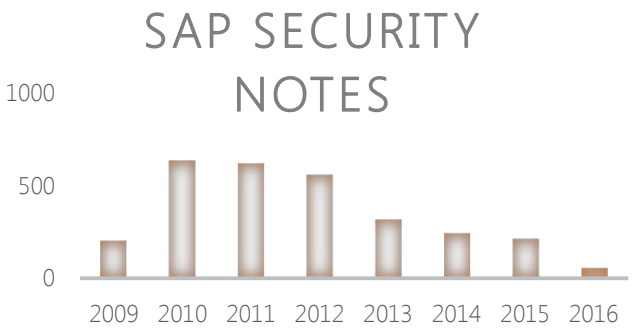
Алексей Голдбергс

Безопасность бизнес-систем

POSITIVE TECHNOLOGIES

ptsecurity.ru

Масштаб проблемы



- ~3000 известных уязвимостей
- ~20 новых уязвимостей каждый месяц
- ~1000 настроек конфигурации
- от 500 пользователей в каждой инсталляции
- постоянные доработки системы

Средняя инсталляция
~30 SAP систем *

Количество серверов в одном ландшафте (до 10) *

Количество мандантов (от 4 до 10).

Итого: ~ 300 серверов
~ 120-300 мандантов

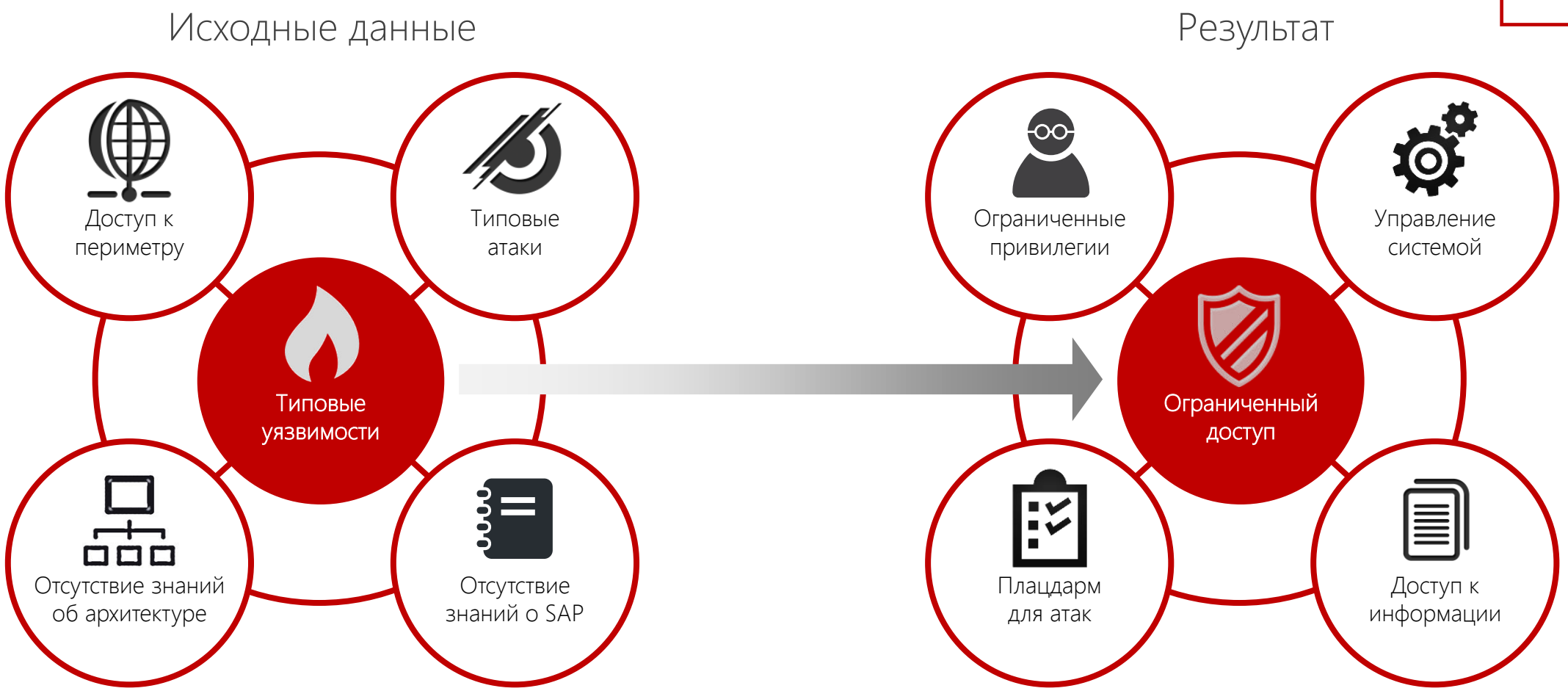
Как правило, 1–2 человека

Задачи:
- контроль уязвимостей
- контроль прав доступа
- контроль действий пользователей/администраторов
- контроль настроек безопасности
- контроль парольной политики
- * анализ ABAP кода

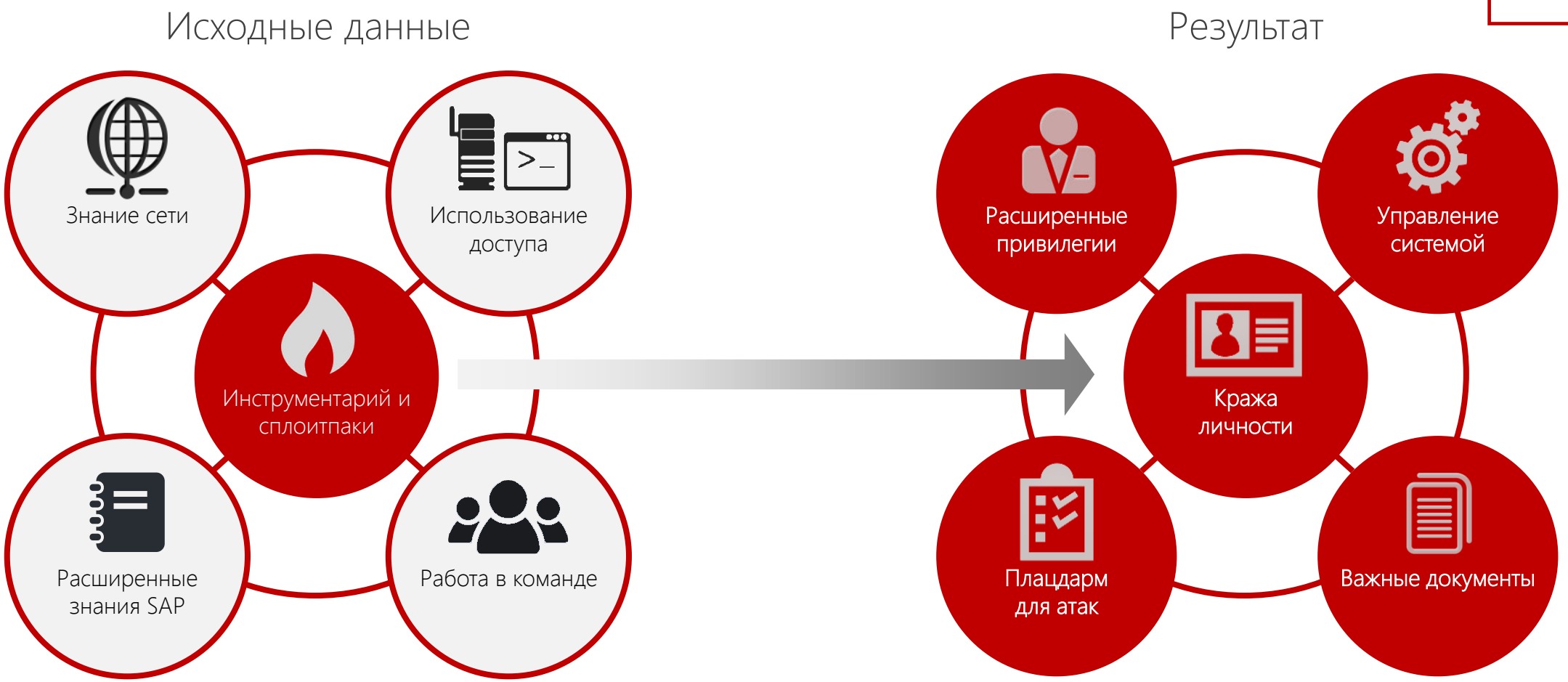
Плохие парни – кто они?

POSITIVE TECHNOLOGIES

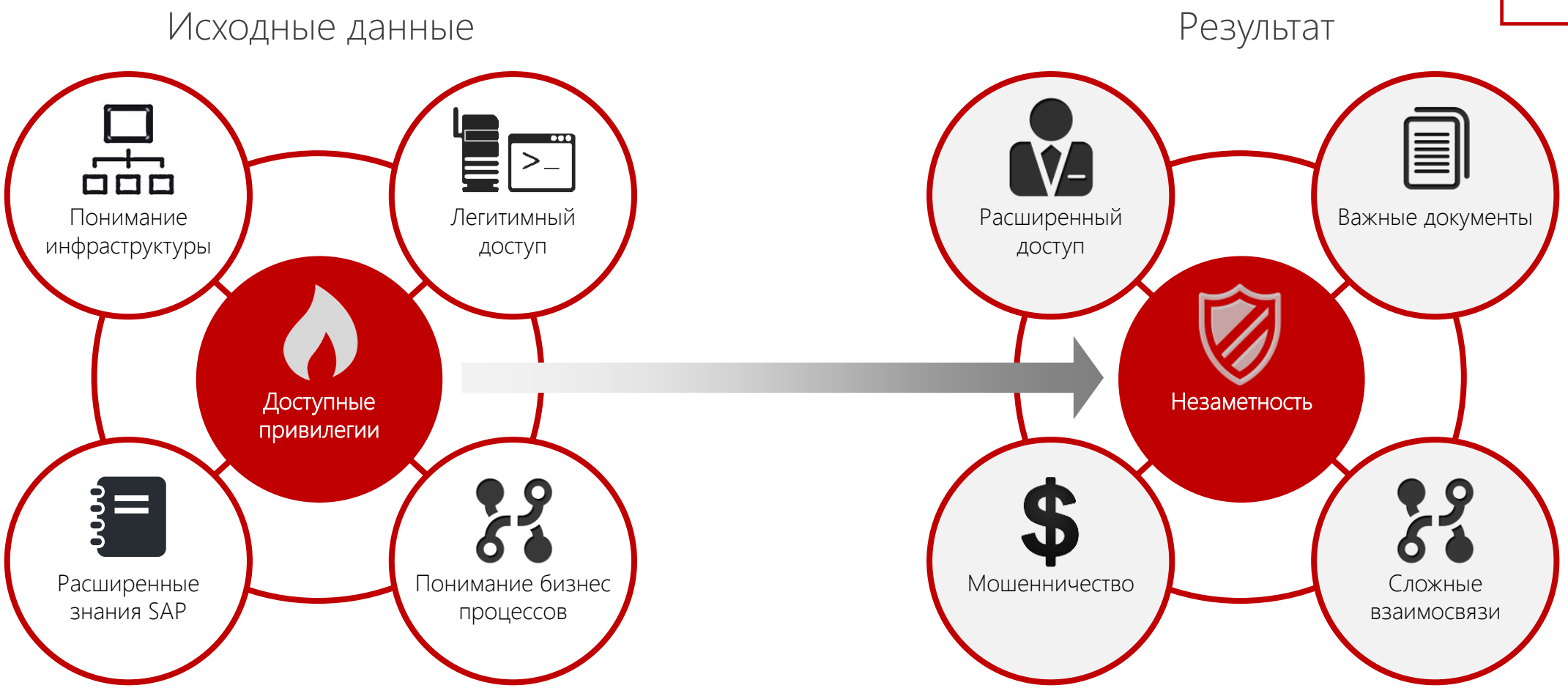
Обычные хакеры



Продвинутые хакеры



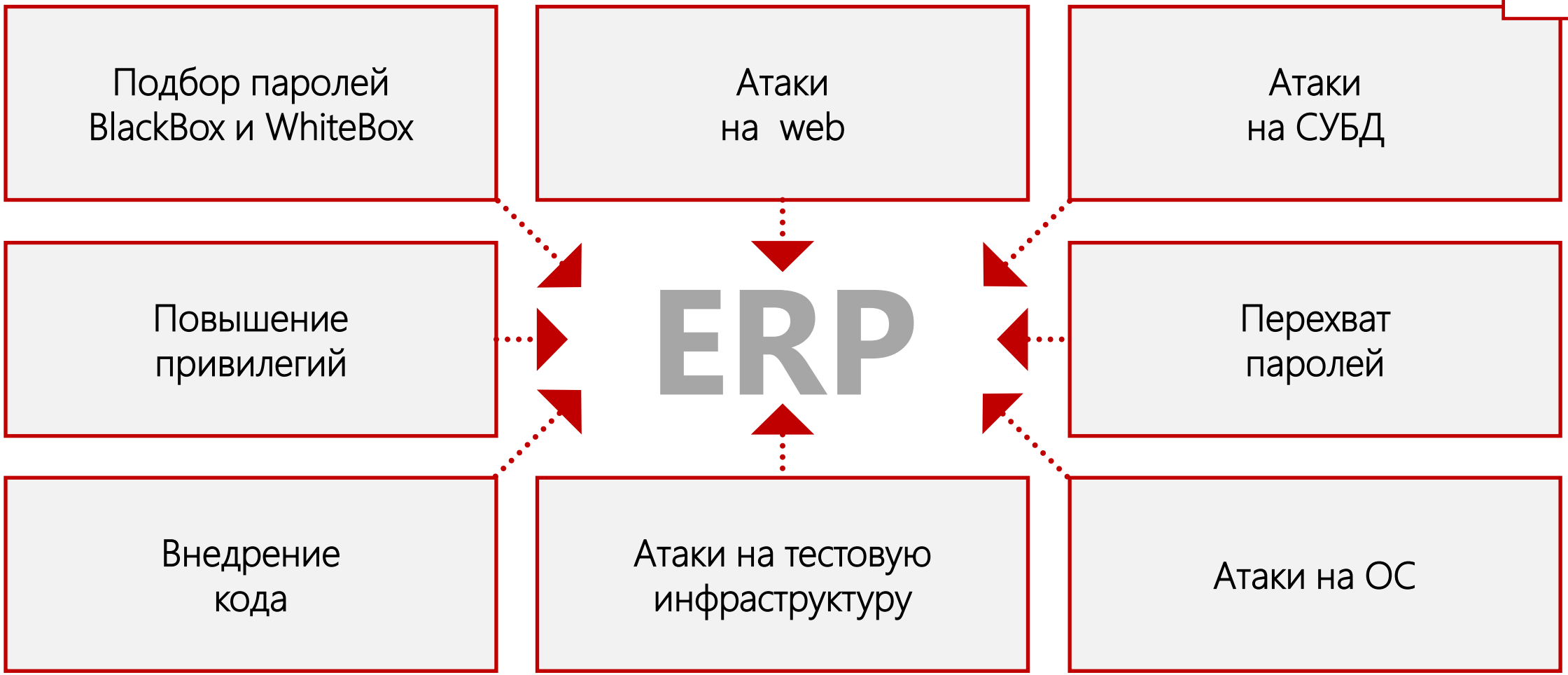
Внутренние злоумышленники



Последствия

Нарушение конфиденциальности	• Утечка данных • Промышленный шпионаж
Проникновение в систему	• Потеря контроля над системой • Плацдарм для дальнейших атак
Мошенничество	• Формирование счетов на оплату • Нарушение бизнес процессов
Потеря управления	• Отсутствие следов взлома • Непрозрачность процессов управления
Нарушение работоспособности	• Потери времени на восстановление • Большие трудозатраты на поддержку

Механика атак

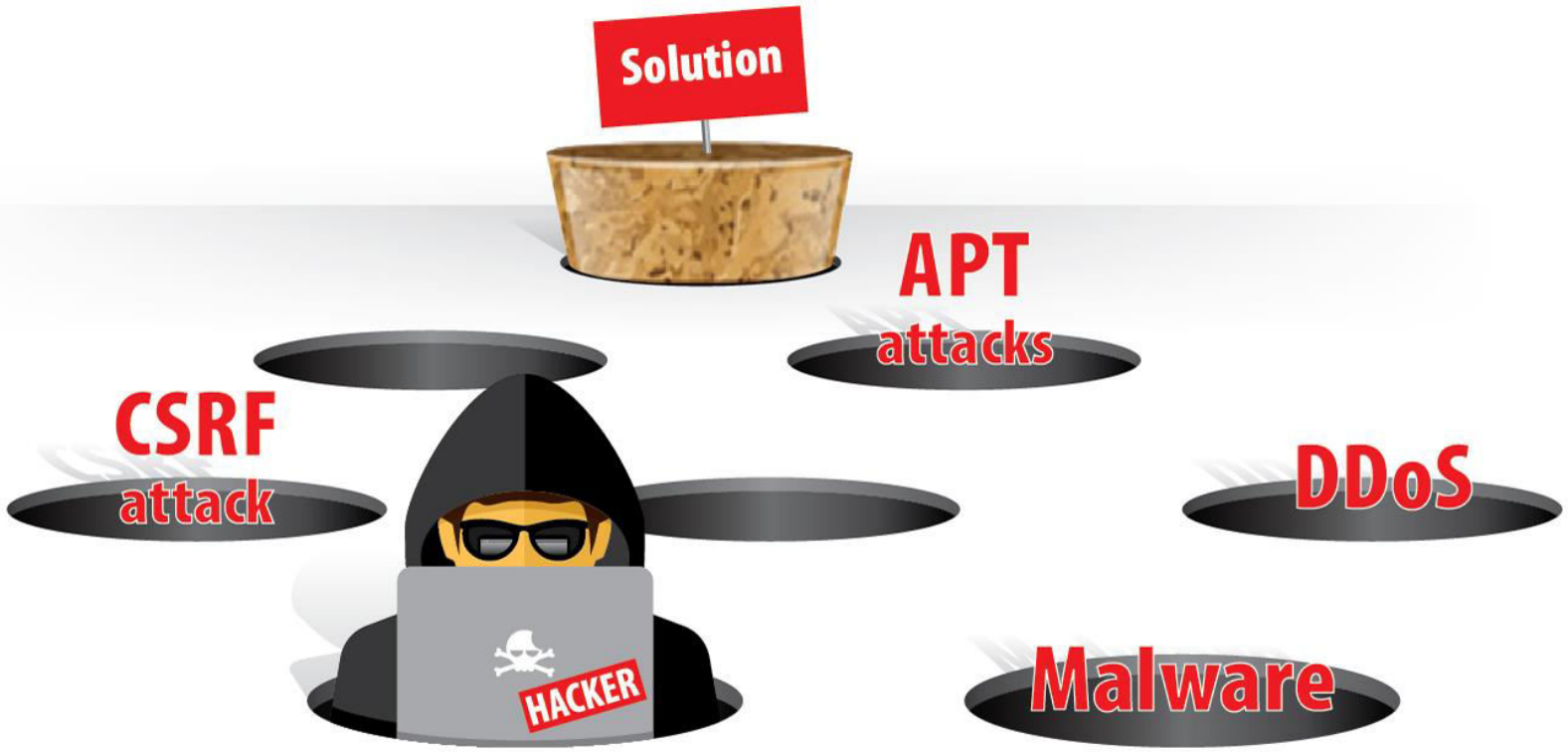


Традиционный подход

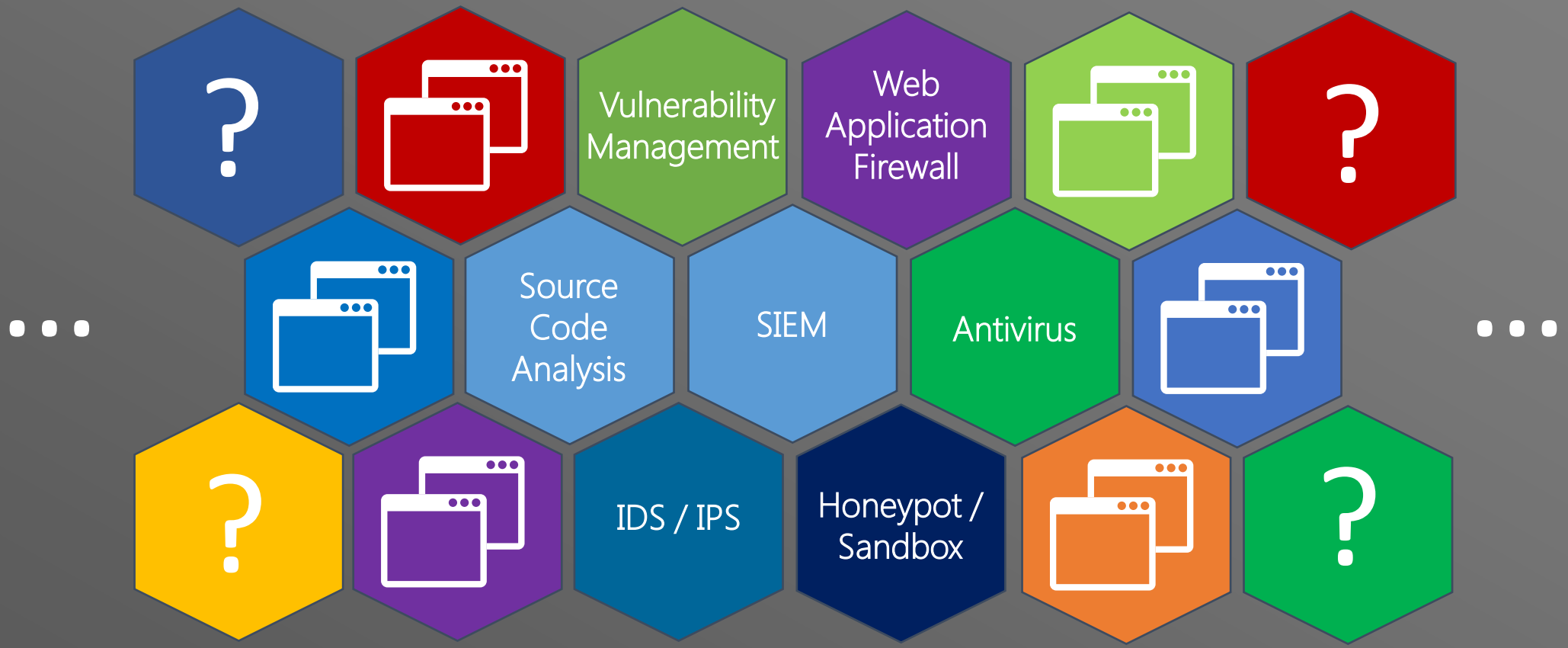
Традиционный подход
похож на игру whack-a-mole:

- сначала, со стороны хакеров, появляется новая угроза
- затем следует реакция индустрии

Чем быстрее и умнее реакция, тем меньше последствий от атак хакеров



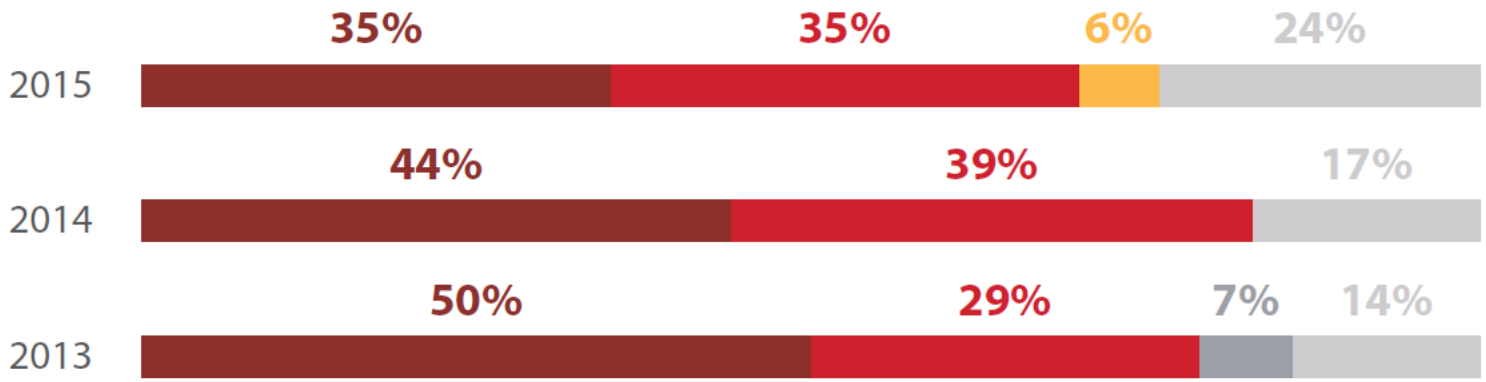
Традиционный подход



Комплексный подход

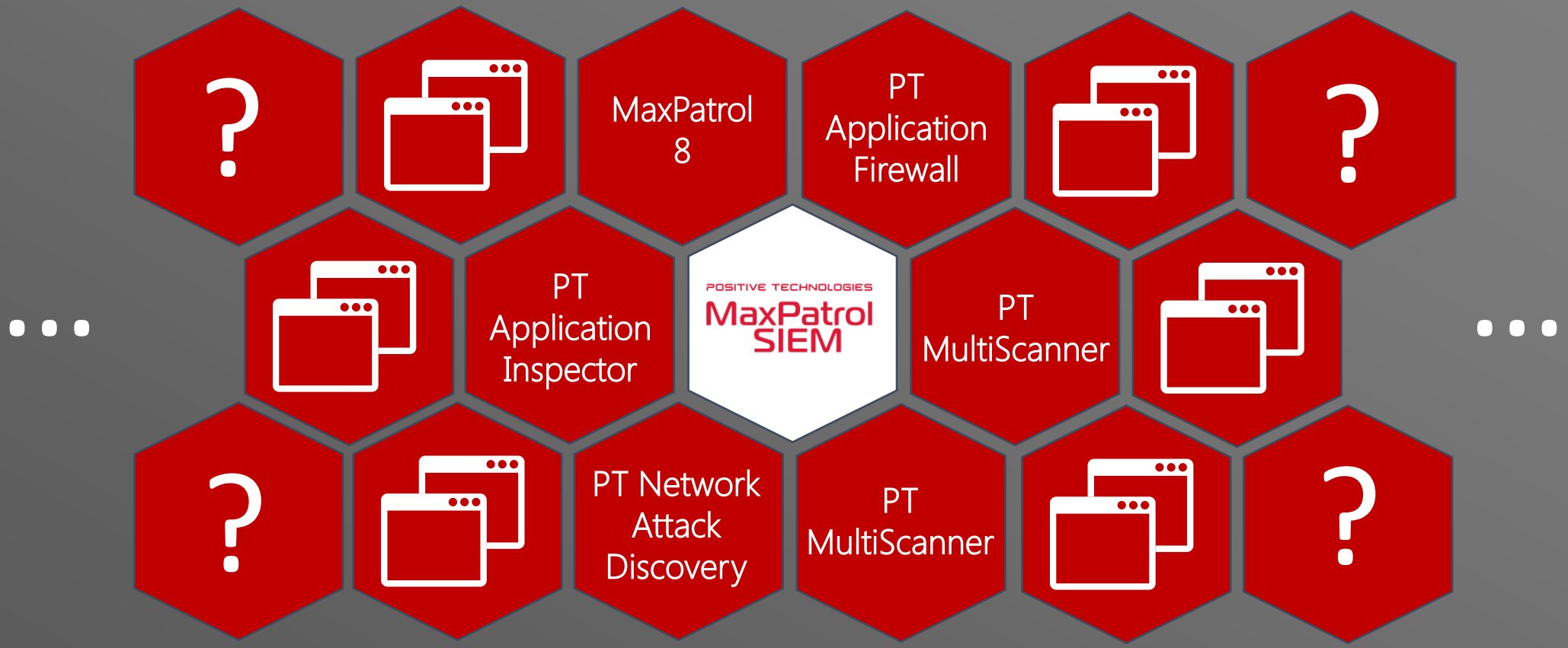

СПАСИБО, КЭП!

Результаты тестов на проникновение



- Любой внешний нарушитель
- Любой нарушитель из пользовательского сегмента ЛВС
- Любой внутренний нарушитель из технологического сегмента
- Любой нарушитель, имеющий удаленный доступ к одному из серверов
- Не установлен

Комплексный подход



Спасибо!

POSITIVE TECHNOLOGIES

ptsecurity.ru