УДК 621.3.06
Підлипський Р. – ст. гр. КН-41
Західноукраїнський національний університет

ПРОГРАМНИЙ МОДУЛЬ АНАЛІЗУ ФАЙЛІВ ЛОГУВАННЯ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Науковий керівник: к.т.н. Майків І.М.

Pidlipskyi R.
West Ukrainian National University

SOFTWARE MODULE FOR ANTIVIRUS SOFTWARE LOG FILES ANALYSIS

Supervisor: Ph.D. Maikiv I.M.

Ключові слова: кібербезпека, файл логування, виявлення загроз, реальний час.
Keywords: cybersecurity, log file, threat detection, real time.

Одним із головних аспектів кібербезпеки [1] є вчасне виявлення потенційних загроз, до того як вони призведуть до шкоди. Кібератаки можуть мати різний характер, тому організації потребують комплексного підходу до їх виявлення та запобігання. Важливим джерелом інформації для завчасного виявлення потенційних загроз є файли логування антивірусного програмного забезпечення (ПЗ), які містять в собі багато корисної інформації про події які відбуваються в мережі або на конкретному пристрої.

Тому, розроблення програмного модуля для аналізу файлів логування є актуальною задачею. Призначення такого модуля - вчасно розпізнати потенційні загрози, будь-які несанкціоновані дії в мережі або пристрої та вчасно повідомити про це відповідальну особу для усунення усіх можливих загроз.

Програний модуль (ПМ) реалізовано по технології Elastic Stack (ELK). Це ефективний набір технологій [2], який забезпечує централізований збір даних, їх перетворення у зрозумілий формат з можливістю подальшого представлення у вигляді графіків та таблиць, що дозволяє бачити процеси які відбуваються у системах та швидко знаходити потрібну інформацію. Структурна схема ПМ наведена на рис. 1.

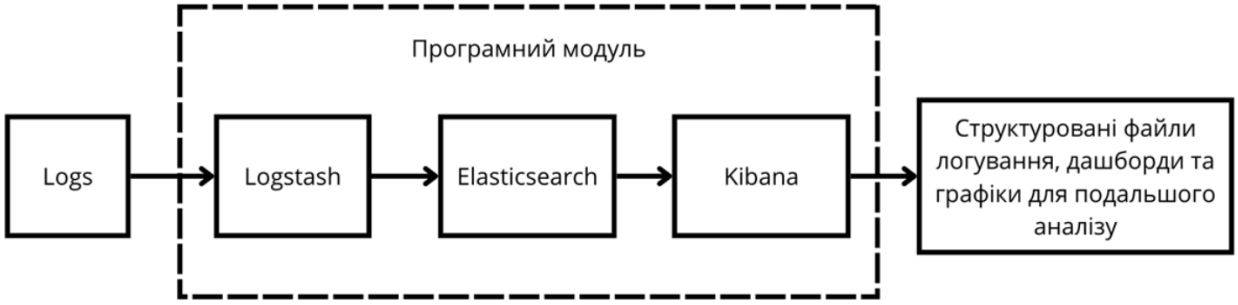

Рисунок 1 – Структура програмного модуля для аналізу файлів логування

ПМ складається із 3 основних модулів: 1) Logstash [3] - інструмент для збору, опрацювання та трансформації файлів логування; 2) Elasticsearch - ефективний пошуковий та аналітичний механізм, який зберігає та індексує великі обсяги даних; 3) Kibana [4] – інтерфейс, призначений для візуалізації даних, які зберігаються в

Elasticsearch. Він дозволяє користувачам створювати графіки, діаграми, панелі моніторингу та проводити аналіз даних в реальному часі.

Програмний модуль реалізований та протестований з використанням різних типів файлів логування. На рис. 2 наведено приклад дашборда, який створений за допомогою Kibana для візуалізації інформації з файлів логування.

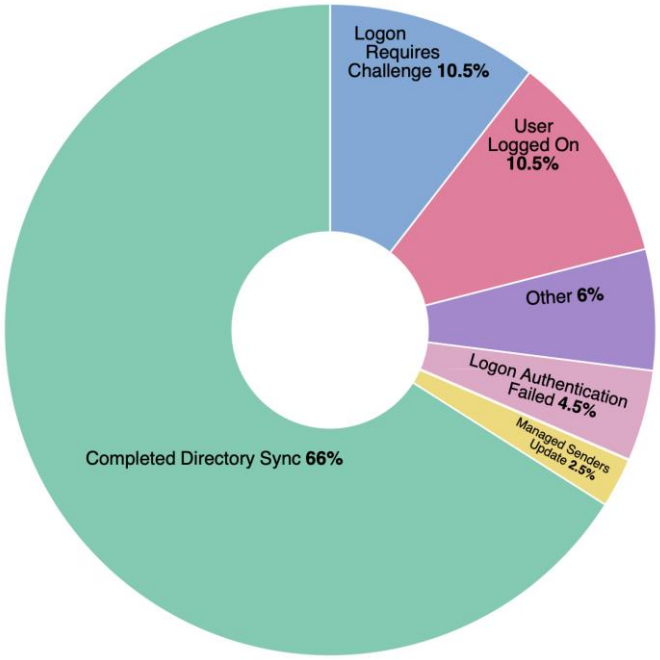

Рисунок 2 – Дашборд для подальшого аналізу файлів логування

Кругова діаграма відображає розподіл подій, де найбільша частка (66%) припадає на успішне завершення синхронізації директорії. Успішна аутентифікація користувача ("User Logged On", 10.5%) значно перевищує невдалу спробу ("Logon Authentication Failed", 4.5%), вказуючи на високий рівень успішних входів до системи.

При виявленні таких загроз [2] програмний модуль може автоматично створювати звіти або ж направляти сповіщення в системи реагування на інциденти, що дозволяє оперативно вживати заходів для зупинки загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Peltier, J. Cybersecurity Essentials**.** - Wiley, 2019. – 400 p.
2. Gormley C, Tong Z. Elasticsearch. The Definitive Guide. - O'Reilly Media, 2015 – 412 p.
3. Smith J., Anderson M. Logstash: The Complete Guide. O'Reilly Media, 2017. - 350 p.
4. Chesnay, L. Kibana Essentials. Packt Publishing, 2016. – 320p.