УДК 004.056
Кубарич З.П., Скарга-Бандурова І.С., д.т.н., проф.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЕФЕКТИВНОГО РЕАГУВАННЯ НА ІНЦИДЕНТИ У SIEM СИСТЕМІ

Z.P. Kubarych, I.S. Skarga-Bandurova, DSc, Prof

USING ARTIFICIAL INTELLIGENCE FOR EFFECTIVE INCIDENT RESPONSE IN SIEM SYSTEM

Зростаюча кількість і складність кібератак підкреслюють нагальну потребу в інноваційних рішеннях для посилення безпеки цифрової інфраструктури. Security Incident and Event Management (SIEM) традиційно покладаються на звичайні механізми портів і переадресації для накопичення журналів подій та їхнього аналізу на основі встановлених сценаріїв. Однак, з розвитком штучного інтелекту (ШІ) і швидкою зміною методологій атак, ці традиційні методи стикаються з істотними перешкодами, особливо при обробці даних у режимі реального часу. Разом з тим, ШІ є багатообіцяючою технологією, яка може значно покращити кібербезпеку та реагування на інциденти.

Мета даного дослідження полягає у розумінні впливу ШІ та розвитку SIEM на основі ШІ для покращення виявлення та обробки інцидентів загрози безпеці. У роботі будуть розглянуті засоби керування на основі штучного інтелекту, які можуть посилити заходи кібербезпеки та дати можливість організаціям ефективно реагувати на загрози.

Системи SIEM на основі штучного інтелекту використовують алгоритми машинного навчання для аналізу великих обсягів даних у режимі реального часу, що дозволяє організаціям ефективніше виявляти загрози та реагувати на них [1]. Завдяки безперервному моніторингу та аналізу мережевого трафіку, поведінки користувачів і системних журналів ці системи можуть виявляти аномалії, шаблони та ознаки компрометації, які можуть залишитися непоміченими аналітиками [2]. Цей проактивний підхід покращує можливості виявлення загроз і реагування на них, скорочуючи час між вторгненням і ліквідацією. Отже, щоб посилити заходи кібербезпеки та дати можливість організаціям залишатися попереду можливих загроз, в роботі заплановано виконання наступних задач:

1. Огляд літератури з технологій штучного інтелекту використовуваних для поліпшення виявлення інцидентів у SIEM системах.
2. Оцінка та порівняння ефективності провідних SIEM-рішень на основі штучного інтелекту за набором певних параметрів.
3. Вивчення можливостей автоматизації реагування на інциденти на основі штучного інтелекту
4. Розробка і тестування алгоритму автоматичного реагування на потенційну кібер загрозу.

Література

1. Bandr Siraj Fakiha. 2020. Effectiveness of Security Incident Event Management (SIEM) System for Cyber Security Situation Awareness. International Journal of Forensic Medical and Toxicological Sciences. [online] Available at: https://medicopublication.com/index.php/ijfmt/article/view/11587/10679.

2. National Institute of Standards and Technology (NIST). 2020. Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection. [online] Available at: https://csrc.nist.gov/pubs/ir/8219/final