РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ МЕРЕЖЕВОЇ АКТИВНОСТІ З ВИКОРИСТАННЯМ ELK STACK

Шмагун В.І., Балагура Д.С., Смірнов А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Моніторинг мережевої активності відіграє ключову роль у забезпеченні інформаційної безпеки та ефективному управлінні мережевими ресурсами. У сучасних інформаційних системах, де постійно збільшується обсяг переданих і оброблюваних даних, необхідно використовувати потужні інструменти для збору, аналізу та візуалізації інформації. Одним із найбільш ефективних рішень для таких задач є стек ELK (Elasticsearch, Logstash, Kibana) [1]. Його використання дає змогу централізовано збирати журнали подій з різних джерел, обробляти їх у реальному часі, а також аналізувати отримані дані для виявлення загроз і аномалій. Гнучка архітектура дозволяє адаптувати систему під конкретні потреби організації та масштабувати її відповідно до зростання навантаження. Використання ELK Stack вимагає імплементації та впровадження певного процесу, який забезпечить всі етапи моніторингу мережевої активності. Так, на першому етапі розгортання ELK Stack необхідно налаштувати збір даних. Для цього використовуються агенти, такі як Filebeat або Winlogbeat, які дозволяють отримувати логи з серверів, мережевого обладнання та інших джерел. Наступним етапом після збору даних є їх обробку за допомогою Logstash або Ingest Pipelines в Elasticsearch. На цьому етапі застосовуються фільтри для нормалізації, розбору та збагачення логів додатковою інформацією. На третьому етапі відбувається аналіз отриманих даних. Аналіз здійснюється в Elasticsearch, який дозволяє виконувати швидкий пошук та виявляти закономірності в мережевій активності. Використання Kibana дає змогу створювати інтерактивні дашборди для візуалізації ключових показників безпеки. Це дозволяє адміністраторам швидко виявляти підозрілі дії та оперативно реагувати на потенційні загрози.

Ефективність моніторингу можна підвищити за рахунок використання машинного навчання для виявлення аномалій у поведінці користувачів та мережевого трафіку. Вбудовані можливості Machine Learning в Elasticsearch дозволяють автоматично визначати відхилення від нормальної поведінки та генерувати сповіщення у разі виявлення підозрілих активностей.

Метою доповіді є аналіз особливостей впровадження ELK Stack у корпоративне середовище, визначення типових викликів, що пов’язані з обробкою великих обсягів логів, їх аналізом, проблемами візуалізації результатів задля ефективного реагування з боку адміністраторів, та надання пропозицій щодо підходів для оптимізації та підвищення ефективності на кожному етапі роботи системи моніторингу.

Список літератури

1. Brown T., Wilson P. Advanced log analysis techniques in Elasticsearch. Network Security Review. 2021. Vol. 6, No. 2. P. 89–95.