Ключові слова: відкриті українські ресурси, доступ до знань, цифрові трансформації, наукові дослідження, освіта, культура.

УДК: 004.77

Станіславчук Денис Олександрович
(наук. керівник – д-р техн. наук, професор Крижановський В. Г.)
Донецький національний університет імені Василя Стуса, м. Вінниця

ВИКОРИСТАННЯ КОНТЕКСТНОЇ ІНФОРМАЦІЇ ДЛЯ АНАЛІЗУ ЛОГІВ АГЕНТАМИ SIEM

Зі збільшенням загроз кібербезпеці та необхідністю захисту інформаційних ресурсів стає все актуальнішою роль SIEM-систем. Важливими інструментами для збору інформації про інформаційну систему є SIEM-агенти. Ця доповідь розглядає особливості, пов’язані з використанням контекстної інформації для фільтрації та пріоритезації логів, як це може покращити роботу SIEM.

Сьогодні інформація є найважливішим ресурсом людства. В сучасному світі, коли кількість інформації постійно зростає, захист і забезпечення безпеки інформації стає дедалі більш важливим завданням. З активним розвитком SIEM-систем попередні методи та структури застарівають. Це призводить до потреби розробки нових способів забезпечення певних функцій.

Мета доповіді – визначення проблем які виникають у разі недостатньої інформованості про процеси; огляд методів, які можуть покращити параметри системи за допомогою аналізу контекстної інформації.

SIEM-агенти – програмне забезпечення, яке збирає логи (журнали подій) та передає їх інструментам SIEM для аналізу. Їх основною особливістю є нормалізація – фільтрація та представлення логів у вигляді, який полегшить роботу інших SIEM-інструментів [1].

Однією з проблем, із якою доволі часто виникають проблеми під час роботи SIEM, є їх слабка інформованість про процеси корпоративної мережі. Під цим мається на увазі, що в мережі проходять важливі процеси, які, звісно ж, генерують логи з доволі високим пріоритетом. До таких подій належать: резервне копіювання, налаштування політик, тестування системи та ін. [2]. Збір та аналіз великої кількості таких логів може призвести до хибних спрацьовувань системи SIEM, яка буде змушена шукати проблему там, де її немає.

Для вирішення цієї проблеми можна використовувати збір та аналіз контекстної інформації, як-от типи користувачів, їх місцезнаходження, звичайні години активності та ін. Ця інформація дасть змогу збільшити точність аналізу та кореляції логів. Рекомендується використання цієї інформації для створення нових алгоритмів фільтрації логів та встановлення пріоритетів. Для реалізації цього пропонується два алгоритми: контекстуальна фільтрація [3] та пріоритезація за допомогою індексу довіри Демпстера–Шафера [4].

Перший алгоритм добре підходить для виділення основних подій, які відбуваються в системі. Він працює приблизно таким чином: зібрані логи збираються в так звані чанки. Так, чанк L_i містить певну частину логів з інтервалу часу P_i (P_i =10 с у прикладі, може набувати різних значень). Далі цей фрагмент передається для фільтрації, яка виділяє основну інформацію з нього. Наступним йде токенайзер, який створює набір пар подія-кількість подій. Вже на основі цих пар виконується оцінювання подій за допомогою методу логарифмічної ентропії.

Другий алгоритм виконує розстановку пріоритетів за допомогою оцінки загрози та індексу довіри. Оцінка загрози – це значення ймовірності реалізації загрози та вартість збитків, яких вона здатна завдати. Індекс довіри – значення, яке обраховується на основі аналізу поведінки джерела логів на поточний момент, до звичайної поведінки. Кількісну оцінку для подальшого призначення пріоритетів можна звести до такої формули:

$$P_i = A * (1 - I_i),$$

де, P_i – кількісна оцінка певної події, A – оцінка можливої загрози, I_i – відношення нинішнього стану системи (час, місце тип користувача) до звичайного стану.

Висновки. Контекстна інформація дає змогу встановити нові правила фільтрації та встановлення пріоритету логів, що допомагає краще розподілити ресурси системи, зменшивши кількість непотрібних глибоких перевірок та фальшивих спрацювань сповіщень безпеки.

Список використаних джерел

1. Dorigo S. Radboud University Nijmegen Security Information and Event Management Master Thesis, 2012.

2. Bhatt S., Manadhata P., Zomlot L. The Operational Role of Security Information and Event Management Systems. Security & Privacy, IEEE. 2014. № 12. P 35–41.

3. Cinque M., Della Corte R., Pecchia A. Contextual filtering and prioritization of computer application logs for security situational awareness. *Future Generation Computer Systems*. 2019. № 111. P. 668–680.

4. Prioritizing intrusion analysis using Dempster-Shafer theory / L. Zomlot, S. C. Sundaramurthy, K. Luo, X. Ou, S. Rajagopalan. *Proceedings of the ACM Conference on Computer and Communications Security,* 2011. October 2011. P. 59–70.

Анотація. Використання контекстної інформації для аналізу логів агентами SIEM сприяє покращенню їх роботи. Розглянуто проблеми, пов'язані з нестачею інформації про процеси корпоративної мережі, та запропоновано методи вирішення через аналіз контексту. Зокрема, розглянуто алгоритми контекстуальної фільтрації та пріоритезації з використанням індексу довіри Демпстера–Шафера. Такий підхід дає змогу оптимізувати роботу системи шляхом зменшення непотрібних перевірок та фальшивих спрацювнь сповіщень безпеки.

Ключові слова: аналіз контекстної інформації, безпека.