Операционная модель SOC
и работа с инцидентами

Андрей Прошин
andrey.proshin@orange.com

orange™ Business Services

Группа Orange: возможности глобального лидера

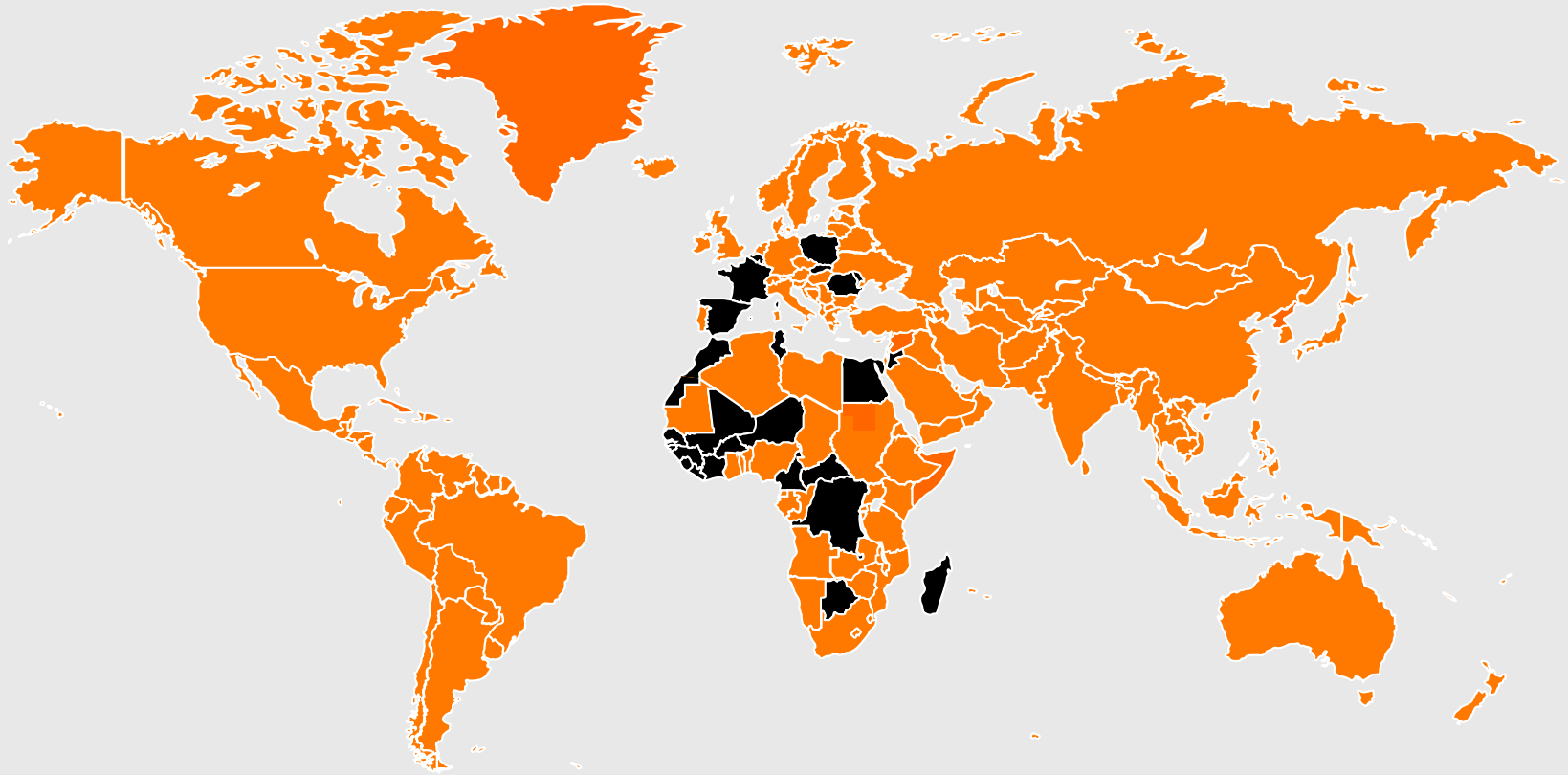
273+ млн
клиентов

€41,1 млрд
выручка в 2017 году

450 000 км
подводных кабелей

€600 млн
ежегодных инвестиций в магистральную инфраструктуру

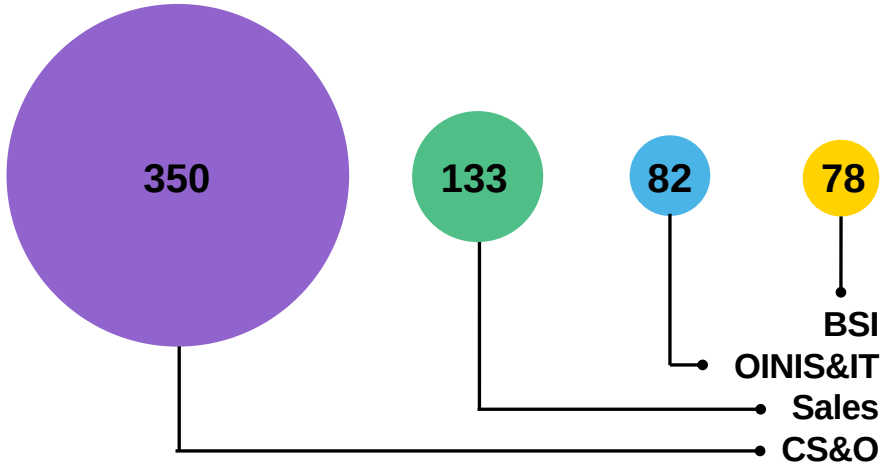
345 000+ точек подключения
Уникальное покрытие по всему миру



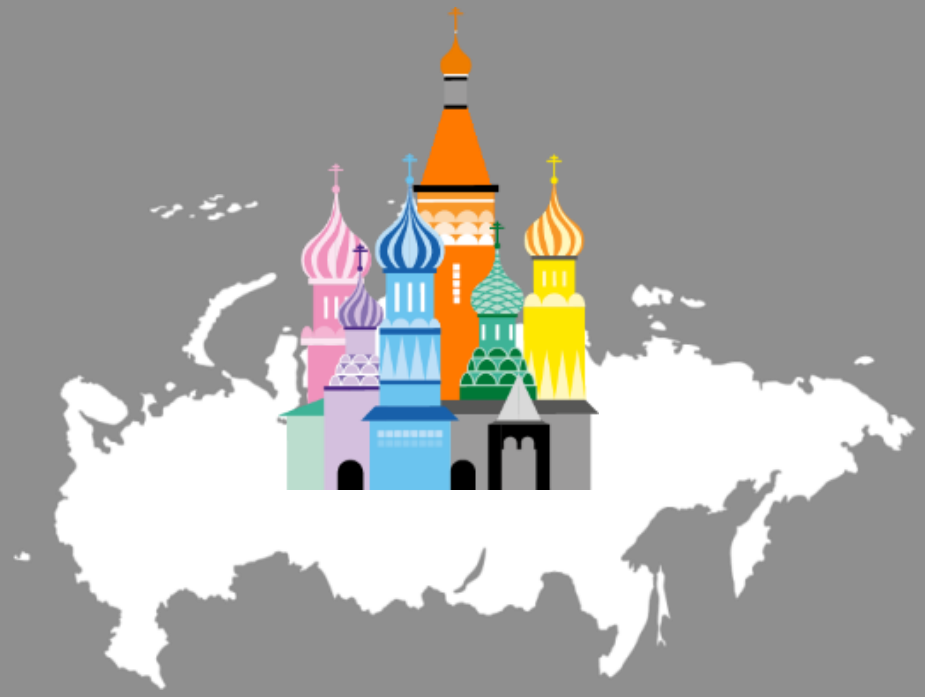
- Крупнейшая в мире бесшовная сеть передачи голоса и данных с предоставлением сквозных услуг связи. Сотрудники в 220 странах и территориях
- Оператор связи для населения в 29 странах
- Нет присутствия Orange Business Services

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

Группа Orange: кибербезопасность

Наша экспертиза

Глобальная сеть SOC и CERT команд

Собственные исследования в рамках Threat Intelligence

Гибкие решения в области управляемых услуг безопасности (MSSP/MDR)

2,100
ИБ экспертов по всему миру

30 лет
защиты критической инфраструктуры

720
международных клиентов

Варианты операционной модели SOC

С чего начать

Поддержка Management Team

Проект подразумевает большие финансовые затраты, вовлечение разных команд и специалистов, создание нового опыта/процесса по работе с инцидентами ИБ

Постановка и утверждение целей

Цели создания SOC должны быть четко определены и согласованы ну уровне руководства компании

Определенный уровень зрелости ИБ

- Модель угроз
- Система защиты периметра
- Защита рабочих станций
- Централизованное логирование

Оценить текущие возможности

Важно оценить текущие возможности вашей компании для создания / модернизации SOC проекта

Технологические платформы

- Предпочтения по вендорам
- Наличие систем, которые могут закрыть часть требований к SOC
- Необходимость интеграции с существующими ИТ / ИБ системами

Экспертиза

- Навыки и экспертиза
- Количество людей

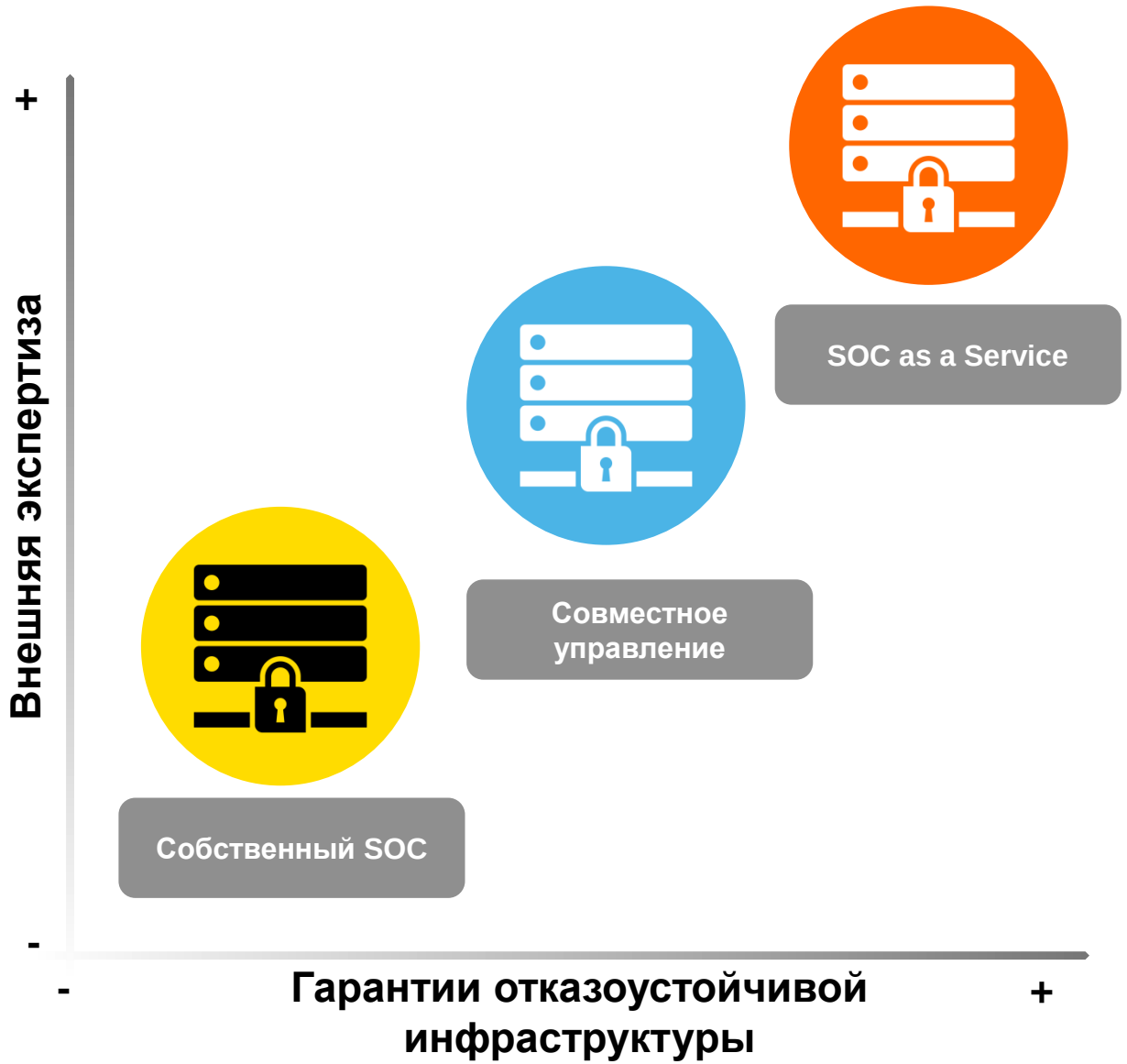
Зрелость ИБ

- Процессы
- Понимание рисков и угроз
- Безопасность как сервис

Также:

- 24x7 или 8x5
- Требуемый уровень SLA (время обнаружения и реагирования)

Операционная модель SOC



Финансы	Хостинг	Аналитик
opex	облако	shared
capex	on premise	выделенный

Сравнение SOC

Параметр	Собственный 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	Собственный 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

Команда SOC. Роли и задачи

Функции ИБ команды

Готовность
к новым угрозам и снижению киберриска

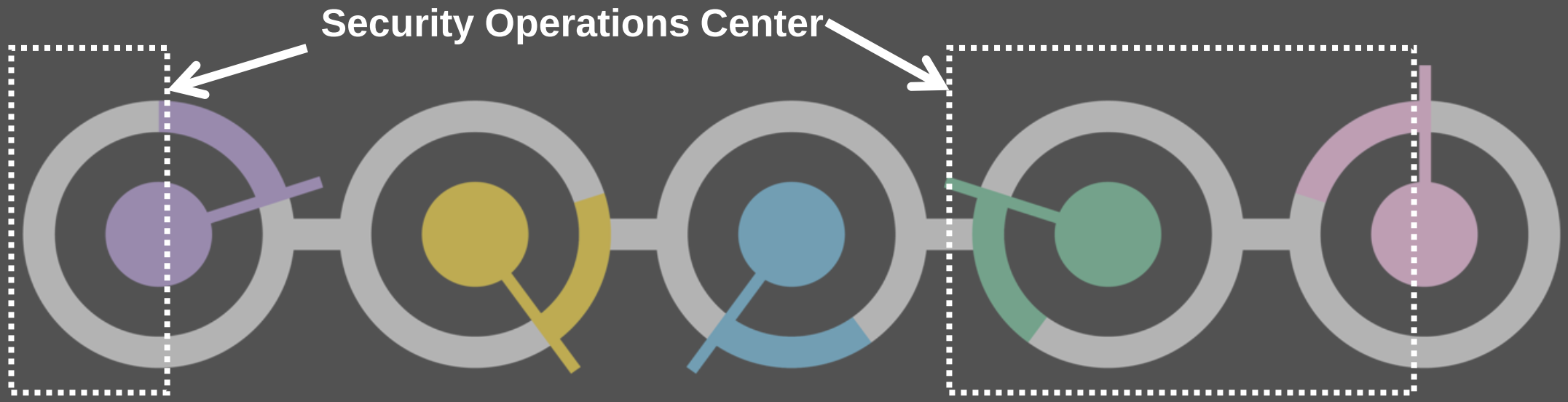
Понимание
ваших ключевых активов, их рисков и подготовка стратегии ИБ

Защита
вашей компании современными технологиями ИБ

Обнаружение
Кибератак путем 24x7 мониторинга событий ИБ

Реагирование
На кибератаки и снижение потенциального ущерба

Функции ИБ команды



Готовность
к новым угрозам и снижению киберриска

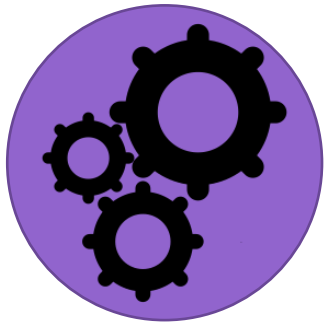
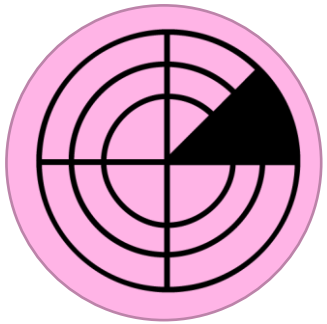
Понимание
ваших ключевых активов, их рисков и подготовка стратегии ИБ

Защита
вашей компании современными технологиями ИБ

Обнаружение
Кибератак путем 24x7 мониторинга событий ИБ

Реагирование
На кибератаки и снижение потенциального ущерба

Функции SOC

Взаимодействие	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.*

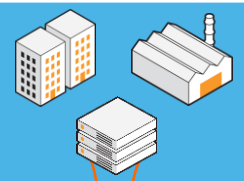
Как работает SOC

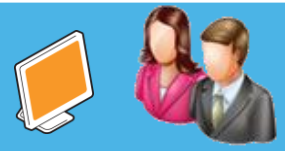
Взаимодействие

Выявление и реагирование

Отчетность

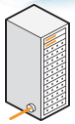
Заказчик



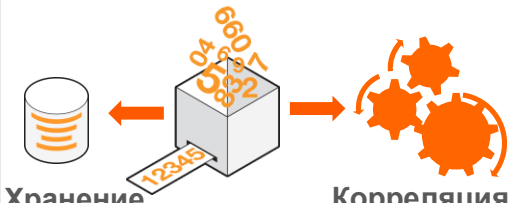


ИБ команда

Директор департамента ИБ



Сбор событий



L1 – 24/7

Аналитик

- Мониторинг
- Квалификация инцидентов
- Подготовка плана противодействия

L2 – 8/5

Эксперт

- Разработка каталога use case
- Снижение False Positive
- Работа со сложными инцидентами
- Отчетность

L3 – 8/5

Консультант

- Pen test эксперт
- SIEM эксперт
- Security Expert

Security Manager

Дополнительные исследования

R&D / Lab

Команды SOC и роли

L1: Оператор SOC

- Первичная оценка и квалификация инцидента. Регистрация карточки инцидента
- При выявлении подозрительных файлов использование «песочницы» для эмуляции и анализа файла.
- Обновление/дополнение базы знаний.
- Разработка рекомендаций/плана по реагированию на инцидент ИБ в соответствии с playbook.
- Взаимодействие с группой реагирования

L2: Аналитик SOC

- Детальный анализ инцидента ИБ по всем доступным источникам информации (SIEM, TI, Sandbox, Vulnerability Scanner)
- Предоставление плана по реагированию на инциденты, не описанные в playbook.
- Выявление ложных срабатываний источников событий.
- Обновление/дополнение правил корреляции/use-case/playbook.
- Помощь в расследование - взаимодействие с Группой реагирования для сбора дополнительной информации об инциденте ИБ.

L3: Эксперт SOC

- Поддержка L2 для анализа инцидентов
- Подключение новых источников событий
- Threat hunting

Группа Реагирования

- Выполнение рекомендаций SOC для локализации и нейтрализации инцидента
- Предоставление дополнительной информации для SOC в плане анализа инцидента
- Уведомление сотрудников SOC о проведенных работах

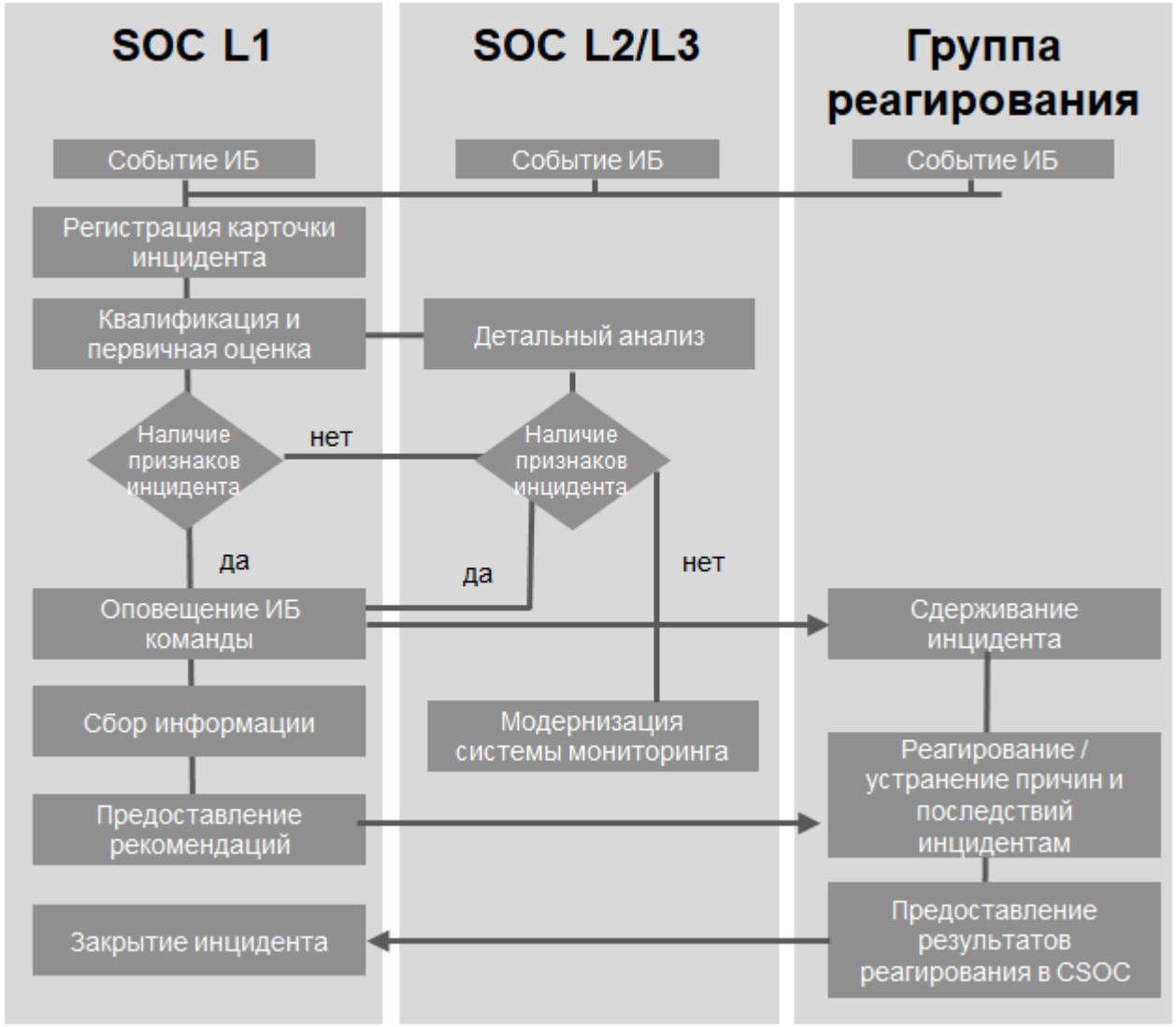
Группа поддержки инфраструктуры SOC

- Мониторинг доступности и работоспособности всех технологических компонентов
- Управление патчами
- Управление производительностью систем
- Резервное копирование и восстановление

Процесс управления инцидентами

Процесс управления инцидентами

Общий процесс работы над инцидентом



- Информация об инциденте может поступить из разных источников (SIEM, сообщение пользователя, внешний провайдер)
- Необходимо установить SLA (TTD, TTC, TTR)
- Часть процессов можно автоматизировать с помощью IRP / SOAR

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.

Спасибо!

Андрей Прошин
Andrey.proshin@orange.com