УДК 004.77 (045)

О. П. Якімов[1]
О. П. Войтович[1]

ELASTICSEARCH ЯК ОПТИМАЛЬНЕ РІШЕННЯ ПОШУКУ ТА АНАЛІЗУ ПОДІЙ КІБЕРБЕЗПЕКИ У РЕЖИМІ РЕАЛЬНОГО ЧАСУ

[1] Вінницький національний технічний університет

Анотація

В цій доповіді запропоновано оптимальний метод збору та аналізу даних на основі використання сучасних інструментів для аналізу подій кібербезпеки. Змодельовано середовище з використанням одного з інструментів проаналізовано аналоги та зроблено висновки.

Ключові слова: пошук, аналіз, інформація, пошуковий двигун, ElasticSearch, кібербезпека.

Abstract

This report proposes an optimal method of data collection and analysis based on the use of modern tools for analyzing cyber security events. The environment was simulated using one of the tools, analogues were analyzed and conclusions were drawn.

Keywords: search, analysis, information, search engine, ElasticSearch, cybersecurity.

Вступ

Дуже складно уявити сучасному світ без інформаційних технологій, вони посіли та займають ключове місце в нашому житті. Їх можна побачити як у повсякденному житті людей, так і у бізнесі, навчанні та роботі. З цього випливає одне із важливих завдань - забезпечення безпеки цих технологій. Останні роки показали, що кібератаки стали серйозною загрозою для не тільки для підприємств, а для цілих держав та їх громадян. В цьому контексті, дослідження проблем кібербезпеки постає дуже актуальним та важливим завданням. У зв'язку з цим, важливо забезпечити ефективний захист інформації від потенційних загроз безпеки, і тому важливо дослідити різні інструменти, які дозволяють ефективно забезпечувати її безпеку.

Метою роботи є розроблення методу для обробки даних, їх індексація, пошук ключової інформації на основі яких буде впроваджуватись захист системи.

Результати дослідження

В ході дослідження було розглянуто сучасні тенденції кібербезпеки та атаки на підприємства. Було визначено, що більша частка атак в першій світовій кібервійні припала саме на атаки на відмову в обслуговуванні. Відповідно до даних CyberPeace Institute, з 1100 проаналізованих кібератак майже 80% припали на DDoS-атаки. Фахівці організації також підкреслюють, що досить складно зрозуміти справжні масштаби впливу кібероперацій на життя людей і чи є цей вплив помітним. [1].

В цих умовах, а також враховуючи вимоги міжнародних стандартів, однією з важливих засобів захисту інформації стає впровадження систем управління інформаційною безпекою та подіями безпеки - SIEM (Security information and event management) [2] [3]. Така система дозволяє виконувати та обробляти чимало задач, вона призначена для збору, аналізу та інтерпретації даних про події в системах безпеки в реальному часі. Головною метою SIEM є забезпечення захисту інформації та мережі, виявлення та реагування на потенційні загрози безпеки, включаючи кібератаки, витоки даних, шкідливі програми та інші загрози.

Отже, для попередження наступних атак на систему потрібно забезпечити її швидким реагуванням, що грунуються на швидкому логувані та аналізі цих даних. Під час роботи в мережі, генерується велика кількість логів, які містять цінну інформацію про події, які відбуваються в системі. Ці логи можуть містити важливі дані про вторгнення, спроби атак та інші події, які можуть призвести до по-

рушення безпеки системи.

Однак, збір та аналіз цих логів може бути складним завданням, особливо у випадку великих обсягів даних.

Проаналізувавши сучасний ринок в пошуку подібних рішень, було визначено ряд інструментів, які можна використовувати для забезпечення цього аспекту кібербезпеки. Такими інструментами стали Splunk, LogRhythm, ArcSight [4]. На таблиці 1 було представлено інструмент, його опис, переваги та недоліки.

Таблиця 1 - Сучасні інструменти

Інструмент	Опис	Переваги	Недоліки
Elasticsearch	Потужний інструмент для зберігання та пошуку логів, моніторингу трафіку та виявлення інцидентів. Має інтуїтивно-зрозумілий інтерфейс, що допомогає з легкістю знайти та організовувати дані.	– Швидкість пошуку та аналізу даних; – Інтеграція з іншими інструментами безпеки; – Можливість масштабування зберігання даних; – Підтримка гнучкої структури даних.	– Потребує високої кваліфікації для налагодження та налаштування; – Вимоги до обладнання для масштабування можуть бути високими; – Потребує витрат на ліцензію та підтримку.
Splunk	Платформа збору та аналізу даних, яка включає інструменти моніторингу, аналізу логів та безпеки. Має зручний інтерфейс, проте на початку можуть виникнути складнощі, так як має великий вибір функцій та можливостей.	– Потужні інструменти аналізу даних; – Широкий функціонал для моніторингу та безпеки; – Легкий в розгортанні та налаштувані.	– Вимоги до обладнання можуть бути високими; – Вимагає високої кваліфікації для налагодження та налаштування; – Потребує витрат на ліцензію та підтримку.
LogRhythm	Платформа для безпеки та аналітики, яка забезпечує збір та аналіз логів, моніторинг вмісту, інтеграцію з вузлами безпеки та інші функції. Має простий та легкий інтерфейс, що покращує його використання навіть новачками.	– Розширені можливості аналізу та виявлення відхилень; – Можливість автоматичного реагування на загрози безпеки; – Інтеграція з іншими системами безпеки	– Висока вартість ліцензування; – Обмежені можливості розширення та модифікації системи
ArcSight	Платформа для безпеки, яка дозволяє збирати та аналізувати дані з різних джерел для виявлення загроз безпеці. Виглядає застаріло посеред своїх конкурентів та вимагає часу щоб його освоїти.	– Розширені можливості моніторингу та аналізу даних; – Можливість інтеграції з іншими системами безпеки	– Висока вартість ліцензування; – Складна установка та конфігурування; – Складний інтерфейс користувача

Отже, проаналізувавши широке коло інструментів було вирішено обрати Elasticsearch. Це потужний інструмент для зберігання та пошуку логів, який дозволяє швидко знаходити та аналізувати дані. Elasticsearch може зберігати логи в режимі реального часу, що дозволяє оперативно реагувати на події та виявляти потенційні загрози для безпеки системи [5]. В ході дослідження цього інструменту було виявлено, що за його допомогою можна шукати інформацію в будь-яких типах файлів, що є суттєвою перевагою для аналізу багатьох джерел та подальшої обробки цієї інформації.

Обравши інструмент можемо приступити до моделювання середовища для аналізу даних. Для того, щоб запустити сервер з Elasticsearch для зберігання та пошуку логів, моніторингу трафіку та виявлення інцидентів необхідно виконати такі кроки: встановити Elasticsearch на сервері та налаштувати

його, налаштувати мережу для збору даних та передачі їх на сервер з Elasticsearch, налаштувати моніторинг трафіку та збір логів на пристроях мережі, налаштувати індексацію даних в Elasticsearch та створити необхідні візуалізації для аналізу даних.

Опісля цих кроків буде перевірена робота системи, те як вона відстежує інциденти та проблеми для покращення системи безпеки в ході моделювання атак. У результаті цих кроків, буде забезпечено належний захист системи, а також зберігання та аналізування даних для виявлення інцидентів та покращення системи безпеки.

Висновки

В результаті виконання роботи було визначено оптимальний метод збору та аналізу даних. Визначено сучасні тенденції кібербезпеки та атаки на підприємства. Було розглянуто ряд інструментів та їх аналогів на сучасному ринку. На основі проведеного дослідження можна зробити висновок, що Elasticsearch - оптимальний інструмент для подальшого використання та розробці рішення для аналізу інформації. В порівнянні з аналогами, Elasticsearch має більш широкі можливості для аналізу даних, підтримку розподіленого середовища та більш зручний інтерфейс, що робить його більш універсальним та простим для використання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ukraine conflict: One year of cyberattacks and operations [Електронний ресурс] – Режим доступу до ресурсу: https://cyberpeaceinstitute.org/news/ukraine-conflict-one-year-anniversary/

2. González-Granadillo, Gustavo, Susana González-Zarzosa, and Rodrigo Diaz. "Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures." Sensors 21.14 (2021): 4759.

3. What is SIEM? | Microsoft Security [Електронний ресурс] – Режим доступу до ресурсу: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

4. ArcSight vs Elastic Stack vs LogRhythm Log Management vs Splunk Enterprise 2023 - Feature and Pricing Comparison on Capterra [Електронний ресурс] – Режим доступу до ресурсу: https://www.capterra.com/siem-software/compare/275325-149304-172899-94317/ArcSight-vs-Elasticsearch-vs-LogRhythm-Enterprise-vs-Splunk

5. What is Elasticsearch? | Elastic [Електронний ресурс] – Режим доступу до ресурсу: https://www.elastic.co/what-is/elasticsearch

Якімов Олександр Павлович — студент групи 1БС-19б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: sasa.jkimov@gmail.com

Науковий керівник: ***Войтович Олеся Петрівна*** — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Yakimov Oleksandr Pavlovich — student of group 1BS-19b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: sasa.jkimov@gmail.com

Scientific supervisor: Voytovych Olesya Petrivna — Candidate of Technical Sciences, Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia,