УДК 004.77 (045)

Д. А. Гончар

В. В. Лукічов

СПОСОБИ АНАЛІЗУ МЕРЕЖЕВИХ ПОДІЙ В SIEM-СИСТЕМАХ

Вінницький національний технічний університет

Анотація

Досліджено технологію SIEM, проаналізовано способи аналізу мережевих подій у SIEM-системах та визначено основні способи які можуть бути використані для розробки системи аналізу мережевих подій в SIEM-системах.

Ключові слова: siem-системи, sim, sem.

Abstract

The SIEM technology was studied, the methods of analyzing network events in SIEM systems were analyzed, and the main methods that could be used to develop a system for analyzing network events in SIEM systems were determined.

Keywords: siem systems, sim, sem**.**

Вступ

SIEM (Security information and event management) у комп'ютерній безпеці є програмними продуктами, які об'єднують управління інформаційною безпекою SIM (англ. Security information management) та управління подіями безпеки SEM (англ. Security event management). Технологія SIEM забезпечує аналіз в реальному часі подій які можуть зашкодити безпеці, отриманих від мережевих пристроїв і додатків. SIEM представлено додатками, приладами або послугами, і використовується також для ведення журналу даних і генерації звітів в цілях сумісності з іншими бізнес-даними [1]. Постачальники продають SIEM як програмне забезпечення, як прилади або як керовані послуги; ці продукти також використовуються для реєстрації даних безпеки та створення звітів для цілей відповідності.

Зважаючи на постійний ріст кількості кібератак та загроз, аналіз мережевих подій в SIEM-системах є дуже актуальною темою дослідження. Центральною проблемою дослідження є розробка та вдосконалення методів аналізу мережевих подій, які дозволять ефективно виявляти загрози та забезпечувати безпеку інформаційних систем.

Теоретична значущість полягає в розробці та вдосконаленні методів аналізу мережевих подій, які використовуються в SIEM-системах. Це дозволяє забезпечувати більш точний та ефективний аналіз подій, що надходять з різних джерел та забезпечувати більш високий рівень безпеки інформаційних систем.
Практична значущість полягає в тому, що розроблені методики аналізу мережевих подій можуть бути застосовані в різних інформаційних системах для виявлення загроз та забезпечення їхнього ефективного протидії [2].

Основні методи аналізу мережевих подій

Основними методами аналізу мережевих подій в SIEM-системах є сигнатурний аналіз, аналіз аномалій, кореляційний аналіз та аналіз потоку даних. Ці методи охоплюють досить велику частину мережевих подій які відбуваються в системі та дозволяють детально розглянути можливі загрози.

- Сигнатурний аналіз - це метод аналізу мережевих подій, який базується на порівнянні активності в мережі з попередньо визначеними шаблонами, які описують конкретні типи атак. Ці шаблони називаються сигнатурами. Якщо активність в мережі відповідає якійсь з визначених сигнатур, то система вважає цю активність підозрілою і сповіщає про це адміністратора.
- Аналіз аномалій - це метод аналізу мережевих подій, який базується на виявленні незвичних або непередбачуваних змін в поведінці мережі. Для використання цього методу система моніторить поведінку мережі на протязі певного періоду часу і будує модель нормальної поведінки мережі. Якщо виявляється якась активність, яка сильно відрізняється від нормальної поведінки, то система вважає цю активність підозрілою і сповіщає про це адміністратора.
- Кореляційний аналіз - це метод аналізу мережевих подій, який базується на взаємозв'язку між різними видами подій. Для використання цього методу система аналізує велику кількість різних видів подій, що виникають в мережі, і шукає зв'язки між ними. Якщо знайдені зв'язки вказують на можливість атаки або іншої підозрілої активності, то система сповіщає про це адміністратора.

— Аналіз потоку даних - це метод аналізу мережевих подій, який базується на моніторингу потоку даних в мережі і виявленні незвичних або підозрілих пакетів даних [3]. Для використання цього методу система аналізує трафік в мережі і спробує визначити, чи є пакети даних, які відрізняються від нормального потоку. Якщо виявляється якийсь підозрілий пакет даних, то система вважає цю активність підозрілою і сповіщає про це адміністратора.

Одним з основних методів аналізу мережевих подій є комбінація різних методів для отримання більш точних результатів. Наприклад, можна поєднувати сигнатурний аналіз з аналізом аномалій, щоб зменшити кількість неправдивих результатів, або поєднувати кореляційний аналіз з аналізом потоку даних, щоб виявляти більше складних атак, які можуть бути приховані в окремих потоках даних.

Висновки

Застосування різних методів аналізу мережевих подій у SIEM-системах дійсно може підвищити ефективність виявлення інцидентів безпеки та забезпечити вищий рівень захисту мережі. Цього можна досягти використовуючи методи описані в роботі. Такі методи дозволять оперативно реагувати на можливі загрози та не допускати виникнення серйозних проблем з безпекою мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Natalia G. Miloslavskaya.Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers. [Електронний ресурс]. - Режим доступу: https://www.researchgate.net/publication/318708872_Analysis_of_SIEM_Systems_and_Their_Usage_in_Security_Operations_and_Security_Intelligence_Centers

2. Mike Tierney. SIEM Use Cases: Implementation and Best Practices [Електронний ресурс]. - Режим доступу: https://blog.netwrix.com/2021/05/05/siem-use-cases/

3. Theyazn H.H Aldhyani. A review of network traffic analysis and prediction techniques [Електронний ресурс]. - Режим доступу: https://www.researchgate.net/publication/339927785_A_review_of_network_traffic_analysis_and_prediction_techniques

Гончар Данило Андрійович – студент групи 1БС-19б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: danya.gonchar.2017@gmail.com.

Лукічов Віталій Володимирович – к. т. н. , доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua.

Danylo Gonchar **–** student of group 1BS-19b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: danya.gonchar.2017@gmail.com.

Vitalii Lukichov **–** PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, e-mail: lukichov.vitalyi@vntu.edu.ua.