УДК 681.12

Б.М. Мороз
О.П. Войтович

ВИЯВЛЕННЯ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ В ПОТОЦІ ПОДІЙ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Вінницький національний технічний університет

Анотація

SIEM-системи є важливим інструментом для виявлення та аналізу інцидентів в кібербезпеці. У дослідженні розглянуто сутність SIEM-систем, подій та інцидентів, а також їх тлумачення відповідно до законодавства. Досліджено принципи функціонування SIEM-систем у процесі прийняття рішень, розглянуто їх компоненти та підсистеми, а також проаналізовано, на чому базуються сучасні рішення SIEM-систем та хто здійснює процес прийняття рішень.

Ключові слова: SIEM-системи, інциденти, події, процес прийняття рішень, кібербезпека

Abstract

SIEM systems are important tools for detecting and analyzing incidents in information security. In this thesis, we examine the essence of SIEM systems, events, and incidents, as well as their interpretation according to legislation. We explore the principles of functioning of SIEM systems in the decision-making process, discuss their components and subsystems, and clarify the basis of modern SIEM system solutions, and who is involved in the decision-making process.

Keywords: SIEM systems, incidents, events, decision-making process, cyber security.

Вступ

У сучасному цифровому світі, загрози кібербезпеки набувають все більшого значення, і виявлення інцидентів стає ключовим завданням для забезпечення безпеки інформаційних систем. Штучний інтелект, що базується на алгоритмах машинного навчання та глибокому аналізі даних, являється потужним інструментом у боротьбі з кіберзагрозами. Використання штучного інтелекту може значно підвищити ефективність виявлення інцидентів кібербезпеки і зменшити час реагування на потенційні загрози. Дослідження в галузі виявлення інцидентів кібербезпеки з використанням штучного інтелекту має великий потенціал для подальшого розвитку та покращення безпеки інформаційних систем. У цьому дослідженні розглядаються принципи та методики використання штучного інтелекту для виявлення інцидентів кібербезпеки в потоці подій, з метою розробки ефективних інструментів для забезпечення безпеки в інформаційному середовищі.

Результати дослідження

SIEM (Security Information and Event Management) системи є комплексними інструментами, які відіграють важливу роль у забезпеченні інформаційної та кібербезпеки [1]. Вони поєднують в собі функції збору, акумуляції, аналізу та реагування на події та інциденти, що відбуваються в мережі комп'ютерів та інших пристроях. SIEM-системи надають цілісний погляд на стан безпеки інформаційних ресурсів, дозволяючи виявляти та реагувати на потенційні інциденти кібербезпеки.

Якщо звернутись до українського законодавства та міжнародних стандартів то, зокрема в ISO 27000, визначають поняття "подія" і "інцидент" в контексті інформаційної безпеки [2,3]. Подія - це будь-яка відхилення від нормального стану, яке може мати значення для безпеки інформації. Інцидент - це подія або послідовність подій, які мають наслідком порушення конфіденційності, цілісності або доступності інформації, або підозру в такому порушенні.

В контексті прийняття рішень SIEM-системи працюють за принципом акумуляції, кореляції та аналізу подій з метою виявлення потенційних інцидентів. Вони збирають дані про події, що відбуваються в інформаційно-комунікаційних системах, такі як: лог-файли, мережеві дані, системні події та інші джерела. Потім ці дані аналізуються та проводиться кореляція для виявлення несподіваних або підозрілих залежностей та зразків, що можуть свідчити про потенційні інциденти в системі. На основі

цього аналізу SIEM-системи генерують сповіщення або приймають автоматичні рішення щодо застосування заходів безпеки, таких як блокування доступу або подальше дослідження події.

Використання штучного інтелекту (ШІ) в SIEM-системах відіграє значну роль у виявленні та аналізі подій інформаційної безпеки в потоці. ШІ дозволяє автоматизувати процеси аналізу та реагування на події, забезпечуючи високу швидкість та точність виявлення потенційних інцидентів [4]. Алгоритми машинного навчання та інтелектуального аналізу даних використовуються для створення моделей, які навчаються на основі історичних даних та здатні розпізнавати аномалії та загрози в реальному часі.

В основному SIEM-системи отримують дані з різноманітних джерел подій, таких як міжмережеві екрани, системи виявлення вторгнень, журнали подій тощо. Ці джерела постачають дані про активності, події та стан безпеки інформаційно-комунікаційних систем [5]. SIEM-система збирає, акумулює та нормалізує ці дані для подальшого аналізу та виявлення потенційних інцидентів.

Також у SIEM-системах використовуються різні методи та алгоритми для прийняття рішень на основі результатів аналізу подій та інцидентів. Ці підсистеми можуть включати правила, евристичні алгоритми, алгоритми машинного навчання та інші методи [6]. В процесі виявлення інцидентів важливу роль відіграє особа або група, відповідальна за прийняття рішень на основі результатів аналізу.

Загалом у сучасних SIEM-системах активно використовуються нові технології, методи та практики для покращення процесу виявлення інцидентів. Наприклад, використання алгоритмів глибокого навчання, аналізу великих обсягів даних (big data), розподіленого обчислення та інших інноваційних підходів. Ці підходи спрямовані на підвищення ефективності та точності виявлення інцидентів у SIEM-системах.

Висновки

Інтеграція штучного інтелекту в SIEM-системи має велику важливість для ефективного виявлення інцидентів в потоці подій та забезпечення кібербезпеки. Використання штучного інтелекту дозволяє покращити швидкість, точність та автоматизацію процесів виявлення інцидентів, що допомагає забезпечити безпеку та захист інформації у сучасних комп'ютерних мережах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Національний інститут стандартів і технологій (NIST). (2021). Security Information and Event Management. https://www.nist.gov/topics/security-information-and-event-management
2. ISO/IEC 27000 family of standards. (2021). International Organization for Standardization. https://www.iso.org/isoiec-27001-information-security.html
3. Закон України про основні засади забезпечення кібербезпеки України. (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)
4. З. В. Гбур. Використання штучного інтелекту в інформаційній безпеці України. Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з питань державного управління (Категорія «Б», Наказ Міністерства освіти і науки України від 28.12.2019 №1643), 4-7.
5. Лабенська, О. (2019). Застосування штучного інтелекту в системах SIEM для виявлення кіберзагроз. Науковий вісник Національного університету цивільного захисту України, (2), 152-160.
6. Орлик, А., & Шкандрик, О. (2021). Сучасні підходи до виявлення та реагування на кіберінциденти в системах SIEM. Наукові праці Харківського національного університету внутрішніх справ, (4), 144-151.

Мороз Богдан Михайлович — аспірант кафедри захисту інформації, Вінницький національний технічний університет, Вінниця

Науковий керівник: ***Войтович Олеся Петрівна*** — канд. техн. наук, доц., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Moroz Bogdan Mykhailovych - graduate student at the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia

Supervisor: ***Voitovych Olesia Petrivna*** – PhD, Associate Professor, Department of Information Protection, Vinnytsia National Technical University, Vinnytsia.