ПРАКТИЧЕСКИЙ ОПЫТ ПРИМЕНЕНИЯ КОММЕРЧЕСКОГО SOC НА ПРИМЕРЕ

РЕАЛИЗОВАННОГО В АО КБ «ЮНИСТРИМ»

СЕРГЕЙ КОХАНЬКО

ОКСАНА ВАСИЛЬЕВА

ПОДГОТОВЛЕНО ДЛЯ SOC-ФОРУМ 2019

Почему и зачем подключили SOC

- Необходимость эффективно противодействовать компьютерным атакам
- Необходимость управлять инцидентами ИБ
- Дефицит времени для построения собственного SOC
- Экономия ресурсов и оптимизация затрат

Основные критерии выбора SOC

- Наличие ИБ Экспертизы у Исполнителя
- Уровень и стоимость предоставляемых услуг
- Скорость внедрения в инфраструктуру
- Отзывы существующих клиентов

Процесс внедрения SOC

- Глубже изучили свою ИТ-инфраструктуру – повысили эффективность процессов
- Получили помощь в выборе места установки агентов
- Получили помощь по оптимальной настройке СЗИ для сбора необходимого количества информации
- Решили проблему получения копии трафика на арендованной виртуальной инфраструктуре

У нас есть SOC!

✓ Имеем инструмент, позволяющий в онлайн-режиме получать информацию, в том числе, для нужд ИТ

✓ Выполнены требования ЦБ

✓ События ИБ

Что дальше?

★ Интеграция в SOC новых средств защиты, постановка на мониторинг элементов ИТ-инфраструктуры

★ Расширение покрытия агентами инфраструктуры Банка

★ Облачные MSS сервисы, интеграция их с SOC

НАЧАЛО ПУТИ

ANGARA
professional assistance

ЕСЛИ ЗАКАЗЧИК ПРИШЁЛ К НАМ – ОН ГОТОВ К УСЛУГАМ СЕРВИС-ПРОВАЙДЕРА

ЧТО ДЕЛАЕМ:

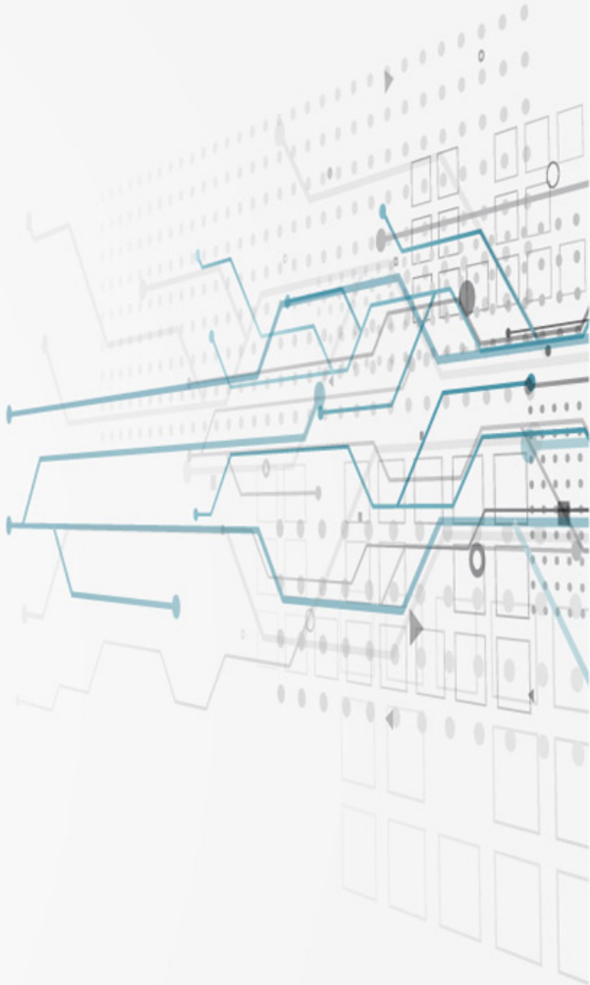
1 ПОДГОТОВКА	2 НАСТРОЙКА	3 ЭКСПЛУАТАЦИЯ
Определяем список ИС, подлежащих подключению к SOC и их критичность.	Согласовываем перечень выявляемых инцидентов ИБ Внедряемся и настраиваем процессы выявления и обработки инцидентов ИБ	Предоставляем услугу согласно SLA.
Заполняет Baseline, шаблон матрицы коммуникаций и эскалаций	Устанавливает компоненты NIDS, HIDS Настраивает источники событий	Подтверждает и реагирует

ANGARA

КЛИЕНТ

BASELINE И ПОЧЕМУ ЭТО ВАЖНО

КАЖДЫЙ ЗАКАЗЧИК ДЛЯ СЕРВИС-ПРОВАЙДЕРА УНИКАЛЕН

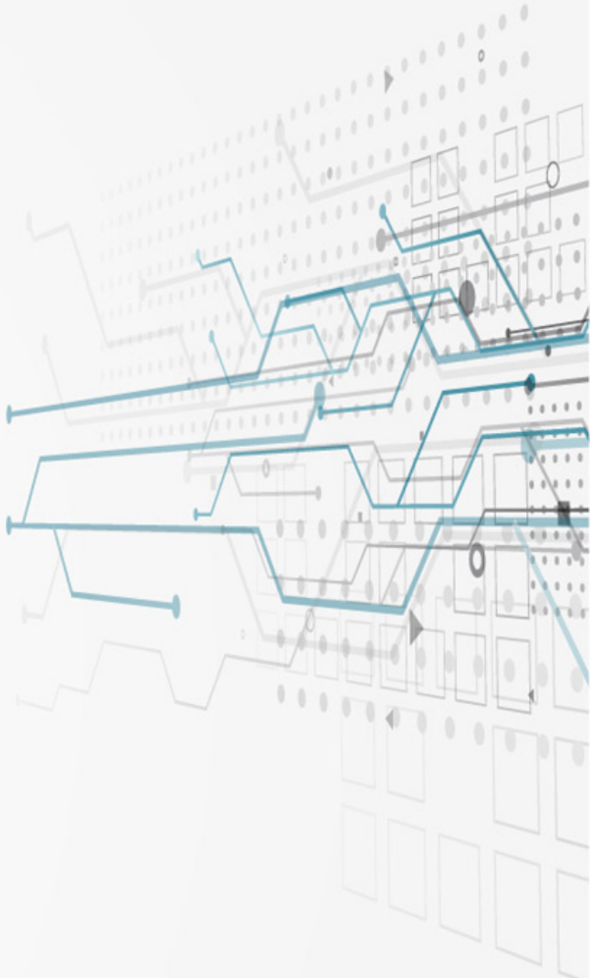


1. Отклонения от базового контроля – достоверный инцидент.

2. Заказчик экономит время при взаимодействии с провайдером

ANGARA
professional assistance

КАК ДОСТИЧЬ СИНЕРГИИ С ЗАКАЗЧИКОМ



1. Совместно с Заказчиком снижать % false
2. Уведомлять об ошибках в настройке инфраструктуры
3. Формировать отчёты по требованиям Заказчика
4. Адаптировать уведомления о расследованиях и полезные рекомендации под Заказчика
5. Дать возможность Заказчику формировать собственные дашборды

ANGARA
professional assistance

РЕЗУЛЬТАТЫ

- ★ SOC инструмент для ИТ
- ★ Контроль исполнения частных политик ИБ
- ★ Демонстрация узких мест в системе ИБ

1 МЕСЯЦ
СРОК ПОДКЛЮЧЕНИЯ

1 РАБОЧИЙ ДЕНЬ
РАЗРАБОТКА ДАШБОРДОВ

< 30 М ВРЕМЯ ПОДТВЕРЖДЕНИЯ
ИНЦИДЕНТА

ДО 4Х РАБОЧИХ ДНЕЙ
РАЗРАБОТКА КОННЕКТОРОВ

< 15 М ВРЕМЯ ОБНАРУЖЕНИЯ
ПОТЕНЦИАЛЬНОГО ИНЦИДЕНТА

< 90 М ВРЕМЯ РАССЛЕДОВАНИЯ
ИНЦИДЕНТА

КОНТАКТЫ

ОКСАНА ВАСИЛЬЕВА

Генеральный директор
Angara Professional Assistance

Email: acrc@angarapro.ru
Сайт: www.angarapro.ru
Телефон: +7-495-269-26-06

СЕРГЕЙ КОХАНЬКО

Руководитель службы информационной безопасности АО КБ «ЮНИСТРИМ»

Email: s.kokhanko@unistream.com
Сайт: www.unistream.com
Телефон: +7-495-225-01-79