BIS SUMMIT 2020

ПРЕДИКТИВНЫЙ АНАЛИЗ РИСКОВ НА ОСНОВЕ ДАННЫХ ИЗ DLP

Подходы, методики, применение

Степан Дешевых

Руководитель отдела развития продуктов, InfoWatch

Удалённая работа обострила необходимость контроля происходящего на рабочем месте

BIS SUMMIT 2020

- Сотрудники оказались оторваны от компании
- Нельзя прерывать бизнес-процессы
- Изменившиеся условия потребовали новых инструментов коммуникации

Удалённая работа обострила необходимость контроля происходящего на рабочем месте

BIS SUMMIT 2020

Раньше



Сейчас

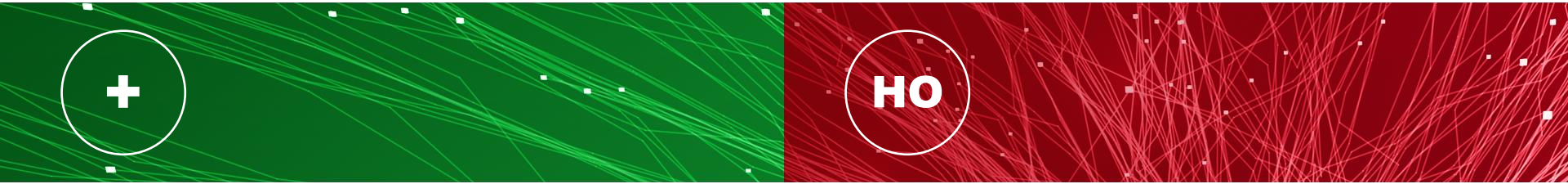





и многие другие

Развитие DLP решает одни проблемы и создаёт другие

BIS SUMMIT 2020



Охват каналов системами перехвата увеличивается

Растёт и сложность восприятия и оценки информации

Как выявить угрозу в океане данных?

BIS SUMMIT 2020

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?

BIS SUMMIT 2020

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

Prediction: дополнительный электронный мозг

BIS SUMMIT 2020

Помогает в потоке событий выявить важные

- **Обратить внимание** офицера на потенциальные или реализующиеся в текущий момент угрозы
- **Визуализировать** их на своём табло или показать в **Vision**

Области применения

- **Информационная** безопасность
- **Экономическая** безопасность
- **Выявление аномалий** поведения сотрудников и потребления ими информации

Применение: увольняющиеся сотрудники

BIS SUMMIT 2020

Мы используем AI / Machine Learning в составе продукта InfoWatch Prediction:

- **Выявляем признаки поведения** сотрудника, сходные с признаками поведения уволившихся
- **Успешно применяем** в двух компаниях и стабильно показываем 4 сотрудников из 10, которые решают уволиться

Потенциал применения технологии

- **Выявление и подсветка аномалий** поведения сотрудников относительно привычного хода вещей

Применение: медленный вывод информации

BIS SUMMIT 2020

Для информационной безопасности

- Автоматическое выделение сотрудников, которые осуществляют **вывод существенных объёмов информации небольшими порциями**

Как выявляется

- Анализируется суммарный вывод информации в режиме «**бегущего окна**»
- Например, подсвечиваются сотрудники, которые **за последние 10 дней вывели больше 500 Мб**

Применение: выявление «прокладок»

BIS SUMMIT 2020

Для экономической безопасности

- Автоматическое выделение компаний, которые **проявляют признаки «прокладок»**

Как выявляется

- Анализ адресата, **выславшего КП** (иногда несколько КП на один конкурс подаются с одного адреса)
- Анализ **количества сообщений** в рамках конкурса
- Срабатывание БКФ **«роскошная жизнь»** или **«финансовые сложности»**

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**

BIS SUMMIT 2020

ОБСУДИМ?

Степан Дешевых

Руководитель отдела развития продуктов, InfoWatch