INFOWATCH®

INFOWATCH для банков

- Требования ЦБ
- Предотвращение утечек
- Управление рисками
- Контроль на удаленке

Татьяна Тюрина

Менеджер по работе с клиентами и партнерами на территории ДФО, InfoWatch

Изменения цифровой среды — новые вызовы

Цифровизация — главный тренд в развитии банковского сектора в 2022 году

Данные — основа цифрового банка

Когда клиенты, аналитика, процессы и know-how в цифре, то все риски в цифре

Риски банковской отрасли

- Ежегодные проверки ЦБ
- Требования – 80% отечественного ПО
- Удаленная работа и гибридный график
- Шпионаж, кража и публикация информации, например о VIP-клиентах, их транзакциях, фото паспортов и карт
- Репутационные угрозы

InfoWatch Traffic Monitor

DLP-система на основе ИИ

Предотвращает утечки на основе полноценного контентного анализа

Лицензии и сертификаты:

- Аккредитация ЦБ РФ
- АРПП «Отечественный софт»
- 5 класс защищённости (СВТ5)
- ФСТЭК России

InfoWatch Traffic Monitor

DLP-система на основе ИИ

Точность контентного анализа

Выше эффективность

Минимум ложных срабатываний

28 патентов на контент-анализ

с 2006 применяем методы машинного обучения

Защищаем данные в условиях постковидной эры:
гибридные рабочие места, облака, приложения, изменения формата коммуникаций

InfoWatch Traffic Monitor

DLP-система на основе ИИ

Контролируем не только основные каналы, но и самые «проблемные»

- Мессенджеры
- Соцсети
- Облачные сервисы
- Проприетарные системы

Классификация текстов «из коробки»: отраслевые и тематические словари

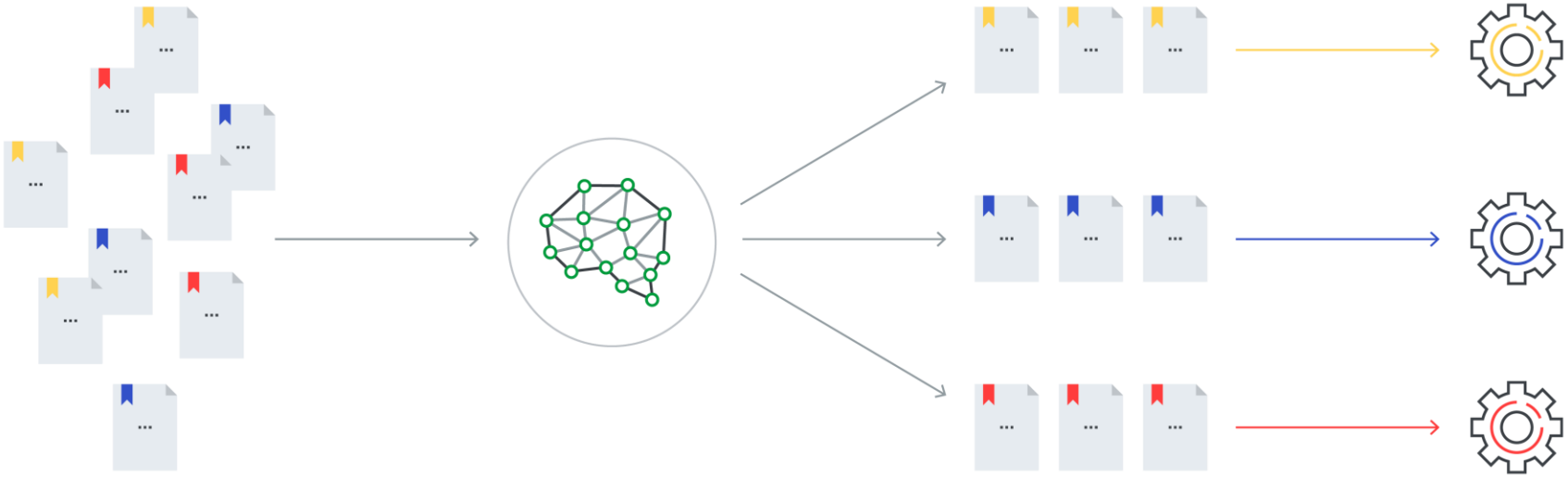
Для точного детектирования и снижения ложных срабатываний

- 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
- ...

Учитываем специфику ваших терминов: доработка базы под каждого заказчика

289 категорий

Новый тип данных? Категоризация документов с помощью технологий ИИ



Неисследованный поток данных

ИИ категорирует ВСЕ документы компании за 1 день

Документы по категориям

Обучение DLP с помощью Автолингвиста

Автолингвист — автоматическое обучение DLP-системы новым категориям документов

INFOWATCH®

→ На документах заказчика

→ Без привлечения экспертов-лингвистов

→ ВСЕ документы за 1 час, а не 10 дней

Специалист ИБ решил обучить классификатор находить документы, похожие на специфические технические условия (ТУ)

Экземпляры технических условий

Обучение классификатора на основе ИИ за 5 минут

Результат — новая категория «Технические условия X»

Настройка политик безопасности DLP-системы

Кейс. Утечки данных клиентов в банках

Банк ипотечного кредитования столкнулся с оттоком клиентов. Расследование показало, что имеет место утечка данных клиентов, контактов и условий кредитования.

- **Утечки персональных данных в финансовом секторе влекут серьёзные последствия: материальный ущерб и штрафные санкции регулятора**

- Задача: оперативно выявлять и предотвращать утечки персональных данных клиентов

Выявляем реквизиты:
детектор текстовых объектов

INFOWATCH®

Поиск

Найти номер банковской карты в общем массиве информации

Проверка контрольных сумм с помощью алгоритма Луна повышает точность детектирования реквизитов

Значение текстового объекта ?

4272290996213260

Проверка

Детектируем все возможные варианты написания

4272290996213260

4272-2909-9621-3260
4272/2909/9621/3260
4272.2909.9621.3260
4272,2909,9621,3260

Результат

Номер карты выявлен независимо от варианта написания

карта 4272-2909-9621-3260 CV 123, пользуйся пока есть возможность

18:07

Защита персональных и других именованных данных

- Список клиентов
- Номенклатура
- Прайс-листы
- Аналитические данные
- Результаты работы ИИ

Невозможно отловить регулярными выражениями

Огромное количество ложных срабатываний.

Представьте, что система срабатывает на каждую подпись к письму!

Как защитить любые именованные данные с минимальным количеством ложных срабатываний?

Детектор выгрузок баз данных проверит соответствие информации полям баз данных

Защита персональных и других именованных данных

Смирнова Мария, ул. Пришвина, 10, кв. 99, +79857733378 12:42

Иванов Петр, ул. Свободы, дом 1к1, кв. 188, +79853377739 12:42

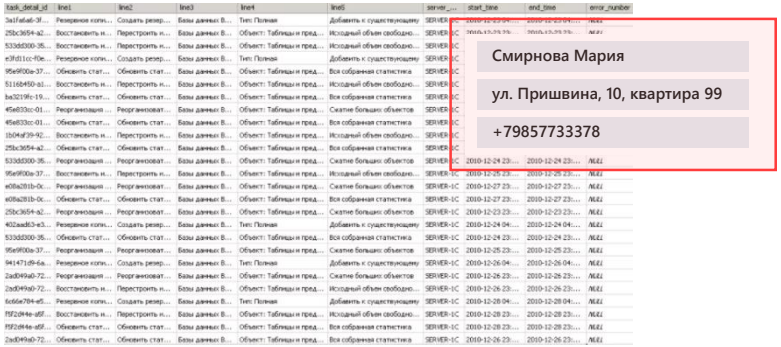
Два идентичных сообщения.

Одно — личная переписка, совет репетитора на дому.

Другое — утечка данных о ключевом клиенте

Ни одна из классических технологий DLP не пригодна для защиты таких данных: список клиентов, номенклатура, складские остатки, прайс-листы, аналитические данные, результаты работы ИИ.

Защита персональных и любых именованных данных: детектор выгрузок баз данных



- → Контролируем **движение конкретных данных,** а не просто доступ к базе
- → Скорость — **100 000 000 записей** в секунду
- → Защищаем **актуальные** данные — динамическое обновление данных

ЗАПАТЕНТОВАНО

Особенности

Для каждой защищаемой сущности (ПДн, база клиентов, поставщиков, сотрудников) несколько критериев срабатывания — например, комбинации полей и порция переданных данных.

Это единственный способ контролировать ПДн или прайс-листы без шквала ложноположительных срабатываний

Детектируем сканы документов: графический классификатор

Низкое качество сканов паспортов, наличие бликов; большое количество ложных срабатываний: технологии текстового анализа и OCR не работают

Результат применения графического классификатора

- При применении постфильтра лица ложные срабатывания **сократились до 0.1%** (без постфильтра — 1%)
- Производительность **выше OCR в 2 раза**

Детектируем сканы банковских карт: технология «картинка в картинке»

INFOWATCH®

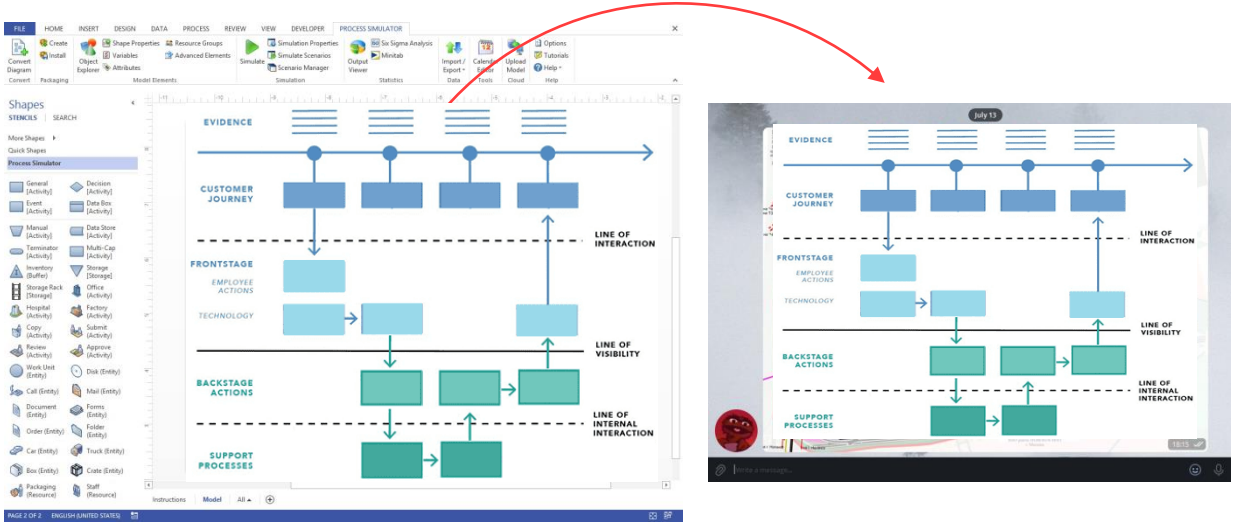
Низкое качество сканов карт, стёртый номер; большое количество ложных срабатываний: технологии текстового анализа и OCR не работают

Результат применения технологии «картинка в картинке»

- Используется префильтр, который с вероятностью **99%** выявляет банковские карты в общем объёме фотографий
- Вероятность ложных срабатываний — **менее 0,1%**
- Запатентованная технология на базе принципов аффинного преобразования
- Не зависит от расположения и масштаба фотографии банковской карты

Защита изображений любого типа с помощью машинного зрения

Машинное зрение защищает конфиденциальные фото, сканы, картинки



Самостоятельное обучение системы

На коллекции документов клиента с помощью технологий машинного обучения.

Создать безопасную экосистему — обеспечить безопасность в условиях цифровой трансформации

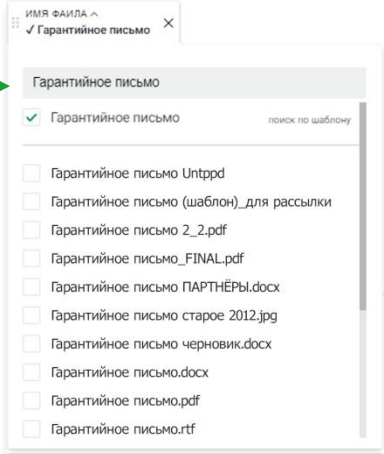
Независимые вендоры интегрируются с нами (Microsoft, Konica Minolta)

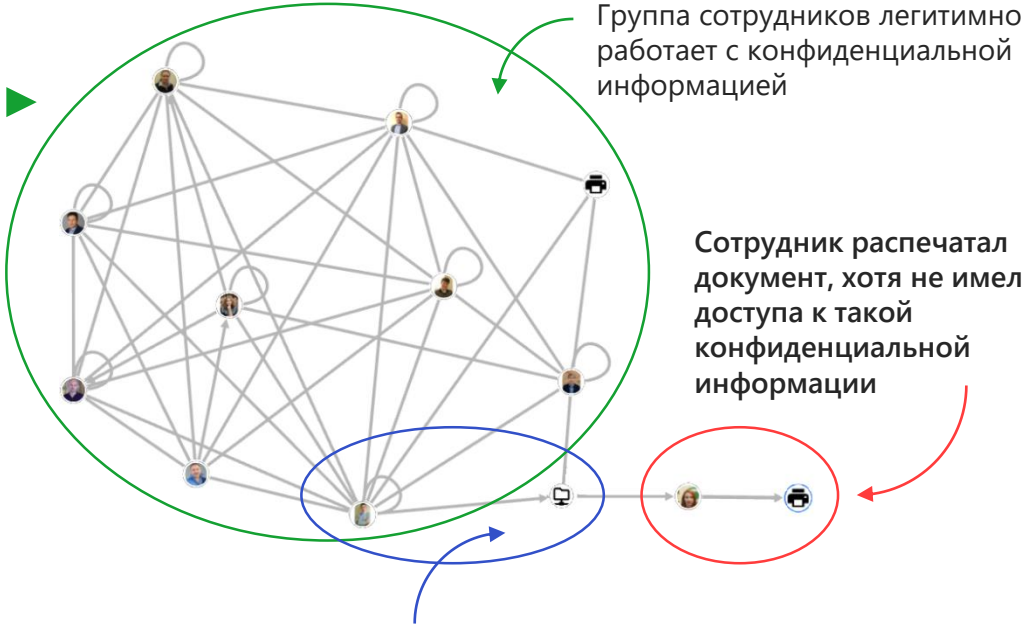
Мы разрабатываем интеграции с **бизнес- и ИТ-системами** (SAP)

С помощью открытого API можно интегрировать **InfoWatch Traffic Monitor с проприетарными системами клиента**

InfoWatch Vision: Расследования занимают минуты, а не часы

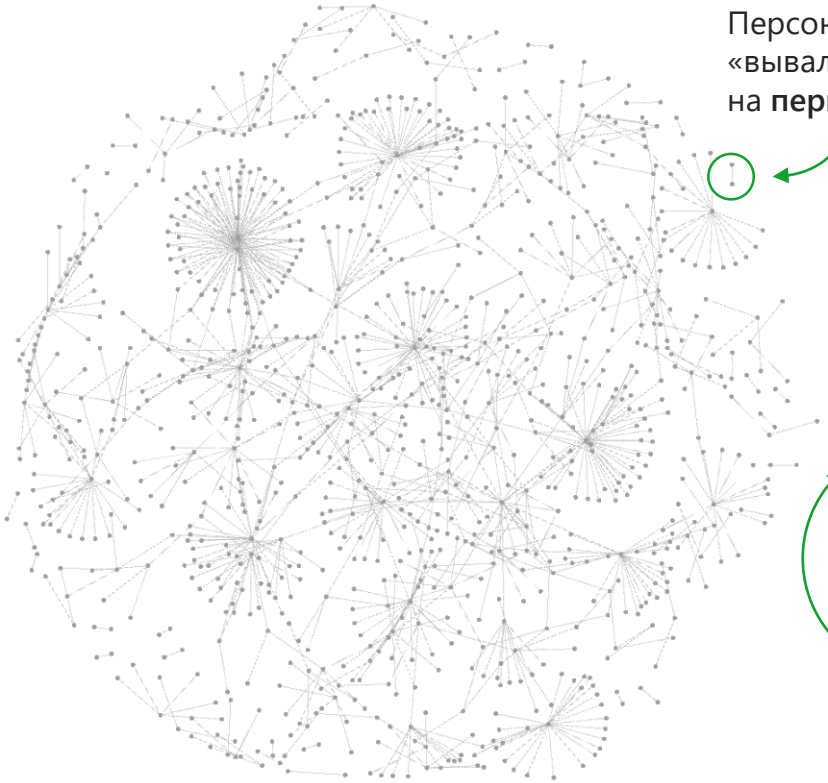
1. В интернете обнаружено фото документа
2. Поиск по общей части в имени файла
3. Граф связей перемещения информации в компании



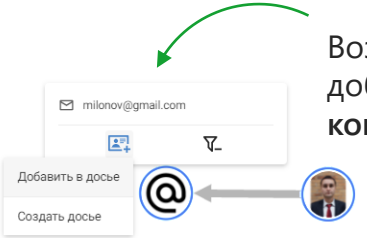


Утечке поспособствовала выгрузка документа в сетевую папку

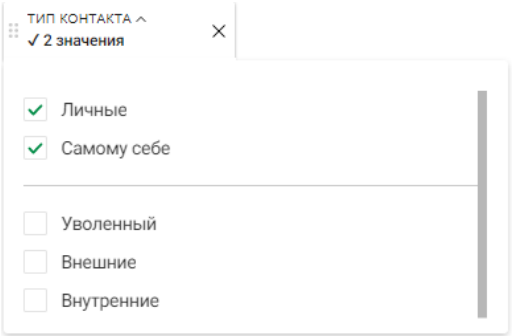
Выявление личных адресов и оценка легитимности взаимодействия



Персональные коммуникации «вываливаются» на **периферию** графа



Возможность добавить **личный контакт** на графе



Фильтр позволяет отобрать все события с личными контактами

+ Фильтр **«Уволенные»** позволяет отобразить переписку с бывшими коллегами

InfoWatch Prediction: рейтинг подозрительных сотрудников

INFOWATCH®

Мессенджеры

Почта

Нарушение политик

АНАЛИЗИРУЕМ

Съёмные устройства

Облака

Цепочки событий

Превышение порогов

НАХОДИМ

Совокупность событий

Аномалии

Повторные нарушения

Вывод информации

Подготовка к увольнению

ПОКАЗЫВАЕМ

Необычные внешние контакты

«Мёртвые души»

Массовое копирование

Найдены аномалии

ОПОВЕЩАЕМ

Топ-5 «рискованных» персон

Вовремя заметить тендерное мошенничество

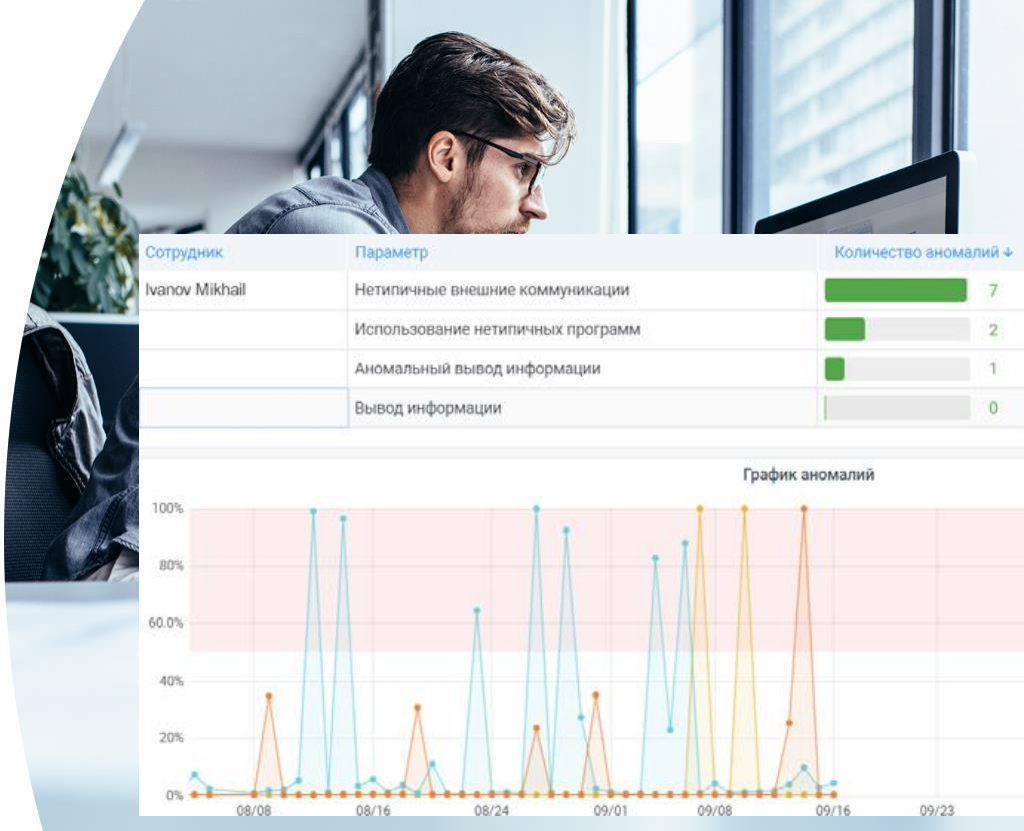
- → У сотрудника появились внешние уникальные адресаты, тет-а-тет
- → Регулярно запускает с флешки файловый менеджер для удалённого доступа к машинам
- → Производил массовое копирование вне рабочего дня

Как заметить аномальное поведение и предотвратить мошенничество заранее?

Вовремя заметить тендерное мошенничество

Prediction автоматически прогнозирует риски и уведомляет о самых опасных.

- → Специалист ИБ получил еженедельное уведомление о топ-персонах в группах риска
- → Подозреваемый сотрудник попал на первое место сразу в трёх категориях
- → После анализа принято решение о дальнейшем разбирательстве



TADVISER
Государство. Бизнес. ИТ

INFOWATCH®

INFOWATCH TRAFFIC MONITOR — ЛУЧШЕЕ ИБ-РЕШЕНИЕ 2021 ПО ВЕРСИИ TADVISER

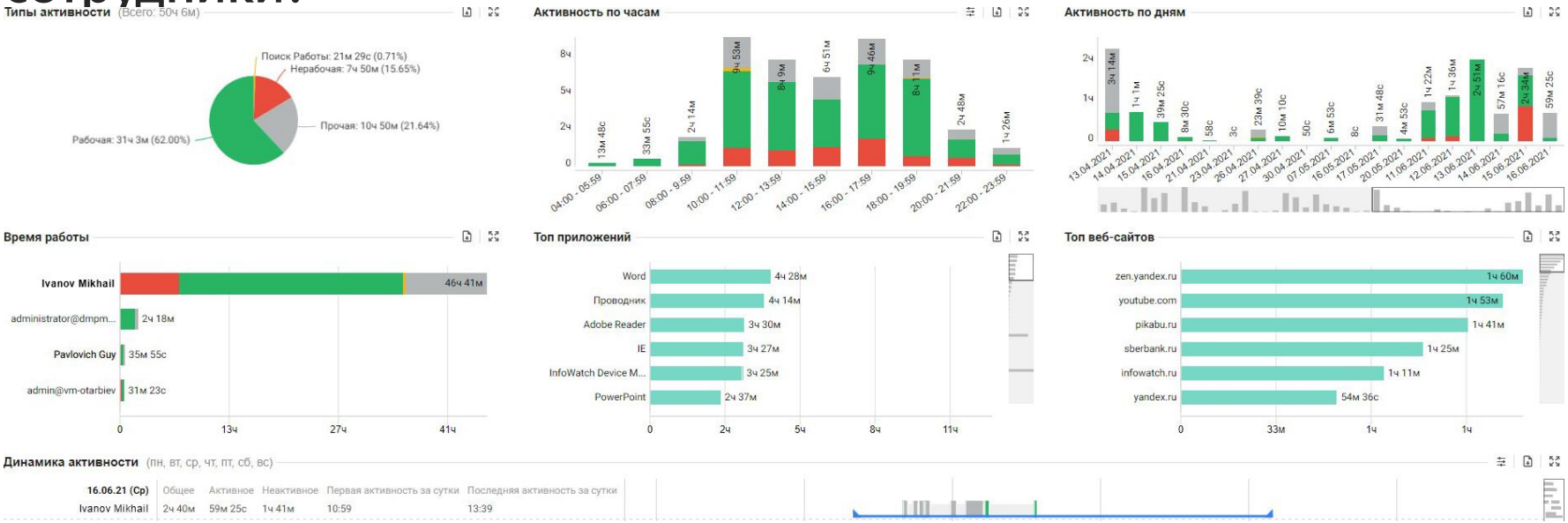
За визуальную и предиктивную аналитику и расширение возможностей DLP-системы

Ускорение расследований в 3–4 раза

Не только блокировка, но и профилактика утечек

Данные для ЭБ, IT, HR...

InfoWatch Employee Monitoring: Чем заняты сотрудники?



Последовательная картина рабочего дня

- → Когда сотрудник начал и закончил работать
- → Когда был на встречах (интеграция с MS Outlook)
- → Сколько из этого времени был за компьютером
- → Сколько из этого времени был активен (в т. ч. периоды бездействия, частые переключения...)

Статистика активности по всей компании, департаменту или сотруднику, например:

- → 60% — рабочая активность
- → 30% — нерабочая
- → 10% — требует разбора

Топ приложений и веб-ресурсов

- → Кем используются
- → Когда
- → Как долго

Поиск использования развлекательных ресурсов

INFOWATCH®

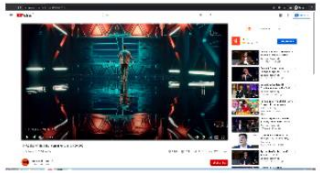
ПЕРСОНА: Все | ДАТА: 18 мая - 16 июня | ФИЛИАЛ: Все | ЧАСЫ: Все | ГРУППА: Все | ОТДЕЛ: Все | ДОЛЖНОСТЬ: Все
ВЕБ-САЙТ: Все | ПРИЛОЖЕНИЕ: Все | ТИП АКТИВНОСТИ: ✓ Нерабочая | НАЗВАНИЕ АКТИВНОГ...: Все | ТЕГ: Все | ПРАВИЛО МАРКИРОВКИ: Все | КОНТАКТ: Все
НАЛИЧИЕ СНИМКА ЭКР...: Все | ВВОДИМЫЙ ТЕКСТ: Все

Лента событий (Всего: 41)

Персона	Тип со...	Рабочая ста...	Дата событ...	Тип активнос...	Приложение	Адрес сайта	Время активной...	Общее время ра...	Правило маркир...	Теги
Ivanov Mikhail		vm-1405.info	16 июня 2021 г. 14:5	Нераб...	Chrome (chrome.exe)	youtube.com	2м 45с	2м 45с	Нерабочая активно	
Ivanov Mikhail		vm-1405.info	16 июня 2021 г. 14:5	Нераб...	Chrome (chrome.exe)	youtube.com	15с	15с	Нерабочая активно	
Ivanov Mikhail		vm-1405.info	16 июня 2021 г. 14:5	Нераб...	Chrome (chrome.exe)	youtube.com	4с	4с	Нерабочая активно	
Ivanov Mikhail		vm-1405.info	16 июня 2021 г. 14:5	Нераб...	Chrome (chrome.exe)	youtube.com	20с	20с	Нерабочая активно	
Ivanov Mikhail		vm-1405.info	16 июня 2021 г. 14:5	Нераб...	Chrome (chrome.exe)		13с	13с	Нерабочая активно	
Ivanov Mikhail		vm-1405.info	16 июня 2021 г. 14:5	Нераб...	Chrome (chrome.exe)		2с	2с	Нерабочая активно	

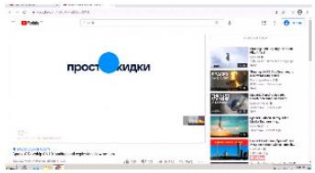
Список сессий (Всего: 4)

3



16.06 • 14:21 - 15:52
Ivanov Mikhail
vm-1405.infowatch.ru

6



09.03 • 16:47 - 20:41
Ivanov Mikhail
dmpm-1405vm.infowatch.ru

О событии

14:55:30
youtube.com
К снимку

14:55:35 MORGENSHTERN. Вечерний Ургант. 08.06.2021 - YouTube - Google Chrome (Incognito)
К снимку

Со скриншотами!

Статистика

- → Кто из сотрудников
- → В какое время
- → Как долго
- → Что смотрел

Факты саботажа: конкретные действия

INFOWATCH®

Лента событий (Всего: 21)

Персона	Тип...	Рабочая ста...	Дата с...	Тип активнос...	Приложение	Адрес сайта	Время ...	Общее ...	Теги
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Рабоч...	Командная Строка (cmd.ex		19с	19с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Рабоч...	Командная Строка (cmd.ex		19с	19с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Рабоч...	Командная Строка (cmd.ex		28с	28с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	docs.microsoft.com	14с	14с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	forum.itvdn.com	2м 31с	2м 31с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	google.com	11с	11с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	google.com	1с	1с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	codeby.net	6с	6с	На рассмотрение
Ivanov Mikhail		vm-1405.in	16 июня 2021 г	Рабоч...	Chrome (chrome.exe)		3м 54с	3м 54с	На рассмотрение
Ivanov Mikhail		vm-1405.in	16 июня 2021 г	Прочая	PuTTY suite (putty.exe)		40с	40с	На рассмотрение
Ivanov Mikhail		vm-1405.in	16 июня 2021 г	Рабоч...	Командная Строка (cmd.ex		53с	53с	На рассмотрение

О событии

18:32:20 Проблема - Как почистить за собой логи и т.п? | Форум информационной безопасности - Codeby.net - Google Chrome
codeby.net/threads/kak-pochistit-za-soboj-logi-i-t-p.63023/
К снимку

как стереть ЫЙД SQL базу

18:32:20
https://www.google.com/search?q=%D0%BA%D0%B0%D0%BA+%D1%81%D1%82%D0%B5%D1%80%D0%B5%D1%82%D1%8C+SQL+%D0%B1%D0%B0%D0%B7%D1%83&rlz=1C1GCEV_enRU882RU882&oq=%D0%BA%D0%B0%D0%BA+%D1%81%D1%82%D0%B5%D1%80%D0%B5%D1%82%D1%8C+SQL+%D0%B1%D0%B0%D0%B7%D1%83&aqs=chrome..69i57j0i22i30l3.9197j0j15&sourceid=chrome&ie=UTF-8

Статистика со скриншотами также покажет действия сотрудника перед сливом документа или шифрованием:

→ Поиск в интернете

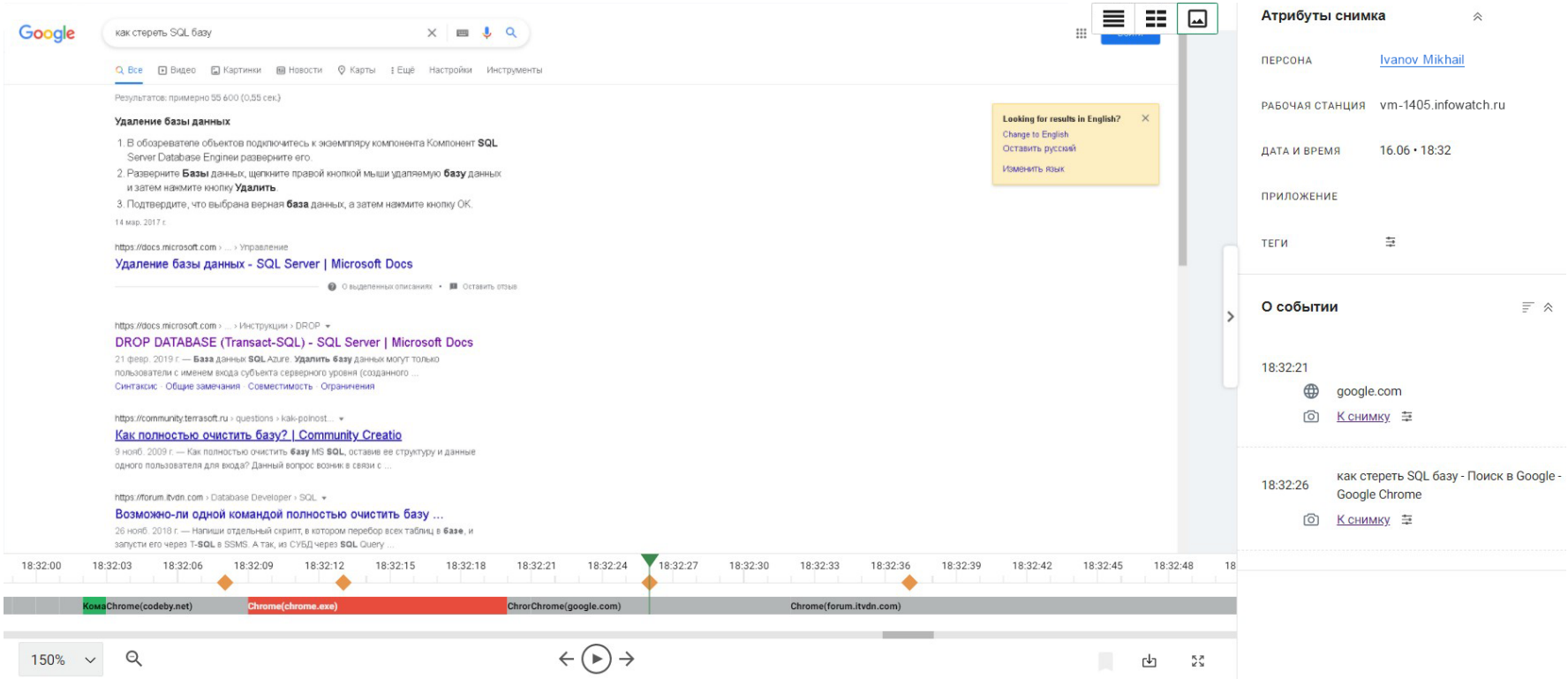
→ Установка и использование приложений

→ Пароль шифрования

Увольняющийся сотрудник в группе риска. При мониторинге обнаружено — ищет способ удалить SQL-базу.

Поиск решения в интернете — как удалить базу SQL?

Факты саботажа: конкретные действия



Скриншот подтверждает поиск способа удалить БД

Факты саботажа: конкретные действия

Поиск | Сохранить | Запросы | Очистить фильтры

Лента событий (Всего: 21)

Персона	Тип...	Рабочая ста...	Дата с...	Тип активнос...	Приложение	Адрес сайта	Время ...	Общее ...	Теги
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Рабоч...	Командная Строка (cmd.ex		19с	19с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Рабоч...	Командная Строка (cmd.ex		19с	19с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Рабоч...	Командная Строка (cmd.ex		28с	28с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	docs.microsoft.com	14с	14с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	forum.itvdn.com	2м 31с	2м 31с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	google.com	11с	11с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	google.com	1с	1с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	codeby.net	6с	6с	На рассмотрение
Ivanov Mikhail		vm-1405.in	16 июня 2021 г	Рабоч...	Chrome (chrome.exe)		3м 54с	3м 54с	На рассмотрение
Ivanov Mikhail		vm-1405.in	16 июня 2021 г	Прочая	PuTTY suite (putty.exe)		40с	40с	На рассмотрение
Ivanov Mikhail		vm-1405.in	16 июня 2021 г	Рабоч...	Командная Строка (cmd.ex		53с	53с	На рассмотрение
Ivanov Mikhail		vm-1405.in	16 июня 2021 г	Прочая	PuTTY suite (putty.exe)		20с	20с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	codeby.net	6с	6с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	xakep.ru	20с	20с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	codeby.net	38с	38с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	google.com	1с	1с	На рассмотрение
Ivanov Mikhail		vm-1405.info	16 июня 2021 г	Прочая	Chrome (chrome.exe)	google.com	1с	1с	На рассмотрение

О событии

18:35:57
К снимку

18:36:02 Command Prompt
К снимку

18:36:04 Command Prompt
ms sql login

18:36:18 Command Prompt
drop database sales

18:36:23 Command Prompt
drop database vip

Подтверждён факт ввода команд по удалению БД

Единое комплексное решение для защиты корпоративных данных

INFOWATCH®

Что случилось?

Дескриптивная аналитика

Почему это случилось?

Диагностическая аналитика

Что может произойти?

Предиктивная аналитика

InfoWatch Traffic Monitor

DLP (Data Loss Prevention) — защита данных от утечек

InfoWatch Activity Monitor

Мониторинг действий пользователей

InfoWatch Vision

Визуальная аналитика данных DLP-системы

InfoWatch Prediction

Предиктивная аналитика данных DLP-системы

Зрелость процессов и продвинутость инструментов

Некоторые клиенты

INFOWATCH®

Министерство обороны Российской Федерации

Федеральная таможенная служба

ТВЭЛ

ИНТЕР РАО КАШИРСКАЯ ГРЭС

МОСКОВСКИЙ ВЕРТОЛЕТНЫЙ ЗАВОД ИМ. М.Л. МИЛЯ

СУХОЙ

Фонд социального страхования

Федеральная налоговая служба

e·on

ОДК Объединённая двигательная корпорация

ОСК

kira

ОБОРОНПРОМ

Ростех ИНФОРМ

ТРАНСНЕФТЬ

ГАЗПРОМ ВНИИГАЗ

СлавНефть

ОАО «ВНИПИ газдобыча»

СОГАЗ СТРАХОВАЯ ГРУППА

ВСК СТРАХОВОЙ ДОМ

HOME CREDIT BANK

Райффайзен БАНК

МТС БАНК

Банк Кольцо Урала

Альфа Капитал

ПЕРВОЕ КРЕДИТНОЕ БЮРО

ВОЗРОЖДЕНИЕ БАНК

Банк Казани

Связь Банк

БАНК Форштадт

ДЕЛЬТАКРЕДИТ Ипотечный Банк

ГАЗПРОМ АВИА

РОСЖЕЛДОР ПРОЕКТ

SPSR express

О'КЕЙ

ДИКСИ

МАГНИТ

STADA

НИАРМЕДИК Сеть семейных клиник

INFOWATCH®

В 87% случаев уже на пилотных проектах InfoWatch выявляются нарушения, требующие безотлагательного вмешательства службы безопасности предприятия или организации

INFOWATCH®

ХОТИТЕ ПОПРОБОВАТЬ ТЕХНОЛОГИИ INFOWATCH В ДЕЛЕ?

/InfoWatchOut

/InfoWatch

/infowatchnews

Татьяна Тюрина

Менеджер по работе с клиентами и партнерами на территории ДФО, InfoWatch

Tatiana.Tyurina@infowatch.com

TM.infowatch.ru