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

МОЖЛИВОСТІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОПЕРАЦІЙНОМУ ЦЕНТРІ БЕЗПЕКИ

S. Yu. Zadorozhnyi, I.S. Skarga-Bandurova, DSc, Prof

HARNESSING ARTIFICIAL INTELLIGENCE FOR SECURITY OPERATIONS CENTRES

Центр Операційної Безпеки (Security Operations Centre або SOC) є центральним пунктом будь-якої організації, який виконує моніторинг, аналіз та реагування на інциденти безпеки. Основна місія SOC полягає в захисті підприємства від порушень та атак, забезпеченні безпеки активів (даних, додатків, інфраструктури тощо) та забезпеченні нормального функціонування. За визначенням [1], SOC є комбінацією людей, процесів та технологій, що забезпечують захист інформаційних систем організації через про активний дизайн та конфігурацію, постійний моніторинг, виявлення непередбачених дій або небажаного стану та мінімізацію шкоди від небажаних ефектів. Для виявлення та протидії кіберзагрозам, SOC повинен збирати дані по всій організації і проводити аналіз в реальному або наближеному до реального часу, використовуючи великі обсяги даних з журналів (наприклад, мережевих та веб-брандмауерів, датчиків мережі, кінцевих точок), систем виявлення та запобігання вторгнень, систем управління ідентифікацією та доступом, та безлічі інших джерел. Однак, незважаючи на всі захисні заходи, організації постійно піддаються кібератакам і порушенням безпеки, що може негативно впливати на їх діяльність. Вузьким місцем в традиційних підходах є те, що процес реагування на інциденти обробляється вручну аналітиками, які отримують сповіщення та аналізують їх, щоб вирішити, яку реакцію вжити. Крім того, традиційні методи породжують велику кількість сповіщень, які перевантажують аналітиків SOC, змушуючи їх визначати пріоритети та приймати відповідні заходи щодо ліквідації. Використання методів штучного інтелекту (AI) та машинного навчання (ML) в SOC може вирішити ці завдання, забезпечуючи більшу точність, швидкість та адаптивність у боротьбі з кіберзагрозами.

Основна мета цього дослідження - оцінити, як методи AI та ML можуть вдосконалити системи запобігання інтрузій (IPS), системи управління інформаційною безпекою (SIEM), та системи запобігання витоку даних (DLP) у контексті SOC. Це дослідження фокусується на аналізі проблем та викликів, з якими стикаються ці системи, та розглядає потенціал AI/ML для їх подолання. У роботі розглядаються наступні дослідницькі запитання:

1. Аналіз проблем та викликів у системах IPS/IDS, SIEM, DLP. Визначення конкретних труднощів, з якими стикаються ці системи, та з'ясування їх взаємозв'язків та впливу на загальну безпеку.
2. Дослідження шляхів впровадження AI/ML для розв'язання визначених проблем, оцінка їх практичних переваг та аналіз викликів для їх впровадження.
3. Впровадження екосистеми вибраних систем. Дослідження можливостей інтеграції систем IPS/IDS, SIEM, DLP у єдину екосистему на базі ШІ та аналіз ефективності такого підходу для підвищення функціональності SOC.

Література

1. Security, R.S.I. (2021). NIST Security Operations Center Best Practices. [online] RSI Security. Available at: https://blog.rsisecurity.com/nist-security-operations-center-best-practices/.