МФИ СОФТ

Защита баз данных:
опыт российских компаний

Технологии защиты баз данных

Отсутствие защиты

Штатный аудит СУБД

Системы классов DAM и DBF

Какие задачи решает система класса DAM?

Сканирование СУБД

Обнаружение баз данных, классификация информации в СУБД, нахождение уязвимостей

Аудит доступа к данным

Перехват запросов и ответов пользователей баз данных и веб-приложений

Отчетность по накопленным данным

Почему решения по защите БД есть не у всех?

Сложная предметная область

- Какие данные хранятся и что защищать?
- Кто к каким данным имеет доступ?
- Какие задачи безопасности в области СУБД?

Высокая стоимость

-Серверы
-Программное обеспечение
-Эксплуатация
-Обучение

Сложность обоснования затрат

- Когда нет четких требований регуляторов.

Complience – двигатель ИБ

- Самый простой способ обосновать внедрение дорогой системы – показать ее необходимость с точки зрения соответствия требованиям регуляторов.
- Для банков и СУБД – это PCI DSS – независимо от страны.

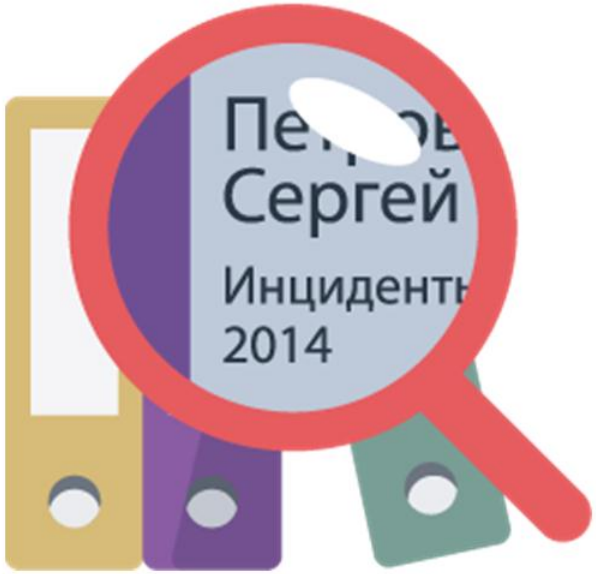
Практика применения систем защиты баз данных

Опыт использования решений класса DAM

Крупный российский банк

- Цель проекта – прохождение аудита PCI DSS
- Установлена DAM-система, включена в режиме аудита, без блокировок

PCI DSS пройден. Каков результат?

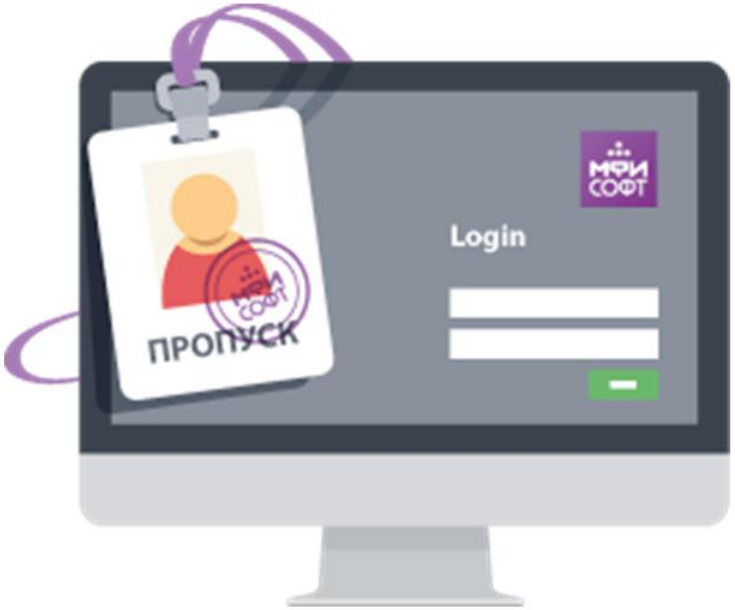


- Настроенные политики под PCI DSS
  - доступ к карточным данным + маскирование;
  - мониторинг администраторов;
- Понимание принципов работы сотрудников с СУБД
- Выявление фактов использования информации без необходимости

Архив VS расследование

- Архив событий необходим, ***чем больше данных, тем лучше***
- Контроль доступа к VIP и выявление инцидентов
  - Несовершенство ролевой модели CRM
  - Просмотр ради любопытства
  - Передача данных внешним «сообщникам»

Адаптация инструкций / изменения в СУБД



Изменение внутри СУБД

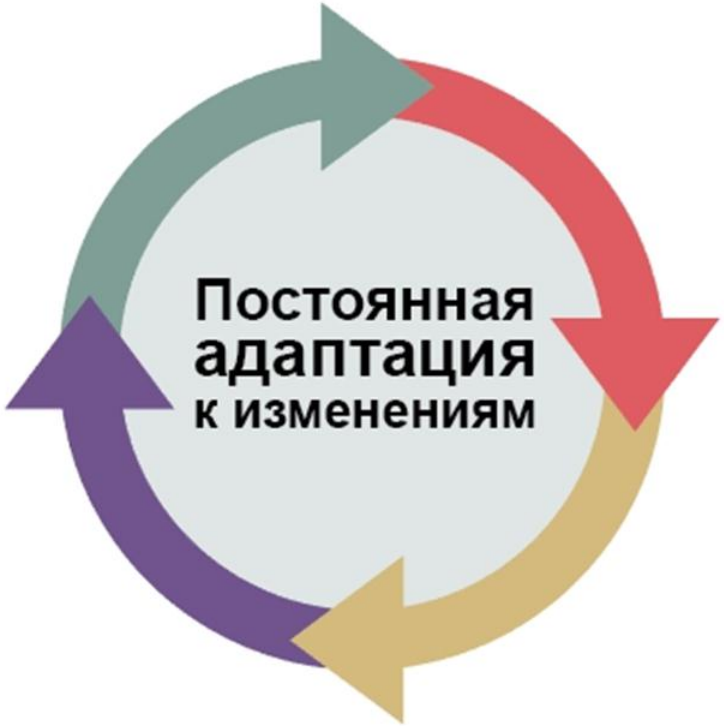
- закрытие системных учетных записей;
- до настройка прав доступа;

Разработка документов

- доработка должностных инструкций;
  - Авторизация администраторов
  - Доступ без необходимости

Раскрытие механизмов и создание «культуры» защиты информации

Работа с DAM системой



- Обследование защищаемых систем
- Анализ и выявление отклонений
- Изменение/разработка нормативных документов
- Реагирование на инциденты, принятие мер

Результат: снижение числа халатных действий с данными клиентов

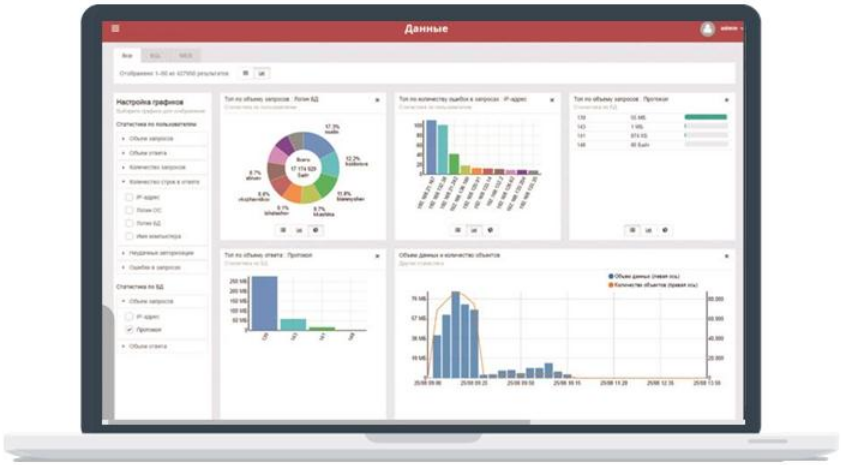
Что имеем сейчас? Выводы

- Политики под PCI DSS – к аудиту готовы
- Оптимальных архив для расследования инцидентов от службы безопасности
- Контроль Администраторов
- Созданная система расследования доступа к VIP (DAM+ SIEM).

МФИ СОФТ

- 10+ лет опыта разработки систем высокой сложности
- Более 300 высококвалифицированных специалистов
- Собственный исследовательский центр для развития новых проектов
- 1500 внедрений решений во всех федеральных округах России
- Система менеджмента качества МФИ Софт сертифицирована на соответствие международному стандарту ISO 9001:2008 Британским институтом стандартов (BSI)

ISO 9001: 2008



Гарда БД

ib.sales@mfisoft.ru
8 (831) 422-11-61
mfisoft.ru