МегаФон SOC

Сервис по выявлению кибератак в режиме реального времени

МегаФон | ПроБизнес

«Если задачей обеспечения безопасности является защита от уже совершенных атак, то значит мы с ней хорошо справляемся.»

Брюс Шнайдер

ПроБизнес

Брюс Шна́йер — американский криптограф, писатель и специалист по компьютерной безопасности. Автор нескольких книг по безопасности, криптографии и информационной безопасности.

Тренд на кибербезопасность

Спрос определяется двумя драйверами: нехваткой оборудования и человеческих ресурсов для быстрой адаптации к новым условиям

Исследование МегаФона

Кибербезопасность перестала быть вопросом только лишь соответствия требованиям регуляторов. Теперь информационная безопасность — одно из основных средств достижения бизнес-целей.

25%
Государственные учреждения

72%
Новых клиентов представляют коммерческие организации

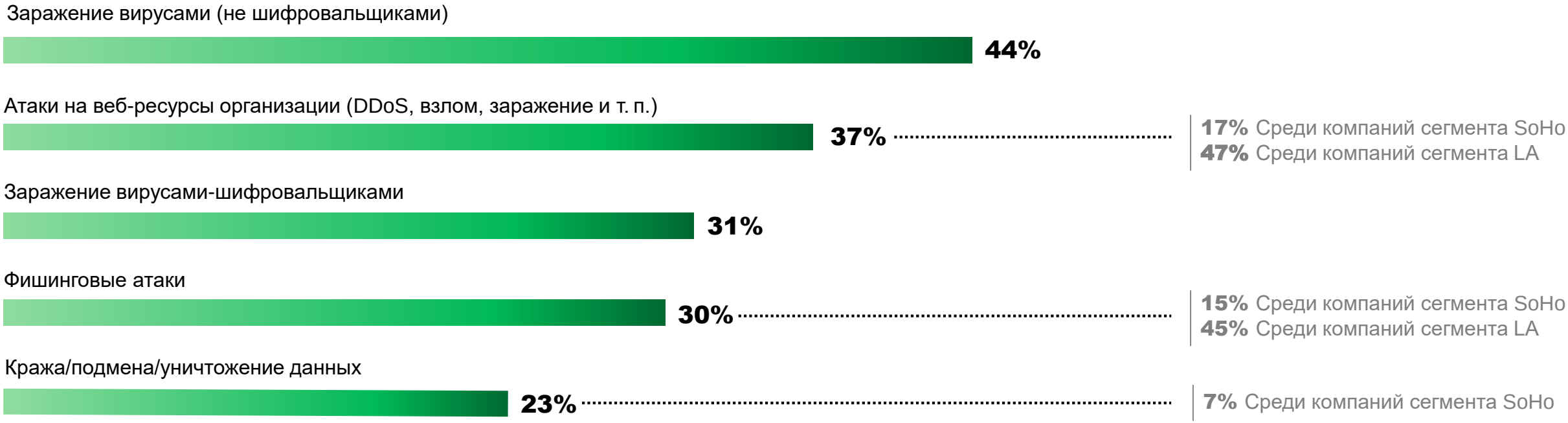
3%
СМИ

ПроБизнес

Киберугрозы, с которыми столкнулись компании за год

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.).

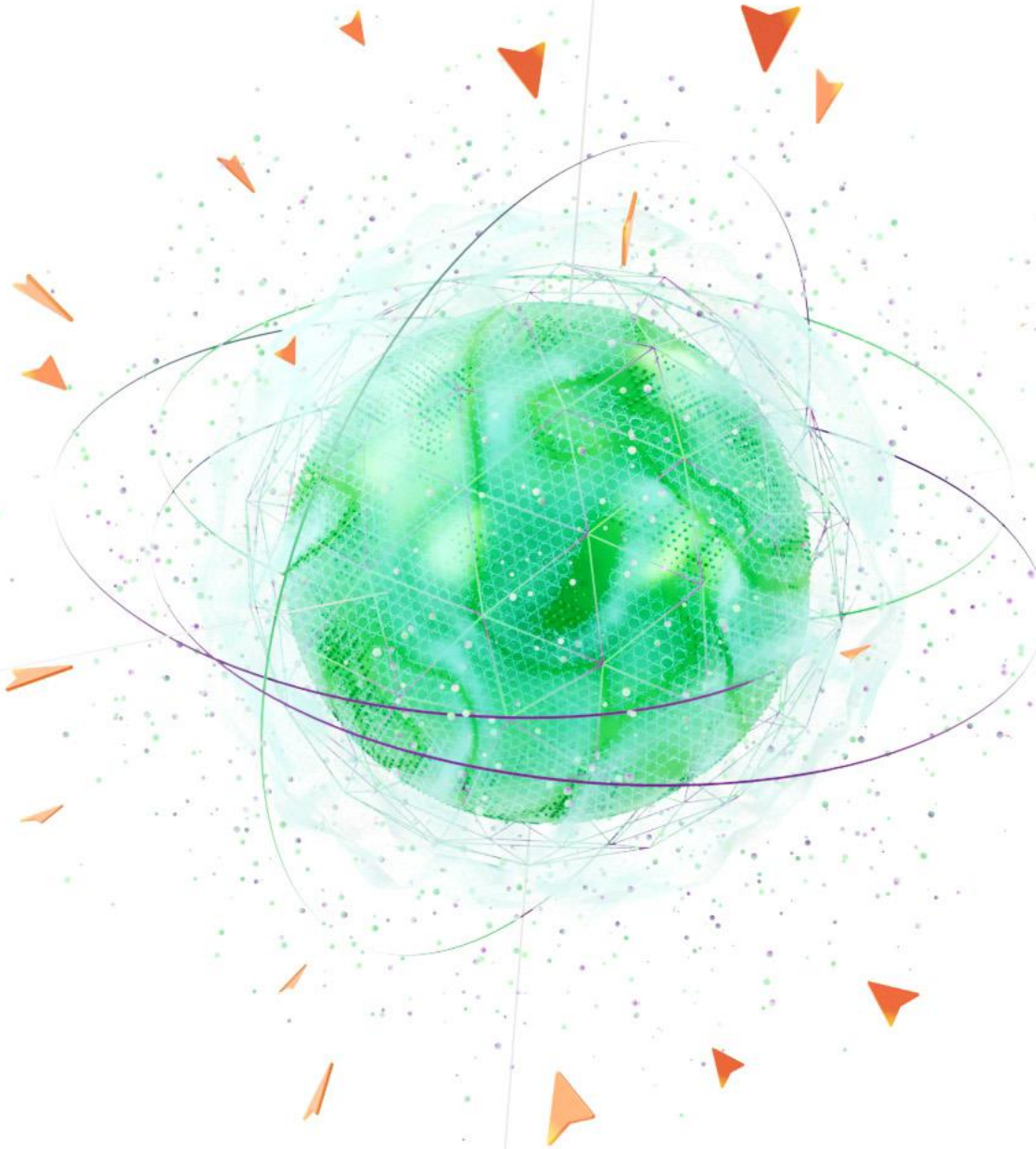
Угрозы/атаки, с которыми столкнулись за год



ПроБизнес

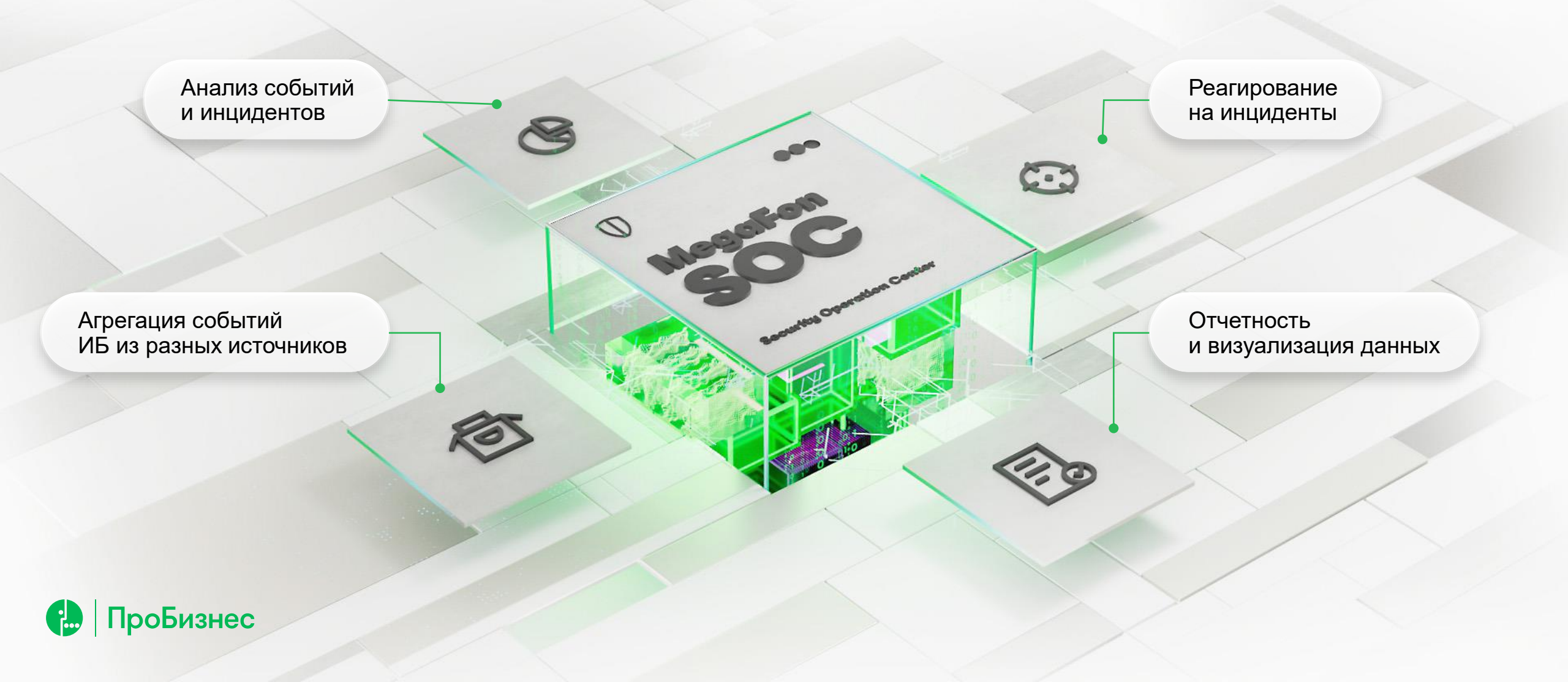
Минусы внутреннего SOC

- Отсутствие бюджета;
- Отсутствие квалифицированных кадров;
- Отсутствие оперативной реакции на инциденты;
- Долгое выстраивание процессов обработки инцидентов;
- Необходима сильная экспертиза для расследования инцидентов.
- Затраты на покупку и внедрение SIEM, IRP;
- Взаимодействие с ГосСОПКА.



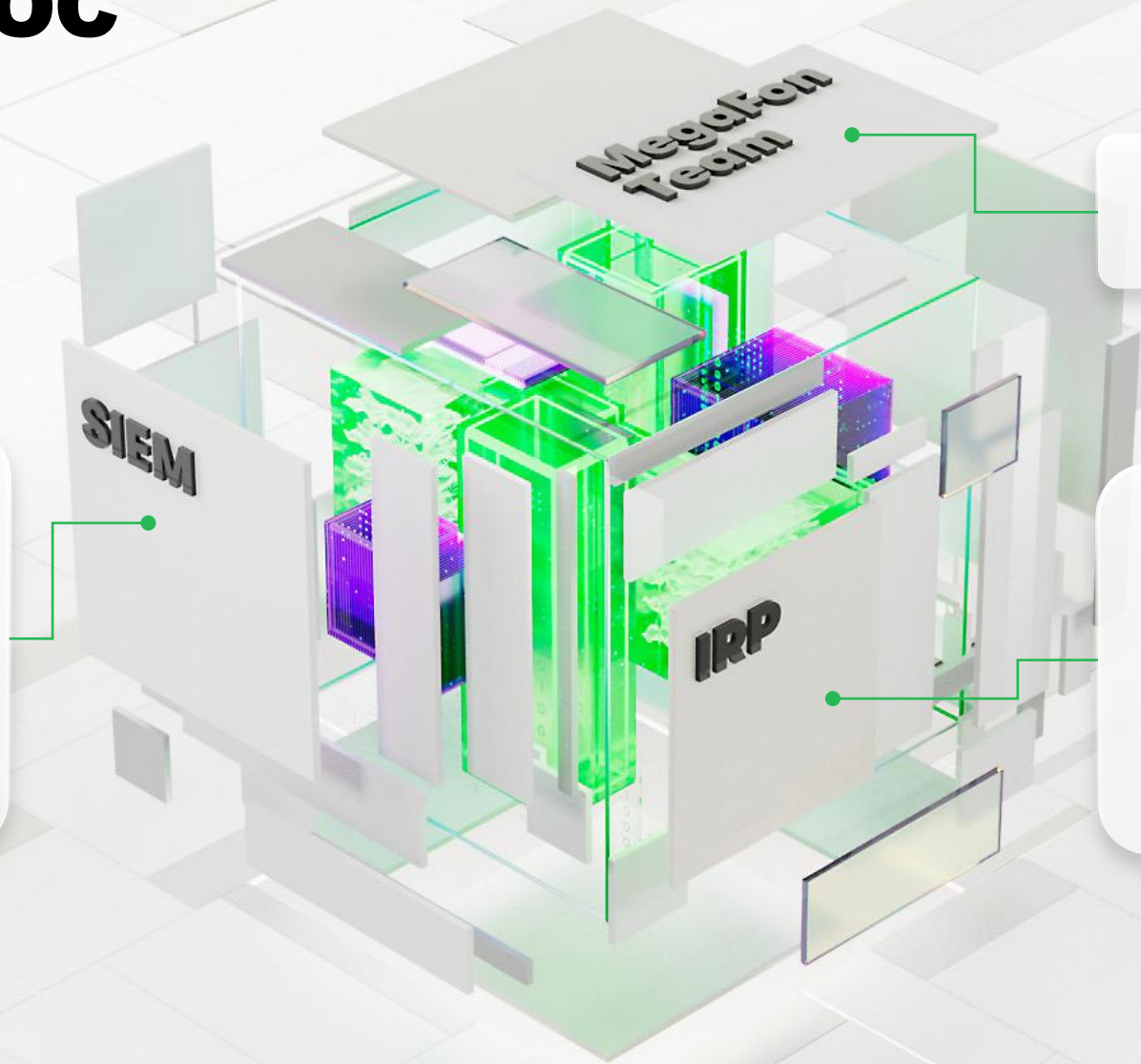
МегаФон SOC

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



ПроБизнес

Из чего состоит МегаФон SOC



Команда экспертов ИБ МегаФона

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

ПроБизнес

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

ПроБизнес

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

ПроБизнес

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

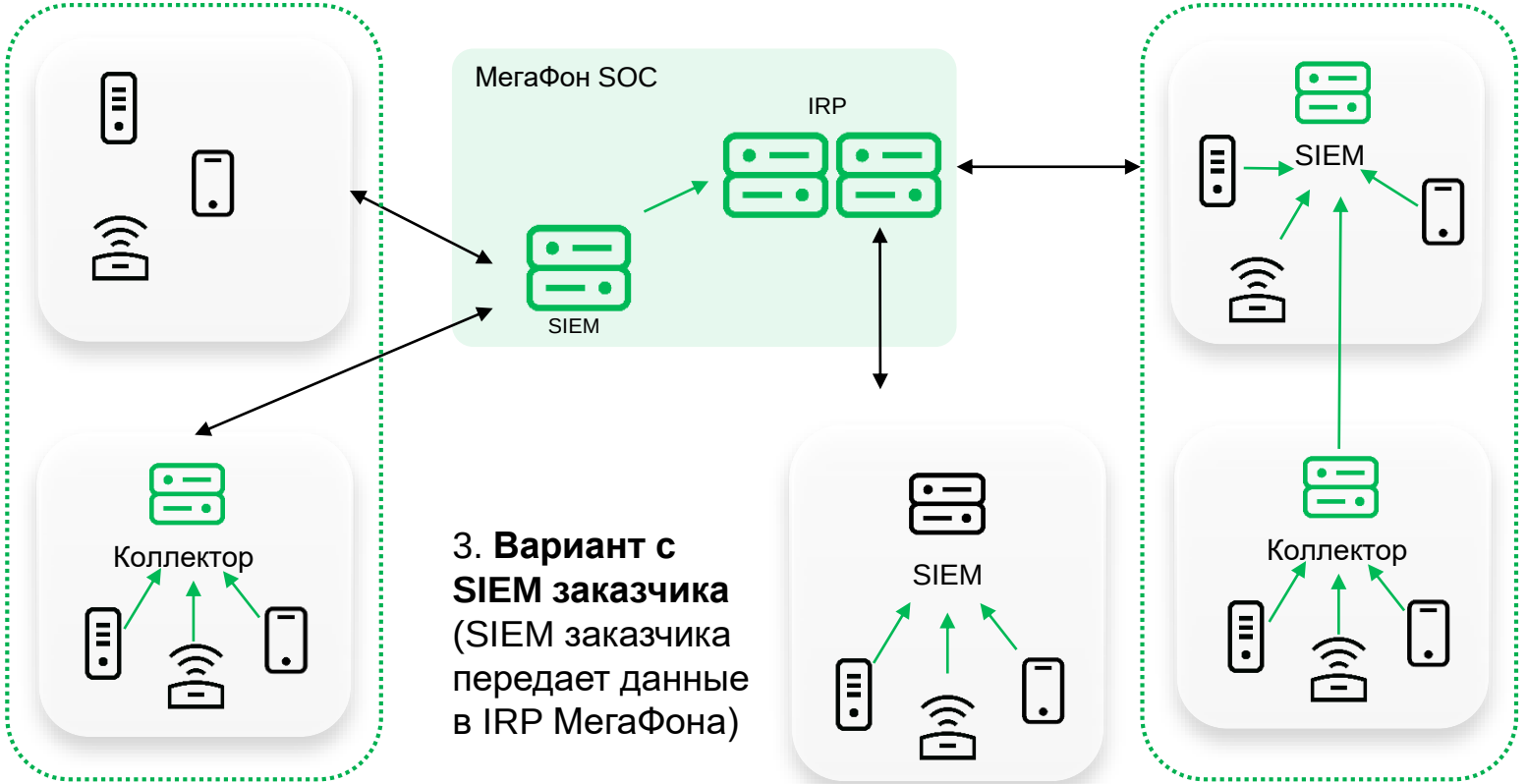
Оформление разработанных сценариев в унифицированный вид для дальнейшего использования линиями при помощи инструментов платформы SOAR — Security Orchestration, Automation and Response (в SOC возможны тысячи сценариев)

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

ПроБизнес

Преимущества услуги МегаФон SOC

- Мультивендорное решение на базе продуктов ведущих российских производителей
- Гибкие варианты оплаты
- Решение, не требующее закупки оборудования клиентом
- Уникальные метрики для анализа на уровне мобильной сети
- Гибкий SLA и гарантированная доступность (99,95%)
- Удобная интеграция со всей линейкой решений МегаФона

Технологии включают бизнес

Мелёхин Артём
Руководитель технической поддержки по облачным и инфраструктурным решениям МегаФона

Artem.Melekhin@megafon.ru

8 800 550 05 55
b2b.megafon.ru

МегаФон | ПроБизнес