# MaxPatrol Carbon

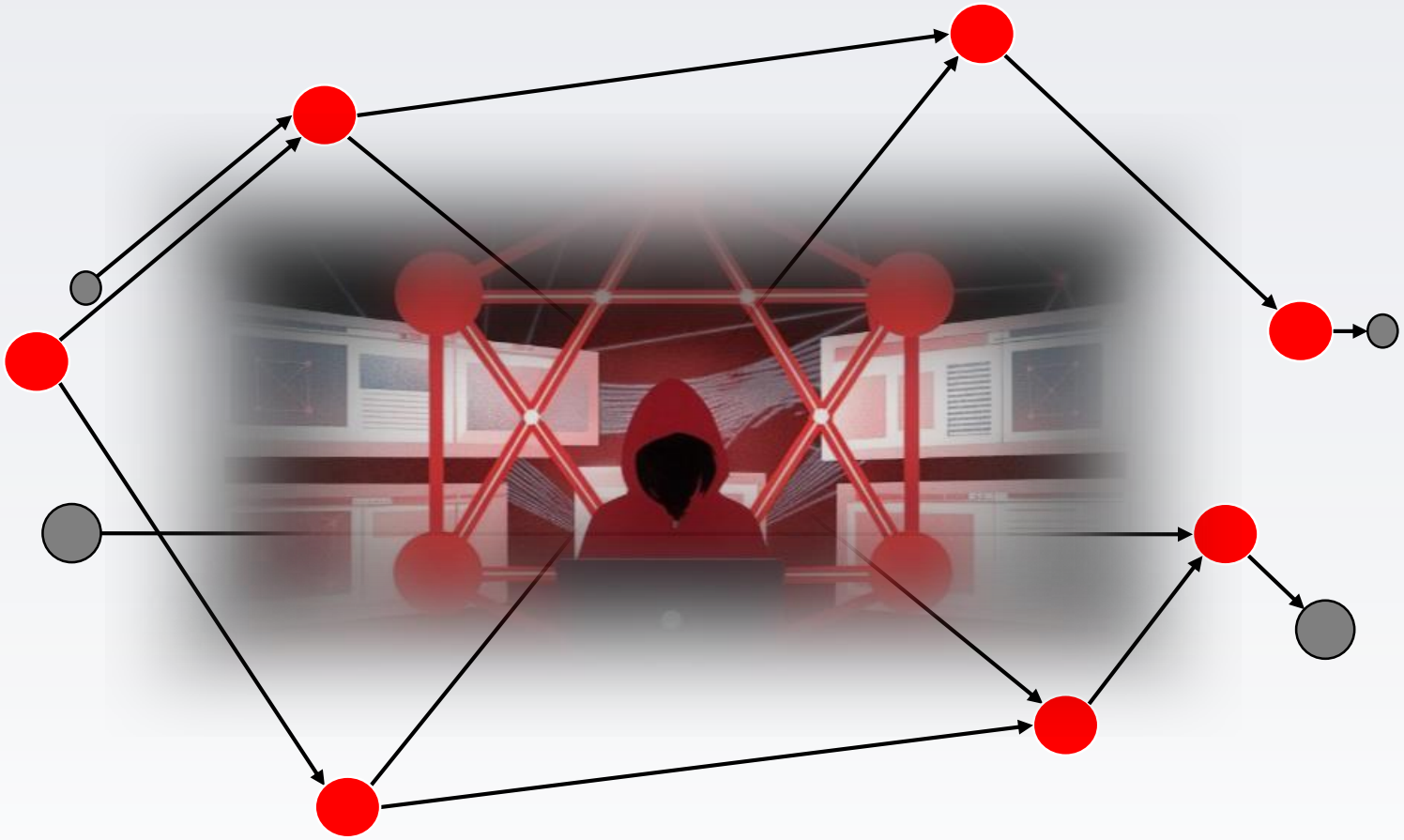
## Разработка в ИБ: как предсказывать атаки злоумышленника?

# whoami

## Дмитрий Елисеев

- Бэкэнд-разработчик MaxPatrol Carbon Positive Technologies
- Победитель олимпиады по программированию алгоритмических задач Positive Hack Days 2025
- Призер полуфиналов чемпионата мира по программированию ICPC 2024, 2025
- Участник многих всероссийских и международных сборов

# Современные киберугрозы



- Проблемы традиционных методов защиты
- Построение графа атак (TME)
- Формальное описание задачи поиска маршрутов
- Алгоритмы расчета маршрутов
- Выводы и подведение итогов

# Проблема привычных методов защиты

## Отсутствие полной карты инфраструктуры

- В сетях есть неучтенные активы, организация о них не знает.
- Первый доступ возможен через забытый сервис с открытым уязвимым портом.

Что нужно: карта всех цифровых активов, связей, доступов и критичных данных (не просто список серверов).

## Проблема недостаточности пентестов

- Результаты устаревают; между тестами защищенность не контролируется.
- 21% организаций тестируются раз в год; пентест — лишь один из тысяч маршрутов.

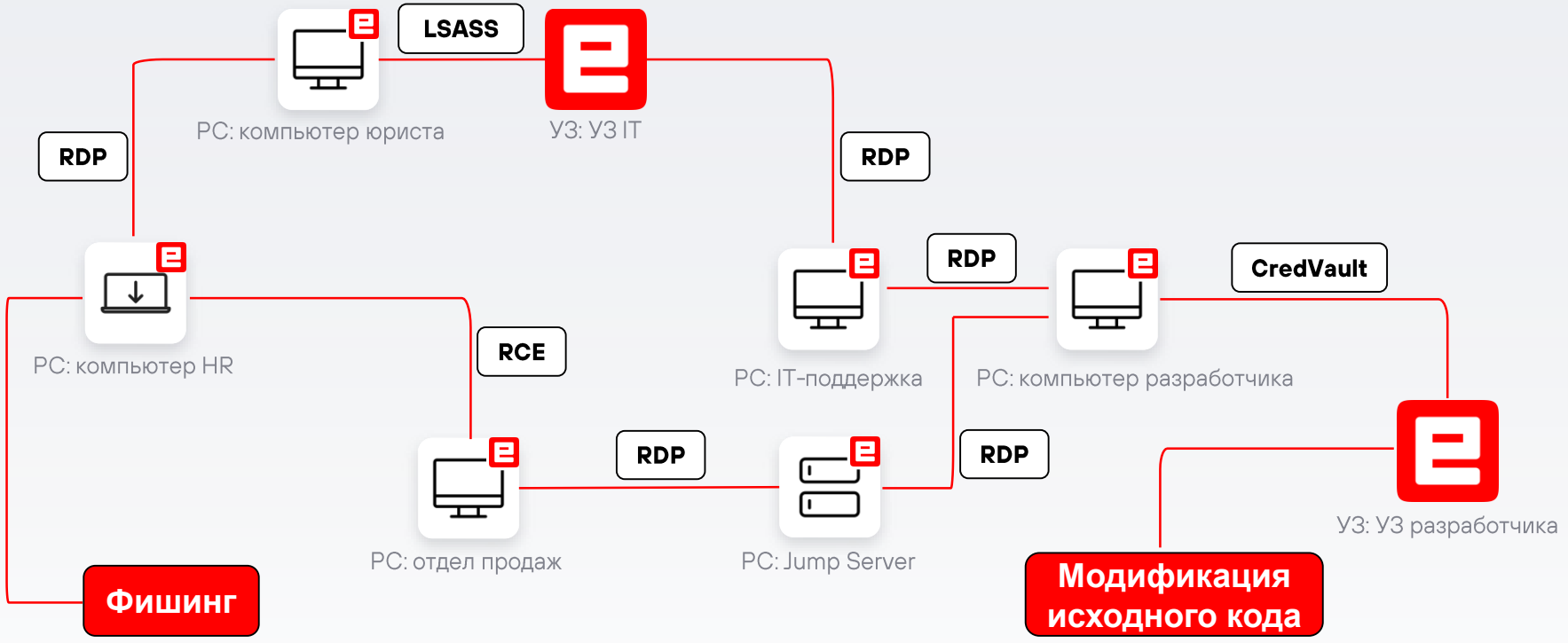
Что нужно: моделировать действия хакера и непрерывно контролировать актуальное состояние защищенности.

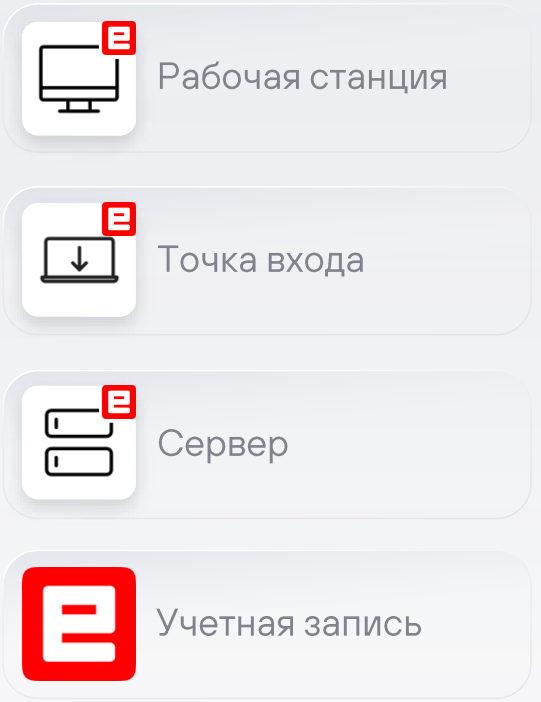
## Непонятно, какие уязвимости критичны

- Уязвимости в ОС, конфигурациях, паролях и правах не равны по опасности.
- Часть проблем организация не готова устранять.

Что нужно: определить, какие слабые места быстрее всего ведут атакующего к цели.

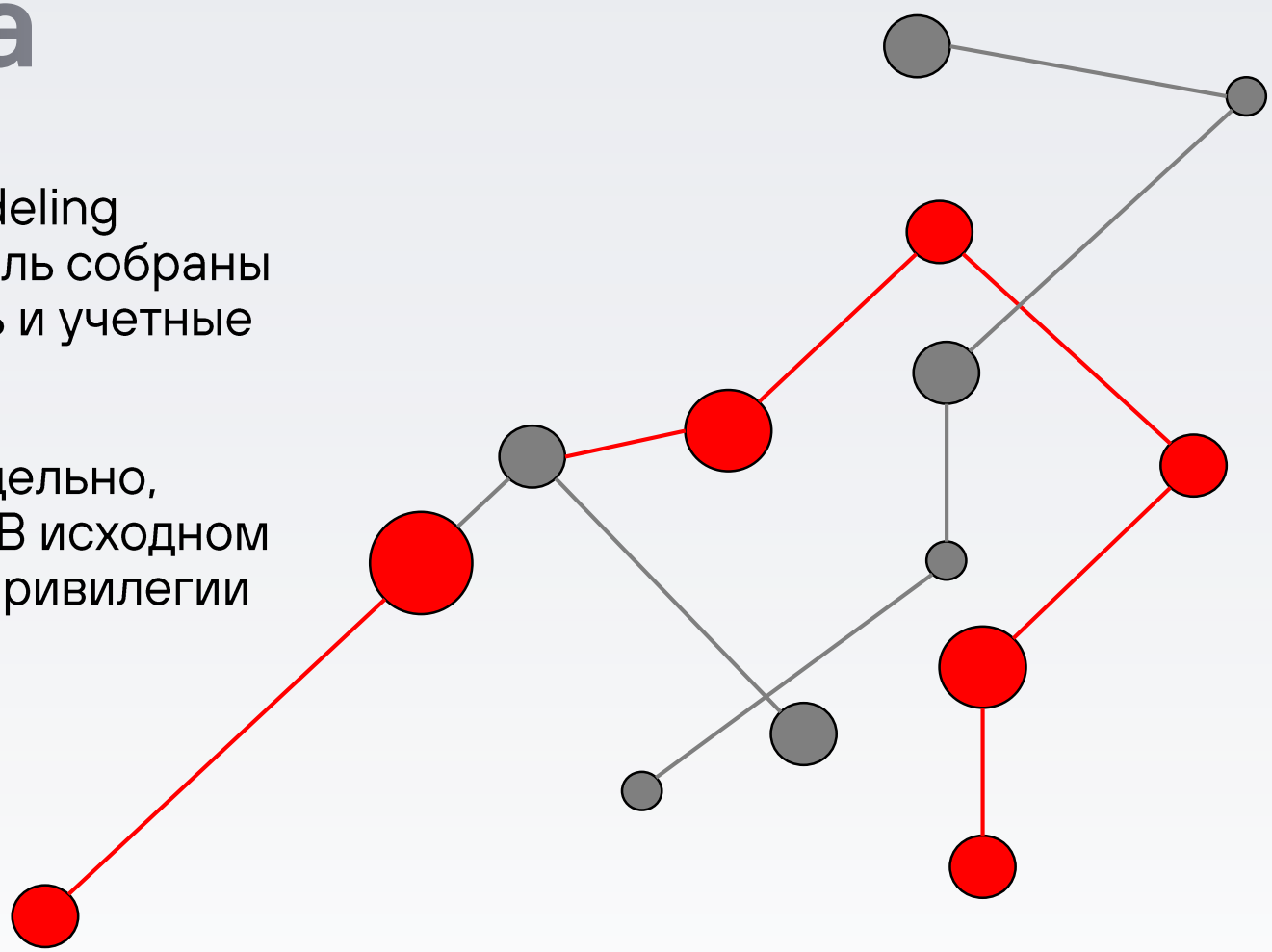
# Поиск потенциальных маршрутов атак



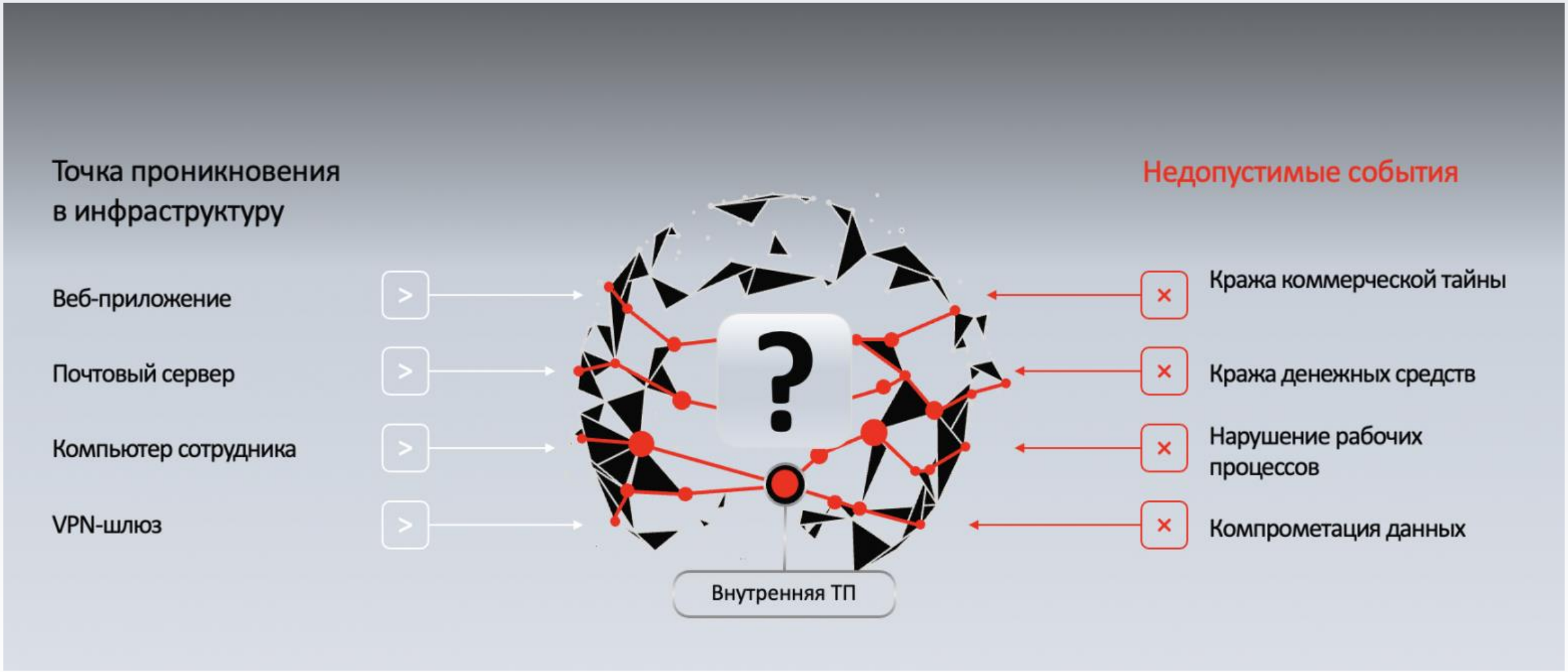



# Процесс создания модели и расчет графа

- Попытка № 1 — Threat Modeling Engine (TME). В одну модель собраны активы, сетевая связность и учетные записи.
- Попытка № 2 — активы отдельно, учетные записи отдельно В исходном графе учитываем только привилегии УЗ, а не все записи сразу.



# Работа графа маршрута атак



# Формальное описание задачи

## Граф атак G = (V, E)

- V — компоненты сети: хосты, учетные записи.
- E — механики атаки: кража учеток.
- $w(e) \in \mathbb{N}$ — вес ребра e, время выполнения механики (TTA), мин.

## Входные данные

- $T \subset V$ — точки входа, уже контролируемые атакующим.
- $R \subset V$ — целевые компоненты, которые нужно захватить.
- P(e, C) — функция привилегий для механики e, где $C \subseteq V$ – это множество уже захваченных учеток.

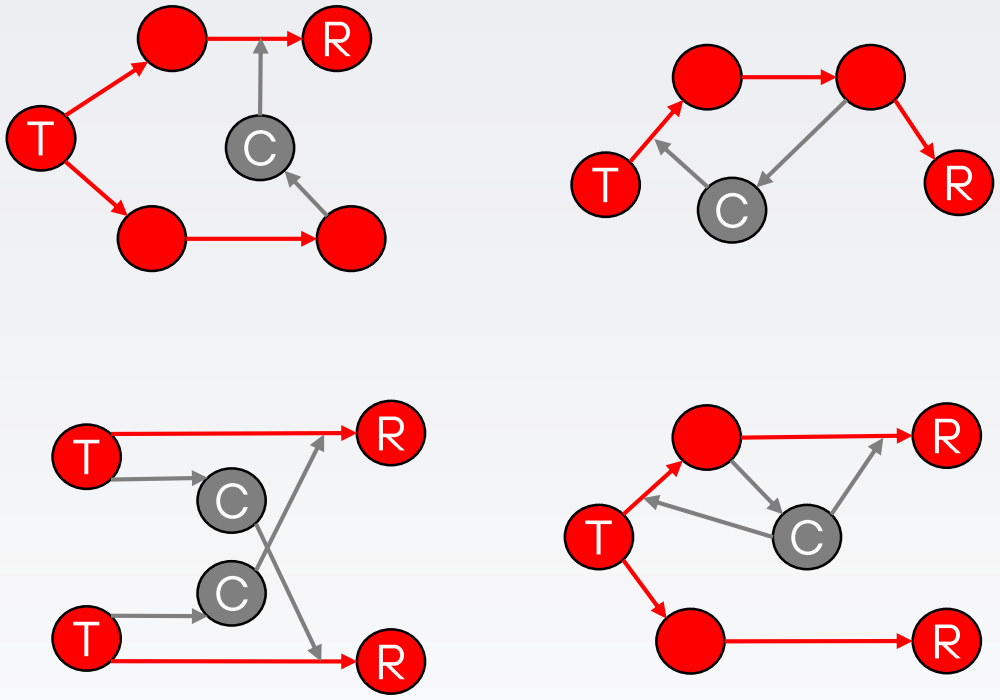
P(e, C) → True | need | False <=> механика выполнима | не хватает УЗ | недоступна.

## Требуется найти

10^6 упорядоченных последовательностей механик $\pi = (e_1, e_2, ..., e_k = R_q)$ таких, что для каждого i механика $e_i$ выполнима с помощью учеток, захваченных на шагах 1 ... i-1, и точек входа T.

Среди всех возможных таких последовательностей нужно выбрать те, у которых время $Time(\pi) = \Sigma\, w(e_i)$ минимально.

# Расчет маршрутов и алгоритм Дейкстры



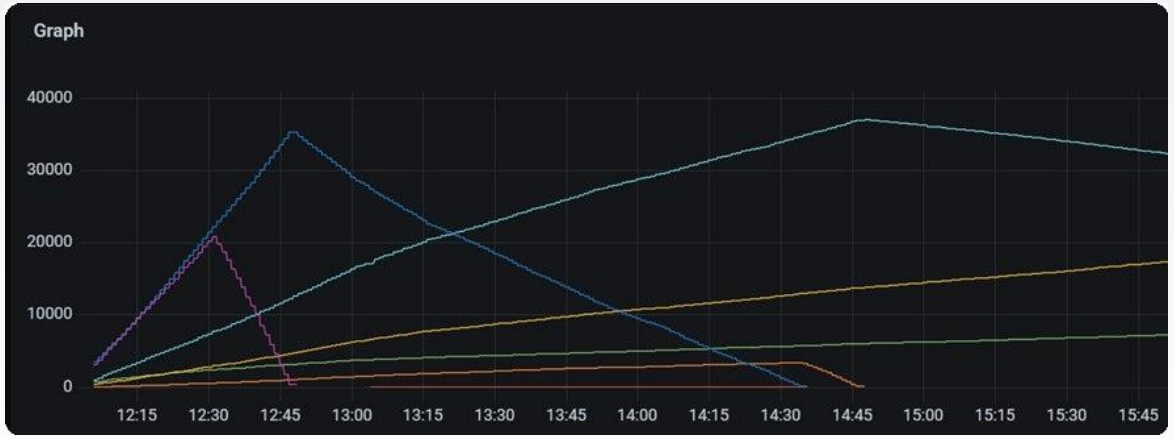

## Предрасчет

- Из всех точек входа запускается алгоритм Дейкстры по графу TME и для каждой достижимой вершины хранится кратчайший путь без учета ограничений.

## Перебор

- Каждая точка входа × каждый риск.
- Из предпосчета берется кратчайший путь до цели. Шаги выполняются по порядку и на каждом проверяются права. Если не хватает cred — вставляется кратчайший путь до нужной учетки, а затем алгоритм рекурсивно продолжается.

# Аналитика


## Анализ данных в Carbon.Routes

Данные о маршрутах атак: от гипотез и SQL запросов до выводов и новых идей

- Проверка гипотез
- Работа с БД и SQL
- Инструменты визуализации
- Анализ графиков и диаграмм
- Теория вероятностей, математика и статистика

# Результаты первых внедрений MaxPatrol Carbon

**1–5%**

критичных недостатков от всей площади атаки

**≤ 4 шага**

наиболее опасные маршруты атак

**~3 ч**

минимальное TTA на проектах

- Единый граф возможностей хакера дает контекст для прогноза маршрутов до критичных систем.
- Основные угрозы сосредоточены на узловых активах: DC, jump-серверы, рабочие станции администраторов.
- Закрытие 1–2 ключевых активов нейтрализует большинство опасных маршрутов.
- Приоритизация по маршрутам эффективнее точечного устранения всех уязвимостей.

# QR-коды

Важность поиска потенциальных маршрутов атак

https://habr.com/ru/companies/pt/articles/909166/

Алгоритмы поиска маршрутов атак

https://habr.com/ru/companies/pt/articles/913386/

Рассчитываем время кибератаки

https://habr.com/ru/companies/pt/articles/921872/

MaxPatrol Carbon

https://ptsecurity.com/products/carbon/