Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *"Методи та засоби аналізу журналів подій Sophos Firewall"*

Виконав: студент

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Пилипів П.В.
підпис (прізвище та ініціали)

Керівник *Лечаченко Т.А.*
підпис (прізвище та ініціали)

Нормоконтроль
підпис (прізвище та ініціали)

Завідувач кафедри *Загородна Н.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«13» 06 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Пилипіву Павлу Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи та засоби аналізу журналів подій Sophos Firewall

Керівник роботи Лечаченко Тарас Анатолійович, д.філ., асистент кафедри кібербезпеки
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «03» 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Технічна документація міжмережевих екранів Sophos, технічна документація ELK стеку.

4. Зміст роботи (перелік питань, які потрібно розробити)

Опис та властивості міжмережевих екранів нового покоління
Опис та аналіз властивостей та характеристик Sophos Firewall
Вибір та обгрунтування методів аналізу журналів подій
Етапи аналізу подій в інформаційно-комунікаційній системи
Розгляд можливостей ELK стеку
Аналіз способів збору журналів подій
Збір логів з агентом та без агента
Syslog-логування
Логування з використанням API та протоколу HTTPS
SNMP-логування
Розгортання та використання ELK стеку для обробки логів
Створення конфігураційного файлу для аналізу
Тестування конфігурації та створення інформаційної панелі
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1. Титульний слайд. 2. Схема роботи міжмережевих екранів. 3. Властивості Sophos Firewall XG. 4. Засіб для перегляду подій Log viewer. 5. Етапи аналізу подій в ІКС. 6. Схема роботи ELK-стеку. 7. Схема конвеєра logstash. 8. Структура фільтру конфігураційного файлу для аналізу журналів подій. 9. Проаналізований лог-файл у середовищі Kibana. 10. Візуалізація даних. 11-13. Частини інформаційної панелі

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, Дата: завдання видав	Підпис, Дата: завдання прийняв
Безпека життєдіяльності, основи охорони праці	Пилипець М.І. д.т.н. професор кафедри МТ	15.06.23	

7. Дата видачі завдання 15.02.2023

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.02 – 19.02	Вик
2.	Підбір джерел про методи та засоби аналізу журналів подій мережевих екранів.	20.02 – 27.02	Вик
3.	Опрацювання джерел в галузі дослідження	28.02 – 16.03	Вик
4.	Розгортання середовища для проведення аналізу журналів подій	17.03 – 20.03	Вик
5.	Тестування роботи конфігураційного файлу для аналізу та створення інформаційної панелі	20.03-05.04	Вик
6.	Оформлення розділу «Аналіз предметної області»	06.03 – 17.04	Вик
7.	Оформлення розділу «Методи збору та аналізу журналів подій»	18.04 – 29.04	Вик
8.	Оформлення розділу «Розробка та тестування конфігурації для аналізу журналів подій»	30.04 – 13.05	Вик
9.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	14.05 – 21.05	Вик
10.	Оформлення кваліфікаційної роботи	22.05 – 05.06	Вик
11.	Нормоконтроль	06.06 – 12.06	Вик
12.	Перевірка на плагіат	10.06 – 16.06	Вик
13.	Попередній захист кваліфікаційної роботи	17.06 – 19.06	Вик
14.	Захист кваліфікаційної роботи	21.06.	

Студент _____ (підпис) Пилипів П.В. (прізвище та ініціали)

Керівник роботи _____ (підпис) Лечаченко Т.А.

АНОТАЦІЯ

Методи та засобі аналізу журналів подій Sophos Firewall // Кваліфікаційна робота ОР «Бакалавр» //Пилипів Павло Володимирович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // С. 60 , рис. – __, табл. – __ , кресл. –__ , додат. – 1.

Ключові слова: аналіз, журнали подій, логи, міжмережеві екрани, Sophos Firewall XG.

Кваліфікаційна робота присвячена створенню алгоритму аналізу журналів подій у вигляді конфігураційного файлу, який проводить аналіз та структуризацію інформації з журналів подій.

У першому розділі кваліфікаційної роботи описані можливості міжмережевого екрану нового покоління Sophos Firewall XG, проаналізовано публікації, які стосуються об'єкту дослідження, обрано та обґрунтовано методи отримання та аналізу журналів подій.

У другому розділі кваліфікаційної роботи розглянуті етапи аналізу подій в ІКС, механізми збору, опрацювання та збереження журналів подій. Проаналізовані методи логування.

У третьому розділі кваліфікаційної роботи описано розгортання програмного забезпечення для аналізу, зберігання та візуалізації журналів подій. Створено конфігураційний файл який проводить аналіз та структуризацію інформації з журналів подій. Візуалізовано отримані дані в інформаційній панелі з допомогою Kibana.

ANNOTATION

Methods and tools for analyzing event logs from Sophos firewalls// Thesis of educational level "Bachelor" // Pylypiv Pavlo Volodymyrovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, SB-41 group // Ternopil, 2023 // P. 60 , fig. - ____, table. - __ , chair. - ___ , added. - 1.

Keywords: analysis, event logs, logs, firewalls, Sophos Firewall XG.

The qualification work is devoted to the creation of an algorithm for analyzing event logs in the form of a configuration file, which analyzes and structures information from event logs.

The first section of the qualification work describes the capabilities of the next generation firewall Sophos Firewall XG, analyzes the publications related to the researched object, selects and substantiates the methods of obtaining and analyzing event logs.

In the second section of the qualification work, considered the stages of event analysis in ICS, mechanisms for collecting, processing and saving event logs. Analyzed logging methods.

The third chapter of the qualification paper describes the deployment of software for analysis, storage and visualization of event logs. A configuration file has been created that analyzes and structures information from event logs. The received data was visualized in the information panel using Kibana.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

NGFW (Next-Generation Firewall) – міжмережевий екран (фаєрвол) наступного покоління.

APTs (Advanced Persistent Threats) – прихована загроза, яка дозволяє отримувати несанкціонований доступ до комп’ютерної мережі та залишається непоміченою на протязі тривалого періоду часу.

LAN (Local Area Network) – комп’ютерна мережа, яка з’єднує комп’ютери в обмеженій зоні, наприклад, у будинку, школі, лабораторії, університетському містечку чи офісній будівлі.

WAN (Wide Area Network) – телекомунікаційна мережа, яка простягається на велику географічну територію.

SSID (Service Set Identifier) – унікальне найменування бездротової мережі, що відрізняє одну мережу Wi-Fi від іншої.

ELK стек – сукупність інструментів для пошуку, опрацьовування та візуалізації журналів – Elasticsearch, Logstash, Kibana.

HTTP (Hyper Text Transfer Protocol) – протокол передачі даних, що використовується в комп'ютерних мережах для передачі гіпертекстових документів.

SIEM (Security information and event management) – програмні продукти, які об'єднують управління інформаційною безпекою SIM (англ. Security information management) та управління подіями безпеки SEM (англ. Security event management).

CVE (Common Vulnerabilities and Exposures) – база даних загальновідомих вразливостей інформаційної безпеки.

ВСТУП

Сучасний розвиток у галузі інформаційних технологій вимагає інтенсивного впровадження мереж різного рівня охоплення – локального, корпоративного та глобального. Усі ці мережі передбачають використання різного мережевого обладнання, зокрема, міжмережевих екранів, маршрутизаторів.

Усі ці пристрої генерують файли журналів подій (логи), в яких записується дані про події пристрою у хронологічному порядку. Журнали подій є потужним інструментом для отримання інформації про події та стан мережі чи хоста. Зокрема, такі файли можуть містити інформацію про мережеві з'єднання, їх кількість, підозрілу активність в мережі, спроби атак, яка може бути використана для виявлення та запобігання можливих атак. Втім перегляд «сирих» журналів подій є малоефективним, оскільки вимагає затрат часу на пошуки потрібної інформації у рядку файлу журналу.

Метою даної кваліфікаційної роботи бакалавра є дослідження методів та засобів аналізу журналів подій на прикладі аналізу логів міжмережевого екрану Sophos Firewall XG.

Для досягнення поставленої задачі було здійснено:

- аналіз властивостей та характеристик міжмережевих екранів нового покоління, зокрема Sophos Firewall XG;
- розглянуто етапи аналізу подій в комп'ютерній системі та програмне забезпечення для збору, опрацювання та зберігання журналів подій;
- аналіз методи отримання та аналізу журналів подій;
- створено конфігураційний файл для аналізу журналів подій та інформаційну панель для візуалізації результатів.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Опис та властивості міжмережевих екранів нового покоління

Раніше міжмережеві екрани працювали на нижніх рівнях мережевого стеку, забезпечуючи базову маршрутизацію та фільтрацію пакетів на основі перевірки адрес, портів та протоколів для переадресації або скидання трафіку. Ця технологія була ефективною для свого часу.

Оскільки загрози перейшли від безпосередніх атак на мережу до зараження внутрішніх систем з допомогою вразливостей у програмних додатках та серверах або за допомогою соціальної інженерії, засоби для захисту мережі повинні були змінювати підхід до безпеки, щоб ефективно протистояти новим методам атак.

Технологія міжмережевих екранів також еволюціонувала, рухаючись вгору по стеку до сьомого рівня, щоб ідентифікувати та контролювати трафік від додатків. Фаєрволи також почали включати технології більш глибокого аналізу вмісту пакетів та пошуку загроз. Вони отримали можливість класифікувати та керувати трафіком, створеним користувачем або додатком, покладаючись не лише на порти та протоколи. Перехід на нові методи захисту мережі породив нові пристрої – міжмережеві екрани наступного покоління Next-Generation Firewall (NGFW).

Міжмережевий екран наступного покоління поєднує в собі традиційні методи поряд з глибоким аналізом пакетів, що включає запобігання вторгненням, отримання відомостей про додатки, політики користувача та можливість перевірки зашифрованого трафіку.

Мережева безпека продовжує покращуватись щоб протистояти все новим і новим загрозам. Сучасні загрози, такі як програми-вимагачі та ботнети є більш розвиненими та невловимими, ніж будь-коли раніше. Ці розвинені загрози звуться Advanced Persistent Threats (APTs) та використовують zero-day методи, тому їх надзвичайно важко виявити.

Безліч організацій вже є скомпрометованими, ставши жертвами APT або ботнетів, і в багатьох випадках навіть не підозрюють про ці загрози.

Одним з вирішень таких проблем є фаєрвол від Sophos.

1.2 Опис та аналіз властивостей та характеристик Sophos Firewall

Sophos Firewall та Sophos XG Firewall – програмні мережеві екрани, які можна розгорнути на персональних комп'ютерах, серверах або віртуальних машинах. Втім, для розгортання фаєрволу для домашнього користування, версія якого є безплатною, сервер або віртуальна машина повинні не перевищувати наступні вимоги:

- центральний процесор не більше ніж з 4 ядрами;
- не більше 6 гігабайт оперативної пам'яті.

Для використання Sophos Firewall та Sophos XG Firewall апаратне або віртуальне забезпечення повинне відповідати наступним характеристикам:

- центральний процесор не більш ніж з чотирма ядрами;
- не більше 6 гігабайт оперативної пам'яті;
- не менше 64 ГБ вільної пам'яті;
- не менше двох мережевих інтерфейсів (LAN та WAN).

Для розгортання Sophos Firewall та Sophos XG Firewall на віртуальній машині потрібно завантажити спеціально налаштовану віртуальну машину з відповідними інструментами та драйверами для гіпервізора. Серед доступних платформ є:

- VMware;
- Hyper-V;
- KVM;
- Citrix XenApp;
- Microsoft Azure.

Sophos XG Firewall був розроблений для вирішення теперішніх та знову виникаючих проблем, а також забезпечення платформи, яка з легкістю може адаптовуватись до зміни мережевої архітектури. XG Firewall пропонує новий підхід до виявлення прихованих ризиків, захисту мережі, виявленню та реагуванню на загрози.

Також у поєднанні з Sophos Antivirus міжмережевий екран Sophos XG Firewall може отримувати інформацію про заражені комп’ютери у мережі та відключати комп’ютер користувача від локальної мережі або сегменту мережі на канальному рівні блокуючи будь-які зв’язки з ним.

Згідно рейтингу фаєрволів, створеному компанією PeerSpot, Sophos Firewall XG посідає 8 місце із загальним рейтингом 8.2 з 10 балів на основі 73 відгуків на порталі [1]. Цей брандмауер популярний серед сегменту великих корпорацій, на який припадає 44% пошукових запитів на PeerSpot. Найпопулярнішою галуззю компаній які цікавляться цим рішенням безпеки, є організації, які займаються розробкою програмного забезпечення. На них припадає 19% від усієї кількості [2].

Порівнюючи фаєрвол нового покоління від Sophos з аналогічним пристроєм виробництва Fortinet, який займає першу позицію у вищезгаданому рейтингу, користувачі підмічають легкість розгортання двох рішень та високу рентабельність застосування цих продуктів у своїх комп’ютерних мережах. Говорячи про модулі захисту, Sophos Firewall XG поступається своєму конкуренту у їх кількості, втім ці модулі є швидше додатковими, ніж обов’язковими. Також користувачі відзначають необхідність ліцензії для кожного окремого модуля FortiGate, в той час як Sophos Firewall XG включає більшість захисних можливостей у нерозширеній ліцензії [3].

Даний фаєрвол надає захист з допомогою двадцяти модулів, серед яких модуль мережевого захисту, модуль веб-захисту, система запобігання вторгнень наступного покоління, захист веб-сервера, зворотний проксі, захист електронної пошти, анти-спам, шифрування електронної пошти, запобігання втраті даних. Також дані фаєрволи можна налаштувати як DHCP-сервер, DNS-сервер та VPN-сервер.

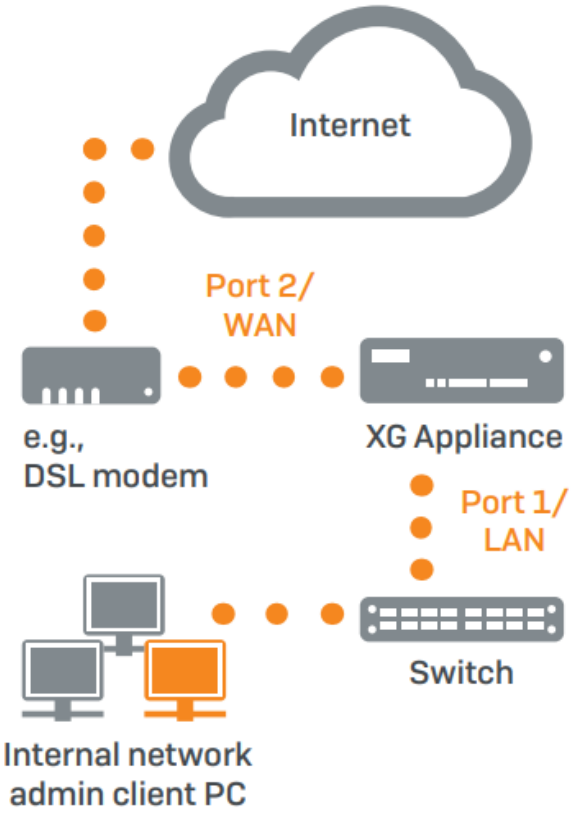


Рисунок 1.1 – Схема роботи брандмауера Sophos

Завдяки скануванню та аналізу трафіку, Sophos Firewall XG дозволяє виявляти мережеві атаки, такі як:

- DoS (Denial of Service) та DDoS (Distributed Denial of Service);
- spoofing (від spoofing – підміна);
- спроби експлуатації уже наявних вразливостей.

DDoS-атака або ж розподілена атака на відмову в обслуговуванні може бути реалізована з допомогою потоку хибних запитів або пакетів від великої кількості географічно розподілених хостів. Під час реалізації цієї атаки може бути використаний флуд UDP, TCP або ICMP пакетами. Існує два методи виконання атаки на відмову обслуговування.

Перший метод це пряма атака на канал зв’язку, який повністю блокується великою кількістю беззмістовних даних. Другий метод полягає в безпосередній атаці на сервер ресурсу. В результаті це може призвести до погіршення роботи цього

серверу або ж його повної недоступності на доволі довгі терміни – від кількох годин до кількох днів.

При виявлені атаки такого типу, Sophos Firewall XG застосовує обмеження трафіку для хосту-джерела або хосту-призначення на 10 секунд. Якщо після закінчення цього терміну DoS/DDoS-атака зупиняється, екран знімає обмеження з хосту. У протилежному випадку лічильник постійно скидатиметься кожні 10 секунд, а обмеження трафіку не будуть зняті. У випадку нової атаки з хосту, який раніше був блокований, брандмауер знову застосує обмеження трафіку [4].

Ще одною атакою, яку брандмауер Sophos XG здатний виявляти та блокувати є атака підміни, також відома як spoofing. Спуфінг – це специфічний тип атаки, спрямований на підміну IP чи MAC-адреси, а також DNS-запису.

Підробка IP-адресу дозволяє приховати справжню адресу зловмисника для доступу до певної мережі. Також така атака часто вчиняється з метою використання дозволів, зарезервованих для IP-адреси, яку використовує зловмисник.

Під час підміни MAC-адресу здійснюється методом надсилання ARP-пакету, який видасть його хост за справжній маршрутизатор, після чого весь трафік користувача буде іти через комп’ютер хакера замість маршрутизатора. Завдяки цьому зловмисник отримає повний контроль над трафіком та зможе відслідковувати запити, які надсилаються в дві сторони. Така атака дозволяє реалізувати іншу атаку, відому як «Людина посередині»(Man-in-the-Middle, MitM).

Для виконання атаки підміни методом підробки DNS-запису, зловмисник використовує змінені записи протоколу Domain Name System, щоб перенаправити трафік користувача із потрібного йому інтернет-сайту на підроблений. Після потрапляння на несправжній сайт, користувачу може бути запропоновано завантажити шкідливе забезпечення, ввести свої облікові дані. Також на таких веб-сторінках можливий запуск шкідливих скриптів, які можуть бути частинами вже інших типів атак [5].

Також Sophos Firewall XG фільтрує трафік на наявність можливих спроб експлуатації уже відомих загроз. База даних таких загроз сформована зі списку відомих вразливостей та дефектів безпеки Common Vulnerabilities and Exposures,

також відомої як CVE. CVE – це словник відомих загроз, кожен запис якого складається з таких розділів:

- CVE ID;
- reference;
- description.

CVE ID починається з префіксу CVE- та записується зі вказанням року, коли було повідомлено про вразливість та номера, присвоєного CVE Numbering Authorities (CNA).

У доповнення до запису CVE ID, CVE містить опис вразливості та посилання на додаткові відомості, повідомлення та рекомендації виробників програмного забезпечення для їх усунення.

Детальність опису для різних загроз відрізняється, але зазвичай він будується за однією схемою:

<проблема> у <версії> <продукту> призводить до <впливу > в результаті <атаки>.

У разі виявлення спроби відомої атаки чи експлуатації вразливості фаєрвол Sophos XG скине з'єднання та заблокує джерело з'єднання на визначений термін.

Для адміністрування міжмережевого екрану та перегляду подій використовується веб інтерфейс. На основній сторінці (Control Center) відображені віджети про стан системи (блок System), події та стан мережі (блок Traffic insight), активність користувачів та стан їхніх комп'ютерів, отриманий від Sophos Antivirus (блок User & device insights) та активні правила мережевого екрану та звіти з них (Reports). Загальна інформація по кожному окремому модулю доступна на відповідних вкладках зліва.

Для перегляду журналів подій потрібно перейти на сторінку Log viewer, натиснувши відповідну кнопку на головній сторінці. Записи містять інформацію про події брандмауера, системи запобіганню вторгнень, фільтрації пошти та решти підключених модулів. Їх можна відсортувати за різними значеннями, наприклад адресою джерела або призначення, протоколом. Журнали відображатимуться

відносно їх новизни, тобто новіші події будуть відображені вище. Втім, потрібно взяти до уваги, що Log viewer дозволяє переглянути події лише за останні 5-7 днів [6].

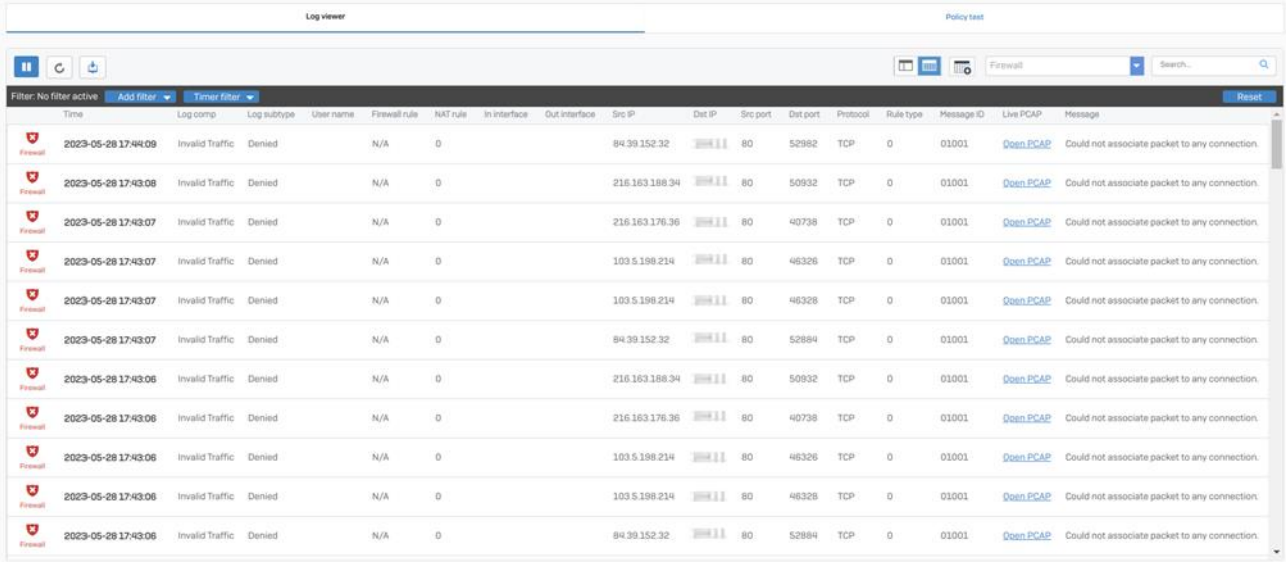


Рисунок 1.2 – Приклад записів журналів у Log viewer

Щоб отримати доступ до старіших записів, прийдеться використовувати інтерфейс командного рядка, який не є зручним для таких задач. Але локально Sophos Firewall зберігає невелику кількість записів для кожного модуля в спеціальному кеші за принципом «перший прийшов, перший пішов», тобто при перевищенні цього ліміту, останні записи будуть стерті. Також ця пам’ять очищується при кожному перезапуску системи. Проте така кількість або час зберігання записів журналів може не задовольняти вимоги політики управління журналами подій. Для довготривалого зберігання таких файлів потрібно налаштувати syslog-сервер та передачу журналів до нього.

Наразі перегляд журналів з допомогою інструмента Log viewer для новіших записів та інтерфейс командного рядка для старіших подій є єдиними доступними засобами.

Проблемою цих методів є те, що розбитими на складові відображаються лише записи п’ятиденної давності, тоді як старіші записи можна переглянути в командному рядку у форматі стрічки, що не є зручним для розуміння та кореляції подій брандмауера, враховуючи кількість сервісів, які підтримують логування:

- брандмауер – інформація про трафік, пов’язаний із конфігурацією брандмауера, наприклад правила брандмауера, фільтрацію MAC-адрес і DoS-атаки;
- IPS – записи про виявлені та відкинуті атаки на основі невідомих або підозрілих моделей (аномалій) і сигнатур;
- антивірус – відомості про віруси, виявлені в трафіку HTTP, HTTPS, FTP, IMAP4, IMAPS, SMTP, SMTPS, POP3 і POPS;
- захист від спаму – ці журнали містять відомості про спам SMTP, SMTPS, POP3, POPS, IMAP4, IMAPS та ймовірні спам-повідомлення;
- фільтрування вмісту – журнали фільтрування вмісту містять відомості про події фільтрації веб-сторінок і додатків, наприклад пов’язані з веб-політиками;
- запис подій системи – журнали подій надають інформацію про конфігурацію, автентифікацію та дії системи;
- захист веб-сервера – журнали захисту веб-сервера містять відомості про події захисту веб-сервера, наприклад політики захисту;
- розширений захист від загроз – журнали розширеного захисту від загроз надають інформацію про події Advanced Threat Protection, такі як падіння або сповіщення;
- бездротовий зв’язок – журнали бездротового зв’язку містять відомості про активність точок доступу та SSIDів;
- Heartbeat – журнали Heartbeat надають інформацію про стан кінцевих точок;
- справність системи – журнали справності системи містять відомості про використання центрального процесора, пам’яті, кількість активних користувачів, інтерфейси та розділи диска;
- захист нульового дня – ці журнали містять записи про всі події захисту нульового дня [7].

1.3 Вибір та об ґрунтування методів вирішення поставленої задачі

Оскільки для перегляду та кореляції журналів подій Sophos Firewall існує лише вбудований переглядач, який не відображає записів, старіших за певний період, мною запропонований метод пересилання записів подій на спеціальний сервер для подальшого їх опрацювання. Для забезпечення належного рівня безпеки буде використане шифрування передачі даних з допомогою протоколів SSL/TLS.

Журнал аудиту подій (Event Log або Audit Log) – це важливі елементи системи безпеки інформаційної системи. Це спеціальні файли, які зберігають інформацію про всі події, що відбуваються в комп'ютерній системі. До таких подій можуть відноситися входи користувачів у систем, встановлення програм, зміни налаштувань системи, виконання файлів, помилки та інші події, що мають відношення до безпеки інформації. У контексті журналів подій мережевого пристрою, зокрема міжмережевого екрану, лог-файли, окрім зазначених вище подій, містять інформацію про вхідні та вихідні з’єднання, заблоковані з’єднання, загрози та інциденти, наприклад виявлені спроби експлуатації вразливості системи або мережеві атаки.

Кожен запис у журналі містить детальну інформацію про подію, включаючи дату та час, тип події, інформацію про джерело, а також подробиці про саму подію.

Існує декілька видів записів журналів:

- записи системи - пов'язані з подіями у системі;
- записи сервера – відображають інформацію про звернення до сервера та виникнення помилок на його стороні;
- записи подій баз даних - спеціальні журнали, які містять в собі інформацію про запити до баз даних і помилки, які виникли у них;
- записи поштових серверів надають інформацію про відправлені та отримані листи, помилки у роботі серверів та їх причини;
- записи планувальника задач cron;

- записи подій кореневого файлу, наприклад, фаєрвола, сервера DNS та інші [8].

Журнал аудиту подій може бути використаний системним адміністратором для аналізу подій, що відбуваються в системі, для виявлення проблем безпеки та для забезпечення відповідності різних стандартів та політик безпеки. Завдяки журналу аудиту подій можна відстежувати дії користувачів та відновлювати роботу системи після виникнення проблем.

Для зручнішого аналізу журналу аудиту подій можуть використовуватися різні інструменти, які дозволяють фільтрувати, сортувати та аналізувати записи в журналі. Ці інструменти допомагають виявляти незвичайні дії користувачів, що можуть свідчити про порушення безпеки. Одним з таких рішень є ELK стек.

Це безплатне програмне забезпечення з відкритим кодом, яке включає в себе засоби для отримання даних, їх зберігання у базі даних, агрегації, кореляції, аналізу та відображення у формі таблиць та великої кількості візуалізацій – графіки, лічильники, кругові діаграми, карти.

1.4 Висновок до першого розділу

У першому розділі роботи було описано фаєрволи нового покоління, зокрема Sophos Firewall XG, його особливості та можливості, проведений перегляд та аналіз публікацій, які мають відношення до об’єкту дослідження, обрано та обґрунтовано методи вирішення поставленої проблеми.

2 МЕТОДИ ЗБОРУ ТА АНАЛІЗУ ЖУРНАЛІВ ПОДІЙ

2.1 Етапи аналізу подій в інформаційно-комунікаційній системі

Аналіз подій в інформаційно-комунікаційній системі – це процес виявлення та оцінки подій, які відбуваються в системі з метою виявлення можливих проблем безпеки або неналежної роботи системи. Цей механізм є важливою складовою систем безпеки та моніторингу інформаційних систем. З його допомогою адміністратор може виявити вразливості системи, атак на неї, а також попереджати виникнення можливих проблем.

Аналіз подій включає наступні етапи:

- збір подій – збір інформації про події, що відбуваються в системі. Це може включати збір логів, метрик, потоків даних та іншої інформації з різних джерел;
- агрегування та кореляція – об'єднання подій в групи за певними параметрами, що дозволяє виявляти залежності між ними та оцінювати загальний вплив на систему;
- аналіз – оцінка подій з точки зору їх відповідності визначеним правилам та шаблонам, що дозволяє виявити можливі проблеми безпеки або неналежної роботи системи;
- візуалізація та повідомлення – в ході цього етапу відображаються результати аналізу в зручному для сприйняття вигляді та повідомлення про виявлені проблеми;
- реагування – вжиття заходів для вирішення виявлених проблем або запобігання подальшій їх появі.

Системи моніторингу можуть отримувати інформацію про події від різних джерел, таких як:

- журнали подій (event logs) операційної системи – ОС зберігає інформацію про події, які сталися на комп'ютері або в мережі, у своїх журналах

подій. Системи моніторингу можуть аналізувати ці журнали і відслідковувати різні типи подій, наприклад, помилки, попередження, інформаційні повідомлення;

- системні інформаційні події (system information events) - ОС також зберігає інформацію про системні події, такі як зміни конфігурації, оновлення програмного забезпечення, встановлення апаратного забезпечення тощо. Ці події можуть бути відстеженні системами моніторингу, щоб допомогти адміністраторам знаходити потенційні проблеми та відстежувати зміни в системі;
- журнали подій додатків - багато додатків мають свої власні журнали подій, де зберігають інформацію про виконання певних дій або помилок, що сталися в програмі. Системи моніторингу можуть аналізувати ці журнали, щоб відстежувати стан додатків і виявляти проблеми;
- мережеві пристрої - мережеві пристрої, такі як маршрутизатори, комутатори, фаєрволи тощо, також можуть мати свої власні журнали подій, які містять інформацію про мережеву активність. Системи моніторингу можуть аналізувати ці журнали, щоб аналізувати вхідний та вихідний трафік, виявляти проблеми в мережі та відстежувати активність користувачів;
- системи безпеки – системи виявлення/запобігання вторгнень моніторять мережевий трафік та системні ресурси з метою виявлення зловмисних атак або аномальної активності. Журнали подій таких пристроїв можуть надавати інформацію про спроби вторгнення, вразливості систем, атаки на додатки та інші події, що вказують на порушення безпеки;
- додаткові джерела – до цих джерел інформації можуть належати системи контролю доступу, системи керування ідентифікацією та автентифікацією, системи керування конфігурацією, системи моніторингу баз даних, фізичні системи безпеки (наприклад, системи відеоспостереження).

Для спрощення процесу аналізу журналів подій, рішення для окремих етапів опрацювання логів об’єднують в одну цілісну систему – SIEM. Ці системи комбінують в собі засоби управління інформаційною безпекою SIM (Security

information management) та управління подіями безпеки SEM (Security event management) [9].

Цей інструмент дозволяє збирати, агрегувати, аналізувати та відображати дані про події безпеки в реальному часі з різних джерел в одному середовищі. До компонентів SIEM належать наступні складові:

- агентів збору даних, які збирають дані про події з різних джерел (наприклад, міжмережевих екранів, систем виявлення/запобігання вторгнень, серверів, тощо).
- централізованого сервера, який отримує дані від агентів збору даних і проводить їх агрегацію, аналіз та відображення;
- інтерфейс користувача, який надає можливість адміністраторам та аналітикам переглядати дані, створювати звіти, налаштовувати правила та реагувати на виявлені загрози.

В залежності від отримуваних даних з пристроїв, SIEM може виявляти загрози безпеки на різних рівнях: на мережевому чи транспортному рівні, на рівні користувачів чи додатків. Крім того, SIEM дозволяє розробляти правила та політики безпеки, які допомагають виявляти підозрілі дії та поведінку користувачів і систем.

У контексті даної роботи роль централізованого сервера для обробки та збереження даних виконуватимуть сервіси Logstash та Elasticsearch. У якості інтерфейсу користувача використовуватиметься програма Kibana. Усі ці рішення об’єднані в одну групу програм відому як ELK стек.

2.2 ELK стек

ELK стек – це скорочення для трьох інструментів з відкритим кодом Elasticsearch, Logstash та Kibana. Ці інструменти об’єднані в одне рішення для синтаксичного аналізу, зберігання, пошуку, аналізу та візуалізацій даних. Журнали опрацьовуються інструментом під назвою Logstash з допомогою спеціальних файлів

конфігурації. Після цього документи надсилаються до Elasticsearch-сервера для зберігання та подальшої візуалізації за допомогою Kibana.

Схема опрацювання інформації стеком зображена на рисунку 2.2.1.

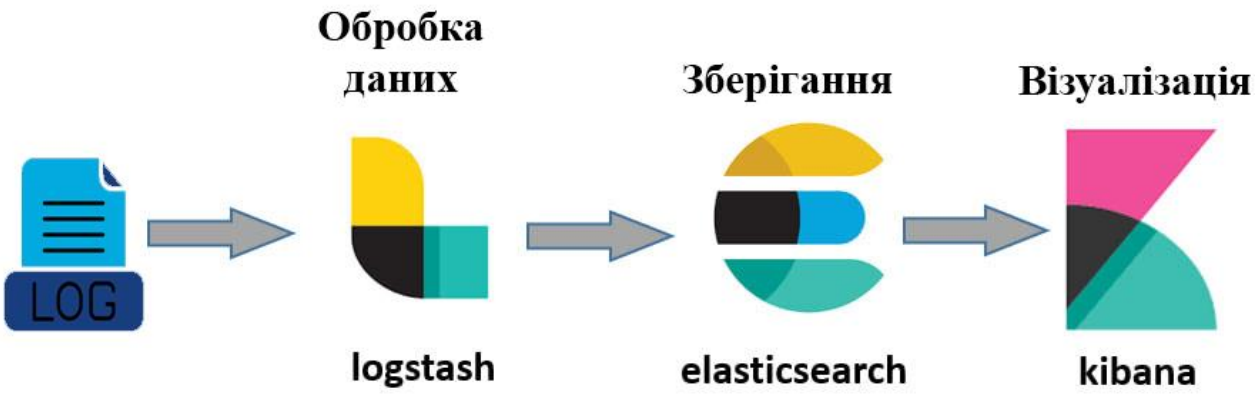


Рисунок 2.2.1 – Схема роботи ELK стеку

Logstash – це безкоштовний конвеєр обробки даних із відкритим вихідним кодом на стороні сервера, який можна використовувати для отримання даних із кількох джерел, їх трансформації та надсилання на подальшу обробку чи зберігання. На відміну від інших більшості схожих сервісів, Logstash дозволяє застосовувати фільтри для вхідних даних та обробляти їх. Logstash не лише агрегує та пересилає дані, а й витягує інформацію з необроблених даних і перетворює її в більш значущу приводячи її до загального формату [10].

Для опрацювання даних, Logstash використовує конфігураційні файли, так звані пайплайни або конвеєри, які складаються з введення (input), фільтру, який містить усі потрібні плагіни для обробки журналів подій, та виводу (output). Типова схема пайплайну Logstash зображена на рисунку 2.2.2.

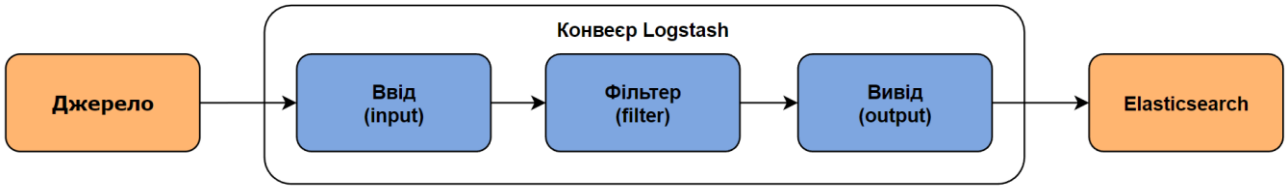


Рисунок 2.2.2 – Схема конвеєра Logstash

Для отримання даних можна використати безліч методів, серед яких передача даних по HTTP або HTTPS протоколах, прослуховування визначених портів по протоколу TCP або UDP, отримання даних від поштових серверів, наприклад IMAP чи SMTP, інструментів та сервісів, для прикладу Amazon S3. Також існує можливість отримання журналів від іншого пайплайну або безпосереднє читання з файлу [11].

Щоб захистити передачу даних, у файлі конфігурації можна вказати SSL сертифікат, який дозволить шифрувати трафік та підвищити його безпеку [12]. Після обробки логів, дані надсилаються у сховище, тобто до Elasticsearch.

Elasticsearch (іноді можна зустріти скорочення ES) — це сучасна пошукова та аналітична система, створена на базі Apache Lucene. Elasticsearch, створена за допомогою Java, є No SQL базою даних, тобто усі дані зберігаються в неструктурований спосіб і що для доступу до інформації не можна використовувати SQL для запиту до них.

У контексті ELK стеку Elasticsearch виконує роль індексатора та сховища для даних. Інформація у ньому зберігається у вигляді JSON документів, які в свою чергу зберігаються на шардах (від англійського shard – осколок). Шарди утворюють вузли (nodes), які зберігаються всередині кластерів. Для спрощення зберігання пов’язаних документів, наприклад журналів подій різних пристроїв, їх можна об’єднати в індекси [13]. Схема кластера Elasticsearch зображена на рисунку 2.2.3.

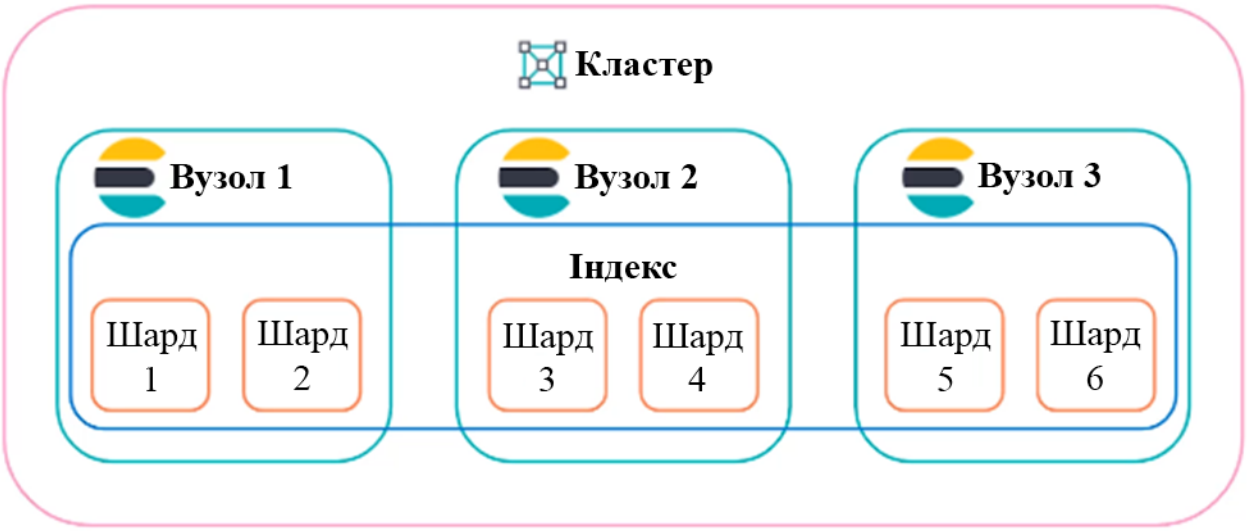


Рисунок 2.2.3 – Кластер Elasticsearch

Kibana – це безкоштовна відкрита інтерфейсна програма, яка розташована поверх Elastic Stack і забезпечує пошук і візуалізацію даних для даних, індексованих у Elasticsearch. З її допомогою можна здійснювати пошук, перегляд та аналіз даних, використовуючи засоби візуалізації, такі як гістограми, секторні діаграми, таблиці, карти, тощо. Об'єднуючи візуалізації в одну інформаційну панель – дашборд, можна отримати потужний засіб для аналізу великої кількості даних у реальному часі. Також використовуючи Kibana можна проводити моніторинг, управління та керування безпекою екземпляра Elastic стеку [14].

Kibana містить декілька вкладок на панелі навігації, як приклад, Discover, Visualize, Dashboard, Stack Management, Dev tools, тощо.

На вкладці Discover можна переглядати дані у табличній формі, обравши потрібний індекс та часовий проміжок. Також у цьому середовищі доступні рядок пошуку та інструмент для створення запитів пошуку.

Вкладка Visualize містить інструменти для створення візуалізацій, використовуючи документи визначеного індексу. Для створення на основі агрегацій доступні графіки, гістограми, секторні діаграми, метрики, тощо.

На сторінці Dashboard можна переглянути уже створені інформаційні панелі, також відомі як дашборди, або створити нову панель використовуючи попередньо створені візуалізації або створити нові.

Stack management надає інструменти для керування Kibana та середовищем Elasticsearch, оновлення Logstash конфігурацій, створення індексів, шаблонів полів для присвоєння їм певного типу згідно Elastic Common Schema.

Інструменти розробки, або ж dev tools, надають можливість використання консолі для звернення до індексів, зміни інформації в середині них або видалення інформації з них, використовуючи HTTP запити такі, як GET, POST, PUT та DELETE. Також доступний інструмент для написання grok-виразів, які використовуються для обробки даних у конвеєрах Logstash.

2.3 Аналіз способів збору журналів подій

Існує декілька методів збору журналів подій з мережевих пристроїв для моніторингу стану мережі. Серед них:

- використання спеціальних агентів для збору даних;
- використання протоколу syslog;
- отримання логів з використанням API;
- використання протоколу SNMP.

2.3.1 Збір логів з агентом та без агента

Одним з класичних підходів до моніторингу мережевого обладнання є інсталяція невеликих програм на обладнані, яке слід контролювати та моніторити. Це ПЗ називається агентом.

Агенти самостійно збирають дані про стан пристрою, на якому вони встановлені, та надсилають їх на центральний сервер для подальшого аналізу. У такому випадку, з’єднання є одностороннім, тобто лише агент зв’язується сервером, в той час як сервер не має такої можливості. Агенти дозволяють зменшити навантаження на головний сервер, збираючи дані самостійно. Також, у випадку, якщо сервер є недоступним з різних причин, записи журналів подій не втрачаються,

оскільки агент може зберігати певну кількість логів та надіслати їх згодом. На рисунку 2.3.1.1 показана схема моніторингу мережі з використанням агенту.

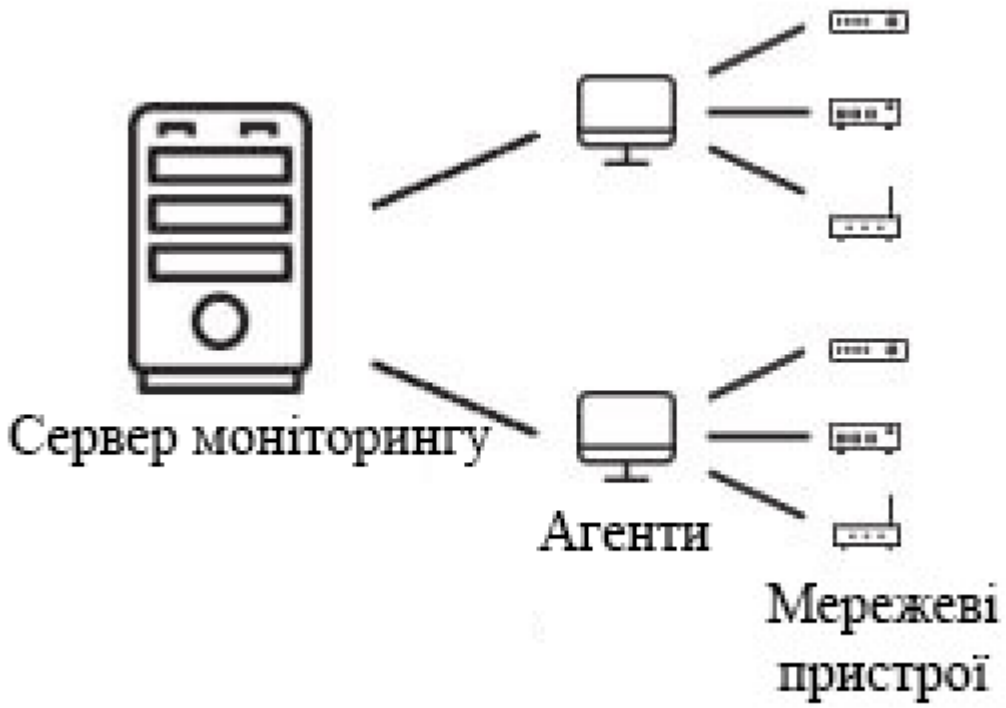


Рисунок 2.3.1.1 – Збіг логів з використанням агентів

До переваг цього методу можна віднести наступні пункти:

- можливість необов’язкової активації протоколів WMI чи SNMP у кінцевій системі;
- вихідне з’єднання через протокол HTTPS від кінцевої точки до сервера моніторингу не вимагає запитів на вхідне підключення до кінцевої точки;
- для роботи не потрібно відкривати усі порти, буде достатньо лише увімкнути необхідні порти;
- журнали подій збираються, навіть при неможливості доступу до центрального серверу моніторингу;
- відсутня необхідність публічних дій на кшталт відкриття портів чи дозвіл зовнішніх мережевих запитів;
- ця техніка моніторингу є більш безпечною.

Але також цей метод має свої мінуси. Так, наприклад, агент здатний зменшити навантаження на центральний сервер моніторингу, але збільшити його на мережевому пристрої, за яким проводиться спостереження, що може негативно вплинути на їх роботу. Також встановлення та управління агентами вимагає певних знань та ресурсів, наприклад, встановлення сторонніх пакетів, тощо.

Протилежним цьому способу є техніка моніторингу мережі без агенту. У таких випадках відстеження здійснюється з використанням протоколів, наприклад syslog, Rest API, або залученням сторонніх компаній. У випадку використання способу безагентного моніторингу мережі, встановлювати агенти на мережеві пристрої не потрібно. На рисунку 2.3.1.2 показана схема моніторингу мережі без агента.

Рисунок 2.3.1.2 – Моніторинг мережі без агента

Перевагами цього методу моніторингу є те, що він не вимагає встановлення сторонніх програм, тобто агентів, на мереже обладнання, та підтримує не лише фізичні хости, а і віртуальні хости та усі види серверів.

Втім, недоліками цього методу є спільні облікові дані для методів авторизації, необхідність активації протоколів WMI та SNMP на кінцевих точках та

неможливість отримувати файли журналів подій у випадку, якщо центральний сервер недоступний.

Ці методи моніторингу є доволі специфічними і їх вибір залежить від декількох факторів:

- потреба надійного логування, яке переривається при недоступності сервера моніторингу;
- безпека передачі даних;
- потреба логування пристроїв, під'єднаних до безпровідної мережі;
- вимоги політик безпеки інформації.

Метод спостереження за мережею за допомогою агентів варто використовувати у випадках, якщо політика безпеки інформації забороняє поширення облікових даних, надавати дозвіл на запити доступу до мережі або відкривати порти. Також, рекомендується використовувати даний метод коли у комп'ютерній мережі невелика кількість пристроїв або використовуються технології безпровідних мереж, оскільки IP-адреси WAN пристроїв постійно змінюється [15].

Безагентний моніторинг найкраще підходить для спостереження та отримання інформації від мережевих пристроїв, таких як сервери, маршрутизатори, тощо. Також він є хорошим рішенням у випадку, якщо у користувача немає бажання встановлювати сторонні програми у своїй мережі та налаштовувати їх.

2.3.2 Syslog-логування

Одним з методів передачі журналів подій при моніторингу мережі без агента є використання протоколу syslog.

Syslog, також відомий як System Logging Protocol, це протокол, який забезпечує передачу файлів журналів подій з мережевих пристроїв на центральний сервер, відомий як syslog-сервер. Цей протокол використовує багаторівневу архітектуру для моніторингу різних мережевих пристроїв, більшість з них, такі як маршрутизатори, комутатори, фаєрволи, підтримують реалізацію цього протоколу.

Для передачі даних, протокол системного журналювання використовує протокол UDP та порт 514. Однак протокол UDP не гарантує підтвердження та доставку даних на стороні одержувача(сервера), оскільки особливістю цього транспортного протоколу є відсутність UDP-з'єднання. Для вирішення цієї проблеми деякі мережеві пристрої використовують протокол TCP, який гарантує підтвердження та доставку даних, та порт 1468. На відміну від SNMP, syslog уникає збирання інформації про пристрої(опитування), зберігаючи простоту та легкість використання.

Протокол системного журналювання має три рівні з унікальними можливостями:

- syslog content: містить фактичну інформацію, наявну в повідомленні про подію;
- syslog application: виконує маршрутизацію, генерацію, інтерпретацію та зберігання повідомлень;
- syslog transport: передає повідомлення через мережу [16].

Повідомлення syslog про події генеруються окремими програмами або компонентами системи. Усі syslog-повідомлення мають стандартний формат, необхідний для обмінну повідомленнями між програмами. Цей формат вимагає наступні елементи повідомлення:

- заголовок (header), який містить поле пріоритету, версії, мітки часу, імені хоста, програми, ідентифікатора процесу та ідентифікатора повідомлення;
- структуровані дані з блоками даних у форматі ключ-значення;
- повідомлення у кодуванні UTF-8, яке містить тег, що ідентифікує процес, який ініціював повідомлення, разом із вмістом повідомлення [17].

Syslog позначає повідомлення ідентифікатором серйозності (severity score), де 0 означає екстрену ситуацію, а 7 використовується під час налагодження системи.

Можливі значення серйозності повідомлень:

- 0 – аварійна система непридатна;

- 1 – Alert: необхідно негайно вжити заходів;
- 2 – Critical: Критичні умови;
- 3 – Error: умови помилки;
- 4 – Warning: умови попередження;
- 5 – Notice: нормальний, але значний стан;
- 6 – Informational: інформаційні повідомлення;
- 7 – Debug: повідомлення рівня налагодження.

Говорячи про методи передачі даних з допомогою протоколу syslog, комунікаційний шлях включає джерело повідомлення, яке створює та надсилає повідомлення, та збирач (collector), тобто сервер журналювання, який приймає та зберігає повідомлення.

Також шлях може містити точки ретрансляції між джерелом та сервером, які можуть здійснювати певну обробку даних під час надсилання повідомлення. Також журнали подій можуть надсилатись до кількох адресатів одразу, в залежності від налаштувань джерела повідомлень.

На стороні сервера діють наступні служби:

- приймач – отримує дані через порт TCP або UDP, втім сам слухач не здатний запитувати дані;
- база даних – оскільки syslog може генерувати великі обсяги даних, сервер зберігання файлів журналів повинен бути налаштованим для обробки цього обсягу;
- програмне забезпечення для обробки даних – це ПЗ, яке працює поверх даних сервера та здатне допомогти автоматизувати завдання, які не вбудовані у процес syslog.

Sophos Firewall XG, як і інші мережеві пристрої також підтримує пересилання журналів з використанням протоколу syslog.

Щоб налаштувати пересилання записів журналів на віддалений syslog-сервер потрібно на сторінці System services у вкладці Log settings додати новий syslog-

сервер та ввести його ім’я, IP-адресу або домен сервера, порт, вказати джерело повідомлень журналів, щоб визначити пристрій, який записав ту чи іншу подію, та формат повідомлень. Також потрібно встановити прапорці біля відповідних сервісів, журнали яких потрібно надсилати на сервер.

Але протокол syslog має суттєвий мінус – дані ним передаються у форматі відкритого тексту, що не є безпечним у випадку передачі записів журналів на віддаленні сервери, наприклад іншим компаніям, які спеціалізуються на забезпеченні інформаційної безпеки мереж підприємств. Для вирішення цієї проблеми, Sophos Firewall надає можливість шифрувати syslog трафік з допомогою протоколу TLS.

Щоб налаштувати безпечне з’єднання між фаєрволом та сервером, можна використати локально підписаний сертифікат або ж зовнішній сертифікат. Перш за все потрібно ввімкнути TLS шифрування на syslog-сервері. Також потрібно згенерувати сертифікат. Для цього на вкладці «Сертифікати» потрібно обрати Центр сертифікації за замовчуванням (англ. Default), натиснути «Згенерувати локально підписаний сертифікат». Після чого ввести потрібні дані та, натиснувши кнопку завантаження, завантажити архів з трьома файлами: RootCertificate.pem, UserCertificate.pem та UserPrivateKey.key. Ці сертифікати потрібно скопіювати у відповідні директорії на syslog-сервері та налаштувати файл конфігурації, ввівши в ньому відповідні імена сертифікатів. Після цих налаштувань потрібно додати syslog-сервер, увімкнувши безпечну передачу записів журналів [18].

2.3.3 Логування з використанням API та протоколу HTTPS

API (Application Programming Interface) – це механізм, який дозволяє двом програмним компонентам спілкуватись між собою за допомогою набору визначень і протоколів. Зазвичай API мають клієнт-серверну архітектуру, тобто програма, яка надсилає запит, є клієнтом, а програма, яка надсилає відповідь, називається сервером [19]. У контексті цієї роботи, ми, як запитувачі журналів подій, виступатимемо у

ролі клієнта, а консоль Sophos Central – у ролі сервера. Схема роботи API зображена на рисунку 2.3.3.1.

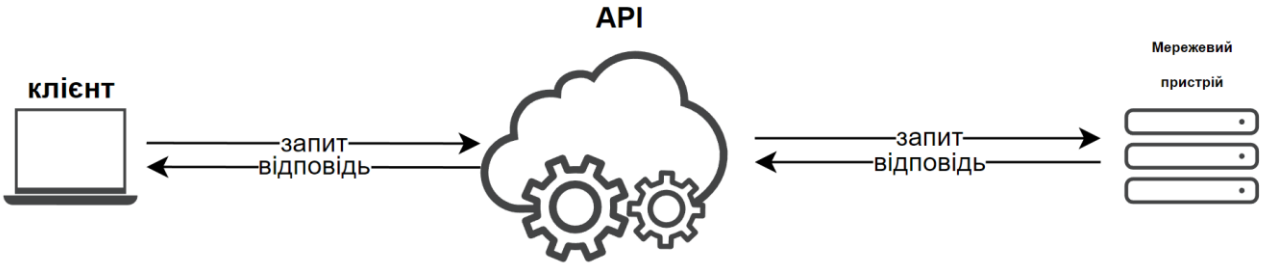


Рисунок 3.2.2.1 – Схема роботи API

Цей спосіб логування використовує HTTP-запити, такі як GET та POST, для отримання журналів подій та їх запису у файл або пересилання на сторонній сервер. Для безпечного передавання інформації використовують захищену версію протоколу HTTP – HTTPS.

Програмна реалізація API для отримання логів від Sophos Firewall XG уже надана компанією Sophos та розміщена у репозиторії Github [20].

Для використання програмного інтерфейсу спочатку потрібно створити облікові дані для доступу через API до консолі керування Sophos Firewall XG. Зробити це можна на відповідній вкладці на порталі Sophos Central. Після цього ми отримаємо два значення – «Client ID» та «Client Secret». Їх потрібно вставити у відповідні поля «client_id» та «client_secret» у файлі config.ini. Після чого потрібно запустити файл «siem.py» та переглянути створений файл results.txt, у якому будуть записані журнали подій за визначений нами термін [21].

2.3.4 SNMP-логування

SNMP (Simple Network Management Protocol) – це стандартний інтернет-протокол прикладного рівня, який використовується для керування пристроями в IP-мережах на основі архітектур TCP/UDP. Він дозволяє відслідковувати керовані мережеві пристрої, такі як, маршрутизатори, комутатори, сервери, міжмережеві

екрани та інші пристрої, які включені через IP через єдину систему керування або програмне забезпечення.

Архітектура SNMP включає:

- станцію керування мережею (Network Management Station або NMS);
- агенти;
- керуюча база даних (Management Information Base);
- керовані компоненти.

Станція керування мережею або Network Management Station – це консоль системи, СКМ віддалено моніторить керовані пристрої, отримує дані, зібрані майстер-агентами, відслідковує продуктивність та надає отриману інформацію в графічному вигляді. Також вбудований менеджер СКМ відповідає за зв'язок з агентами.

Агенти діляться на два види: майстер-агент та підагент або субагент.

Майстер-агент – це програма, яка пов'язує мережеві менеджери та субагенти. Майстер-агент аналізує вхідні запити мережевого менеджера СКМ та пересилає їх до субагентів, отримують інформацію, створюють відповідь та відправляють його менеджеру. Майстер-агент повідомляє менеджера, якщо запит некоректний, невірно сформований або запрошена інформація є недоступною.

Субагент – це програма, яка надається постачальником разом з мережевим пристроєм, використовується в конкретній базі даних (MIB). Субагент збирає інформацію про майстер-агента, налаштовує параметри майстер-агента, відповідає на запити менеджера. У кожного керованого компонента є відповідний субагент.

Керуюча база даних або ж Management Information Base (MIB) є базою даних, яка містить інформацію для управління мережевими пристроями. Інформація з неї може бути запитана та встановлена агентом.

Керованими компонентами є будь-які комп'ютери та мережеві пристрої під'єднані до мережі та з вбудованим субагентом. Окрім маршрутизаторів, комутаторів, серверів, до таких компонентів можуть відноситись IP-камери, IP-

телефони, принтери, тощо. Також до керованих компонентів можна віднести антивірусні програми, системи резервного копіювання даних.

Для отримання даних з мережевих пристроїв, зміни інформації про об’єкт SNMP у керуючій базі даних та відправлення сповіщень використовуються відповідні методи:

- Get – запит, відправлений СКМ на керований пристрій для отримання значень з MIB;
- GetNext – схоже з Get, але отримує значення наступного ідентифікатора об’єкта у дереві MIB;
- GetBulk – використовується для отримання великої кількості даних з таблиці MIB;
- Set – використовується СКМ для зміни параметрів керованого пристрою;
- Response – відправляється СКМ для зміни значення керованого пристрою. Виконується у відповідь на методи GetRequest, GetNextRequest, GetBulkRequest, GetBulkRequest та SetRequest;
- Trap – ініціюється агентом, він використовується для сповіщення СКМ про помилку або подію, яка відбувається на керованому пристрої;
- Inform – схожа з методом «Trap», також ініціюється агентом, але у відповідь МСК повинна надіслати InformResponse.

Також протокол SNMP дозволяє адміністратору керувати різними додатакми та хмарними сервісами. Протокол має достатньо функціоналу для виконання операцій з перепризначення IP-адрес, віддаленого скидання паролів та відслідковування навантаження на сервери з метою отримання сповіщень про перевищення допустимого порогу навантаження [22].

2.4 Висновки до другого розділу

У другому розділі кваліфікаційної роботи було розглянуто етапи аналізу подій в інформаційно-комунікаційній системі, механізм збирання, опрацювання та збереження журналів подій на основі сервісів Logstash, Elasticsearch та Kibana, також відомі як ELK стек. Також були проаналізовані методи логування, зокрема методи з агентами та без, логування з використанням протоколу Syslog, отримання журналів подій з допомогою спеціальних API та збір інформації через протокол SNMP.

3 РОЗРОБКА ТА ТЕСТУВАННЯ КОНФІГУРАЦІЇ ДЛЯ АНАЛІЗУ ЖУРНАЛІВ ПОДІЙ

3.1 Розгортання та використання стеку ELK для обробки логів

Для використання ELK стеку, перш за все потрібно окремо встановити його компоненти у наступному порядку:

- Elasticsearch;
- Kibana;
- Logstash;
- Beats;
- APM;
- Elasticsearch Hadoop.

Встановлення програм саме у такому порядку гарантує, що компоненти, від яких залежить кожен продукт, будуть на своєму місці [23]. Втім, для виконання поставленого завдання можна не встановлювати Beats, APM та Elasticsearch Hadoop.

Встановити ELK стек можна використовуючи сервіси хмарних обчислень Amazon Web Services (AWS), Google Cloud Platform (GCP) або Microsoft Azure або ж встановлюючи стек локально на комп’ютер чи сервер.

Для вирішення поставленої у кваліфікаційній роботі задачі було встановлено ELK стек локально. Як зазначалось вище, першим потрібно встановити Elasticsearch. Для цього з офіційного сайту завантажуємо потрібний файл встановлення з розширенням .msi для Windows10 або архів (tar.gz для MacOS та будь-яких Linux-систем, .zip для встановлення на Windows). Також доступні пакети для встановлення на системи, створені на основі Debian (Ubuntu, Debian, тощо), системи на основі RPM (Centos, Red Hat, тощо) та завантаження Elasticsearch у вигляді контейнера Docker.

Оскільки у роботі використовується комп’ютер з встановленою на ньому системою Windows10, встановлення Elasticsearch проводитиметься з використанням

програми встановлення з розширенням .msi. Спосіб встановлення з архіву є менш зручним, оскільки виконується у командному рядку, в той час як файл встановлення є майстром установки.

Після запуску потрібно вказати папку, куди встановиться Elasticsearch. Наступним кроком є вибір як саме запускатиметься Elasticsearch – як служба при кожному запуску операційної системи або вручну лише при потребі. Третім етапом встановлення є налаштування сервера. Серед доступних опцій:

- ім’я кластера;
- ім’я вузла (node);
- роль вузла;
- кількість доступної оперативної пам’яті;
- налаштування мережі (імена хостів, номери портів, тощо).

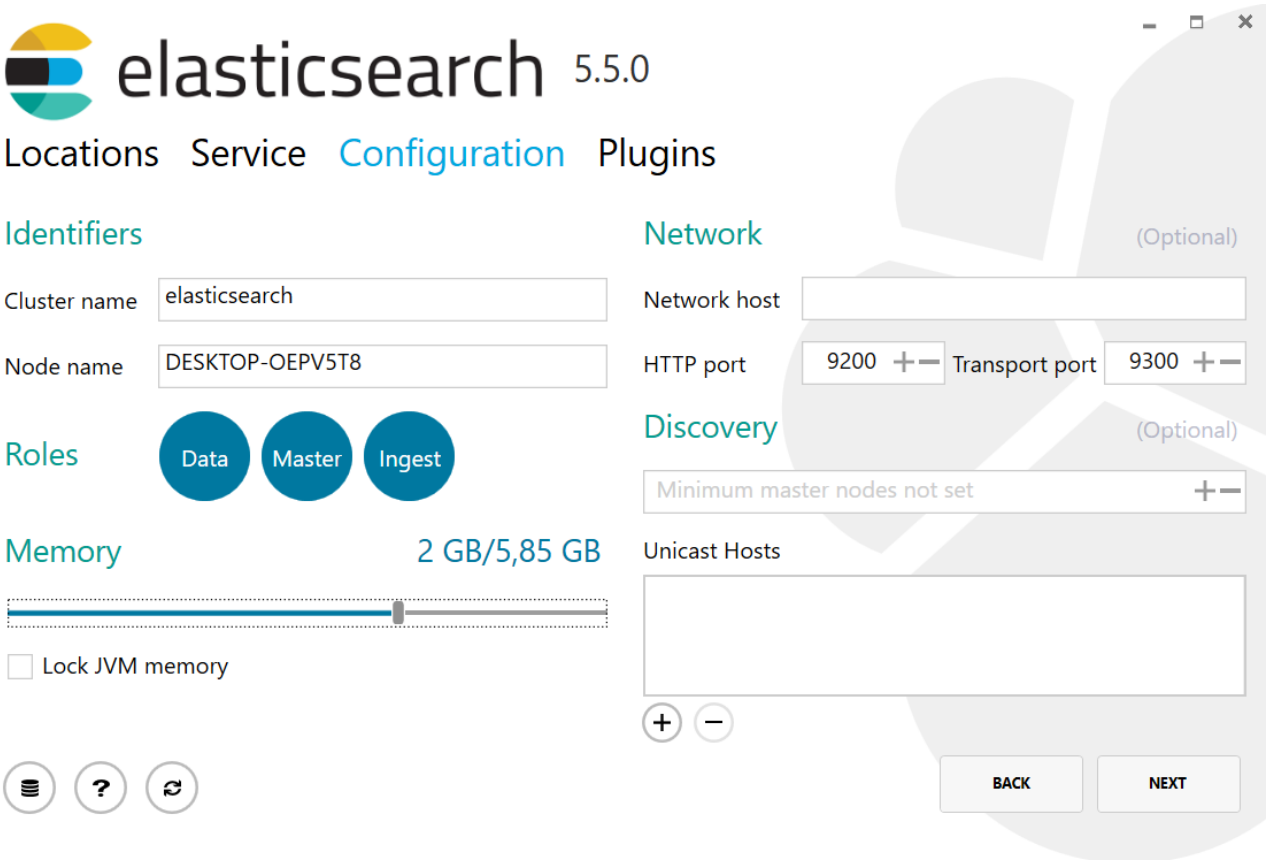


Рисунок 3.1.1 – Третій крок встановлення Elasticsearch

Після закінчення встановлення, відкриваємо командний рядок, переходимо у папку, де встановлений Elasticsearch та запускаємо його командою

«bin\elasticsearch.exe» або запускаємо сервіс з використанням відповідної програми. У результаті, на адресі локального хоста (127.0.0.1) з портом 9200 побачимо результат, який зображений на рисунку 3.1.1.

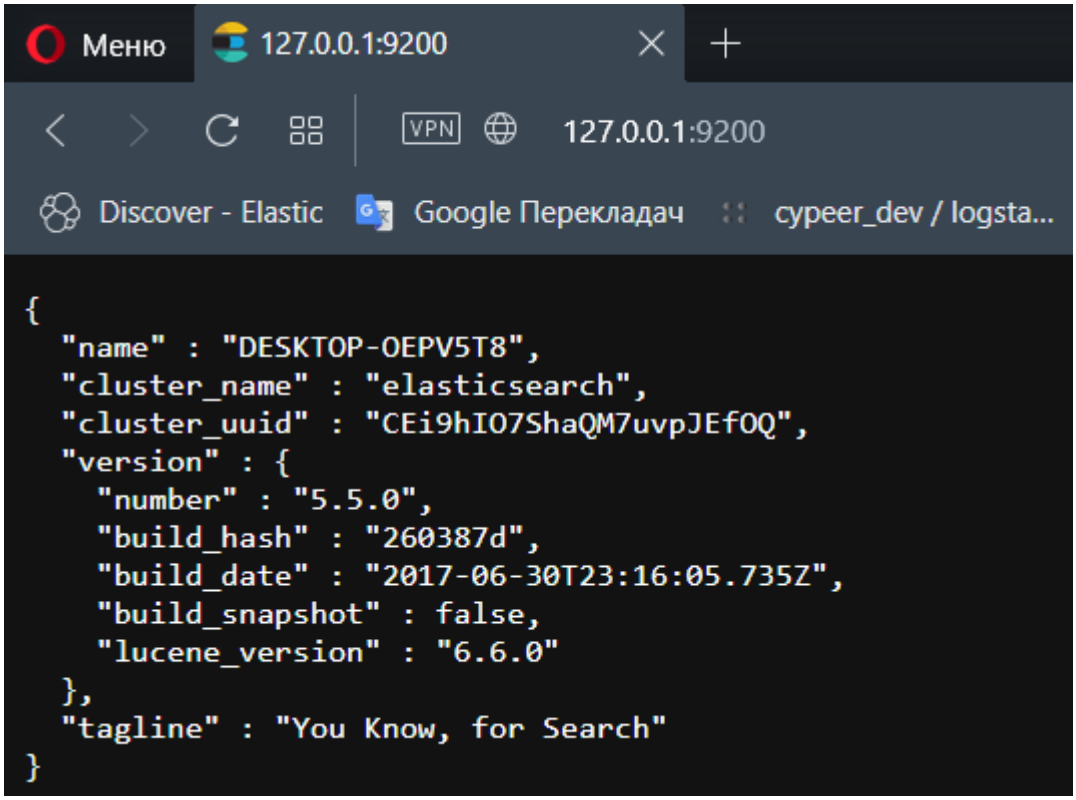


Рисунок 3.1.1 – Результат запуску Elasticsearch

Наступним кроком є встановлення Kibana. Для цього завантажуємо та розпаковуємо відповідний архів, після чого у командному рядку потрібно перейти у директорію, де розпакована Kibana та запустити її командою «bin\kibana.bat». У результаті побачимо повідомлення про те, що статус змінився з ініціалізації до зеленого (Status changed from uninitialized to green – Ready) [24]. Щоб пересвідчитись у коректній роботі сервісу, потрібно перевірити localhost на порті 5601 (порт Kibana за замовчуванням). Вигляд Kibana поданий на рисунку 3.1.2.

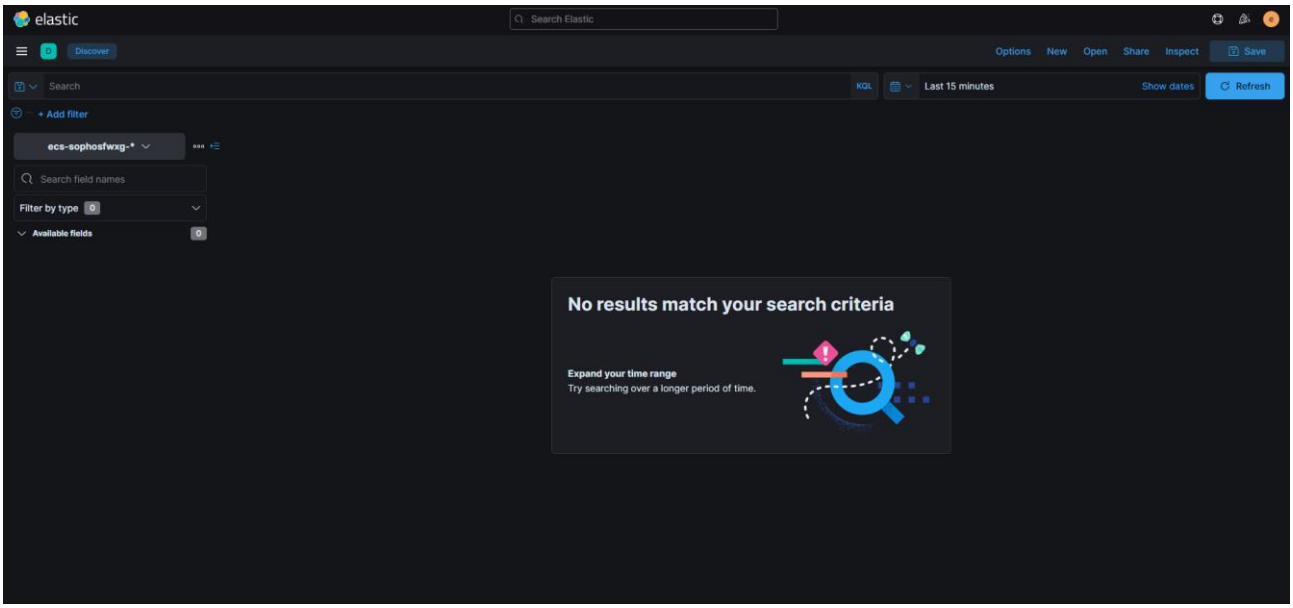


Рисунок. 3.1.2 – Вигляд Kibana

Третім потрібним компонентом ELK стеку є Logstash. Його встановлення аналогічне зі встановленням Kibana. Щоб протестувати цей сервіс, достатньо запустити простий конфігураційний файл без жодний плагінів та опрацювати файл журналу. Як результат, у Kibana ми можемо побачити лог-файл, опрацьований пайплайном Logstash:

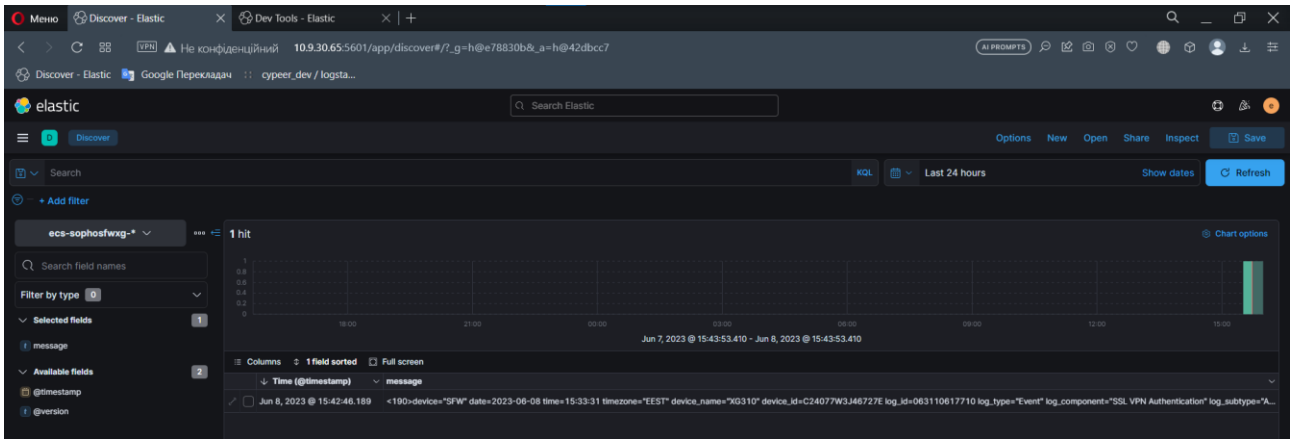


Рисунок 3.1.3 – Файл журналу завантажений у Kibana

Для забезпечення безпеки інформації використовується пакет X-pack, який встановлюється окремо для кожного модуля – Elasticsearch, Kibana-plugin та Logstash-plugin. Ідея полягає у створені користувачів та наданням їм можливостей, відповідно до виданих привілеїв, наприклад «читання», «запис», «видалення», тощо.

Для безпеки документів в індексі можна застосувати два види безпеки – безпека на рівні документа та на рівні поля.

Безпека на рівні документа обмежує документи, до яких користувачі мають доступ для читання. Зокрема, обмеження діє на документи, до яких можна отримати доступ через API для читання документів [25].

Безпека на рівні полів обмежує поля, до яких користувач може отримати доступ для читання. Аналогічно безпеці на рівні документа, цей тип безпеки обмежує доступ до полів через спеціальні API [26].

Для активації цих типів безпеки потрібно виконати відповідні POST-запити використовуючи вбудовані інструменти розробки – DevTools.

3.2 Створення конфігураційного файлу для аналізу

Наступним кроком є створення конфігураційного файлу Logstash. Конфігурація складається з двох обов'язкових елементів: канал для вхідної інформації (input) та канал для вихідної інформації (output). Цього буде достатньо для отримання інформації на вході (input) та її пересилання на інший адрес на виході (output).

Втім для аналізу журналів подій або іншої інформації необхідно додати хоча б один фільтр-плагін, який міститиме потрібні плагіни для витягнення інформації з логів, їх трансформації, тощо. Загальний вигляд Logstash-конфігурації поданий у лістингу 3.2.1.

Лістинг 3.2.1 – Загальна структура Logstash конвеєра

```
input {

}
filter {

}
output {

}
```

На вході потрібно налаштувати потрібні плагіни введення, наприклад отримання логів через протокол Syslog, HTTP, читання інформації з файлу, отримання даних з уже існуючого кластера Elasticsearch.

Оскільки на міжмережевому екрані Sophos Firewall XG було налаштовано syslog-логування, для input було обрано плагін syslog. Вигляд плагіну після налаштування поданий у лістингу 3.2.2.

Лістинг 3.2.2

```
input {
    syslog {
        port => 514
        host => 10.10.34.12
    }
}
```

Значення «port» визначає порт для прослуховування. Параметр «host» містить в собі адрес, який прослуховується.

Наступним кроком є налаштування частини filter. У ній відбувається парсинг, тобто розбір, логів на поля, редагування значень полів, створення нових полів або видалення непотрібних.

Одним з найважливіших плагінів для розбору журналів подій на компоненти є grok-плагін, який витягує поля з логів відповідно до написаної схеми – grok-виразу.

Втім, перш ніж почати створювати grok-вирази, потрібно врахувати у якій структурі Elasticsearch зберігає дані. Оскільки Elasticsearch є NoSQL базою даних, дані тут зберігаються неструктуровано. Кожне окреме повідомлення зберігається як документ у форматі JSON, що є аналогом SQL таблиці. Сукупність документів об’єднуються в один індекс за аналогією з базою даних SQL. Структура документу подана на рисунку 3.2.1.

```
{
  "_index": "ecs-sophosfwxg-alias",
  "_type": "_doc",
  "_id": "DAMHm4gBDWxF7Wj95z6k",
  "_version": 1,
  "_score": 1,
  "_source": {
    "message": "<190>device=\"SFW\" date=2023-06-08 time=15:33:31 timezone=\"EEST\" device_name=\"XG310\" device_id=C24077W3J46727E log_id=063110617710 log_type=\"Event\"
    log_component=\"SSL VPN Authentication\" log_subtype=\"Authentication\" status=\"Successful\" priority=Information user_name=\"pavlo.pylypiv@gmail.com\" usergroupname=\"\"
    auth_client=\"SSLVPN\" auth_mechanism=\"AD\" reason=\"\" src_ip=188.42.212.31 message=\"User pavlo.ppylypiv@gmail.com authenticated successfully to login to SSLVPN through AD
    authentication mechanism\" name=\"\" src_mac=",
    "@timestamp": "2023-06-08T12:42:46.189Z",
    "@version": "1"
  },
  "fields": {
    "@timestamp": [
      "2023-06-08T12:42:46.189Z"
    ],
    "@version": [
      "1"
    ],
    "@version.keyword": [
      "1"
    ],
    "message": [
      "<190>device=\"SFW\" date=2023-06-08 time=15:33:31 timezone=\"EEST\" device_name=\"XG310\" device_id=C24077W3J46727E log_id=063110617710 log_type=\"Event\" log_component=\"SSL
      VPN Authentication\" log_subtype=\"Authentication\" status=\"Successful\" priority=Information user_name=\"pavlo.pylypiv@gmail.com\" usergroupname=\"\" auth_client=\"SSLVPN\"
      auth_mechanism=\"AD\" reason=\"\" src_ip=188.42.212.31 message=\"User pavlo.ppylypiv@gmail.com authenticated successfully to login to SSLVPN through AD authentication mechanism\"
      name=\"\" src_mac="
    ]
  }
}
```


Рисунок 3.2.1 – Структура документу Elasticsearch

Звідси випливає, що поля в Elasticsearch зберігаються у форматі «ключ : значення», де ключ може бути підполем іншого поля, наприклад «[file][hash][sha256]», де поле «sha256» є підполем «hash», яке у свою чергу є підполем «file».

Також варто врахувати, що найкраще називати поля згідно визначених правил, зазначених у Elastic Common Schema. Вона створена для максимізації сумісності та повторного використання полів, а також для уніфікації імен полів, щоб їх можна було використати для порівняння з інформацією з інших індексів [28].

Схема визначає набір кореневих полів, наприклад, source. , destination. , threat. , file. , network. , тощо, та їхні можливі підполя. Наприклад, source.ip, destination.port, threat.name, network.protocol та інші. Звісно використання власних полів не забороняється, але їх імена потрібно враховувати для подальшої кореляції.

Для створення частини фільтру файлу конфігурації можна використовувати різні плагіни. Одним з найважливіших для аналізу структурованих даних, наприклад, записів журналу подій, є плагін grok.

Grok використовує регулярні вирази, як шаблонні, тобто стандартні, так і написані самим розробником для більш специфічних потреб. З їх допомогою Logstash здатний витягувати дані з повідомлення та поміщати їх у відповідні поля документу JSON. Стандартний вигляд grok-виразу є наступним:

%{SYNTAX:SEMANTIC}.

SYNTAX позначає шаблон, який буде використано для тексу у журналі події, в той час як SEMANTIC надає ідентифікатор для цього синтаксису в аналізованих журналах. Іншими словами, SEMANTIC це назва поля, яку ми присвоюємо інформації, яка підійшла під SYNTAX, тобто шаблон. Наприклад для значення IP-адреси 10.10.132.42 буде застосований шаблон %{IP:[source][ip]}.

%{IP} – це вже готовий шаблон, який підбере тільки значення IP-адрес четвертої та шостої версій. Окрім нього, також існують шаблони які дістають лише інформацію без пробілів – %{NOTSPACE}, інформацію до певного знаку – %{DATA}, числа – %{NUMBER}, MAC-адреси – %{MAC}, дату та час різних форматів – %{SYSLOGTIMESTAMP}, %{TIMESTAMP_ISO8601}, тощо.

Наприклад, для парсингу журналу події автентифікації Sophos Firewall XG, можна використовувати grok-плагін разом з регулярним виразом, поданими у лістингу 3.2.3.

Лістинг 3.2.3 – Grok-вираз для парсингу журналу події

```
<%{NUMBER:[log][syslog][priority]}>device="%{DATA:[observer][ven
dor]}" date=%{DATA:date} time=%{DATA:time} timezone="%{DATA:timezone}"
device_name="%{DATA}"                  device_id=%{DATA:[observer][id]}
log_id=%{NUMBER:[event][id]}    log_type="%{DATA:[event][subdataset]}"
log_component="%{DATA:[event][dataset]}"
log_subtype="%{DATA:[observer][action]}"
status="%{DATA:[event][outcome]}"        priority=%{DATA:[log][level]}
user_name="%{DATA:[source][user][name]}"
usergroupname="%{DATA:[source][user][group][name]}"
auth_client="%{DATA:[network][authentication][client]}"
auth_mechanism="%{DATA:[network][authentication][mechanism]}"
reason="%{DATA:[event][reason]}"          src_ip=(%{IP:[source][ip]}|)
message="%{DATA:[event][reason]}"                        name="%{DATA}"
src_mac=(%{MAC:[source][mac]}|)
```

Загальний вигляд grok-плагіну поданий у лістингу 3.2.4.

Лістинг 3.2.4 – Структура плагіну grok

```
grok {
    match => {
        "field" => [
```

```
                'grok1',
                'grok2'
            ]
        }
        tag_on_failure => ['_grok_failure']
    }
```

Де параметр «field» вказує яке саме поле буде аналізуватись з допомогою масиву регулярних виразів, записаних у квадратних дужках.

У результаті проходження файлу журналу крізь даний плагін, у Kibana відображається уже проаналізований лог з усією інформацією, яку було можливо дістати.

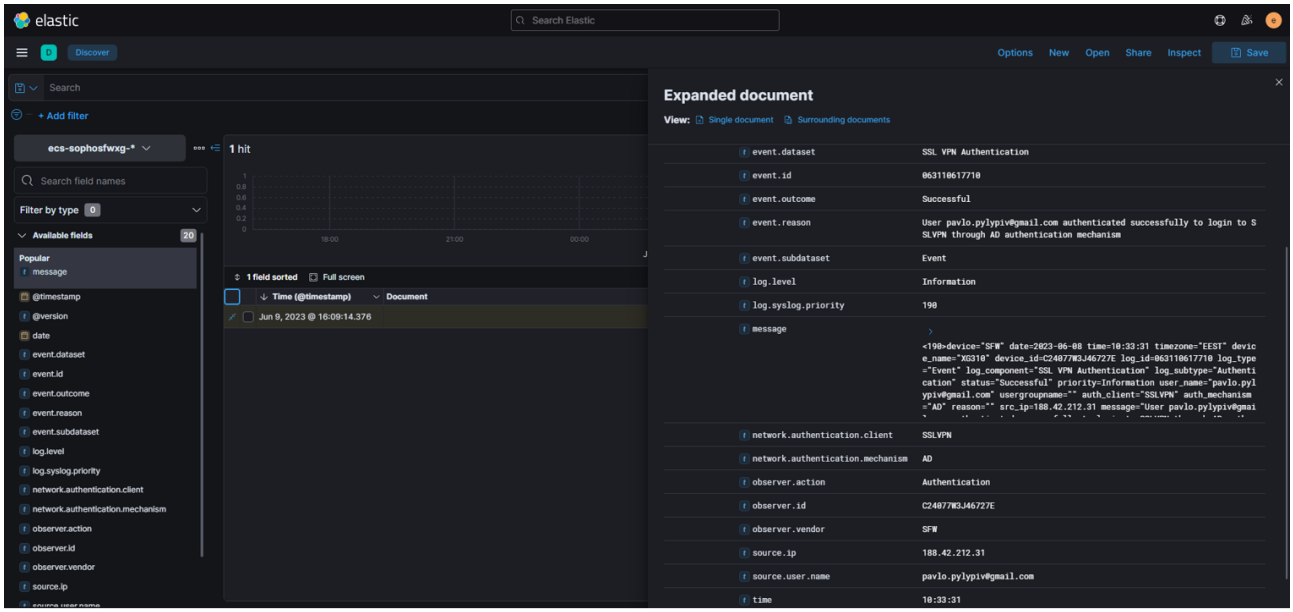


Рисунок 3.2.2 – Проаналізований лог-файл у Kibana

Окрім плагіну grok, також існують спеціальні плагіни для проведення операцій над новостворених або уже існуючими полями (плагін mutate), створення коректної мітки часу, яка витягнута з журналу події (плагін date), агрегація даних за спільними критеріями (плагін aggregate), впровадження коду мовою Ruby (плагін ruby).

3.3 Тестування конфігурації та створення інформаційної панелі

Тестування конвеєра Logstash можна здійснити звичайним запуском та передачею через нього потрібних даних. Якщо конфігурація написана правильно, тобто немає синтаксичних помилок, файл запуститься та почне опрацьовувати дані. У протилежному випадку помилка буде виведена у консоль.

Також logstash-плагіни, зокрема grok, сигналізують про невдачу або невідповідність даних до регулярних виразів додаючи у поле «tags» відповідні значення – за замовчуванням вони можуть набувати значень «_grokparsefailure» для grok-плагіна або «_mutate_error» для плагіну mutate. Решта плагінів теж мають свої теги за замовчуванням. Також ці теги можна налаштовувати вручну, що є зручним, коли дані опрацьовують декілька grok або інших плагінів.

Для перевірки правильності конфігурації достатньо пересвідчитись у відсутності значень поля «tags», що означатиме те, що усі журнали подій мали відповідні регулярні вирази, а помилки плагіну mutate відсутні.

У результаті були отримані опрацьовані файли журналів, які відображаються у Kibana та зображені на рисунку 3.3.1

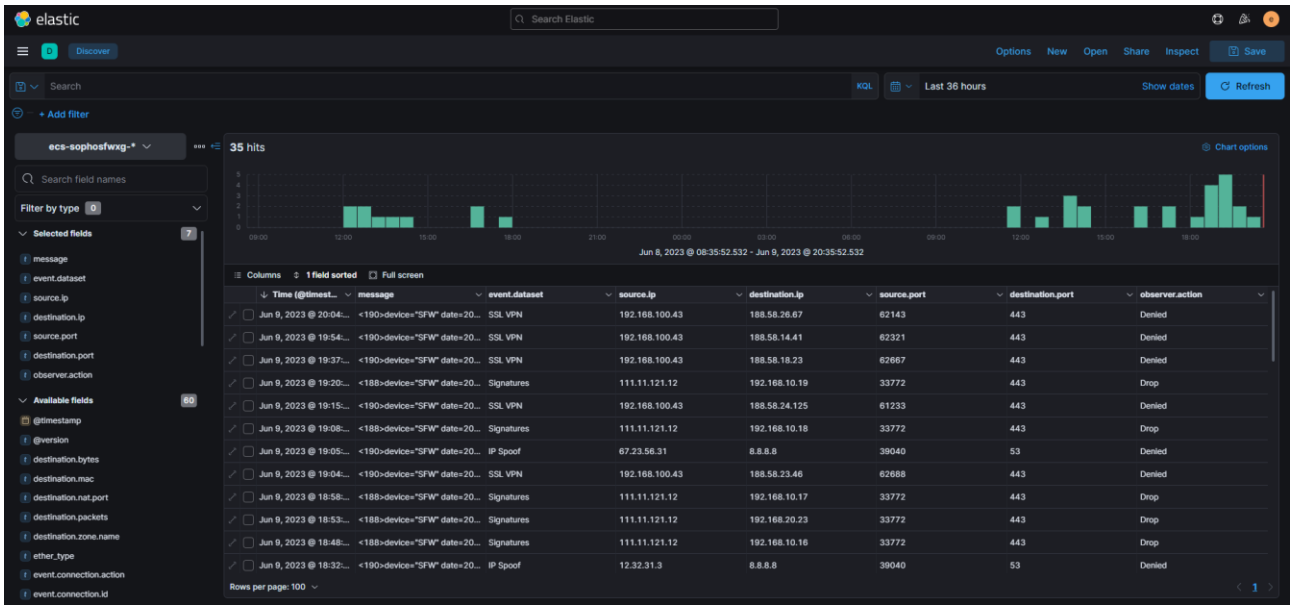


Рисунок 3.3.1 – Структуровані журнали подій у середовищі Discover

Використовуючи Discover уже можна проводити аналіз подій, оскільки інструменти дозволяють здійснити пошук за словами чи реченням у повідомленні, відсортувати дані за міткою часу або вказати за який проміжок часу потрібно вивести інформацію, відфільтрувати дані за існуванням або значенням поля. Втім для більш комплексного аналізу, Kibana надає можливість візуалізації даних об'єднуючи їх в інформаційні панелі.

Для створення інформаційної панелі достатньо натиснути відповідну кнопку у вкладці «Dashboard», втім вона буде пустою. Наступним кроком є створення візуалізацій. На вибір Kibana пропонує створити візуалізації на основі агрегацій, візуалізації з використанням машинного навчання, власноруч створені візуалізації та мапи, які працюють з полями широти та довготи.

Найкраще для візуалізації даних журналів подій використовувати візуалізації на основі агрегацій. Серед них доступними є графіки, метрики кількох видів (metric, gauge, goal), вертикальні та горизонтальні гістограми, кругові діаграми та таблиці. Також, при умові використання плагіну geoip, який геолокує IP-адреси, доцільно використовувати мапи.

Для їх створення потрібно обрати «Візуалізації на основі агрегацій» (Aggregation based) та вибрати потрібний тип. Наступним кроком потрібно обрати індекс, дані з якого будуть візуалізованими, після чого у конструкторі візуалізації обрати потрібну агрегацію чи агрегації, обрати потрібні поля та натиснути кнопку «Update». Процес створення візуалізації з IP-адресами джерела та їх адресами призначення поданий на рисунку 3.3.2.

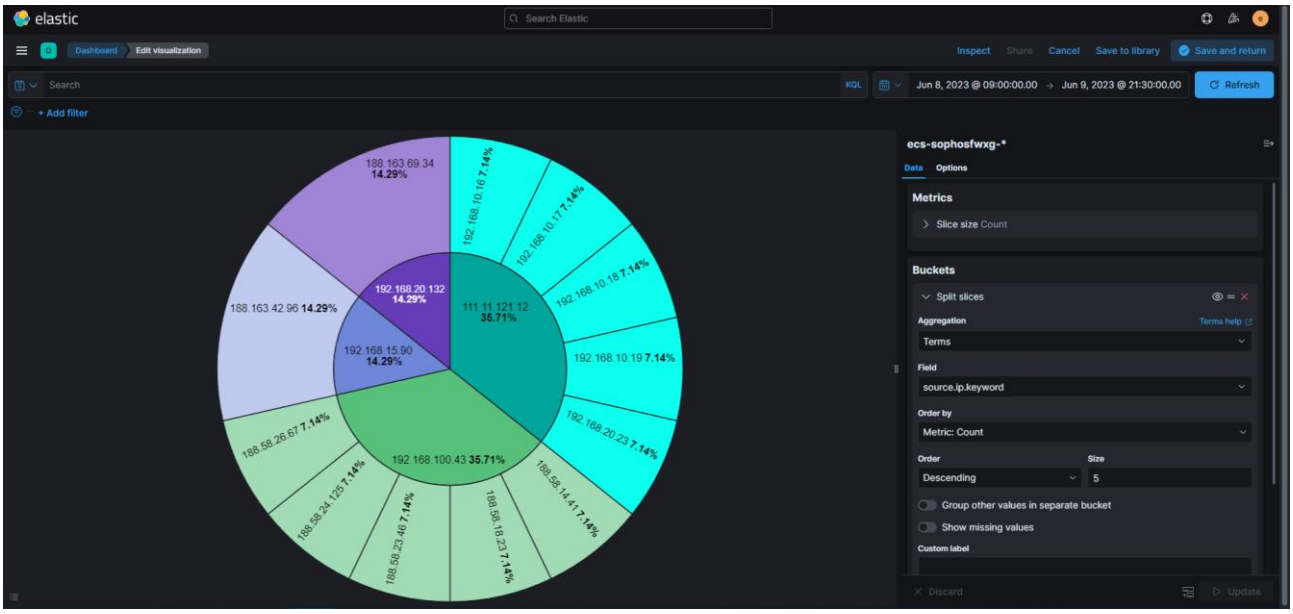


Рисунок 3.3.2 – Процес створення візуалізації

У результаті була створена інформаційна панель з візуалізаціями інформації з журналів подій Sophos FWXG. Було використано візуалізації таких типів, як графік, метрики, кругова діаграма, стовпчаста діаграма, таблиця та хмарка тегів. Частина інформаційної панелі подана на рисунку 3.3.3. Вся панель подана у додатку А.

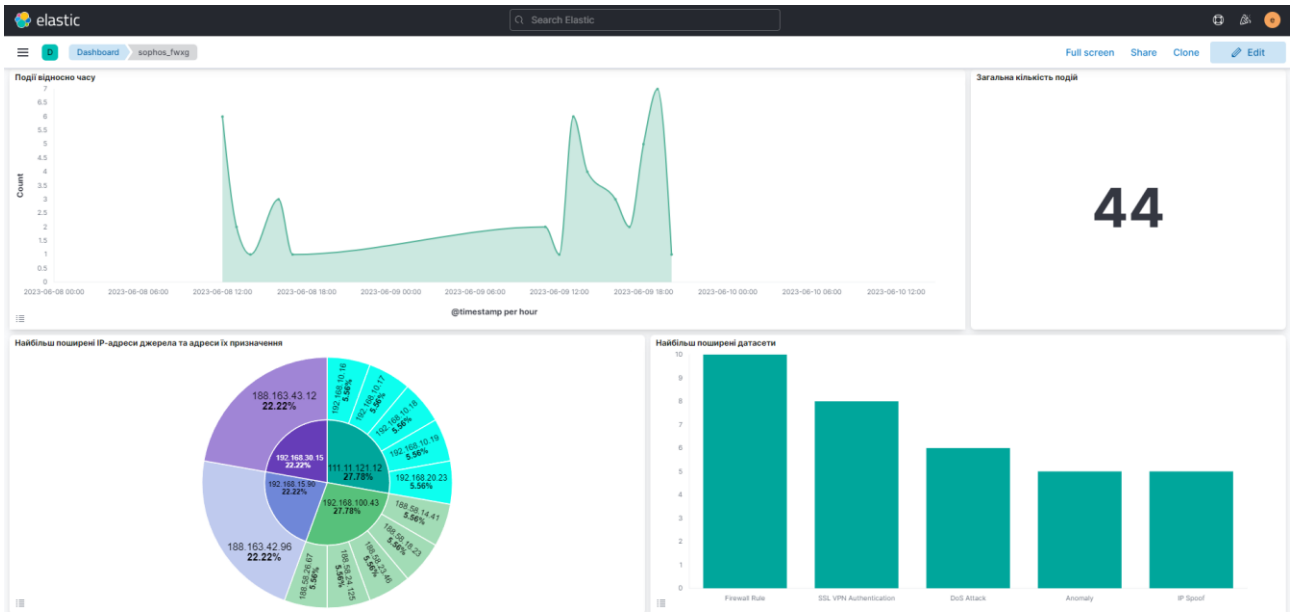


Рисунок 3.3.3 – Частина створеної інформаційної панелі

3.4 Висновки до третього розділу

У третьому розділі кваліфікаційної роботи було розгорнено ELK стек для аналізу файлів журналів подій. З метою забезпечення інформації, що обробляється був встановлений додатковий пакет X-Pack, який дозволяє створювати користувачів та надавати їм доступ до сервісів відповідно їх привілеїв.

Було спроектовано та протестовано конфігураційний файл Logstash для аналізу та розбиття журналів подій на поля. Створена інформаційна панель для зручнішого аналізу подій міжмережевого екрану Sophos FW XG.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Електробезпека при експлуатації комп’ютерного обладнанання

Заходи щодо усунення небезпеки ураження електричним струмом зводяться до правильного устаткування та електричних кабелів. Інші заходи щодо забезпечення електробезпеки, збігаються з загальними заходами пожеже- та електробезпеки.

В якості профілактичних заходів для забезпечення пожежної безпеки слід використовувати приховану електромережу, надійні розетки з пожежебезпечних матеріалів, силові мережі живлення устаткування виконувати кабелями, розрахованими на підключення в 3-5 разів більшого навантаження, включати й виключати живлення обладнання за допомогою штатних вимикачів. Потрібно регулярно робити очистку внутрішніх частин комп'ютерів, іншого устаткування від пилу, розташовувати комп'ютери на окремих неспаленних столах. Для запобігання іскріння необхідно рідше встромляти і виймати штепсельні вилки з розеток.

Вимоги електробезпеки приміщень, де встановлені електронно-обчислювальні машини (ЕОМ) та комп’ютерне обладнання подані у ДНАОП 0.00-1.31-18. Відповідно до цього нормативного документу під час проектування систем електропостачання, монтажу основного електрообладнання та електричного освітлення будівель та приміщень для ЕОМ необхідно дотримуватись вимог Правил влаштування електроустановок (ПВЕ), Правила технічної експлуатації (ПТЕ), Правила безпечної експлуатації (ПБЕ), ДБН В. 2.5-23-2018 «Проектування електрообладнання об’єктів цивільного призначення», Правила пожежної безпеки в Україні, а також вимог нормативно-технічної експлуатаційної документації заводу-виробника.

Комплекс необхідних заходів з техніки безпеки визначається, виходячи з видів електроустановки, її номінальної напруги, умов середи, типу приміщення і доступності електроустаткування.

ЕОМ є однофазним споживачем електроенергії, що живиться від змінного струму 220 В від мережі із заземленою нейтраллю. ПК відноситься до електроустановок до 1000 В закритого виконання, всі струмопровідні частини знаходяться в кожухах. За способом захисту людини від ураження електричним струмом, ЕОМ і периферійна техніка повинні відповідати 1 класу захисту.

Лінія електромережі для живлення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ виконується як окрема групова трипровідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів і прокладається від стійки групового розподільчого щита, розподільчого пункту до розеток живлення

У приміщенні, де одночасно експлуатується або обслуговується більше п'яти персональних ЕОМ, на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення [29].

Неприпустимим є підключення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ до звичайної двопровідної електромережі, в тому числі — з використанням перехідних пристроїв.

При розташуванні в приміщенні за його периметром до 5 персональних ЕОМ, використанні трипровідникового захищеного проводу або кабелю в оболонці з негорючого або важкогорючого матеріалу дозволяється прокладання їх без металевих труб та гнучких металевих рукавів.

Металеві труби та гнучкі металеві рукави заземлюються. Заземлення повинно відповідає вимогам ДНАОП 0.00-1.21-18 "Правила безпечної експлуатації електроустановок споживачів". Заземлені конструкції, що знаходяться у приміщеннях (батереї опалення, водопровідні труби, кабелі із заземленим відкритим екраномЦ), мають бути надійно захищені діелектричними щитками або сітками від випадкового дотику.

При використанні комп’ютерної техніки є неприпустимим:

- експлуатація кабелів та проводів з пошкодженою або такою, що втратила захисні властивості за час експлуатації, ізоляцією; залишення під напругою кабелів та проводів з неізольованими провідниками;
- застосування саморобних продовжувачів, які не відповідають вимогам ПВЕ до переносних електропроводок;
- застосування для опалення приміщення нестандартного (саморобного) електронагрівального обладнання або ламп розжарювання;
- користування пошкодженими розетками, розгалужувальними та з’єднувальними коробками, вимикачами та іншими електровиробами, а також лампами, скло яких має сліди затемнення або випинання;
- підвішування світильників безпосередньо на струмопровідних проводах, обгортання електроламп і світильників папером, тканиною та іншими горючими матеріалами, експлуатація їх зі знятими ковпаками (розсіювачами);
- використання електроапаратури та приладів в умовах, що не відповідають вказівкам (рекомендаціям) підприємств-виготовлювачів.

Під час експлуатації враховуються наступні заходи безпеки: конструктивні, схемно-констуктивні та експлуатаційні.

Конструктивні заходи забезпечують захист від випадкового дотику до струмопровідних частин за допомогою захисних оболонок і ізоляції струмоведучих частин. Ступінь захисту оболонки повинен відповідати класу пожежонебезпечної зони приміщення П-IIа. Для ступеня захисту оболонки IP-44.

Схемно-конструктивні заходи призначені для забезпечення захисту від ураження електричним струмом при дотику до металевих оболонок, які можуть опинитися під напругою в результаті аварії. У даному приміщенні в комп'ютерах застосовується занулення. Біля монітора передбачена подвійна ізоляція.

До експлуатаційних заходів відноситься дотримання правил техніки безпеки при роботі з високою напругою і запобіжні заходи:

- дозвіл на монтаж, обслуговування та ремонт ЕОМ, заміна деталей, блоків повинні здійснюватися тільки при повному відключенні ЕОМ від живлення;

- заземлені конструкції приміщення повинні бути надійно захищені діелектричними щитками або сітками для запобіганню випадковим дотикам.

4.2 Надзвичайні ситуації: визначення причини, класифікація

Основними причинами виникнення надзвичайних ситуацій є:

- аварії і катастрофи (на виробництві, транспорті, інженерних мережах і т.ін.);
- стихійні лиха (природні катаклізми): землетруси, бурі, урагани, повені, снігові замети і т.ін;
- епідемії, епізоотії, епіфітотії (значні розповсюдження інфекційних захворювань або уражень відповідно серед людей, сільськогосподарських тварин і рослин);
- збройні конфлікти та інші фактори соціального і політичного характеру.

Аварія — небезпечна подія техногенного характеру, що створює на об'єкті, території, або акваторії загрозу для життя і здоров'я людей і призводить до руйнування будівель, споруд, обладнання і транспортних засобів, порушення виробничого або транспортного процесу чи завдає шкоди довкіллю.

Катастрофа — великомасштабна аварія з тяжкими, трагічними наслідками.

Вивчення причин виникнення виробничих аварій і катастроф свідчить про їх велике різноманіття, але за суттю ці причини можна об'єднати в дві групи.

Перша — це проектно-виробничі помилки і порушення (помилки при проектуванні підприємств, порушення будівельних норм і правил, низька якість будівельних робіт, використаних матеріалів і конструкцій, порушення техніки безпеки і технологічних процесів виробництва, відсутність постійного контролю за потенційно небезпечними об'єктами).

Друга група причин обумовлена тим, що не всі явища природи пізнані.

Великі темпи сучасного науково-технічного прогресу створили умови для великої концентрації радіаційно-, хімічно-, та вибухонебезпечних виробництв. По залізницям і трубопроводам транспортуються в великій кількості небезпечні

речовини. В наслідок цього зросла ймовірність виникнення значних аварій і катастроф.

Стихійні лиха є причиною утворення катастрофічних наслідків. За даними ООН за останні 50 років наслідки стихійних лих відчули більш ніж 1 млрд. людей, в них загинуло понад 2 млн. [30]

На території України можуть виникати НС природного характеру досить часто і у великих масштабах. Так, землетрус силою 9 балів може охопити західні, південно- західні регіони і Крим на загальній площі біля 27 тис.км^2. Прибережні райони басейну Чорного моря можуть виявитися під впливом цунамі (морські хвилі від підземного землетрусу). Щорічно окремі райони потерпають від дій бурь, ураганів, повеней та інших явищ. Особливо катастрофічним була повінь внаслідок підриву росіянами дамби Каховської ГЕС в червні 2023.

Війна завжди була великим лихом. Людство Землі перенесло більше 14500 воєн, в яких загинуло 3640млн. людей [31]. На сьогодні накопичена велика кількість сучасної зброї в тому числі ядерної, і сучасних засобів доставки її до цілей: міжконтинентальних балістичних ракет (МБР), підводних човнів-ракетоносців, стратегічної й тактичної авіації, що дозволяють доставити заряди до цілей в короткі терміни. Час польоту МБР на відстань 11-12 тис.км. складає всього 30-40 хв.

Враховуючи масштабність і збільшену ймовірність виникнення НС, перед суспільством існує проблема захисту населення, матеріальних цінностей і навколишнього середовища в умовах мирного і воєнного часу. Вирішення цієї проблеми базується на завчасному прогнозуванні та оцінки наслідків можливих НС в конкретному регіоні, на об'єкті і проведенні заходів щодо запобігання НС і зниженню їх негативних наслідків. Прогнозування обстановки можливе на знанні характеристик осередків ураження, що утворюються в разі виникнення надзвичайних ситуацій.

Осередком ураження (ОУ) називається територія, на якій в результаті дії уражаючих факторів виникли руйнування будівель і споруд, пожежі, зараження атмосфери і місцевості та ураження людей, сільськогосподарських тварин і рослин.

ОУ може утворитися під впливом одного уражаючого фактора (простий), або під впливом декількох первинних і вторинних уражаючих факторів (складний).

Відповідно до причин походження подій, що можуть зумовити виникнення НС на території України, розрізняються:

- НС техногенного характеру — транспортні аварії (катастрофи), пожежі, аварії з викидом небезпечних речовин, руйнуванням споруд та будівель, аварії на інженерних мережах і спорудах життєзабезпечення, гідродинамічні аварії на греблях, дамбах;
- НС природного характеру — небезпечні геологічні, метеорологічні, гідрологічні морські та прісноводні явища, деградація грунтів чи надр, природні пожежі, зміна стану повітряного басейну, інфекційна захворюваність людей, сільськогосподарських тварин, масове ураження сільськогосподарських рослин хворобами чи шкідниками, зміна стану водних ресурсів та біосфери;
- НС соціально-політичного характеру, пов'язані з протиправними діями терористичного і антиконституційного спрямування: здійснення або реальна загроза терористичного акту (збройний напад, захоплення і затримання важливих об'єктів, ядерних установок і матеріалів, систем зв'язку та телекомунікацій, напад чи замах на екіпаж повітряного або, морського судна), викрадення (спроба викрадення) чи знищення суден, захоплення заручників, встановлення вибухових пристроїв у громадських місцях, викрадення або захоплення зброї, виявлення застарілих боєприпасів.

Надзвичайні ситуації воєнного характеру, пов'язані з наслідками застосування зброї масового ураження або звичайних засобів ураження, під час яких виникають вторинні фактори ураження населення внаслідок зруйнування атомних і гідроелектричних станцій, складів і сховищ радіоактивних і токсичних речовин та відходів, нафтопродуктів, вибухівки, транспортних та інженерних комунікацій.

НС екологічного характеру — зміна стану повітряного та водного басейнів внаслідок викидів небезпечних хімічних, радіоактивних і біологічних речовин.

Відповідно до територіального поширення, обсягів заподіяних або очікуваних економічних збитків, кількості людей, які загинули, за класифікаційними ознаками визначаються чотири рівні надзвичайних ситуацій:

- Загальнодержавний;
- регіональний;
- місцевий;
- об'єктовий.

До загальнодержавного рівня відноситься НС, яка розвивається на території двох та більше областей або загрожує транскордонним перенесенням, а також у разі, коли для її ліквідації необхідні матеріальні і технічні ресурси у обсягах, що перевищують власні можливості окремої області.

До регіонального рівня відноситься НС, яка розгортається на території двох та більше адміністративних районів або загрожує перенесенням на територію суміжної області України, а також у разі, коли для її ліквідації необхідні матеріальні і технічні ресурси у обсягах, що перевищують власні можливості окремого району.

До місцевого рівня відноситься НС, яка виходить за межі потенційно небезпечного об'єкта, загрожує поширенням самої ситуації або її вторинних наслідків на довкілля, сусідні населені пункти, інженерні споруди, а також у разі, коли для її ліквідації необхідні матеріальні і технічні ресурси у обсягах, що перевищують власні можливості потенційно-небезпечного об'єкта, але не менш одного відсотка обсягу видатків відповідного бюджету. До місцевого рівня також належать всі надзвичайні ситуації, які виникають на об'єктах житлово-комунальної сфери та інших, що не входять до затверджених переліків потенційно-небезпечних об'єктів.

До об'єктового рівня відноситься НС, яка розгортається на території об'єкта або на самому об'єкті, і наслідки якої не виходять за межі об'єкта або його санітарно- захисної смуги.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було створено алгоритм для аналізу та візуалізації інформації з журналів подій міжмережевого екрану Sophos Firewall XG.

В ході виконання першого розділу кваліфікаційної роботи було проаналізовано характеристики та властивості міжмережевих екранів нового покоління на прикладі міжмережевого екрану Sophos Firewall XG. Були розглянуті публікації, які стосуються об’єкту дослідження, а також обрані та обґрунтовані методи вирішення поставленої задачі.

У другому розділі кваліфікаційної роботи було розглянуто етапи аналізу подій в комп’ютерній системі, а також програмне забезпечення для збирання, опрацювання та збереження журналів подій на основі ELK стеку. Також були проаналізовані методи отримання журналів подій, зокрема варіант збору інформації з агентом та без нього. З використанням прикладного програмного інтерфейсу (API), протоколів Syslog та SNMP.

Третій розділ кваліфікаційної роботи присвячений виконанню поставленого завдання. Для його реалізації було розгорнуто ELK стек, який включає в себе сервіс для аналізу інформації Logstash, сервер для зберігання даних Elasticsearch та сервіс для графічного відображення інформації та її візуалізації Kibana. Для безпосереднього втілення вирішення задачі було створено конфігураційний файл Logstash, який дозволяє опрацьовувати потік даних, витягуючи з них потрібні дані та поміщаючи її у відповідні поля. Також для спрощення аналізу інформації з журналів подій було створено інформаційну панель.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

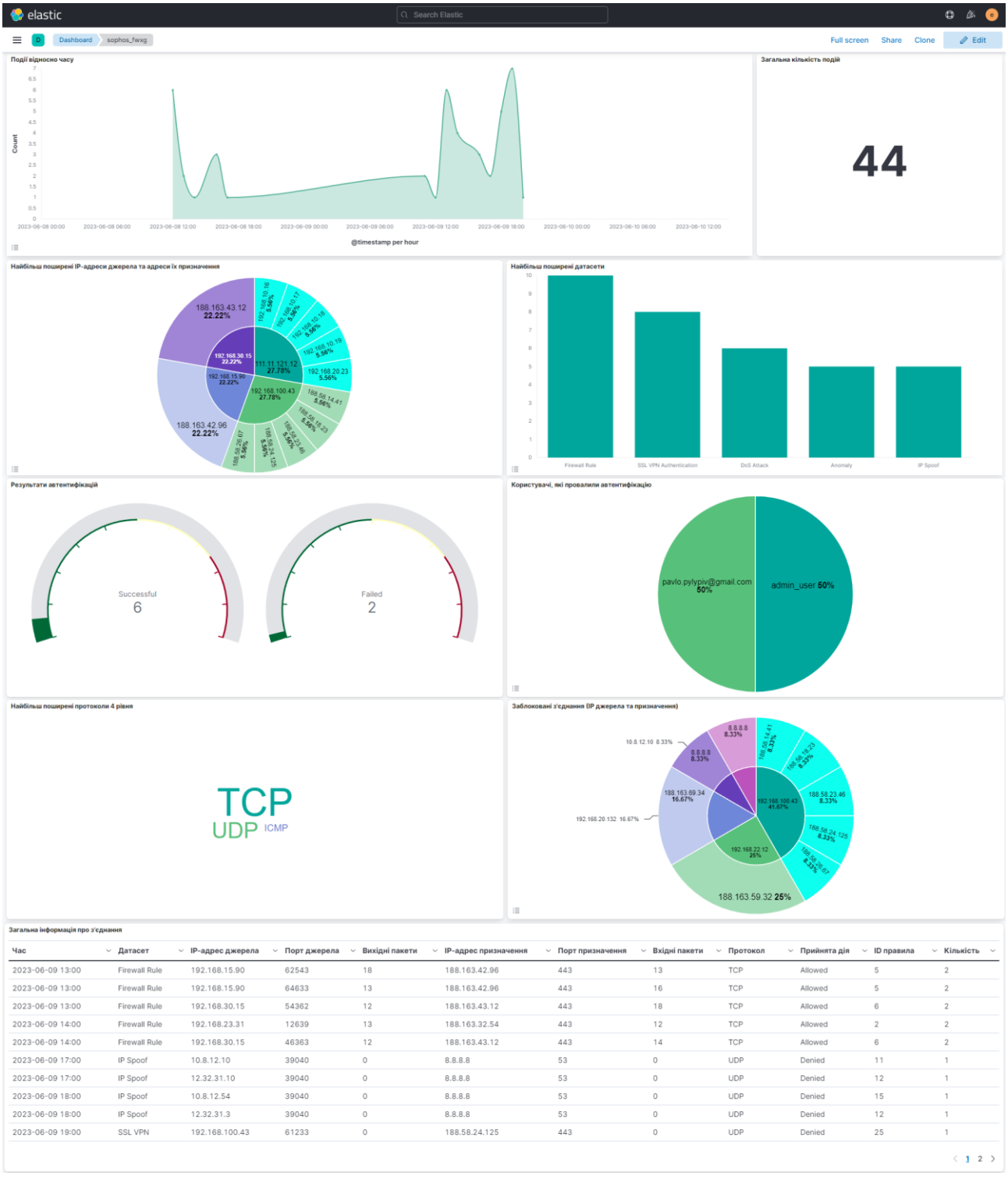
1. Best Firewall Software. Top 8 Firewalls URL: https://www.peerspot.com/categories/firewalls
2. Sophos XG Reviews URL: https://www.peerspot.com/products/sophos-xg-reviews
3. Fortinet FortiGate vs Sophos XG comparison URL: https://www.peerspot.com/products/comparisons/fortinet-fortigate_vs_sophos-xg
4. DoS attacks URL: https://doc.sophos.com/nsg/sophos-firewall/19.5/help/en-us/webhelp/onlinehelp/AdministratorHelp/IntrusionPrevention/IPSDoSAttacks/index.html
5. Що означає спуфінг? Виявлення та запобігання URL: https://hideez.com/uk-ua/blogs/news/spoofing-prevention
6. Firewall reporting storage by firewall model URL: https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/FirewallManagement/FirewallReportingLicensing/FirewallReportingStorage/index.html
7. Log settings URL: https://doc.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/SystemServices/LogSettings/index.html#logs.
8. Лог: що це, навіщо потрібен і де його знайти? URL: https://hyperhost.ua/info/uk/log-shcho-tse-navishcho-potriben-i-de-yogo-znayti
9. Why is SIEM important? URL: https://www.ibm.com/topics/siem
10. Logstash 101: Using Logstash in a Data Processing Pipeline URL: https://www.bmc.com/blogs/logstash-using-data-pipeline/
11. Input plugins URL: https://www.elastic.co/guide/en/logstash/current/input-plugins.html
12. Secure Logstash Connections Using SSL Certificates URL: https://www.linode.com/docs/guides/secure-logstash-connections-using-ssl-certificates/
13. What is Elasticsearch? URL: https://www.elastic.co/what-is/elasticsearch

14. What is Kibana? URL: https://www.elastic.co/what-is/kibana
15. Agent-based vs Agentless monitoring: A Comparison URL: https://www.manageengine.com/network-monitoring/help/agent-based-vs-agentless-monitoring.html
16. What is Syslog URL: https://www.solarwinds.com/resources/it-glossary/syslog
17. What is Syslog URL: https://www.sumologic.com/syslog/
18. Configure a secure connection to a syslog server using a locally-signed certificate from Sophos Firewall URL: https://doc.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/SystemServices/LogSettings/LogsConfigureSecureSyslogServerXGCertificate/index.html
19. What Is An API (Application Programming Interface)? URL: https://aws.amazon.com/what-is/api/
20. Sophos-Central-SIEM-Integration URL: https://github.com/sophos/Sophos-Central-SIEM-Integration
21. Sophos Central APIs: Send alert and event data to your SIEM URL: https://support.sophos.com/support/s/article/KB-000036372?language=en_US
22. How Does SNMP Work And How to Configure It? URL: https://community.fs.com/blog/understanding-snmp.html
23. Installing the Elastic Stack URL: https://www.elastic.co/guide/en/elastic-stack/current/installing-elastic-stack.html
24. Installing the ELK Stack on Windows URL: https://logz.io/blog/elk-stack-windows/
25. Document level security URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/document-level-security.html
26. Field level security URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/field-level-security.html
27. The Complete Guide to the ELK Stack URL: https://logz.io/learn/complete-guide-elk-stack/#elasticsearch

28. Using ECS. Design Principles URL: https://www.elastic.co/guide/en/ecs/current/ecs-principles-design.html
29. Вимоги до електробезпеки у офісних приміщеннях з комп’ютерною технікою URL: https://cpo.stu.cn.ua/Oksana/posibnik/1140.html
30. За 51 рік через стихійні лиха у світі загинуло понад 2 млн людей URL: https://suspilne.media/483469-za-51-rik-cerez-stihijni-liha-u-sviti-zaginulo-ponad-2-mln-ludej-vsesvitna-metereologicna-organizacia/
31. Війни в історії людства та нинішня війна в Іраку URL: https://www.radiosvoboda.org/a/901246.html

Додаток А

Створена інформаційна панель



Час	Датасет	IP-адрес джерела	Порт джерела	Вихідні пакети	IP-адрес призначення	Порт призначення	Вхідні пакети	Протокол	Прийнята дія	ID правила	Кількість
2023-06-09 13:00	Firewall Rule	192.168.15.90	62543	18	188.163.42.96	443	13	TCP	Allowed	5	2
2023-06-09 13:00	Firewall Rule	192.168.15.90	64633	13	188.163.42.96	443	16	TCP	Allowed	5	2
2023-06-09 13:00	Firewall Rule	192.168.30.15	54362	12	188.163.43.12	443	18	TCP	Allowed	6	2
2023-06-09 14:00	Firewall Rule	192.168.23.31	12639	13	188.163.32.54	443	12	TCP	Allowed	2	2
2023-06-09 14:00	Firewall Rule	192.168.30.15	46363	12	188.163.43.12	443	14	TCP	Allowed	6	2
2023-06-09 17:00	IP Spoof	10.8.12.10	39040	0	8.8.8.8	53	0	UDP	Denied	11	1
2023-06-09 17:00	IP Spoof	12.32.31.10	39040	0	8.8.8.8	53	0	UDP	Denied	12	1
2023-06-09 18:00	IP Spoof	10.8.12.54	39040	0	8.8.8.8	53	0	UDP	Denied	15	1
2023-06-09 18:00	IP Spoof	12.32.31.3	39040	0	8.8.8.8	53	0	UDP	Denied	12	1
2023-06-09 19:00	SSL VPN	192.168.100.43	61233	0	188.58.24.125	443	0	UDP	Denied	25	1