ИНФОСИСТЕМЫ ДЖЕТ

От DLP к расследованиям

Дмитрий Михеев,
эксперт Центра информационной безопасности
компании «Инфосистемы Джет»

DLP – это навсегда

Законы, практики и due diligence

План – закон, выполнение – долг

Делай все по регламенту

и будь счастлив

Все очень скучно

Риски, учет, автоматическая реакция, статистика.

Повторять до блеска

Риски, учет, автоматическая реакция, статистика.

DLP и реальная жизнь

Реальная жизнь

гораздо интереснее

Что мы на самом деле ищем в утечках?

В реальной жизни DLP – это живые люди

Houston, we have A……..

- **Что именно произошло и почему?**
- **Что за человек мог так сделать?**
- **Кого именно можно подозревать и кто скорее всего сделал?**
- **Что еще мог сделать такой человек?**
- **Какие следующие вероятные его или ее шаги?**
- **Что за информацию еще нужно иметь для расследования и какова ее точность?**
- **Достаточно ли доказательств?**

- **Что именно предпринять далее?**

Единство и борьба

Нарушитель – какой он?

- **Экология нарушения**
  - **Место-время, инструмент-объект, рутина-новизна**
- **Социальный климат и роли**
  - **Профессия и род занятий**
  - **Образование**
  - **Скажи мне, кто твой друг и другие связи.**
- **Выгоды и Возможности = Действия**
  - **Перекосы оценки последствий**
- **Устойчивое поведение**
  - **Нарушитель изменяет мир своими действиями**
  - **.**
- **Развитие и изменение поведения**
  - **Взросление и опыт**
  - **Обучение**
  - **Карьера**

Что мы собственно хотим получить?

- **Сбор и обработка информации о людях и их поведении в удобном для анализа виде**

  Все эти тонкости нужно уметь записать и найти.

- **Помощь в принятии решений по нарушениям**
  - **Регламенты**
  - **Подсказки**
  - **Шаблоны**

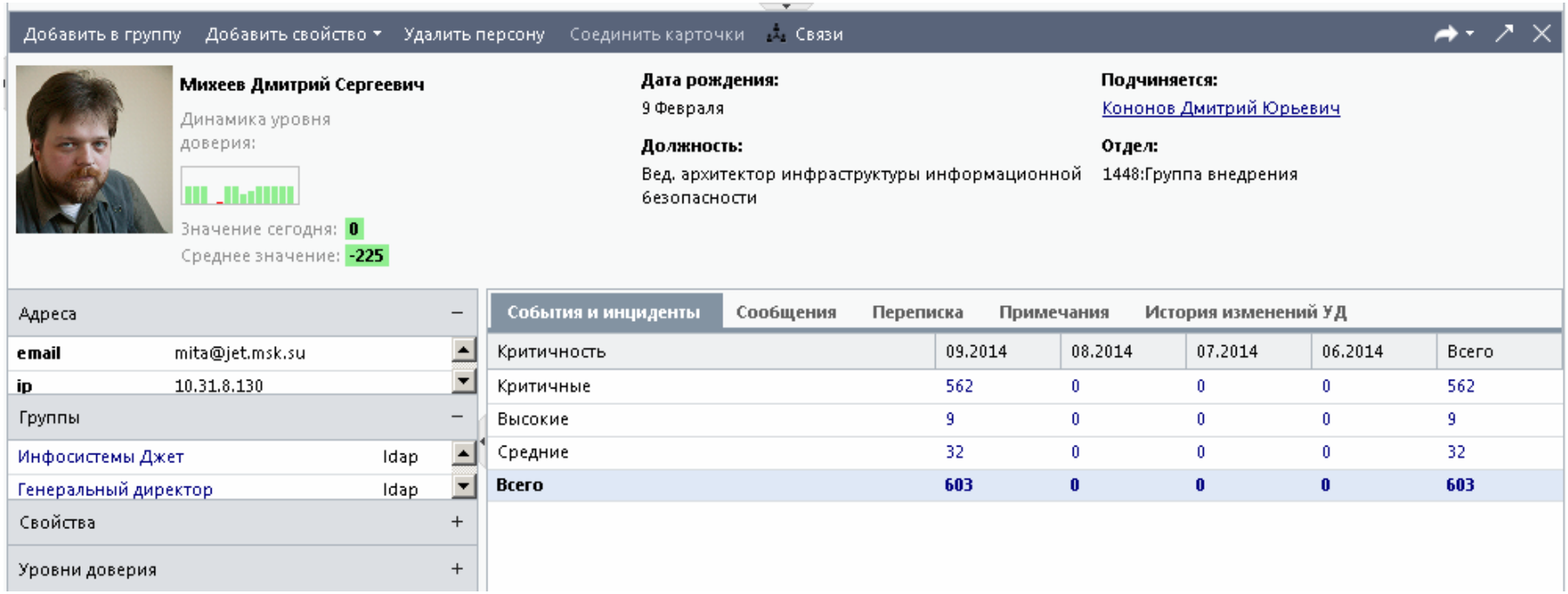
- **Экономию сил, времени и других ресурсов**

- **Документальную и организационную поддержку**

Если коротко:

- Чтобы регламенты соблюдались (сами);
- Чтобы риски было можно быстро описать;
- Контролировать все нужные каналы утечки;
- Приносить реальную пользу;
- **Иметь инструменты на случай неучтенных рисков;**
- **Найти, кто виноват.**

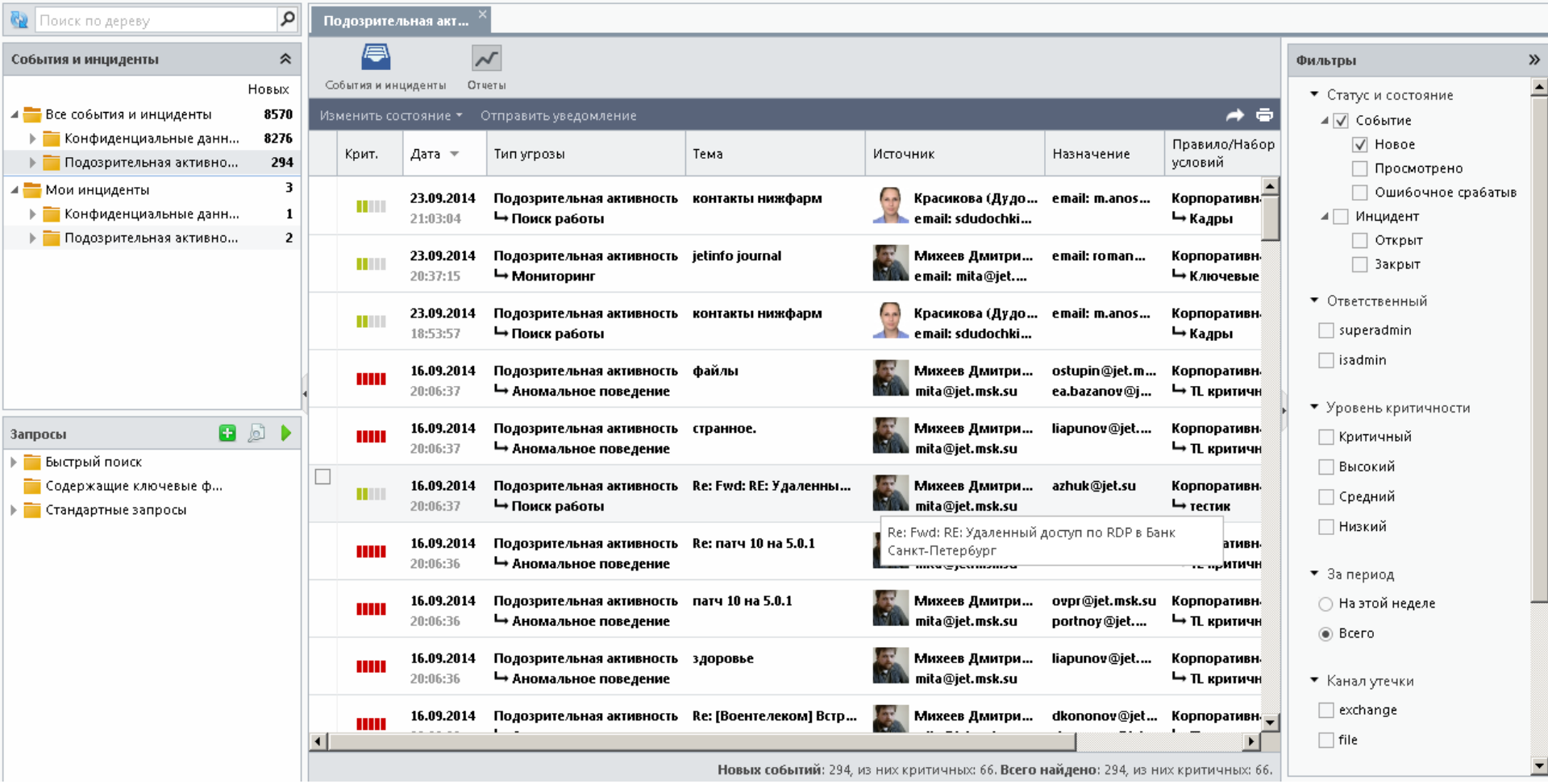
Досье и накопление знаний о человеке



Досье и накопление знаний о человеке

- Адреса и свойства
- Группы AD и собственные
- Срезы по переписке
- Инциденты
- Уровень доверия
- Дополнение данных извне

Что мы сделали в новой версии «Дозор-Джет»?



Что мы сделали в новой версии «Дозор-Джет»?

Что мы сделали в новой версии «Дозор-Джет»?

- Скоринг поведения пользователя и детектирование аномалий
- Уровень доверия, инциденты и досье
- Связи между пользователями
- Уточнения политики – шаблоны документов, исключения и другие механизмы

Простые радости жизни

Что далее?

- Работа с инцидентами как бизнес-процесс
- Интеграция с SOC и другими средствами
- Развитие детектирования аномалий
- Автоматизация регламентов разбора

ИНФОСИСТЕМЫ ДЖЕТ

Спасибо за внимание!

Дмитрий Михеев,
mita@jet.msk.su