Получите от пентестов ещё больше ценности

Ожидания и реальность от автоматизации

CTRLHACK

Спикер

Сергей Куприн

генеральный директор

CtrlHack

Более 10 лет менеджер ИБ:

- Исследования
- Разработка
- Консалтинг

Когда-то давно:

- Дежурный сисадмин
- Автоматизация бизнес-процессов
- Сплоиты забавы ради

CtrlHack

Продукты:

* Симуляция кибератак
* Автоматизация наступательной безопасности

Ценность:

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

О чём доклад

Автоматизация 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

Внутренний пентест

Уклонение от обнаружения не требуется

Выявить уязвимости и слабости, подтвердить реализацией атак

Обычно достаточно одного значимого «пробива»

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

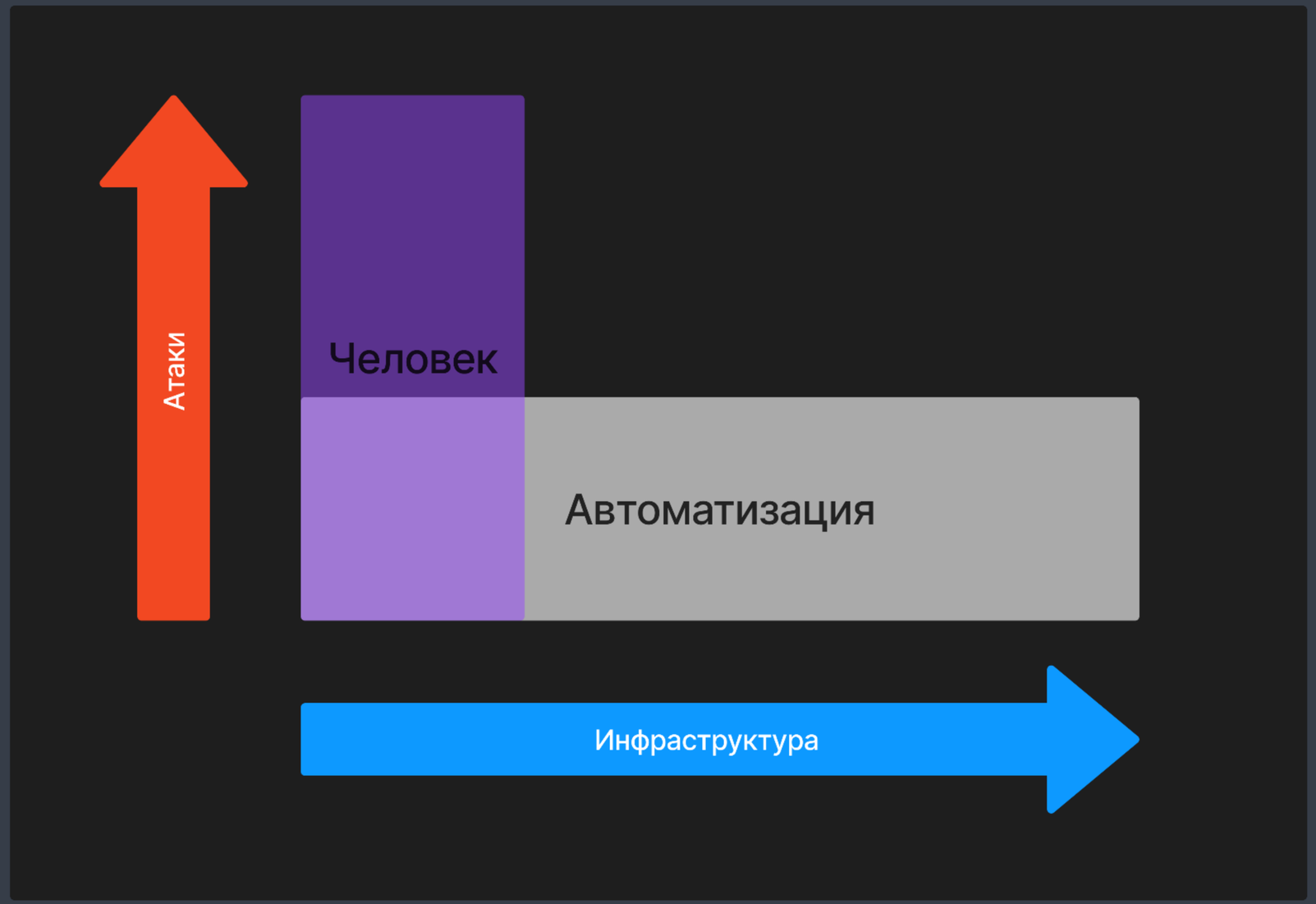
04 Затруднено тиражирование и воспроизведение

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

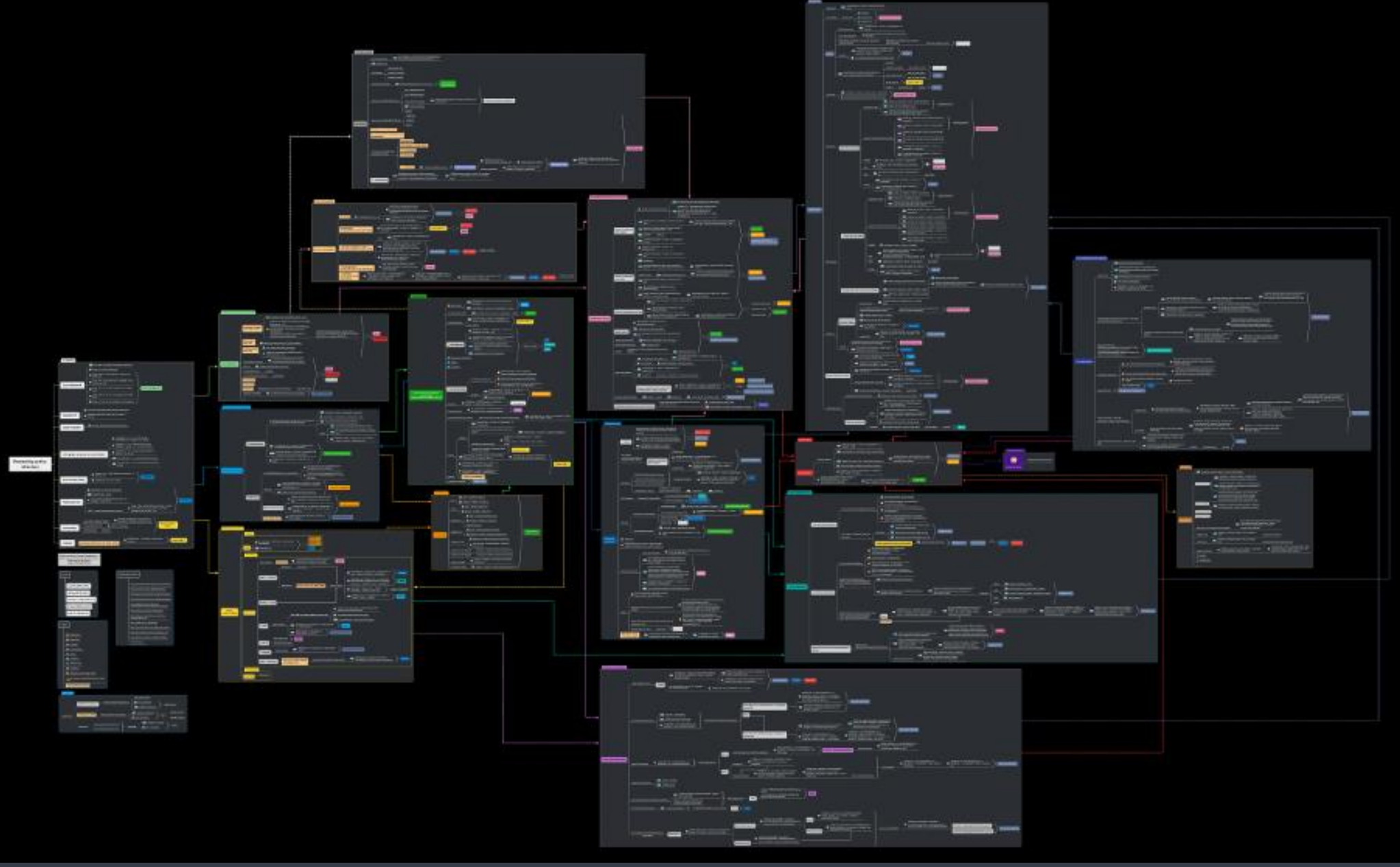


Для кого?

* *Нет своей команды*
  - Повышение зрелости
  - Понимание угроз и мер противодействия
* *Есть своя команда*
  - Рутина – машине, творчество – человеку!
  - Автоматизация специфических атак
* *Для всех*
  - Повышение эффективности
  - В любой момент фактическая оценка устойчивости к распространённым атакам

Популярные атаки 2022-2023

1. *AD CS ESC*
2. *PrintNightmare*
3. *WebDav + NtlmRelay*
4. *Слабые пароли*
5. *Ошибки конфигурации ACL*



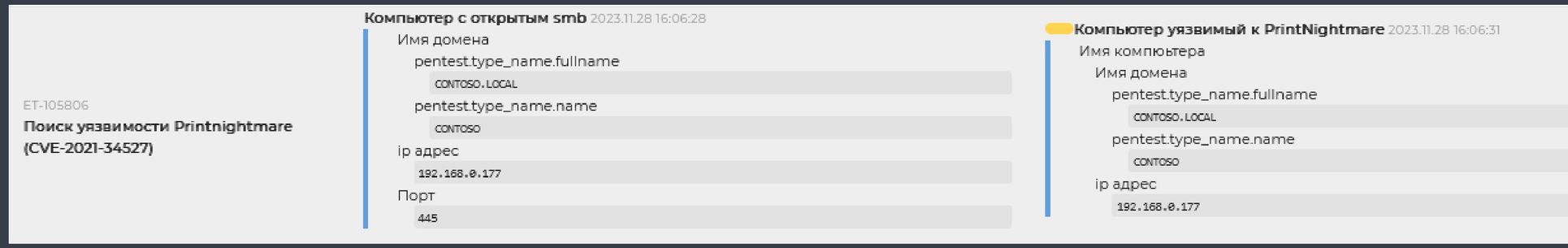
https://orange-cyberdefense.github.io/ocd-mindmaps/

02 | Реальность

Elite RedTeam Operator

КонтролХак пытается в автопентест

Идея и реализация



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

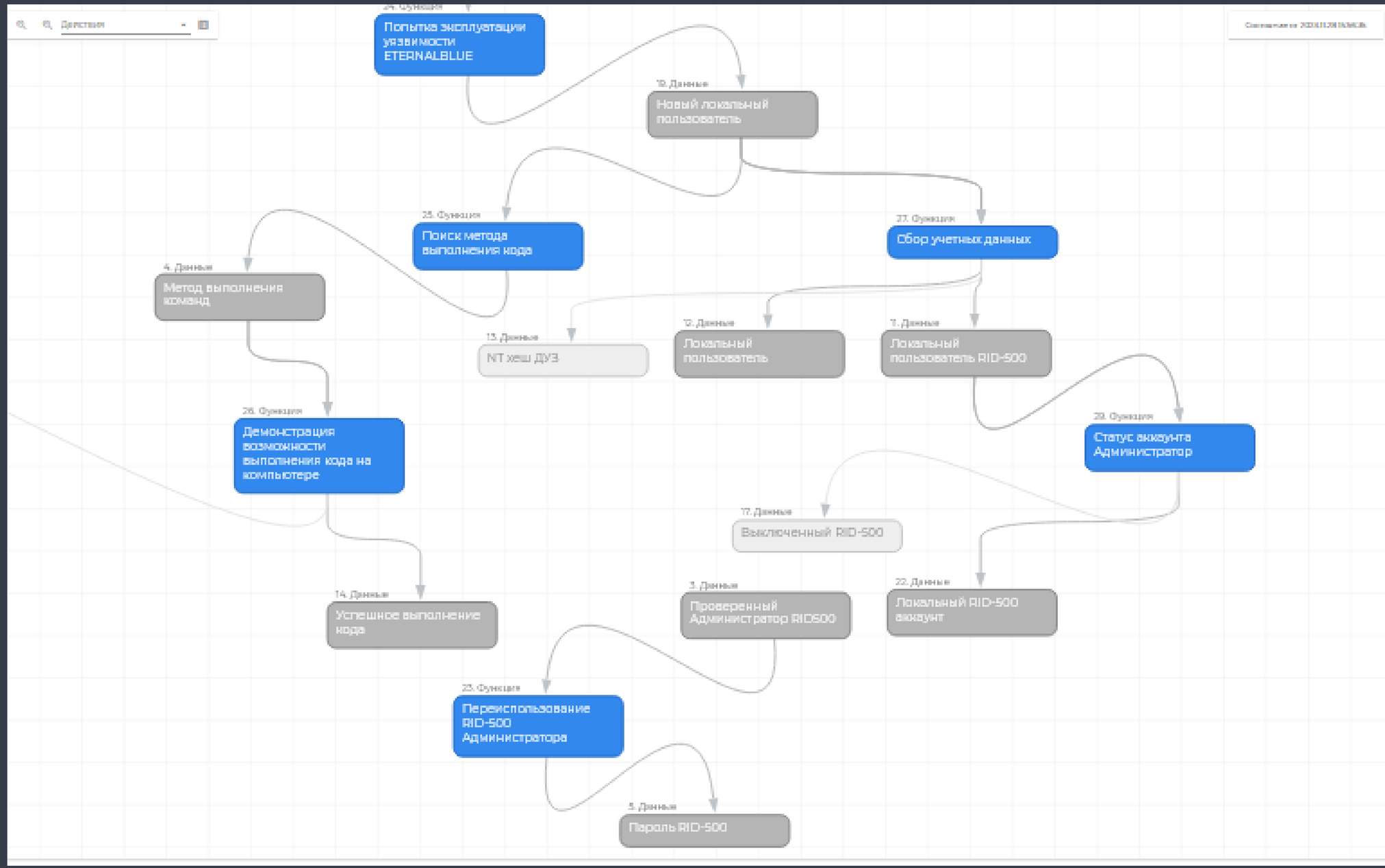
Реализовано:
29 атакующих функций

Подготовлено:
62 атакующих функций

Среди них:

1. *Перебор хэшей*
2. *PrintNightmare*
3. *NtlmRelay*
4. *PetitPotam*
5. *ASReproasting/Kerberoasting*

Пример


Действия
24. Функция
Попытка эксплуатации уязвимости ETERNALBLUE
19. Данные
Новый локальный пользователь
25. Функция
Поиск метода выполнения кода
27. Функция
Сбор учетных данных
4. Данные
Метод выполнения команд
13. Данные
NT хеш ДУЗ
12. Данные
Локальный пользователь
1. Данные
Локальный пользователь RID-500
28. Функция
Демонстрация возможности выполнения кода на компьютере
29. Функция
Статус аккаунта Администратор
17. Данные
Выключенный RID-500
14. Данные
Успешное выполнение кода
3. Данные
Проверенный Администратор RID500
22. Данные
Локальный RID-500 аккаунт
23. Функция
Переиспользование RID-500 Администратора
5. Данные
Пароль RID-500

Заключение

01 «Красной кнопки» не существует

02 Базовые атаки и часто встречающиеся уязвимости/слабости

03 Не только эффективность, но и развитие осознанности и компетенций

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

СПАСИБО!

ВСЕГДА РАДЫ СОТРУДНИЧЕСТВУ