INFOWATCH®

ВЗГЛЯНЕМ ПО-НОВОМУ НА ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ИНФОРМАЦИИ

в условиях затянувшейся удалёнки

Степан Дешевых
Руководитель отдела развития продуктов InfoWatch

Удалённая работа обострила необходимость контроля происходящего на рабочем месте

- Нельзя прерывать бизнес-процессы
- Сотрудников не видно и не слышно
- Изменившиеся условия потребовали новых инструментов коммуникации

Удалённая работа обострила необходимость контроля происходящего на рабочем месте

INFOWATCH®

Раньше

Сейчас

zoom

slack и многие другие

Как навести порядок на удалёнке?

- Навести порядок в цифровых активах

- Создать регламенты, по которым будут работать сотрудники

- Выдать сотрудникам оборудование, на котором сможете осуществлять контроль в соответствии с регламентами

А что делать с полученными данными?

А куда развиваться дальше?

INFOWATCH®

1. **Менять подходы** к выявлению утечек и заниматься не только констатацией фактов утечек, но и:
   - Проводить **полноценные расследования** для выявления всех причин утечек
   - Заниматься **профилактикой утечек**
   - **Идти** от констатации фактов утечки **к их прогнозированию**

---

2. **Расширять области применения,** предлагая DLP-системы в качестве инструмента экономической безопасности, HR-службам, другим подразделений и руководству

Принципиальные недостатки DLP-систем

INFOWATCH®

1	**Анализ** перехваченных сообщений производится **вне контекста** предыдущих сообщений	• Пример: 3 КП от разных компаний с одного адреса • Пример: 3 КП от разных компаний с разных адресов, но с минимальными временными интервалами • Пример: группа риска «Жизнь не по средствам»
2	DLP-системы автоматически **не обрабатывают факт отсутствия информации** (а отсутствие информации — это тоже информация)	• Пример: отсутствие активности в течение, например, 45 суток — признак инцидента ИБ (не удалённый вовремя аккаунт уволенного сотрудника) или инцидента ЭБ («мёртвая душа») • Пример: отсутствие поздравлений — один из признаков фиктивного или аффилированного контрагента

Как выявить угрозу в океане данных?

Предпосылки

- **Угроза** в современной системе **выглядит** не как одно событие, а **как цепочка**
- Цепочки событий **отличаются от нормальных**
- Цепочки событий одной и той же угрозы **похожи между разными компаниями**

Как выявить угрозу в океане данных?

Решение: Prediction

- **Накапливает знания** о типичных угрозах
- **Выделяет в потоке событий цепочки** характерные для угроз и обозначает риски
- **Адаптируется** к специфичным внутри компании условиям с помощью алгоритмов AI / Machine Learning

INFOWATCH®

МОДУЛЬ INFOWATCH PREDICTION

Модуль InfoWatch Prediction. Принципы работы

- **Широкий круг решаемых задач, например:**
  - Выявление аномалий поведения объектов
  - Выявление взаимосвязанных событий (цепочек событий)
  - Автоматизация выявления принадлежности к группам риска
  - Выявление признаков корпоративного мошенничества по известным паттернам
- **Возможность быстрой настройки под задачи пользователя**

Модуль InfoWatch Prediction. Принципы работы

- **Полноценный поведенческий анализ объектов**

— **Персон** — коммуникации и их характер (на основе статистики и лингвистического анализа), статистика и характер действий на р/с, статистика и характер работы с приложениями, статистика и характер работы с информацией и т. п.

— **Документов** — статистика и характер пересылок, работы и хранения, аномальные отклонения от нормальных маршрутов перемещения документов и режимов обработки

— **Коммуникаций** — анализ статистики и характера переписки с контрагентом позволяет, например, выявлять признаки мошеннических схем типа «диллерская матрёшка»

Цели поведенческого анализа — выявление аномалий поведения, выявление потенциально опасных цепочек действий, выявление принадлежности к группам риска

Модуль InfoWatch Prediction. Кейсы

«Мёртвые души»

- **Выводим в интерфейс счётчик событий за последние 45 дней**
- **Фильтруем**
  - По значению «0»
  - Исключаем также аккаунты, от которых и не должно быть событий в системе DLP
- **Получаем список аккаунтов с нулевой активностью**
- **Проверяем цепочки. Например «Приказ на увольнение» - «Активность 0»**

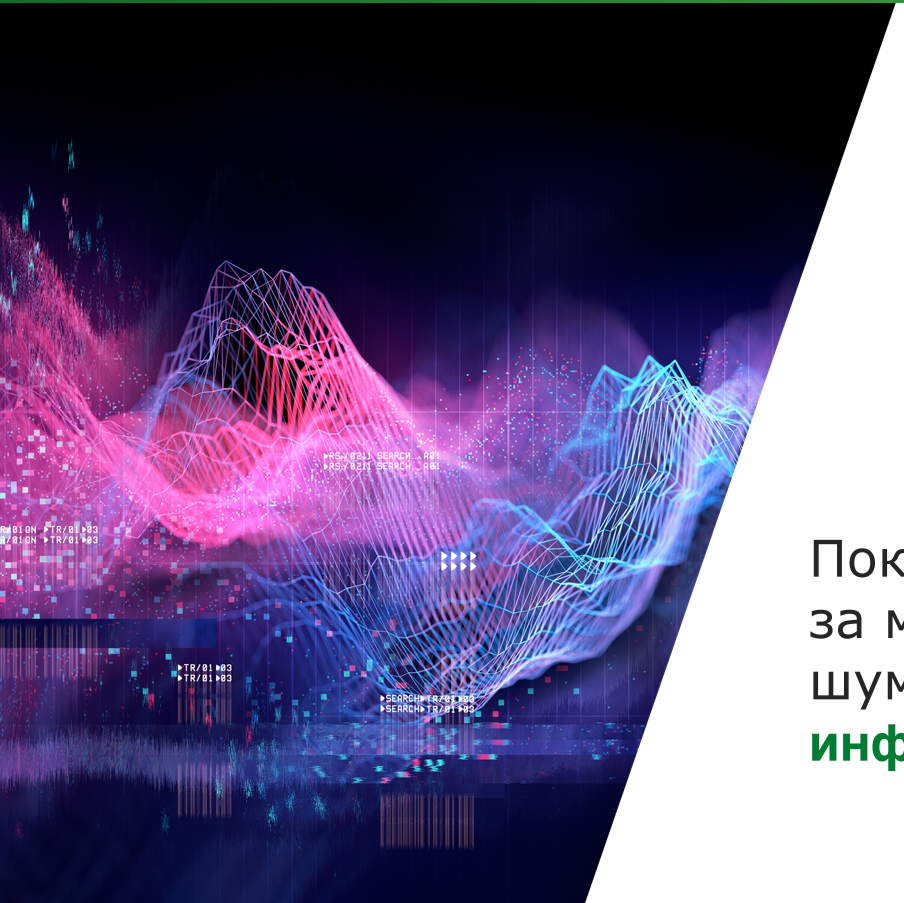
Чем больше компания, тем сложнее поиск угроз в океане данных

InfoWatch Prediction

- Широкий спектр задач: **ЭБ, ИБ**
- Агрегирует **знания многих ОБ**
- Ищет **паттерны угроз** и подсвечивает их
- Может использовать **алгоритмы ML**
- Помогает **сфокусироваться на главном**
- Позволяет **не только реагировать на уже произошедшее** и разбираться в причинах, **но и предвидеть риски**

InfoWatch Vision — это «BI для DLP»

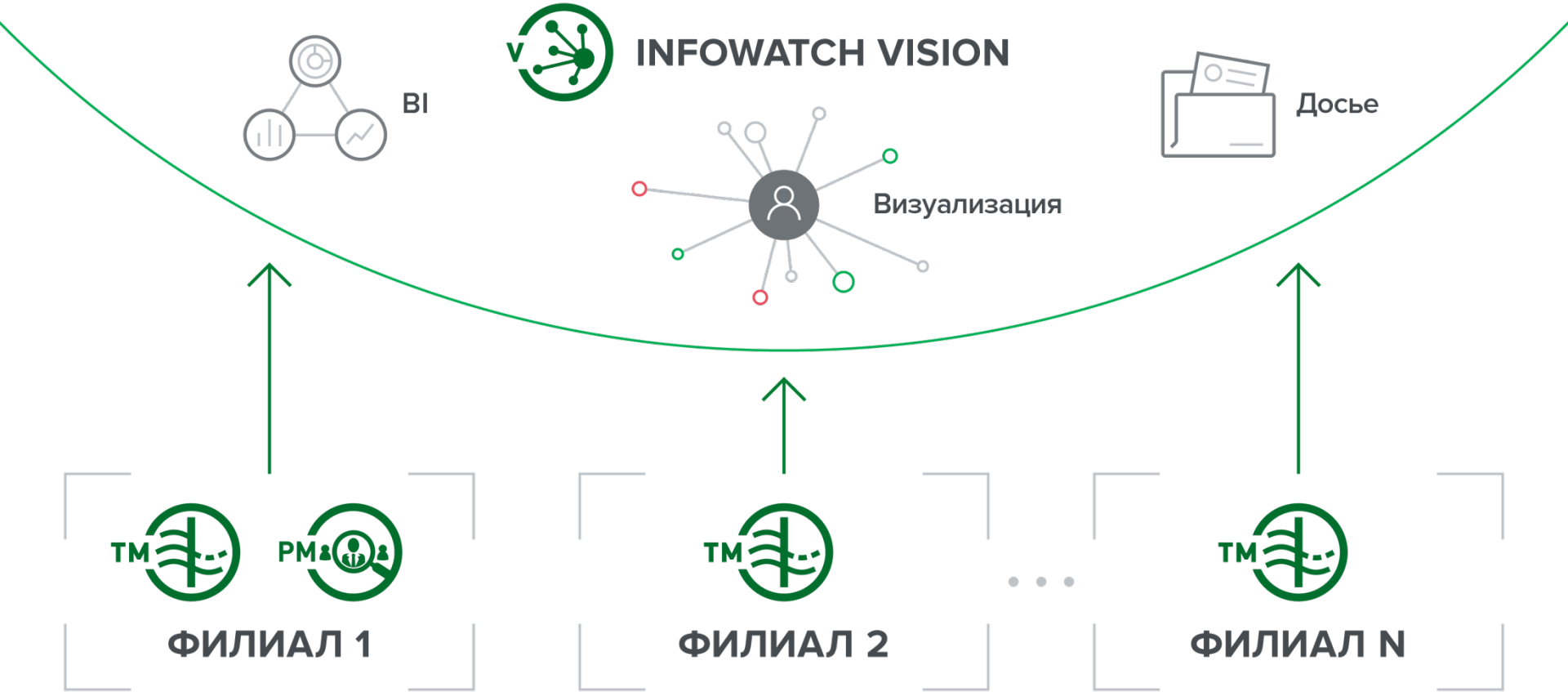
INFOWATCH®



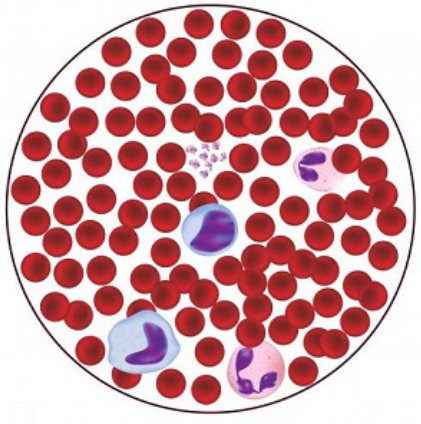
Инструмент визуального анализа данных, который повышает КПД и расширяет область применения DLP-системы InfoWatch Traffic Monitor

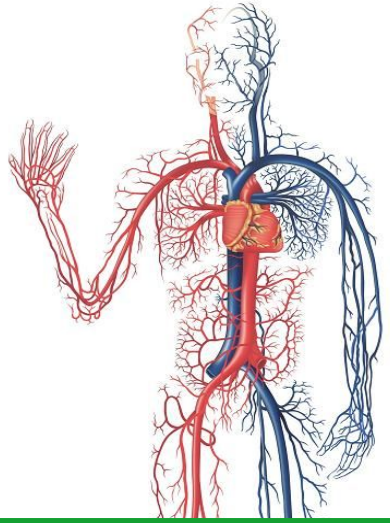
Показывает историю, которая кроется за миллионами сухих фактов, убирает шум и **подсвечивает полезную информацию**

Что такое InfoWatch Vision



О чём могут рассказать данные





Обычное DLP-решение

— Анализ отдельных событий
— Круг общения одной персоны
— Маршрут перемещения файла

InfoWatch Vision

— Карта коммуникаций всей компании
— Маршруты перемещения конфиденциальной информации
— Drill-down с уровня компании до отдельных событий

INFOWATCH®

Больше возможностей применения для топ-менеджеров и HR-служб

- **Обнаружить проблемы взаимодействия** между подразделениями
- **Выявить узкое место** в коммуникациях и центры экспертизы
- **Восстановить разорванные связи** при увольнении сотрудника
- **Выявить внутренние конфликты** и нарушения правил коммуникации
- **Учесть неформальные связи** при принятии управленческих решений

Мы растём вместе с нашими клиентами

INFOWATCH®

Чем больше компания, тем сложнее поиск угроз в океане данных.

Есть решение

InfoWatch Activity Monitor

Сбор и протоколирование действий сотрудников

InfoWatch Traffic Monitor

Контентный анализ и обогащение протокола

InfoWatch Vision

Helicopter view и поддержка расследований

InfoWatch Prediction

От алгоритмов InfoWatch — целеуказание на возможные проблемы

БУДЕМ ПРОБОВАТЬ РЕШЕНИЯ INFOWATCH В ДЕЛЕ?

Степан Дешевых
Руководитель отдела развития продуктов InfoWatch

INFOWATCH®

Больше полезной информации:

/InfoWatchOut

/InfoWatch

/infowatchnews

Подписывайтесь на рассылки

Stepan.Deshevykh@infowatch.com

infowatch.ru