ANGARA SECURITY

Внедрение модульной Системы управления событиями и инцидентами информационной безопасности в рамках проекта для Capital Group

CG CAPITAL GROUP

Capital Group — лидер в сегменте элитной недвижимости и небоскребостроении.
На протяжении 29 лет специализируется на строительстве самых сложных и знаковых объектов Москвы – многофункциональных комплексов, жилой и коммерческой недвижимости.
В портфеле компании — 9 млн кв. м реализованных, строящихся и проектируемых объектов.

Лидерские позиции компании в сфере девелопмента обеспечены профессиональной экспертизой, уникальными отраслевыми компетенциями и применением последних технологических решений – как в строительстве, так и в подразделениях бэк-офиса. Применение таких решений требует особенного внимания к вопросам информационной безопасности.

Центр киберустойчивости Angara SOC

- Внедрение SIEM решения для создания полной видимости IT инфраструктуры
- Разработка проектной документации
- Подключение актуальных источников событий
- Мониторинг и управление инцидентами ИБ (SIEM/IR(P)) (On-Premise & Outsource)
- Автоматизация управления и реагирования на инциденты ИБ (IR(P)/SOAR) (On-Premise & Outsource)
- Выездные расследования и форензика (DFIR)

Задачи внедрения

- Производить учёт и управление жизненным циклом атак и инцидентов информационной безопасности;
- Выстроить процесс постоянного анализа большого объема данных, поступающих от источников;
- Выявлять отклонения от нормального поведения контролируемых систем;
- Обрабатывать полученные данные и находить взаимосвязи между ними;
- Оповещать операторов об обнаруженных инцидентах;
- Развивать экспертизу сотрудников Заказчика.

Этапы работ

- Обследование сбор данных об IT ландшафте Заказчика
- Внедрение системы MP SIEM
- Подключение распределенных площадок, источников для сбора ИБ событий в MP SIEM
- Организация каналов связи между площадками Angara SOC и Capital Group, интеграция новой SIEM с действующими процессами SOC
- Адаптация правил корреляции событий, разработка и описание правил реагирования
- Начало оказания услуг, процесс гармонизации взаимодействий между подразделениями Capital Group и Angara SOC
- Непрерывное развитие текущих практик обогащение процессов ИБ

Схема взаимодействия

Site:

- МСЭ
- DLP
- APM
- Антивирусы
- Серверы
- IDS/IPS-системы

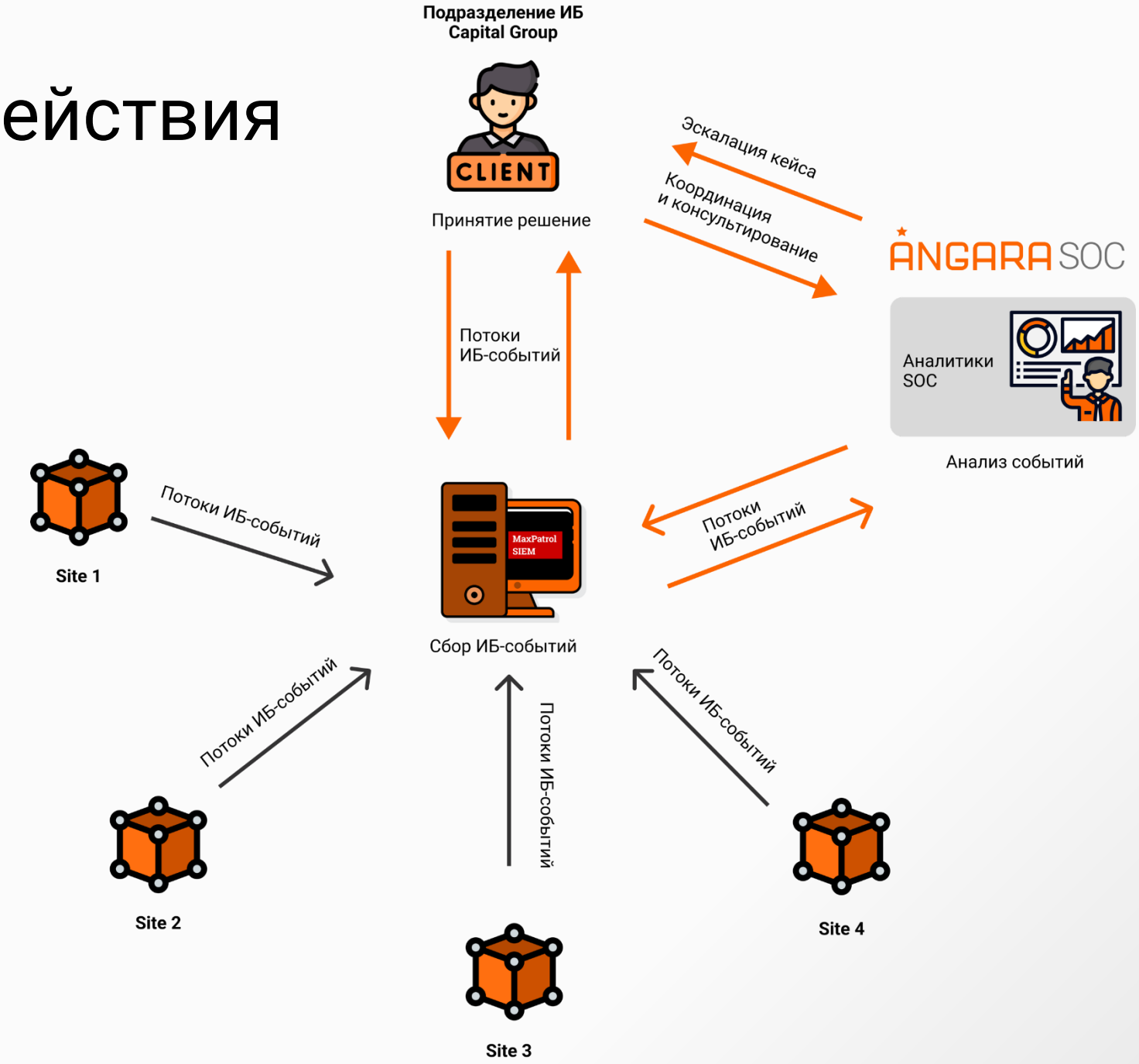
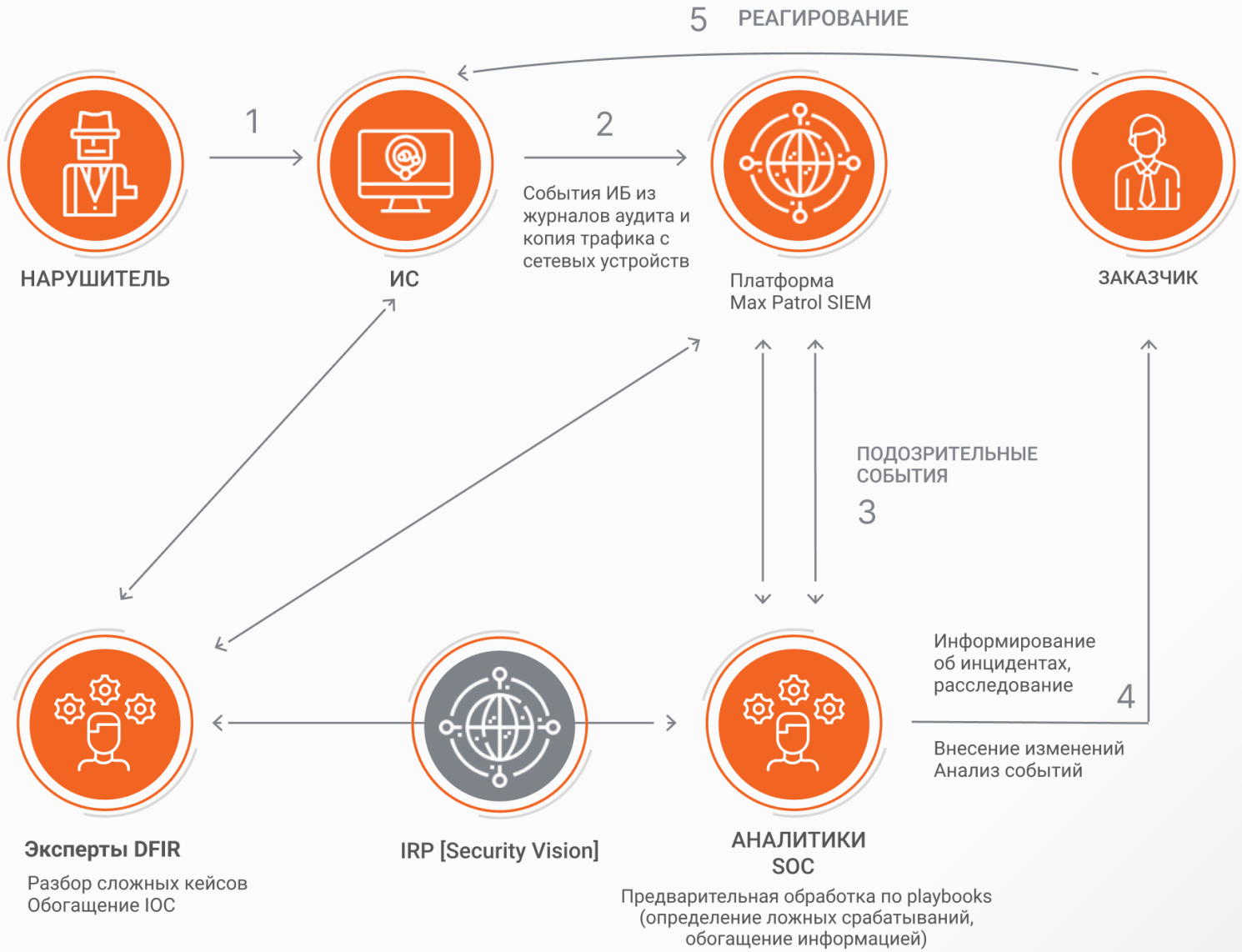


Схема работы после внедрения



Результаты внедрения

Автоматизирован процесс управления жизненным циклом инцидентов ИБ

Фиксированный SLA позволяет понимать, насколько быстро будет отработан инцидент информационной безопасности

Нет необходимости в найме сотрудников смен мониторинга, экспертов DFIR

Прозрачность в сопровождении и настройке используемых систем

ANGARA
SECURITY