Використання штучного інтелекту для автоматизації виявлення та пріоритезації інцидентів інформаційної безпеки

УДК 004.056:004.8

Ірина Лозова[1], Михайло Різак[2], Євгеній Педченко[3]

Державний університет інформаційно-комунікаційних технологій,
[1]illozovaya@gmail.com, [2]advokat.rizak@gmail.com, [3]ympedchenko@gmail.com

Сучасний розвиток інформаційних технологій супроводжується постійним зростанням кількості кіберінцидентів та ускладненням механізмів атак. Центри моніторингу безпеки (SOC) змушені обробляти значні обсяги подій безпеки, що призводить до перевантаження аналітиків та збільшення часу реагування на інциденти. Традиційні підходи, засновані на статичних правилах кореляції, не забезпечують достатньої швидкості та точності аналізу подій. У зв'язку з цим актуальним є використання технологій штучного інтелекту (ШІ) та платформ класу SOAR (Security Orchestration, Automation and Response), які дозволяють автоматизувати процеси виявлення, аналізу та пріоритезації інцидентів інформаційної безпеки [1].

Метою роботи є дослідження можливостей використання штучного інтелекту для автоматизації виявлення та пріоритезації інцидентів інформаційної безпеки, а також практична реалізація SOAR-сценарію у середовищі Make.com із використанням зовнішніх Threat Intelligence-сервісів та AI-модуля.

Питання автоматизації процесів реагування на інциденти активно досліджуються у сучасній науковій літературі. У роботі [4] розглядаються принципи побудови SOAR-рішень для автоматизації поведінкових honeypot-систем та механізмів реагування на загрози. В роботі [2] описано можливості сервісу VirusTotal щодо отримання репутаційних характеристик IP-адрес, доменів та файлів через API. Документація [3] містить опис можливостей великих мовних моделей Anthropic Claude для автоматизації аналізу кіберзагроз і формування рекомендацій щодо реагування. У роботі [5] запропоновано багаторівневу агентну AI-модель для автоматизації процесів SOC. Аналіз публікацій показує, що поєднання SOAR-платформ, сервісів Threat Intelligence та AI-модулів дозволяє значно підвищити ефективність роботи SOC та скоротити час первинного аналізу інцидентів.

У межах роботи було реалізовано автоматизований сценарій реагування на інциденти у середовищі Make.com. Сценарій включав декілька взаємопов'язаних етапів: приймання подій через Webhook, збагачення даних за допомогою сервісу VirusTotal, аналіз інциденту за допомогою AI-модуля Anthropic Claude, маршрутизацію результатів та автоматичне формування повідомлень (рис.1).

На першому етапі модуль Webhook приймав вхідний JSON-об'єкт, який містив IP-адресу, опис події та ідентифікатор системи. Далі за допомогою HTTP-запиту до API сервісу VirusTotal виконувалось отримання репутаційних характеристик IP-адреси, зокрема кількості malicious, suspicious, harmless та undetected-спрацювань [2].

Після цього дані передавались до AI-модуля Anthropic Claude Simple Text Prompt, який виконував аналіз події та формував структуровану JSON-відповідь із полями risk_level, summary та action. Модель здійснювала автоматичну оцінку рівня ризику інциденту та визначала рекомендовану дію: alert або log [3]. Для подальшої обробки результатів використовувався модуль Parse JSON, який перетворював відповідь моделі у структуровані поля.

Рис.1. Загальна схема сценарію в Make.com

На етапі маршрутизації застосовувався Router, який залежно від значення action виконував різні сценарії реагування. Якщо подія визнавалась критичною, система автоматично надсилала повідомлення до Telegram. Для менш критичних подій інформація записувалась до Google Sheets з метою ведення журналу аудиту.

У процесі тестування використовувалися як інциденти, пов'язані з потенційними brute-force атаками, так і приклади легітимної активності користувачів. Для тестового інциденту модель Claude сформувала значення risk_level = 62 та action = alert, що дозволило автоматично маршрутизувати подію до Telegram-каналу аналітика без додаткової ручної перевірки (рис. 2).

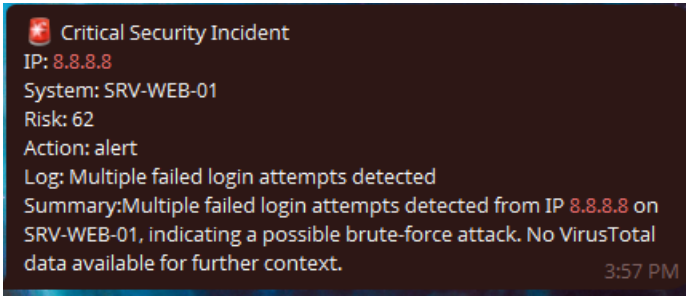

Рис. 2. Приклад фінального сповіщення в Telegram

Отримані результати показали, що запропонований підхід дозволяє автоматизувати значну частину первинного аналізу інцидентів інформаційної безпеки. Інтеграція Threat Intelligence та AI-моделі забезпечує швидке оцінювання ризику та скорочує час реагування на інциденти. Крім того, використання SOAR-підходу дозволяє знизити навантаження на SOC-аналітиків та підвищити ефективність процесів моніторингу безпеки.

Таким чином, результати дослідження підтверджують доцільність використання штучного інтелекту та SOAR-платформ для автоматизації виявлення та пріоритезації інцидентів інформаційної безпеки. Подальші дослідження можуть бути спрямовані на інтеграцію додаткових джерел Threat Intelligence, удосконалення моделей оцінювання ризику та розширення автоматизованих механізмів реагування.

1. SANS Institute. AI-Driven SecOps: Unifying Controls, Automating Response, and Advancing the Modern SOC Using Cortex XSIAM. 2025. URL: https://www.sans.org/white-papers/ai-driven-secops-unifying-controls-automating-response-advancing-modern-soc-using-cortex-xsiam.
2. VirusTotal. API Overview. URL: https://docs.virustotal.com/reference/overview.
3. Anthropic. Anthropic Claude Documentation. URL: https://platform.claude.com/docs/en/home.
4. Umesh Bartwal, Subhasis Mukhopadhyay, Rohit Negi, Shashank Shukla. Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots. 2022. URL: https://doi.org/10.1109/DSC54232.2022.9888808.
5. Jay Roy, Sandeep Singh. AgentSOC: A Multi-Layer Agentic AI Framework for Security Operations Automation. 2026. URL: https://doi.org/10.1109/ICAIC67076.2026.11395783.

Методологія забезпечення мережевої ізоляції та динамічного масштабування ресурсів у середовищі змагального кіберполігону

УДК 004.056:378.147

Богдан Маліцький[1], Михайло Євдокімов[2], Данило Куташ[3], Василь Різак[4]

Ужгородський національний університет,
[1]bohdan.malitskyi@uzhnu.edu.ua, [2]mykhailo.yevdokimov@uzhnu.edu.ua,
[3]danylo.kutash@student.uzhnu.edu.ua, [4]vrizak@uzhnu.edu.ua

Проведення CTF-чемпіонату регіонального масштабу ставить низку технічних вимог до інфраструктури: ізоляція вразливих сервісів від основної мережі закладу освіти, контрольований віддалений доступ для учасників з різних міст, можливість швидко повертати середовище у вихідний стан між раундами та одночасна робота з десятками учасників. Виконати ці вимоги на базі діючого навчального кіберполігону можливо лише за умови комплексної адаптації його архітектури – на рівні платформи віртуалізації, мережі, доступу та змагальної системи. Метою роботи є розробка та впровадження методології,