ІНТЕГРАЦІЯ SIEM В СТРУКТУРІ ISMS ІЗ ЗАСТОСУВАННЯМ AI

Іванський І.О., Нехороших Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

В сучасних умовах зростання кількості кіберзагроз, ефективне управління інформаційною безпекою стає критично важливим для організацій. Системи SIEM відіграють ключову роль у структурі ISMS, забезпечуючи централізований збір і аналіз подій безпеки. Однак традиційні SIEM-рішення мають обмеження у виявленні складних та невідомих атак. Інтеграція технологій штучного інтелекту дозволяє підвищити ефективність SIEM за рахунок автоматизації аналізу даних, виявлення аномалій та швидшого реагування на інциденти. Водночас така інтеграція потребує врахування низки технічних і організаційних викликів.

Метою доповіді є дослідження особливостей інтеграції SIEM у структуру ISMS із використанням технологій штучного інтелекту, зокрема аналіз їх впливу на ефективність виявлення загроз, автоматизацію процесів моніторингу та реагування, а також визначення основних переваг та ризиків, пов'язаних із застосуванням AI у кібербезпеці.

SIEM – це настроювана система обліку подій безпеки, яка збирає та аналізує дані про події безпеки з локальних і хмарних середовищ. SIEM допомагає вживати заходів реагування для усунення проблем, що завдають шкоди організації, а також забезпечує дотримання вимог щодо відповідності та звітності [1]. SIEM виконує роль центрального аналітичного та оперативного компонента в рамках Системи управління інформаційною безпекою (ISMS), забезпечуючи підтримку таких ключових процесів, як оцінка ризиків, виявлення інцидентів, реагування на інциденти та моніторинг дотримання вимог. Система інтегрується з іншими елементами ISMS, зокрема з політиками безпеки, системами контролю доступу та інструментами управління вразливостями, утворюючи єдину екосистему безпеки.

Постійний моніторинг інформаційної безпеки (ISCM) визначається як постійне відстеження стану інформаційної безпеки, вразливостей та загроз з метою забезпечення прийняття обґрунтованих рішень щодо управління ризиками в організації. Програма допомагає забезпечити, щоб впроваджені засоби контролю безпеки залишалися ефективними, а операції не виходили за межі встановлених організаційних рівнів прийнятного ризику з огляду на неминучі зміни, що відбуваються з часом. ISCM, як важливий етап у системі управління ризиками (RMF) організації, надає посадовим особам організації доступ до інформації, пов'язаної з безпекою, на запит, що дозволяє своєчасно приймати рішення з управління ризиками, включаючи рішення щодо авторизації [2]. Забезпечити ефективний моніторинг у масштабах всієї організації неможливо лише за допомогою ручних або лише за допомогою автоматизованих процесів. У випадках, коли застосовуються ручні процеси, вони мають бути повторюваними та піддаватися перевірці, щоб забезпечити послідовність їхнього виконання. Автоматизовані процеси, зокрема

використання автоматизованих допоміжних інструментів, наприклад, інструментів сканування вразливостей, пристроїв для сканування мережі, можуть зробити процес безперервного моніторингу більш економічно вигідним, послідовним та ефективним [2]. Типова архітектура SIEM з використанням штучного інтелекту включає джерела даних, зокрема кінцеві точки, мережеві пристрої, хмарні сервіси, рівні збору та нормалізації даних, системи зберігання даних, такі як «озера даних» (data lakes), аналітичні механізми на базі моделей штучного інтелекту та машинного навчання, а також компоненти для координації реагування, наприклад, SOAR. Така багаторівнева архітектура забезпечує масштабованість та гнучкість операцій з безпеки. Традиційні системи управління інформацією та подіями безпеки (SIEM) мають обмеження в обробці великих обсягів даних та виявленні складних загроз. Щоб подолати ці обмеження, інтеграція платформ SIEM з озерами даних та штучним інтелектом є перспективним напрямком розвитку. [3] Алгоритми штучного інтелекту та машинного навчання здатні виявляти складні схеми атак і нові загрози, які можуть залишитися непоміченими традиційними системами SIEM [2].

Ці технології постійно навчаються на основі даних, покращуючи свою здатність виявляти нові та невідомі загрози (атаки «нульового дня») шляхом розпізнавання ледь помітних закономірностей або аномалій у поведінці, які можуть свідчити про зловмисну діяльність. Системи на основі штучного інтелекту та машинного навчання можуть інтелектуально аналізувати дані, щоб зменшити кількість помилкових спрацьовувань, розрізняючи звичайну активність і реальні загрози [2].

Інтеграція штучного інтелекту та машинного навчання в існуючі системи SIEM може бути складним і ресурсомістким процесом. Однією з проблем, пов'язаних із застосуванням штучного інтелекту та машинного навчання в системах SIEM, є брак прозорості, який часто називають проблемою «чорного ящика» [2]. Отруєння даних: ця загроза пов'язана з введенням помилкових, сфальсифікованих або неправильних даних у навчальний або валідаційний набір шляхом отримання законного або незаконного доступу через зловживання недосконалими механізмами аутентифікації та авторизації. Бекдори в моделях: отримані моделі можуть бути схильні до загроз у вигляді бакдорів, які розкривають їх внутрішню роботу (порушення конфіденційності), впливають на їх функціонування (порушення цілісності) або погіршують/скасовують їх продуктивність (вплив на доступність) [4].

Впровадження технологій генеративного штучного інтелекту в операції з кібербезпеки відкриває як безпрецедентні можливості, так і значні ризики для організацій у всьому світі [5]. Наприклад, недостатня надійність та вразливість моделей і алгоритмів ШІ, як-от, суперечливе виведення та маніпулювання моделями, атаки на кіберфізичні системи на базі ШІ, маніпулювання даними, що використовуються в системах ШІ [4]. Сьогодні організації стикаються зі змінами в ландшафті загроз, де фішингові кампанії, створені за допомогою ШІ, досягають безпрецедентного рівня складності, атаки на основі супротивного

машинного навчання націлені на системи виявлення, а автоматизовані зловмисники діють у масштабах, які раніше були неможливими. Організації впроваджують гібридні системи прийняття рішень, процеси аналізу з використанням штучного інтелекту та моделі співпраці на основі ескалації, які зберігають людський контроль, водночас використовуючи штучний інтелект для масштабування та прискорення процесів [5].

Перехід від статичного виявлення загроз на основі сигнатур до динамічних моделей з інтегрованим штучним інтелектом є найфундаментальнішою адаптацією архітектури, що спостерігається в різних організаційних контекстах.

Замість повної заміни існуючих систем організації демонструють моделі еволюційної адаптації, які ґрунтуються на вже сформованих основах, водночас враховуючи специфічні особливості та можливості штучного інтелекту [5].

Отже, інтеграція систем управління інформацією та подіями безпеки (SIEM) у структуру системи управління інформаційною безпекою (ISMS) із використанням технологій штучного інтелекту є важливим етапом розвитку сучасних підходів до кіберзахисту. Використання AI та машинного навчання дозволяє значно підвищити ефективність виявлення загроз, зокрема складних та невідомих атак, а також автоматизувати процеси моніторингу та реагування на інциденти.

Застосування інтелектуальних алгоритмів сприяє зменшенню кількості помилкових спрацьовувань, підвищує швидкість аналізу великих обсягів даних та забезпечує більш адаптивний підхід до управління безпекою.

Разом із тим інтеграція AI у SIEM супроводжується рядом викликів, серед яких складність впровадження, недостатня прозорість моделей, ризики отруєння даних та наявність потенційних вразливостей у самих алгоритмах.

Список літератури

1. Овчаренко, М. Ю., & Сєвєрінов, О. В. (2019). Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки / ЧДТУ, НТУ" ХПІ", ВА ЗС АР, УТіГН, ДП" ПД ПКНДІ АП".

2. National Institute of Standards and Technology. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST SP 800-137. URL: https://csrc.nist.gov/pubs/sp/800/137/final

4. Integrating Security Information and Event Management (SIEM) with Data Lakes and AI: Enhancing Threat Detection and Response URL: https://www.researchgate.net/publication/384905295_Integrating_Security_Information_and_Event_Management_SIEM_with_Data_Lakes_and_AI_Enhancing_Threat_Detection_and_Response

5. European Union Agency for Cybersecurity. Artificial Intelligence Cybersecurity Challenges URL: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

6. Advances in AI-driven Cybersecurity Systems URL: https://arxiv.org/abs/2506.12060