

Инт¹ра

Тестирование на проникновение: нюансы и особенности

Степанов Валерий, Т1 Интеграция

Мультивендорные
СЗИ

Процессы СУИБ

Квалифицированный
штат



Высокий уровень
защищенности

Выполнение
требований
регулятора

Зачем нужен пентест

ДИБ

Защита
информации

Оценка
уязвимостей

Соответствие
регуляторным
требованиям

Бизнес

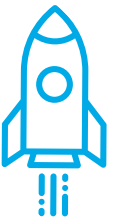
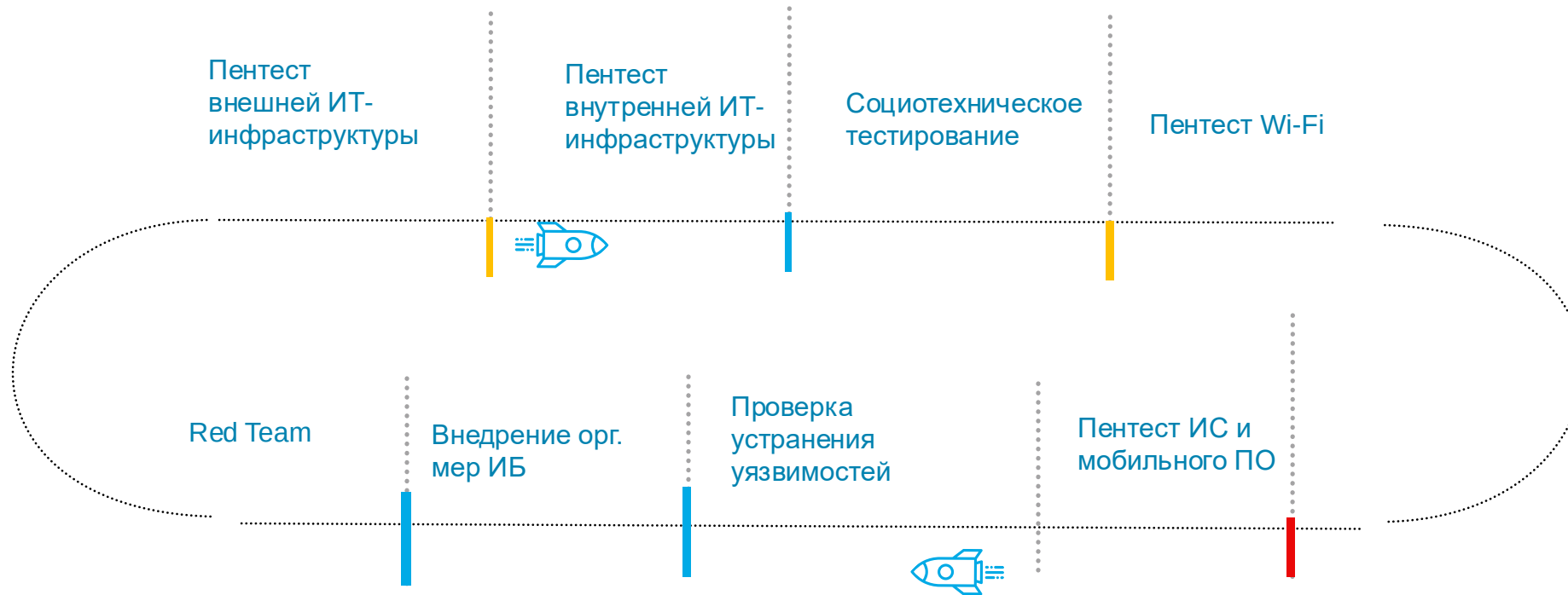
Защита активов

Митигация рисков
НСА

Конкурентное
преимущество

Комплексный подход

Инт¹ра



При проведении пентестов (тестирования на проникновение) с точки зрения заказчика важно обратить внимание на следующие ключевые нюансы:

1. **Цели и объем тестирования:** Четкое определение целей пентеста и границ тестируемых систем – критически важный шаг. Заказчик должен заранее обозначить, какие системы, приложения или сети подлежат тестированию, а также какие конкретные угрозы и уязвимости необходимо проверить.
2. **Выбор квалифицированных специалистов:** Важно выбирать команду с подтвержденной экспертизой и опытом в проведении пентестов. Необходимо проверить аккредитации, сертификаты и примеры предыдущих работ, чтобы убедиться в компетентности специалистов.
3. **Согласование сроков и методов тестирования:** Заказчику следует заранее согласовать сроки выполнения пентеста, а также методы и подходы, которые будут использоваться. Это поможет избежать недоразумений и обеспечить согласованность действий команды тестировщиков с бизнес-процессами организации.
4. **Отчетность и рекомендации:** Заказчик должен ожидать качественный отчет по результатам пентеста, который должен содержать не только выявленные уязвимости, но и рекомендации по их устранению. Важно, чтобы отчет был понятным и доступным для различных уровней управления.
5. **Конфиденциальность и безопасность данных:** Заказчику следует обратить внимание на вопросы конфиденциальности и безопасности данных, которые могут быть использованы в ходе тестирования. Необходимо заключить соглашение о неразглашении (NDA) и обсудить меры по защите информации, чтобы минимизировать риски утечки данных.

Эти нюансы помогут заказчику максимально эффективно организовать процесс пентестирования и получить необходимые результаты для улучшения безопасности своих систем.

Поговорим о насущном 2МР

Инт¹ра

Банк России рекомендует при проведении пентеста актуализировать:

- Модель угроз
- Техзадание
- Соглашение об ответственности
- План восстановления



Банк России

Самостоятельный пентест:

- Пентест не должны проводить сотрудники ИБ (вероятно, во избежание конфликта интересов)
- Подрядчик, в свою очередь, должен иметь пункт «б» лицензии ТЗКИ и подтвержденный трехлетний опыт проведения работ в финансовых организациях
- Сотрудники подрядчика не должны находиться за пределами РФ и не должны участвовать в создании/эксплуатации системы защиты информации финансовой организации



Конференция
ИТ-холдинга Т1

Инт¹ра