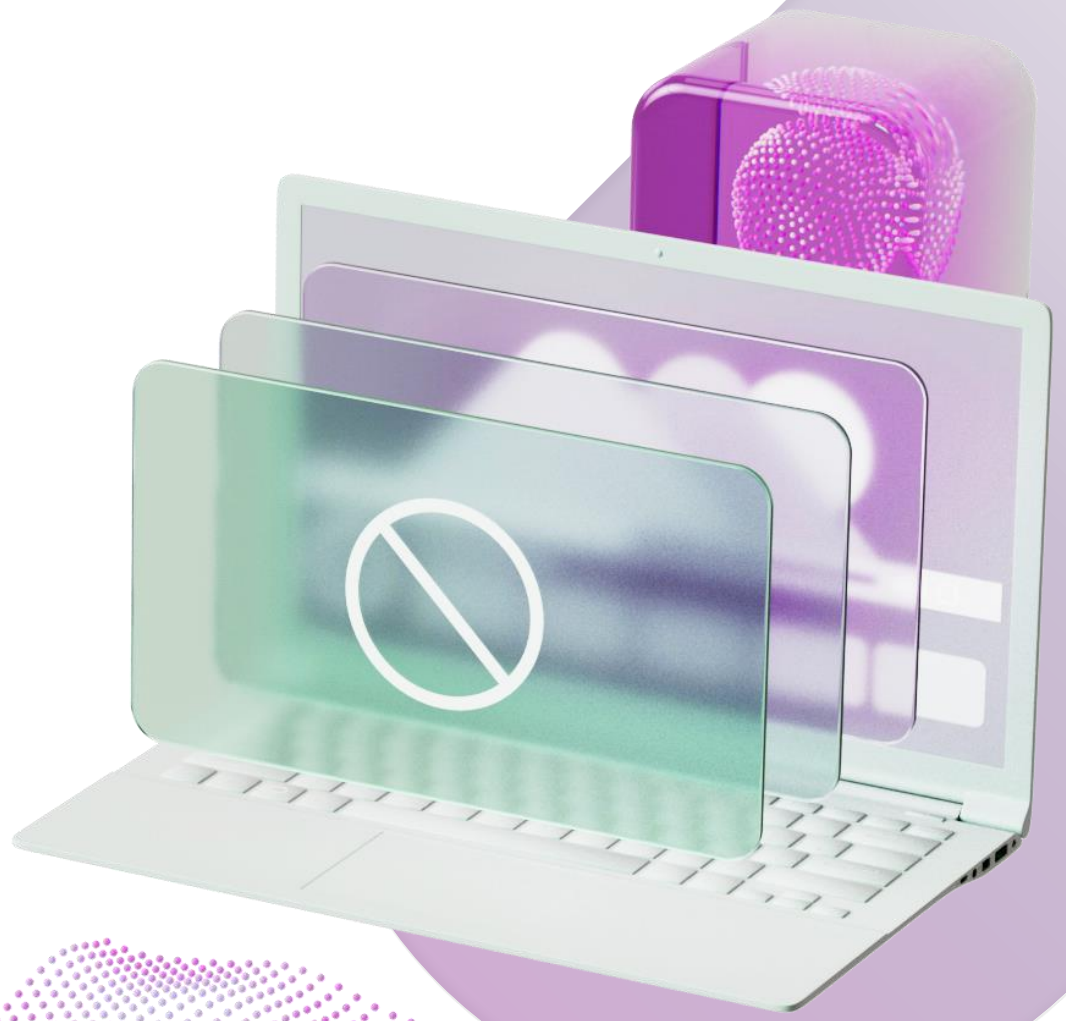
1. Обследование (без отчета)
2. Модель угроз, акт классификации
3. Техническое задание, тех-проект, ОРД
4. Анализ защищенности
5. Аттестационные испытания

Кому это нужно, кому обязательно

Любая ГИС должна быть аттестована

Риски, последствия

1. Приостановка работы ГИС
2. Любые санкции на усмотрение регулятора



МегаФон | ПроБизнес

МегаФон DLP

Система отслеживания документов и предотвращения утечек конфиденциальных данных через электронную почту, файловые хранилища, USB-устройства и любые другие сервисы и приложения.

- Управление политиками доступа и анализ их эффективности
- Контроль основных каналов коммуникаций, подключаемых устройств и VoIP-телефонии
- Полный мониторинг и анализ деятельности и рабочего времени сотрудников
- Выявление злоумышленников и нелояльных сотрудников
- Ведение архива всех бизнес-коммуникаций
- Инструментарий для расследования инцидентов безопасности и предиктивный анализ

МегаФон | ПроБизнес

Защита баз данных

Комплексная система защиты баз данных
от копирования, изменения и удаления информации.
Блокировка несанкционированных действий пользователей.

- Аудит операций с БД в режиме реального времени
- Соответствие стандартам ЦБ РФ (СТО БР ИСС) и PCI DSS
- Контроль действий администраторов
- Полностью российское решение, сертифицированное ФСТЭК
- Предотвращение попыток внешнего вторжения в СУБД
- Соответствие закону о персональных данных ФЗ-152

МегаФон | ПроБизнес

Защита от DDoS-атак

Эффективная защита от сетевых атак, направленных на отказ веб-ресурса, инфраструктуры.
Защитит бизнес от финансовых и репутационных потерь.

- Решение сертифицировано ФСТЭК России и входит в реестр отечественного ПО
- Противодействие атакам ёмкостью до 300 Гбит/с
- Защита от всех современных типов атак на сетевом уровне и на уровне веб-приложений
- Время реакции на атаку от 5 сек.
- Выделенная служба мониторинга и реагирования 24/7/365

Защита ресурса на канале любого провайдера

Срок подключения от 1 часа
(в том числе под атакой)

МегаФон | ПроБизнес

Криптозащита

Услуга гарантированно защищает вашу информацию при ее передаче по открытым каналам связи. Ни оператор связи, ни производитель оборудования, ни злоумышленники — никто не имеет доступа к защищаемым данным

Услуга «Криптозащита» построена на базе решений российских производителей криптооборудования

Криптошлюзы используют только российские криптоалгоритмы (ГОСТ 28147-89, ГОСТ 34.10/34.11-2012, ГОСТ 34.12/34.13-2015)

Можно создать VPN «с нуля» либо организовать систему шифрования в уже существующей VPN

Экономия на капитальных затратах на закупку оборудования и персонале для обслуживания

Возможности решения:

– Выбор вендера из ТОР 3 российских лидеров криптооборудования

– Платформа сертифицирована ФСБ России

– Снижение капитальных затрат при выборе сервисной модели

– Возможность создания отказоустойчивого кластера

Security Awareness

Платформа по повышению осведомленности сотрудников в сфере информационной безопасности с понятным запоминающимся контентом и возможностью проверить знания при помощи имитированных фишинговых атак.

- Обучающие курсы
- Тестовые задания
- Выявление уязвимых сотрудников
- Имитация фишинга
- Подробная аналитика
- СДО (Система дистанционного обучения)
- Контроль процесса прохождения курсов
- Адаптация под ваши требования
- Решение включено в реестр ПО

МегаФон | ПроБизнес

МегаФон WAF

Надежная защита веб-приложений от взломов, утечек данных и сбоев в работе

- Реализован на базе отечественного программного обеспечения
- Обнаруживает и блокирует атаки нулевого дня и атаки, использующие известные уязвимости веб-приложений
- Работает в автоматическом режиме
- Устойчив к распространенным методикам обхода механизмов защиты WAF

WAF защищает приложение от атак злоумышленников:
- Веб-атак
- Бот-атак
- Атак на API
- “Умных” DDOS атак на приложения

Реализован в двух вариантах:

Software-as-a-Service

Услуга, предоставляемая из облака

On-Premises

Программное обеспечение, установленное в сетевой инфраструктуре клиента

МегаФон NGFW

Комплексная услуга по защите информационных ресурсов клиента от сетевых атак и вирусов, фильтрация доступа его сотрудников в Интернет

- Реализован на базе отечественного программного обеспечения
- Позволяет интегрировать разрозненные функции сетевой защиты
- Создает единую точку выхода в Интернет и применяет единые политики безопасности
- Снижает расходы на администрирование и закупку оборудования и программного обеспечения

NGFW защищает сетевую инфраструктуру от атак злоумышленников :
- Веб-атак
- Почтового спама
- Вирусов
- DDOS-атак на сетевую инфраструктуру

а так же осуществляет фильтрацию интернет-запросов пользователей

Предоставляется в двух вариантах:

В облаке МегаФона (SaaS)

В сетевой инфраструктуре клиента (On-Premises)

МЕГАФОН | ПроБизнес

Технологии включают бизнес