Информзащита
Системный интегратор

У нас пентест!
Предупредите всех

Дмитрий Колышкин
руководитель направления анализа защищенности

www.infosec.ru

Классический пентест и его проблемы

Ограничен по времен (порядка 1 месяца)

Ограничен по области исследования

Осведомлены практически все

Результат работ может быть нерелевантным текущей ситуации

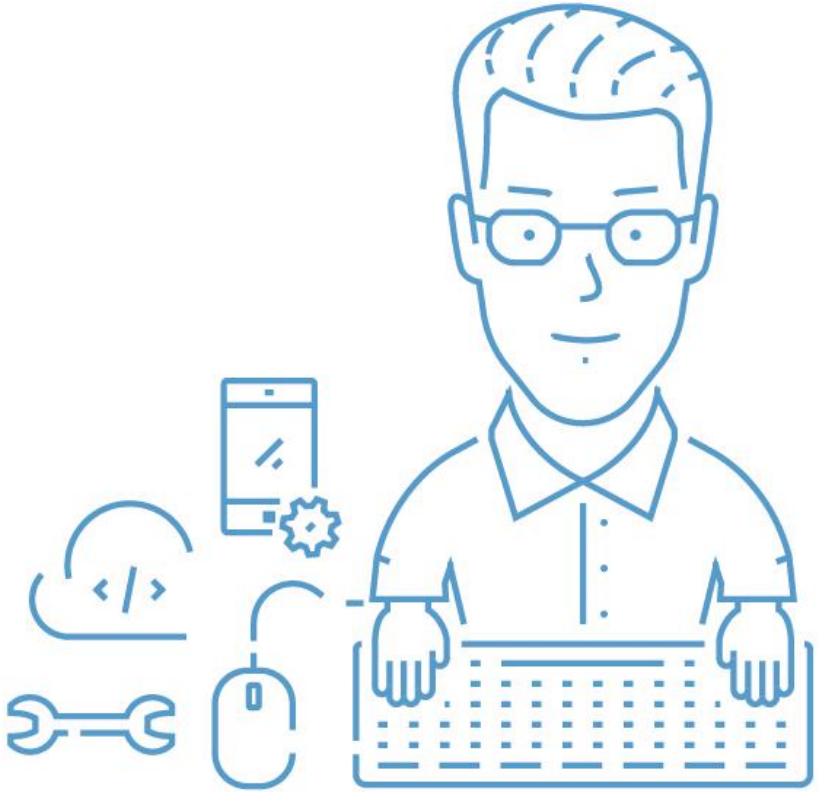
Осведомленность о пентесте – нерелевантные результаты?

Сотрудники могут совершаться следующие действия:

Отключать уязвимые сервера

Скрывать чувствительную информацию (например, пароли в текстовых файлах)

Проводить активное противодействие пентесту



RedTeam как панацея?

Основные отличия **RedTeam**:

Сроки гораздо длиннее

Область исследования гораздо шире

Скрытный процесс

В рамках редтима можно получить информацию не только о технических уязвимостях, но и о корректности действий сотрудников

Иди туда, не знаю, куда...

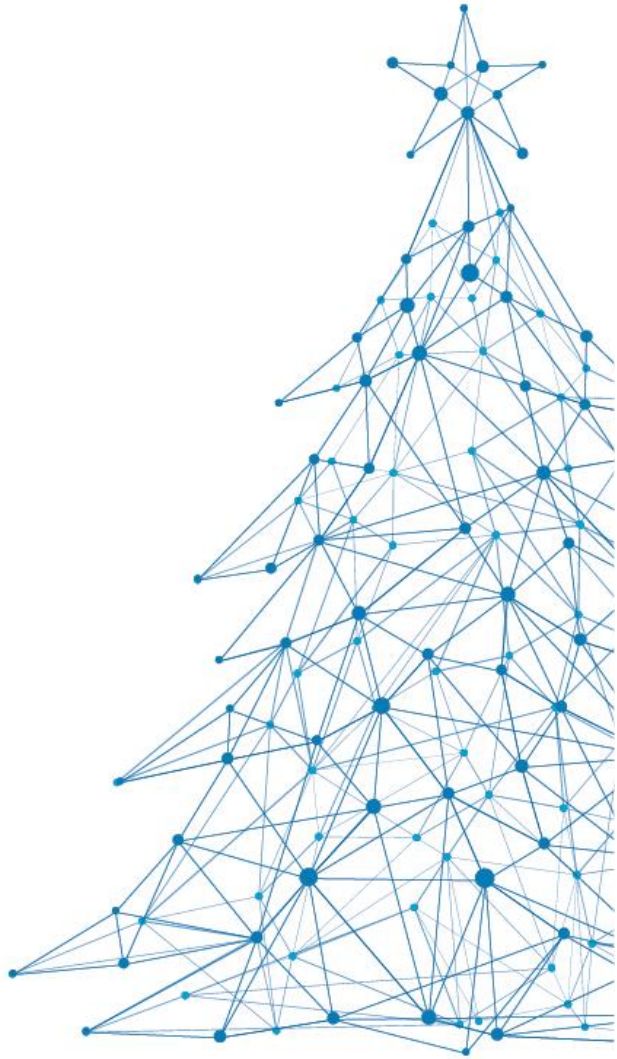
Типовые атаки и подходы обнаруживаются легко даже без наличия отдела мониторинга:

Заведение привилегированных пользователей

Использование инструментов наподобие PsExec, Meterpreter, Mimikatz...

Массовое сканирование портов и сервисов

Подобные действия, как правило, для администраторов «выглядят как новогодняя елка»



...найди то, не знаю что

Некоторые атаки не выявлялись даже при наличии SOC в компании:

Социальная инженерия

Таргетированные атаки, не массовые рассылки

Атаки на ActiveDirectory

Delegation, Kerberoasting, Golden Ticket, ...

Привилегированный доступ к критичным сетевым сегментам

Административный доступ к управлению компонентам инфраструктуры

Киберучения как способ превентивного противодействия

Атакующим интересны

нестандартные вектора

Информзащита
Системный интегратор

Информационная безопасность 24x7x365

Центр противодействия кибератакам IZ SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Системный интегратор

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Центр противодействия мошенничеству

antifraud@infosec.ru

Сервисный центр

+7 495 981 92 22
support@itsoc.ru
www.itsoc.ru

Пресс-служба

pr@infosec.ru