Выбор DLP-системы.

Как сориентироваться в разнообразии рынка и выбрать оптимальное решение?

Артём Пахомов

Архитектор по информационной безопасности

Информзащита
Группа компаний

Разнообразие рынка DLP-систем

Разнообразие рынка DLP-систем

Разнообразие рынка DLP-систем

Как выбрать оптимальное решение?

1. Принципы работы системы
   - ✓ Инциденты или архив
   - ✓ Мониторинг или блокировка
2. Определение ключевых требований и расстановка приоритетов
   - ✓ Общие требования
   - ✓ Требования к инфраструктуре
   - ✓ Требования к интерфейсу
3. Пилотное тестирование

1. Принципы работы системы

- **Инциденты или архив**
- ✓ Мониторинг или блокировка

Инциденты или архив

Работа с инцидентами

Работа с архивом данных

Инциденты или архив

Работа с инцидентами

- ✓ *Умеренные требования к хранилищу*
- ✓ *Не противоречит законодательству*

Работа с архивом данных

- ✓ *Есть возможность создать новую политику и повторно проверить по ней накопленный архив*

1. Принципы работы системы

- ✓ Инциденты или архив
- ➢ **Мониторинг или блокировка**

Мониторинг или блокировка

Блокировка передачи/обработки защищаемых данных

Преимущества

- ✓ *Снижается риск утечки информации*

Недостатки

- ✓ *Увеличивается риск остановки бизнес-процессов*
- ✓ *Увеличивается количество обращений в техподдержку*

2. Ключевые требования

- ➢ **Общие требования**
- ✓ Требования к инфраструктуре
- ✓ Требования к интерфейсу

Контроль сетевого трафика

Протоколы

- ✓ *http*
- ✓ *https*
- ✓ *ftp*
- ✓ *NNTP*
- ✓ *IM (Icq, Jabber, …)*

Переписка по электронной почте

- ✓ *Внешняя*
- ✓ *Внутренняя*

Контроль рабочих станций

Обработка защищаемых данных на уровне рабочих станций

- ✓ *Локальные диски*
- ✓ *Внешние носители (USB, CD/DVD)*
- ✓ *Буфер обмена*
- ✓ *Печать*
- ✓ *Приложения*
- ✓ *Протоколы (http, https, ftp, …)*
- ✓ *IM (Icq, Jabber, …)*

Контроль рабочих станций

Хранение защищаемых данных на рабочих станциях

- ✓ *Сканирование данных, хранящихся на локальных дисках*

Контроль сетевых ресурсов

Хранение защищаемых данных на сетевых ресурсах Компании

- ✓ *Общие каталоги*
- ✓ *Web-порталы*
- ✓ *Базы данных*
- ✓ *Системы документооборота*

Другие каналы утечки информации

Контроль передачи данных на мобильные устройства

Контроль над данными, расположенными в «облаках»

…

Общие требования

Технологии анализа данных

Ключевые слова

Регулярные выражения

Цифровые отпечатки документов

Детектирование печатей

Распознавание текста в изображениях

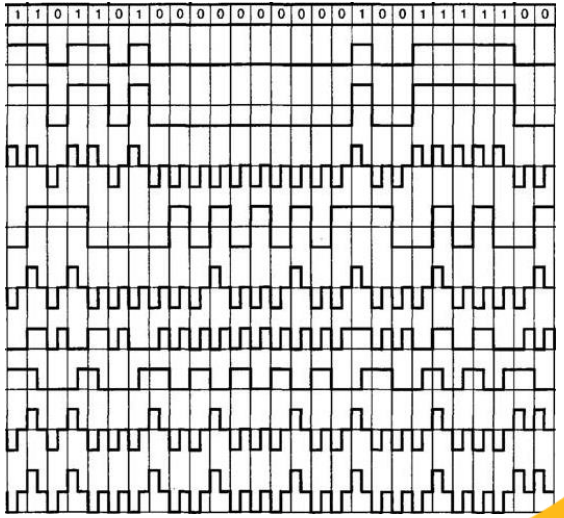
Общие требования

Поддерживаемые типы данных

Поддерживаемые форматы документов

Распознавание голосового трафика

Распознавание текста в изображениях



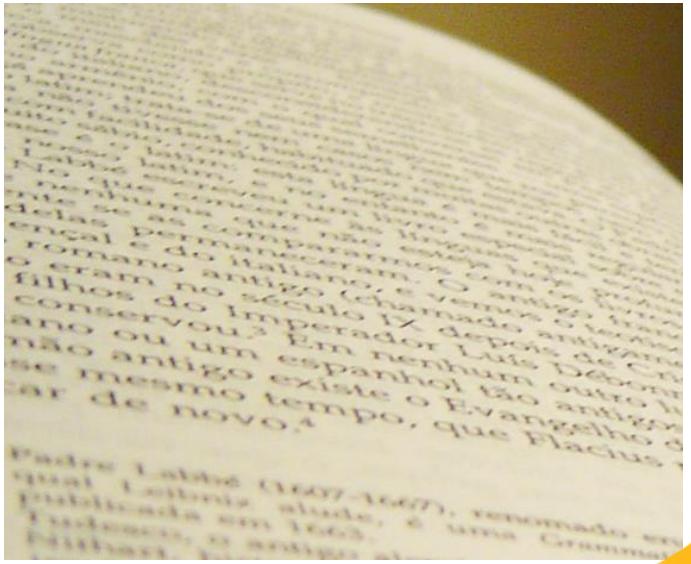
Общие требования

Локализация

Поддержка русского языка при анализе данных

Поддержка морфологии

Русскоязычный интерфейс системы



Прочие возможности и требования

Дополнительные возможности

- ✓ *Организация процесса расследования инцидентов (WorkFlow)*
- ✓ *Применение системы в целях обучения пользователей работе с защищаемой информацией*

Дополнительные требования

- ✓ *Наличие российских сертификатов*

2. Ключевые требования

- ✓ Общие требования
- ➢ **Требования к инфраструктуре**
- ✓ Требования к интерфейсу

Требования к инфраструктуре

АПК (апплайнс)

- ✓ *Отсутствие дополнительных лицензий на ОС*
- ✓ *Техническая поддержка одного вендора*

ПО

- ✓ *Возможность выбора аппаратной платформы*
- ✓ *Возможность виртуализации*

Требования к инфраструктуре

Возможности интеграции со сторонними решениями

Службы каталогов (LDAP)

- ✓ *Единые учётные данные пользователей*
- ✓ *Возможности использования групп и пользователей из каталога*

Почтовая инфраструктура

- ✓ *Задержка отправки сообщений до проверки офицером безопасности*

Системы документооборота

Системы управления инцидентами ИБ

2. Ключевые требования

- ✓ Общие требования
- ✓ Требования к инфраструктуре
- ➢ **Требования к интерфейсу**

Требования к интерфейсу

Локализация

Удобство управления

Консоль управления

- ✓ *Управление через единую консоль (web-консоль / ПО на стороне клиента)*
- ✓ *Разрозненные консоли*

Конфигурация новых политик

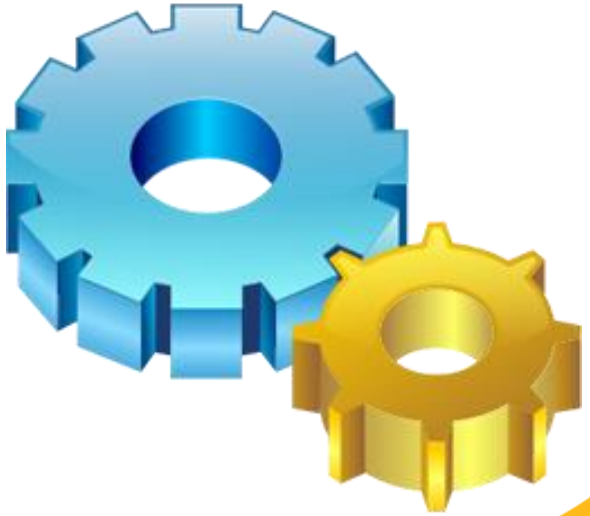
Обслуживание системы и БД

3. Пилотное тестирование

Пилотное тестирование

Проводить или нет?

Сколько продуктов тестировать?



Пилотное тестирование позволяет:

- ✓ *Подтвердить результаты оценки*
- ✓ *Приобрести первоначальный опыт работы с системой*
- ✓ *Проверить возможности интеграции в имеющуюся инфраструктуру*

Спасибо!

Информзащита
Группа компаний