

---

# ПЕРВАЯ РОССИЙСКАЯ ПЛАТФОРМА АВТОМАТИЧЕСКОГО ПЕНТЕСТА CTRLHACK ART BEZDNA



ПЯТАКОВ МАКСИМ  
Сооснователь CTRLHACK



СОЛОВЬЕВ ВЛАДИМИР  
Руководитель направления внедрения средств защиты  
отдела технических решений

## 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, запрограммированных 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



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»

## ЗАПУСК ТЕСТА

### «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»

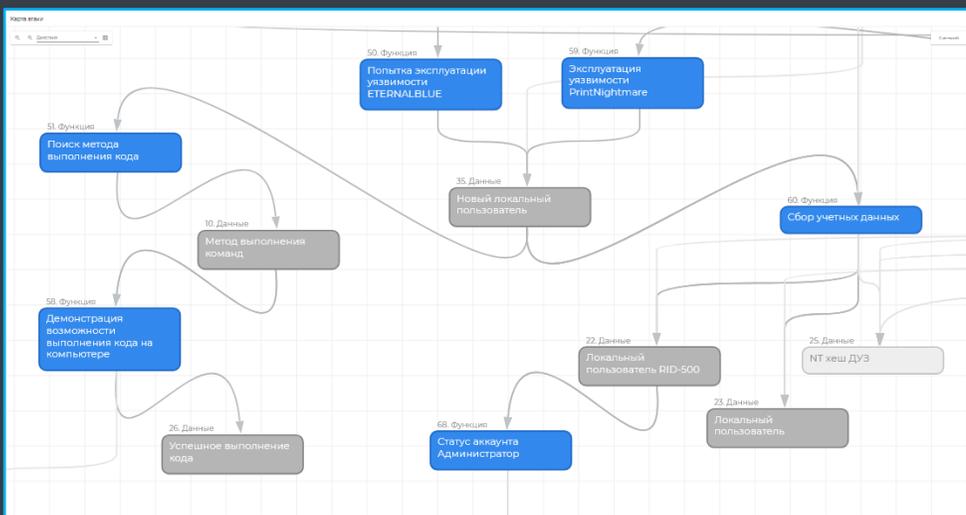
Оценка риска в случае компрометации определенного пользователя

- дополнительно задаются данные пользователя



## ХОД ВЫПОЛНЕНИЯ

каждый шаг выполнения теста отображается на экране и в отчете



## ЗАДАНИЯ

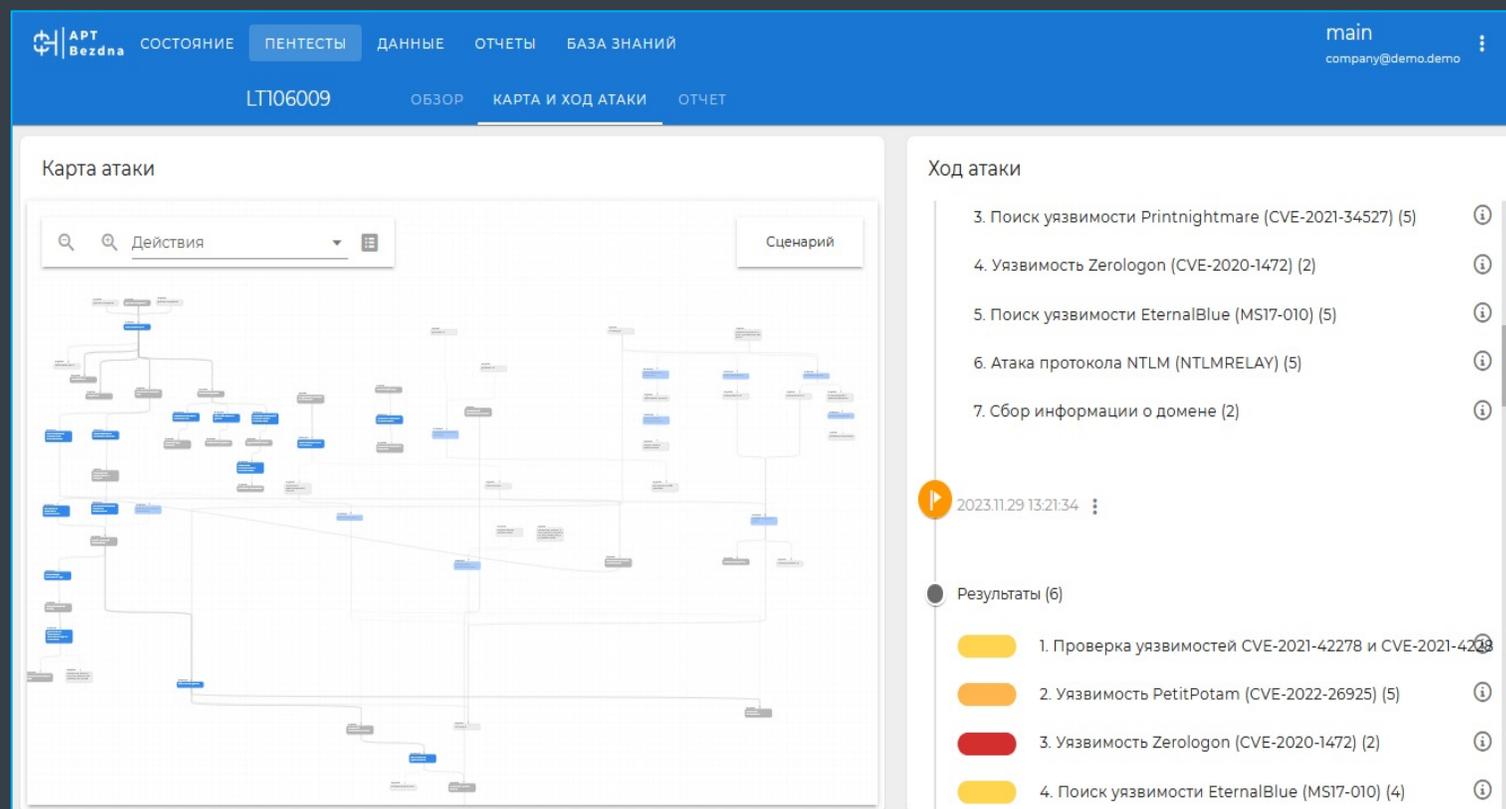
все тесты отображаются в одном окне

	Имя задания	Создание	Обновление	Действия
В работе	LT-106009 Новый пентест Демонстрация	несколько секунд назад	несколько секунд назад	
Завершен	LT-105795 CA - 11/28/2023 16:05:31	21 час назад	21 час назад	
Завершен	LT-105736 CA - 11/28/2023 15:54:32	21 час назад	21 час назад	
Завершен	LT-105637 CA - 11/27/2023 21:00:56	2 дня назад	2 дня назад	
Завершен	LT-105471 CA - 11/27/2023 18:48:33	2 дня назад	2 дня назад	
Завершен	LT-105409 CA - 11/27/2023 01:18:00	3 дня назад	3 дня назад	
Завершен	LT-105354 CA - 11/27/2023 00:47:38	3 дня назад	3 дня назад	
Завершен	LT-105296 CA - 11/27/2023 00:15:23	3 дня назад	3 дня назад	

# 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

Обзор действий и их описание

☰ ДАННЫЕ ⓘ АТАКА NoPac (CVE-2021-42278 и CVE-2021-42287)

Показать данные

Действие	Входные данные	Результаты
ET-106042 Атака NoPac (CVE-2021-42278 и CVE-2021-42287)	<b>КД уязвимый к NoPac</b> 2023.11.29 13:21:34 Контроллер Домена Имя КД dc2 Имя домена pentest_type_name.fullname contoso.LOCAL pentest_type_name.name contoso ip адрес 192.168.0.4	<b>TGS билет пользователя</b> 2023.11.29 13:21:47 Получен TGS билет /opt/saved_tgs/mssql_admin_dc1.contoso.local.ccache
ET-106043 Атака NoPac (CVE-2021-42278 и CVE-2021-42287)	<b>КД уязвимый к NoPac</b> 2023.11.29 13:21:34 Контроллер Домена Имя КД dc1 Имя домена pentest_type_name.fullname contoso.LOCAL pentest_type_name.name contoso ip адрес 192.168.0.3	<b>TGS билет пользователя</b> 2023.11.29 13:21:47 Получен TGS билет /opt/saved_tgs/mssql_admin_dc1.contoso.local.ccache

Обзор действий и их описание

☰ ДАННЫЕ ⓘ АТАКА NoPac (CVE-2021-42278 и CVE-2021-42287)

**Название:**  
Атака NoPac (CVE-2021-42278 и CVE-2021-42287)

**Краткое описание:**  
NoPac это цепочка атак из состоящая из двух уязвимостей. CVE-2021-42278 и CVE-2021-42287  
[CVE-2021-42278](#) позволяет обойти уязвимость системы безопасности, которая позволяет потенциальным злоумышленникам выдать себя за контроллер домена с помощью спуфинга учетной записи **sAMAccountName** учетной записи компьютера.  
**CVE-2021-42287**  
[CVE-2021-42287](#) уязвимость обхода безопасности, которая влияет на сертификат атрибута привилегий Kerberos (PAC) и позволяет потенциальным злоумышленникам олицетворять контроллеры домена.

**Рекомендации по снижению выявленного риска:**

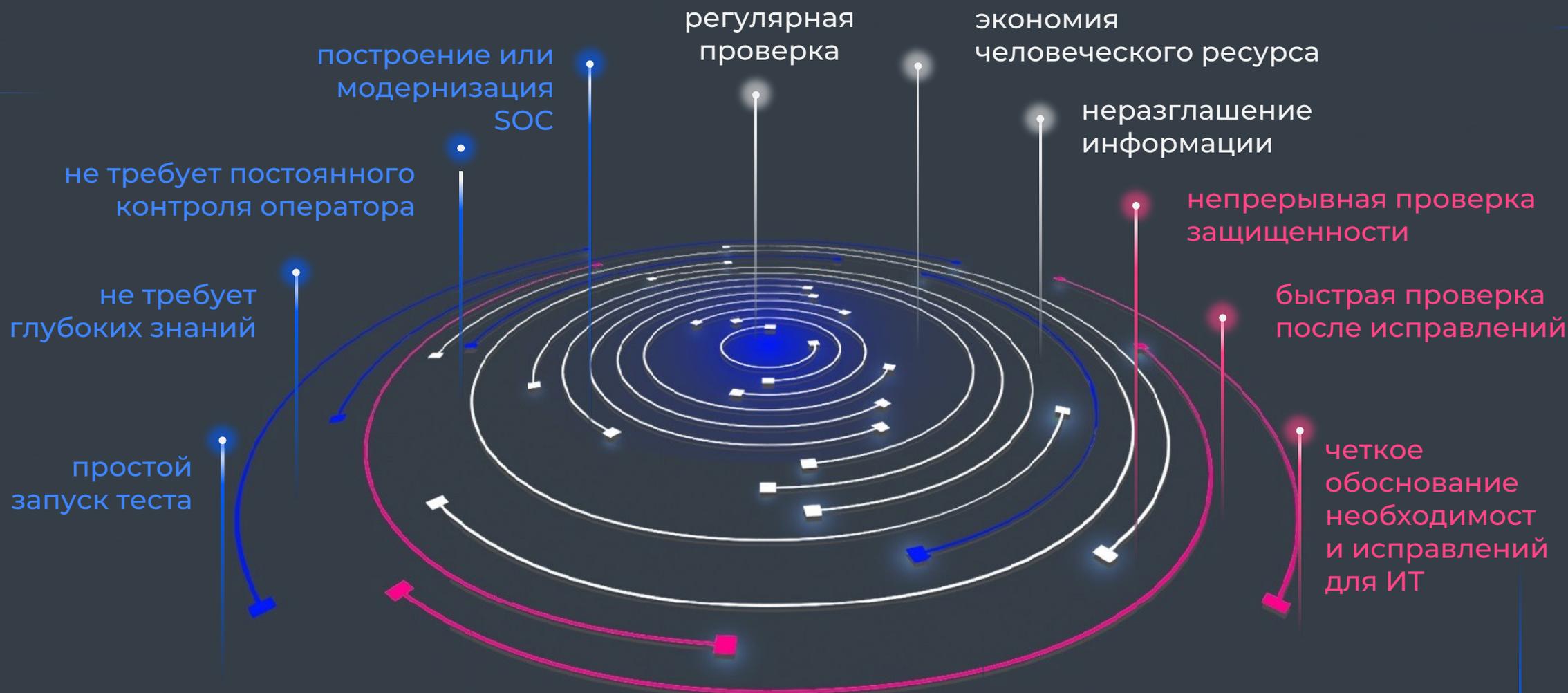
- <https://support.microsoft.com/ru-ru/topic/kb5008380-обновления-проверки-подлинности-cve-2021-42287-9dafac11-e0d0-4cb8-959a-143bd0201041#~:text=Сводка потенциальным%20злоумышленникам%20олицетворять%20контроллеры%20дом ена.>
- <https://support.microsoft.com/ru-ru/topic/kb5008102-изменение-изменений-диспетчера-учетных-записей-безопасности-active-directory-cve-2021-42278-5975b463-4c95-45e1-831a-d120004e258e#~:text=Сводка записи%20sAMAccountName%20учетной%20записи%20компьютера.>

## ВЫПОЛНЕННЫЕ ТЕСТЫ ПОЗВОЛЯЮТ ПРОВЕРИТЬ:

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



# ПРЕИМУЩЕСТВА



## 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

# DEMO





СПАСИБО ЗА  
ВНИМАНИЕ

ООО «КОНТРОЛХАК»

+7 (495) 789 72 97

[info@ctrlhack.ru](mailto:info@ctrlhack.ru)

[www.ctrlhack.ru](http://www.ctrlhack.ru)

