CTRLHACK APT BEZDNA

ИТОГИ ТЕСТИРОВАНИЯ НОВОГО РЕШЕНИЯ СРЕДИ ЗАКАЗЧИКОВ АО «ДИЛОГНАУКА»

ПЯТАКОВ МАКСИМ

Сооснователь CTRLHACK

СОЛОВЬЕВ ВЛАДИМИР

Руководитель направления внедрения средств защиты отдела технических решений

ПРОДУКТЫ

CTRLHACK

BAS FELIX

Симуляция кибератакующих техник.

Проверка работы СЗИ и правил детектирования в SIEM.

Выполнение атомарных техник.

APT BEZDNA

Автоматический pentest.

Проверка выполнимости векторов атак.

Связные сценарии симуляции.

CTRLHACK APT BEZDNA

ПЛАТФОРМА АВТОМАТИЗИРОВАННЫХ ВНУТРЕННИХ ПЕНТЕСТОВ

Реализует различные возможные сценарии проведения атак

РОБОТ

Автоматически отрабатывает основные действия, выполняемые пентестерами в большинстве пентестов

СЦЕНАРИИ

сценарии внутреннего пентеста включают хакерские техники, методы пентестеров, эксплуатацию уязвимостей, методы выявления ошибок в конфигурациях

ЦЕЛИ И РЕЗУЛЬТАТ

CTRLHACK

Цель - определить выполнимость векторов атак, запрограммированных в системе, без ограничений человеческого фактора

РЕЗУЛЬТАТ

- приоритизация уязвимостей,
- выявление слабых мест в конфигурациях,
- выявление слабых паролей,
- выявление проблем в списках доступа,
- выявление проблем в сегментации сети,
- достижение критичных целей

ПЛАТФОРМА

CTRLHACK

без агентов

автоматическое выполнение

техники Windows, Linux

повторный запуск теста

ПРОСТОЙ ЗАПУСК

Три шага
Не требуются знания методов пентеста или хакерских техник

РЕЗУЛЬТАТ

Детальный отчет о каждом шаге выполнения теста

ВАРИАНТЫ ТЕСТА:

- «Черный ящик»
- «Серый ящик»

CTRLHACK

ЗАПУСКТЕСТА

«ЧЕРНЫЙ ЯЩИК»

Имитация ситуации в которой хакер имеет доступ к сети и не обладает дополнительными данными

- выбор начальной точки атаки
- выбор диапазона IP-адресов

«СЕРЫЙ ЯЩИК»

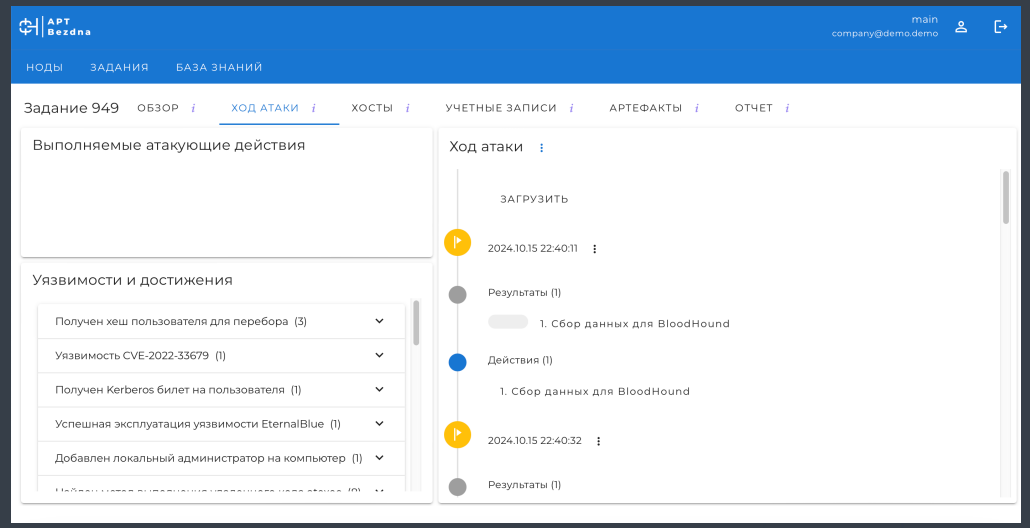
Оценка риска в случае компрометации определенного пользователя

- дополнительно задаются данные пользователя

ИНТЕРФЕЙС

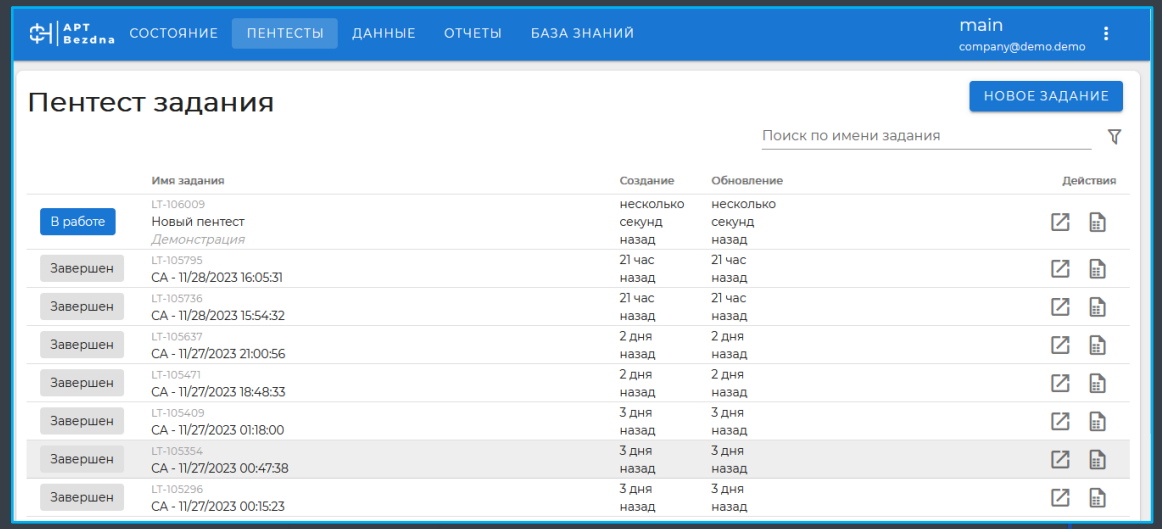
ХОД ВЫПОЛНЕНИЯ

каждый шаг выполнения теста отображается на экране и в отчете



ЗАДАНИЯ

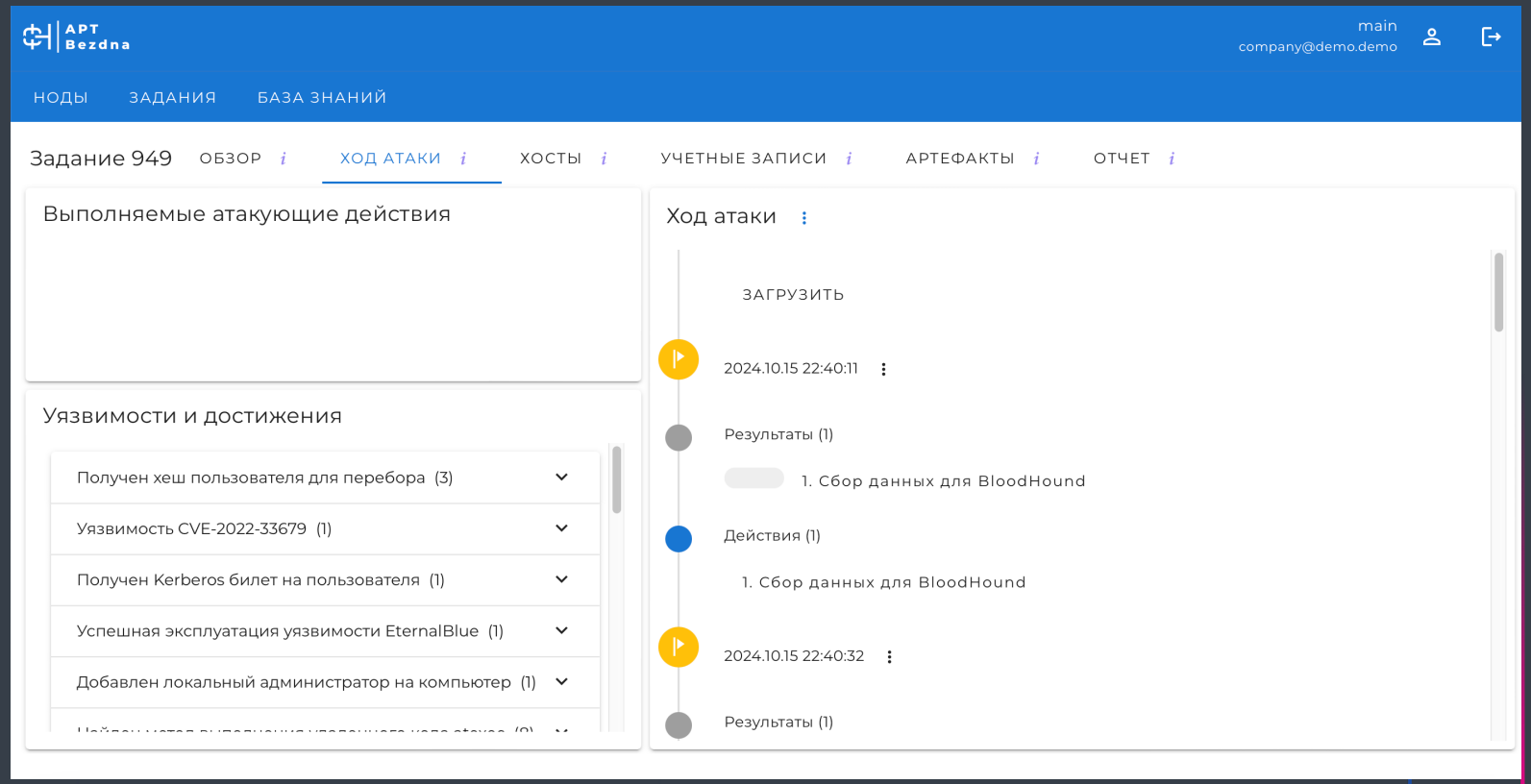
все тесты отображаются в одном окне



РЕЗУЛЬТАТ

РЕЗУЛЬТАТ ВЫПОЛНЕНИЯ ТЕСТА представлен в виде таймлайна

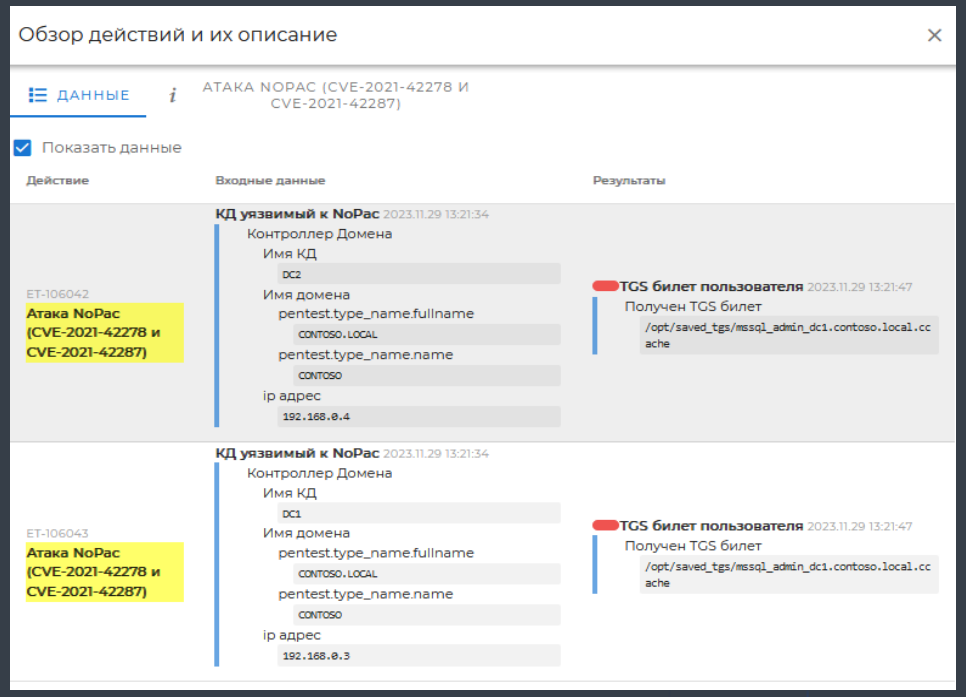
- можно оценить ход развития атаки
- можно определить первичную корневую проблему, позволившую выполнить атаку

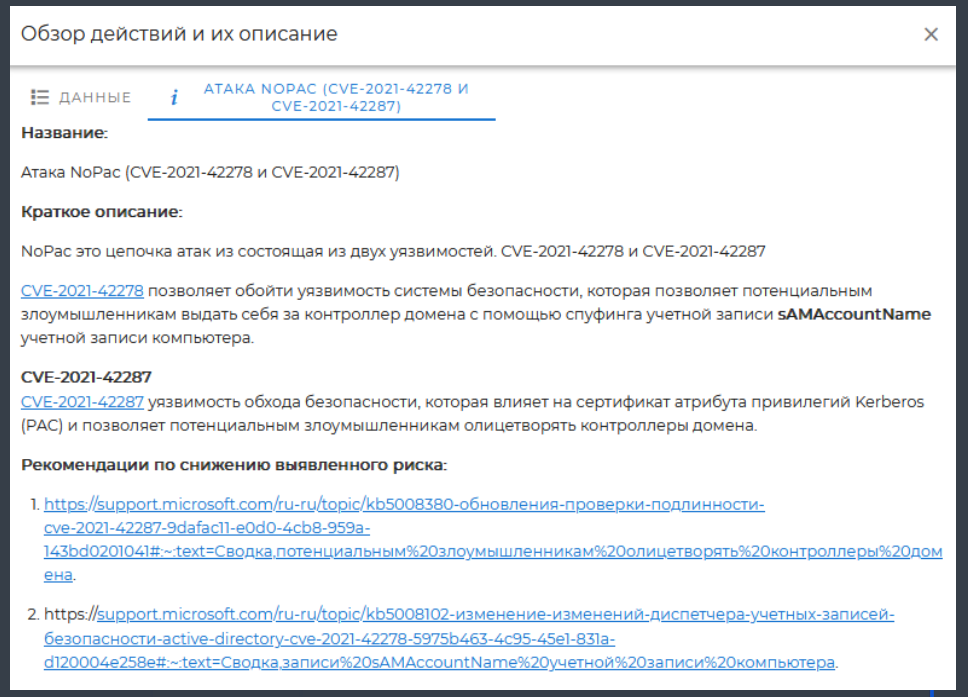


РЕЗУЛЬТАТЫ

ДЛЯ ВСЕХ ШАГОВ ТЕСТА :

- дано детальное описание
- приведены все полученные результаты
- даны рекомендации по устранению





ЧТО УЖЕ ИСПОЛЬЗУЕТСЯ?

CTRLHACK

СКАНЕРЫ УЯЗВИМОСТЕЙ

для выявления уязвимостей, которые могут использоваться в атаках

МИНУСЫ

- выдают очень большой объем данных
- сложная приоритезация уязвимостей
- не учитывают наличие СЗИ
- не показывают возможность эксплуатации во время атаки

РУЧНОЙ PENTEST

для определения возможности выполнения векторов атаки

МИНУСЫ

- ограниченный набор техник
- только часть инфраструктуры
- зависимость от квалификации пентестеров
- длительный срок
- результат раз в полгода или год

ПРЕИМУЩЕСТВА

CTRLHACK

регулярная проверка

неразглашение информации

не требует постоянного контроля оператора

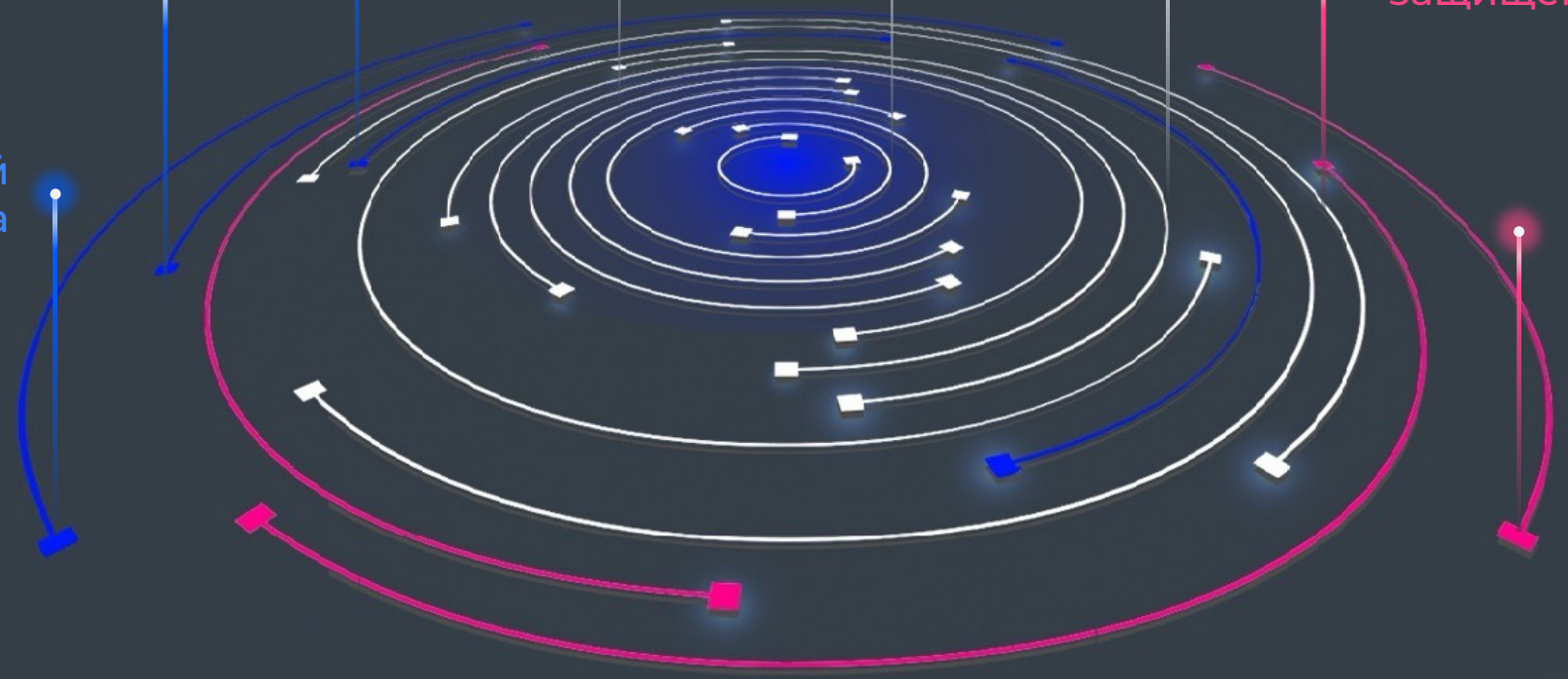
экономия человеческого ресурса

не требует глубоких знаний

непрерывная проверка защищенности

простой запуск теста

быстрая проверка после исправлений



CTRLHACK

ЧТО ДАЕТ РЕЗУЛЬТАТ В ПЕНТЕСТАХ?

- Ошибки конфигурации в центре сертификации MS AD
- Слабые пароли пользователей
- Перенаправление трафика NTLM-Relay
- Ошибки конфигурации ACL в MS AD
- PrintNightmare (CVE-2021-34527)

ЕСТЬ В APT BEZDNA

CTRLHACK

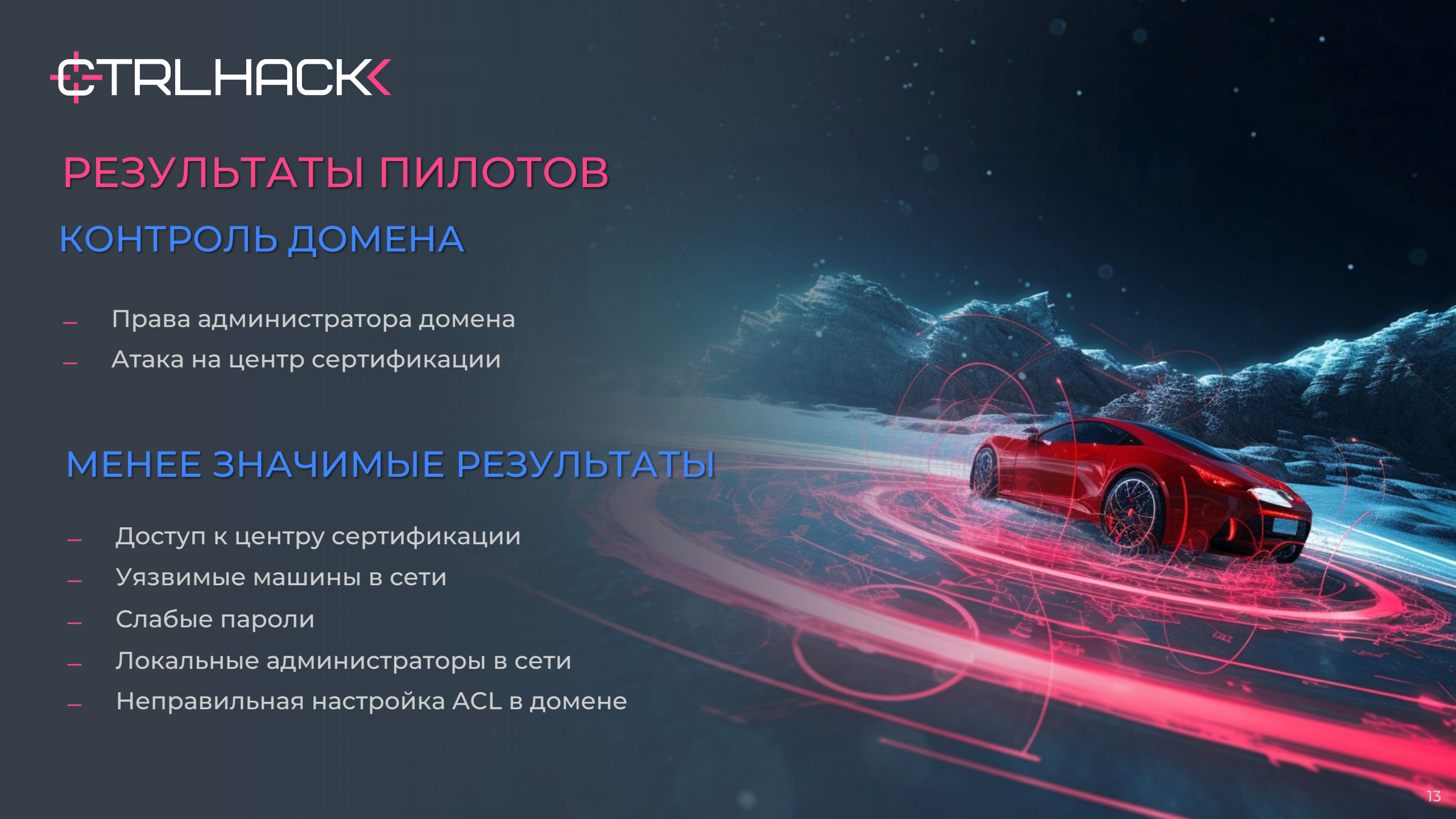
РЕЗУЛЬТАТЫ ПИЛОТОВ

КОНТРОЛЬ ДОМЕНА

- Права администратора домена
- Атака на центр сертификации

МЕНЕЕ ЗНАЧИМЫЕ РЕЗУЛЬТАТЫ

- Доступ к центру сертификации
- Уязвимые машины в сети
- Слабые пароли
- Локальные администраторы в сети
- Неправильная настройка ACL в домене



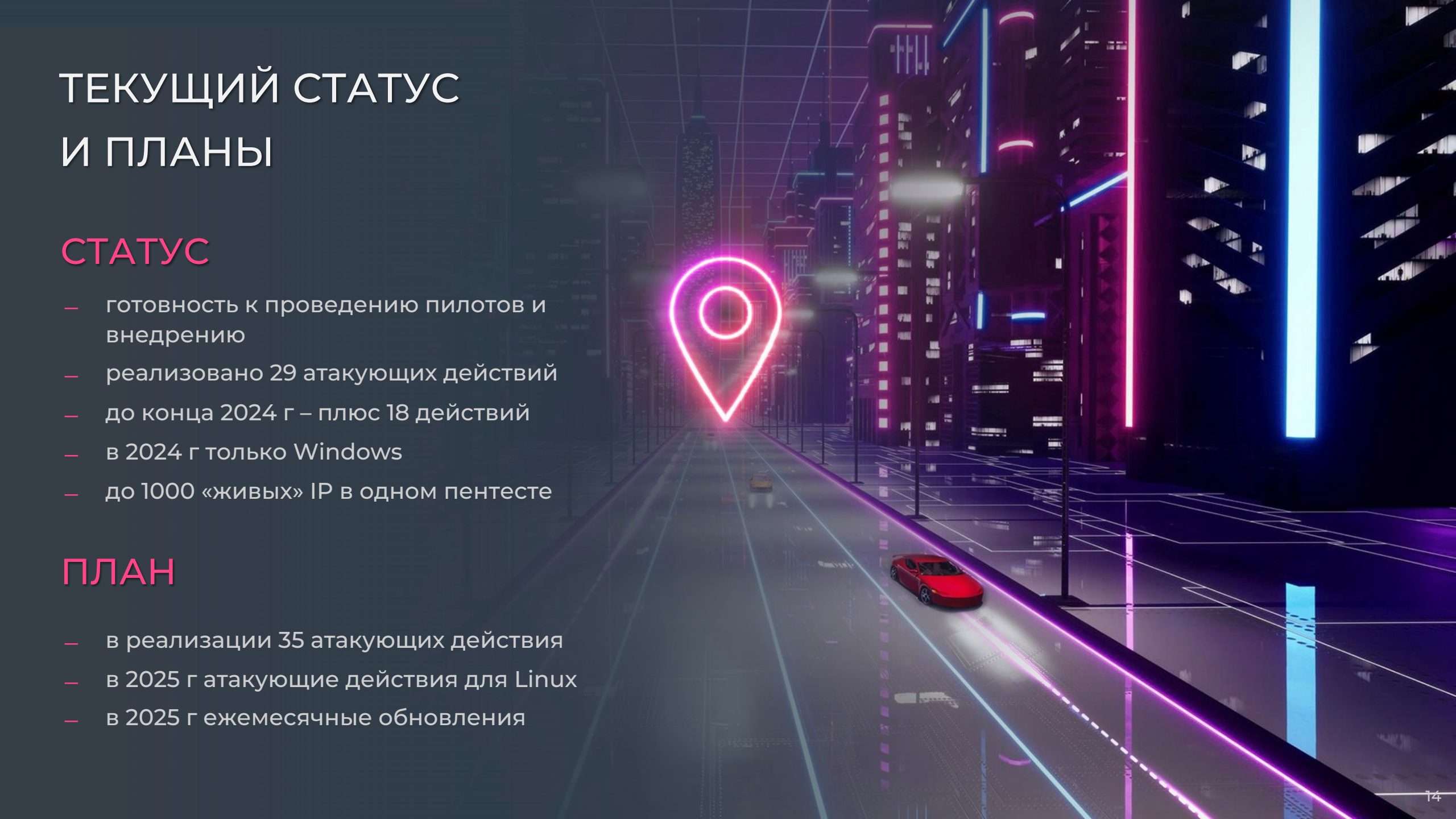
ТЕКУЩИЙ СТАТУС И ПЛАНЫ

СТАТУС

- готовность к проведению пилотов и внедрению
- реализовано 29 атакующих действий
- до конца 2024 г – плюс 18 действий
- в 2024 г только Windows
- до 1000 «живых» IP в одном пентесте

ПЛАН

- в реализации 35 атакующих действия
- в 2025 г атакующие действия для Linux
- в 2025 г ежемесячные обновления



CTRLHACK

DEMO

CTRLHACK

СПАСИБО ЗА ВНИМАНИЕ

ООО «КОНТРОЛХАК»
+7 (495) 789 72 97
info@ctrlhack.ru
www.ctrlhack.ru