INFOWATCH®

Новые возможности в продуктах InfoWatch и практика их применения

2023

Светлана Марьясова

Заместитель руководителя направления по развитию бизнеса на территории СФО и УрФО

Статистика утечек данных в январе — феврале 2023

INFOWATCH®

на **70%** больше, чем за январь — февраль 2022

26 утечек баз данных с количеством записей >100 000 в каждой

Источник: Экспертно-аналитический центр InfoWatch, предварительные данные, 2023

— Получите аналитические отчёты ЭАЦ InfoWatch бесплатно!

2023 —

гибридный вектор воздействия

Сотрудник вольно или невольно становится одним из звеньев атак

Неприятности случаются.
Поэтому важен полный контроль

— **Контролировать все необходимые каналы коммуникаций,** включая все облака и веб-сервисы вне зависимости от протокола

— **Защищать все важные документы и бланки,** даже если о новом типе документа не сообщили службе ИБ

— **Понимать тематику переписки** — или телефонных переговоров!

— **Прогнозировать нарушения,** даже если они только готовятся

— **Соответствовать требованиям** по импортозамещению

INFOWATCH®

InfoWatch Traffic Monitor — система защиты от утечек информации на основе технологий искусственного интеллекта

- Контролирует ВСЕ необходимые каналы
- НАХОДИТ то, что пропускает любая другая система защиты от утечек
- Покажет ВСЕХ ПРИЧАСТНЫХ к инциденту
- Позволяет увидеть ПОДГОТОВКУ инцидента
- АВТОМАТИЗИРУЕТ настройку политик безопасности

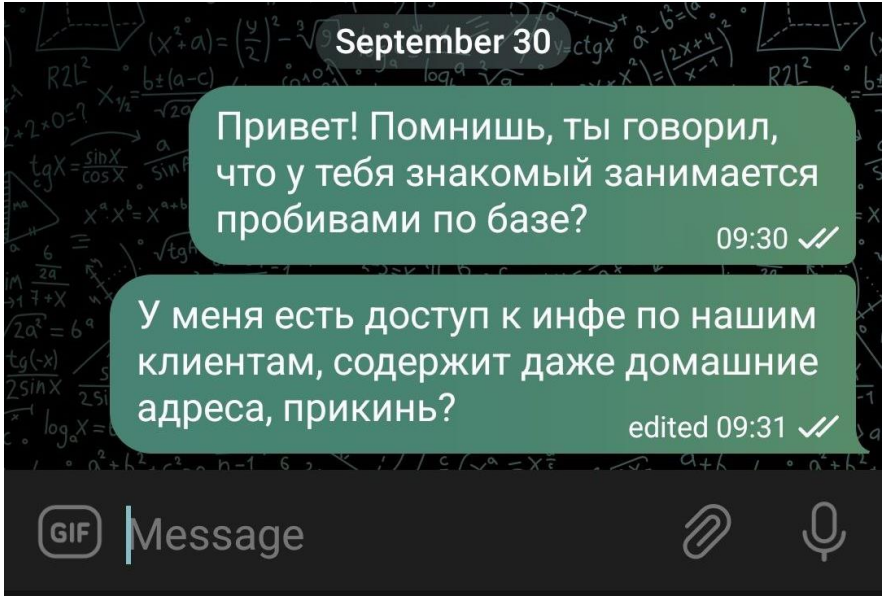
Понимаем тематику документа и даже простой переписки

У многих наших клиентов до 20 словарей одновременно. И регулярно появляются новые категории документов.

— **289 категорий**
— **Учитываем транслит, опечатки, литспик**
— **42 языка, 20 — с полной морфологией**

— Авиапромышленная
— Автопромышленная
— Агропромышленная
— Атомная
— Банковская
— Геологическая
— Госструктуры
— Гостайна
— Железнодорожная
— Инженерно-производственная
— Ислам
— Исходный код
— Космическая
— Медицинская
— МФЦ
— Налоговая
— Нарушение законодательства
— Нелояльные сотрудники
— Нефтегазовая
— Нецензурная лексика
— Религиозная
— Страховая
— Строительная
— Судостроение
— Таможенная
— Телекоммуникационная
— Торговая
— Транспортировка нефти
— Фармакологическая
— Христианство
— Экстремизм
— Энергетическая
— ...

Понимаем тематику документов и переписки



— **Девиантное поведение**
9 320 терминов

— **Пагубные привычки и зависимость**
4 440 терминов

— **Проблемы с законом, задолженности**
5 000 терминов

— **Геополитика**
3 категории, 6 подкатегорий

— **Мошенничество и угроза ИБ**
1 категория, 17 подкатегорий

БКФ соответствуют актуальной повестке

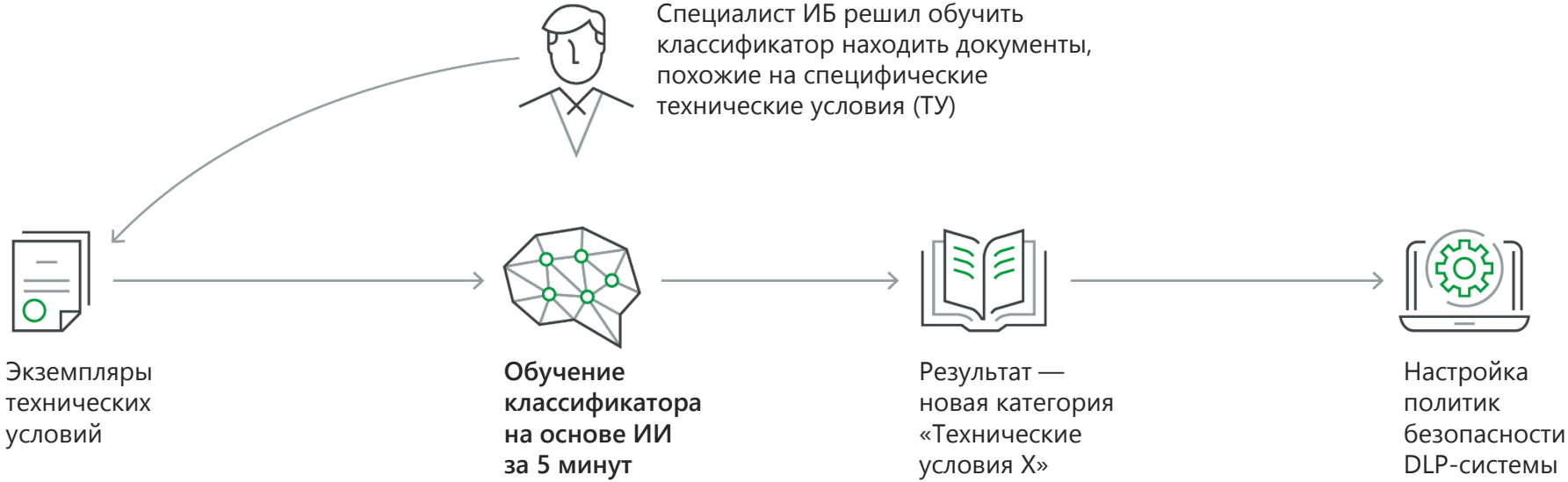
Автоматическое обучение системы защиты от утечек информации

INFOWATCH®

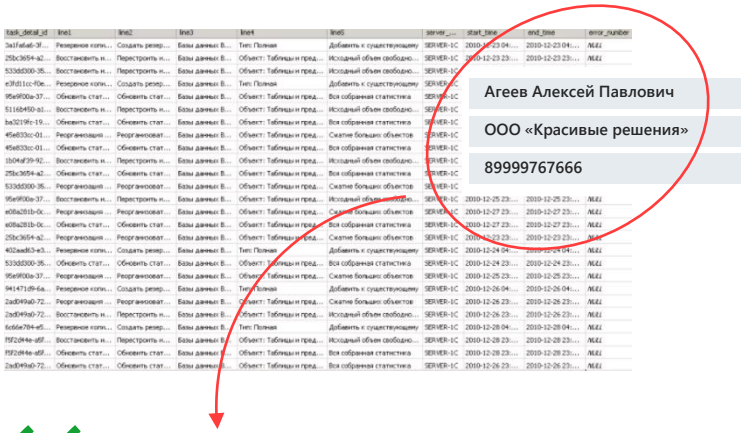
На документах заказчика

Без привлечения экспертов-лингвистов

ВСЕ документы за 1 час, а не 10 дней



Предотвращаем утечку ПДн клиентов и другой информации из баз данных



- Контролируем движение конкретных данных, а не просто доступ к базе
- Скорость — 100 000 000 записей в секунду
- Защищаем актуальные данные — динамическое обновление
- Несколько критериев срабатывания, например, комбинации полей и порция переданных данных

— Есть что для меня?

— Записывай: Алексей Палыч Агеев, 89999767666, директор компании «Красивые решения»

— Ага

— Звони после обеда, пока добрый

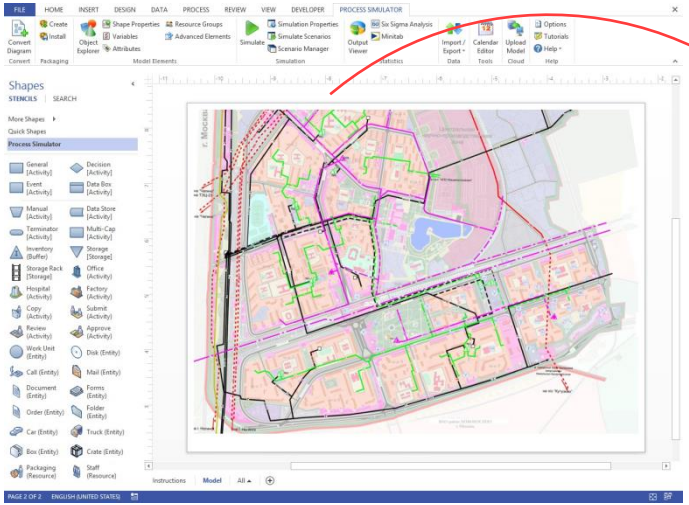
— Бюджеты есть?

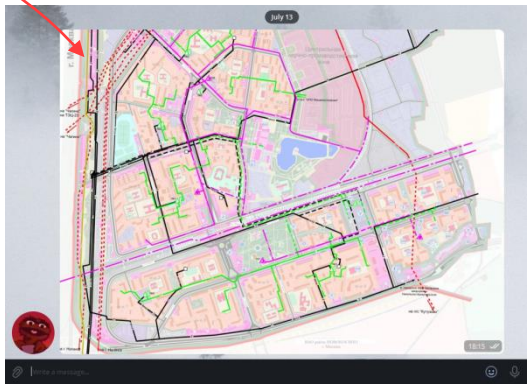
— В прошлый раз заказал на 3 миллиона

Защита изображений любого типа с помощью машинного зрения

INFOWATCH®

Машинное зрение защищает конфиденциальные фото, сканы, картинки





Готовые категории

—Паспорт гражданина РФ

—Технические чертежи

—Географические карты

Самостоятельное обучение системы

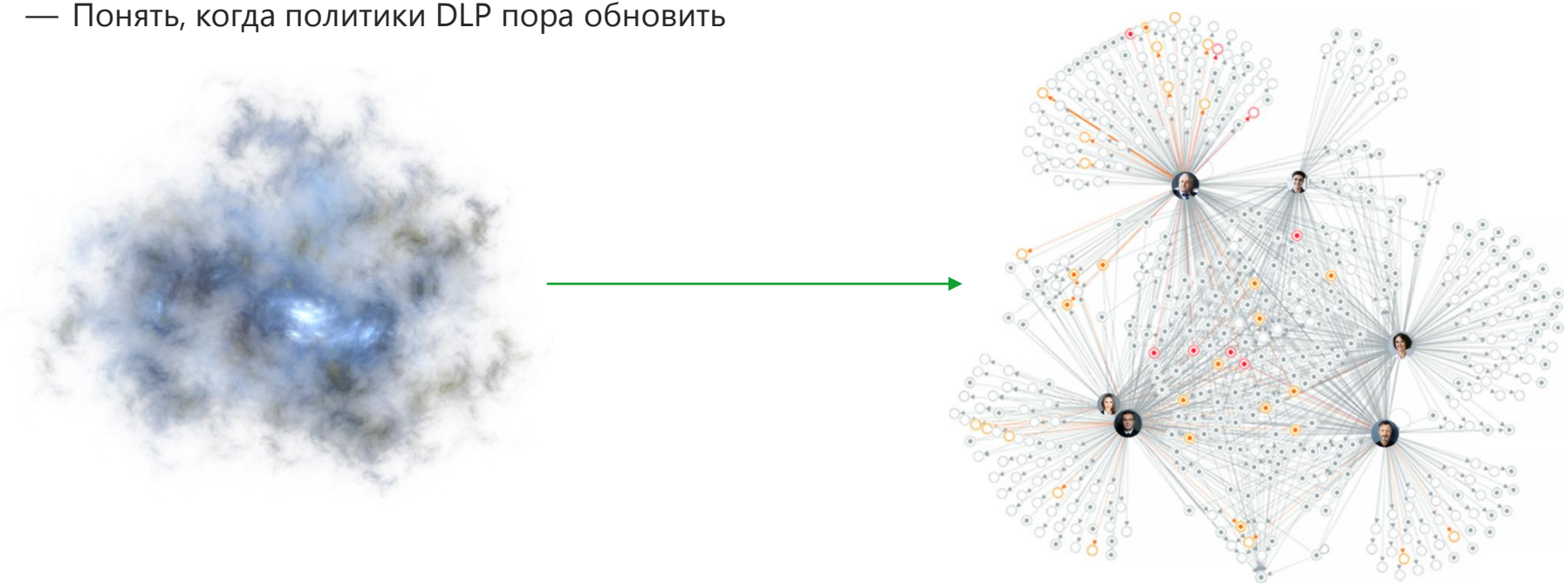
На коллекции документов клиента с помощью технологий машинного обучения.

InfoWatch Vision — визуальная аналитика данных системы защиты от утечек

— За утренним кофе проанализировать последние события в поисках инцидентов

— За минуты найти все связанные с инцидентом события и увидеть общую картину на графе связей

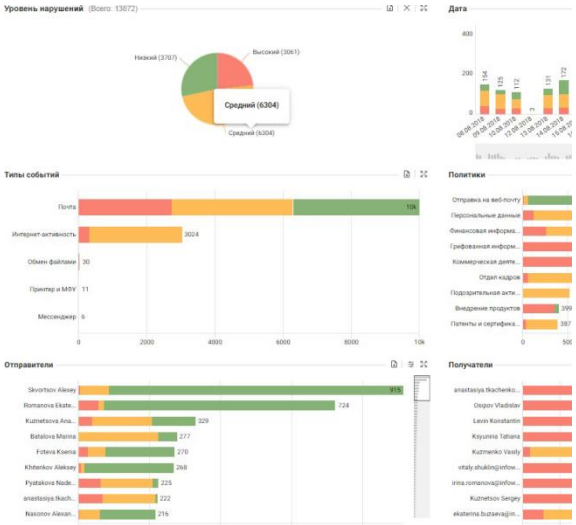
— Понять, когда политики DLP пора обновить



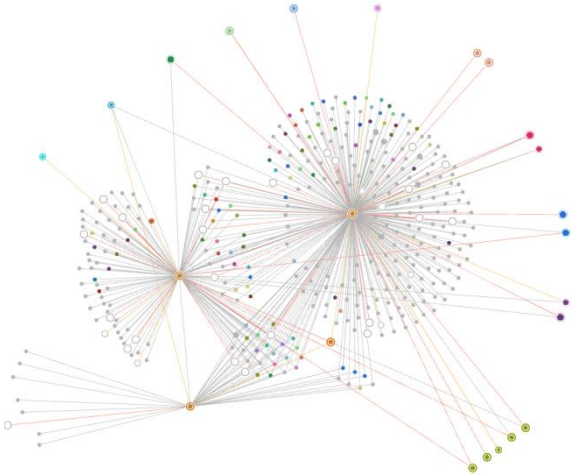
Моментальное переключение между разными срезами данных

Релиз Vision 2.8
12/2022

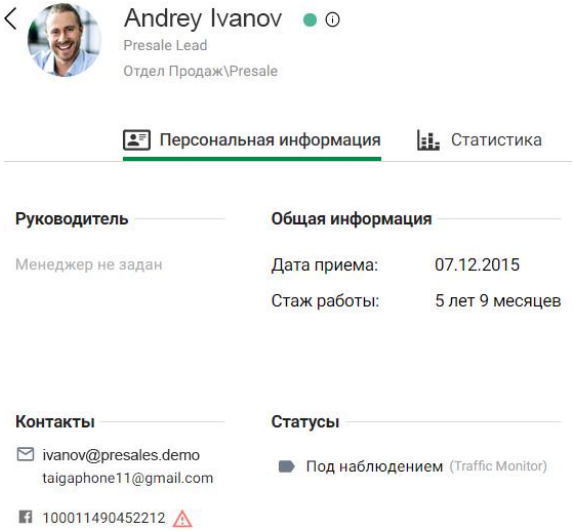
Сводная статистика



Динамический граф связей



Досье сотрудников

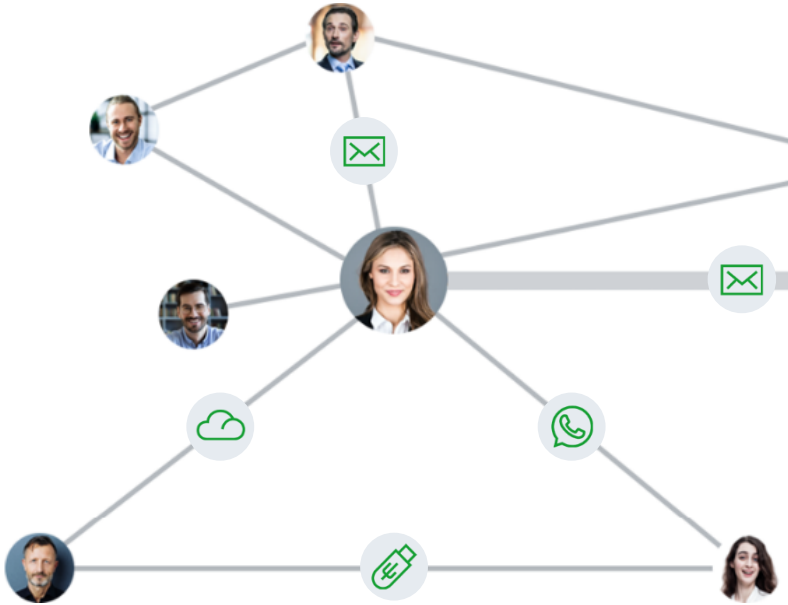


Сквозные фильтры

Сохраняют значения при переключении среза данных для сохранения контекста

От кого к кому перемещался определённый файл

Релиз Vision 2.8
12/2022



Можно отследить последовательность

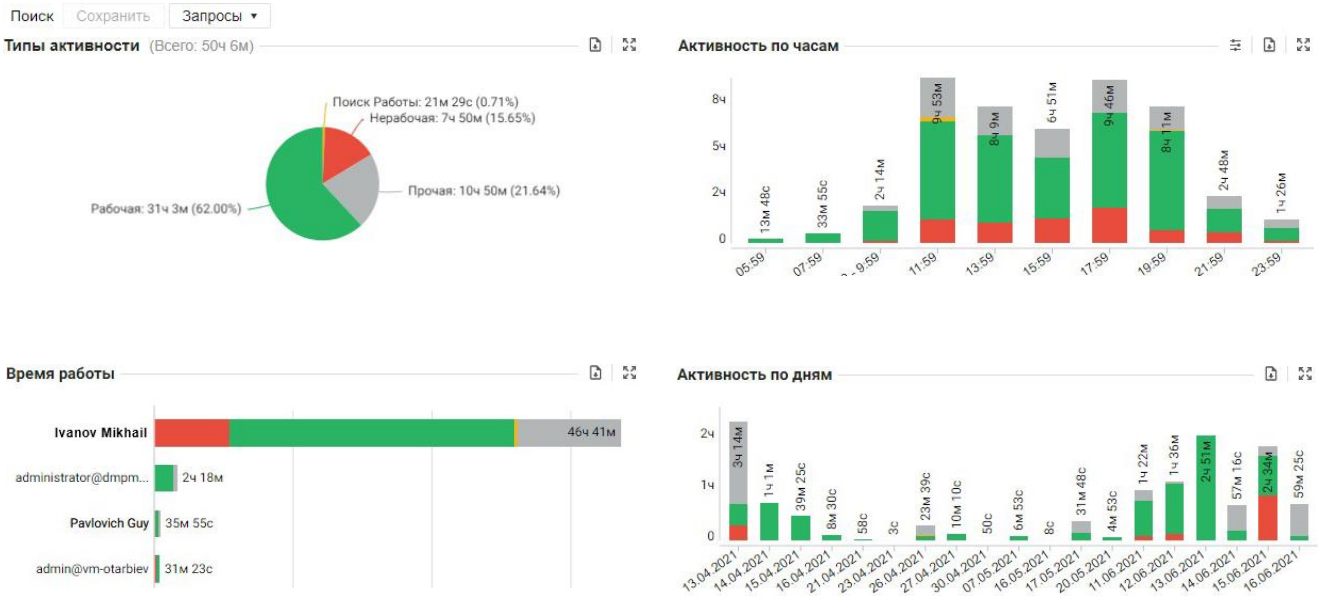
Связи подсвечиваются по очереди

InfoWatch Activity Monitor — полная картина рабочего дня

INFOWATCH®

*H1 2023

InfoWatch Activity Monitor представляет данные в удобном для анализа виде



— **10 виджетов** — конфигурируемый рабочий стол

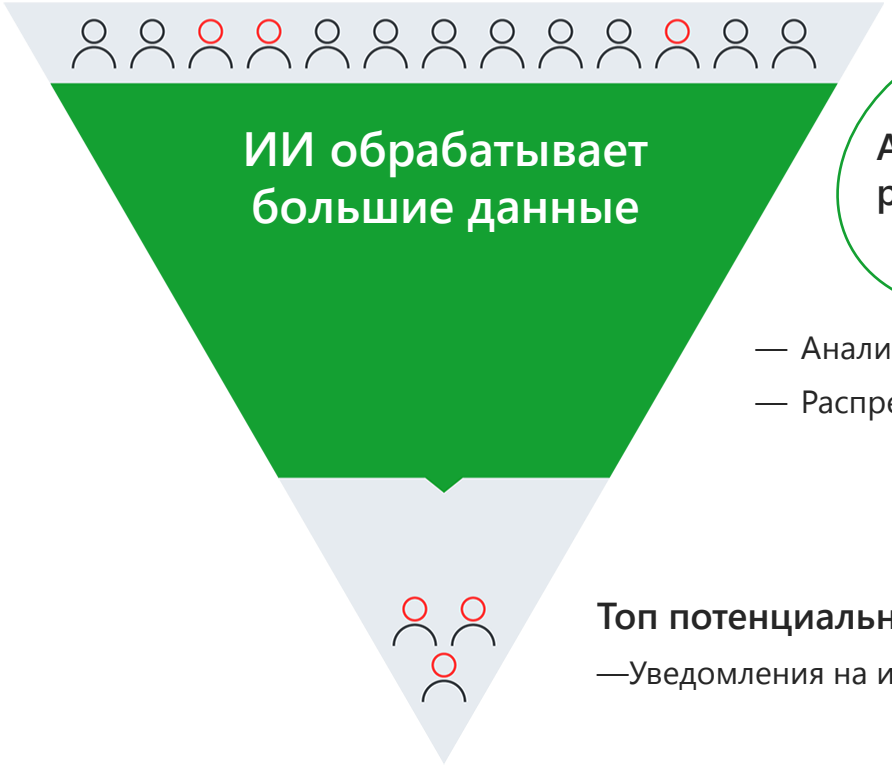
— **37 фильтров** для анализа данных на разных срезах

— **Интерактивные диаграммы,** на которых можно указать область для применения фильтра

Статистика


INFOWATCH®
60–70%
инцидентов ИБ можно предотвратить заранее — на стадии подготовки!*
*Опыт клиентов Prediction

InfoWatch Prediction — UBA-система на основе искусственного интеллекта



Автоматически, раз в час

— Анализ действий и коммуникаций сотрудников

— Распределение по группам риска

Топ потенциальных нарушителей → **Специалист ИБ принимает ключевые решения**

—Уведомления на имейл

Автоматическое формирование рейтинга подозрительных сотрудников

INFOWATCH®

230+
параметров

Чаще, чем обычно
отправляет данные самому себе, на флешку, на печать, в облако

Чаще, чем обычно
обсуждает увольнение, отсылает резюме, заходит на hh.ru

Больше, чем у коллег
новых адресатов, переписок тет-а-тет

Отклонения от нормы, статистические показатели, прямые признаки → **Автоматическое распределение сотрудников по группам риска и формирование рейтинга**

- Аномальный вывод информации
- Подготовка к увольнению
- Нетипичные внешние коммуникации
- Снижение производительности
- Отклонение от бизнес-процессов
- Нелояльные сотрудники

Интеграция с российскими приложениями и системами

INFOWATCH®

Поддержка отечественных ОС

INFOWATCH®

ASTRA LINUX®

РЕДОС

alt linux

Серверы

Red OS 7.3.1 и 7.3.2
Astra Linux Special Edition 1.6
Astra Linux Special Edition 1.7
MS Windows Server

RHEL 7.x
CentOS 7.x
Oracle Linux 7.x

Агенты

Red OS 7.3.1
Astra Linux Special Edition 1.6
Astra Linux Special Edition 1.7
Alt Linux Workstation 10

MS Windows
MS Windows Server

PostgresPro

PostgreSQL

Поддержка сертифицированных БД

Контроль телефонных переговоров

- Оповещает **о переговорах с конкурентами** и с адресатами из чёрных списков
- Выявляет коммуникации **на рискованные темы**
- Оповещает о передаче **конфиденциальной информации**
- Позволяет анализировать **карту и интенсивность коммуникаций** на графе связей
- Оповещает **о подготовке к увольнению,** нетипичных контактах и снижении лояльности
- Ретроспективный поиск по содержимому разговора для **расследований**

InfoWatch — надёжная защита от утечек и прогнозирование инцидентов

INFOWATCH®

Данные в покое

Трафик

Действия

Что случилось?

InfoWatch Data Discovery
DCAP-возможности

Аудит хранения данных на файловых ресурсах организации

InfoWatch Traffic Monitor
DLP-система на основе ИИ

Надёжная защита от утечек и контроль трафика

InfoWatch Activity Monitor

Цифровая картина рабочего дня для расследования инцидентов ИБ и работы с группами риска

Почему это случилось?

InfoWatch Vision
BI-возможности для DLP

Оперативная обстановка, ускорение расследований и отчёты

Что может произойти?

InfoWatch Prediction
UBA-система на основе ИИ

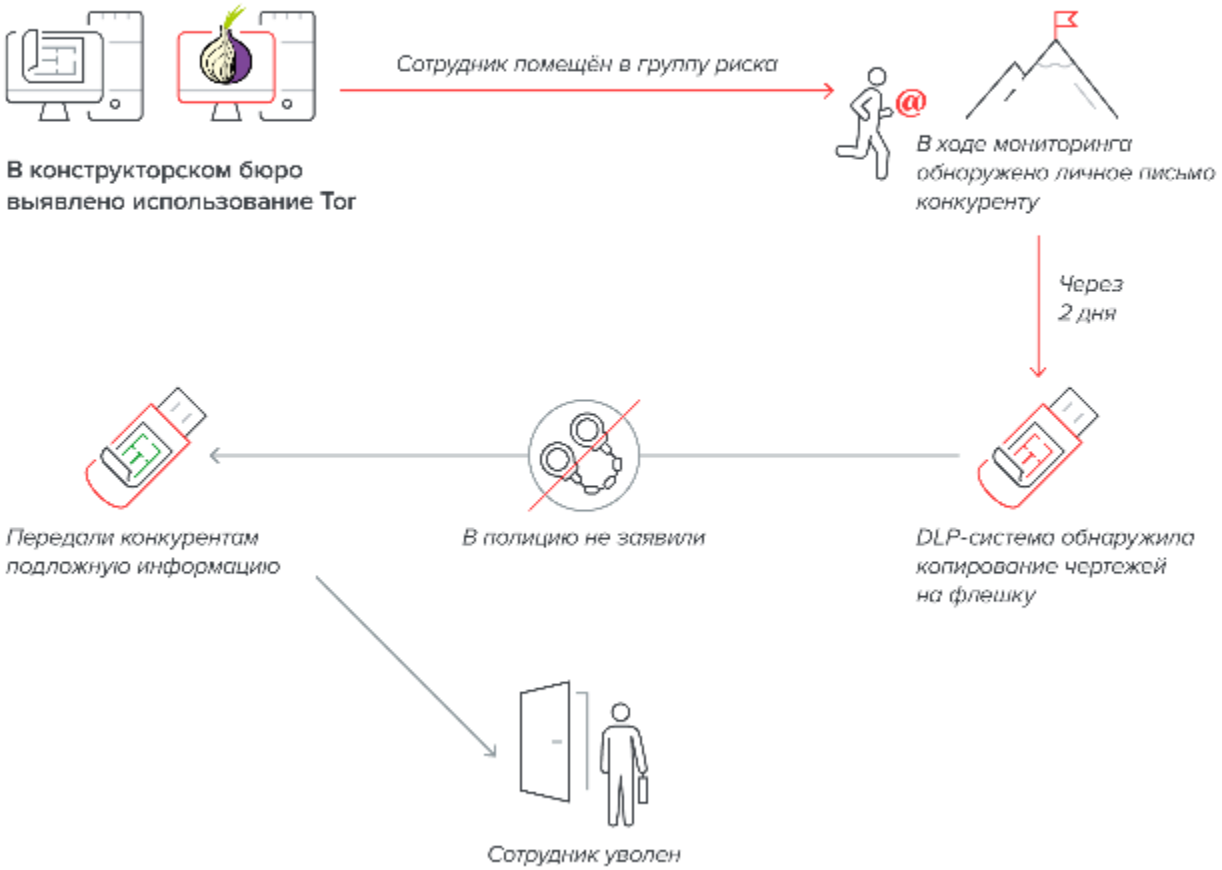
Автоматизация оценки рисков, рейтинг подозрительных сотрудников

Интеграции

INFOWATCH®

КЕЙСЫ НАШИХ КЛИЕНТОВ

Предотвращение промышленного шпионажа



Итог

Предотвращена утечка на миллионы рублей.

Недобросовестный конкурент потерпел убытки.

Profit

Выявление факта промышленного шпионажа

Горнодобывающая компания перешла под контроль государства после ухода иностранной компании

Часть сотрудников высылала отчёты бывшему руководству

1	**Prediction**	Специалист ИБ получил уведомление о сотрудниках в группе риска «Нетипичные внешние коммуникации»
2	**Traffic Monitor**	Специалист ИБ поставил сотрудников на контроль, ужесточил политики безопасности и вовремя заметил нарушения — пересылку конфиденциальных материалов
3	**Vision**	На графе связей по интенсивности коммуникаций выявлена организованная группа нарушителей
4	**Activity Monitor**	Специалист ИБ собрал доказательную базу — как готовился и протекал слив информации

Сговор зампреда банка с поставщиком услуг

У зампреда банка уровень дохода не соответствовал расходу. Выяснилось, что он был в сговоре с поставщиком услуг	**Банк нёс финансовые потери от неэффективных закупок**

1	**Activity Monitor**	Сотрудник интересовался и приценивался к люксовым авто и ЖК, которые не смог бы позволить на одну зарплату
2	**Traffic Monitor**	— В переписке WhatsApp сработали БКФ «Мошенничество», «Угроза ИБ» и «Родственные связи». Сотрудник взят на контроль
		— Выявлена переписка с родственником, который работал в компании-подрядчике. Обсуждалась мошенническая схема
3	**Activity Monitor**	Скриншоты переписки, аудиозапись переговоров в онлайн-конференции легли в доказательную базу

Слив базы поставщиков с ценами в условиях ограниченных поставок

Сотрудник готовился слить базу поставщиков конкурентам	**Конкурент хотел предложить поставщику лучшие условия, чтобы выкупать весь объём. Компания могла попасть под угрозу ликвидации**

1	**Data Discovery**	— При автоматическом аудите файлов на ПК сотрудника обнаружена информация о ключевых поставщиках и ценах закупки
		— В личной беседе сотрудник сказал, что информация попала на его компьютер по ошибке
2	**Activity Monitor**	Специалист ИБ проверил действия сотрудника за ПК. Обнаружил, что сотрудник искал способ обойти DLP и какую ответственность он может понести

Обнаружить хищение имущества

ИТ-специалист вместо списания офисной техники продавал ее на Авито	**Компания могла понести финансовый ущерб и юридические издержки**

1	**Vision**	Специалист ИБ на графе связей обнаружил необычно активную переписку между обычно не связанными между собой отделами. Проанализировал переписку – сотрудники обсуждали покупку офисной техники. В переписке найдена файл с прайс-листом.
2	**Vision**	— Сотрудник ИБ отфильтровал переписку по имени файла прайс-листа. По последовательности передачи файла между сотрудниками нашел источник – ИТ-специалиста, который первый начал распространять прайс-лист. — Офисная техника в файле очень похожа на оборудование из офиса.
3	**Activity Monitor**	Анализ действий сотрудника показал: ИТ-специалист **провел списание старой техники и выставил её на продажу на сайте Авито. Для подделки документов использовал графический редактор**

Обнаружить подготовку к увольнению

Подготовка к увольнению	**Компания могла понести издержки связанные с увольнением и утечкой информации**

1	**Prediction**	Сотрудник попал на 1 место в рейтинге сразу в 2 категориям (нетипичные коммуникации, подготовка к увольнению)
2	**Activity Monitor**	Сотрудник ИБ проанализировал активность сотрудника в сети и обнаружил что сотрудник посещает сайт hh.ru, а также взаимодействует с внешними адресами, высылая информацию различного рода.
3	**Traffic Monitor**	Система автоматически заблокировала отправку файлов.

Курьезный случай

1	**Activity Monitor**	Была обнаружена активность одного из сотрудников в ночное время. Система автоматически сделала скриншоты экрана и фото с камеры. Оказалось сотрудник ночевал в офисе и играл в компьютерные игры.

INFOWATCH®

МЫ УЛУЧШАЕМ ПРОДУКТ БЛАГОДАРЯ ВАМ!

infowatch.ru

Светлана Марьясова

Заместитель руководителя направления по развитию бизнеса на территории СФО и УрФО

+7 950 415 32 00
Svetlana.Maryasova@infowatch.com

/InfoWatch /InfoWatchOut