ДиалогНаука

Автоматизация пентеста в распределенных сетях

Валерий Филин
Технический директор
CITUM

Владимир Соловьев
Руководитель направления внедрения средств защиты "ДиалогНаука"

План

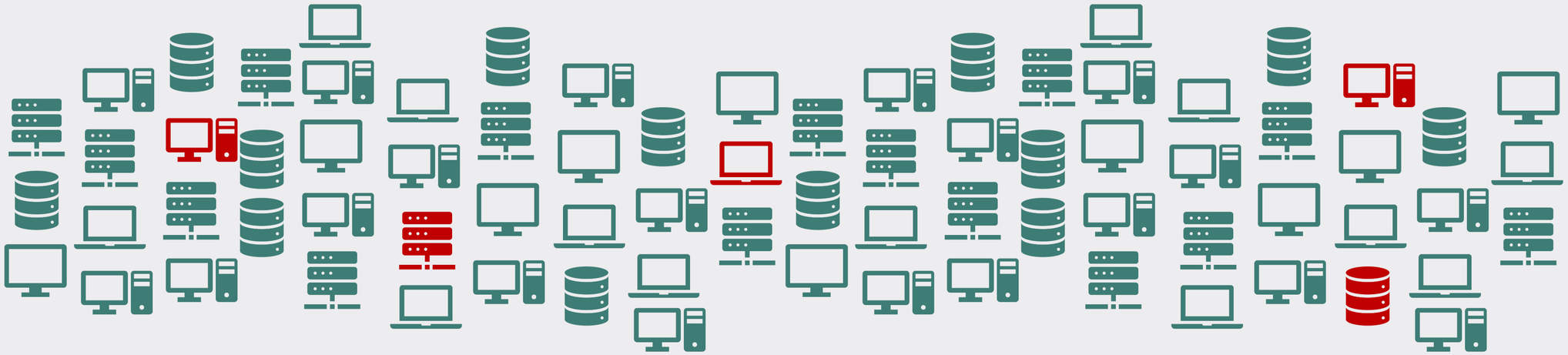
- Сложности тестирования больших сетей
- Как может помочь автоматизация?
- Схема внедрения Pentera в распределенной сети
- Особенности автопентеста в распределенной среде
- Примеры решений на основе реальных проектов

ДиалогНаука

Сложности тестирования защищенности крупных распределенных сетей

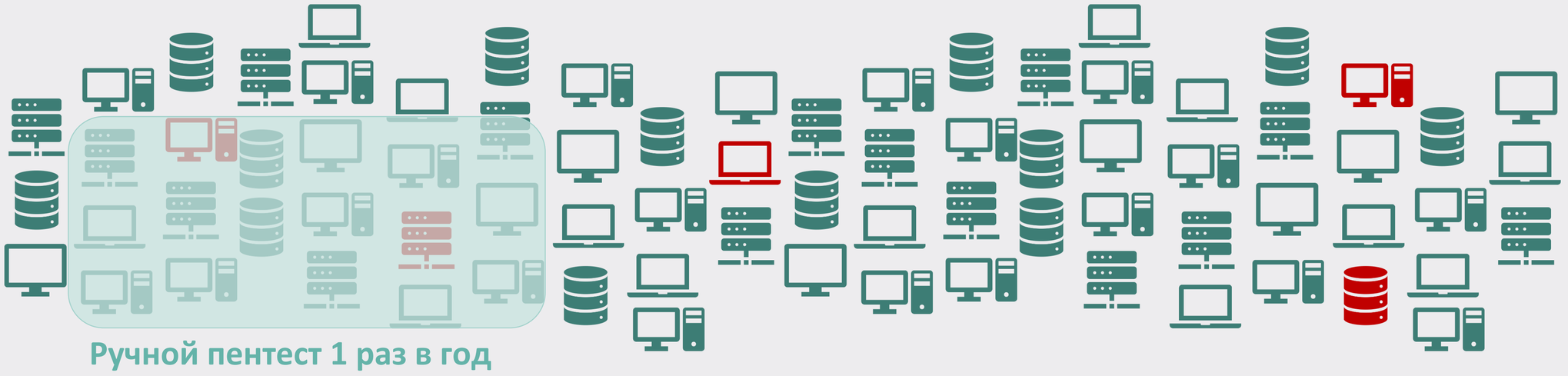
Тестирование больших сетей

Основные вызовы



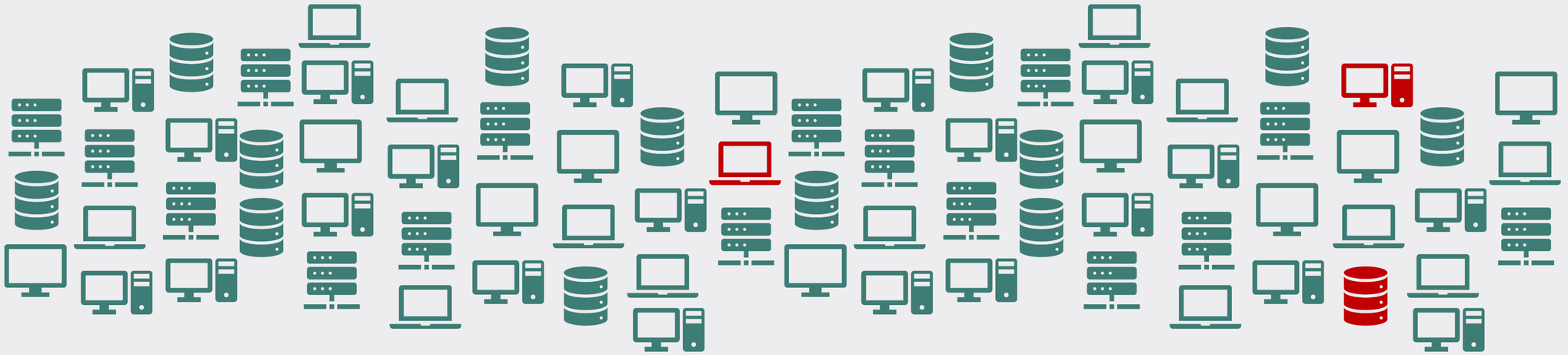
Тестирование больших сетей

Основные вызовы



Тестирование больших сетей

Основные вызовы



Тестирование больших сетей

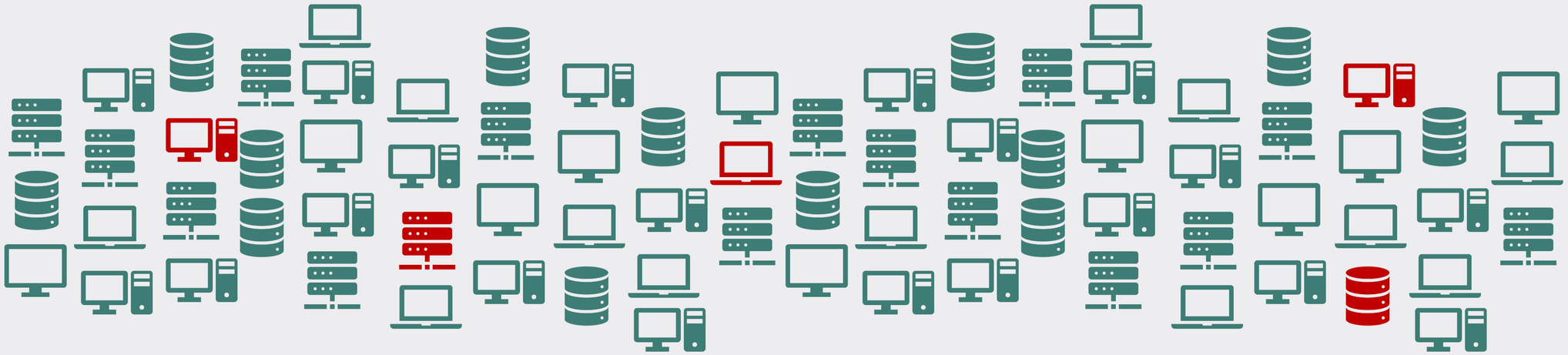
Основные вызовы

ДиалогНаука

Как может помочь автоматизация?

Автоматизированный пентест

Ключевые выгоды



Автоматизированный пентест

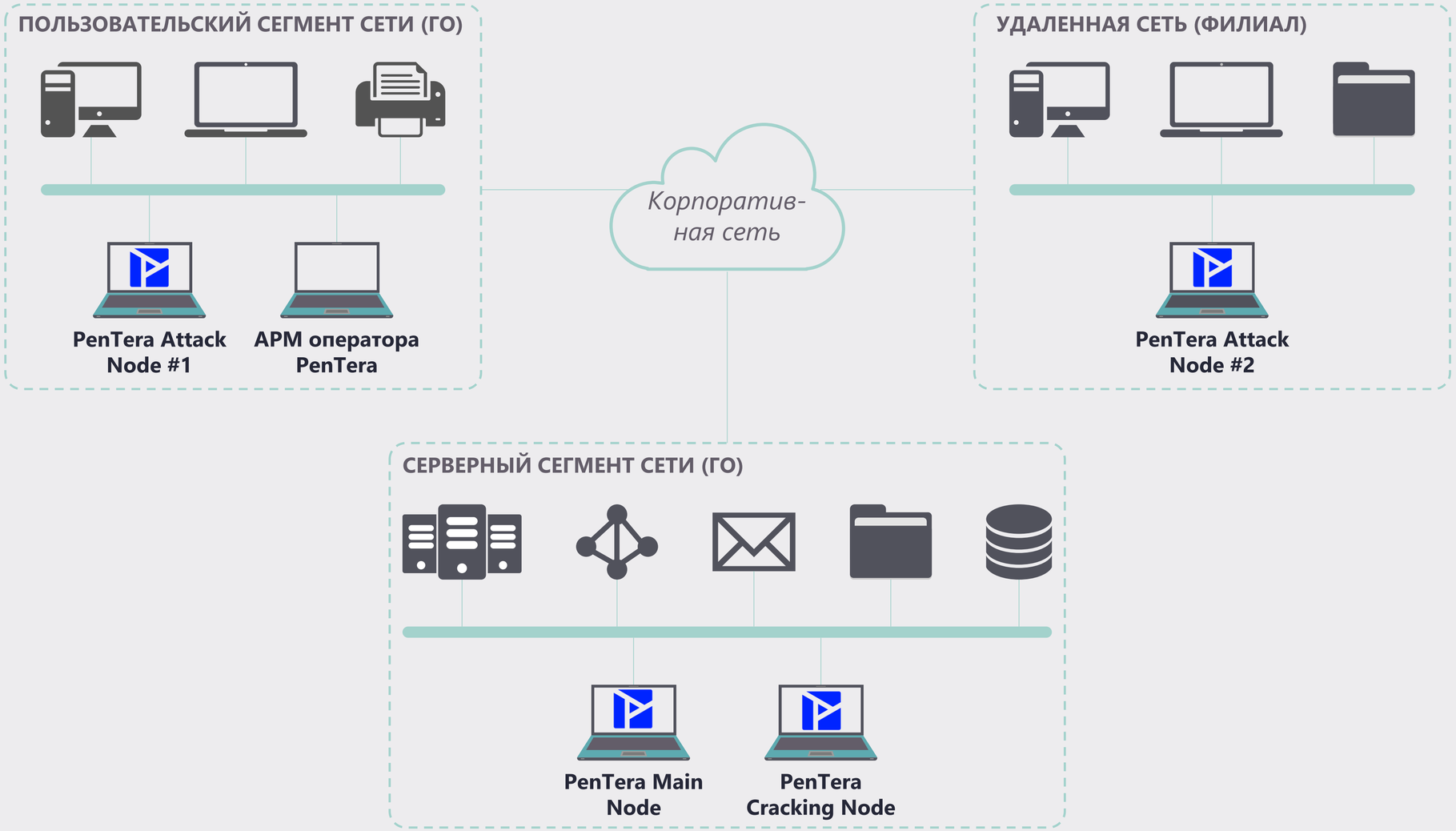
Ключевые выгоды

Автопентест 1 раз в неделю

ДиалогНаука

Схема внедрения Pentera в распределенной сети

Типовая схема внедрения



ДиалогНаука

Особенности автопентеста в распределенной среде

Ключевые параметры проекта

- Ключевые технические параметры проекта:
  - Принципиальная схема развертывания
  - Требуемые вычислительные ресурсы
  - Требуемые сетевые доступы
- Вопросы для разработки технического решения:
  - Масштаб сети (количество уникальных IP-адресов)
  - Какими ресурсами обладает злоумышленник?
  - Где находятся потенциальные цели атак?
  - Требуемая регулярность проверок

Пример расчета

- Вводная информация:
  - Масштаб сети – 5000 IP
  - Начальные точки: 3 пользовательских сегмента
  - Модель злоумышленника: внутренний (с у/д и без у/д)
  - Наиболее критичные активы: серверный сегмент ГО
  - Регулярность проверок: 1 раз в месяц
- Ключевые технические параметры проекта:
  - Состав решения: 1 узел управления MN, 1-3 атакующих узла AN
  - Доступы: между узлами MN и AN двусторонняя связь (TCP 8080, 22)

ДиалогНаука

Примеры реальных проектов

Пример проекта: банк

- Вводная информация:
  - Масштаб сети – 7000 IP
  - Начальные точки: различные пользовательские сегменты
  - Модель злоумышленника: внутренний (с у/д и без у/д)
  - Регулярность проверок: 1 раз в неделю
- Техническое решение:
  - Три независимые инсталляции по 6 атакующих узлов в каждой
  - Каждая инсталляция занимается тестированием своей зоны
  - Результат: еженедельное тестирование всей сети в двух режимах

Пример проекта: промышленность

- Вводная информация:
  - Масштаб сети – более 20000 IP
  - Сценарии тестирования – 36 различных направлений атак
  - Модель злоумышленника: внутренний (без у/д)
  - Дополнительно важна теоретическая оценка уязвимостей
  - Регулярность проверок: анализ уязвимостей - 1 раз в месяц, пентест – 1 раз в квартал
- Техническое решение:
  - Две независимые инсталляции: для задач VM (6 узлов) и автопентеста (50+ узлов)
  - Результат: ежеквартальный пентест по всем 36 интересующим сценариям

Пример проекта: банк (пентест ДЗО)

- Вводная информация:
  - Масштаб сети – более 20000 IP (включая сети ДЗО)
  - Сценарии тестирования – по 1 начальной точке для каждого ДЗО
  - Модель злоумышленника: внутренний (без у/д и с у/д)
  - Централизованный анализ отчетов по всем проверкам в единой консоли в ГО
  - Регулярность проверок: 1 раз в 2-4 недели проверка одного из ДЗО в двух режимах
- Техническое решение:
  - Распределенная установка: 1 узел управления в ГО, по 1 атакующему узлу в ДЗО, 2 мобильные инсталляции для выездных проверок

Есть вопросы?

Мы готовы ответить:

vfilin@citum.ru
+7(903)765-3862

v.solovev@dialognauka.ru
+7(915)387-9139