

ВПЛИВ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ОПТИМІЗАЦІЇ ПРОМПТІВ НА ЕФЕКТИВНІСТЬ ВИЯВЛЕННЯ ЗАГРОЗ У СИСТЕМАХ SIEM

¹ Вінницький національний технічний університет

Анотація

У роботі досліджується впровадження штучного інтелекту у систему SIEM для підвищення точності та ефективності аналізу логів шляхом використання різних промптів, що впливають на результати виявлення інцидентів кібербезпеки.

Ключові слова: штучний інтелект, система SIEM, кібербезпека, аналіз логів, промпти.

Abstract

The work investigates the implementation of artificial intelligence in the SIEM system to increase the accuracy and efficiency of log analysis by using various prompts that affect the results of detection of cyber security incidents.

Keywords: artificial intelligence, SIEM system, cyber security, log analysis, prompts.

Вступ

Сучасні системи управління інформаційною безпекою та подіями (SIEM) відіграють ключову роль у забезпеченні кібербезпеки [1]. Зі зростанням обсягів даних і складності кіберзагроз, традиційні методи обробки та аналізу логів стають менш ефективними. Інтеграція штучного інтелекту (ШІ) у систему SIEM пропонує нові можливості для автоматизації процесів виявлення загроз і зменшення часу реакції на інциденти кібербезпеки [2]. Мета дослідження полягала у вивченні впливу різних формулювань промптів (інструкцій) для ШІ на якість і точність аналізу логів у системах SIEM.

Результати дослідження

За основу нашого дослідження стало використання ШІ з використанням моделі GPT-3.5 Turbo від OpenAI [3]. У процесі дослідження впровадження ШІ для автоматизації аналізу логів у системах SIEM було встановлено, що одним із ключових чинників, який впливає на ефективність і глибину результатів, є формулювання запитів або так званих промптів. Було проведено кілька експериментів із використанням різних підходів до побудови промптів, що дозволило виявити важливу закономірність: чим більш конкретний і структурований запит, тим більша кількість інформації надається ШІ, а результати стають більш придатними для оперативного реагування на загрози та управління безпекою.

На першому етапі експерименту було застосовано загальні промпти, які містили простий запит на аналіз логів із метою виявлення інцидентів безпеки. Ці запити не надавали чітких вказівок щодо типів загроз або методів аналізу. Результати, отримані ШІ, були поверхневими: система вказувала на потенційні загрози, але без додаткових деталей чи класифікації за рівнем критичності. Такий підхід дозволяв виявити базові інциденти, однак не забезпечував глибокого аналізу, що необхідно для прийняття більш зважених рішень у системі кіберзахисту.

Цей процес виглядав наступним чином, в запит до моделі прикріплювались спеціальні параметри у вигляді двох важливих складових: role system і role user, параметри, які визначають контекст роботи ШІ та його взаємодію із запитом. Параметр role system встановлює основний контекст або "особистість" ШІ, тобто визначає, що система (ШІ) виступає як експерт у кібербезпеці, що має знання про аналіз логів для запобігання кіберзагрозам. Надання основного контексту є ключовим елементом, який впливає на те, як ШІ інтерпретує запити, аналізує дані і які методи використовує для отримання

результатів. Отож, було сформовано промпт, частина якого виглядає наступним чином:

```
{ "role": "system", "content": "Ви помічник, який знає інформацію про кібербезпеку та як аналізувати журнали для запобігання кіберзагрозам і атакам." }
```

Після чого, запит було відправлено на аналіз задалегідь підготовлений ряд логів, які містили в собі розподілену атаку на відмову в доступі. В результаті ШІ надав короткий звіт, що не включав детальної класифікації загроз або рекомендацій, який зображений на рисунку 1.

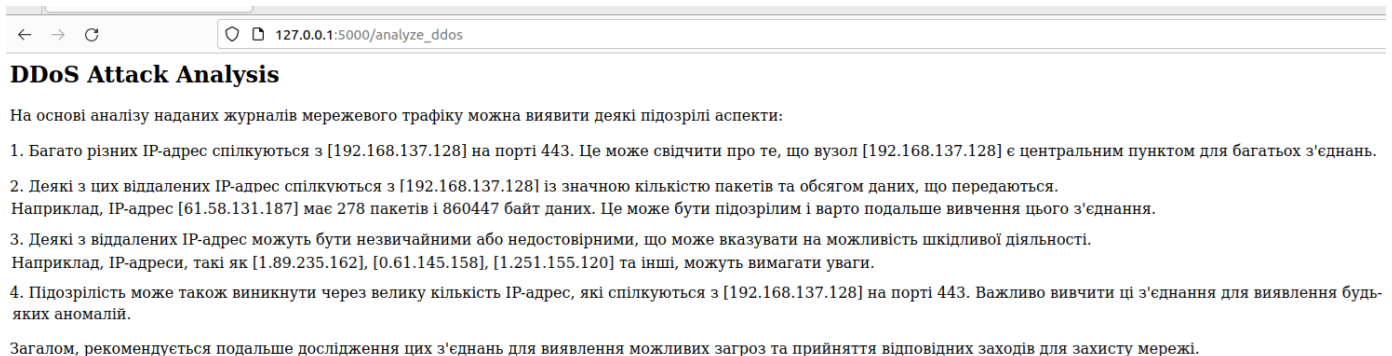


Рисунок 1 – Отримані результати з використанням простого промпту

На наступному етапі експерименту було застосовано деталізовані промпти, які включали конкретні інструкції щодо аналізу логів. У цих запитах вказувалися аспекти, на які ШІ мав звертати особливу увагу, такі як поведінковий аналіз користувачів, пошук аномалій у доступі до критичних ресурсів, аналіз активності під час неробочих годин та ідентифікація використання уразливих протоколів. Також було включено прохання класифікувати загрози за рівнем критичності та надати рекомендації щодо подальших дій для усунення інцидентів [4].

Результати другого підходу значно відрізнялися. ШІ не тільки визначив загрози, але й класифікував їх за рівнями ризику (високий, середній, низький), вказав індикатори компрометації (IoC) та надав детальні рекомендації щодо подальшого реагування. Більше того, було згенеровано звіт з ключовими метриками, які можна використовувати для загального огляду стану безпеки системи. Результати з використанням конкретизованого промпту зображено на рисунку 2.

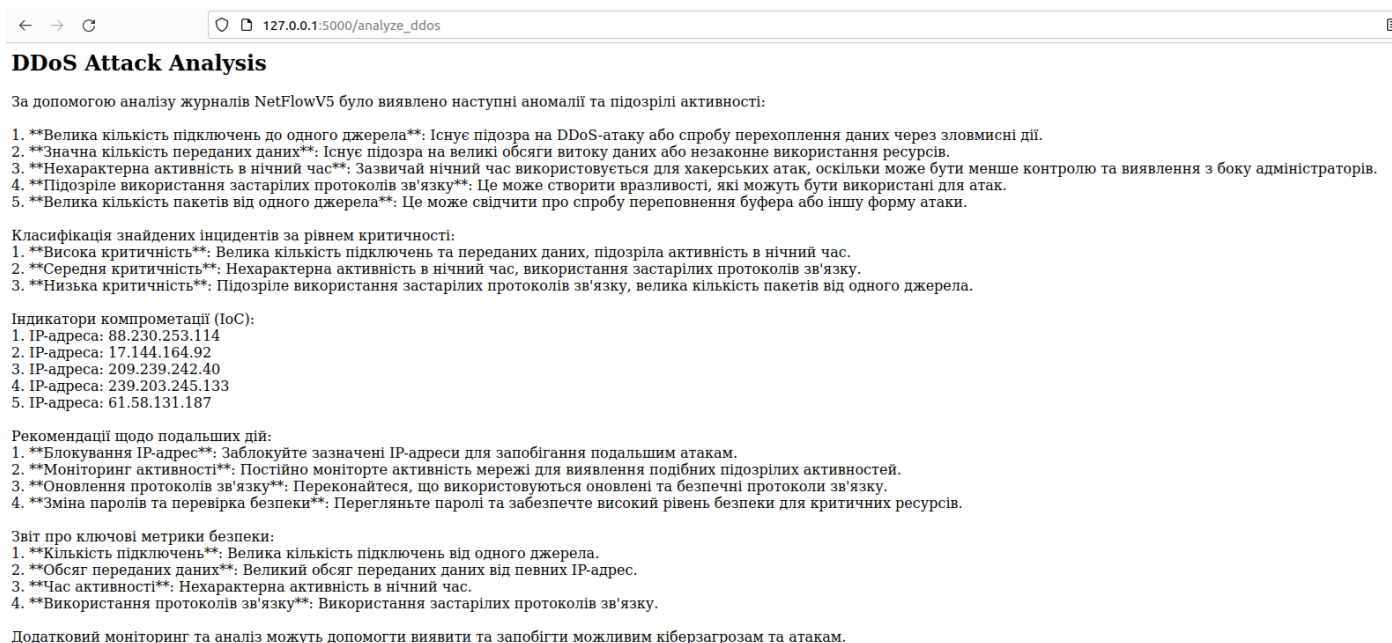


Рисунок 2 – Отримані результати з використанням розширеного промпту

Використання такого запиту дозволило отримати не лише фактичні дані щодо загроз, але й контекст, який значно спрощував подальшу роботу з результатами аналізу, що є критично важливим для оперативного реагування та підвищення ефективності системи захисту.

Проведені експерименти демонструють, що специфіка і структура промпту є вирішальними для отримання детальних і практичних результатів аналізу логів у системах SIEM. Загальні запити забезпечують базову інформацію, тоді як більш детальні й чітко структуровані інструкції дозволяють отримати повний спектр необхідних даних, включаючи класифікацію загроз і рекомендації для подальших дій. Такий підхід дозволяє покращити точність виявлення кіберзагроз, підвищує ефективність управління інцидентами та надає можливість оперативно реагувати на потенційні загрози, що вкрай важливо для підтримки надійної кібербезпеки.

Висновки

Впровадження штучного інтелекту у системи SIEM дозволяє суттєво підвищити ефективність управління інформаційною безпекою за рахунок автоматизації процесів аналізу логів та виявлення загроз. Основний висновок дослідження полягає в тому, що успіх використання ШІ безпосередньо залежить від якості формулювання промптів. Деталізовані, структуровані та контекстуальні промпти забезпечують більш точне та швидке виявлення загроз, мінімізуючи кількість хибнопозитивних результатів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. González-Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*. 2021. Т. 21, № 14. С. 4759. URL: <https://doi.org/10.3390/s21144759> (дата звернення: 23.10.2024).
2. Uccello, F., Pawlicki, M., D'Antonio, S., Kozik, R., Choraś, M. (2024). Towards Hybrid NIDS: Combining Rule-Based SIEM with AI-Based Intrusion Detectors. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the Second International Conference on Advances in Computing Research (ACR'24). ACR 2024. Lecture Notes in Networks and Systems, vol 956. Springer, Cham. URL: https://doi.org/10.1007/978-3-031-56950-0_21 (дата звернення: 23.10.2024).
3. Models - OpenAI API. *Open AI API*. URL: <https://platform.openai.com/docs/models/gpt-3-5-turbo> (дата звернення: 23.10.2024).
4. Korzynski, Pawel, et al. "Artificial intelligence prompt engineering as a new digital competence: Analysis of generative AI technologies such as ChatGPT." *Entrepreneurial Business and Economics Review* 11.3, 2023. С: 25-37 (дата звернення: 23.10.2024).

Якімов Олександр Павлович — студент групи ІБС-23м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: sasa.jkimov@gmail.com

Войтович Оlesia Петрівна — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет

Науковий керівник: **Войтович Оlesia Петрівна** — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Yakimov Oleksandr Pavlovich — student of group IBS-23m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: sasa.jkimov@gmail.com

Voytovych Olesya Petrivna — Candidate of Technical Sciences, Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia,

Scientific supervisor: Voytovych Olesya Petrivna — Candidate of Technical Sciences, Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia,