Гнип М. В., магістрант гр. ІСТм-20-1,
Єфіменко А. А., канд. техн. наук, доцент,
зав. кафедри КІ та КБ
Державний університет «Житомирська політехніка»

ЗАГАЛЬНА ХАРАКТЕРИСТИКА СУЧАСНИХ ВІДКРИТИХ SIEM-СИСТЕМ

Інструменти SIEM (Security Information and Event Management) є невід'ємною частиною IT-налаштувань, які підтримують важливі бізнес-операції в сучасній цифровій економіці. Термін SIEM є комбінацією двох наступних практик в управлінні мережею та безпекою:

- SEM (управління подіями безпеки) – аналіз журналів і кореляція подій (часто в режимі реального часу) для протидії загрозам безпеки та інцидентам;
- SIM (управління інформацією про безпеку) – збір та керування журналами та звітність для внутрішніх аудитів або дотримання вимог.

SIEM або система управління інформацією та подіями безпеки, є фундаментальним елементом для забезпечення кібербезпеки. Програмне забезпечення SIEM дозволяє використовувати утиліти, необхідні для ефективного управління журналами, виявляє вторгнення, кореляцію подій, збір інформації про загрози, управління інцидентами, виконання стандартів відповідей та оцінки вразливості. Звичайно, різні інструменти SIEM будуть віддавати пріоритет варіативним функціям. Важливо, щоб користувач зрозумів основи SIEM, перш ніж вибрати інструмент, який він хоче використовувати. Незалежно від того, вирішить він встановити безкоштовну або платну програму SIEM, слід звернути увагу на наступні важливі фактори: виявлення вторгнень: ефективний підхід до виявлення вторгнень має вирішальне значення. Інструмент повинен відрізняти нешкідливі невдалі спроби входу від інтенсивних, симптоматичних атак. Ключовим моментом є аналіз даних у реальному часі; автоматичні інформування та оповіщення: SIEM рішення повинно попереджувати користувача про виникнення будь-яких проблем; ведення журналу подій допомагає виявити незвичайну активність у режимі реального часу та ретельно її дослідити; інтелектуальне виявлення загроз: SIEM рішення повинно бути здатним прогнозувати потенційні загрози, що вимагає порівняння інформації про останні загрози з поточними; зберігання та фільтрація даних: дані повинні зберігатися в архіві, щоб при необхідності на них можна було посилатися, інформуючи про подальші виявлення загроз. Ці дані повинні бути доступні для пошуку та фільтрації для того, щоб користувачі могли легко і швидко орієнтуватися; візуалізація даних може бути надзвичайно корисна для їх інтерпретації. Графіки, лічильники та кольорове кодування мають змогу миттєво надати користувачу представлення про те, що відбувається в системі; відповідні вимоги: завжди корисно мати програмне забезпечення SIEM, яке надає змогу забезпечити надання необхідних нормативних вимог; сумісність: програмне забезпечення SIEM має бути сумісним із наявною системою, оскільки тільки так воно дозволить користувачам мати всебічне представлення про поточні події.

Важливо відзначити, що інструменти та методи SIEM значно вдосконалилися за останнє десятиліття, розвиваючи свій функціонал у реагуванні на інциденти. Сьогодні багато передових інструментів SIEM використовують алгоритми машинного навчання або прогнозний статистичний аналіз, щоб проаналізувати більше даних за короткий час. Ці інструменти спрощують адміністрування IT-інфраструктури, пропонуючи не тільки детальну видимість корпоративних середовищ, але й надаючи ефективні інтелектуальні дані замість нескінченного потоку журналів і сповіщень.

Успішна стратегія SIEM – це досить дорога інвестиція. Це зумовлено тим, що управління SIEM є ресурсомістким процесом, який вимагає оптимальної продуктивності, оскільки без SIEM рішення система буде схильна до безлічі небезпек. Безкоштовні відкриті SIEM рішення можуть допомогти користувачеві у вирішенні даної проблеми не використовуючи фінансові ресурси. IT-фахівці всього світу діляться своїм досвідом щодо налаштування, що означає, що сам інструмент постійно розвивається. Але безкоштовні інструменти просто не здатні запропонувати повноцінне рішення корпоративного рівня SIEM.

Основна проблема відкритих SIEM-систем полягає в тому, що вони можуть бути вразливими і не зможуть виявити шахрайську активність. Ці програми зазвичай мають невеликий бюджет, тому вони менш зручні у використанні, ніж їх платні аналоги. Вони, зазвичай, вимагають більше зусиль і часу для підтримки їх нормального функціонування. Більше того, для використання відкритих SIEM-систем доведеться покладатися лише на свій досвід, оскільки користувач не матиме змогу зателефонувати у підтримку та отримати відповіді на свої запитання.