Один день из жизни специалиста по ИБ: процедура управления инцидентами, выявленными DLP

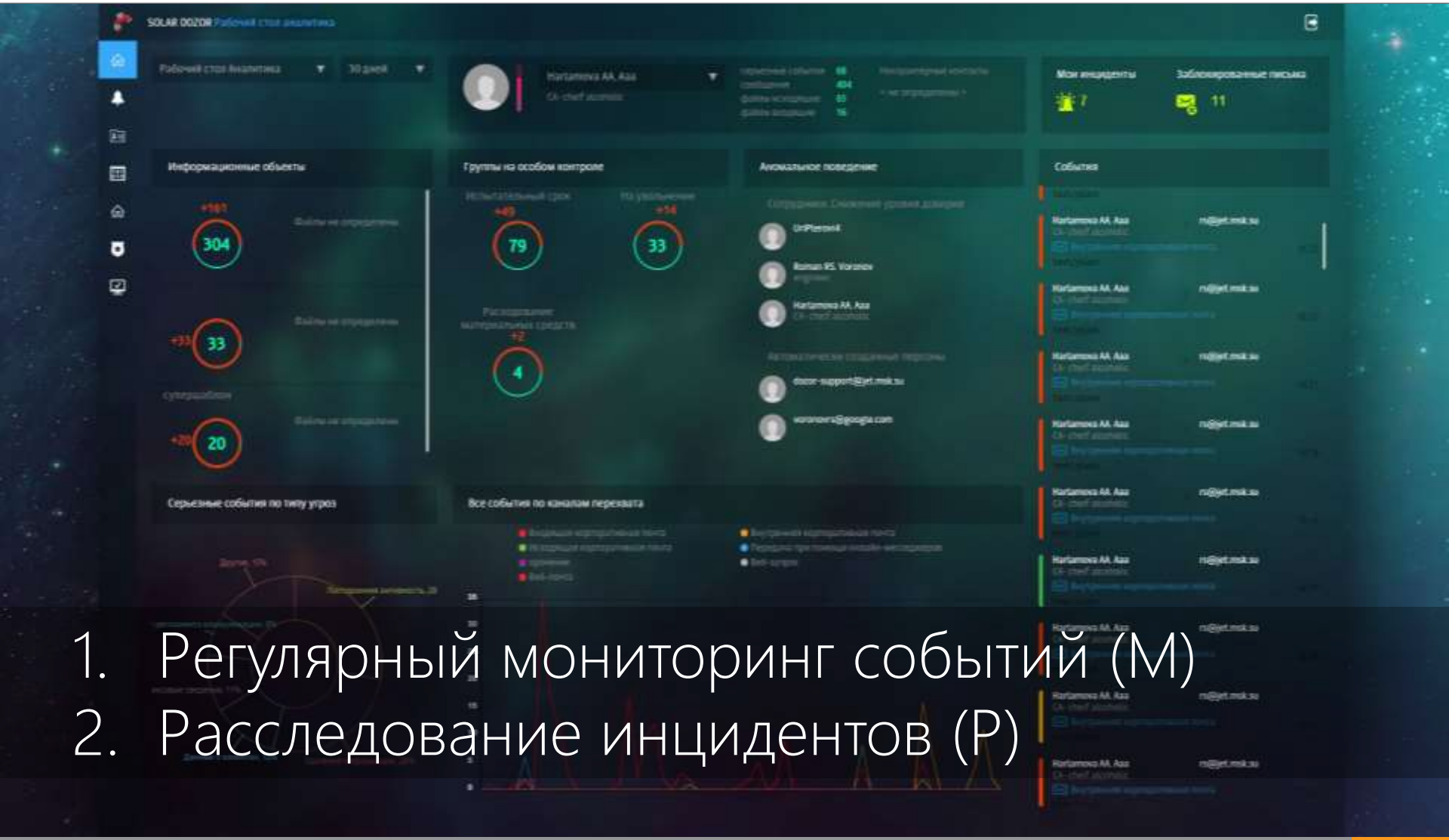
Прозоров Андрей, CISM
Руководитель экспертного направления
Компания Solar Security

Мой блог: 80na20.blogspot.com
Мой твиттер: twitter.com/3dwave

2015-10

DLP является средством автоматизации, но и специалист по ИБ без работы не останется…

Типовые сценарии работы с DLP



1. Регулярный мониторинг событий (М)
2. Расследование инцидентов (Р)

Зачем это нужно?

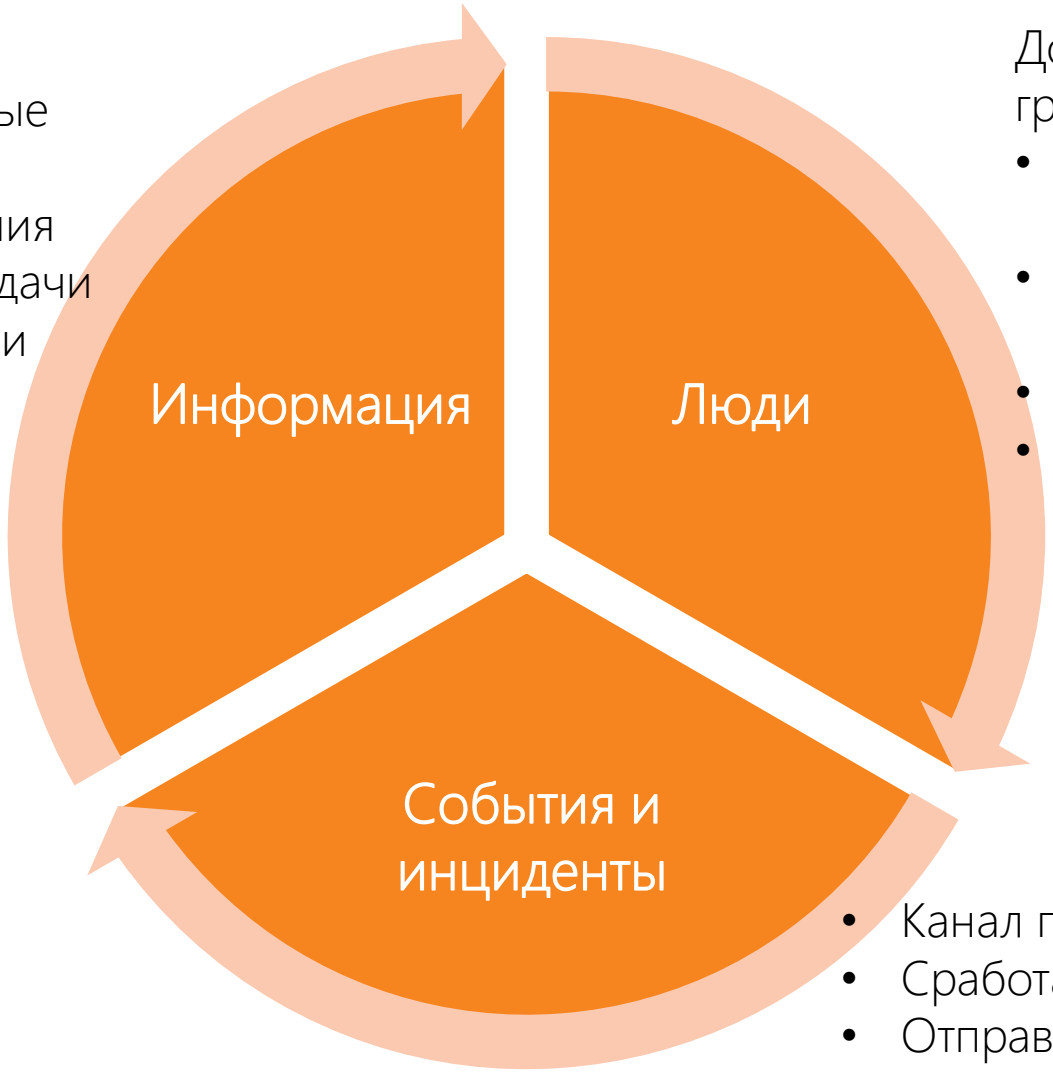
- Не каждое «событие» переходит в «инцидент» (M)
- Инциденты важно вовремя выявить (ограничения для дисциплинарных наказаний по ТК РФ) (M)
- Не за все «утечки» можно наказать строго (например, при записи информации на флешку нет факта «разглашения»). Но можно найти и другие нарушения… (P)
- Важно понимать, единственный инцидент или сотрудник регулярно нарушает (P)
- Можно выявить аномальное поведение и связи (M, P)
- Можно выявить всех участников (P)

Важнейшими элементами DLP становятся Архив всех сообщений и Инструменты работы с ним

Фокус внимания на самое важное

Досье на информационные объекты:

- места хранения
- каналы передачи
- отправители и получатели

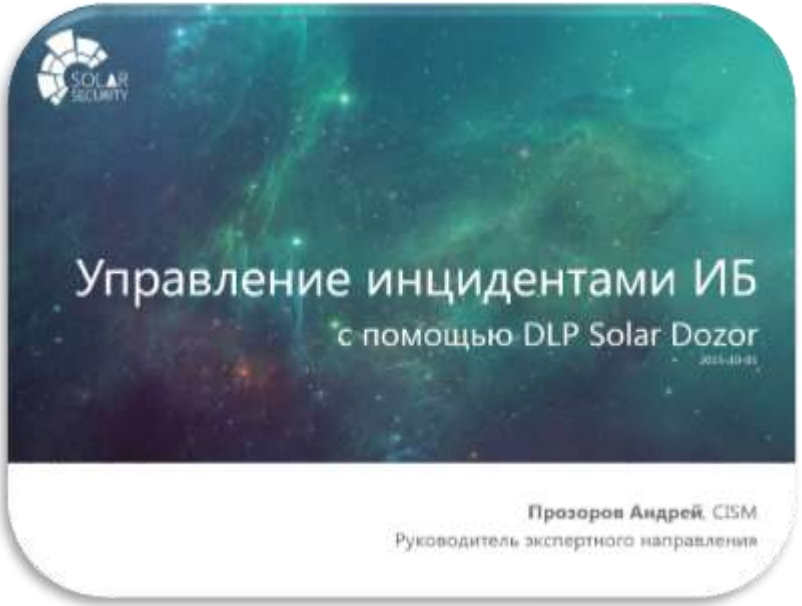


Досье на персон и группы:

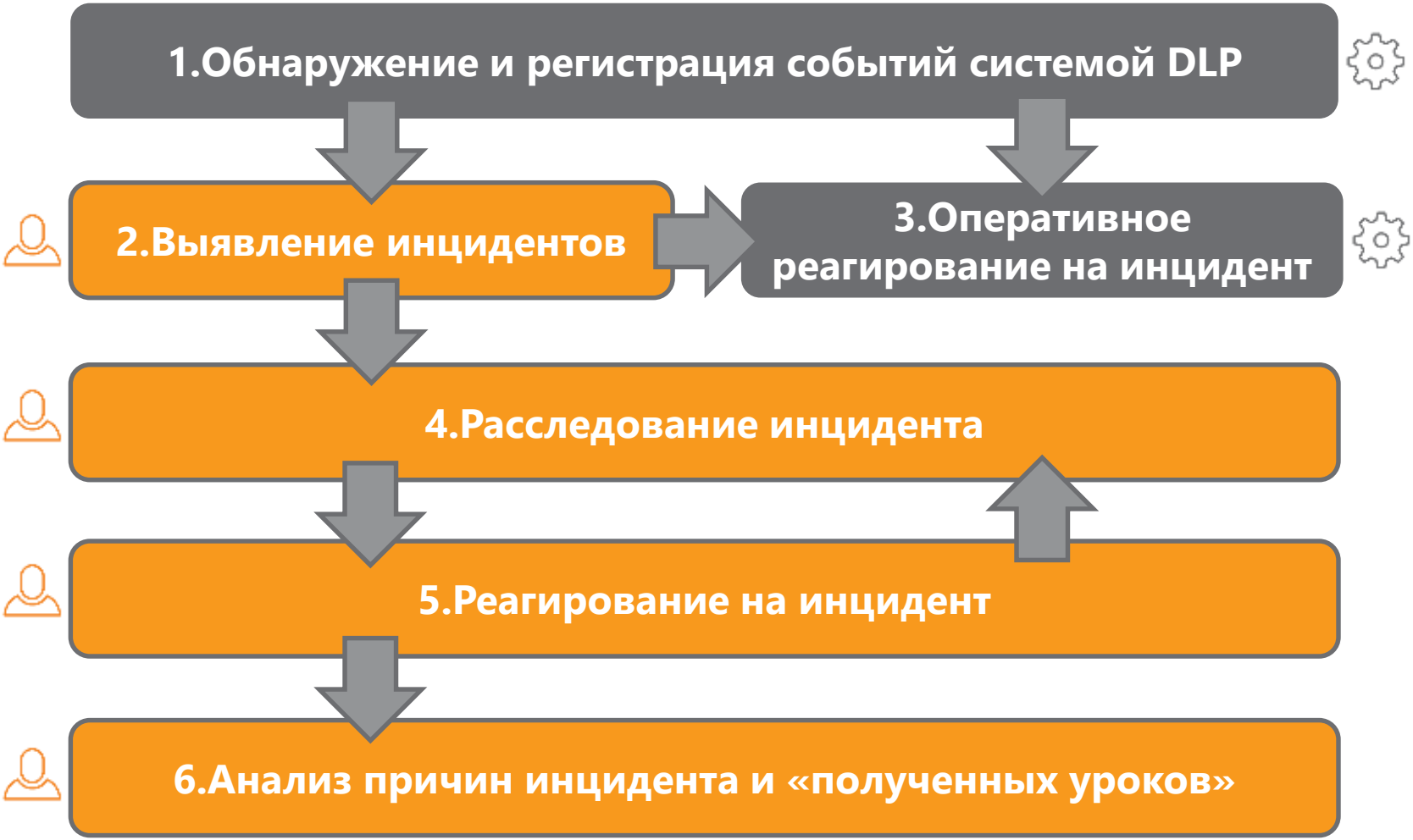
- Общая информация
- События и инциденты
- Граф-связей
- Уровень доверия («карма»)

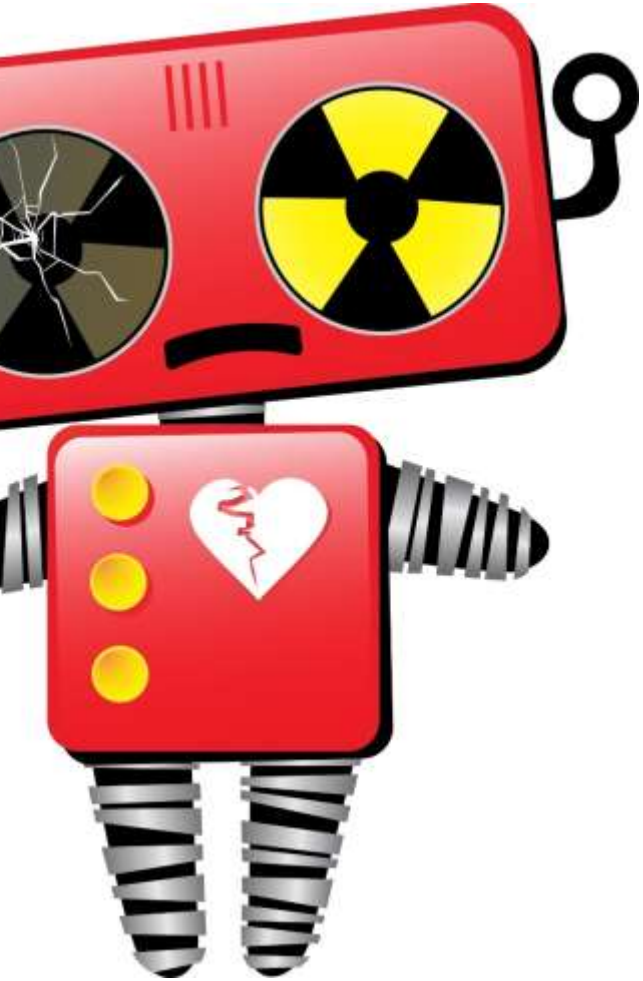
- Канал передачи
- Сработавшая политика
- Отправители и получатели


SOLAR SECURITY
Управление инцидентами информационной безопасности с помощью DLP Solar Dozor
v1.3 2015-08


Управление инцидентами ИБ
с помощью DLP Solar Dozor
Прозоров Андрей, CISM
Руководитель экспертного направления

Полная процедура управления инцидентами (DLP)





Специалисты по ИБ часто не знают, что можно (нужно) делать с выявленными нарушителями

Пример модели принятия решения по инциденту (по сумме баллов)

1. ***Какова величина ущерба?***
   Крупный – 6; Неизвестно или пока нет, но может быть – 3; Ущерба нет – 1
2. ***Выявлен ли умысел сотрудника?***
   Да – 3; Неизвестно – 1; Нет, инцидент по ошибке – 0
3. ***Какой уровень доверия к сотруднику?***
   Низкий – 3; Обычный – 1; Высокий – 0
4. ***Были ли у сотрудника инциденты до этого?***
   Да – 2; Нет – 0
5. ***Какова вероятность, что инцидент повториться у этого сотрудника?***
   Высокая – 3; Средняя (скорее нет, маловероятно) – 1; Низкая – 0

до 6 – вариант А; 6-12 – вариант Б; 13 и больше – вариант В

Решение в случае виновности сотрудника

А) По решению ИБ

1. Перевод в группу «Особый контроль»
2. Получение объяснительной*
3. Профилактическая беседа

Б) По решению руководства и HR

4. Лишение благ и привилегий (втч и лишение прав доступа)
5. Дисциплинарные взыскания:
   - замечание
   - выговор

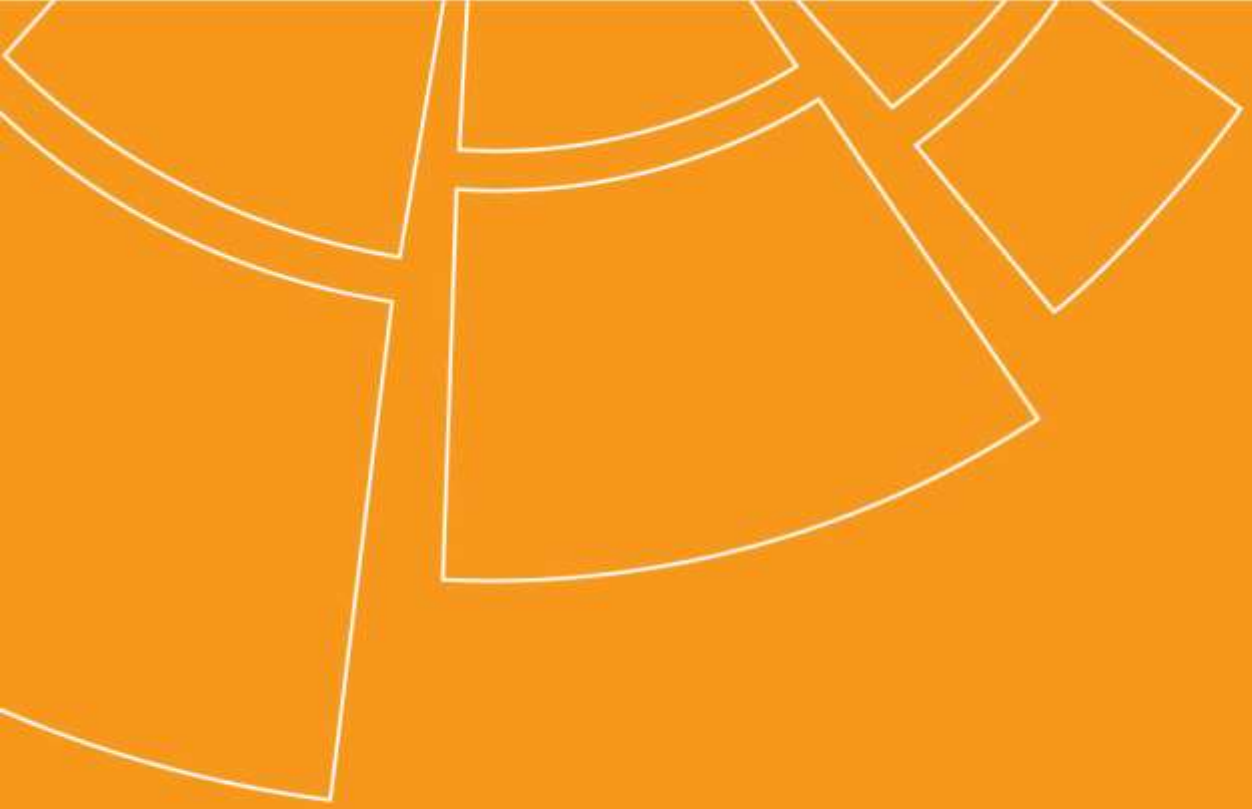
В) По решению руководства, HR, юристов и ИБ. Необходимо четкое понимание процедур и высокий уровень «бумажной безопасности»

   - увольнение по соответствующим основаниям
6. Увольнение по инициативе работника / по соглашению сторон
7. Возмещение ущерба
8. Уголовное преследование
9. Прочее

Вместо подведения итогов

На этом у меня все.

Напомню, что работа с DLP складывается из 2х составляющих: регулярный мониторинг событий и расследование инцидентов. А хорошие DLP системы упрощают такую работу…



Спасибо за внимание!

Прозоров Андрей, CISM

Мой блог: 80na20.blogspot.com
Мой твиттер: twitter.com/3dwave