Группа ВТБ

PCI DSS.
К правильной цели приводит правильный путь

Василий Андреевич Окулесский, к.т.н.

Москва, 2015

Банк Москвы

Группа ВТБ

PCI DSS. Начало

Наши цели выполнения требований стандарта:

- ✓ Предотвращение финансовых потерь, связанных с инцидентами нарушения безопасности данных платежных карт
- ✓ Повышение надежности систем ИБ Банка в интересах клиентов и бизнес-партнеров
- ✓ Уход от штрафных санкций и ограничений со стороны международных платежных систем за несоответствие требованиям стандарта

Область применимости стандарта

- ✓ Процессинг
- ✓ АБС
- ✓ ДБО
- ✓ Web-ресурсы
- ✓ Сеть банкоматов и платежных терминалов
- ✓ . . .

Группа ВТБ

Подход к выполнению требований PCI DSS

Приоритеты в проекте:

- ✓ Нацеленность на реальную оценку соответствия, а не на формальное выполнение требований
- ✓ Адаптация существующих механизмов защиты для обеспечения соответствия требованиям
- ✓ Получение максимум эффективности от внедрения новых подсистем ИБ в интересах всех бизнес-процессов Банка

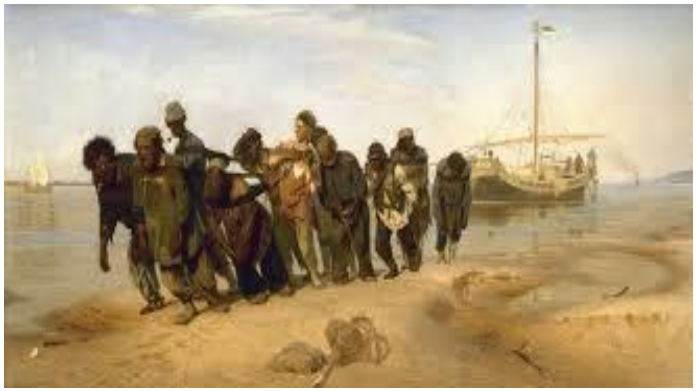
Банк Москвы

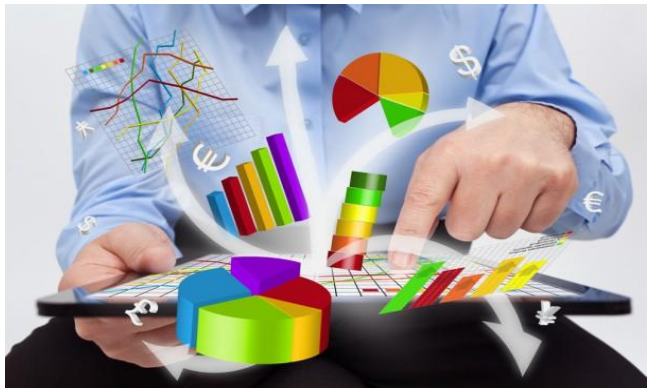
Группа ВТБ

От лог-менеджмента к полноценному SIEM

Требование стандарта 10.6

«Review logs and security events for all system components to identify anomalies or suspicious activity»





Группа ВТБ

Выгоды от внедрения SIEM

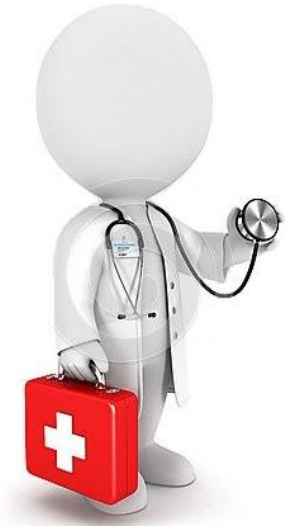
- ✓ Мониторинг и корреляция событий для выявления реальных инцидентов ИБ
- ✓ Регулярная отчетность о выявленных нарушениях политики ИБ
- ✓ Соблюдение нормативных требований по управлению инцидентами ИБ (PCI DSS, СТОБР ИББС, Защита ПДн)
- ✓ Оценка эффективности применяемых средств защиты за счет непрерывного анализа событий и инцидентов ИБ
- ✓ Снижение ущерба от инцидентов за счет своевременного и эффективного реагирования и сбора доказательной базы
- ✓ Сокращение расходов на аудит и контроль событий за счет централизации информации о состоянии ИБ
- ✓ . . .

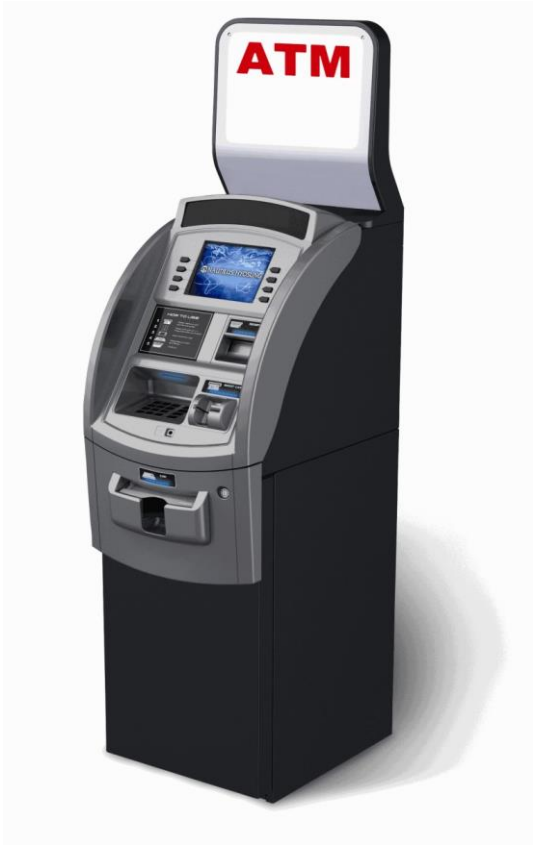
Группа ВТБ

Банкоматы по контролем

Внедрение специализированного решения для мониторинга и защиты банкоматов позволило:

- ✓ Защитить сеть банкоматов от внутренних и внешних атак
- ✓ Оптимизировать затраты на контроль работы сети банкоматов
- ✓ Создать эффективный процесс управления сетью банкоматов
- ✓ Обеспечить соответствия требованиям стандарта PCI DSS



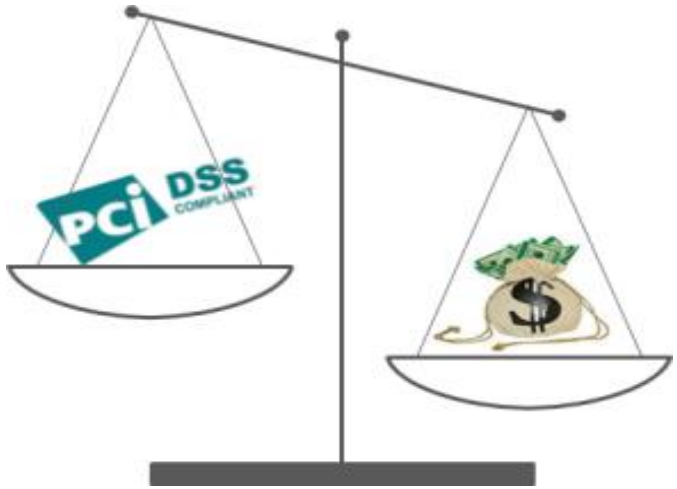


Куда привел путь соответствия PCI DSS?

- ✓ Увеличение эффективности бизнес-процессов
- ✓ Прозрачность механизмов обеспечения ИБ
- ✓ Повышение уровня ИБ в целом

Наши рекомендации

- ✓ Максимально **сокращать область действия стандарта** (в первую очередь за счет сегментации сети и исключение номеров карт из информационных систем).
- ✓ **Привлекать только опытные компании-интеграторы**, которые способны реализовать проект полностью: от проведения аудит и разработки плана исправлений, до его реализации, включая внедрение тех.средств, постановки процессов и разработки нормативной документации.
- ✓ **Заключать долгосрочные договора**, результатом работ по которым будет не только первоначальная сертификация, но подтверждение статуса в дальнейшем.
- ✓ С учетом того, что проект находится на стыке интересов подразделений ИТ, ИБ и процессинга, требует от этих подразделений значительных трудозатрат, но при этом не дает для них значительных выгод, необходимо **заручиться поддержкой top-менеджмента компании**.



Группа ВТБ

СПАСИБО ЗА ВНИМАНИЕ!

Банк Москвы