RedTeam
Практические аспекты

Tinkoff.ru

Май, 2018

whoami

- Попов Андрей
- Ведущий аналитик по информационной безопасности в Tinkoff.ru
- 4 года в ИБ банковской сферы;
- 6 лет в консалтинге ИБ, основная специализация «Практический анализ защищенности».

Задачи практического анализа защищенности

Атаки

Выявление проблем ИБ, оценка возможности реализации атак, повышение эффективности процессов информационной безопасности...

Расследования

Участие в расследовании инцидентов информационной безопасности.

Экспертные задачи

Участие в решении нестандартных задач информационной безопасности возникающих внутри Компании (внутренний консалтинг).

Pentest vs RedTeam

Vulnerability management

Оценка защищенности информационной инфраструктуры путем проведения инструментального анализа (автоматизирование сканирование на наличие известных уязвимостей и недостатков и последующий анализ полученных данных).

Penetration test

Моделирование действий потенциального злоумышленника с целью выявления проблем информационной безопасности в компонентах информационной инфраструктуры.

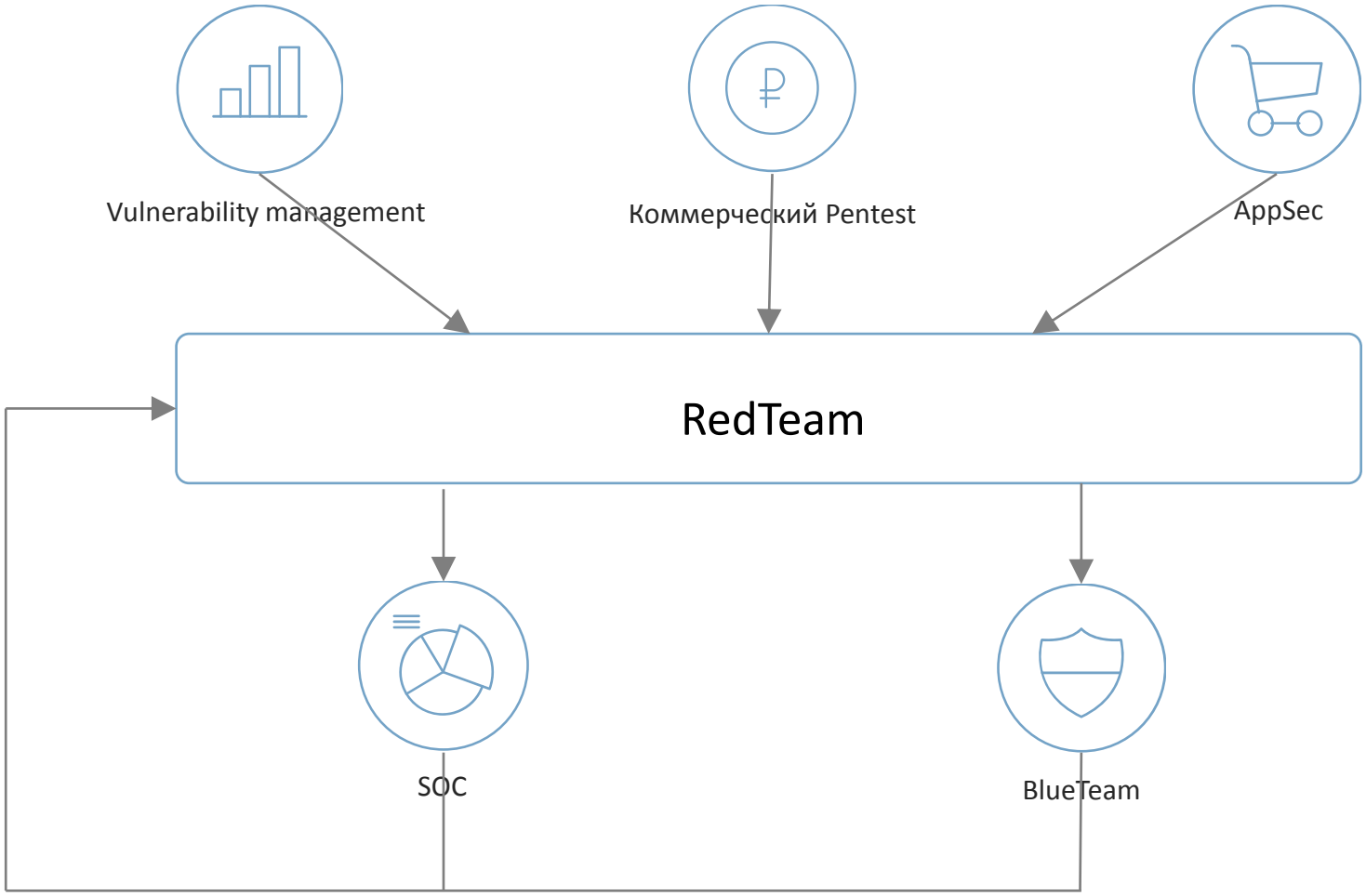
RedTeam

Реализация реальных атак «дружественной» командой с целью повышения эффективности работы защитных механизмов.

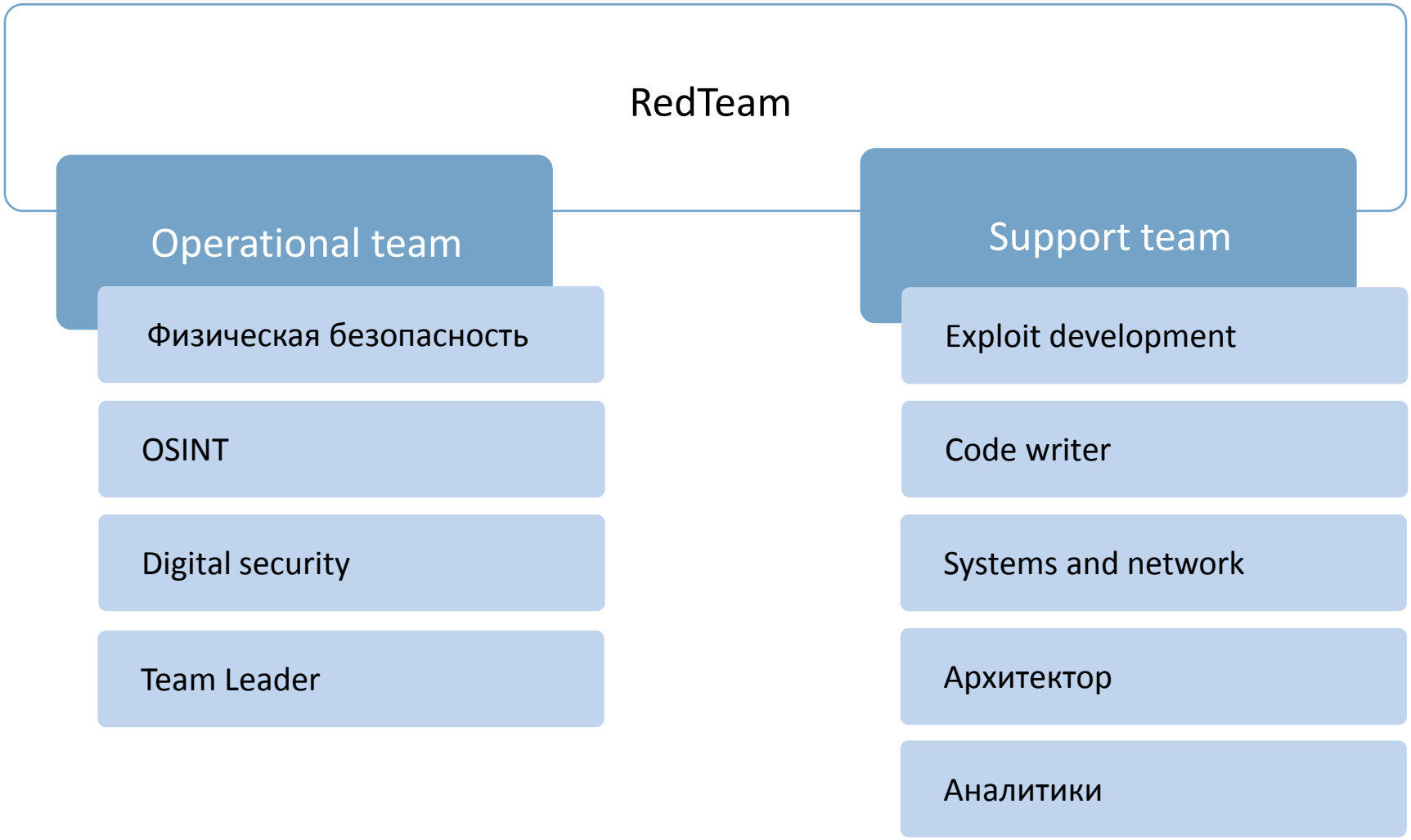
Pentest ≠ RedTeam

	Pentest	RedTeam
Концептуальная цель	Выявление проблем ИБ	Повышение эффективности ИБ
Границы работ	«Белый» список	Вся компания, не ограниченные методы
Модель злоумышленника	Утвержденная модель	Без строгой привязки к модели
Длительность	Ограниченная (недели)	Не ограниченная (месяцы)
Взаимодействие	Прямое с выделенным представителем	Как правило отсутствует
Потребитель	Compliance requirements, Выстроенные процессы аудитов, мониторинга.	Зрелые процессы ИБ

Эффективная коллаборация



Идеальный RedTeam



Что выбрать?

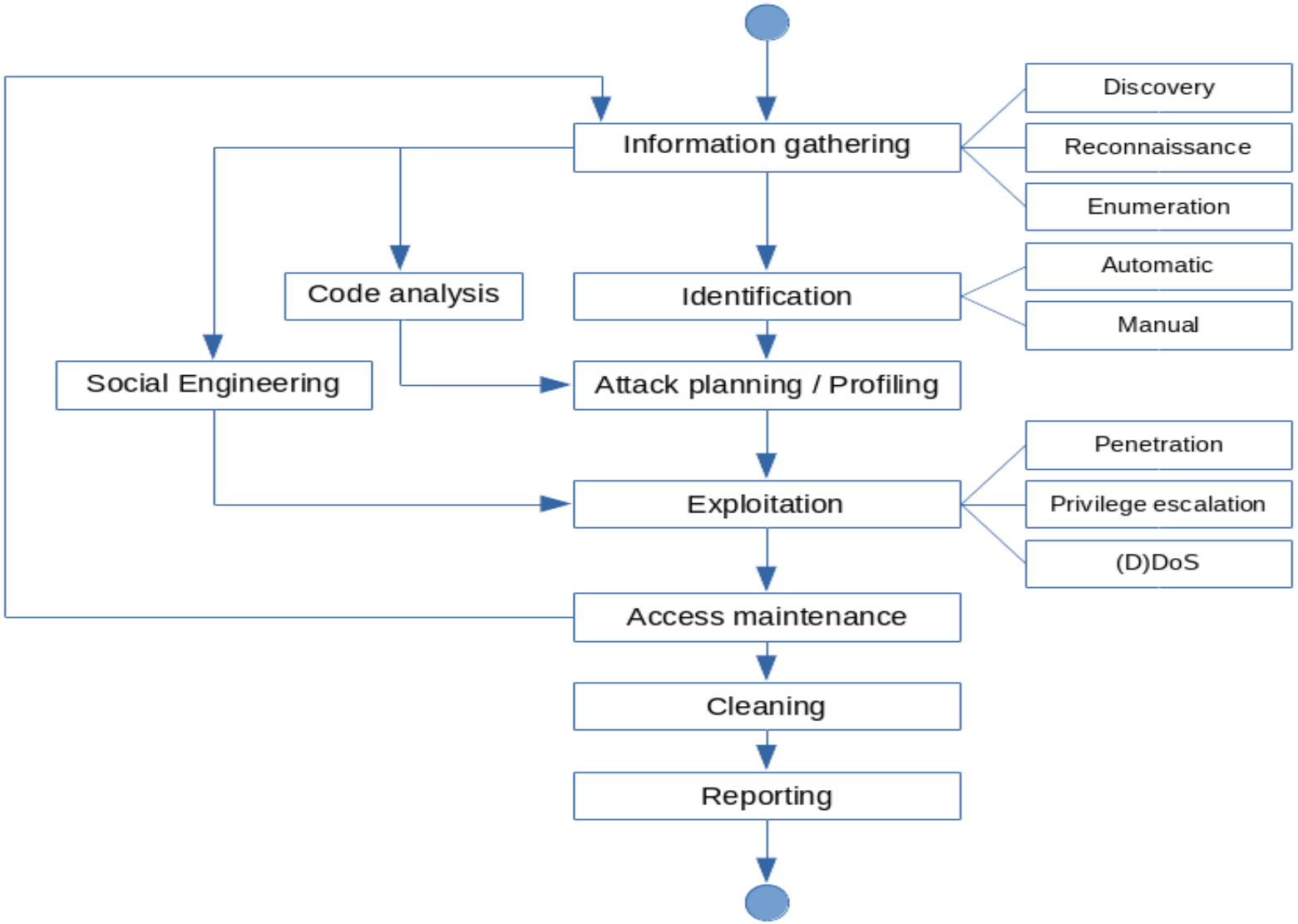
	Начальный / Повторяемый	**Определенный**	**Управляемый / Оптимизируемый**
Недостаточный	VM	VM, коммерческий PT	VM, PT + коммерческий PT
Определенный	VM	VM, коммерческий PT	VM, RT + коммерческий PT

Pentest не лучше RedTeam, RedTeam не лучше Pentest.

Обычно «пентестеры» и redteam это одни и те же люди, использующие различные методы и техники для выполнения различных задач оценки защищенности информационной инфраструктуры.

Не надо использовать RedTeam для поиска как можно большего колличества уязвимостей, и не надо использовать PenTest для моделирования APT.

Примеры


Information gathering
Discovery
Reconnaissance
Enumeration
Code analysis
Identification
Automatic
Manual
Social Engineering
Attack planning / Profiling
Exploitation
Penetration
Privilege escalation
(D)DoS
Access maintenance
Cleaning
Reporting

Тинькофф

Дальше действовать будем мы!

Tinkoff.ru

JETSECURITY
CONFERENCE 2018

IX ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ

31 мая, 2018
Radisson Resort, Zavidovo