falcongaze®

Кейс клиента

Нелояльность сотрудников | Утечка информации | Внутренняя угроза

Переманивание сотрудников

В этом кейсе мы рассмотрим, как с помощью DLP-системы Falcongaze SecureTower удалось выявить факт переманивания сотрудника недобросовестным контрагентом и предотвратить хищение чувствительных данных компании.

Проблема

В связи с существенным расширением штата логистическая компания, специализирующаяся на рефрижераторных перевозках по России, столкнулась с необходимостью усилить контроль за действиями сотрудников, потому что:

- у них есть доступ к клиентским базам и маршрутам, они точно знают цены на услуги и могут передать их конкурентам;
- утечка персональных данных клиентов и сотрудников влечет за собой материальные и репутационные риски, а также штрафы от регуляторов;
- находить, обучать и вводить в должность новых логистов — это дорого и затратно по времени;
- сфера работы компании — доставка охлажденной замороженной продукции, сбои в процессах могут повлечь издержки от 200 000 до 5 000 000 рублей.

Решение

Для защиты конфиденциальной информации, а также для обеспечения контроля за работой всех логистов компания приобрела SecureTower.

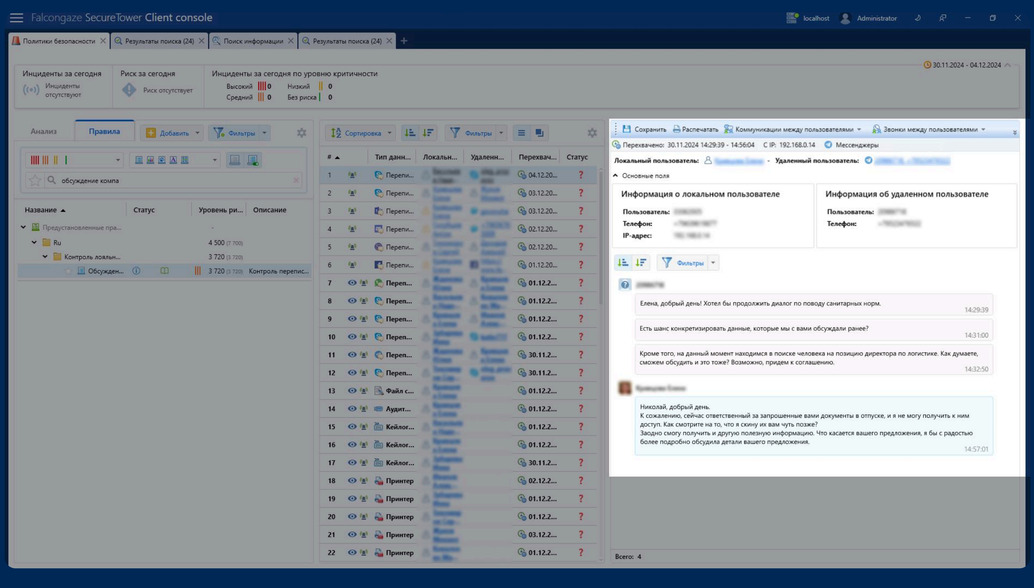
Система перехватывала и анализировала данные в таких каналах:

- электронная почта по протоколам SMTP, IMAP, MAPI и их шифрованным аналогам;
- мессенджеры (Telegram, Viber, Skype и еще 15 менее популярных аналогов);
- интернет (посещенные сайты, социальные сети, web-версии электронной почты, облачные хранилища и проч.);
- локальные и сетевые принтеры;
- буфер обмена;
- подключаемые устройства с внешней памятью и проч.

По истечении второго месяца использования SecureTower оповестила о сработке двух стандартных правил безопасности «Поиск новой работы» и «Обсуждение компании». Нарушителем значился один из опытных логистов.

Система среагировала на переписку в Telegram с одним из контрагентов, заключившим договор на оказание услуг по перевозке охлажденной и замороженной продукции авторефрижераторами.

В перехваченных сообщениях контрагент рассказывал о перспективе открыть логистическое направление в своей компании, консультировался о том, какие автомобили будут отвечать задачам бизнеса, а также задавал вопросы по соблюдению санитарных и гигиенических норм при обработке транспорта. Также добавил, что присматривает человека на должность директора по логистике, указал примерный уровень заработной платы. При этом обсуждались не только рабочие, но и личные вопросы.

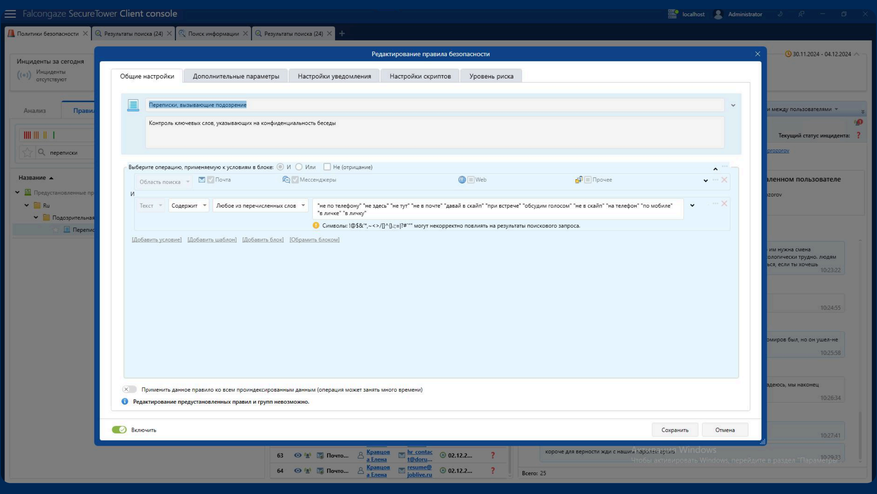


Модуль «Политики безопасности» (область поиска — почта, мессенджеры)

Логиста взяли на дополнительный контроль. Были созданы правила, ограничивающие для данного пользователя копирование информации на внешние ресурсы: в облачные хранилища, на почтовые сервисы, USB-устройства с внутренней памятью и проч.

На заметку! Для легитимного внедрения DLP-системы необходимо под подпись проинформировать сотрудников о том, что с целью контроля качества выполняемых работ работодатель в праве осуществлять контроль деятельности персонала, в том числе с использованием электронно-информационных средств.

Спустя две недели SecureTower оповестила о сработке двух предустановленных правил безопасности: «Переписки, вызывающие подозрения» и «Обсуждение компании».

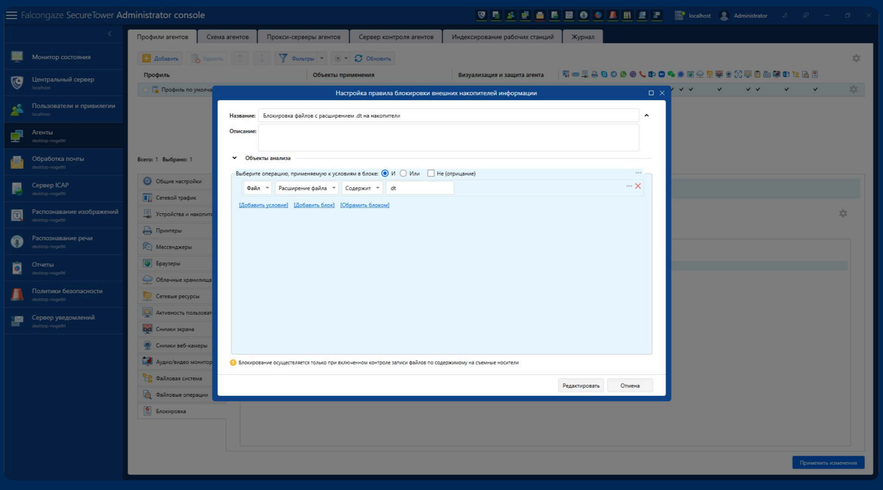


Модуль «Политики безопасности» (настройки правила безопасности)

В тексте переписки логист критически отзывался о руководителе и говорил о том, что недоволен текущим уровнем заработной платы и отношением к себе — и по истечении контракта планирует уходить из компании. В этой же переписке представитель контрагента предложил продолжить разговор по личному телефону.

Демотивированному логисту сообщили, что с ним не будут продлевать контракт. В качестве причины разрыва трудовых отношений показали переписку с контрагентом.

Вскоре SecureTower оповестила офицера безопасности о попытке копирования файла с расширением .dv на съемный флеш-носитель. Попытка хищения была зарегистрирована в нерабочее время и пресечена правилом блокировки.



Консоль Администратора (Правило блокировки внешних накопителей информации)

Удалось установить, что сотрудник задержался на работе после 18:00 под предлогом, что нужно завершить задачи, и выгрузил базу клиентов из 1С. Затем отключил рабочую станцию от интернета и попытался сохранить документ на USB-флешку. Несмотря на отсутствие связи с сервером, система заблокировала передачу.

На заметку! DLP-система SecureTower перехватывает данные даже при отсутствии связи с сервером и, если это было настроено в системе, блокирует нежелательные операции с файлами.

Результат

- **Выявлен нелояльный сотрудник**

  До завершения срока действия контракта логиста отправили на удаленку, чтобы он не демотивировал остальных сотрудников. Также были отозваны доступы от сервисов и систем компании.

- **Пресечено хищение чувствительных данных**

  SecureTower предупредила хищение данных более чем 40 клиентов компании. Речь идет в первую очередь о тарифах и фиксированных ставках. Помимо этого, система защитила номера телефонов, юридический и фактический адреса, адреса складов, а также отчеты и другую чувствительную информацию.

- **Завершено сотрудничество с недобросовестным контрагентом**

  В связи с недобросовестным поведением со стороны контрагента сотрудничество было завершено.

Модули, которые были использованы:

🚨 Политики безопасности

Активность пользователей

falcongaze®