USSC-SOC и R-SOC: мониторинг в тандеме

Руслан Амиров

Директор USSC-SOC

Формирование комплексного предложения

- Аудит ИБ
- Разработка ОРД
- ИБ АСУ ТП
- Проектирование и внедрение
- Развитие и поддержка SOC
- Расследование и реагирование на сложные инциденты ИБ

- R-SOC
- Защита от DDoS-атак
- WAF
- ГОСТ VPN
- DLP
- Универсальный шлюз безопасности
- Анализ защищенности

Построение коммерческого SOC

Как строить:

- Самостоятельно
- Привлечь системного интегратора

Ключевой состав SOC:

- Сотрудники
- Технологии
- Процессы
- Знания

Можно ли построить SOC без этих элементов?

Коммерческий SOC: технологии

Первоочередные компоненты:

- Средства сбора событий
- Средства преобразования событий
- Средства обнаружения инцидентов
- Средства обработки инцидентов
- Средства автоматизации
- Инфраструктура

Вторая очередь – развитие:

- EDR/XDR
- On-site TIP
- UEBA
- NTA

Как будет работать SOC без XDR?

Коммерческий SOC: процессы

USSC SOC

Мониторинг ИБ	Управление инцидентами ИБ	Инвентаризация активов	Подключение Заказчиков
Управление знаниями	Развитие контента обнаружения и реагирования	Управление инфраструктурой	Управление отчетностью
Взаимодействие с Заказчиками	Управление данными киберразведки	Проактивый поиск угроз	Другие процессы

Зачем столько процессов?

Коммерческий SOC: сотрудники

Кто требуется в первую очередь:

- Руководитель
- Аналитики L1
- Аналитики L2/L3
- Инженеры

Вторая очередь – развитие:

- Аналитики Threat Hunting
- Аналитики киберугроз (Threat Intelligence)
- Специалисты по компьютерной криминалистике (DFIR)
- Пентестеры

Коммерческий SOC: знания

USSC SOC

Эксплуатация средств SOC	Мониторинг ИБ	Обработка инцидентов: базовый triage, развернутый анализ	Обслуживание средств и инфраструктуры
Контент по обнаружению и реагированию на инциденты	Применение данных киберразведки	Проактивный поиск угроз	Форензика

Создание R-SOC

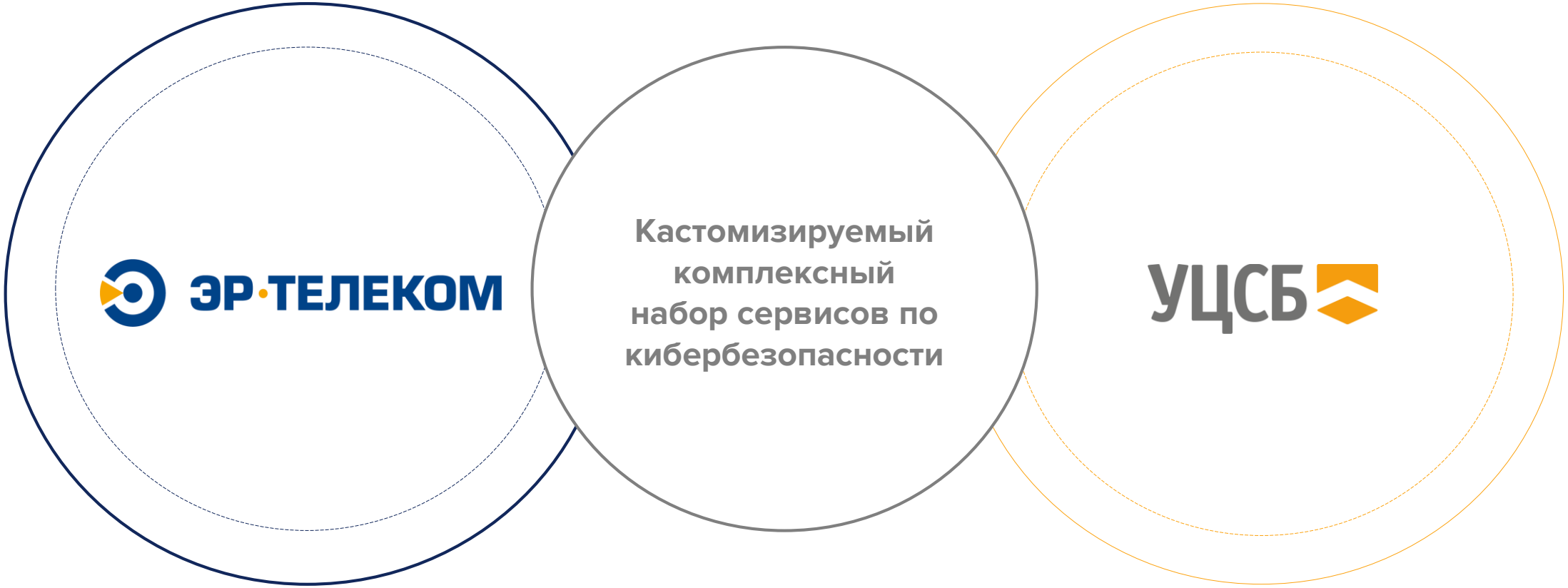
1. Определение бизнес-требований к SOC, вариантов архитектуры, состава решений, набора документации
2. Бюджетирование и конкурсные процедуры
3. Проектирование
4. Внедрение
5. Поиск и обучение сотрудников
6. Опытная эксплуатация
7. Приемо-сдаточные испытания
8. Подключение пилотного Заказчика
9. Подключение коммерческих Заказчиков

Как ускорить? Что можно сделать параллельно?

Ключевые вопросы при создании R-SOC

Ключевые вопросы	Проблематика
Внедрение новых решений	Неизвестные ранее продукты
Новая организационная структура	Управление и развитие
Набор сотрудников	Поиск и отбор
Обучение сотрудников	Поддержание компетенций
Масштабирование	Увеличение числа Заказчиков
Интеграция в экосистему продуктов B2B	Органичное внедрение услуг в портфель
Отличия от других SOC	Внедрение преимуществ
Наполнение знаниями	Поиск, проверка, использование в работе

Измеряемый эффект



Security Operations Center

Руслан Амиров

Директор USSC-SOC

ramirov@ussc.ru

soc.ussc.ru