Подключение к SOC:
как подготовиться

Максим Коршунов
maxim.korshunov@orange.com

orange™ Business Services

Группа Orange: возможности глобального лидера

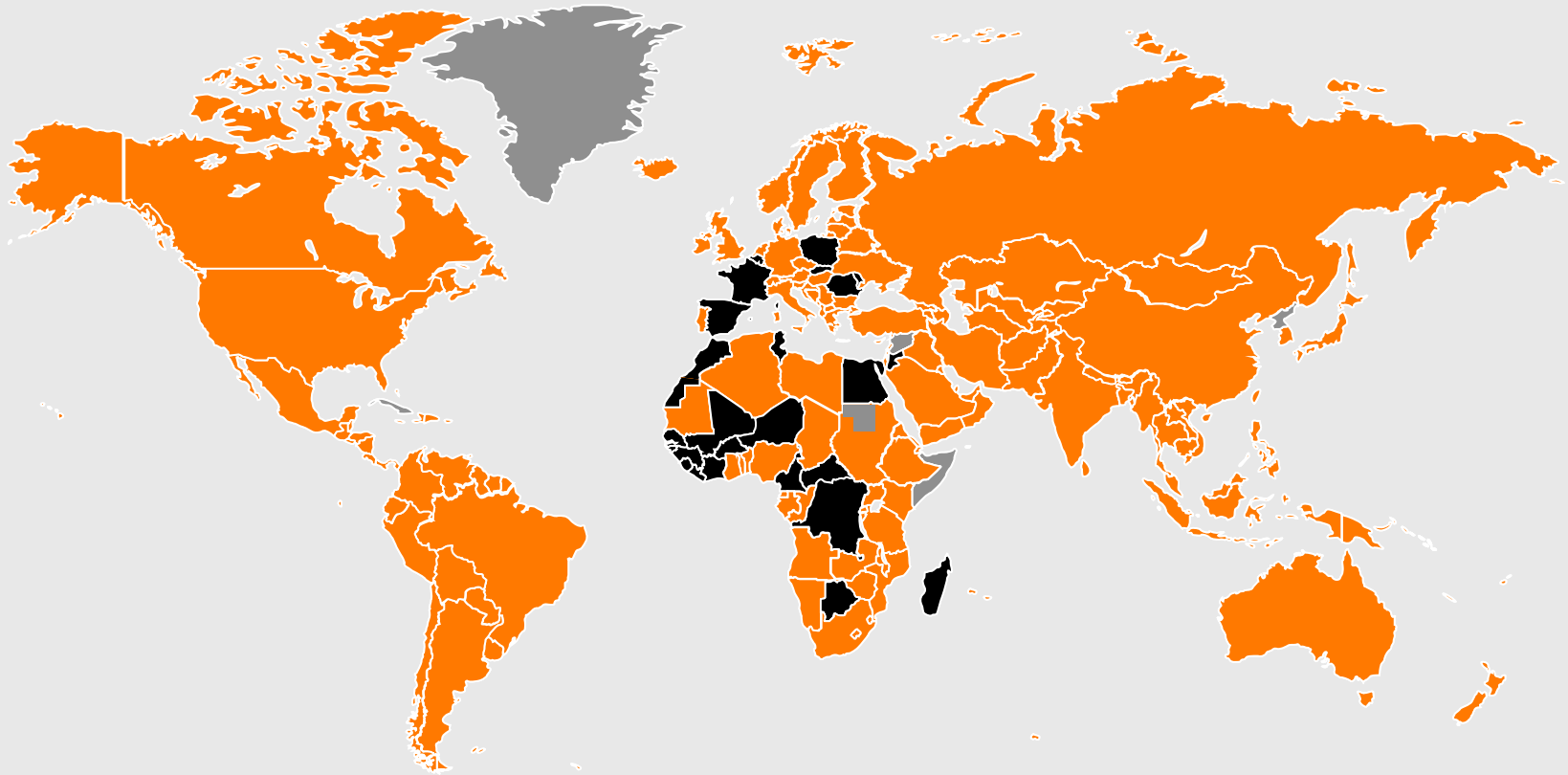
273+ млн
клиентов

€41,1 млрд
выручка в 2017 году

450 000 км
подводных кабелей

€600 млн
ежегодных инвестиций в магистральную инфраструктуру

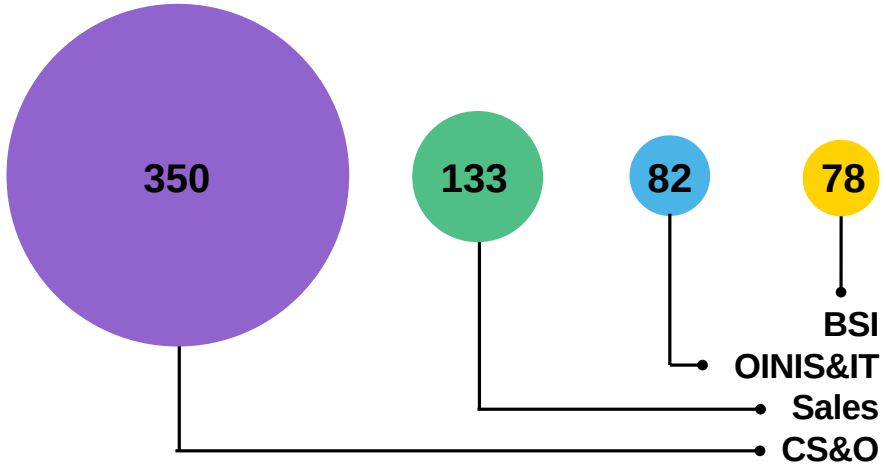
345 000+ точек подключения
Уникальное покрытие по всему миру



- Крупнейшая в мире бесшовная сеть передачи голоса и данных с предоставлением сквозных услуг связи. Сотрудники в 220 странах и территориях
- Оператор связи для населения в 29 странах
- Нет присутствия Orange Business Services

Orange в России

- B2B-подразделение группы Orange: провайдер цифровых сервисов с экспертизой в области телекоммуникаций
- Единственный международный оператор связи с собственной инфраструктурой
- Присутствуем в 220 странах и территориях
- Сильные местные компетенции: центр инноваций и центр мониторинга киберугроз (SOC)
- Создаем инновации для крупного бизнеса: 8 из 10 крупнейших российских компаний Forbes-2000 Top-10 – наши клиенты*



800+ сотрудников

В России с 1958 года (SITA)

- 31 отделение
- 13 офисов продаж
- 1500 корпоративных клиентов

*according to Top-2000 Forbes 2018 rating

Проблемы подразделений безопасности

- **Нехватка специалистов**
  51% компаний испытывают дефицит ИБ специалистов
- **Отсутствие средств идентификации актуальных угроз**
- **Отсутствие понимания методов реагирования на угрозы**
- **Выполнение требований законодательства**
- **Высокая стоимость владения оборудованием и ПО**

Решение – Security Operations Center

Проблемы

- **Нехватка специалистов.**
  51% компаний испытывают дефицит ИБ специалистов
- **Отсутствие средств идентификации актуальных угроз**
- **Отсутствие понимания методов реагирования на угрозы**
- **Выполнение требований законодательства**
- **Высокая стоимость владения оборудованием и ПО**

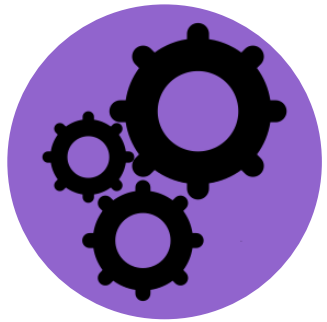
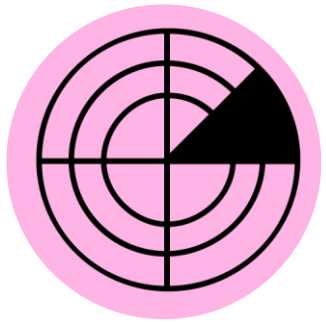
SOC

- **Привлечение экспертизы**
- **Каталог сценариев детектирования**
- **Реагирование на инциденты согласно рекомендациям экспертов**
- **Лицензируемая деятельность**
- **Готовая инфраструктура в составе решения**

Выгода

- **Снижение затрат на персонал и рисков с ним связанных**
- **Возможность идентификации актуальных угроз среди «белого шума»**
- **Предотвращение или снижение потерь в случае реализации угрозы**
- **Соответствие требованиям ФЗ**
- **Снижение капитальных затрат на оборудование**

Функции SOC

Подключение	Выявление	Реагирование	Отчетность
			
▪ Сбор событий* ▪ Настройка систем контроля ▪ Разработка сценариев атак	▪ Выявление угроз ▪ Анализ угроз ▪ Контроль ресурсов	▪ Разработка рекомендаций по реагированию ▪ Разработка рекомендаций по модернизации	▪ Отчет по событиям и инцидентам ▪ Планы по модернизации

**- Сбор событий – сбор записей из электронных журналов различных устройств, о всевозможных активностях связанных с этими устройствами. Например: разблокировка компьютера, обращение к сетевому ресурсу, запуск файла.*

Пример взаимодействия

Вредоносное ПО и взаимодействие с C&C, трафик не был заблокирован FW на периметре сети

Сценарий:

- Вредоносное ПО закрепилось на хосте, запустилось из-под профиля пользователя (не было прав администратора на этой машине), установил C&C сессию с интернет-хостом и прошел незамеченным для межсетевого экрана на периметре сети
- Аналитики CyberSOC проводят первичную аналитику и предоставляют данные для сдерживания инцидента
- ИТ/ИБ команда после информирования CSOC заблокировала доступ на FW (изоляция хоста) и провела интервью с пользователем
- Аналитики CyberSOC проводят более детальный анализ логов и инцидента, идентифицирует вредоносный процесс и готовит дополнительные рекомендации по реагированию
- ИТ/ИБ выполнила очистку хоста и команда вернула начальные правила МЭ.

Сравнение СОКов

Параметр	Свой SOC	SOC as a Service
Контроль	Полный	Частичный
Понимание информационных потоков	Высокое	Низкое или отсутствует
Гибкость в настройке	Высокая	Средняя
Скорость развертывания	От полугода (обычно 2-3 года)	2-4 месяца
Режим работы (обычно)	5 x 8	24 x 7
Возможности по реагированию	Высокие	Средние / Высокие (MDR)
Скорость масштабирования	Средняя	Высокая
Уровень компетенций	Средний	Высокий
Форма наибольших затрат	CAPEX	OPEX
Предсказуемость затрат	Непредсказуемые	Предсказуемые
Гарантии (финансовые и т.п.)	Отсутствуют	Возможны
Зависимость от каналов связи	Средняя	Высокая
Хранение данных о безопасности	Локально	За пределами организации / гибридно
Права на технологии и процессы	Принадлежат заказчику	Принадлежат провайдеру
Уровень независимой экспертизы / взгляд со стороны	Низкий	Высокий
Выделенный персонал заказчика	Да	Тоже да, но меньше

Сравнение СОКов

Параметр	Свой SOC	SOC as a Service
Контроль	Полный	Частичный
Понимание информационных потоков	Высокое	Низкое или отсутствует
Гибкость в настройке	Высокая	Средняя
Скорость развертывания	От полугода (обычно 2-3 года)	2-4 месяца
Режим работы (обычно)	5 x 8	24 x 7
Возможности по реагированию	Высокие	Средние / Высокие (MDR)
Скорость масштабирования	Средняя	Высокая
Уровень компетенций	Средний	Высокий
Форма наибольших затрат	CAPEX	OPEX
Предсказуемость затрат	Непредсказуемые	Предсказуемые
Гарантии (финансовые и т.п.)	Отсутствуют	Возможны
Зависимость от каналов связи	Средняя	Высокая
Хранение данных о безопасности	Локально	За пределами организации / гибридно
Права на технологии и процессы	Принадлежат заказчику	Принадлежат провайдеру
Уровень независимой экспертизы / взгляд со стороны	Низкий	Высокий
Выделенный персонал заказчика	Да	Тоже да, но меньше

Что клиенты ждут от SOC

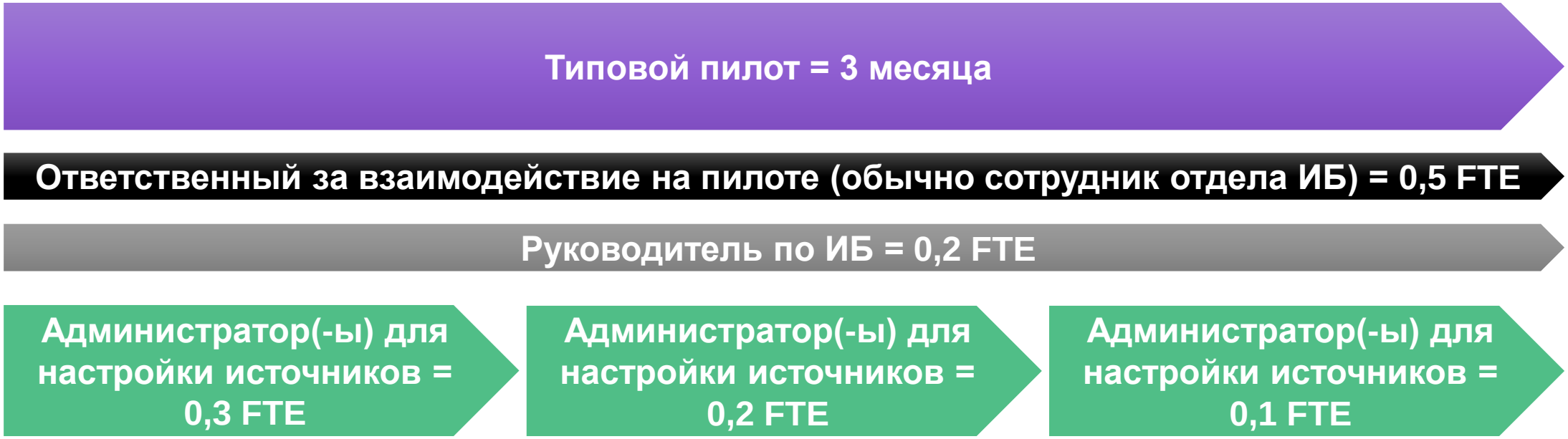
Миф

- СОК защитит от компьютерных атак
- СОК мониторит все (всю инфраструктуру)
- Основа СОК – это SIEM
- Для начала можно взять СОК из коробки / «как у всех» / «как обычно», а потом подстраивать
- У меня толковые админы – дайте инструкции и все сделаем быстро
- У меня толковые админы – вся инфраструктура описана
- Бесплатный пилот, почему бы и нет
- Уже проводили пилот, все готово для еще одного

Реальность

- СОК позволяет вовремя отреагировать на угрозу
- Мониторить все очень дорого. Часть угроз стоит закрыть превентивными мерами защиты.
- SIEM лишь инструмент, главное процессы
- СОК из коробки либо не принесет пользы, либо не взлетит вовсе, поэтому всегда кастомизация
- Админы решают свой поток задач, что-то дополнительное всегда с низким приоритетом
- Данные устарели, причину см. выше
- Без необходимой вовлеченности и выделения ресурсов = waste time
- Одинаковых СОКов не бывает. Многое на пилоте надо пересматривать / переделывать

Бесплатный пилот ≠ 0 рублей



* - а так же железо для реализации коллекторов сбора логов и транспортных серверов

** - FTE (Full-Time Equivalent) - эквивалент полной занятости

Частые ошибки и проблемы

- Отсутствие понимания собственной инфраструктуры (что и где находится, как используется, кто ответственный, что разрешено/запрещено)
- Отсутствие понимания актуальных угроз
- Отсутствие политик ИБ и процессов управления ИБ
- Отсутствие средств защиты
- Отсутствие реагирования/обратной связи

- Видимость сока оставляет желать лучшего – большое количество FP / FN
- Работа по типовым сценариям создает лишь ощущение безопасности
- Длительный период реагирование или его отсутствие делают СОК бесполезной тратой денег

С чего начать? Quick start

Вопросы первого порядка

- Есть ли у меня актуальная схема сети?
- Внедрены ли у меня политики безопасности ?
- Знаю ли я актуальные для моей инфраструктуры угрозы?
- Есть ли у меня люди для реагирования и полномочия ставить им задачи?
- Есть ли у меня средства защиты для реагирования?
- Знаю ли я всех ответственных за инфраструктуру?

Вопросы второго порядка

- Сколько это будет мне стоить?
- Что начать мониторить в первую очередь (периметр, публичные сервисы, DMZ, внутреннюю сеть, удаленных пользователей)? Определить этапы - начать с малого и набирать обороты
- Есть ли / будет ли у меня бюджет на подключение SOC?
- Для мониторинга надо собирать логи. А как? Сформировать концепцию схемы сбора логов

Готовы ли вы к SOC?

Checklist

Musthave – без чего не стоит обращаться к СОК
Актуальные и достаточные данные о собственной инфраструктуре (что и где находится, как используется, кто ответственный, что разрешено/запрещено, понимание что контролируешь сам/на что сможешь повлиять)
Наличие базовых СЗИ (FW, IDS/IPS, AV etc.)
Наличие внедренных политик ИБ
Понимание актуальных угроз
Поддержка на уровне руководства
Бюджет
Определены и наделены полномочиями люди ответственные за реагирование
Определены ответственные за инфраструктуру
Желательно иметь – позволит повысить ценность SOC уже на старте
Наличие модели угроз
Процесс реагирования на инциденты
План по развитию ИБ
Концепция схемы сбора логов
Не является преимуществом – скорее всего потребуется переделывать
Реализованная схема сбора логов / Заранее настроены источники событий
Уже внедренная SIEM

Спасибо!
#Stayathome

Максим Коршунов
maxim.korshunov@orange.com

orange™ Business Services