PHDays 2025

Дмитрий Резов

Младший исследователь

udv|group

Интересные темы, озвученные на конференции

Детектирование атак

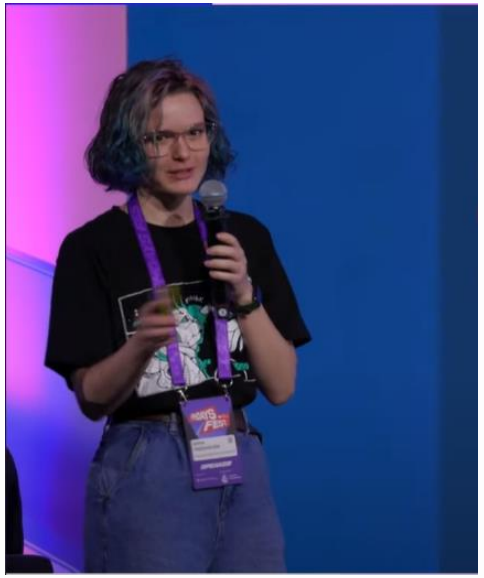
Детектирование атак, отделение конкретных типов атак от обшей массы инцидентов.

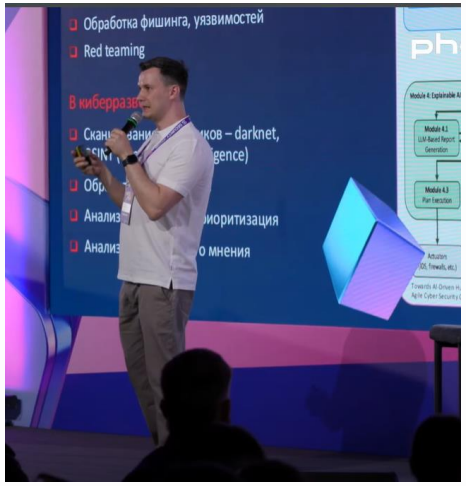
Поиск схожих цепочек хакерской активности

Исходя из данных по атаке выделяется инцидент из размеченных данных инцидентов, которые произошли раньше. Маркеры – техники, тактики и схожие хосты.

Очень много агентов

Использование LLM агентов для SOC, для анализа логов, для OSINT. И для много чего еще...

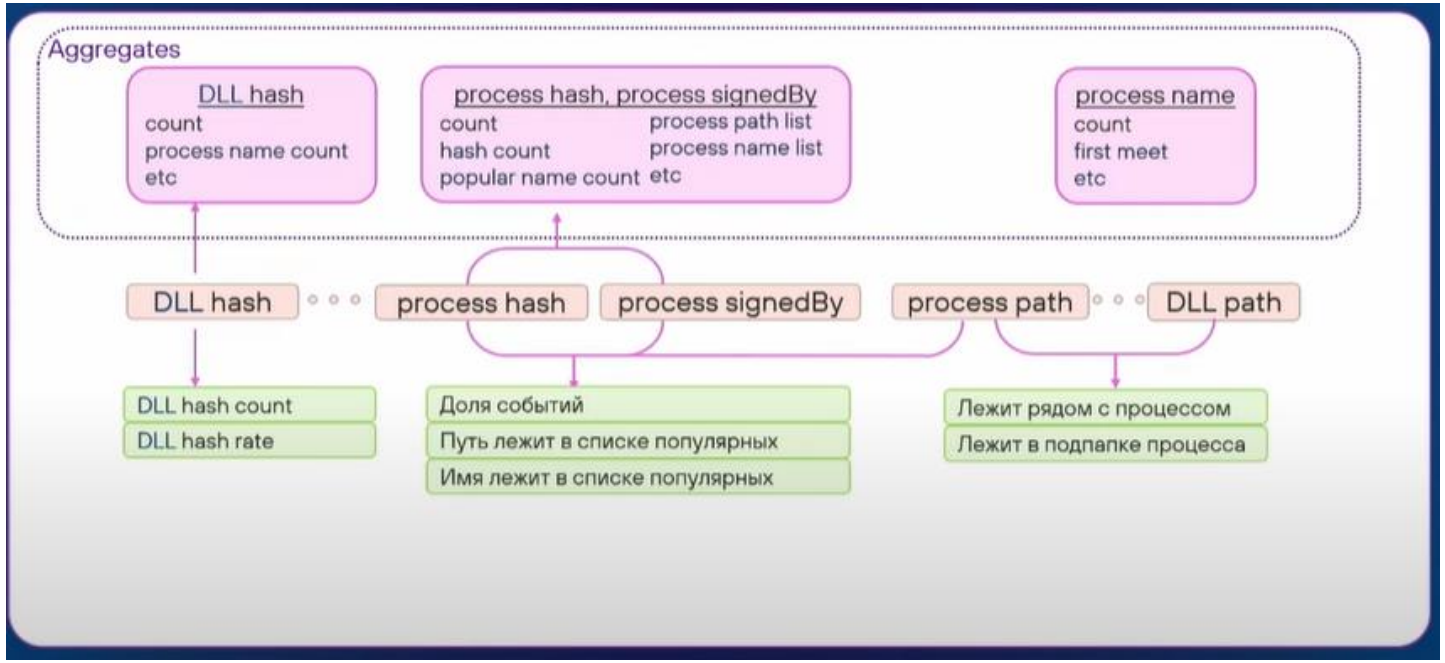




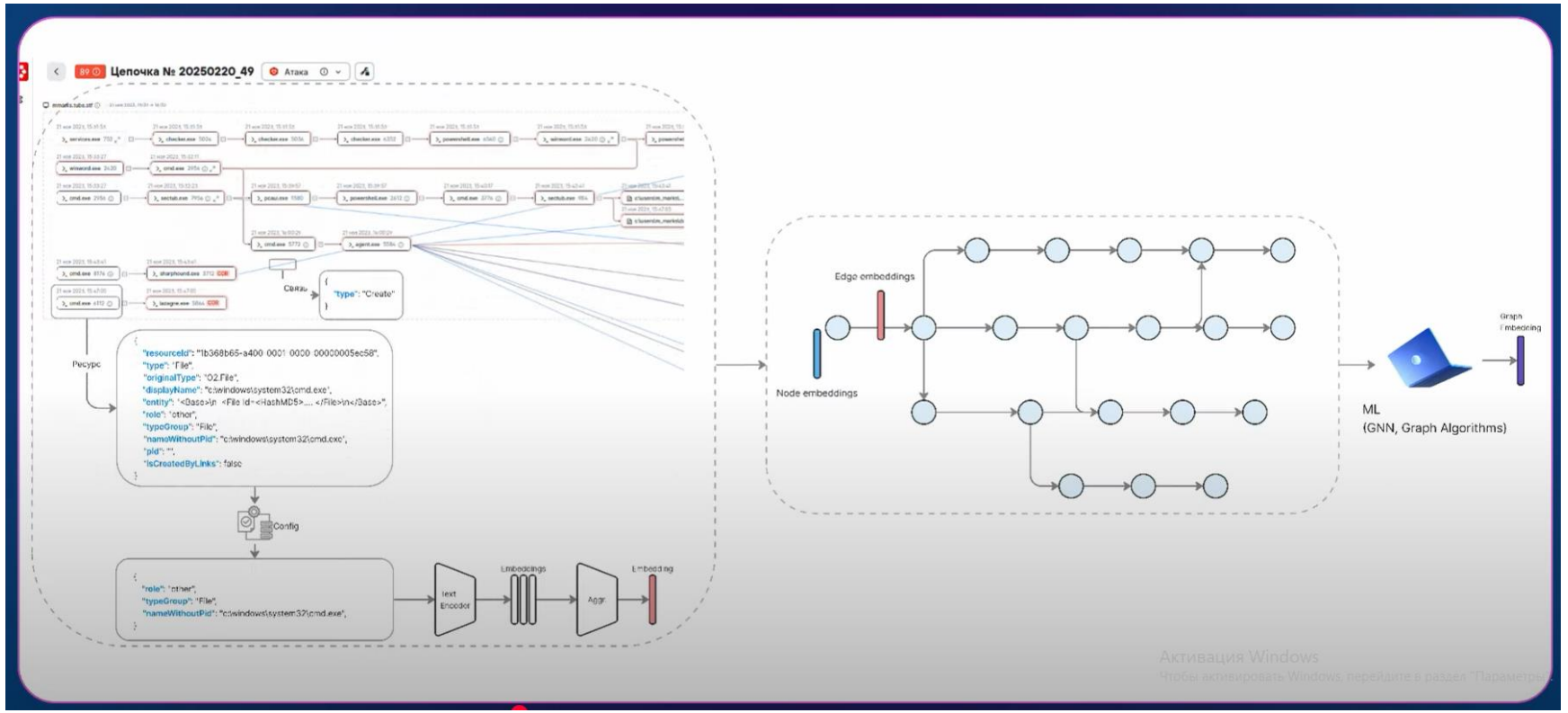
Детектирование конкретных типов атак

Детектирование атаки hijacking из всех получаемых данных

- Рассказывает про бустинг в рамках решения задачи
- Различные улучшения, например добавочные данные в виде фичей, описывающих структуру библиотек

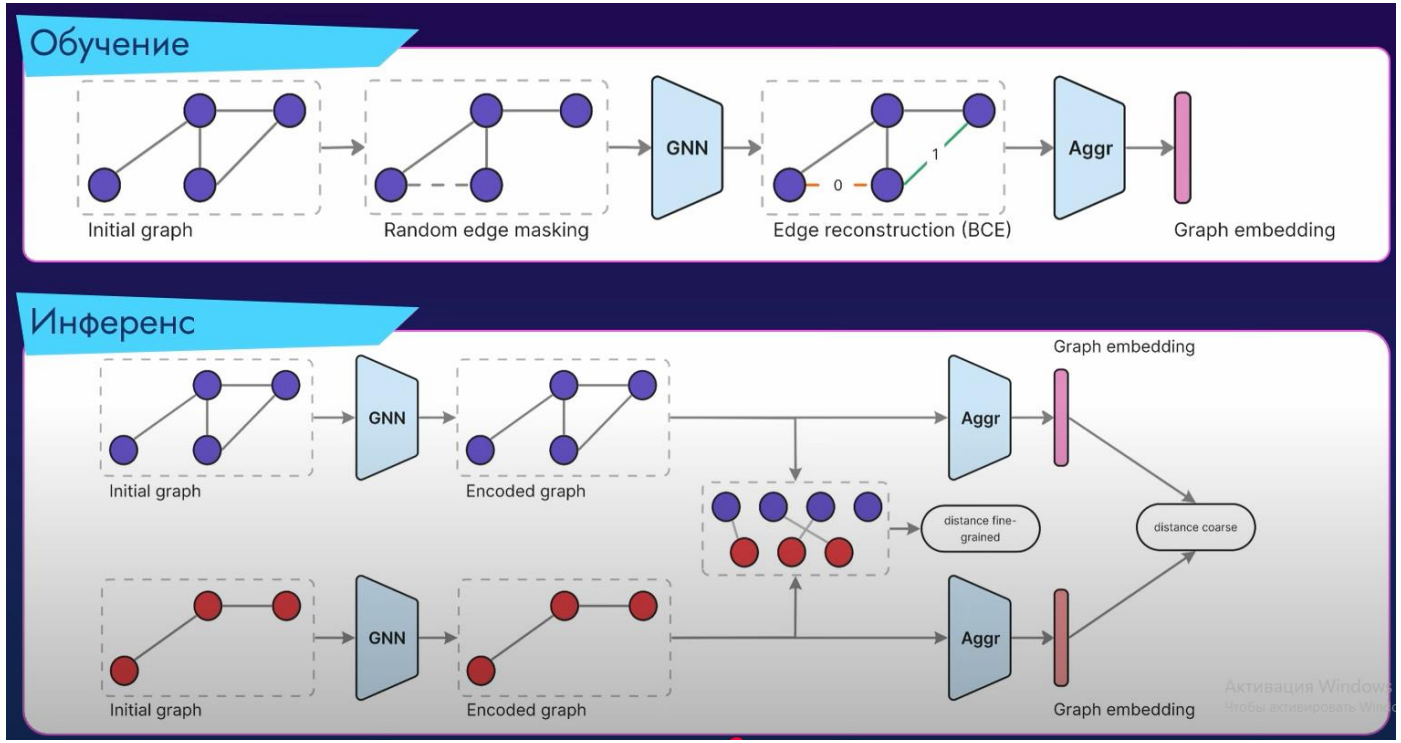


Поиск схожих цепочек хакерской активности



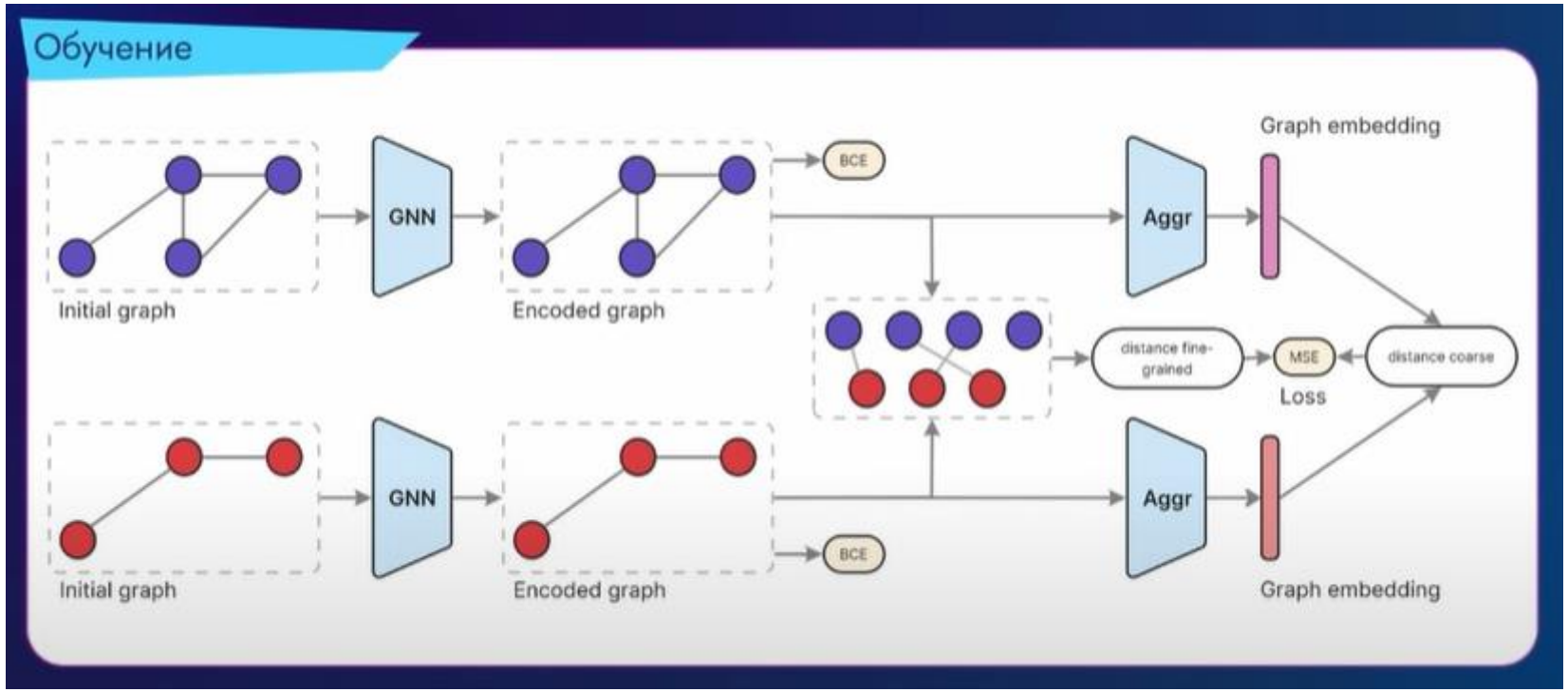
- Создание графа атаки, вершины это ресурсы (файлы, сервисы и т.д.), ограниченный список ребер.
- Кодирование текстовых вершин и их полей
- Создание графа эмбеддингов

Поиск схожих цепочек хакерской активности



- Сопоставление вершин графа известных атак и вершин графа развивающейся атаки
- Расчет близости векторов эмбеддингов графов

Поиск схожих цепочек хакерской активности



Пайплайн инференса используется для обучения, чтобы уменьшить вычислительные затраты на сопоставление вершин графов и сохранить качество поиска

Поиск схожих цепочек хакерской активности

	Mode	Aux. loss	Distance	Precision@1	Precision@3	RR	Recall@1	Recall@3
Masked-GNN	coarse	no	cos	84.0	79.6	86.9	80.1	81.2
Masked-GNN	coarse	yes	cos	***89.6***	***83.2***	***90.9***	**85.0**	**83.5**
Masked-GNN	fine-grained	no	cos	97.2	90.3	97.5	96.7	93.3
Masked-GNN	fine-grained	yes	cos	96.2	**92.1**	97.0	94.3	94.1
Masked-GNN	fine-grained	yes	chord	**98.1**	92.0	**98.1**	**97.0**	**94.2**

На таблице:

1. Mode:
   1.1. coarse – сравнение эммбеддингов графов
   1.2. fine-grained – пайплайн с сопоставлением вершин графа
2. Aux. loss – маркер обучения через пайплайн инференса

LLM Агенты...

О чем все доклады:
- Когда стоит применять агенты?
- База про агенты, фреймворки
- Немного про архитектуру

Доклады по теме:
- LLM и агенты, разгоняем SOC
- ИИ агенты в кибербезопасности

Интересные доклады (AI + ИБ)

- Поиск схожих цепочек хакерской активности - https://www.youtube.com/watch?v=oR4oBWVKWq4&ab_channel=PositiveEvents
- От данных к действиям ML в сердце DFIR - https://www.youtube.com/watch?v=CrAhkrxVJSI&ab_channel=PositiveEvents
- Разработка ML модели для детектирования DLL Side Loading - https://www.youtube.com/watch?v=xiaUIEI5r7g&ab_channel=PositiveEvents
- LLM и агенты, разгоняем SOC - https://www.youtube.com/watch?v=nfh-67pTOIw&ab_channel=PositiveEvents
- ИИ агенты в кибербразведке - https://www.youtube.com/watch?v=CnHhVn9_qjs&ab_channel=PositiveEvents

udv|group

Спасибо!

Контакты

commercial@udv.group
8-800-511-65-51

Адрес

620100, г. Екатеринбург,
ул. Сибирский тракт, 12,
строение 7, этаж 4

Сайт

udv.group