Четыре причины автоматизировать пентест

Валерий Филин
Технический директор

CITUM – экспертный дистрибьютор

Как проверить эффективность ИБ?

Инвестиции в решения ИБ с каждым годом растут

Угрозы
сложнее и агрессивнее

Дефицит кадров
3 млн. к 2020 году[1]

Регуляторы требуют
проверки защищенности

[1] Отчет Gartner 2017

Зачем нужен пентест?

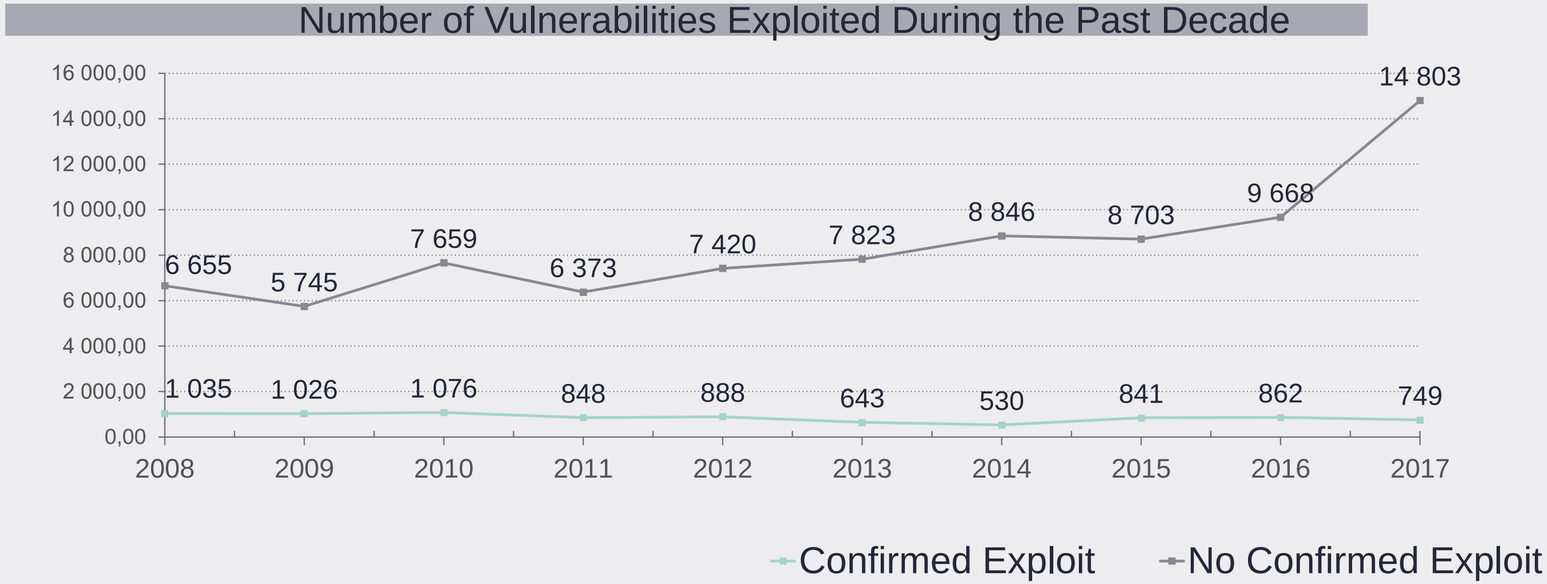
Сканеры дают поверхностную оценку:

Тысячи гипотетических уязвимостей

Усредненная оценка критичности

Не учитывает специфику сети

Фокус на уязвимостях ПО



В 2017 году только 5% всех известных уязвимостей были проэксплуатированы в действительности

Тестирование на проникновение

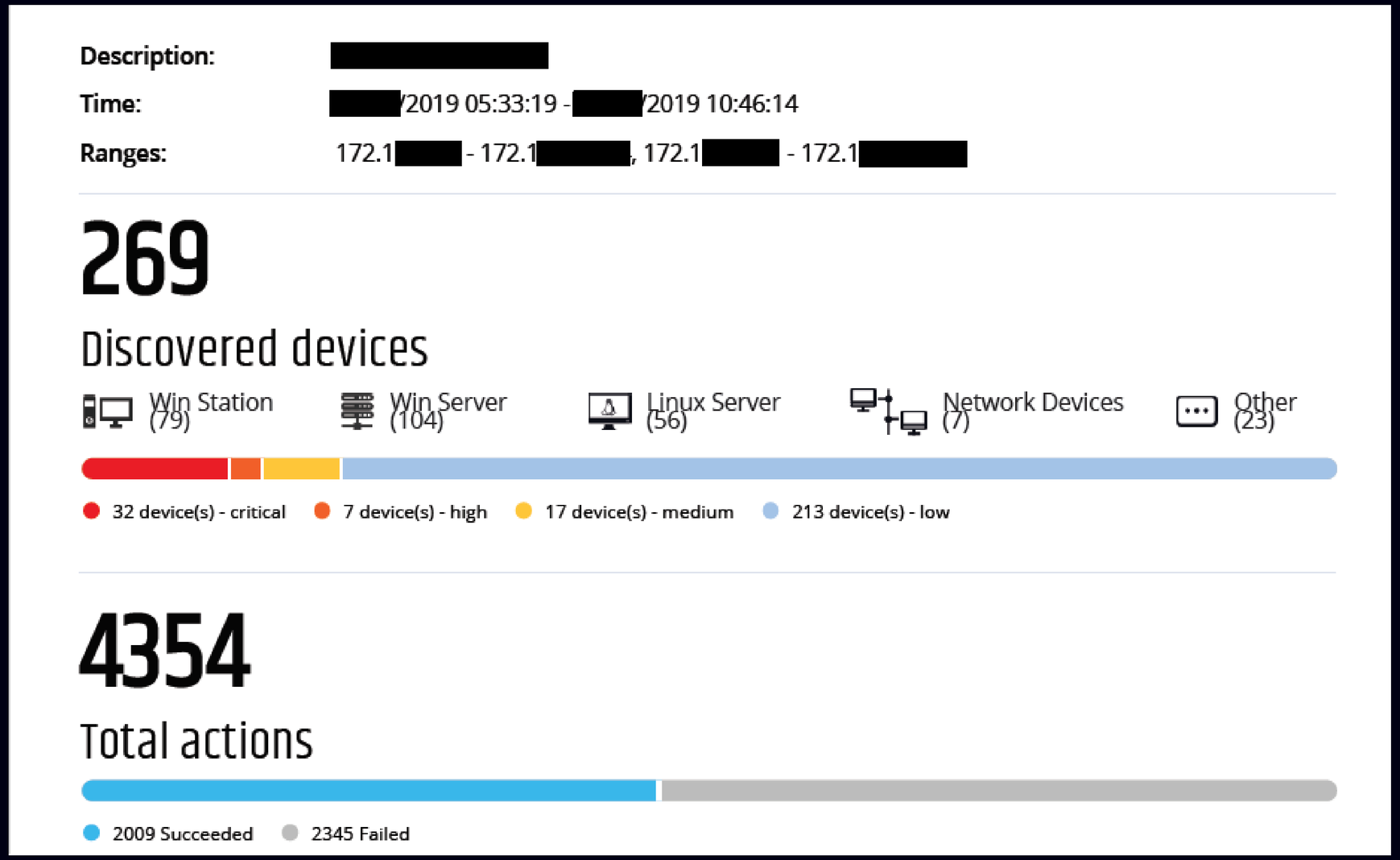
- Конкретная сеть
- Конкретные начальные условия
- Конкретная цель
- Активная эксплуатация
- Подтвержденные векторы атак
- Релевантные рекомендации

Причина №1. Скорость

- Анализ сети из 500 IP ~ 1 неделя
- Итог работы ~ 5-10 векторов атак
- Больший масштаб ~ недели-месяцы

Скорость машинного пентеста

- Продолжительность пентеста – около 5ч
- Скорость работы – более 800 операций в час
- Всего успешных операций – более 2000
- Найдено векторов атак – более 500
- Использовано уязвимостей – 13

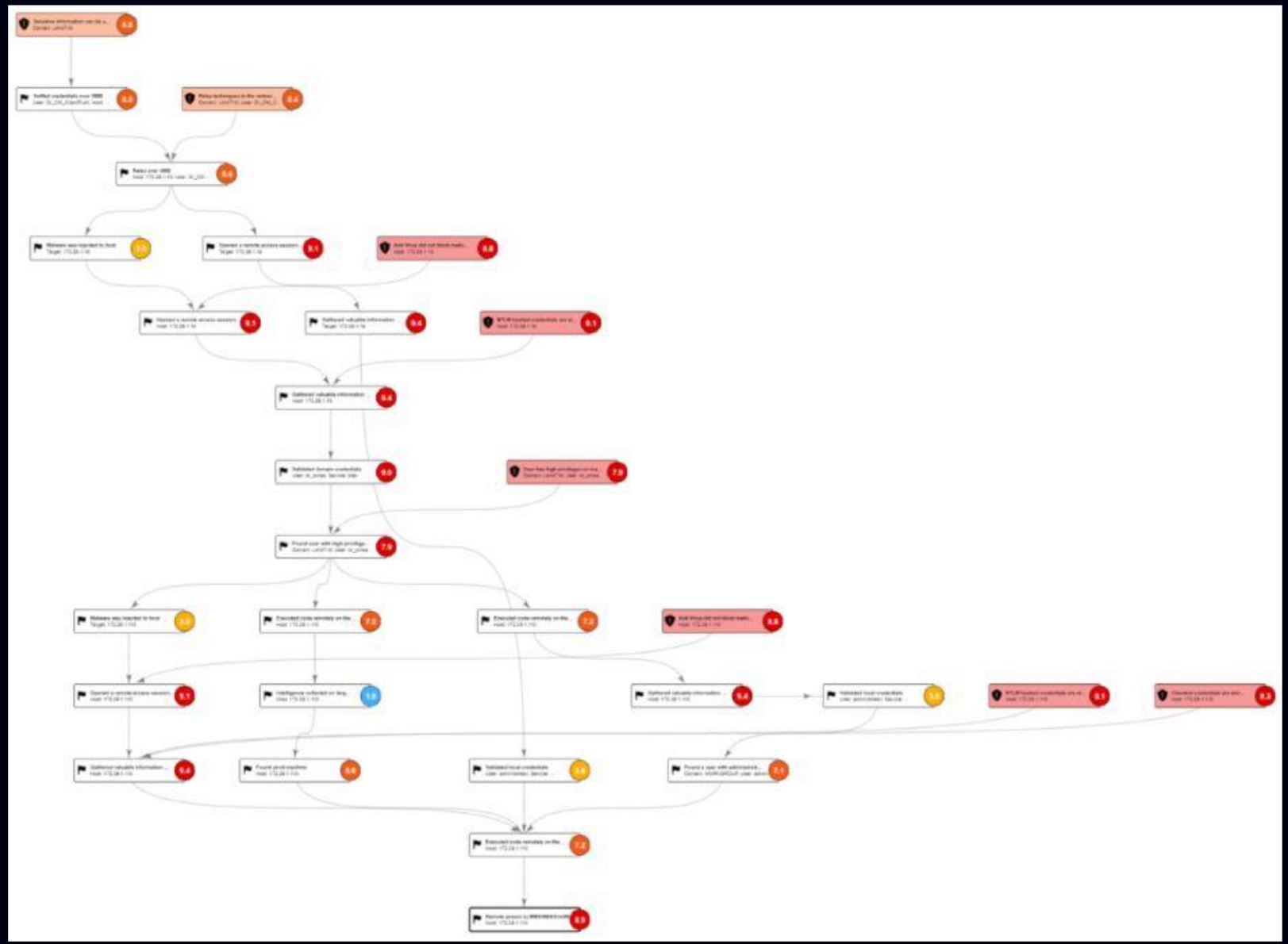


Причина №2. Масштаб

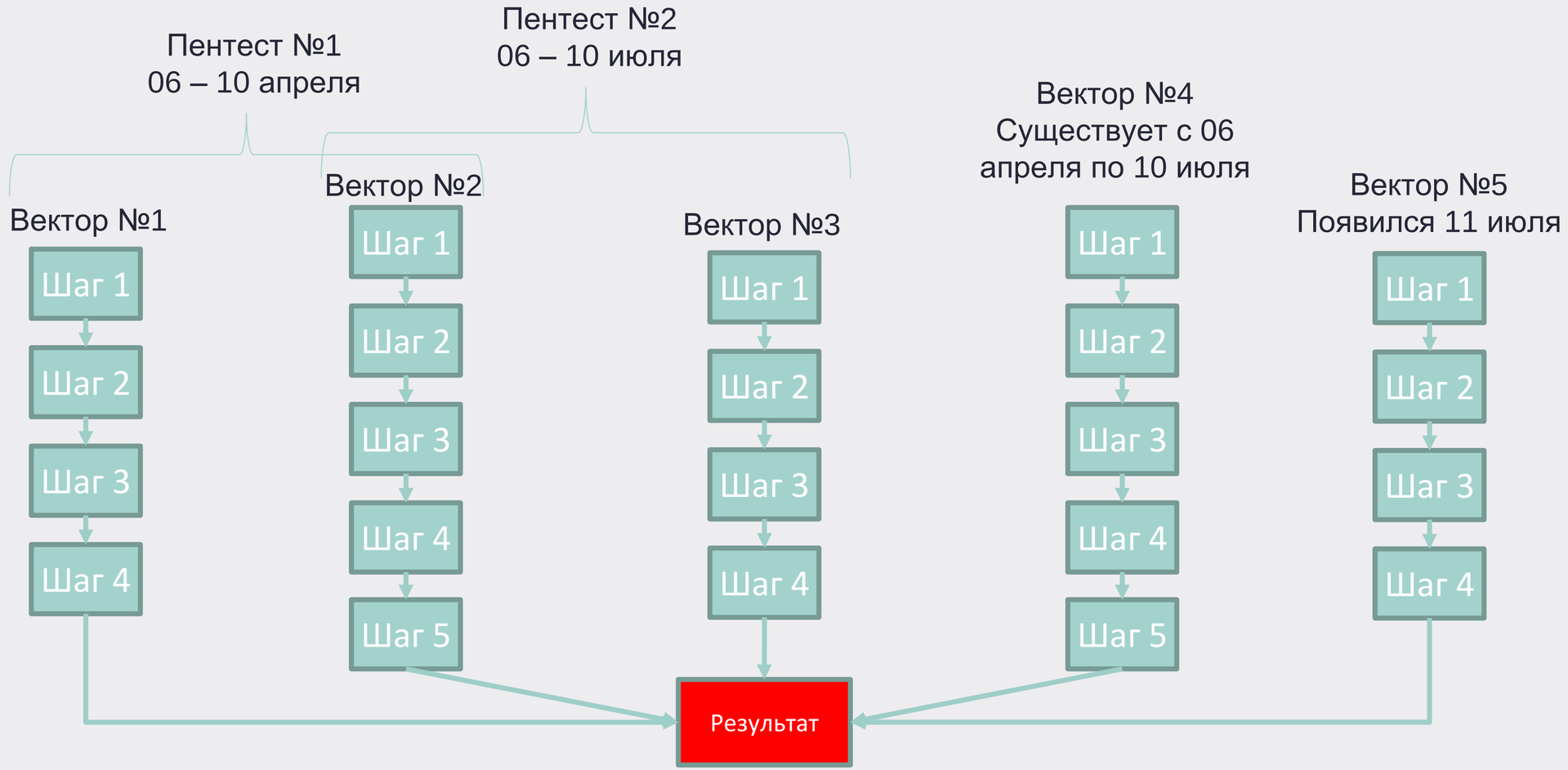
- Оценка сверху:
  - 2 уязвимости => 2 вектора
  - 3 уязвимости => 6 векторов
  - …
  - 10 уязвимостей => ~3,6 млн векторов
- Для сети > 10000 IP полноценный пентест невыполним
  - Трудозатраты ~ человеко-месяцы

Масштаб машинного пентеста

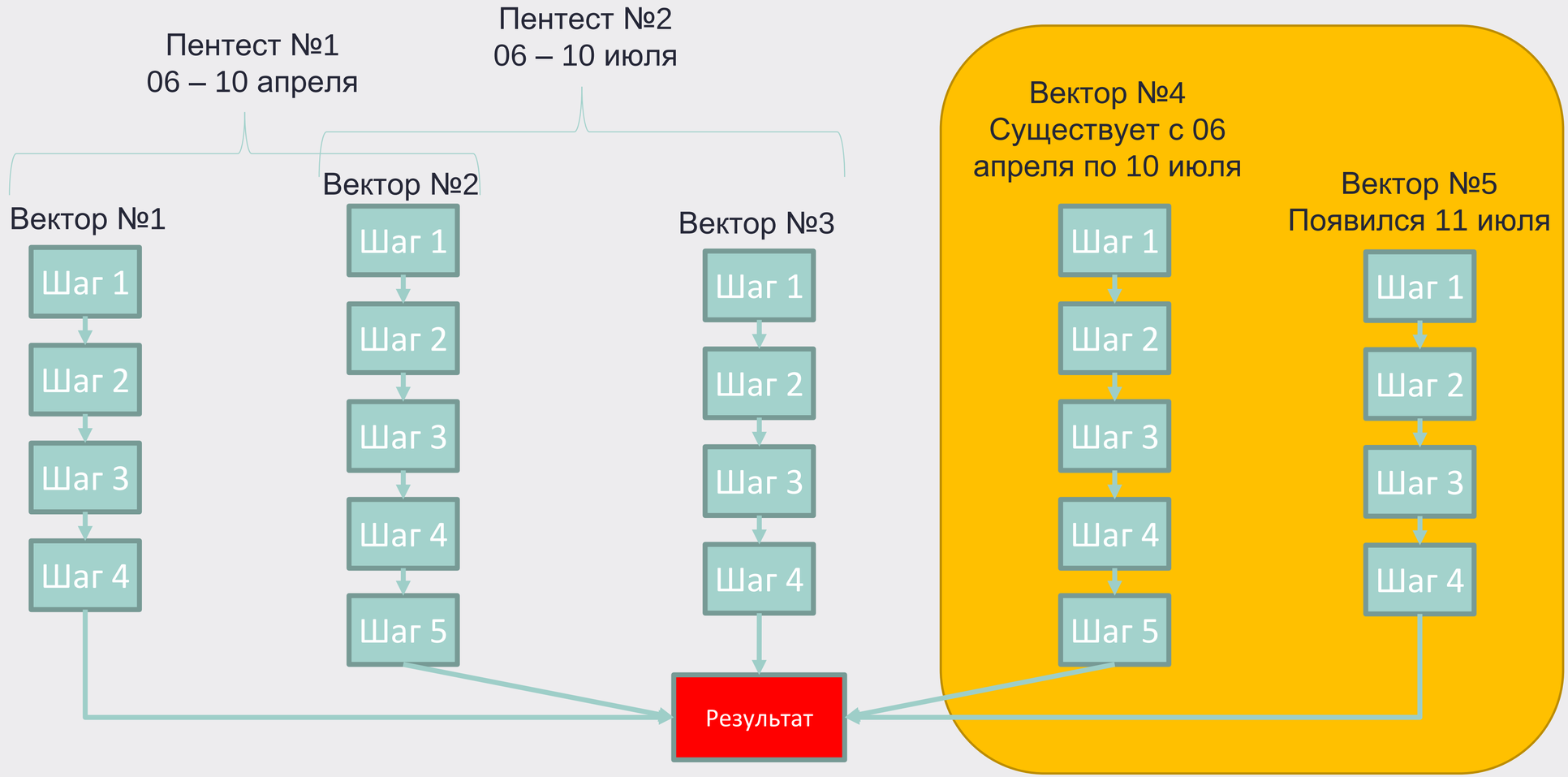
- Оценка всех возможных действий в масштабе
- Полная картина защищенности
- Все достижимые векторы атак
- За разумное время



Причина №3. Целостность



Причина №3. Целостность



Целостность машинного пентеста

- Регулярная проверка по четкой методике
- Быстрое обнаружение новых векторов
- Отслеживание трендов

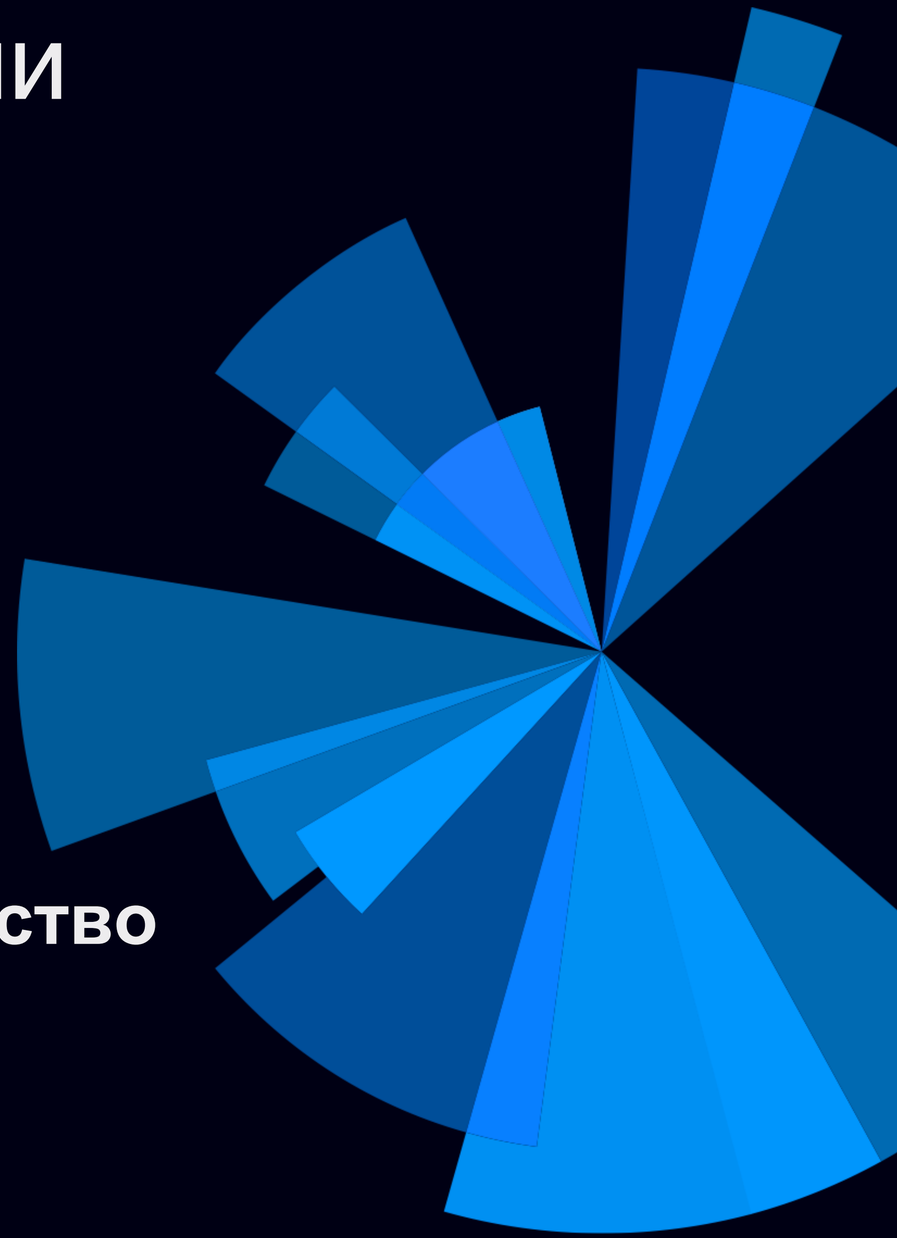
Причина №4. Стоимость

Показатель	Значение
Стоимость типового пентеста на 1000 IP	X
Сопутствующие трудозатраты заказчика на проект пентеста	Y
Совокупная стоимость полноценного пентеста на 5000 IP	5*X + Y
Стоимость ежеквартального полноценного пентеста на 5000 IP в год	20*X + 4*Y
Стоимость ежемесячного полноценного пентеста на 5000 IP в год	**60*X + 12*Y**
Стоимость решения автоматизации на 5000 IP (любое количество пентестов в год)	**~10-15*X**

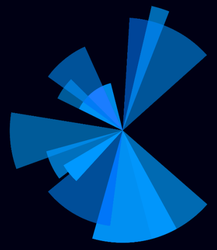
Преимущества автоматизации

- Высокая скорость анализа
- Непрерывная проверка защищенности
- Произвольное масштабирование
- Экономия человеческого ресурса
- Целостный результат оценки
- Неразглашение информации

Алгоритмы - машине, человеку – творчество



Решение



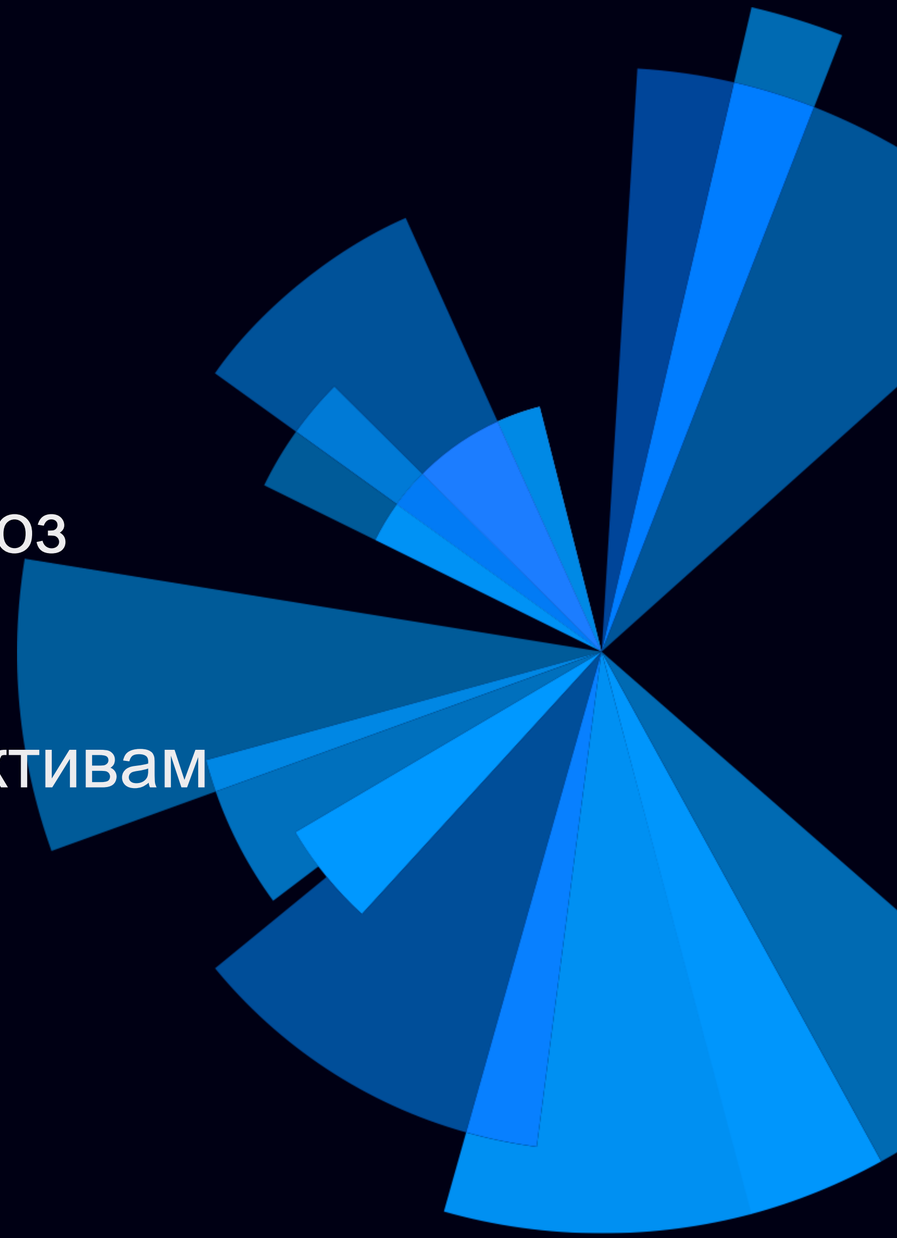
PenTera™ /

By Pcysys

Первая в мире платформа
автоматизации тестов на проникновение

Преимущества PenTera

- Быстрый запуск в работу
- Возможность автономного анализа
- Быстрое получение результатов
- Проверка самых актуальных техник и угроз
- Безопасная эксплуатация
- Тестирование специфичных сценариев
- Демонстрация векторов атак к ценным активам
- Полное представление о векторе атаки
- Высокоуровневая категорийная оценка
- Гибкая детализация отчетов
- Экономически эффективный подход



Есть вопросы?

Мы готовы ответить:
vfilin@citum.ru
+7(903)765-3862