УДК 004.056

А. А. Гук

СИСТЕМИ МОНІТОРИНГУ МЕРЕЖ НА ОСНОВІ ELK STACK

Вінницький національний технічний університет

Анотація
Розглянуто систему моніторингу мереж на основі Elastic Stack.
Ключові слова: кібербезпека, мережа, elastic, моніторинг інформаційної безпеки.

Abstract
The network monitoring system based on Elastic Stack is considered.
Keywords: cybersecurity, network, elastic, information security monitoring.

Для запровадження якісної системи моніторингу мереж існує безліч причин. Моніторинг мережі надає інформацію, необхідну мережевим адміністраторам для підтвердження оптимальної роботи мережі. За допомогою таких інструментів, як програмне забезпечення для моніторингу мережі, адміністратори можуть заздалегідь виявляти неполадки, підвищувати ефективність і т.д. [1]. Є багато інструментів для цього, одним з яких є ELK Stack, що допомогає при збиранні та обробці логів.

ELK Stack — це інструмент, що якраз дозволяє виконувати ці всі функції. Складається він з продуктів з відкритим кодом, а саме Elacticsearch, Logtash та Kibana, що показано на рис. 1.

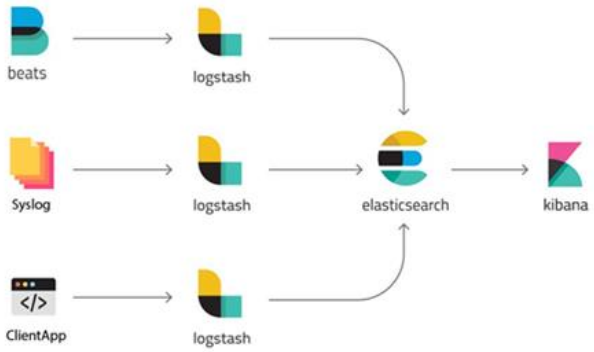

Рисунок 1 – Схема ELK Stack

Logstash - це утиліта для обробки логів подій з різних джерел, за допомогою якої можна виділити поля і їх значення в повідомленні, також можна налаштувати фільтрацію і редагування даних [2]. Після всіх маніпуляцій Logstash перенаправляє події в кінцеве сховище даних. Утиліта налаштовується тільки через конфігураційні файли. Джерелами можуть слугувати як стандартні сервіси операційної системи , такі як syslog, так і спеціальні “Beats”- набір програм-колекторів даних з низькими вимогами до ресурсів, які встановлюються на клієнтських пристроях для збору системних журналів і файлів. Beats-ів є дуже багато, для прикладу Filebeat, Metricbeat, Packbeat, Winlogbeat, Auditbeat та інші [3]. Навіть якщо потрібний знайти не вдалось — його можна написати власноруч.

Elasticsearch - це добре підходить для моніторингу мереж, адже з його допомогою можна зручно фільтрувати логи за необхідними параметрами, та здійснювати висновки відповідно них

Elasticsearch є нереляційним сховищем (NoSQL) документів у форматі JSON, і пошуковою системою на базі повнотекстового пошуку Lucene. Апаратна платформа - Java Virtual Machine, тому системі потрібна велика кількість ресурсів процесора і оперативної пам'яті для роботи.

Elasticsearch грає роль ядра всієї системи, поєднуючи функції бази даних, пошукового і аналітичного движків. Швидкий і гнучкий пошук забезпечується за рахунок аналізаторів тексту, нечіткого пошуку, підтримки східних мов [4].

Кожне повідомлення, що надходить, як з Logstash так і за допомогою API запиту, індексується як "документ" - аналог таблиці в реляційних SQL. База досить схожа на Mongo DB.

Вся робота з базою даних будується на JSON запитах за допомогою REST API, ,що дозволяє

додавати, переглядати, модифікувати і видаляти дані в форматі: питання - відповідь. Для того щоб всі відповіді на запити візуалізувати була написана Kibana, яка вдає із себе веб сервіс.

Kibana дозволяє шукати \ брати дані і запитувати статистику з бази даних elasticsearch, на основі відповідей будуються безліч красивих графіків і дашбоардів. Також система має функціонал адміністрування бази даних elasticsearch. Приклад дашбоарду зробленого задопомогою Kibana зображено на рис. 2 [5].

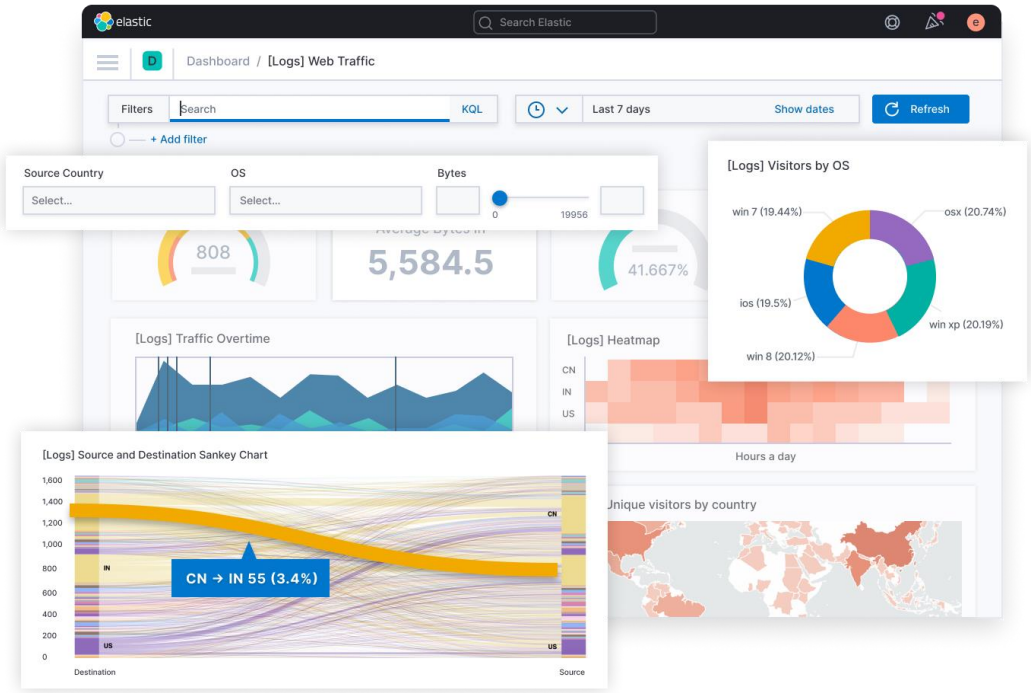

Рисунок 2 – Дашбоард Kibana

Висновки

Таким чином, при потребі створення системи моніторингу мереж, ELK stack є дуже гарною допоміжною утилітою, адже він є безкоштовним продуктом з відкритим кодом, а отже з безліччю можливостей кастомізації та має майже повний список інструментів для обробки результатів моніторингу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Что такое мониторинг сети?: веб-сайт. URL: https://www.cisco.com/c/ru_ru/solutions/automation/what-is-network-monitoring.html#~%D0%9F%D1%80%D0%B5%D0%B8%D0%BC%D1%83%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B0 (дата звернення: 04.03.2021)
2. Elastic stack: анализ security логов. Введение: веб-сайт. URL: https://habr.com/ru/company/tssolution/blog/480570/ (дата звернення: 04.03.2021)
3. What are Elasticsearch Beats?: A survey: веб-сайт. URL: https://www.objectrocket.com/resource/what-are-elasticsearch-beats/ (дата звернення: 04.03.2021)
4. 3 товарища в поиске и аналитике Big Data: Elasticsearch, Logstash и Kibana: веб-сайт. URL: https://www.bigdataschool.ru/blog/what-is-elk.html (дата звернення: 04.03.2021)
5. Kibana: Explore, Visualize, Discover Data | Elastic: веб-сайт. URL: https://www.elastic.co/kibana (дата звернення: 04.03.2021)

Гук Андрій Андрійович – студент групи 1БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: guk.and00@gmail.com

Guk Andrii A. — Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : guk.and00@gmail.com