Ковальчук І. В., магістрант,
Головня О. С., к.пед.н.,доцент,
Державний університет «Житомирська політехніка»

РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ ТА АНАЛІЗУ БЕЗПЕКИ НА ОСНОВІ SIEM ПЛАТФОРМИ GRAYLOG

Зростання загроз у галузі кібербезпеки та необхідність постійного моніторингу та аналізу інцидентів створюють потребу у вдосконаленні систем безпеки. Дослідження стану розробки проблеми в науково-практичних публікаціях підтверджує нестачу ефективних засобів моніторингу та аналізу безпеки, які б забезпечували повний огляд за потенційно небезпечною активністю у мережі та надійну ідентифікацію загроз.

У сучасній науці існують різноманітні підходи до вирішення проблем безпеки через SIEM платформи, але багато з них мають обмеження у швидкості обробки та аналізі великих обсягів даних, а також у складності налаштування та інтеграції з іншими системами [3].

SIEM (Security Information and Event Management) – це платформа для збору, аналізу та відображення даних з різних джерел для виявлення потенційних загроз безпеці. Використання SIEM підвищує ефективність виявлення та реагування на інциденти. Проте саме використання системи SIEM не гарантує повної надійності, але її наявність є ключовим індикатором чіткої політики кібербезпеки в організації. В більшості випадків кібератаки не залишають явних слідів, тому ефективніше використовувати журнали подій для виявлення загроз. Можливості управління журналами SIEM роблять їх центральним інструментом для забезпечення прозорості мережі.

Більшість програм безпеки зазвичай фокусуються на вирішенні проблеми менших загроз в масштабі мікрорівня, пропускаючи при цьому більшу картину кіберзагроз. Система виявлення вторгнень (IDS) рідко здатна надати більш широкий аналіз, ніж просто моніторинг пакетів та IP-адрес. Крім того, у журналах обслуговування фіксуються переважно лише сесії користувачів та зміни конфігурації. SIEM інтегрує ці системи та інші подібні до них, щоб забезпечити повний огляд будь-якого кіберінциденту через моніторинг у реальному часі та аналіз журналів подій [3].

Мета дослідження полягає в розробці та впровадженні інтегрованої системи моніторингу та аналізу безпеки на базі SIEM платформи Graylog, яка забезпечує централізований збір, агрегацію та аналіз журналів подій з усіх компонентів інформаційної системи.

Graylog – це відкрита та гнучка SIEM платформа, яка дозволяє збирати, аналізувати та візуалізувати дані з різних джерел, таких як логи, потоки даних тощо [1]. Вона надає широкі можливості налаштування та розширення, що робить її ідеальним вибором для розробки системи моніторингу та аналізу безпеки.

Розгортання Graylog складається з 3 компонентів:

1. Сервер Graylog.Він обслуговує веб-інтерфейс користувача/API і дає змогу взаємодіяти з Graylog. Від налаштування входів, сповіщень, індексів до інформаційних панелей.
2. Opensearch (раніше Elasticsearch). Opensearch – це місце, де фактично зберігаються та індексуються ваші журнали.
3. MongoDB. Використовується для зберігання метаданих Graylog.

Для нашого налаштування ми встановимо всі 3 компоненти на одному сервері, таким чином створивши одновузлове розгортання Graylog.

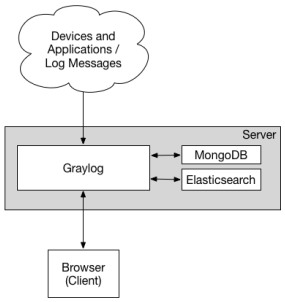

Рис. 1. Діаграма мінімального налаштування Graylog

Система моніторингу та аналізу безпеки на основі Graylog дозволяє ефективно виявляти та реагувати на потенційні загрози безпеки в реальному часі. Вона надає зручний інтерфейс для аналізу журналів подій, можливості створення складних запитів та гнучкі налаштування сповіщень.

Реалізація системи моніторингу та аналізу безпеки на основі SIEM платформи Graylog дозволяє підприємствам ефективно виявляти кіберзагрози та реагувати на них, зменшуючи час реакції на інциденти та підвищуючи загальний рівень безпеки інформації [2]. Практичне значення полягає в можливості застосування розробленої системи в організаціях будь-якого масштабу для підвищення рівня кібербезпеки та зменшення ризику інформаційних загроз.