Accenture Security

ACCENTURE SOC/SIEM Примеры

Подготовлено для SOC-Forum v 2.0

ИБ В АКСЕНЧЕР

Аксенчер. Информационная безопасность в числах

Аксенчер – международная компания, оказывающая услуги в области управленческого консалтинга, технологий и аутсорсинга. Обладая уникальной экспертизой, широчайшими возможностями во всех отраслях и направлениях экономической деятельности, а также глубоко изучая опыт наиболее успешных компаний мира, Аксенчер помогает повысить эффективность бизнеса своих Клиентов

20+ лет
опыта консалтинга в сфере ИБ

Сотрудники 3,400+

1 млн +
конечных систем под управлением

5,000+
рисков устраняется каждый год

350+
ожидающих решения и уже полученных патентов, связанных с ИБ

100 миллионов+
Предоставленных учетных записей

30 миллионов+
контролируемых учетных карточек

330+
Клиентов в 67 странах

Обработка
5млрд.+
событий ИБ каждый день

15,000+
обслуживаемых устройств ИБ

Достигнуто в
>30x
более быстрое обнаружение инцидентов

Анализ и обработка **миллиардов** событий ИБ

Управление крупнейшими системами мониторинга ИБ

Обеспечение облачной безопасности, управления и контроля для
20,000+
виртуальных машин

Центры компетенции
в Индии, Филиппинах, Чехии, США и Аргентине

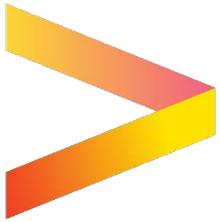
Ускорение процессов миграции в облачные среды на **20%** за счет оптимизации ИБ

Accenture Security

ВНЕДРЕНИЕ SOC В КРУПНЫЙ ЕВРОПЕЙСКИЙ БАНК

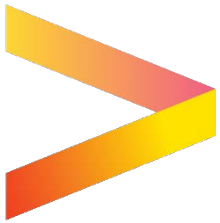
С чего все начиналось?

Синопсис



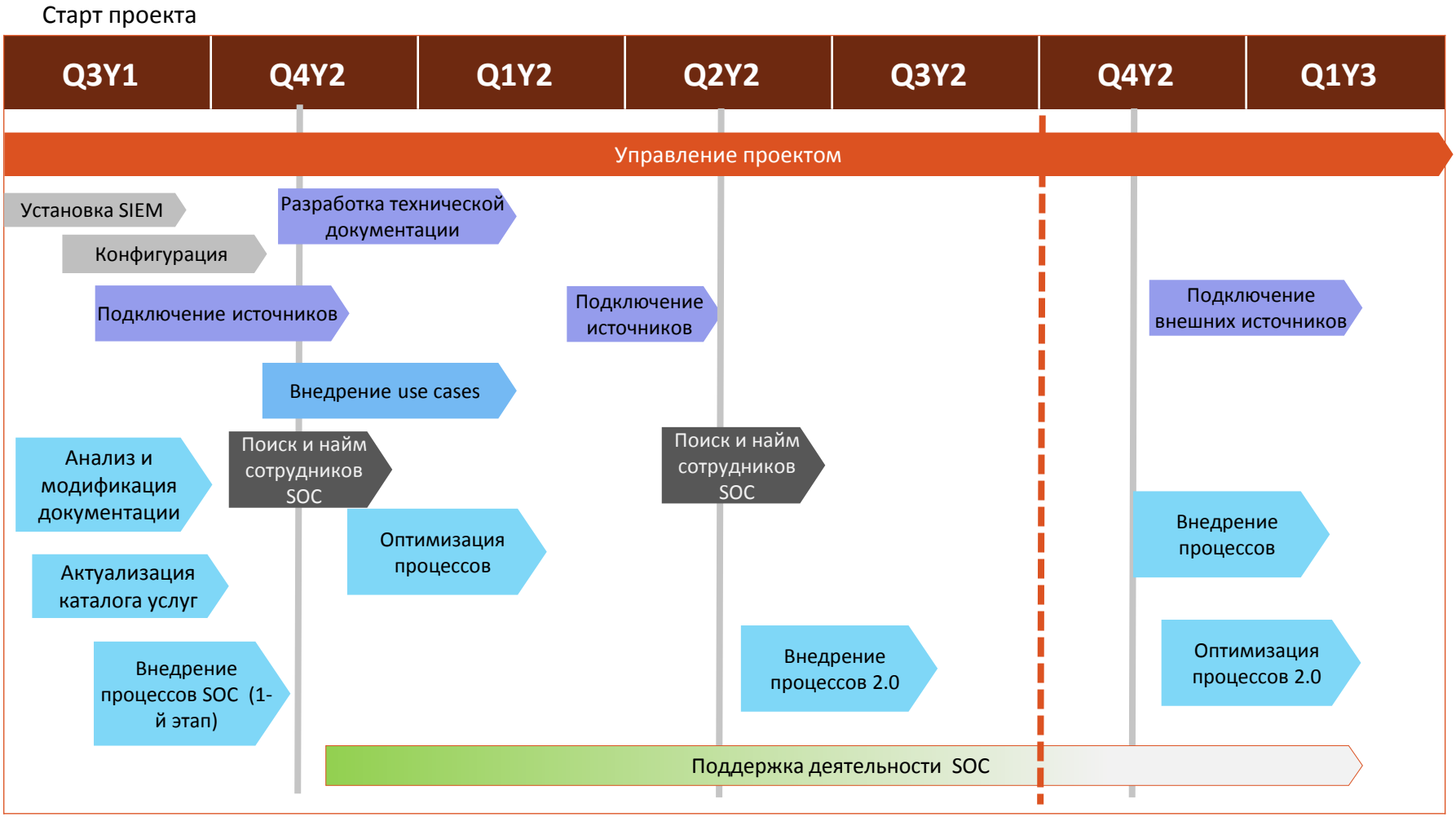
Клиент осуществил покупку дочернего Банка, в котором уже было внедрено решение по мониторингу ИБ. Однако, решение не соответствовало корпоративным стандартам Клиента, а также не имело поддержки производителя (линейку сняли с производства)

Задачи



- Оптимизация и трансформация функций ИБ дочернего Банка
- Compliance (соответствие корпоративным стандартам Клиента)
- **Соответствие новым уровням угроз – построение SOC**
- Разработка дорожной карты по ИБ
- Внедрение нового решения по мониторингу ИБ согласно корпоративному стандарту

Как мы это делаем?



Внимание: Сроки указаны приблизительно

Accenture Security

SOC: **постепенный рост**

Этап 1. Базовое внедрение

- Работа 5x8
- 4000 log sources
- 50 000 источников событий
- 100 000 network flows per minute
- 10 000 events per minute
- Реализация процесса управления инцидентами на основе SIEM
- Ограниченное количество событий
- Количество сотрудников SOC – 7-9

Внедрение SOC было разбито на 3 этапа: постепенное увеличение зрелости и управляемости

Этап 2. Продвинутое внедрение

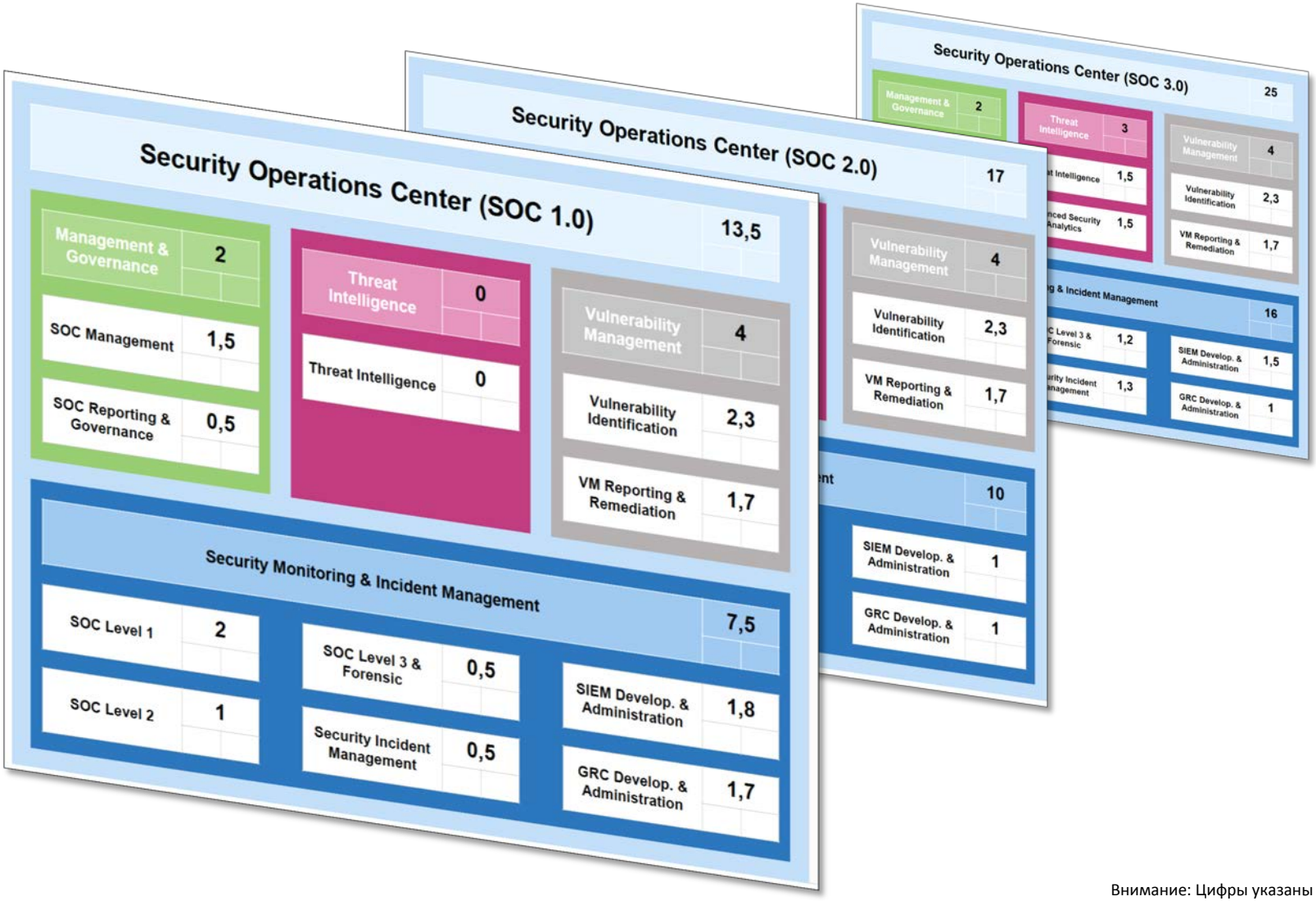
- Работа 5x16
- Количество сотрудников – 17
- + Управление угрозами
- Увеличение количества источников
- + 8 use cases
- Оптимизация существующих процессов

Этап 3. Целевое состояние

- Работа 7x24
- Реализация процесса анализа угроз и уязвимостей
- Оптимизация существующих процессов
- Внедрение использования внеіних источников информации об угрозах и уязвимостях
- 600 000 network flows per minute
- 40 000 events per minute

Дальнейшее совершенствование

Постепенный рост - конкретно



Внимание: Цифры указаны приблизительно

Accenture Security

Основные результаты

Рекомендации по улучшению документации по ИБ (мониторинг и управление инцидентами)

Документированные процессы операционной деятельности SOC

Рекомендации по изменению каталога услуг SOC

Оптимизированные процессы SOC (мониторинг, управление инцидентами, анализа и управления угрозами), включая KPI

Дорожная карта внедрения процессов и развёртывания SOC

Компетенции и требования к персоналу SOC для каждого этапа внедрения

Формирование организационной структуры SOC для каждого этапа внедрения

Передача знаний и операционная поддержка на начальных этапах проекта

Управление проектом

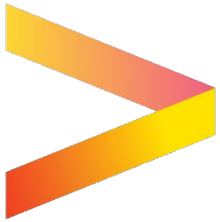
Помощь в подборе персонала

Интеграция с другими инициативами по ИБ

ВНЕДРЕНИЕ SIEM В КРУПНЫЙ БАНК ЕВРОПЫ

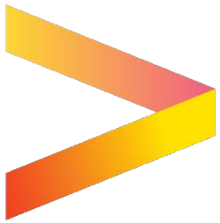
С чего все начиналось?

Синопсис



Клиенту требовалось оказание консультационных услуг при внедрении нового решения по мониторингу информационной безопасности, которое позволит реализовать новый функционал и заменит существующее решение.

Задачи



- Внедрение системы SIEM
- Настройка SIEM в соответствии с требованиями Клиента
- Разработка вариантов интеграции SIEM с другими системами
- В рамках проекта должны были быть разработаны:
  - 40 сценариев использования
  - 5 информационных панелей
  - 5 шаблонов отчетов
  - Несколько коннекторов

Подход к реализации

Требования и объём работ

- Какие будут сервисы?
- Разработка требований (обсуждали на семинаре)
- Анализ существующей архитектуры и функционала: что можно использовать, а что – нет
- Разработка и утверждение детального плана работ

Реализация SIEM была разбита на 3 части: от требований к развертыванию операций.

Техническая реализация

- Развертывание системы: подключение источников, доступ к данным.
- Настройка системы: внедрение use case, отчетности, правил корреляции и т.д.
- Разработка документации
- Тестирование системы с использованием тест-данных

Операционная реализация

- Обучение персонала Клиента использованию системы, проведение семинаров. Совместная работа Заказчика и Аксенчер
- «Живое» тестирование: оценивается возможность и удобство обработки событий с учетом процессов и технологий, разработанных в рамках проекта
- Сдача системы в промышленную эксплуатацию
- Доработка и устранение недостатков

Работоспособная система. Сотрудники Заказчика знают, как работать с этой системой.

СПАСИБО ЗА ВНИМАНИЕ!

КОНСТАНТИН СМИРНОВ
KONSTANTIN.SMIRNOV@ACCENTURE.COM