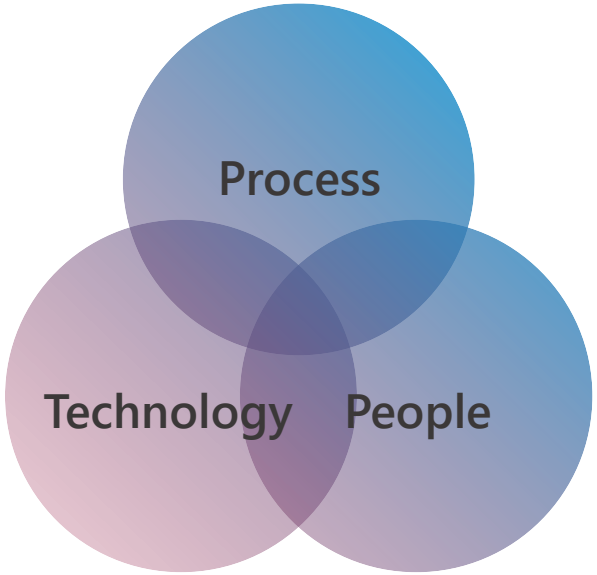

softline
We know we can
INFOSECURITY
a Softline company
Что такое SOC построить?
Александр Дворянский
«Инфосекьюрити»

SECURITY OPERATIONS CENTER



Three Interrelated Components
of ~~a SOC~~ Everything

В SOC реализованы функции мониторинга, оценки и защиты информационных систем

We know we can

softline®

INFOSECURITY
a Softline company

ЗАЧЕМ НУЖЕН SOC

ЦЕЛИ:

- Снижение рисков хищения данных и денежных средств
- Обеспечение непрерывности бизнеса
- Снижение тяжести последствий инцидентов
- Регуляторы…

РЕЗУЛЬТАТ:

- Выявление кибератак на ранних стадиях
- Максимально быстрый разбор инцидентов в большем количестве информационных систем

С ЧЕГО НАЧАТЬ

Определить защищаемые активы и основные угрозы

Оценить предполагаемые потери

Обосновать получение бюджета!

ВАРИАНТЫ ПОСТРОЕНИЯ SOC

ВНУТРЕННИЙ SOC

Компания сама или с помощью консультантов строит процессы, обучает специалистов, создает и поддерживает SOC

SOC AS SERVICE

Компания заключает договор с провайдером на сервис SOC с установленным SLA (Service Level Agreement)

ГИБРИДНЫЙ SOC

Компания делегирует часть функций SOC сервис-провайдеру, остальные функции поддерживает самостоятельно

	ISOC	**ISOC + PT MaxPatrol SIEM**

ВАРИАНТЫ ПОСТРОЕНИЯ SOC в чем разница

ВНУТРЕННИЙ SOC	SOC AS SERVICE	ГИБРИДНЫЙ SOC
Стоимость		
$$$ SIEM (Лицензия) $$$ Инфраструктура $$$ Внедрение системы $$$ Сервис 24/7	$ SIEM (Лицензия) $ Инфраструктура $$ Внедрение системы $$ Сервис 24/7	$$$ SIEM (Лицензия) $$$ Инфраструктура $$ Внедрение системы $$ Сервис 24/7
Скорость внедрения		
От 12 месяцев	3-4 месяца	6-12 месяцев
Преимущества		
Обработка и хранение событий на своей стороне	Гибкость в предоставлении сервиса	Обработка и хранение событий на своей стороне Гибкость в предоставлении сервиса

ОСНОВНЫЕ ПРОЦЕССЫ

01 | МОНИТОРИНГ

02 | ОЦЕНКА УГРОЗЫ

03 | ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

04 | ПОДДЕРЖКА ИНФРАСТРУКТУРЫ

ВИД СВЕРХУ

Аналитики
и инженеры

Дежурная смена
мониторинга

IRP
(SOAR)

Регламенты

SIEM
и не только

Threat
Intelligence

* Средства защиты

ОБЛАЧНЫЙ SOC

We know we can

softline

С ЧЕГО НАЧАТЬ

Выбрать провайдера

Определить объем сервиса

Подключить!

ПРЕИМУЩЕСТВА СЕРВИС-ПРОВАЙДЕРА

Экономия ресурсов

Снижаются затраты (оборудование, персонал) на инфраструктуру для управления инцидентами*

Фиксированные SLA

Клиент понимает, как быстро будет обработан инцидент или решен определенный вопрос

Решение проблемы кадров

Не нужно искать дорогих специалистов и обучать своих: сервис сопровождают профильные эксперты

Оперативная реакция

Сервис предоставляется в режиме 24/7, поэтому вся информация об угрозах и уязвимостях поступает своевременно

Ожидаемый результат

Затраты и сроки внедрения сервиса заранее определены договором с провайдером

Дополнительные сервисы

Сервис-провайдер может взять на сопровождение СЗИ и IT-инфраструктуру клиента

ЭТАПЫ ПОДКЛЮЧЕНИЯ

01 АНАЛИТИКА И КОНСАЛТИНГ

- Анализ инфраструктуры (ОС, СУБД, ПО, СЗИ, сетевое оборудование)
- Анализ текущих процессов сбора событий и реагирования на инциденты

02 ОРГАНИЗАЦИЯ КАНАЛОВ СВЯЗИ

- Получение доступов
- Настройка защищенного сетевого канала
- Настройка защищенного почтового канала

03 ПОДГОТОВКА ИНФРАСТРУКТУРЫ

- Настройка систем сбора и передачи событий
- Подключение источников
- Настройка оповещений и доступа к дашбордам

04 СОГЛАСОВАНИЕ ВЗАИМОДЕЙСТВИЯ

- Определение схемы подключения новых источников
- Определение схем оповещения об инцидентах и эскалации

05 СОГЛАСОВАНИЕ SLA

- Установление режима работы
- Определение приоритета и скорости реагирования на инциденты
- Определение параметров и сроков отчетности
- Выбор срока хранения данных

06 ВВЕДЕНИЕ В ЭКСПЛУАТАЦИЮ

- Тестирование
- Запуск мониторинга событий и реагирования на инциденты

НАШ ОПЫТ

2009 – 2015

SOC для одного заказчика

2015 – 2018

SOC для группы компаний

2018 – н.в

Облачный SOC

ЭКСПЕРТИЗА И ПРОЦЕССЫ ISOC

Эффективность работы SOC обуславливается рядом уникальных характеристик комманды «Инфосекьюрити»

9 лет управления инцидентами ИБ

База знаний и use case
по обработке инцидентов

Опыт предоставления
сервиса компании
с количеством сотрудников
35.000

Участник FIRST, статус CERT

Соглашение НКЦКИ позволяющее
выступать
в роли корпоративного центра ГосСОПКА
класса «А»

Использование актуальных данных
Threat Intelligence

Более 50 сотрудников участвующих
в мониторинге и реагировании
и более 70 профильных экспертов

КОМАНДА ISOC

В команде более 40 экспертов, занимающихся непосредственно мониторингом и расследованиями инцидентов.

Кроме того, с ними в непрерывном режиме взаимодействуют более 60 профильных инженеров по различным направлениям информационной безопасности.

ПЕРВАЯ ЛИНИЯ
Мониторинг и оповещение 24/7

ВТОРАЯ ЛИНИЯ
Анализ инцидентов 24/7

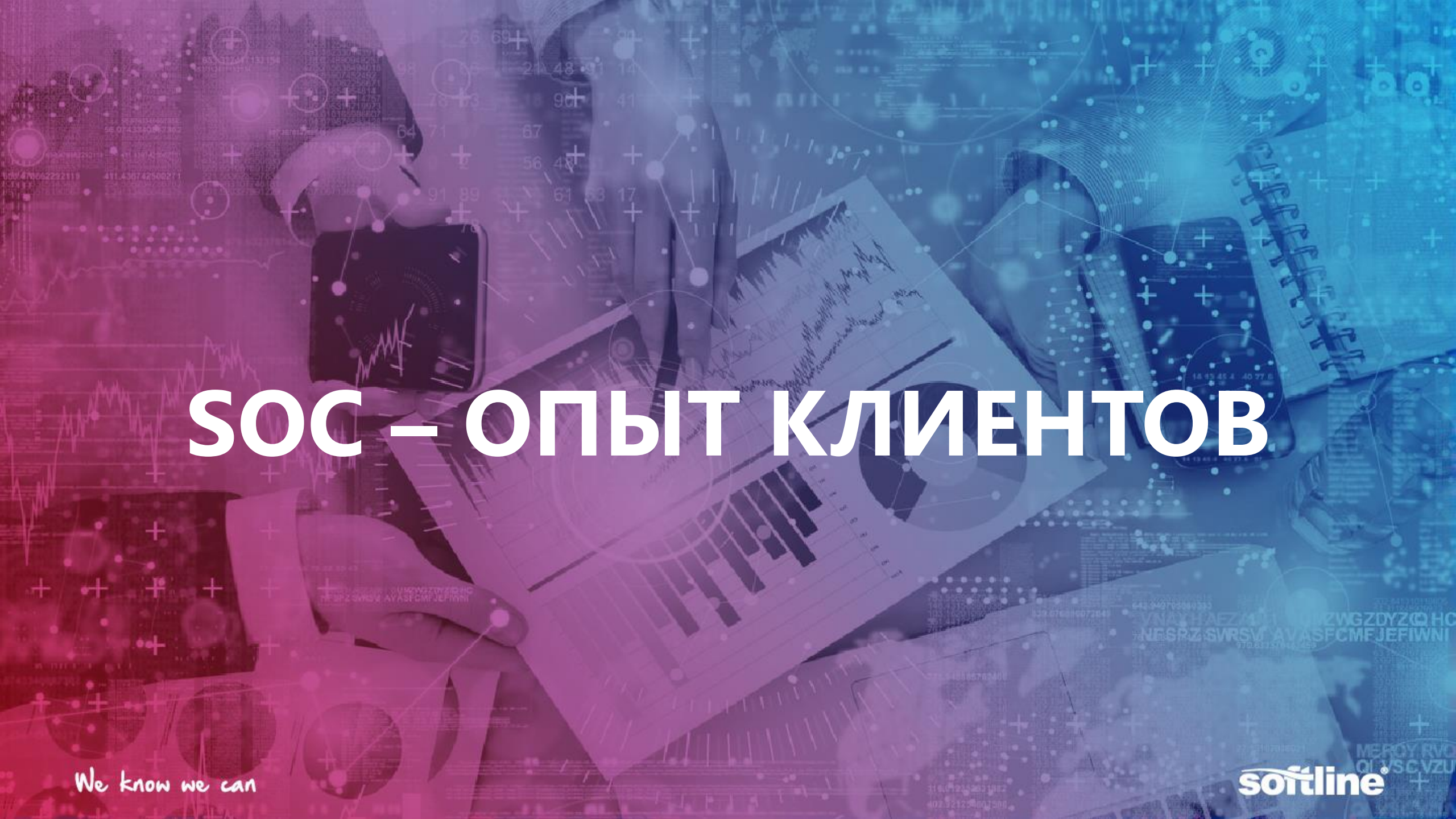
ТРЕТЬЯ ЛИНИЯ
Расследования 8/5

СЕРВИСЫ ИБ
Реагирование на инциденты 24/7

АНАЛИТИКА
Правила реагирования

РАЗРАБОТКА
Платформа и автоматизация

ЭКСПЛУАТАЦИЯ ISOC
Сопровождение инфраструктуры ISOC



SOC – ОПЫТ КЛИЕНТОВ

We know we can

softline

ЧАСТНАЯ ФИНАНСОВАЯ КОРПОРАЦИЯ

ЗАКАЗЧИК:

Крупный частный диверсифицированный финансовый холдинг в РФ.

ПРЕДПОСЫЛКИ ПРОЕКТА:

- Инциденты ИБ, которые привели к крупным финансовым потерям
- Больше 15 различных бизнесов, живущих в одной сетевой инфраструктуре
- Единая служба ИБ
- Основная часть сервисов ИБ на аутсорсинге

ИСТОРИЯ УСПЕХА:

Рассматривалось несколько вариантов решений SOC.
По результатам тестирования и сравнения методик был выбран ISOC за счет:

- Оптимальной стоимости (свои разработки + автоматизация)
- Наличие экспертизы и возможность оперативно реагировать на инциденты за счет централизации всех сервисов ИБ
- реализации на основе Big Data (обработка и хранение больших объемов)
- SLA высокого уровня (время реагирования, 24/7/365)

ГОСУДАРСТВЕННАЯ КОМПАНИЯ

ЗАКАЗЧИК:

1. ПАО Государственная транспортно-лизинговая компания.
2. (ГТЛК) – крупнейшая лизинговая компания России. ГТЛК обеспечивает реализацию государственной поддержки транспортной отрасли, формирование эффективной инфраструктуры, привлечение внебюджетных инвестиций, развитие отечественного машиностроения, наряду с цифровой трансформацией и повышением операционной эффективности компании.

ПРЕДПОСЫЛКИ ПРОЕКТА:

- Наличие дочерних структур за рубежом
- Разветвленная сетевая инфраструктура
- Требования ФЗ – 187
- Атаки зарубежными группировками хакеров

ИСТОРИЯ УСПЕХА:

Рассматривалось несколько решений SOC. По результатам тестирования и сравнения был выбран ISOC за счет:

- Оптимальной стоимости (свои разработки + автоматизация)
- Индивидуального подхода к требованиям клиента
- Гибридная реализация на базе PT SIEM
- SLA высокого уровня (время реагирования, 24/7/365)
- Статуса официального корпоративного центра ГосСОПКА
- Сертификации Infosecurity CERT университетом Карнеги-Меллон

СЕРВИС ISOC В SBI BANK

ЗАКАЗЧИК:

Зарубежный банк, принадлежащий японской корпорации SBI. Предлагает онлайн-решения по управлению семейными финансами, продукты и сервисы для предпринимателей, обслуживает крупных корпоративных клиентов. В России работает с 1994 года. Управляет инвестиционными фондами в размере $8.2 млрд. Основные клиенты — юридические лица.

ПРЕДПОСЫЛКИ ПРОЕКТА:

В 2018 году акционеры утвердили новую стратегию SBI Банка: сохранив сотрудничество с крупными корпоративными клиентами, выйти на российский рынок с комплексными решениями для розничных клиентов и предпринимателей.

Задача — новый уровень IT и ИБ:

- преобразовать IT-инфраструктуру
- защитить пользовательские данные
- максимально снизить репутационные риски

ИСТОРИЯ УСПЕХА:

Рассматривалось несколько решений SOC. По результатам тестирования и сравнения был выбран ISOC за счет:

- Оптимальной стоимости (свои разработки + автоматизация)
- Индивидуального подхода к требованиям клиента
- Реализации на основе Big Data (обработка больших объемов)
- SLA высокого уровня (время реагирования, 24/7/365)
- Статуса официального корпоративного центра ГосСОПКА
- Сертификации Infosecurity CERT университетом Карнеги-Меллон

ИТ - КОМПАНИЯ

ЗАКАЗЧИК:

ПРЕДПОСЫЛКИ ПРОЕКТА:

Оказание услуг по поддержке ИТ-инфраструктуры для государственных структур.

ИСТОРИЯ УСПЕХА:

Рассматривалось несколько решений SOC. По результатам тестирования и сравнения методик был выбран ISOC за счет:

- Оптимальной стоимости (свои разработки + автоматизация)
- SLA высокого уровня (время реагирования, 24/7/365)
- Статуса официального корпоративного центра ГосСОПКА

ВМЕСТО «СПАСИБО ЗА ВНИМАНИЕ»

ЛУЧШЕ ПРИЕЗЖАЙТЕ В ГОСТИ НА ЖИВУЮ ДЕМОНСТРАЦИЮ!

We know we can

softline®