Черно-белый мир информационной безопасности

Пентесты… нужны!

- Катализатор инвестиций в ИБ
- Узнать об 0-day раньше плохих парней
- Реальный способ проверить защищенность

Пентесты… не нужны!

- Пентест конечен (не бывает «полного пентеста»), а уязвимости – нет
- Поиск 0day занимает много времени и стоит много денег. А смысл?
- Там, где нету контролей ИБ, проверять нечего

PCI DSS… полезен!

- Очень зрелый по сути (технический, требует пентеста)
- Ориентирован на конкретную проблему (утечку данных карт)
- Контролируется внешними QSA

PCI DSS… бесполезен!

- Monkey business. Превращает аудит в формальность
- Безопасность - не профиль платежных организаций. Они воспринимают PCI DSS как навязанное зло
- Состояние на конкретный момент времени. Сколько мы знаем историй взлома PCI compliant организаций?

APT… существует!

- Технологии стали сложнее, порог вхождения в "хакерство" ниже, опасность взлома выше
- Много нового в нападении, ничего нового в защите
- Это отражение эволюции взломов: сначала ради забавы, потом ради наживы, и вот теперь - ради стратегического доминирования

APT… не существует!

- Все “APT-взломы” это же набор тех же самых атак, что мы знали раньше
- APT - это способ компании оправдать свою несостоятельность в ИБ
- Что нового привносит APT, о чем я раньше не знал? Что нового должен делать, чего раньше не делал?

И так можно рассуждать

обо всем

Спасибо :-)