ISOC:

ТРАНСФОРМИРУЕМ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Cloud | Security | Big Data | Mobility

Digital Transformation and Cyber Security Solution Provider

INFOSECURITY

softline 25 Years in IT

Зачем нужен SOC

ЦЕЛИ:

Снижение рисков хищения данных и денежных средств

Обеспечение непрерывности бизнеса

Снижение тяжести последствий инцидентов

РЕЗУЛЬТАТ:

Выявление кибератак на ранних стадиях

Максимально быстрый разбор инцидентов в большем количестве информационных систем

Варианты построения SOC

ВНУТРЕННИЙ SOC

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

PT SIEM+Сервис

SOC AS A SERVICE

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

ISOC

ГИБРИДНЫЙ SOC

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

ISOC + PT SIEM

Варианты построения SOC. В чем разница

ВНУТРЕННИЙ SOC	SOC AS A 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		
6-12 месяцев	3-4 месяца	4-6 месяцев
ПРЕИМУЩЕСТВА		
Обработка и хранение событий на своей стороне	Гибкость в предоставлении сервиса	Обработка и хранение событий на своей стороне Гибкость в предоставлении сервиса

Преимущества сервис-провайдера

ЭКОНОМИЯ РЕСУРСОВ

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

ФИКСИРОВАННЫЕ SLA

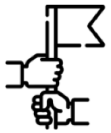
Клиент понимает, как быстро будет обработан инцидент или решен определенный вопрос

РЕШЕНИЕ ПРОБЛЕМЫ КАДРОВ

Не нужно искать на рынке дорогих специалистов или 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

Технологический состав SOC

В работе ISOC используются следующие основные технические компоненты:

ISOC SIEM

Система обработки событий ИБ и выявления инцидентов – собственная разработка «Инфосекьюрити».

Система включает в себя модуль аналитики, приемник событий, хранилище логов, транспортный модуль, модуль управления инцидентами. Дашборды и отчеты обеспечивают визуализацию данных.

ЗАЩИЩЕННЫЙ КАНАЛ СВЯЗИ

Подключение по протоколу TLS.

Канал может быть построен через Интернет или с помощью выделенной линии, соединяющей площадки клиента и ISOC.

Мы можем использовать сетевое оборудование клиента с функциями шифрования или предоставить свой криптошлюз.

СБОРЩИК СОБЫТИЙ

Сервер в инфраструктуре заказчика, который аккумулирует события с источников (системы управления средств защиты, рабочие станции и тд) и отправляет их по защищенному каналу в приемник событий на стороне ISOC.

КОННЕКТОР К ГОССОПКА

Модуль, обеспечивающий передачу информации об инцидентах в НКЦКИ в соответствии с требованиями 187-ФЗ «О безопасности критической информационной инфраструктуры»

ISOC IRP

Модуль автоматизации. При выявлении инцидентов подключается к узлу, где была зафиксирована потенциально опасная активность, собирает расширенную информацию и удаляет вредоносное ПО встроенным альтернативным антивирусом.

КОННЕКТОР К IRP

Сервер в инфраструктуре заказчика, обеспечивающий взаимодействие ISOC IRP с узлами под управлением ОС Windows и средствами защиты.

Экспертиза и процессы ISOC

Эффективность работы SOC обусловливается рядом уникальных характеристик компании «Инфосекьюрити».

8 лет опыта управления инцидентами ИБ

Участник FIRST, статус CERT, договор с ГосСОПКА

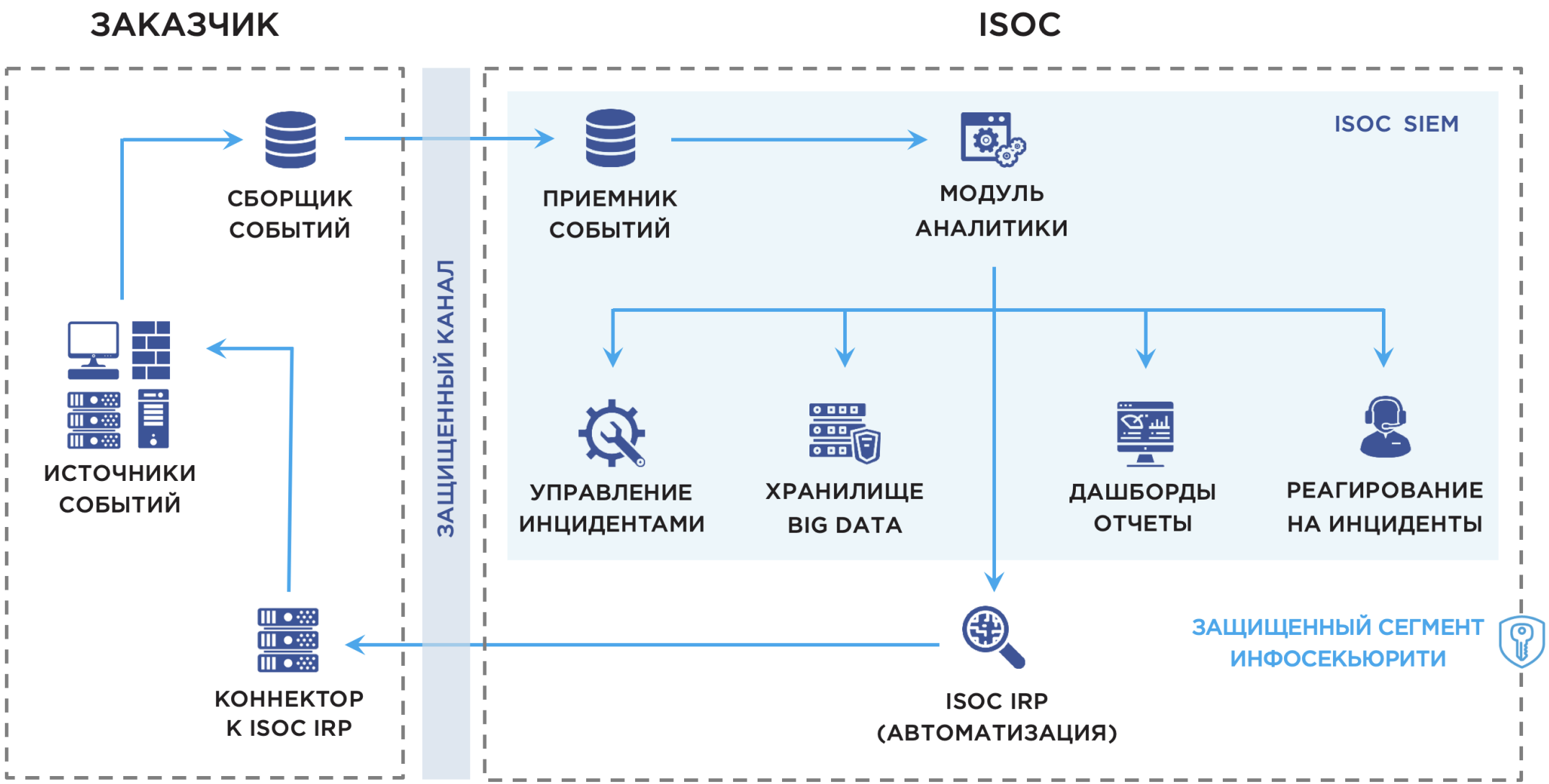
База знаний и use case по обработке инцидентов

Использование актуальных данных Threat Intelligence

Опыт предоставления сервиса в компании
на 30 000 сотрудников

30 сотрудников мониторинга и реагирования и 60 профильных инженеров

Архитектура взаимодействия



Как работает ISOC

Информация с источников

Клиент может выбрать необходимый набор услуг в зависимости от своих потребностей

МОНИТОРИНГ

1. СОЗДАНИЕ ЗАЯВКИ И EMAIL-ОПОВЕЩЕНИЕ
2. РАСШИРЕННОЕ ОПОВЕЩЕНИЕ ПО ТЕЛЕФОНУ

РЕАГИРОВАНИЕ

3. ПЕРВИЧНЫЙ АНАЛИЗ И ОБРАБОТКА ИНЦИДЕНТА
4. ПРИМЕНЕНИЕ КОНТРМЕР В ИНФРАСТРУКТУРЕ
5. ПОДКЛЮЧЕНИЕ ЭКСПЕРТА К ONLINE-АНАЛИЗУ
6. РАСШИРЕННАЯ ПОДДЕРЖКА И КОНСУЛЬТАЦИИ

Этапы подключения

Предварительный этап до начала работ — согласование договора, включая перечни источников, правила реагирования, ответственных лиц, параметры ценообразования.

1 АНАЛИТИКА И КОНСАЛТИНГ:

Анализ инфраструктуры (ОС, СУБД, ПО, средства защиты, сетевое оборудование)

Анализ текущих процессов сбора событий и реагирования на инциденты

2 ОРГАНИЗАЦИЯ КАНАЛОВ СВЯЗИ:

Настройка шифрованного сетевого канала

Настройка шифрованного почтового канала

Получение сетевых доступов и технических учетных записей

3 НАСТРОЙКА ИНФРАСТРУКТУРЫ:

Настройка сборщиков и приемщиков событий

Подключение источников

Настройка оповещений и доступов к дашбордам

4 СОГЛАСОВАНИЕ ВЗАИМОДЕЙСТВИЯ:

Определение схемы подключения новых источников

Определение схем оповещения об инцидентах и эскалации

5 СОГЛАСОВАНИЕ ПАРАМЕТРОВ SLA:

Установление режима работы

Выбор срока хранения данных

Определение приоритета и скорости реагирования на инциденты, а также параметров и сроков отчетности

6 ВВЕДЕНИЕ В ЭКСПЛУАТАЦИЮ:

Тестирование

Запуск мониторинга событий и реагирования на инциденты

Ценообразование

Стоимость сервиса ISOC рассчитывается исходя из нескольких параметров:

Режимы реагирования и работы третьей линии

РЕЖИМ

Количество инцидентов на обработку

ОБРАБОТКА

Объем инфраструктуры (источники разных типов)

МАСШТАБ

Кейс: продажа SOC в зарубежный банк

СТОИМОСТЬ ПРОЕКТА
Пилот:
1.1 млн ₽
Ежегодное обслуживание:
5 млн ₽

ЗАКАЗЧИК:
зарубежный банк, который предлагает онлайн-решения по управлению семейными финансами, продукты и сервисы для предпринимателей, обслуживает крупных корпоративных клиентов. В России работает более 20 лет. Управляет инвестиционными фондами в размере нескольких миллиардов долларов. Основные клиенты — юридические лица.

ПРЕДПОСЫЛКИ ПРОЕКТА

В 2018 году акционеры утвердили новую стратегию 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 первого этапа после сравнения методик и возможностей были отобраны ISOC и Solar JSOC. Выиграли конкурс за счет:

- низкой стоимости (собственные разработки + автоматизация)
- индивидуального подхода к требованиям клиента
- реализации на основе BigData (обработка больших объемов)
- SLA высокого уровня (время реагирования, 24/7/365)
- статуса официального корпоративного центра ГосСОПКА
- сертификации Infosecurity CERT университетом Карнеги-Меллон

Наши клиенты


GO GLOBAL
GO CLOUD
GO INNOVATIVE