



От DLP к расследованиям

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

DLP – это навсегда





Делай все по регламенту
и будь счастлив



Риски, учет, автоматическая
реакция, статистика.

Повторять до блеска

Риски, учет, автоматическая
реакция, статистика.

Реальная жизнь
гораздо интереснее

LIFE
IS
SIMPLE
SO
WE
COMPLICATE

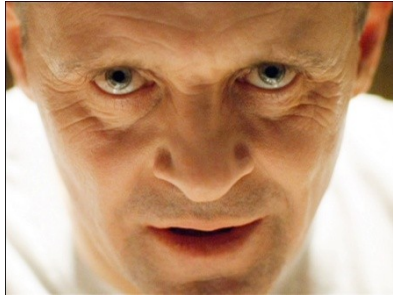
Что мы на самом деле ищем в утечках?



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?**



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



boshiaiparel.com made-in-china.com

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**

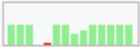


- Чтобы регламенты соблюдались (сами);
- Чтобы риски было можно быстро описать;
- Контролировать все нужные каналы утечки;
- Приносить реальную пользу;
- **Иметь инструменты на случай неучтенных рисков;**
- **Найти, кто виноват.**

Досье и накопление знаний о человеке

Добавить в группу Добавить свойство ▾ Удалить персону Соединить карточки Связи



Михеев Дмитрий Сергеевич
Динамика уровня доверия:

Значение сегодня: **0**
Среднее значение: **-225**

Дата рождения:
9 Февраля
Подчиняется:
[Кононов Дмитрий Юрьевич](#)
Должность:
Вед. архитектор инфраструктуры информационной безопасности
Отдел:
1448:Группа внедрения

Адреса

email mita@jet.msk.su

ip 10.31.8.130

Группы

Инфосистемы Джет Idap

Генеральный директор Idap

Свойства

Уровни доверия

События и инциденты

Сообщения

Переписка

Примечания

История изменений УД

Критичность	09.2014	08.2014	07.2014	06.2014	Всего
Критичные		562	0	0	562
Высокие		9	0	0	9
Средние		32	0	0	32
Всего		603	0	0	603

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



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

Поиск по дереву

События и инциденты

Новых

- Все события и инциденты 8570
 - Конфиденциальные данн... 8276
 - Подозрительная активно... 294
- Мои инциденты 3
 - Конфиденциальные данн... 1
 - Подозрительная активно... 2

Запросы

- Быстрый поиск
- Содержащие ключевые ф...
- Стандартные запросы

Подозрительная акт...

События и инциденты | Отчеты

Изменить состояние | Отправить уведомление

Крит.	Дата	Тип угрозы	Тема	Источник	Назначение	Правило/Набор условий
■ ■ ■	23.09.2014 21:03:04	Подозрительная активность ↳ Поиск работы	контакты нижфарм	Красикова (Дудо... email: sdudochki...	email: m.anos...	Корпоративн... ↳ Кадры
■ ■ ■	23.09.2014 20:37:15	Подозрительная активность ↳ Мониторинг	jetinfo journal	Михеев Дмитри... email: mita@jet...	email: roman...	Корпоративн... ↳ Ключевые
■ ■ ■	23.09.2014 18:53:57	Подозрительная активность ↳ Поиск работы	контакты нижфарм	Красикова (Дудо... email: sdudochki...	email: m.anos...	Корпоративн... ↳ Кадры
■ ■ ■ ■	16.09.2014 20:06:37	Подозрительная активность ↳ Аномальное поведение	файлы	Михеев Дмитри... email: mita@jet.msk.su	ostupin@jet.m... ea.bazanov@j...	Корпоративн... ↳ ТЛ критичн
■ ■ ■ ■	16.09.2014 20:06:37	Подозрительная активность ↳ Аномальное поведение	странное.	Михеев Дмитри... email: mita@jet.msk.su	liapunov@jet...	Корпоративн... ↳ ТЛ критичн
■ ■ ■	16.09.2014 20:06:37	Подозрительная активность ↳ Поиск работы	Re: Fwd: RE: Удаленны...	Михеев Дмитри... email: mita@jet.msk.su	azhuk@jet.su	Корпоративн... ↳ тестик
■ ■ ■ ■	16.09.2014 20:06:36	Подозрительная активность ↳ Аномальное поведение	Re: патч 10 на 5.0.1	Михеев Дмитри... email: mita@jet.msk.su	ovpr@jet.msk.su portnoy@jet...	Корпоративн... ↳ ТЛ критичн
■ ■ ■ ■	16.09.2014 20:06:36	Подозрительная активность ↳ Аномальное поведение	здоровье	Михеев Дмитри... email: mita@jet.msk.su	liapunov@jet...	Корпоративн... ↳ ТЛ критичн
■ ■ ■ ■	16.09.2014	Подозрительная активность	Re: [Воентелеком] Встр...	Михеев Дмитри...	dkononov@jet...	Корпоративн...

Новых событий: 294, из них критичных: 66. Всего найдено: 294, из них критичных: 66.

Фильтры

- Статус и состояние
 - ☒ Событие
 - ☒ Новое
 - ☐ Просмотрено
 - ☐ Ошибочное срабатыв
 - ☐ Инцидент
 - ☐ Открыт
 - ☐ Закрыт
- Ответственный
 - ☐ superadmin
 - ☐ isadmin
- Уровень критичности
 - ☐ Критичный
 - ☐ Высокий
 - ☐ Средний
 - ☐ Низкий
- За период
 - ☐ На этой неделе
 - ☒ Всего
- Канал утечки
 - ☐ exchange
 - ☐ file

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

Почему Дед Мороз всегда счастлив?

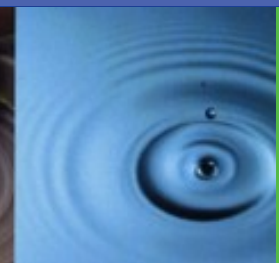
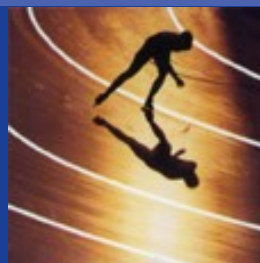


Потому что он знает, где живут все
плохие девчонки.

joyreactor.cc

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





Спасибо за внимание!

Дмитрий Михеев,
mita@jet.msk.su