

КАК ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА ПОМОГАЕТ ПРЕДОТВРАЩАТЬ КОРПОРАТИВНОЕ МОШЕННИЧЕСТВО

ПРИМЕРЫ



Пётр Дьячков

Менеджер по развитию
продуктов, InfoWatch

**В ХОДЕ СЛЕДСТВИЯ
ГЛАВНОЕ**

НЕ ВЫЙТИ НА САМИХ СЕБЯ

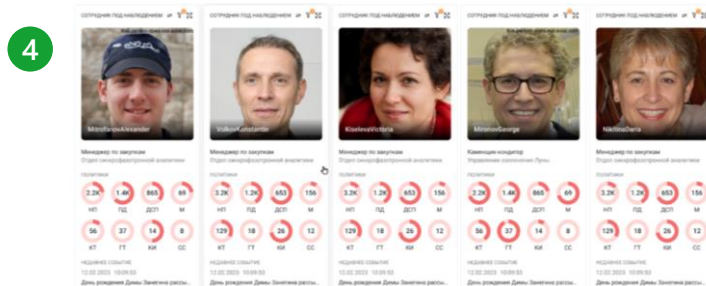
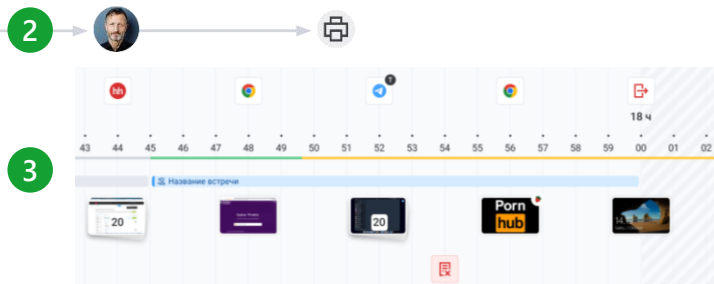
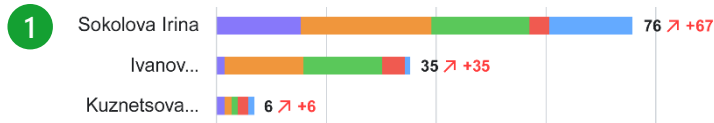
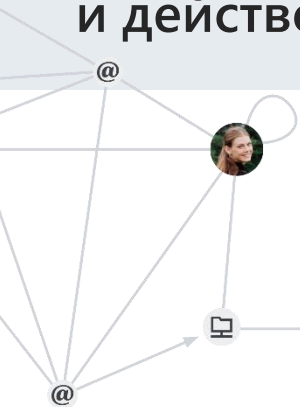
У опытного
специалиста
ЭБ достаточно
наработок,
чтобы
доверять
интуиции

DLP нового поколения — прогнозирование и управление рисками ИБ и ЭБ



- Распределяем сотрудников по группам риска по подозрительным шаблонам и аномальному поведению
- Оповещаем о наличии подозрительных связей и компрометирующих интересов, которые могут привести к искам против организации, заведению административных или уголовных дел на сотрудников
- Выявляем признаки корпоративного мошенничества — например, необоснованных закупок, воровства
- Даём инструменты для проведения расследований и сбора доказательной базы

Что позволяет быстро реагировать на угрозы и действовать на опережение?



1. Рейтинг подозрительных сотрудников по группам риска: на кого обратить внимание в первую очередь
2. Интерактивный граф связей: все задействованные в мошеннической схеме, пособники и случайные потерпевшие
3. Интерактивная временная шкала: восстановить последовательность действий подозреваемого сотрудника — установить степень вины, умысел и мотив
4. Настраиваемые рабочие панели: для мониторинга оперативной обстановки или системного наблюдения за сотрудниками на контроле
5. Блокнот расследований: формировать отчёт без применения стороннего ПО

Подготовка нарушения — почти всегда аномальное поведение



70% случаев — перед нарушением сотрудник ведёт себя нетипично

Не так, как раньше



Сотрудник N
сейчас

Сотрудник N вчера, позавчера,
неделю или месяц назад

Не так, как коллеги



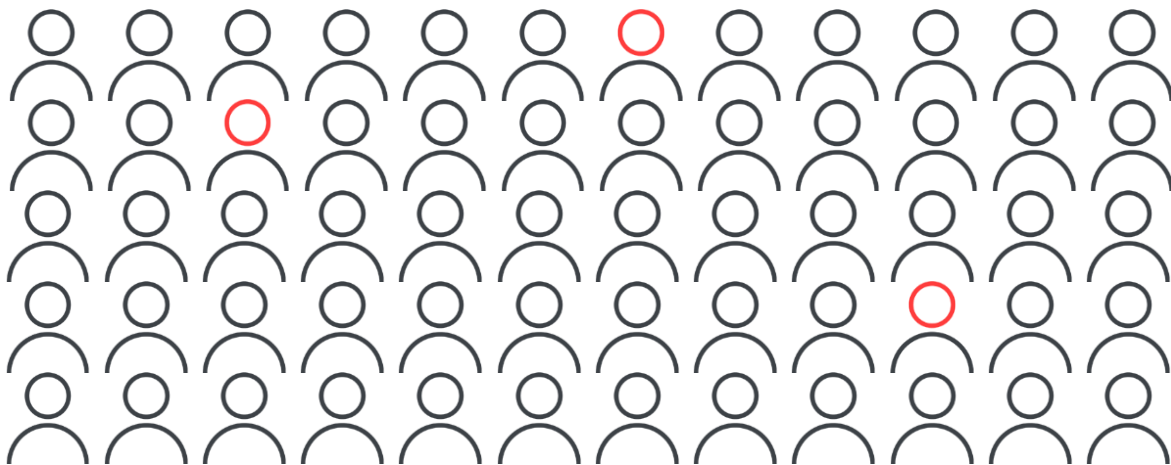
Сотрудник N

Департамент, где работает
сотрудник N

Выявить подозрительных сотрудников — просмотреть и сопоставить сотни тысяч событий



Внутреннее чутьё и анализ событий DLP поможет, если сотрудники «как на ладони» или их в компании <50



Как анализировать поведение, если сотрудников больше?

Анализ совокупности данных DLP и системы мониторинга действий сотрудника



Переписка в мессенджерах



Переписка в почте



Работа с внешними накопителями



Работа с облачными хранилищами



Отправка на печать



Данные кейлоггера



Обнаружение объектов защиты



Нарушение политик



Использование приложений

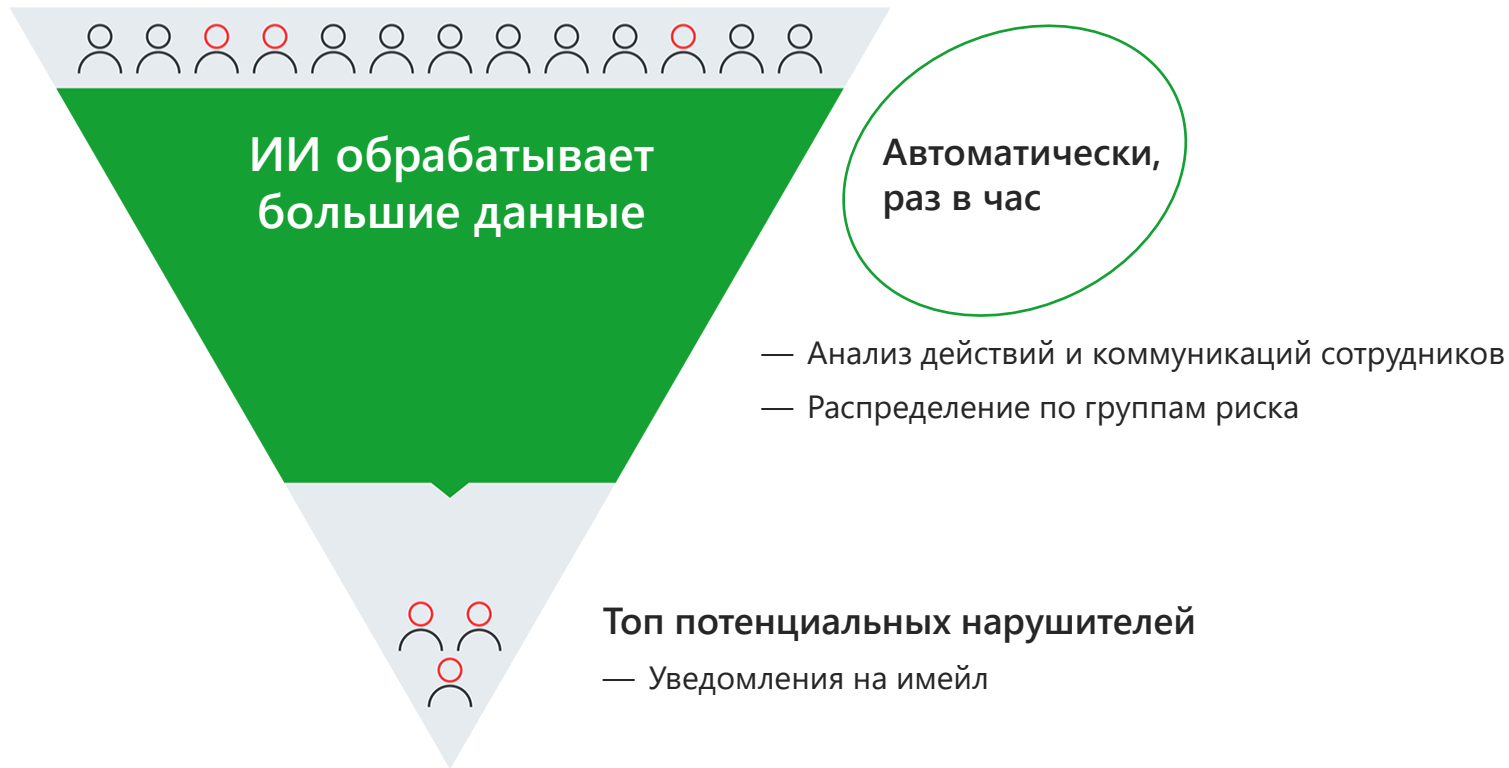


Посещение веб-сайтов



Рабочая и нерабочая активность

InfoWatch Prediction — поведенческая аналитика на основе искусственного интеллекта



Автоматический анализ действий и коммуникаций сотрудников



Искусственный интеллект учитывает

- Количественные параметры
- Аномальности
- Регулярности
- Нерабочее время
- Тренды

Автоматическое распределение сотрудников по группам риска



Рейтинг в группе риска =

- + Набор аномалий и их значимость
- + Набор паттернов и их уровень риска

Аномальный вывод информации

Подготовка к увольнению

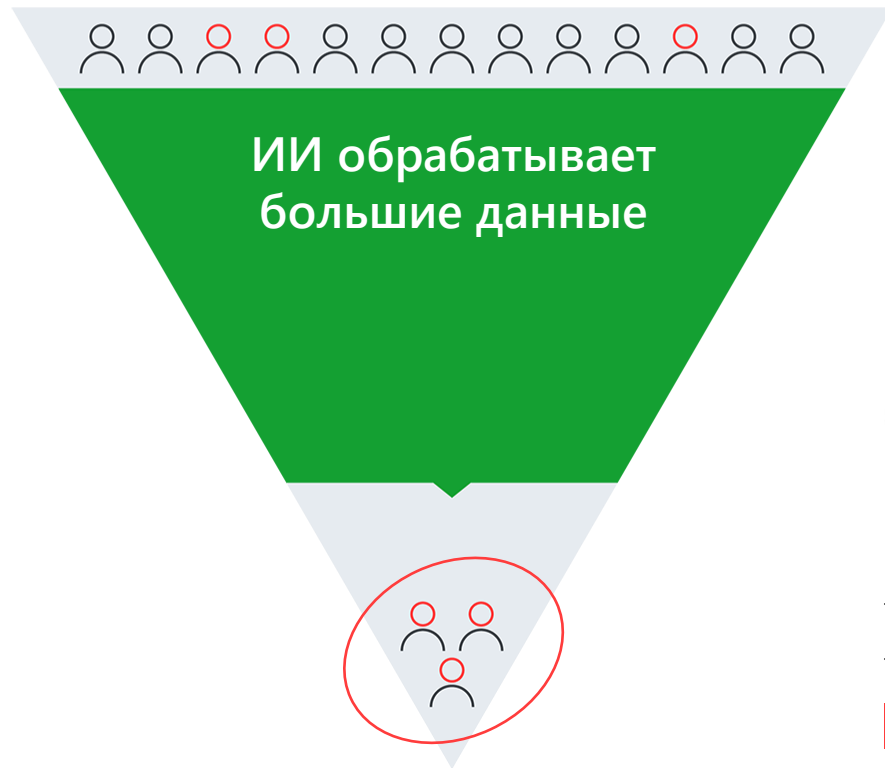
Нетипичные внешние коммуникации

Отклонение от бизнес-процессов

Нелояльные сотрудники

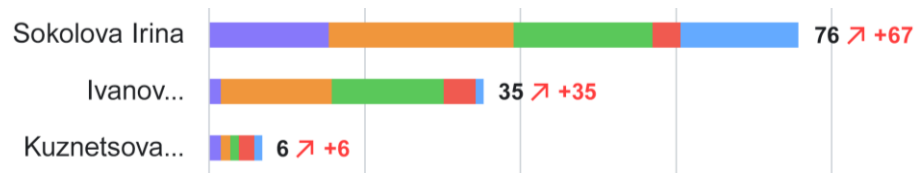
Снижение производительности

Автоматическое составление рейтинга подозрительных сотрудников



Совокупный рейтинг подозрительных сотрудников =

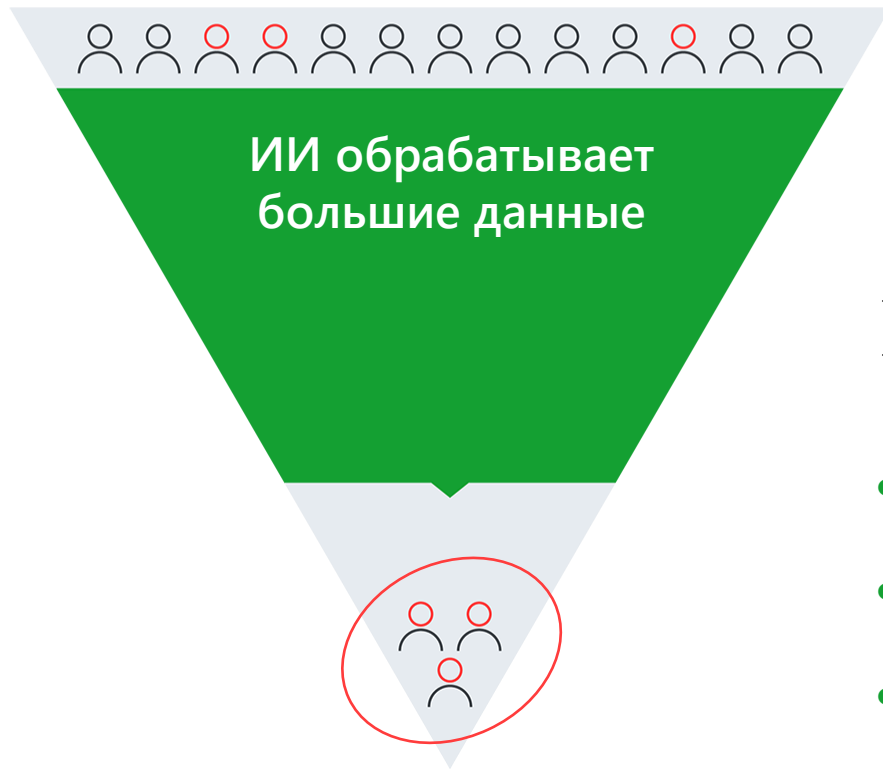
- + Набор аномалий и уровень риска
- + Паттерны поведения
- + Группы риска и их опасность



- Сотрудник может попасть сразу в несколько групп
- Сортировка по уровню риска и по его изменению

ВРУЧНУЮ НЕВОЗМОЖНО

Рейтинг подсказывает, на кого обратить внимание и проверить



Специалист ИБ получит уведомление об изменении рейтинга. Он может поставить сотрудников на контроль и провести проверку:

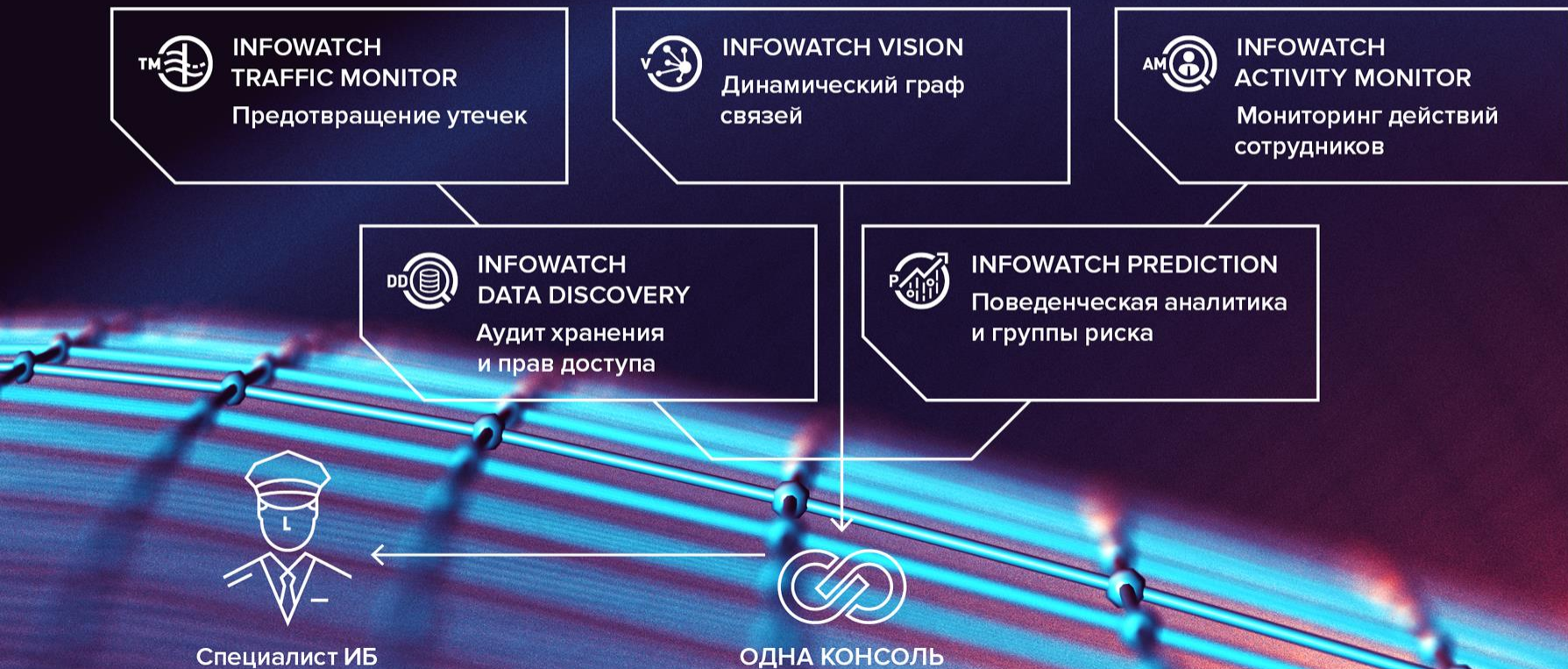
- Динамика аномалий
- Переход к деталям событий для проверки подозрений



- **Досье InfoWatch Prediction**
Динамика аномалий и цепочки событий
- **InfoWatch Activity Monitor**
Действия сотрудника за ПК — со скриншотами и аудио
- **InfoWatch Traffic Monitor и InfoWatch Vision**
События DLP-системы и граф коммуникаций

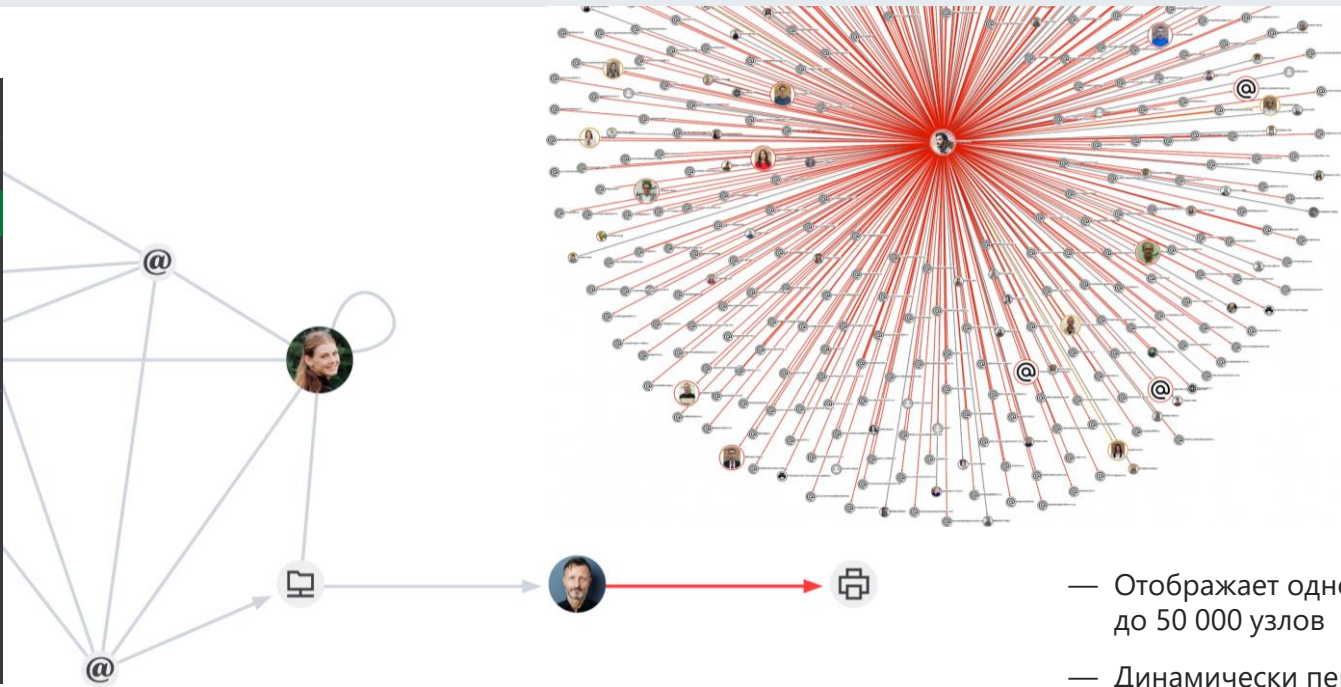
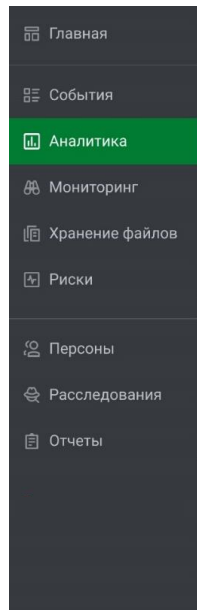
Центр расследований InfoWatch

Единая консоль DLP: События. Персоны. Файлы. Риски. Аналитика



Интерактивный граф связей

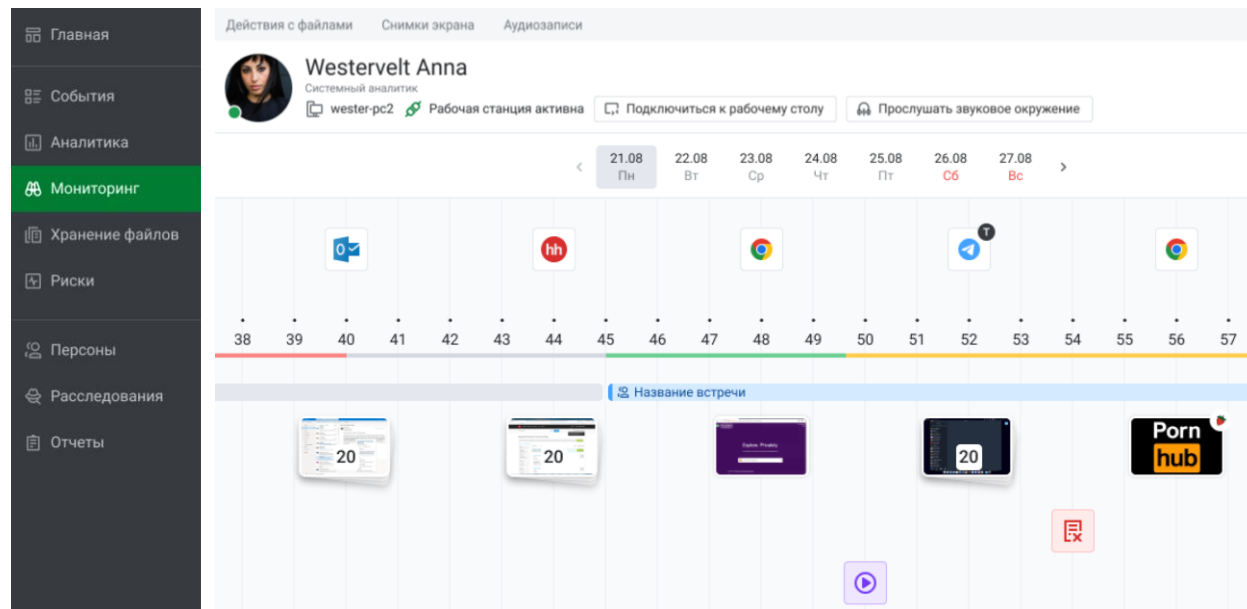
Найти всех соучастников, выявить неявные связи и пути перемещения документов



- Отображает одновременно до 50 000 узлов
- Динамически перестраивается при применении фильтров
- Данные для фильтрации можно выбрать прямо на графе

Интерактивный таймлайн действий

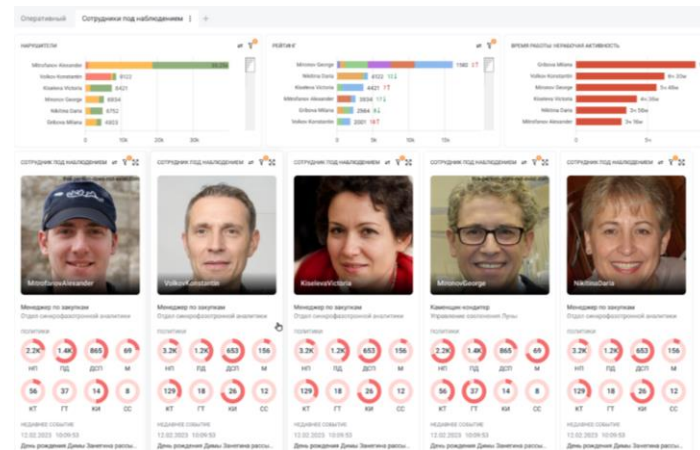
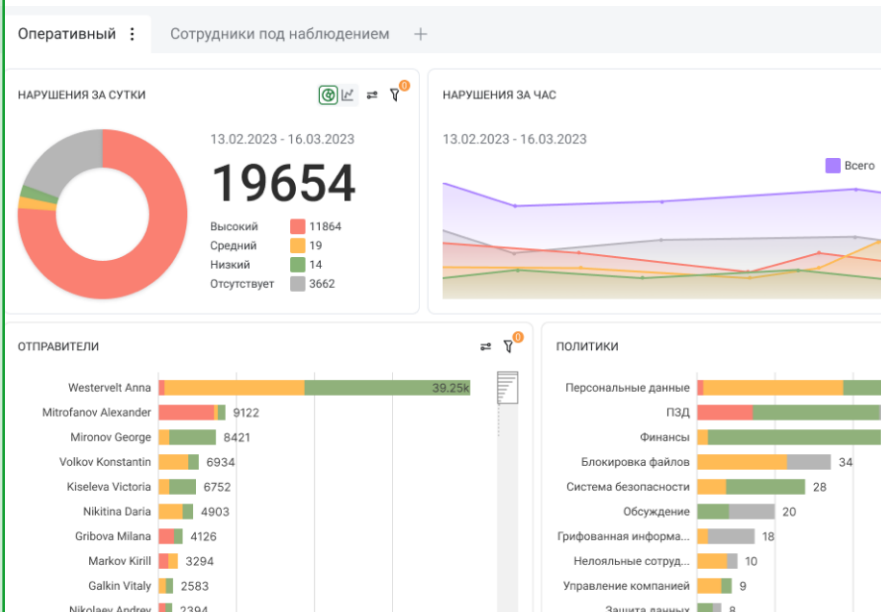
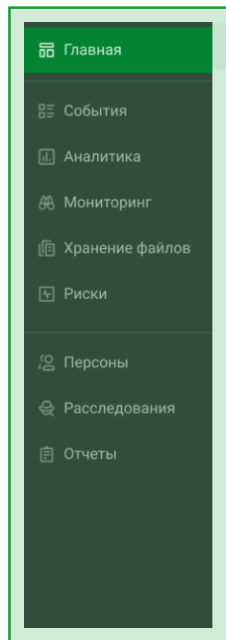
Восстановить полную картину — что делал сотрудник до, во время и после инцидента



- Проходы по СКУД, входы и выходы из учётной записи, введённый с клавиатуры текст, поисковые запросы и открытые сайты, работа файлами и приложениями, снимки экрана, аудиозаписи и их расшифровка
- Визуализирует картину рабочего дня и позволяет восстановить контекст
- По клику на элементы таймлайна доступны детали всех событий

Настраиваемые рабочие панели

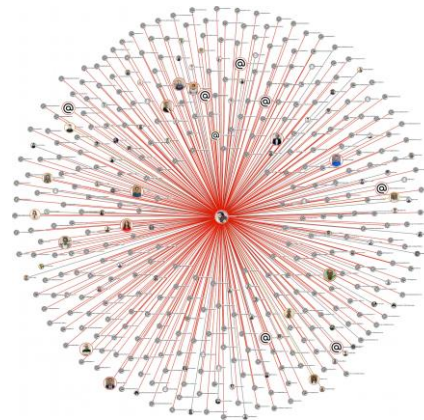
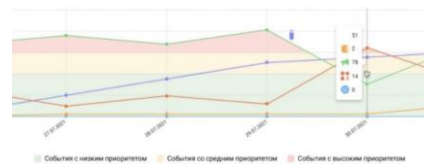
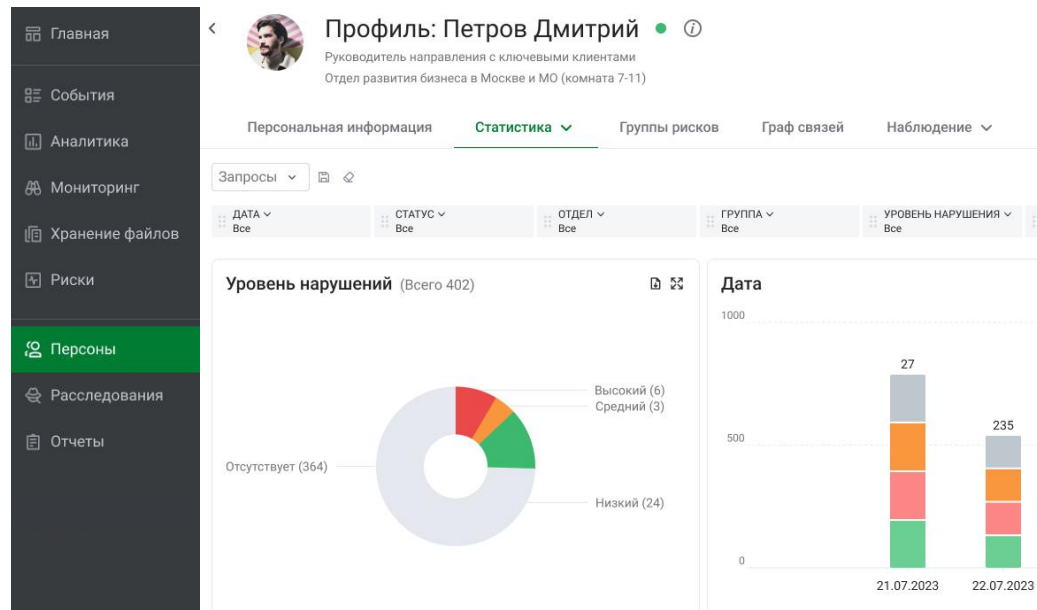
Искать самые критичные инциденты или сконцентрироваться на персонах под особым контролем



- 38 виджетов на выбор
- Можно настроить положение, порядок и размер

Единое досье сотрудников

Исчерпывающая информация по персоне



Персональная информация, нарушения, риски, карта коммуникаций, аудиозаписи с микрофона ПК, снимки и видео экрана

Редактор расследований

Обобщить, представить в соответствии с методологией или формой отчётности

Главная

События

Аналитика

Мониторинг


Хранение файлов


Риски


Персоны


Расследования

Отчеты




1  Maltseva Ksenya
Системный аналитик




2  Событие




3  Событие

4  Название файла.doc
26.27 KB

5 Мальцева Ксения предпринимает попытки с конкурентами в обход Компании.

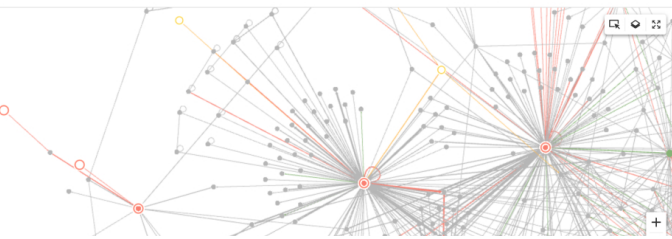
27 марта 2023 г., 12:50:53    Работы в завод ИМ. Я.М. Сверлова ДЗЕРЖИНСК TM_1 (3022) ⋮

27 марта 2023 г., 12:50:53    Отправка данных на веб ресурс: 10.60.20.192 TM_1 (3022) ⋮

27 марта 2023 г., 12:50:53    Передача фалов по FTP 178.16.25.36 TM_1 (3022) ⋮

Передача персональных данных

ПЕРИМЕТР	ИНТЕГРАЦИЯ	ЧАСЫ	ДАТА	ПРИЛОЖЕНИЕ	ОТДЕЛ	ОТПРАВИТЕЛЬ	ПОЛУЧАТЕЛЬ
Все	Все	Все	19 апреля - 18 мая	Все	Все	Все	Все
ТИП ФАЙЛА	ПОКИНУЛО ПЕРИМЕТР	НАЛИЧИЕ ВЛОЖЕНИЙ	СТАТУС	ТЕМА ПИСЬМА			
Все	Все	Все	Все	Все			



Список событий 43205

Mitryaev Evgeniy → v-files-01.infowatch.ru

Копирование файла на сетевой ресурс \\V-FILES-01.infowatch.ru\Privat...

Mitryaev Evgeniy → 10.70.10.98

Отправка данных на веб-ресурс: 10.70.10.98

Mitryaev Evgeniy → 10.70.10.98

Отправка данных на веб-ресурс: 10.70.10.98

Mitryaev Evgeniy → Не удалось определить

Ввод текста с клавиатуры в приложение

Mitryaev Evgeniy → 10.70.10.77

Отправка данных на веб-ресурс: 10.70.10.77

Mitryaev Evgeniy → 10.70.10.77

Формирование результатов расследования в виде документа без перехода в сторонние приложения

1. Добавить досье персон — объекта расследования и связанных лиц
2. Добавить события DLP-системы из Vision
3. Добавить изображения — скриншоты ПК, фото, сканы документов, скриншоты графа связей и диаграммы виджетов
4. Приложить любые файлы
5. Написать пояснения

Кейс. Выявление факта промышленного шпионажа

Горнодобывающее предприятие перешло государству после ухода иностранной компании.
Часть сотрудников высылала отчёты бывшему руководству

1	Главная+ Риски	Специалист СБ получил уведомление о сотрудниках в группе риска «Нетипичные внешние коммуникации»
2	Главная+ События	Специалист СБ поставил сотрудников на контроль, ужесточил политики безопасности и вовремя заметил нарушения — пересылку конфиденциальных материалов
3	Аналитика	На графе связей по интенсивности коммуникаций выявлена группа нарушителей
4	Мониторинг	Специалист СБ собрал доказательную базу — как готовился и протекал слив информации

Кейс. Тендерное мошенничество.






Анализ рейтинга сотрудников

Специалист СБ обнаружил на 1 месте в рейтинге InfoWatch Prediction сотрудника департамента конкурсных закупок

Рейтинг

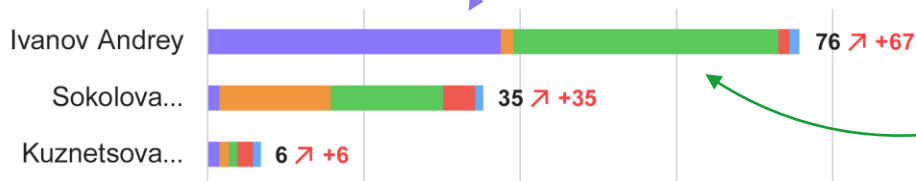
↓ По уровню риска

По изменению уровня риска

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

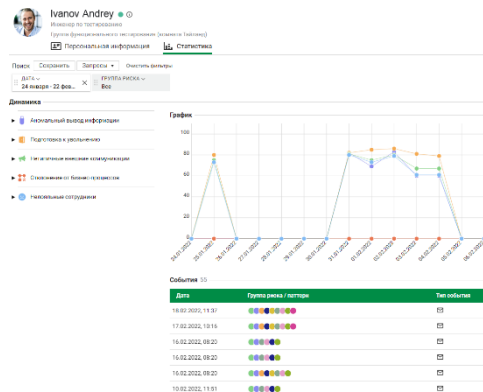
Аномальный вывод информации

Нетипичные внешние коммуникации



Кейс. Тендерное мошенничество.

Проверка деталей в досье



1 Некоторым потенциальным контрагентам информация о предстоящих закупках рассылалась лично, без добавления коллег в копию, общение неформальное

2 В рабочий день за пределами рабочего времени скопировано более 400 корпоративных документов →



Проверка деталей событий

- **Сотрудник отправил:** информацию о тендерах, КП, решения совета директоров, информацию об отгрузках, приглашения на тендеры
- **Под действие политик попало только 35 файлов из 400, остальные в «серой зоне»**

Последующий контроль выявил предоставление преференций некоторым контрагентам. Руководству компании вовремя предоставлен отчёт. Политики безопасности обновлены

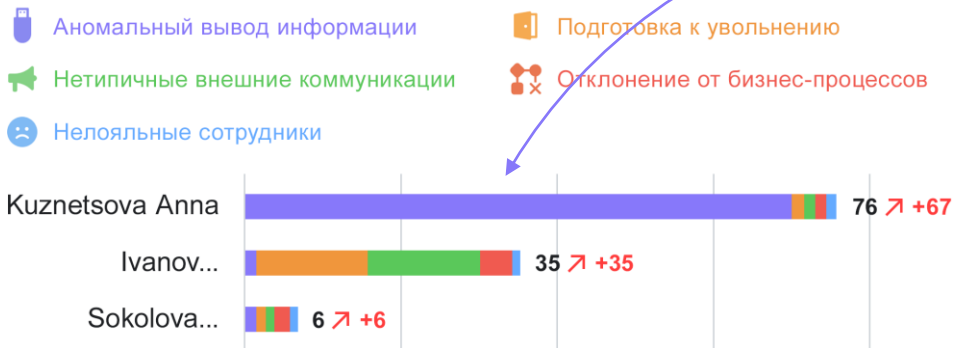
Кейс. Массовый вывод информации. Анализ рейтинга сотрудников

Специалист СБ обнаружил на 1 месте в рейтинге InfoWatch Prediction инженера производственно-технического отдела

Рейтинг

↓ По уровню риска

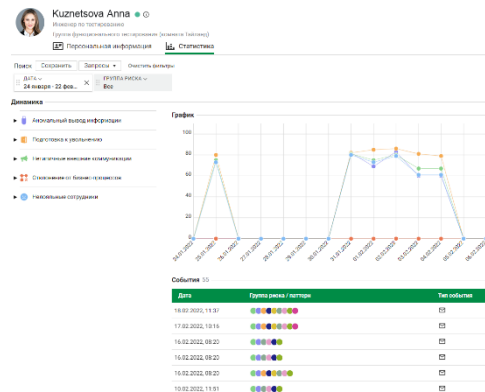
По изменению уровня риска



Аномальный вывод информации

Кейс. Массовый вывод информации.

Проверка деталей в досье



1 На протяжении недели, даже в выходные, массово копировал документы на внешний носитель — **800 документов** →

Проверка деталей событий

- Сотрудник отправил: технологические карты, акты, согласующие письма, паспорта качества, журналы продукции, личные документы под паролем — рекомендации по трейдингу, кредитные договоры
- Под действие политик попало только 18 файлов из 800, остальные в «серой зоне»

2 Самые массовые копирования, более 200 и 400 файлов, за границами рабочего дня — до 9:00 и после 18:00

Сотрудник поставлен на особый контроль. Ужесточена политика копирования на внешние носители. Файлы под паролем проверены на предмет утечки

Расследования и контроль выходят на новый уровень



- **Единая консоль: персоны, события, файлы, аналитика, риски**

Быстро анализировать разные срезы данных, сопоставлять с виду разрозненные события — все данные под рукой

- **Интерактивные инструменты**

Граф связей и временная шкала — кликабельные, с детализацией и мгновенной перестройкой

- **Поведенческая аналитика**

Машинное обучение для обработки больших данных — возможность сконцентрироваться на ключевых решениях

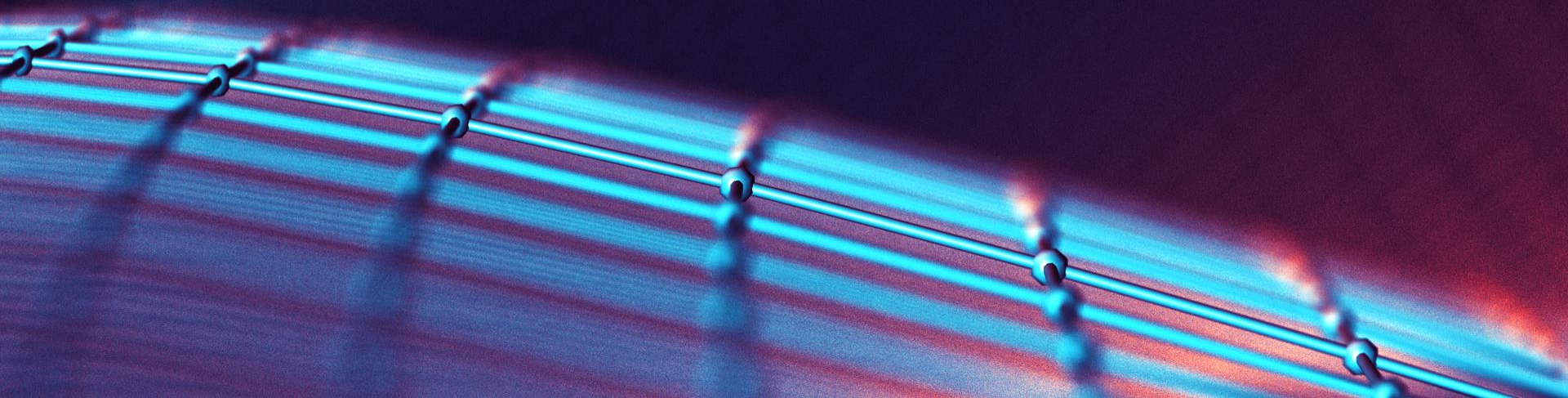
Зарегистрируйтесь на онлайн-премьеру
Центра исследований InfoWatch!



ЕДИНАЯ КОНСОЛЬ СРЕДСТВ ИБ: СОБЫТИЯ. ПЕРСОНЫ. ФАЙЛЫ. АНАЛИТИКА. РИСКИ

infowatch.ru

В 3 раза быстрее сбор
значимых обстоятельств
и контроль сотрудников
под наблюдением



БРОНИРУЙТЕ БЕСПЛАТНЫЙ ПИЛОТ

PREDICTION.INFOWATCH.RU

Как получить максимум от поведенческой аналитики InfoWatch?

Спецпредложение от Академии InfoWatch —
бесплатное обучение до 14.04.24

ПРОМОКОД «АКАДЕМИЯ2024»



Пётр Дьячков

Менеджер по развитию продуктов,
InfoWatch

Petr.Diachkov@infowatch.com