УДК 681.12

І. Д. Лазуренко
О. П. Войтович

СИСТЕМА УПРАВЛІННЯ ЛОГАМИ «GRAYLOG»

Вінницький національний технічний університет

Анотація

Аналіз існуючих систем керування логами в задачах кібербезпеки, що дозволяє зробити більш ефективним прийняття рішень що пошуку, обробки та формування звітності щодо подій відповідно до керування інцидентами кібербезпеки.

Ключові слова: кібербезпека, керування інцидентами, системи керування логами, системи SIEM, система GrayLog.

Abstract

Analysis of existing log management systems in cybersecurity tasks, which allows for more effective decision-making about search, processing and reporting of events in accordance with cybersecurity incident management.

Keywords: cyber security, incident management, log management systems, SIEM systems, GrayLog system.

Вступ

У сучасному світі питання комп'ютерної безпеки займає одну з найважливіших ланок, яка наявна на будь якому підприємстві, сайті або звичайних домашніх комп'ютерах. Для запобігання несанкціонованого втручання чи підозрілої поведінки у системі, бажано слідкувати за усіма подіями, що відбуваюсь в середині неї. SIEM – це програмне забезпечення для захисту, що дає організаціям змогу детально відстежувати події у всій корпоративній мережі й реагувати на загрози ще до того, як вони зможуть завдати шкоди [1].

Метою роботи є ознайомитись з принципами управління логами за допомогою системи GreyLog, та його імплементації у систему керування інцидентами інформаційної та кібербезпеки..

Результати дослідження

Для SIEM найбільш важливою функцією є аналіз середовища в режимі реального часу. Такий механізм дає змогу виявити загрози до того як вони вплинуть на основні процеси в середовищі. Як реалізацію механізму спостереження за подіями в реальному часі були створені логи, котрі являють собою системну інформацію про роботу сервера, комп'ютера чи дій користувача або програм в мережному середовищі.

Логи необхідні для протоколювання інформації, після чого адміністратор опрацьовує цю інформацію і робить висновки щодо коректної роботи системи.

Опрацювання великої кількості логів займає досить велику кількість часу, оскільки всі вони зберігаються в окремих папках, та постійно змінюються, що значно ускладнює їх аналіз. Саме для цього використовуються сторонні програмні засоби для підвищення ефективності роботи з логами, однією з цих програм є система GrayLog.

GrayLog – це платформа для опрацювання логів з відкритим кодом [2]. До його переваг можна віднести можливість відправки повідомлень різними способами. Таку можливість надає підтримка спеціального формату GELF (Graylog extended log format), який підходить для логування з інших додатків. Логи в такому форматі можуть бути відправлені по TCP, UDP, HTTP та AMQP. Також GrayLog має низку пакетів для взаємодії з сучасними мовами програмування такими як: Python, PHP, Golang, JavaScript, C#.

Аналіз інформаційних джерел показав, що серед програм-аналогів можна визначити низку таких додатків: Grafana Loki [3], ElasticSearch + Logstash + Kibana (ELK-стек) [4].

Grafana – програмна система візуалізації даних, орієнтована дані систем IT-моніторингу. Реалізована як веб-додаток у стилі панелей з діаграмами, графіками, таблицями, попередженнями. Як недоліки в порівнянні з GrayLog можна виділити меншу кількість потоків даних, меншу кількість вхідних форматів даних та меншу кількість можливих розширень [3].

ELK-стек - найчастіше іменований ElasticSearch, надає можливість збирати журнали всіх систем і програм, аналізувати їх і створювати візуалізації, щоб слідкувати за програмами та інфраструктурою, швидше усувати проблеми, аналізувати систему безпеки та багато іншого. У порівнянні з GrayLog, ELK-стек є більш гнучким та має ширший функціонал, але процес налаштування цього додатку складніше та потребує більш детального розуміння його окремих компонентів [4].

Було проведено аналіз програмної складової системи GrayLog [5], а саме: ознайомлення з інтерфейсом програми, її функціоналом та проведено базові налаштування.

Як переваги у застосуванні додатків для управління логами можна визначити:

1. Значно менші затрати часу на пошук необхідної інформації.
2. Можливість фільтрації інформації за певними критеріями, таким як: час, ключові слова чи назва запису.
3. Можливість створення звітів.
4. Можливість налаштування оповіщень при виникненні помилок чи інших подіях та інцидентах.

Протягом підготовки фахівців з кібербезпеки важливим є розуміння та обробка подій в реальному часі є досить значною. Ознайомитись з поняттям «лог» та вміння їх обробляти чи розуміти буде корисно, як для системних адміністраторі, так і для програмістів, що займаються питанням кібербезпеки. Дана тема є актуальною, оскільки будь який сервіс веде звітність про події, що відбуваються в середині, а можливість розуміти, що саме відбувається, дасть змогу виявити підозрілі події та усунути їх завчасно.

Для практичного освоєння цієї теми рекомендується встановити віртуальну машини з операційною системою Ubuntu, розвернути на ній сервер та клієнт, з якими буде працювати GrayLog. Виконати підключення додатку та ознайомитись на практиці з можливими типами фільтрації логів. Спробувати налаштувати попередження по електронній пошті при виявлення певних подій, наприклад порушень периметру. Спробувати провести несанкціоновані дії створивши нового клієнта, котрий буде втручатись в роботу сервера.

Висновки

В ході дослідження було встановлено, що використання системи GrayLog як системи SIEM для сканування та аналізу логів підвищує продуктивність, зменшую кількість затраченого часу на обробку інформації та підвищую швидкість виявлення інцидентів у системі. Таким чином, при використанні засобів для обробки подій можна запобігти виникнення великої кількості інцидентів кібербезпеки, поки вони не нанесуть великої шкоди мережного середовищу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке SIEM? Електронний ресурс [URL]. — https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem (06.03.2023).

2. Технічна документація по Graylog. Електронний ресурс [URL]. — https://go2docs.graylog.org/5-0/what_is_graylog/what_is_graylog.htm (06.03.2023).

3. Grafana, програмне забезпечення з відкритим кодом. Електронний ресурс [URL]. — https://ubunlog.com/uk/нагляд-за-аналізом-програмного-забезпечення-grafana/ (07.03.2023).

4. ELK-стек для чого? Електронний ресурс [URL]. — https://1devops.tech/elk-stack/ (07.03.2023).

5. Graylog Extended logging Format. Електронний ресурс [URL]. — https://docs.docker.com /config/containers/logging/gelf/

Лазуренко Іван Дмитрович **—** студент групи 1БС-21МС, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: lazurenko.iw@gmail.com

Науковий керівник: ***Войтович Олеся Петрівна*** — к-т техн. н., доцент, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Lazurenko Ivan Dmitrovich **—** student of group 1BS-21MS, Faculty of Information Technologies and Computer Engineering, Vinnitsa National Technical University, Vinnitsa, e-mail: lazuren-ko.iw@gmail.com

Academic supervisor: ***Voytovych Olesya Petrivna*** — PhD, Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia.