УДК 004.7

Адамчук Р.С., здобувач
Дячук О. Ю., ст. викладач
Державний університет «Житомирська політехніка»

ПРОГРАМНА ПІДСИСТЕМА ГЕНЕРАЦІЇ, МОНІТОРИНГУ ТА АНАЛІЗУ ПОДІЙ КІБЕРБЕЗПЕКИ НА ОСНОВІ ЛОГІВ МЕРЕЖЕВОГО ОБЛАДНАННЯ CISCO

У сучасних інформаційно-комунікаційних системах мережеве обладнання є одним із ключових джерел подій кібербезпеки [1], оскільки саме воно фіксує спроби несанкціонованого доступу, збої інфраструктури та аномалії продуктивності. Проте експоненційне зростання обсягів журнальних даних (Syslog) призводить до проблеми інформаційного шуму, що ускладнює оперативне виявлення критичних інцидентів [7] та збільшує середній час реагування (MTTR).

Метою даної роботи є розробка програмної підсистеми генерації, моніторингу та кореляційного аналізу подій кібербезпеки на основі Syslog-повідомлень мережевого обладнання Cisco [3]. Підсистема реалізує гібридну модель аналізу, що поєднує текстові події журналювання з числовими метриками продуктивності та логікою кінцевого автомату. Експериментальна апробація підтвердила ефективність підходу щодо зменшення інформаційного шуму та підвищення достовірності виявлення інцидентів.

Запропонована підсистема спрямована на аналіз великих обсягів журнальних даних мережевого обладнання Cisco [2]. На відміну від традиційних підходів, що розглядають Syslog-повідомлення ізольовано, рішення формує логічні інциденти у часовому контексті.

Програмна реалізація виконана мовою Python та включає модуль генерації подій, аналітичне ядро оброблення логів і інтерактивний інтерфейс моніторингу.

Для обробки Syslog-повідомлень реалізовано алгоритм парсингу на основі регулярних виразів, що забезпечує автоматичне виділення часових міток, типів подій та тексту повідомлень [4].

Рисунок 1 – Приклад фрагменту коду Python

Підсистема працює у потоковому режимі, що дозволяє аналізувати події у процесі їх надходження та відображати актуальний стан системи.

У межах дослідження розроблено програмний генератор Syslog-повідомлень, який імітує роботу маршрутизаторів та комутаторів Cisco. Генератор формує як фонові інформаційні повідомлення, так і детерміновані сценарії інцидентів, що складаються з послідовності взаємопов’язаних логів.

Особливістю є інтеграція метрик продуктивності безпосередньо у Syslog-повідомлення, що дозволяє одночасно обробляти текстові події та числові показники без зовнішніх джерел даних [6].

Якість та достовірність генерації логів підтверджено експериментально. На рис. 2 наведено приклади синтетичної достовірності згенерованих повідомлень, що відповідають реальним Syslog-повідомленням Cisco.

Рисунок 2 – Приклади синтетичної достовірності генерації логів

Центральним елементом підсистеми є аналітичне ядро, яке реалізує алгоритми парсингу, класифікації та кореляції подій. Ключовим архітектурним рішенням є використання гібридного кінцевого автомату (FSM), що керує життєвим циклом інцидентів.

Використання FSM забезпечує стабільність статусів інцидентів шляхом переходу між станами лише за умов повторюваності або тривалості подій, що зменшує кількість хибно-позитивних спрацювань [5].

Наукова новизна полягає у поєднанні кореляційного аналізу Syslog-подій з моделлю кінцевого автомату для формування стабільних логічних інцидентів у реальному часі.

Стан системи під час розвитку критичного інциденту наведено на рис. 3, де відображено одночасно:

- текстові Syslog-повідомлення;
- критичний стан FSM;
- пікові значення завантаження CPU.

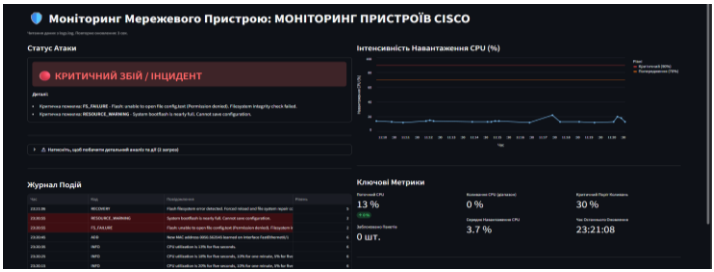

Рисунок 3 – Стан системи під час критичного інциденту

Однією з ключових переваг розробленої підсистеми є реалізація кореляційної візуалізації, яка поєднує логічний та ресурсний стани мережевого пристрою. Оператор отримує можливість в одній точці інтерфейсу зіставити причину інциденту та його вплив на продуктивність.

Окрім виявлення інцидентів, система формує підказки щодо можливих дій з їх усунення. На рис. 4 наведено приклад інтерфейсу з рекомендаціями для адміністратора, які формуються на основі типу події та її контексту.

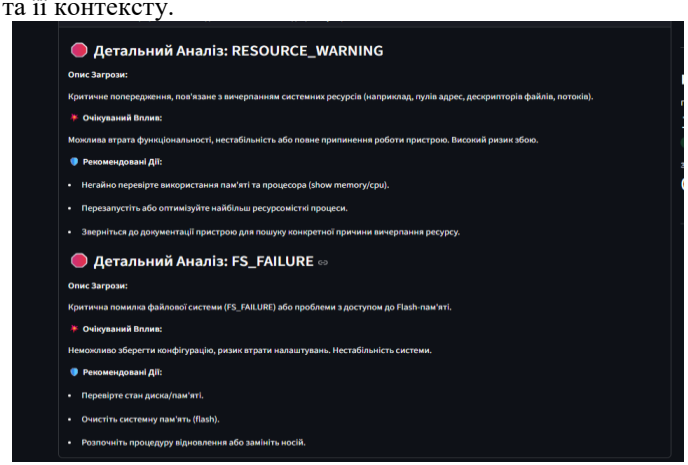

Рисунок 4 – Інтерфейс аналізу інцидентів та рекомендацій для реагування

Запропонований підхід скорочує час реагування та знижує когнітивне навантаження на оператора.

Апробація розробленої підсистеми проводилася на серії змодельованих сценаріїв, що охоплювали нормальну роботу мережі, агреговані атаки типу brute force та критичні перевантаження ресурсів. У ході тестування підтверджено коректність:

- генерації подій;
- агрегації однотипних логів;
- кореляції подій і метрик;
- переходів FSM між станами.

Результати експериментів свідчать про зменшення кількості відображених подій та підвищення інформативності моніторингу.

Подальший розвиток розробленої програмної підсистеми доцільно спрямувати на розширення підтримуваних типів Syslog-повідомлень мережевого обладнання Cisco, зокрема шляхом охоплення повного спектра системних, безпекових та сервісних логів, визначених у офіційній документації виробника. Це дозволить підвищити повноту охоплення подій та забезпечити більш точну кореляцію інцидентів у складних мережевих середовищах. Окрім цього, перспективним напрямом є адаптація підсистеми для аналізу логів мережевого обладнання інших виробників (Juniper, MikroTik, Huawei тощо), що забезпечить уніфікований підхід до моніторингу подій кібербезпеки в мультивендорних інфраструктурах та розширить практичну застосовність запропонованого рішення.

Розроблене рішення має практичну цінність та може бути використане як самостійний інструмент моніторингу або як модуль у складі корпоративних систем безпеки. Важливою перевагою є те, що підсистема не обмежується лише середовищем моделювання і може бути у будь-який момент інтегрована з реальним мережевим обладнанням без необхідності суттєвих змін архітектури, забезпечуючи коректну роботу в умовах реальної інфраструктури.

Список використаних джерел

1. Cisco Systems. System Message Logging (Syslog). URL: https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.htm
2. He S., Zhu J., He P., Lyu M. R. A Survey on Automated Log Analysis for Reliability Engineering. arXiv. 2020. URL: https://arxiv.org/abs/2009.07237
3. RFC 5424. The Syslog Protocol / ed. by R. Gerhards. Internet Engineering Task Force (IETF), 2009. 39 p. URL: https://datatracker.ietf.org/doc/html/rfc5424
4. Cisco IOS Syslog Messages Explained. NetworkLessons. URL: https://networklessons.com/system-management/cisco-ios-syslog-messages
5. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST SP 800-94. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf
6. He P., Zhu J., Zheng Z., Lyu M. R. Drain: An Online Log Parsing Approach with Fixed Depth Tree // 2017 IEEE International Conference on Web Services (ICWS). 2017. P. 33–40. URL: https://jiemingzhu.github.io/pub/pjhe_icws2017.pdf
7. OWASP Foundation. A09:2021 Security Logging and Monitoring Failures. URL: https://owasp.org/Top10/2021/A09_2021-Security_Logging_and_Monitoring_Failures/