топологічні властивості даних та сприяння ефективній візуалізації та розумінню структури складних інформаційних наборів методу зменшення розмірності UMAP. Також зазначено, що нова технологія WebGPU, яка використовує графічний процесор для високопродуктивних обчислень, надає потужний інструментарій для аналізу великих даних у реальному часі, сприяючи розвитку нових програмних рішень та дослідженню в області медичних відкриттів. Визначено, що розробка методу зменшення розмірності UMAP на WebGPU дозволить пришвидшити та зробити обробку великих даних набагато більш ефективною.

Список використаних джерел

1. Umap-learn.readthedocs.io [Інтернет]. UMAP: Uniform Manifold Approximation and Projection for Dimension Reduction [цитовано 28 лют. 2024]. Доступно на https://umap-learn.readthedocs.io/en/latest/
2. Developer.mozilla.org [Інтернет]. WebGPU API [цитовано 28 лют. 2024]. Доступно на https://developer.mozilla.org/en-US/docs/Web/API/WebGPU_API

УДК 004.942+519.68

АНАЛІЗ НАБОРІВ ДАНИХ МЕРЕЖЕВОГО ТРАФІКУ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ АТАК

Мєшков В.І., аспірант, mieshkov.v.i@nmu.one, НТУ «Дніпровська політехніка»

Зростання мережевих атак є однією з головних проблем сучасної кібербезпеки (рис. 1) [1]. З кожним роком кіберзлочинці стають все більш винахідливими, використовуючи новітні технології та методики для проведення своїх атак. Вони постійно шукають слабкі місця в системах безпеки компаній та індивідуальних користувачів, що змушує останніх постійно оновлювати свої захисні механізми.

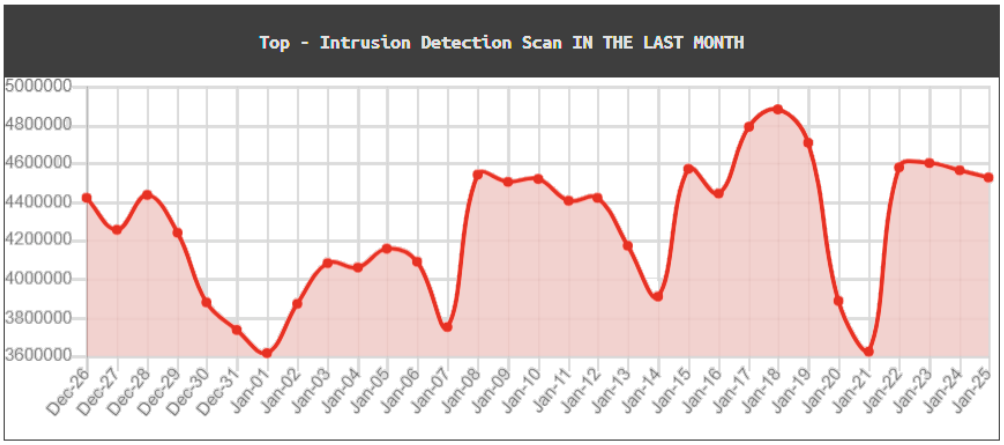

Рисунок 1 – Графік виявлених атак за період з 26.12.2023 по 25.12.2024

Найбільш розповсюджені атаки типу Brute force, DoS, Portscan, Intrusion. (рис. 2).

Top - Intrusion Detection Scan IN THE LAST MONTH		
1	Bruteforce.Generic.Rdp.a	47.37%
2	Bruteforce.Generic.Rdp.d	15.09%
3	Intrusion.Win.MS17-010.o	13.89%
4	Scan.Generic.PortScan.TCP	7.44%
5	DoS.Generic.Flood.TCPSYN	6.35%
6	Scan.Generic.PortScan.UDP	6.25%
7	Intrusion.Win.MS17-010.p	2.22%
8	Bruteforce.Generic.Rdp.c	0.18%
9	Intrusion.Generic.CVE-2021-44228.a	0.14%
10	Intrusion.Win.MS17-010.e	0.13%

Рисунок 2 – Розповсюджені атаки

Одним з ефективних способів боротьби з кіберзагрозами є інтелектуальний аналіз мережевого трафіку. Цей метод включає в себе використання алгоритмів машинного навчання та штучного інтелекту для аналізу великих обсягів даних, що проходять через мережу. Інтелектуальний аналіз дозволяє ідентифікувати аномалії у мережевому трафіку, які можуть свідчити про спробу атаки або вже відбулася атаку.

Застосування інтелектуального аналізу мережевого трафіку надає компаніям важливі переваги в боротьбі з кіберзагрозами. Перш за все, це дозволяє значно автоматизувати процес виявлення атак, забезпечуючи миттєву реакцію на загрози завдяки швидкому аналізу великих обсягів даних. Ця особливість критично важлива у сучасному цифровому світі, де кожна затримка може призвести до серйозних втрат.

Далі, точність ідентифікації загроз значно підвищується через застосування алгоритмів машинного навчання, які навчаються на історичних даних про атаки, дозволяючи системі краще розпізнавати та класифікувати потенційні загрози в майбутньому. Така здатність до самовдосконалення є ключовою для забезпечення високого рівня захисту.

Ще одна важлива перевага полягає у можливості прогностичного аналізу. Системи на основі штучного інтелекту можуть не лише виявляти існуючі загрози, але й прогнозувати майбутні атаки, аналізуючи поточні тенденції та поведінку мережі. Це дозволяє бути на крок попереду кіберзлочинців, адаптуючи свої захисні стратегії заздалегідь.

Нарешті, використання інтелектуального аналізу допомагає знизити кількість помилкових спрацювань (тривог), які часто виникають у традиційних системах безпеки. Завдяки більш точному розпізнаванню загроз, компанії можуть зосередитися на реальних загрозах, знижуючи непотрібні витрати ресурсів та часу на відповідь на помилкові спрацьовування. Ця оптимізація

процесу реагування на загрози є важливим кроком у підвищенні ефективності заходів кібербезпеки.

Для розробки та вдосконалення систем інтелектуального аналізу мережевого трафіку, фахівцям потрібні реалістичні та різноманітні набори даних, які містять приклади реальних мережевих атак і нормального трафіку. Ці набори даних служать основою для тренування та тестування алгоритмів машинного навчання, дозволяючи ефективно виявляти та прогнозувати кіберзагрози. Серед найбільш відомих та широко використовуваних наборів даних для аналізу мережевої безпеки варто виділити:

– DARPA – один з перших наборів даних, розроблений Оборонним агентством передових дослідницьких проєктів США, який містить симульовані мережеві атаки та використовується для розвитку систем виявлення атак.

– KDD Cup 99 – цей набір даних був представлений на конкурсі KDD Cup 1999 року і став класикою у сфері досліджень з виявлення атак завдяки своїй різноманітності атак.

– NSL-KDD – є удосконаленою версія KDD Cup 99, створена для вирішення деяких недоліків оригінального набору даних, зокрема, зменшення кількості записів для ефективнішого тренування моделей.

– DEFCON – набори даних з змагань DEFCON, які містять реальні сценарії мережевих атак, підходять для тестування систем безпеки.

– CAIDA – набори даних від Центру прикладних досліджень в області інтернету (CAIDA) включають детальні дані про мережевий трафік, які можуть бути використані для аналізу безпеки.

– LBNL/ICSI – набір даних, створений співробітництвом Лабораторії Берклі та Інституту комп'ютерних наук ICSI, містить зразки мережевого трафіку для аналізу.

– CDX – дані з Кіберзахисних вправ (Cyber Defense Exercise), організованих військовими академіями, включають реалістичні сценарії атак.

– Kyoto – набір даних з Університету Кіото, який включає реальний мережевий трафік та дані про атаки, зібрані протягом тривалого часу.

– Twente – дані з університету Твенте включають мережевий трафік, що містить зразки нормальної поведінки та атак.

– ISCX2012 – набір даних з Інституту кібербезпеки університету Нью-Брансвіку, який містить ретельно підготовлені сценарії атак та нормального трафіку.

– AFDA – набір даних для аналізу фреймів даних, що включає різноманітні типи мережевих атак.

– CIC-IDS2017, CSE-CIC-IDS2018 – сучасні набори даних, розроблені Канадським інститутом кібербезпеки, які містять широкий спектр сучасних мережевих атак.

У таблиці 1 [2] представляє перелік наборів даних, які широко використовуються в дослідженнях мережевого трафіку, разом із типами атак, що вони охоплюють. Кожен набір даних має свою унікальну колекцію мережевого

трафіку, яка включає як нормальні, так і зловмисні дії, що дозволяє розробникам систем безпеки випробувати та вдосконалити алгоритми виявлення та протидії кібератакам.

Таблиця 1 – Аналіз наборів даних

Набір даних	Тип атак	Розробник набору даних
DARPA	DoS, U2R, R2L, Probe	MIT Lincoln Laboratory
KDD Cup 99	DoS, U2R, R2L, Probe	University of California
NSL-KDD	DoS, U2R, R2L, Probe	University of California
DEFCON	Telnet Protocol Attacks	Shmoo Group
CAIDA	DDoS	Center of Applied Internet Data Analysis
LBNL	Malicious traces	Lawrence Berkeley National Laboratory
CDX	Buffer Overflow	United States Military Academy
Kyoto	Normal and Attack sessions	Kyoto University
Twente	Malicious traffic, Side-effect traffic, Unknown traffic, and Uncorrelated alerts	Twente University
ISCX2012	DoS, DDoS, Bruteforce, Infiltration	University of New Brunswick
AFDA	Zero-day attacks, Stealth attack, C100 Webshell attack	University of New South Wales
CIC-IDS2017	Brute force, Portscan, Botnet, DoS, DDoS, Web, Infiltration	Canadian Institue of Cyber Security
CSE-CIC-IDS2018	Brute force, Portscan, Botnet, DoS, DDoS, Web, Infiltration	Canadian Institue of Cyber Security

Найбільшу цікавість в подальшому досліджені набору даних є CIC-IDS2017 [3]. Це набір даних містить інформацію про мережевий трафік за 5 днів роботи мережі (з понеділка по п’ятницю) у форматі PCAP. Файли містять наступну інформацію: понеділок – нормальна активність в мережі (Benign) (обсяг даних – 11 Гб), вівторок – атаки (FTP-Patator, SSH-Patator) та нормальна активність в мережі (Benign) (обсяг даних – 11 Гб), середа – атаки (DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoS slowloris, Heartbleed Port) та нормальна активність в мережі (Benign) (обсяг даних – 13 Гб), четвер – атаки (Web Attack – Brute Force, Web Attack – Sql Injection, Web Attack – XSS, Infiltration) та нормальна активність в мережі (Benign) (обсяг даних – 7,8 Гб) та п’ятниця – атаки (Botnet, PortScan, DDoS) та нормальна активність в мережі (Benign) (обсяг даних – 8,3 Гб).

Висновок. Використання різноманітних наборів даних, таких як CIC-IDS2017, дозволяє фахівцям у сфері кібербезпеки аналізувати та розуміти широкий спектр кібератак і загроз, яким сьогодні піддаються мережеві системи.

Набір даних CIC-IDS2017, зокрема, забезпечує детальну базу для аналізу, оскільки він включає широкий спектр сучасних кібератак, таких як DDoS, DoS, веб-атаки, атаки на основі скриптів та багато інших. Цей набір даних не лише містить велику кількість мережевих взаємодій, але й деталізує різноманітні

параметри трафіку, які можуть бути використані для глибокого аналізу поведінки мережі та ідентифікації потенційних аномалій.

Важливість аналізу таких наборів даних полягає в можливості тренувати і випробувати алгоритми машинного навчання, що сприяє розробці більш ефективних та адаптивних систем виявлення атак.

Список використаних джерел

1. IDS. IDS - Intrusion Detection Scan [Електронний ресурс] / IDS // CYBERTHREAT REAL-TIME MAP. – 2024. – Режим доступу до ресурсу: https://cybermap.com/stats#country=27&type=OAS&period=w.
2. Thakkar, Ankit & Lohiya, Ritika. (2020). A Review of the Advancement in Intrusion Detection Datasets. Procedia Computer Science. 167. 636-645. 10.1016/j.procs.2020.03.330.
3. CIC. Intrusion detection evaluation dataset (CIC-IDS2017) [Електронний ресурс] / CIC // Canadian Institute for Cybersecurity. – 2017. – Режим доступу до ресурсу: https://www.unb.ca/cic/datasets/ids-2017.html

УДК 004.42

WEB-СЕРВІС ДЛЯ ОРАНІЗАЦІЇ СПІЛЬНИХ ПОЇЗДОК

Морщ Д.Г., студент, d.g.morshch@student.khai.edu, НАКУ «ХАІ»
Шевченко І.В., к. т. н., доцент, i.shevchenko@khai.edu, НАКУ «ХАІ»

Актуальність роботи. У сучасному світі зростає популярність спільних поїздок як зручного та ефективного засобу транспортного переміщення. Заощадження часу, ресурсів та зниження екологічного впливу стають важливими аспектами для багатьох людей.

Проєкт присвячений розробленню та впровадженню web-сервісу для організації спільних поїздок, що дозволить користувачам легко та ефективно планувати та здійснювати поїздки разом. Цей проєкт відповідає вимогам сучасного суспільства до інноваційних технологій у сфері транспортної логістики та сприятиме створенню більш сталих та зручних транспортних систем.

Розглянемо найпопулярніші аналоги для організації спільних поїздок, їх переваги та недоліки.

Uber – це американська технологічна компанія, яка надає послуги таксі та поїздок на замовлення через мобільний застосунок. Uber має широкий вибір послуг, поділ витрат при спільних поїздках, зручний та доступний інтерфейс. Використання цього сервісу у годину пік призводить до значної переплати, сервіс має проблеми безпеки та конфіденційності даних.

BlaBlaCar – це французька платформа для спільного використання