ПЕРВАЯ РОССИЙСКАЯ ПЛАТФОРМА АВТОМАТИЧЕСКОГО ПЕНТЕСТА CTRLHACK APT BEZDNA

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.

ЧТО УЖЕ ИСПОЛЬЗУЕТСЯ?

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

ПЛАТФОРМА АВТОМАТИЗИРОВАННЫХ ВНУТРЕННИХ ПЕНТЕСТОВ

Реализует различные возможные сценарии проведения атак

ЦЕЛЬ

определяет достижимость векторов атак, запрограм-мированных в системе, без ограничений человеческого фактора

СЦЕНАРИИ

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

РЕЗУЛЬТАТ

приоритезирует уязвимости, выявляет слабые места в конфигурациях, определяет реальные векторы кибератак

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
- настройка параметров запуска

«СЕРЫЙ ЯЩИК»

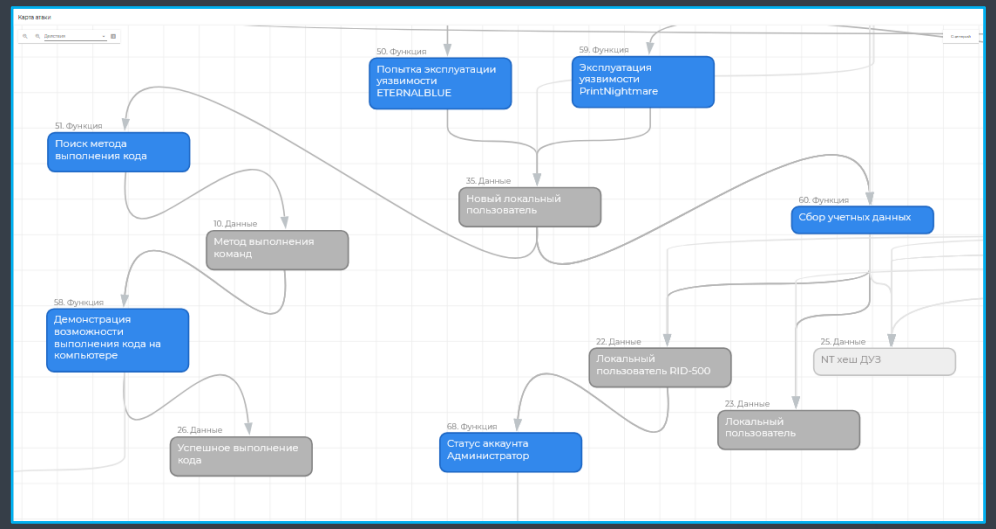
Оценка риска в случае компрометации определенного пользователя

- дополнительно задаются данные пользователя

ИНТЕРФЕЙС

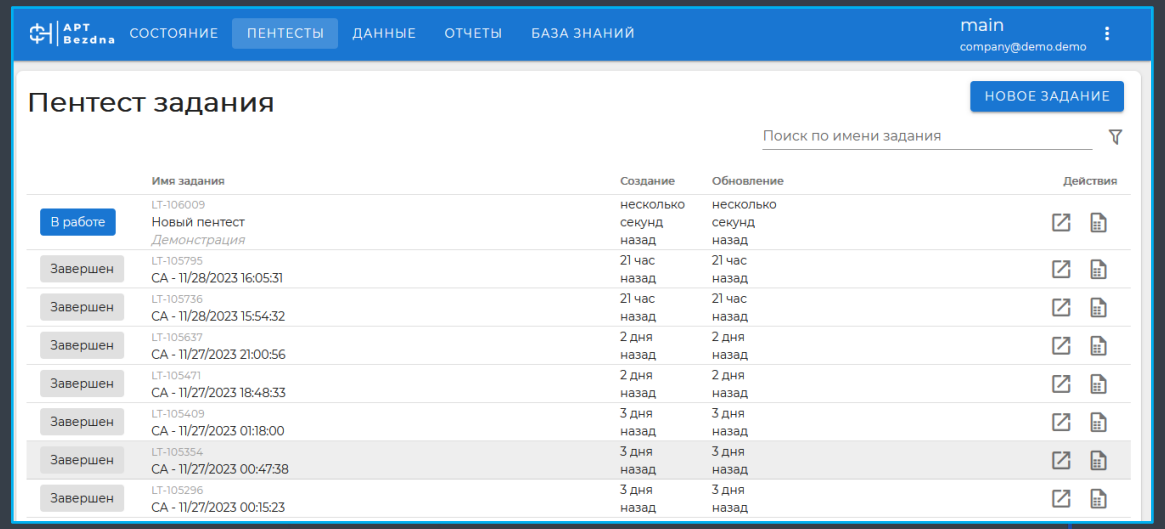
ХОД ВЫПОЛНЕНИЯ

каждый шаг выполнения теста отображается на экране и в отчете



ЗАДАНИЯ

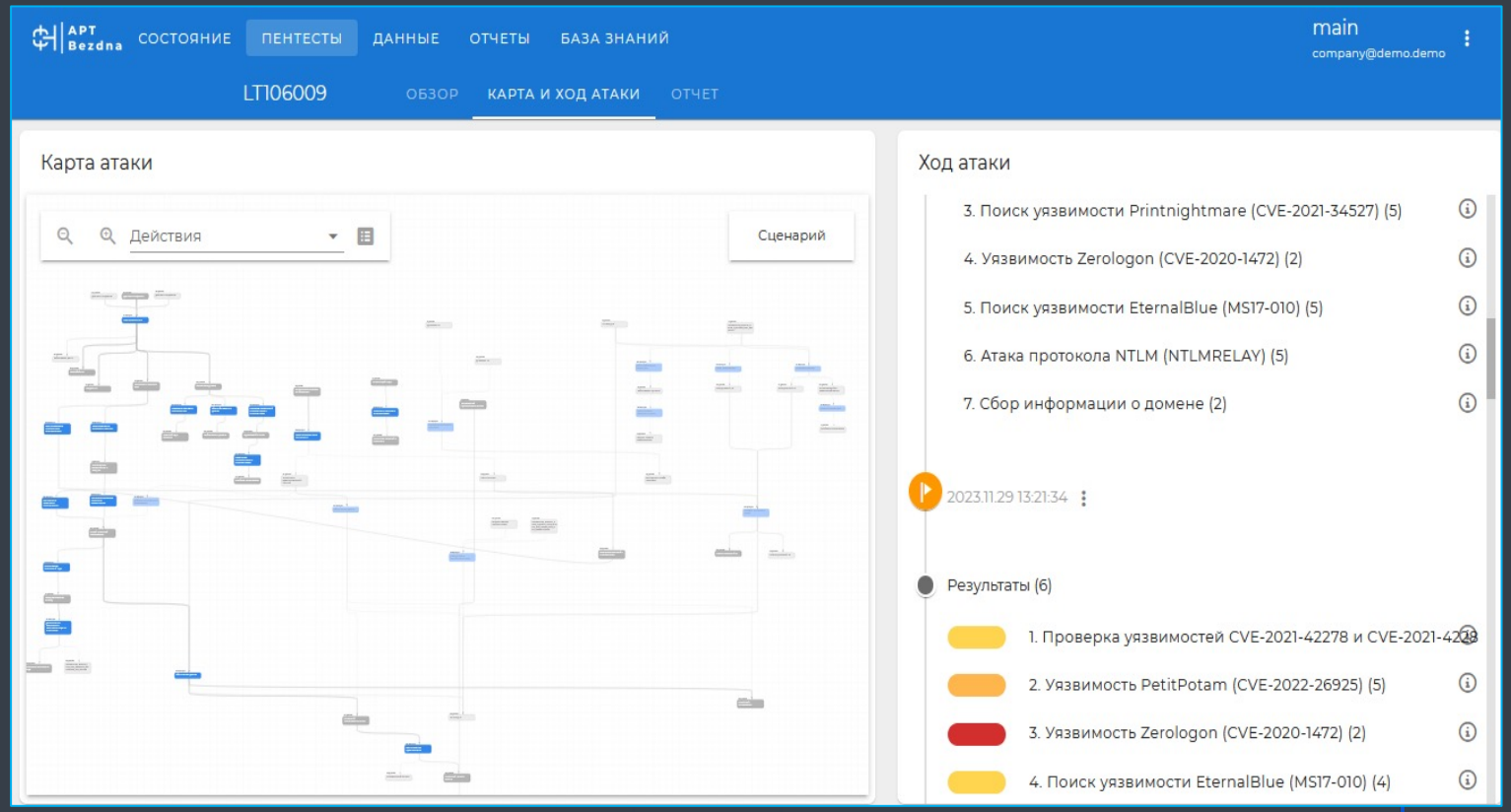
все тесты отображаются в одном окне



РЕЗУЛЬТАТ

РЕЗУЛЬТАТ ВЫПОЛНЕНИЯ ТЕСТА представлен в виде графической карты, что дает возможность:

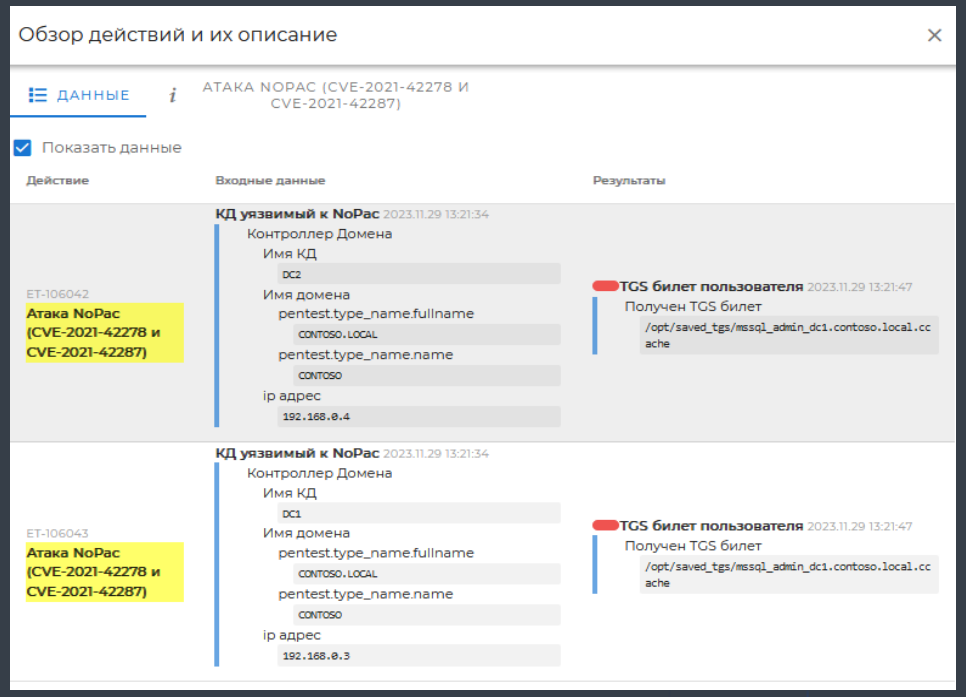
- оценить ход развития атаки
- определить первичную корневую проблему, позволившую выполнить атаку

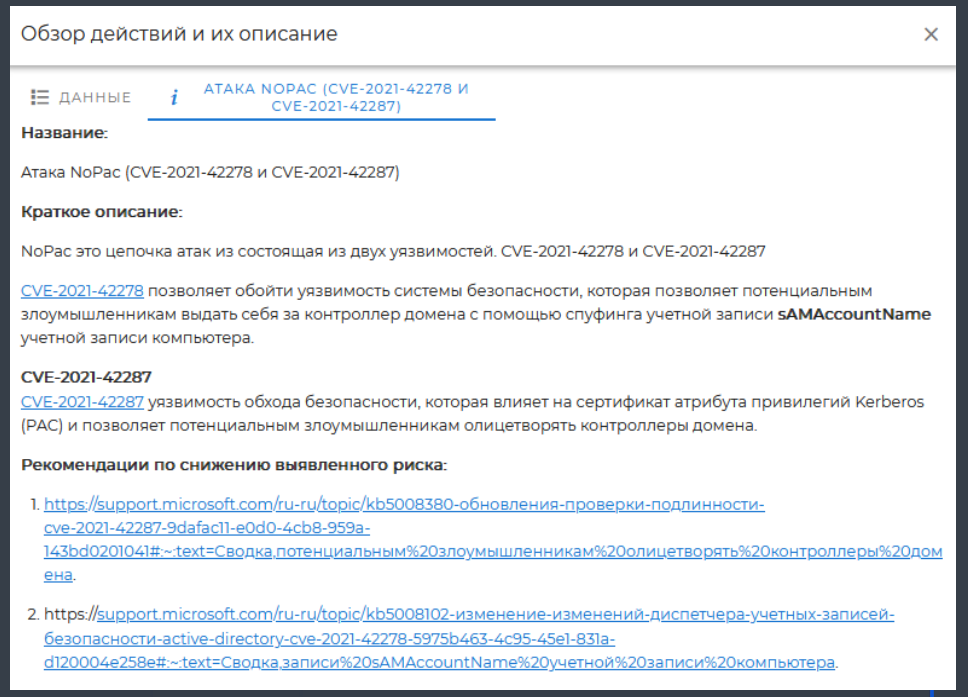


РЕЗУЛЬТАТЫ

ДЛЯ ВСЕХ ШАГОВ ТЕСТА :

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





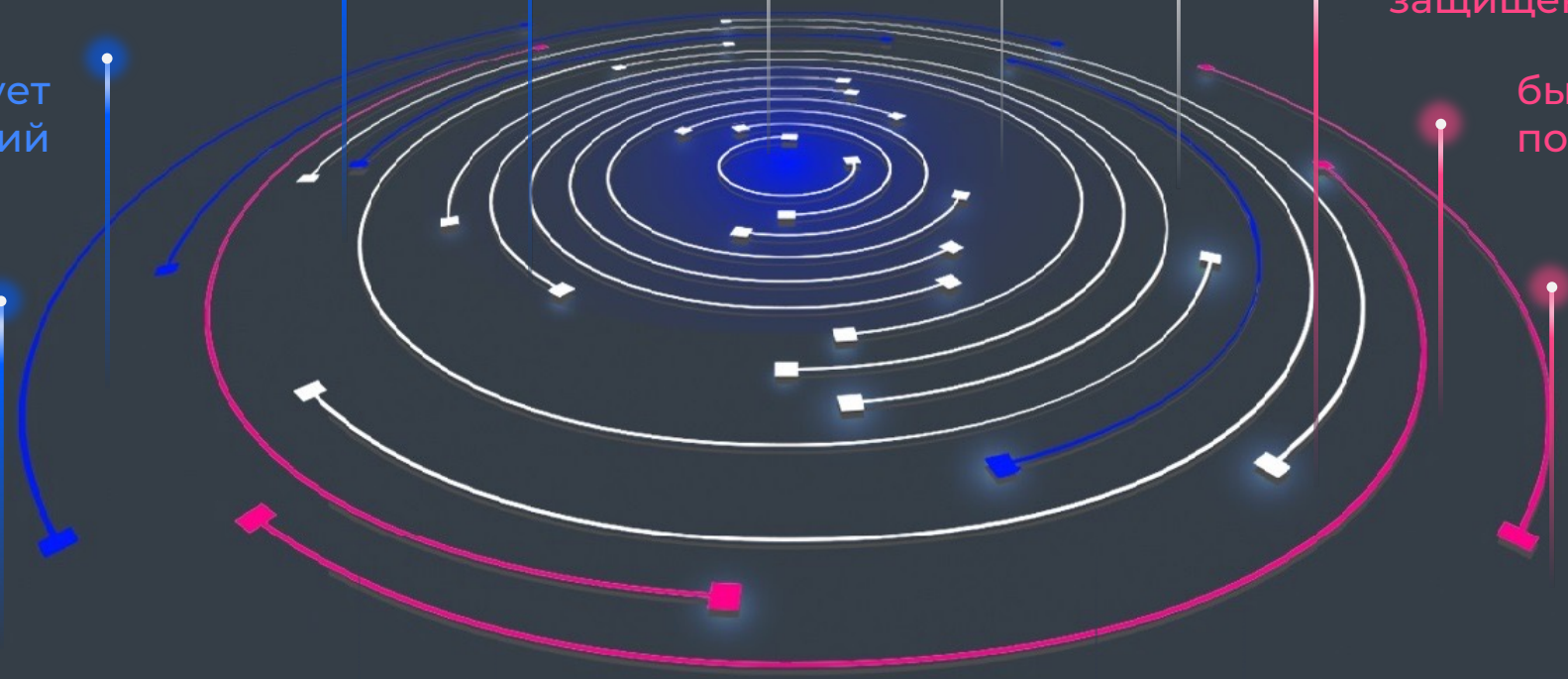
CTRLHACK

ВЫПОЛНЕННЫЕ ТЕСТЫ ПОЗВОЛЯЮТ ПРОВЕРИТЬ:

- корректрность доменных политик и настроек ОС
- качество управления привилегиями
- эффективность средств защиты
- эффективность процессов реагирования
- защищенность активов
- возможность эксплуатации уязвимостей

ПРЕИМУЩЕСТВА

CTRLHACK



построение или модернизация SOC

регулярная проверка

экономия человеческого ресурса

не требует постоянного контроля оператора

неразглашение информации

непрерывная проверка защищенности

не требует глубоких знаний

быстрая проверка после исправлений

простой запуск теста

четкое обоснование необходимост и исправлений для ИТ

CTRLHACK

ОТЛИЧИЯ ОТ СУЩЕСТВУЮЩИХ РЕШЕНИЙ

- скорость работы
- гибкие настройки в части хода выполнения пентеста (исключение шагов, исключение узлов для некоторых шагов, подтверждение для оператора на некоторых шагах)
- возможность добавления данных в выполняемый пентест
- возможность передачи данных из ранее выполненных пентестов в новый пентест
- возможность добавления своих атакующих функций и эксплойтов.
- возможность одновременного выполнения нескольких пентестов

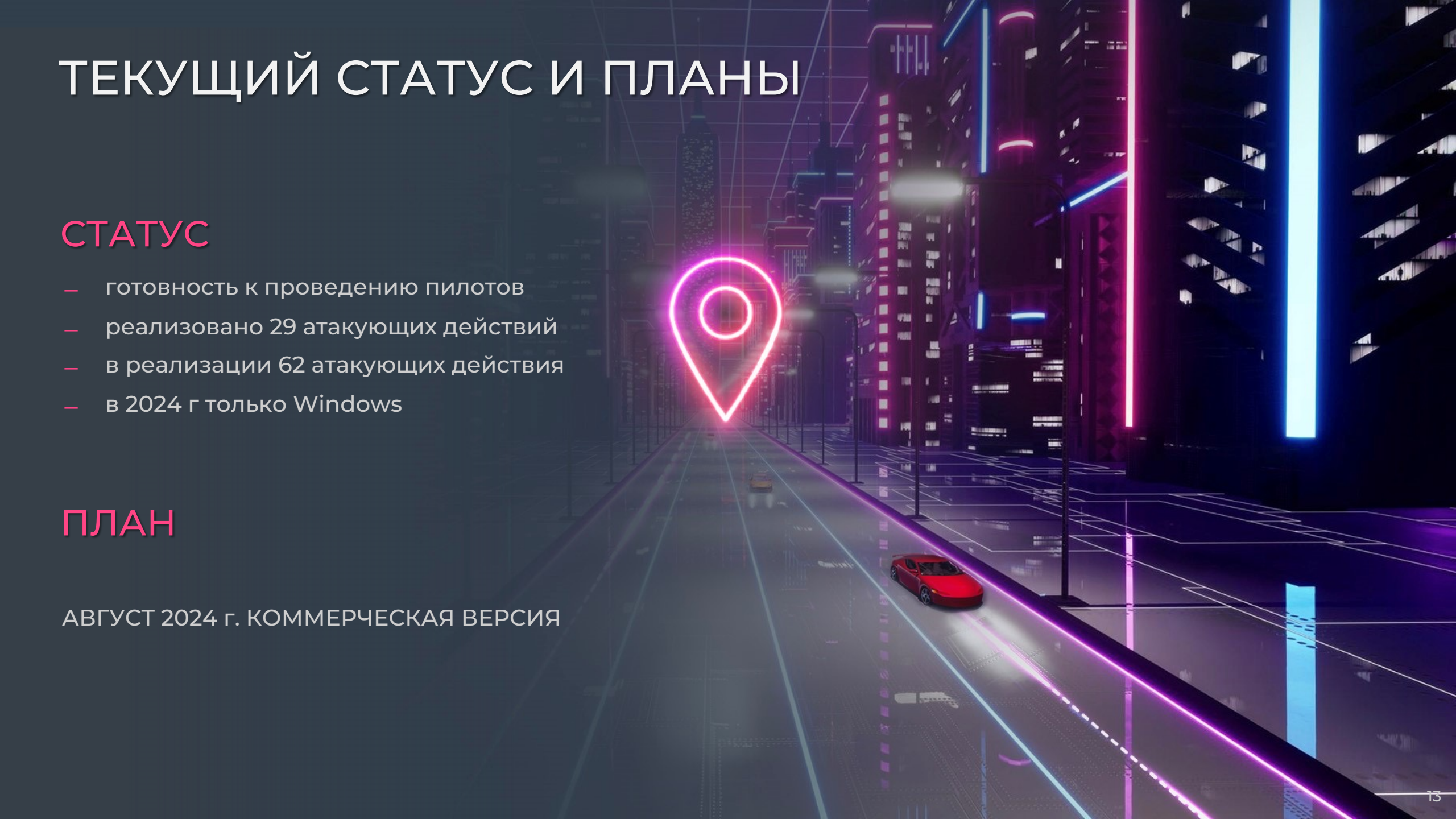
ТЕКУЩИЙ СТАТУС И ПЛАНЫ

СТАТУС

- готовность к проведению пилотов
- реализовано 29 атакующих действий
- в реализации 62 атакующих действия
- в 2024 г только Windows

ПЛАН

АВГУСТ 2024 г. КОММЕРЧЕСКАЯ ВЕРСИЯ



CTRLHACK

DEMO

CTRLHACK

СПАСИБО ЗА ВНИМАНИЕ

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