DLP:
ОТ ПОДБОРА К АНАЛИТИЧЕСКОМУ СОПРОВОЖДЕНИЮ

ЗАЧЕМ НУЖНА DLP-СИСТЕМА

DLP (Data Loss Prevention)

Система для предотвращения утечек конфиденциальной информации, проведения расследований и мониторинга сотрудников

Цели

- Снижение количества и тяжести последствий от утечки данных
- Оценка продуктивности и лояльности сотрудников

Задачи

- Контроль всех потоков информации, пересекающих периметр
- Выявление фактов хранения и передачи конфиденциальной информации вне бизнес-процессов
- Проверка соблюдения регламентов и процедур
- Разоблачение мошеннических схем
- Расследование инцидентов

КОМУ ПОМОЖЕТ DLP-СИСТЕМА

01 Собственники бизнеса, ТОП-менеджмент

предотвращение ущерба / возврат потерь

исполнение требований законов

формирование доказательной базы

обнаружение уязвимостей
в бизнес-процессах

02 Служба безопасности

контроль взаимодействия с партнерами

поиск инсайдеров

контроль неформальных связей в организации
и нетипичных контактов

защита наиболее критичных процессов
и ценных кадров

03 Служба информационной безопасности

предотвращение утечек КИ

контроль движения КИ

дополнительные сведения
по инцидентам

04 Функциональные руководители, HR

эффективность сотрудников

обстановка в коллективе

уязвимость и лояльность сотрудников

ВЕНДОРНЫЕ РЕШЕНИЯ

INFOWATCH®

SEARCHINFORM
INFORMATION SECURITY

Гарда Предприятие
Защита от утечек информации

Solar Dozor

falcongaze

STAFFCOP

ZECURION

DeviceLock DLP

Стахановец
система контроля сотрудников

Symantec™

FORCEPOINT
POWERED BY Raytheon

McAfee™
Together is power.

НАШИ УСЛУГИ

1 ПЕРВИЧНАЯ КОНСУЛЬТАЦИЯ

2 ПОДБОР ПОДХОДЯЩЕЙ DLP

3 ПОСТАВКА DLP-РЕШЕНИЯ

4 ПИЛОТ DLP

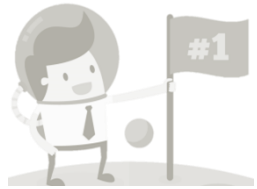
5 ВНЕДРЕНИЕ DLP

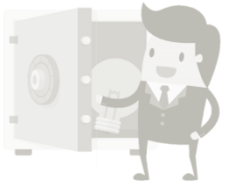
6 ОБУЧЕНИЕ

ПЕРВИЧНАЯ КОНСУЛЬТАЦИЯ

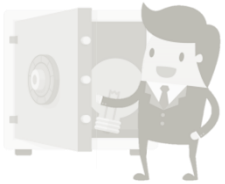
ОПИСАНИЕ УСЛУГИ

- Поможем определить потребности и задачи в рамках проекта по внедрению или сопровождению DLP-решения
- Проконсультируем по возможностям использования информации из DLP-системы сразу несколькими подразделениями для выявления рисков в их зоне ответственности



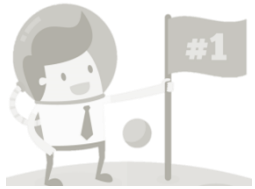


ПОДБОР ПОДХОДЯЩЕЙ DLP



ОПИСАНИЕ УСЛУГИ

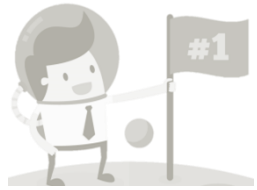
- Проведем экспертную оценку рынка и дадим рекомендации по наличию необходимого функционала среди различных решений
- Сравним возможности различных решений по критериям клиента
- Оценим функционал конкретного решения. Акцентируем внимание на сильных и слабых сторонах



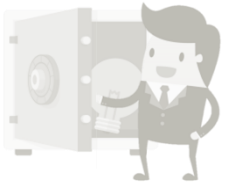
ПОСТАВКА DLP-РЕШЕНИЯ

ОПИСАНИЕ УСЛУГИ

- Поможем сформировать запрос на покупку с оптимальным объемом функционала при адекватной стоимости
- Предоставим дополнительную скидку

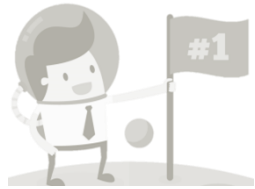


ПИЛОТ DLP



ОПИСАНИЕ УСЛУГИ

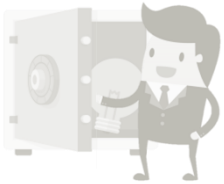
- Подготовим информацию
  об основных преимуществах
  и недостатках тестируемой системы
- Проведем пилотное внедрение
- Настроим систему и выявим
  потенциальные инциденты
- Наглядно продемонстрируем
  основные принципы работы
  и озвученные особенности системы



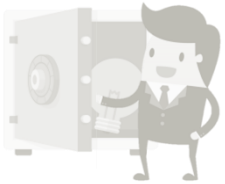
ВНЕДРЕНИЕ DLP

ОПИСАНИЕ УСЛУГИ

- Разработаем архитектуру решения и ТЗ для будущего проекта
- Проведем промышленное внедрение ПО
- Настроим политики выявления критичной информации
- Предоставим рекомендации по снижению рисков



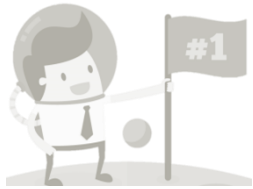
ОБУЧЕНИЕ



ОПИСАНИЕ УСЛУГИ

Проконсультируем по организации продуктивного использования системы:

- Как оптимально контролировать утечку данных
- Как собрать информацию для проведения расследования
- Как выявлять потенциальные риски и нецелевое использование ресурсов
- Как поддерживать настройки системы в актуальном состоянии



АУТСОРСИНГ

1 АНАЛИТИЧЕСКОЕ СОПРОВОЖДЕНИЕ

2 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

3 ДОКУМЕНТАЛЬНОЕ И ЮРИДИЧЕСКОЕ КОНСУЛЬТИРОВАНИЕ

4 ПРЕДОСТАВЛЕНИЕ ОБЛАКА

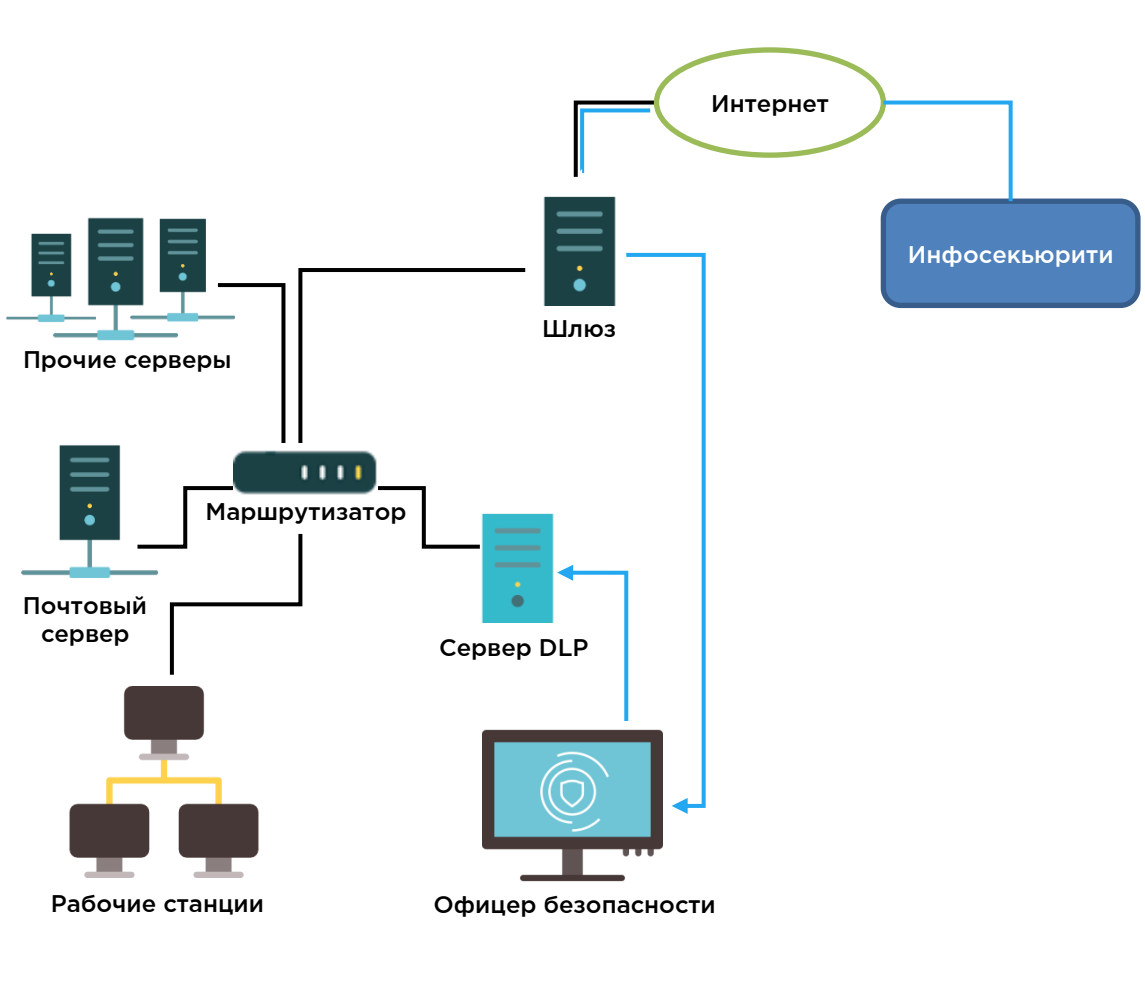
СХЕМА РЕАЛИЗАЦИИ

1 Выявление потребностей и определение SLA

2 Подписание NDA

3 Согласование доступов и учетных записей

4 Обмен информацией



АНАЛИТИЧЕСКОЕ СОПРОВОЖДЕНИЕ

МОНИТОРИНГ КАНАЛОВ

- Контроль обработки, передачи и хранения конфиденциальной информации
- Предварительный ручной анализ всех событий
- Описание каждого потенциального инцидента (анализ содержимого файлов, нарушенных регламентов и дополнительных факторов риска)

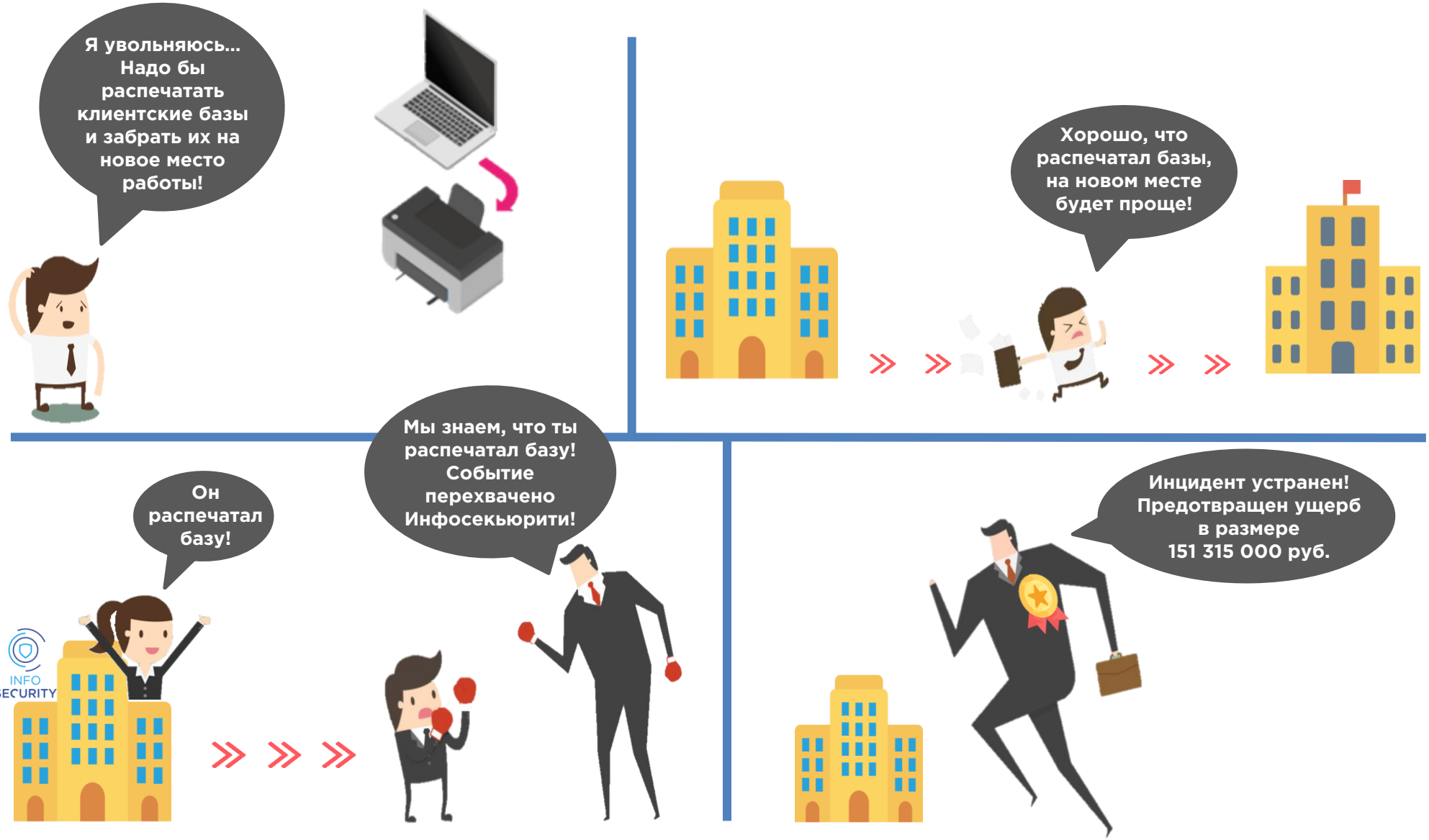
РАССЛЕДОВАНИЯ

- Обработка запросов в свободной форме от различных структур клиента
- Предоставление подробного отчета и сопутствующих материалов по итогам расследования
- Поиск информации как по случаям утечки данных, так и по любым процессам компании

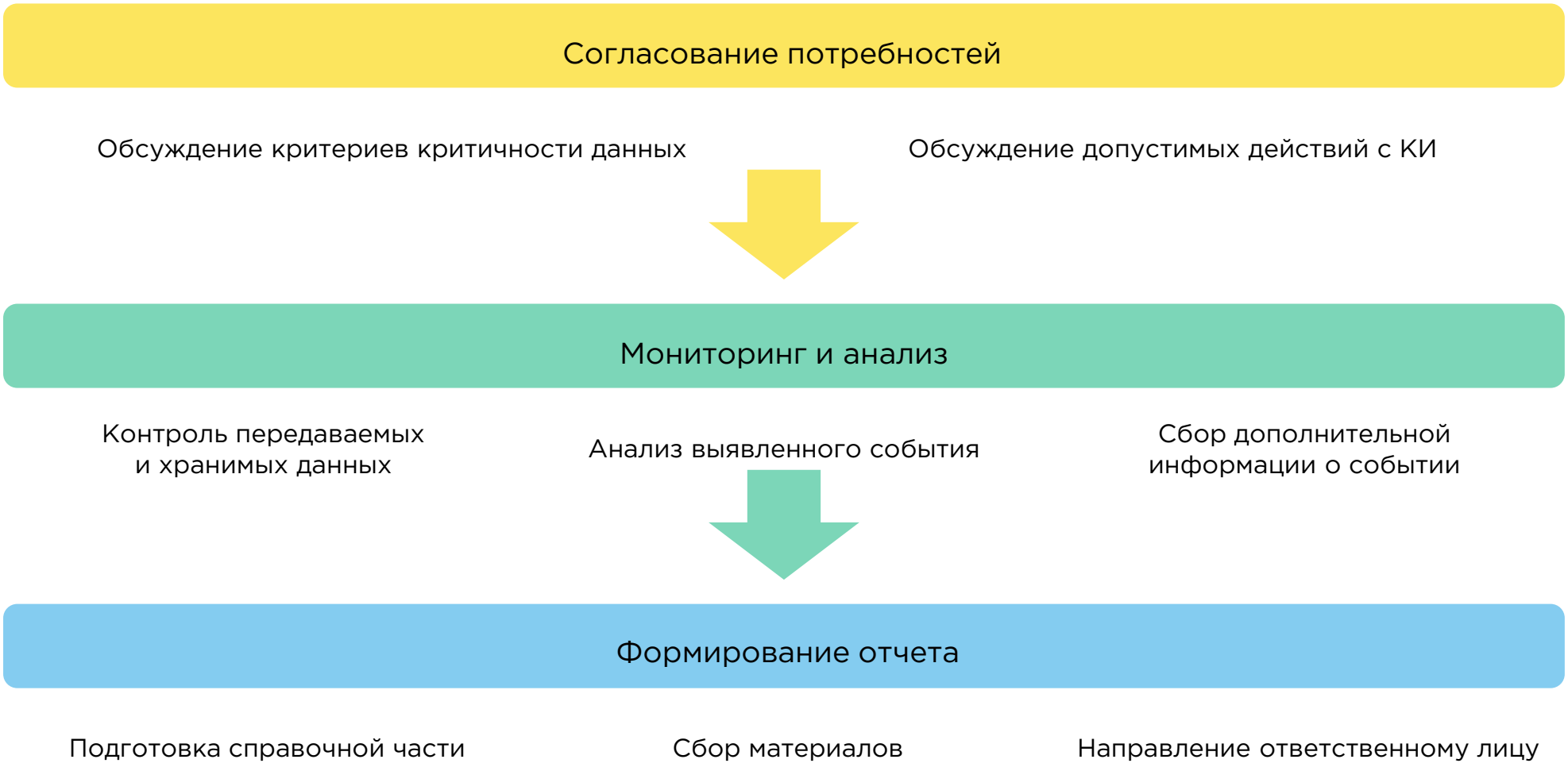
ПРОФИЛИРОВАНИЕ

- Анализ эффективности работы сотрудников (интернет-активность, запуск приложений, периоды бездействия)
- Выявление групп риска в коллективе (зависимость, конфликтность, широкие полномочия)
- Контроль лояльности ключевых сотрудников

МОНИТОРИНГ КАНАЛОВ. КАК ЭТО РАБОТАЕТ?

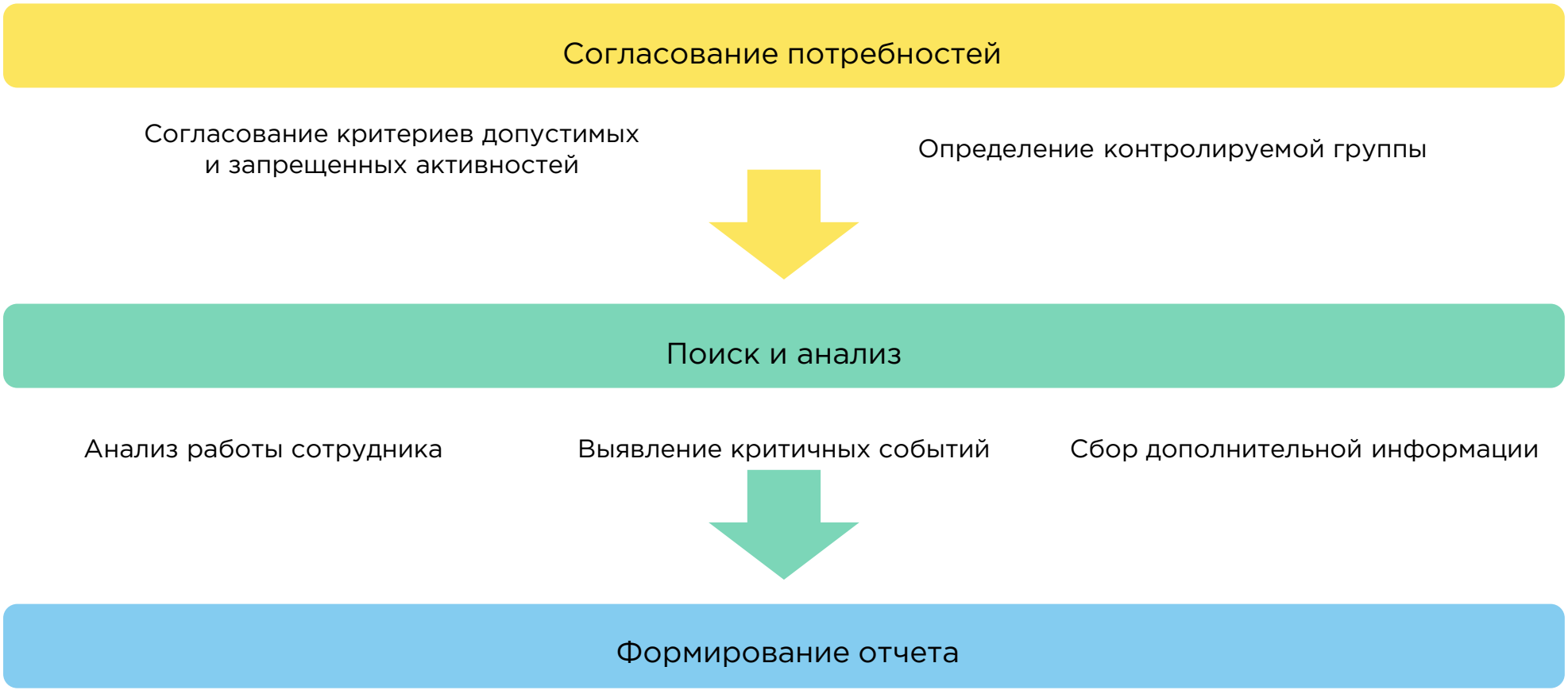


МОНИТОРИНГ КАНАЛОВ. ЭТАПЫ

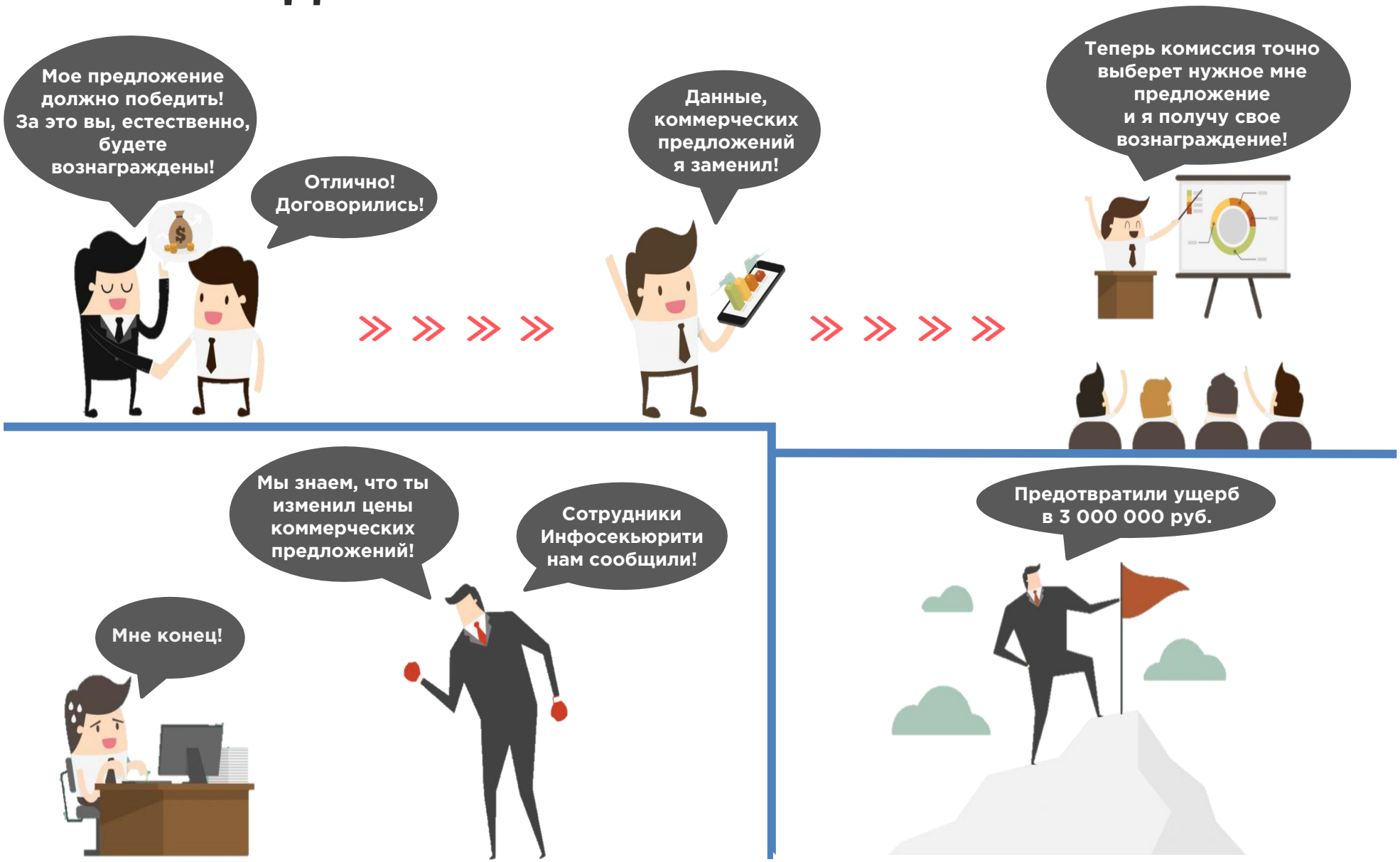


ПРОФИЛИРОВАНИЕ

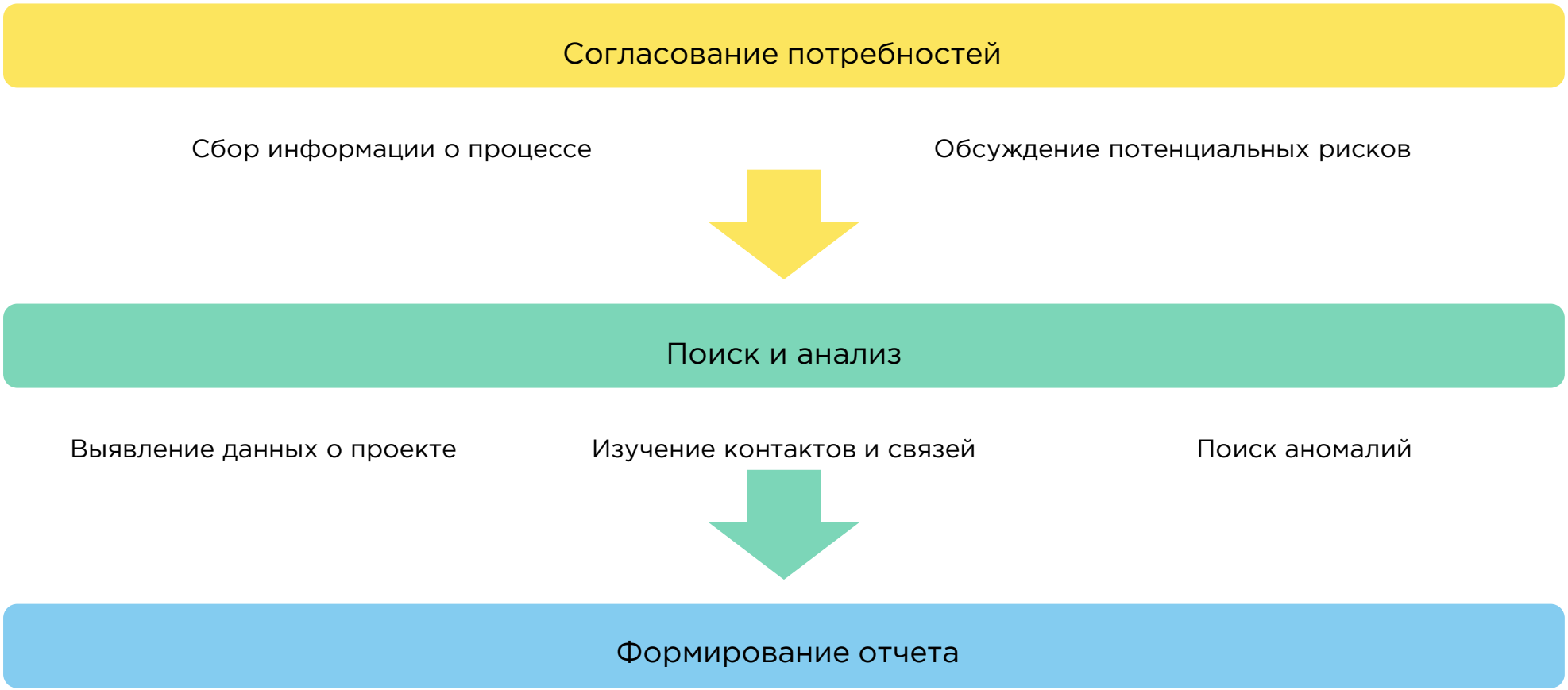
ПРОФИЛИРОВАНИЕ. ЭТАПЫ



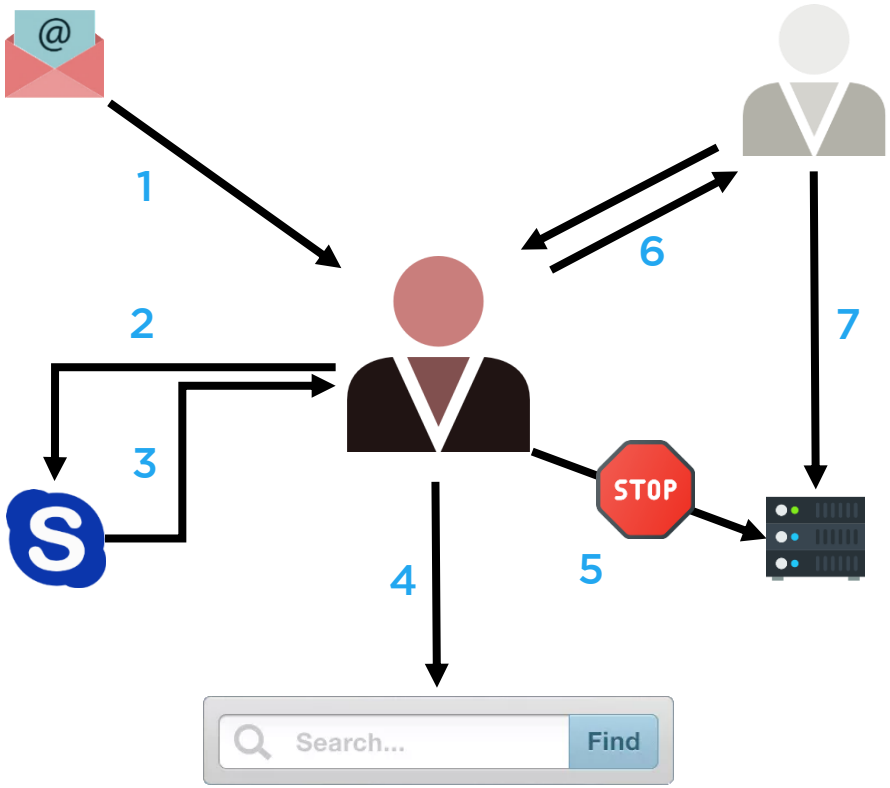
РАССЛЕДОВАНИЯ



РАССЛЕДОВАНИЯ. ЭТАПЫ



ПОИСК И АНАЛИЗ



Все ЭТИ действия прямо или косвенно фиксируются DLP системой.

1. Сотруднику компании на корпоративную почту приходит коммерческое предложение (КП) от поставщика.
2. Сотрудник в мессенджере сообщает, что готов помочь победить в тендере за вознаграждение.
3. Поставщик соглашается.
4. Сотрудник ищет в поисковом сервисе, как поменять готовые КП в базе данных.
5. Сотрудник пытается получить доступ в базу данных, где хранятся КП. Ему это не удается.
6. Сотрудник обращается к своему коллеге за помощью и предлагает поделить вознаграждение. Коллега соглашается.
7. Коллега получает доступ в базу данных и меняет поступившие от других компаний КП.

Совершены мошеннические действия. Данные изменены!

ПОДДЕРЖКА

ТЕХНИЧЕСКАЯ

- Проконсультируем по любым вопросам в части DLP-решений
- Проверим, как функционирует установленное решение, и исключим возможность перебоев

ДОКУМЕНТАЛЬНАЯ

- Обновим документацию по работе с коммерческой тайной до актуального состояния
- Проконсультируем при обработке запросов регуляторов и контрагентов

ЮРИДИЧЕСКАЯ

- Поможем составить заявления и обращения в правоохранительные органы

ПРЕДОСТАВЛЕНИЕ ОБЛАКА

ОПИСАНИЕ УСЛУГИ

Вся собираемая информация по защищенному каналу передается на отказоустойчивые серверы обслуживаемые Инфосекьюрити.

Организуем техническую поддержку и своевременное обновление системы

МИФЫ И ЗАБЛУЖДЕНИЯ

Вы получите доступ к нашей критичной информации

- Регулярные проверки сотрудников на полиграфе, в т.ч. по запросу заказчика
- Настройка ограниченного доступа / списки исключений
- 8 лет безупречной репутации (соблюдение NDA)

Мы становимся вашими заложниками

- Вы имеете доступ ко всем хранилищам информации и можете самостоятельно проверять достоверность предоставляемой информации

Слишком дорого

- Калькулятор для расчета стоимости = гибкость
- Потери от инцидента могут быть фатальны для компании
- Нет проблем с наймом и содержанием в штате собственной команды аналитиков, которых очень сложно искать

Зачем тогда нам СБ и ИБ?

- Отлаженный процесс взаимодействия с СБ/ИБ - дополняем, а не заменяем. Повышается эффективность и результат работ
- Они смогут освободить свои ресурсы и заняться другими важными задачами

Куда мы теперь денем нашу DLP? Она вам не подойдет?

- Имеем опыт работы со всеми представленными на рынке отечественными DLP-системами, знаем их сильные и слабые стороны

О КОМПАНИИ

Преимущества

Сотрудничество с ТОП-5 российских финансовых структур с 2010 года

Наличие высококвалифицированных кадров, умеющих работать в том числе с Big Data

Предоставление различных вариантов лицензирования, пакетных услуг аутсорсинга и скидок

Работа в соответствии с утвержденными параметрами SLA

Оперативная наладка процессов взаимодействия с подразделениями заказчика

Непредвзятое отношение при выявлении и разборе инцидентов

Пример внедрения

Более 30 000 пользователей

Филиальная сеть по всей России

Срок хранения данных более 5 лет

В среднем за год:

- 3000 инцидентов на обработку
- 300 запросов на расследования
- 200 человек на особом контроле ежедневно

gk-is.ru