Application of Large Language Models for Event Analysis and Entity Recognition in Cybersecurity

Dmytro Lande[1], Elina Shnurko-Tabakova[2]

[1] National Technical University of Ukraine - Igor Sikorsky Kyiv Polytechnic Institute

[2] Index Systems ltd.

Abstract

This paper examines approaches to leveraging large language models (LLMs) for event analysis in cybersecurity, focusing on semantic indexing tasks during the creation of a database for the Attack Index system. It also covers the development of an analytical environment, as well as the creation of thematic summaries, digests, and semantic maps through interactions with LLMs.

Keywords: large language models (LLM), cybersecurity, Attack Index, semantic indexing, hacker groups, analytical reports, semantic maps.

Introduction

In the modern world, cybersecurity is a crucial component of national and corporate security. Given the large volume of data generated in real time, it is necessary to develop effective tools for quick and accurate analysis of such data. One such system is the Attack Index (https://attackindex.com), which was created to detect and analyze information attacks, as well as to predict information operations in cyberspace [1]. The system allows for assessing the level of information security, detecting anomalies in information flows, and monitoring the dynamics of thematic publications.

The use of large language models (LLMs) plays a significant role in enhancing the effectiveness of modern analytical systems [2]. LLMs enable the automation of complex tasks such as entity recognition, classification of emotional tones in publications, building semantic connections between various participants and events, and forecasting the development of situations.

Thanks to their ability to process and analyze natural language, LLMs allow the system to quickly adapt to new informational threats by detecting even the smallest changes in the information space. This enables operators of the Attack Index system to promptly identify anomalies that may indicate the beginning of an information attack and take appropriate measures to neutralize it.

1. Semantic Extraction: Detection and Recording of Entities in Big Data Analysis for Cybersecurity

An important application of large language models in the Attack Index system is semantic extraction of entities from large volumes of data [3]. Using specific prompts, it is possible to detect entities such as hacker groups, individuals, organizations, and other elements related to cyberattacks. A key aspect is the

model's ability to work with unstructured or semi-structured data, such as text messages on the Internet or social media, which allows for the detection of hidden threats [4].

Mathematical Formalization:

Let $D = \{d_1, d_2, ..., d_n\}$ be a set of documents containing cybersecurity data, where each document d_i is a text or a set of metadata. For each document d_i, we want to obtain a set of entities $E = \{e_1, e_2, ..., e_m\}$, where e_k is an entity, which could be a hacker group, person, organization, etc.

Prompt 1: "We need to find hacker groups and their members in the text. Identify all the groups involved in cybersecurity attacks and list them in a numbered list. Here is the document for analysis: …"

Prompt 2: "List all official organizations that appear in this text related to cyber threats or cybersecurity and display them in a numbered list. Here is the document for analysis: …"

Let's consider the document "Cyber Brief 24-11 - October 2024" (https://cert.europa.eu/ publications/threat-intelligence/cb24-11/) and apply the given prompts to it.

1. *LockBit Ransomware Group*
2. *APT29 (Russia-linked)*
3. *GoldenJackal*
4. *UAT-5647 (Russia-speaking group)*
5. *Kimsuky (North Korea-linked)*
6. *Andariel (North Korea-linked)*
7. *NoName (Pro-Russia Hacktivist Group)*

etc.

The results of processing prompt 1 are as follows:

1. *Europol*
2. *Irish Data Protection Commission*
3. *Moldova's Information and Security Service*
4. *Dutch Police*
5. *US Department of Justice*
6. *US Federal Bureau of Investigation (FBI)*
7. *CISA (Cybersecurity and Infrastructure Security Agency)*

etc.

2. Formation of Analytical Reports

Thanks to large language models, the Attack Index system is capable of generating automated analytical reports that include key points from the collected information. This allows for identifying key aspects of information operations, such as their

initiators, scale, and intensity. Prompts for identifying the main points of a document help highlight important text fragments and generate reports that are convenient for further analysis and decision-making.

Mathematical Formalization:

Let $T=\{t_1,t_2,\ldots,t_k\}$ be the set of points extracted from a document. Each point t_i is a part of the text that holds high importance for understanding the main information. Formally, each document d_i is transformed into a set of points:

$$T_i=\{t_1,t_2,\ldots,t_k | t_j \in T_i \text{ and point } t_j \text{ is contained in document } d_i\},$$

where T is the set of all possible points. Large language models (LLMs) are used to automatically extract these points, highlighting important fragments of text to construct the analytical report.

Prompts for identifying the main points of a document:

Prompt 3: "Summarize the key ideas of this document, highlighting the main points."

Prompt 4: "Create a brief report based on this text, pointing out the key points and arguments."

The results from processing Prompt 3 are as follows:

1. *Cyber Policy and Law Enforcement**:***
   - *Ireland fined LinkedIn €310 million for GDPR violations.*
   - *Moldova blocked Russian websites ahead of elections to curb influence.*
   - *Europol conducted a global operation against the LockBit ransomware group, leading to arrests and seizures of infrastructure.*
   - *Various nations (Turkey, Russia) blocked Discord for failing to comply with data-sharing requests amid criminal activity concerns.*
2. *Cyberespionage**:***
   - *Russian-linked APT29 conducted an extensive information-gathering campaign, while North Korea-linked actors targeted German defense contractors.*
   - *China-nexus hackers targeted phones of US political figures, while North Korea's Kimsuky group breached German companies.*
   - *GoldenJackal targeted high-security, air-gapped government networks, including an embassy in Belarus.*
3. *Cybercrime**:***
   - *North Korea's Andariel group collaborated with Play ransomware operators.*

- *European targets faced threats from the Strela Stealer malware, exploiting obfuscated JavaScript to capture sensitive data.*

Russia-linked groups targeted the UK's ambulance services and Ministry of Defence as part of hybrid warfare strategies…

The results of processing prompt 4 are as follows:

1. Cyber Policy and Law Enforcement in Europe:

- ***Ireland** imposed a fine of €310 million on **LinkedIn** for GDPR violations, specifically for insufficient user information on targeted advertising data usage.*
- ***Europol** conducted an operation against the **LockBit** group, arresting four individuals linked to the ransomware organization.*
- ***Moldova** blocked pro-Russian websites, including **Dzen**, **Rutube**, and **Yandex**, ahead of the presidential elections.*
- ***Japan** sentenced a criminal for using **AI** to develop ransomware software.*

2. Cyber Espionage:

- ***APT29**, linked to Russia, conducted a large-scale information gathering campaign, disguising malicious **RDP** files as trusted software.*
- *Hackers tied to **North Korea** compromised the German defense firm **Diehl Defence** through phishing attacks involving fake job offers.*
- *A cyberattack targeting the **Dutch Police** was likely carried out by a state-sponsored actor.*

3. Cybercrime:

*The most active ransomware groups in Europe were **LockBit3** and **Ransomhub**, targeting sectors such as technology, manufacturing, education, construction, and healthcare.*

3. Formation of Semantic Maps

Thanks to large language models, it is possible to create semantic maps that visualize the connections between various entities and events. These maps allow for a quick understanding of the structure of information attacks, identification of key points of influence, and participants. The Attack Index system integrates this process into its tools, using software to build semantic maps based on GraphViz [5]. Prompts for building such maps help identify patterns in the data and visualize them in a convenient form for analysts.

Mathematical Formalization:

A semantic map can be represented as a graph G = (V, E), where: V — the set of nodes representing entities (such as individuals, organizations, hacker groups, etc.),

E — the set of edges representing relationships between entities (e.g., shared attacks, connections via social media publications).

Each entity $v_i \in V$ has a weight determined by its importance in the context of an information operation. Edges $e_{ij} \in E$ have a weight that defines the intensity of the interaction between entities: w_{ij}= the number of common publications between v_i and v_j.

For constructing semantic maps, an LLM is used to find relationships between entities based on text and context.

Prompt for building semantic maps:

Prompt 5: "Provide a list of pairs of hacker group names that are connected through their operations and resources in cyberspace in the format 'group1; group2' from the provided text."

Based on the data generated by the system using the graph analysis and visualization tool CSV2Graph (https://bigsearch.space/uli.html), the corresponding graph is displayed (Figure 1).

Conclusions

This paper presents an innovative approach to analyzing information attacks using the Attack Index system, which leverages large language model (LLM) technologies for processing and interpreting large volumes of data. The use of LLMs allows for the automation of key stages in the analysis, including entity extraction, semantic map construction, and the generation of analytical reports, significantly improving the efficiency and accuracy of the system in detecting and responding to information threats.

By using LLMs, the system can automatically detect key entities such as hacker groups, individuals, organizations, and other critical elements of information attacks. This accelerates the data collection process and reduces the risk of human errors in manual analysis.

The system enables deep analysis of large information sets, identifying anomalies and information operations. With the help of LLMs, it is possible to accurately forecast the stages of information attack development, enabling prompt responses to changes in the situation.

The automated creation of analytical reports highlighting key points and entities based on text analysis allows for the development of user-friendly interfaces for cybersecurity professionals. The semantic maps created by LLMs help visualize the relationships between different participants in information attacks, greatly simplifying and enhancing the decision-making process.

LLMs allow for the identification and classification of interaction types between entities within an information operation, as well as the assessment of the intensity and scale of attacks. This aids in better understanding the attack structure and its potential consequences.

The novelty of the proposed approach lies in the integration of large language models to automate and enhance the processes of analyzing information attacks. Compared to traditional methods, the Attack Index system based on LLMs is capable of:

- increasing the speed of data analysis and processing, allowing for the rapid identification of new threats;

- expanding the capabilities for forecasting the development of information attacks based on the analysis of large data sets in real-time;

- enhancing the accuracy and effectiveness of anomaly detection and identifying relationships between entities, which has typically been difficult to achieve using traditional analytical methods.

This approach reduces the time required to analyze large data volumes and improves the quality of detecting and responding to information threats, which are crucial aspects of cybersecurity in the context of modern hybrid wars and complex information operations.

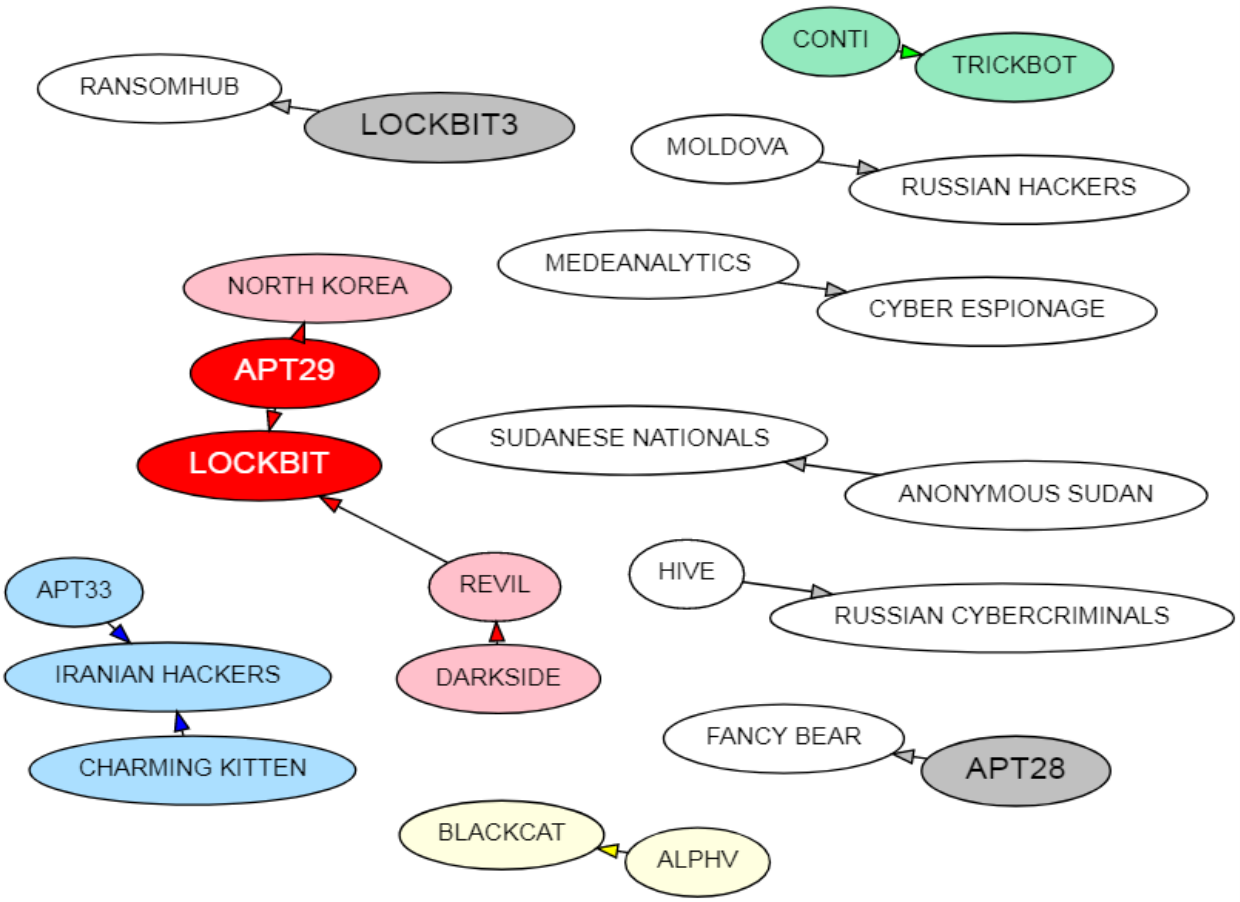

Figure 1. Semantic map constructed based on document analysis

References

1. Комплекс комп'ютерних програм "Система аналізу динаміки інформацыних потоків "Attack Index" / Шнурко-Табакова Е.В., Табаков

Д.В., Ланде Д.В., Гончаров К.О., Осадчук А.Є. // Україна. Свідоцтво про реєстрацію авторського права на твір N 92209 від 20.09.2019

2. Dmytro Lande, Leonard Strashnoy. GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now. - Kyiv: Engineering, 2023. - 168 p. ISBN 978-966-2344-94-3. URL: http://dwl.kiev.ua/art/gpt/
3. Оброблення надвеликих масивів даних (Big Data) : навчальний посібник. / Д.В. Ланде, І.Ю. Субач, А.Я. Гладун. - Київ: ТОВ "Інжиніринг", 2021. - 168 с. ISBN 978-966-2344-83-7. URL: http://dwl.kiev.ua/art/bigdata/
4. Dmytro Lande, Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system. Theoretical and Applied Cybersecurity, 2019. - N. 1. - pp. 103-108. URL: http://tacs.ipt.kpi.ua/article/view/169091/168863
5. Ланде Д.В. OSINT у кібербезпеці : навч. пос. / Ланде Д.В. - Київ: ТОВ "Інжиніринг", 2024. - 522 с. ISBN 978-966-2344-97-4. URL: http://dwl.kiev.ua/art/OSINT/