



Непрерывный автоматический пентест инфраструктуры

Ожидания и реальность от автоматизации



Продукты:

- * Симуляция кибератак
- * Автоматизация наступательной безопасности

Ценность:

- * Повышение эффективности технических средств и процессов
- * Развитие компетенций выявления и предотвращения атак



BAS Felix

*Симуляция
кибератакующих техник*



APT Bezdna

Автоматический пентест



О чём доклад

*Автоматизация
внутренних
пентестов*



00

Вводная часть

01

Ожидания

02

Реальность

00



Вводная часть

Наступательная безопасность и анализ защищённости

Повышает в целом эффективность ландшафта ИБ в организации.

Тренирует способность выявлять и реагировать.

Фактическая оценка уровня защищенности.

* *Пентест*

Уязвимости и слабости инфраструктуры

* *RedTeam*

Моделирование реального атакующего

* *PurpleTeam*

Покрытие спектра атакующих техник блокированием, выявлением и реагированием



Преимущества ручного пентеста



01

Эффективность не зависит от разнообразия инфраструктур и конфигураций

02

Тщательный анализ захватываемых хостов

03

Доступны атаки требующие hands-on-keyboard и нестандартных решений

04

Поиск и применение новых инструментов в моменте

Слабые стороны ручного пентеста



01

Ограничено время и
трудозатраты

02

Затруднена валидация
устранения выявленных
угроз

03

Частичное покрытие
инфраструктуры

04

Затруднено
тиражирование и
воспроизведение

01



Ожидания

Что потенциально даст автоматизация?

* Прозрачность

- Тщательный перебор целей
- Управление собранными данными

* Воспроизводимость

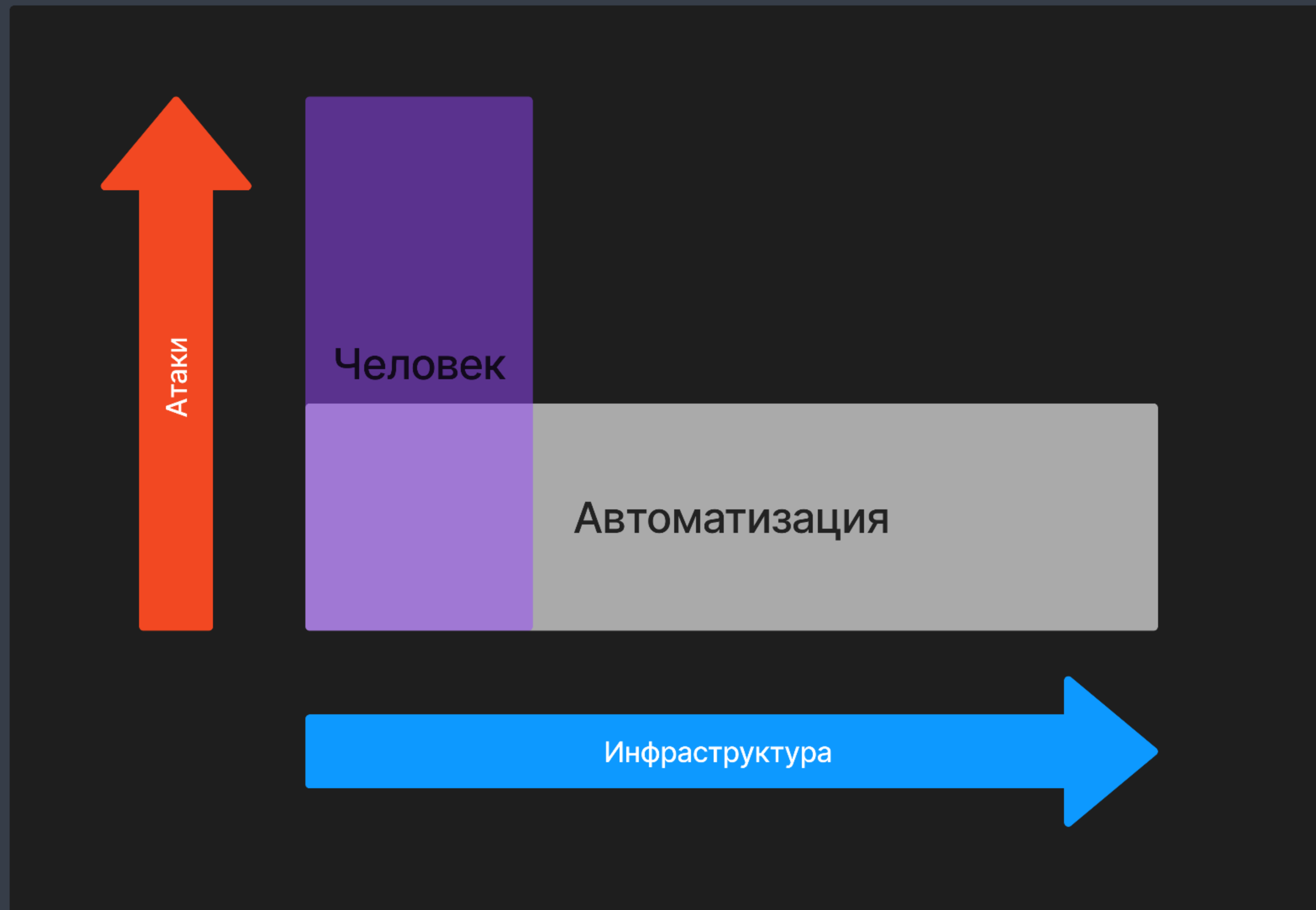
- Контролируемая валидация выявленных угроз
- Тиражирование атак

* Оптимизация

- Снижение трудозатрат
- Приоритезация целей



Целесообразность



Для кого?

* Нет своей команды

- Повышение зрелости
- Понимание угроз и мер противодействия

* Есть своя команда

- Рутинная – машине, творчество – человеку!
- Автоматизация специфических атак

* Для всех

- Повышение эффективности
- В любой момент фактическая оценка устойчивости к распространённым атакам



02 | Реальность

⌘ | ***APT***
Bez dna

Идея и реализация

ET-105806 Поиск уязвимости Printnightmare (CVE-2021-34527)	Компьютер с открытым smb 2023.11.28 16:06:28	Компьютер уязвимый к PrintNightmare 2023.11.28 16:06:31
	Имя домена pentest.type_name.fullname CONTOSO.LOCAL pentest.type_name.name CONTOSO ip адрес 192.168.0.177 Порт 445	Имя компьютера Имя домена pentest.type_name.fullname CONTOSO.LOCAL pentest.type_name.name CONTOSO ip адрес 192.168.0.177

Данные и сценарий

Данные определяют ход выполнения сценария

Спецификация атакующей функции:

- Входящие типы данных
- Исходящие типы данных

Выполнение сценария:

- Все данные обработаны
- Новых данных нет



Состав атак

Реализовано:

29 атакующих
функций

Подготовлено:

62 атакующих
функций



Среди них:

1. *Перебор хэшей*

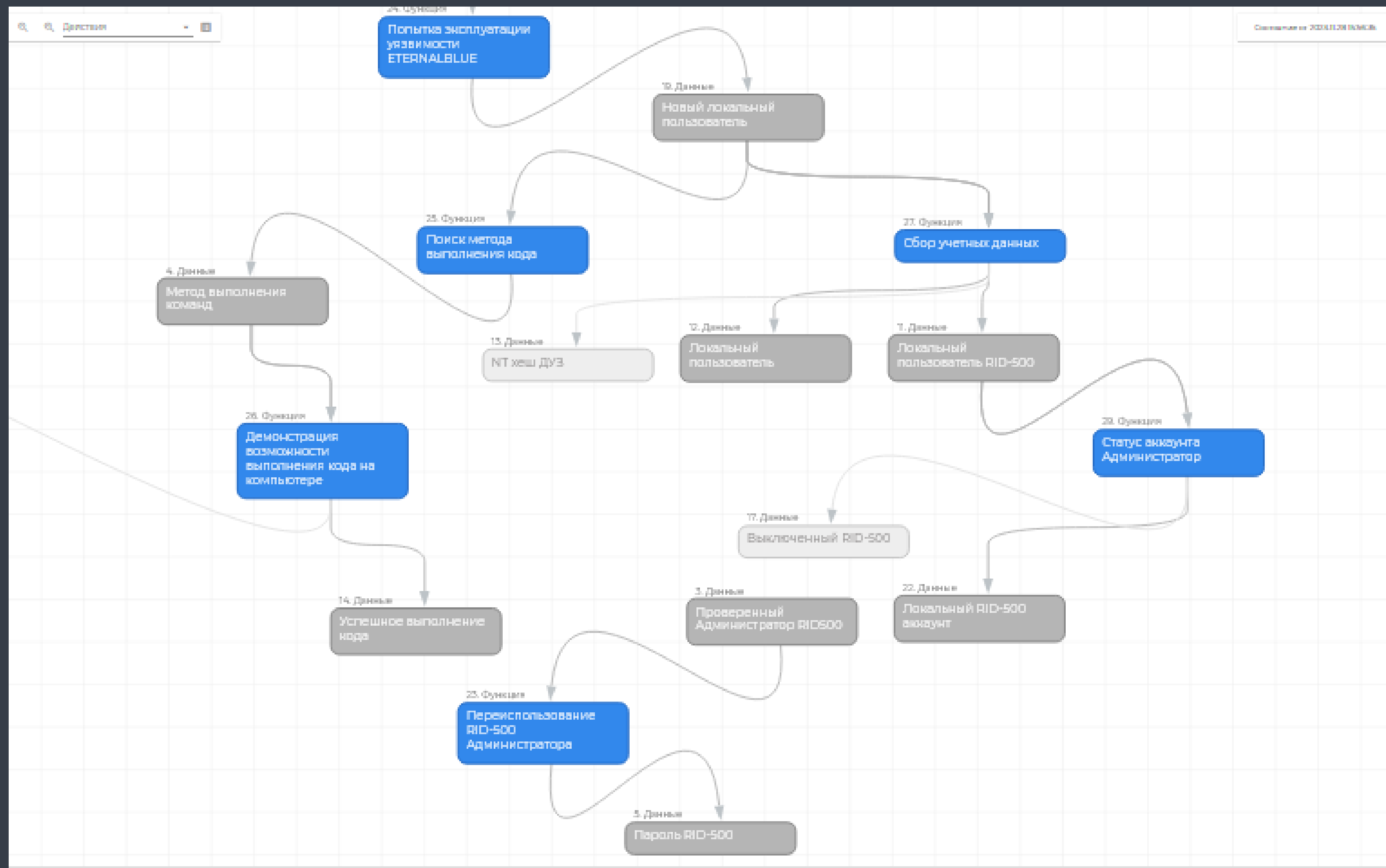
2. *PrintNightmare*

3. *NtlmRelay*

4. *PetitPotam*

5. *ASReproasting/Kerberoasting*

Пример



Заключение

01

«Красной кнопки» не существует

02

Базовые атаки и часто встречающиеся уязвимости/слабости

03

Не только эффективность, но и развитие осознанности и компетенций





Bezдна доступна для
пилотов, начиная с
2024.Q1

Записывайтесь!

ООО «КОНТРОЛХАК»

+7 (495) 789 72 97

info@ctrlhack.ru



СПАСИБО!

ВСЕГДА РАДЫ СОТРУДНИЧЕСТВУ