УДК 004.7:8
О. Швець; М. Стадник, к.т.н, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИЯВЛЕННЯ ПІДОЗРІЛИХ ДІЙ ТА СПРОБ АТАК З ВИКОРИСТАННЯМ АНАЛІЗУ ТРАФІКУ З AMAZON CLOUD WATCH

UDC 004.7:8
O. Shvets; M. Stadnyk, Ph.D.

DETECTION OF SUSPICIOUS ACTIVITIES AND ATTACK ATTEMPTS USING TRAFFIC ANALYSIS FROM AMAZON CLOUD WATCH

Штучний інтелект (ШІ) покращує традиційний підхід до аналізу мережевого трафіку. Завдяки своїм можливостям обробки великих обсягів даних і виявлення складних патернів, ШІ стає незамінним інструментом у боротьбі з кіберзагрозами, включаючи атаки типу «отруєння кешу», DoS, DDoS, аналіз вмісту трафіку (вміст пакетів для виявлення шкідливого коду, фішингових атак), детекцію ботнетів, що використовуються для розповсюдженню спаму [1].

ШІ-системи можуть визначати відхилення від шаблону нормального трафіку, які можуть вказувати на атаку. Наприклад, раптовий сплеск запитів до незвичайного домену або зміни в поведінці користувача. Також системи штучного інтелекту створюють детальний профіль кожного користувача, включаючи звички перегляду, географічне розташування, браузер для використання. Будь-які відхилення від цього профілю можуть свідчити про компрометацію облікового запису. Також ШІ системи можуть прогнозувати потенційні атаки на основі аналізу історичних даних та трендів .

Amazon Cloud Watch – це потужний інструмент, який дозволяє не лише збирати дані про вашу інфраструктуру в AWS, але й проводити глибокий аналіз мережевого трафіку. Завдяки цій функціональності можливим є наступне:

- Виявлення аномалії. З використанням Amazon CloudWatch можливо достатньо швидко виявити піки трафіку, незвичайні шаблони або різкі спади, що можуть свідчити про проблеми з веб-сервісом або атаку.
- Оптимізувати витрати: Проаналізувавши обсяги трафіку, можливо оптимізувати розмір інстансів та інших ресурсів, знизивши таким чином витрати.
- Усунути проблеми з продуктивністю: Виявивши вузькі місця в мережі, можливо покращити загальну продуктивність сервісу чи додатку.
- Забезпечити безпеку: Аналізуючи трафік, можливо виявити підозрілу активність, яка може свідчити про спробу хакерської атаки.

Набір даних містив записи веб-трафіку, зібрані через AWS CloudWatch, спрямовані на виявлення підозрілих дій і потенційних спроб атак. Дані були згенеровані шляхом моніторингу трафіку до робочого веб-сервера з використанням різних правил виявлення для ідентифікації аномальних шаблонів. Первинний набір даних складався із 16 параметрів (час створення, час закриття зв'язку, IP джерела, кількість байтів отриманих, кількість надісланих байтів, країна, код відповіді HTTP, IP отримувача). Для класифікації трафіку було використано моделі Random Forest, CNN, Dense. Також було виявлено позитивну кореляцію між вхідними та вихідними байтами. Це свідчить про те, що більші байти на вході зазвичай відповідають вищим байтам на виході, що вказує на двонаправлений зв'язок між сервером і клієнтами.

Література

1. Abbasi M., Shahraki A., Taherkordi A. Deep learning fornetwork traffic monitoring and analysis (NTMA): A survey. Computer Communications 170, 2021, p. 19–41.