Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: Засоби захисту центру оперативної безпеки підприємства

Виконавець: студент IV курсу, групи КБ-42

_____ **Данило ТАБАЧЕНКО**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Лариса МИРУТЕНКО	

Нормоконтроль	Андрій ФЕСЕНКО	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-42** **Данила Олексійовича Табаченка**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Засоби захисту центру оперативної безпеки підприємства

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Структура та функції центру оперативної безпеки, архітектура та механізми роботи системи управління подіями та інформаційною безпекою

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Нормативно-правова база у сфері ІБ, інциденти інформаційної безпеки, функції центру оперативної безпеки, порівняння SIEM систем, архітектура та принципи роботи SIEM систем.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Вибір і компонування засобів для налаштування системи управління подіями та інформаційною безпекою підприємства.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видала _____ (підпис) Лариса МИРУТЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Данило ТАБАЧЕНКО (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 4.11.2022	*виконано*
2	Аналіз відкритих джерел	28.01.2023 –20.02.2022	*виконано*
3	Обґрунтування вибору рішення	24.02.2023 – 04.03.2023	*виконано*
4	Функціональні характеристики центру оперативної безпеки	05.03.2023 – 24.03.2023	*виконано*
5	Нормативно правові аспекти роботи центу оперативної безпеки	25.03.2023 – 07.04.2023	*виконано*
6	Засоби захисту центру оперативної безпеки	07.04.2023 – 12.04.2023	*виконано*
7	Види та функціональні характеристики SIEM систем	12.04.2023 – 16.04.2023	*виконано*
8	Функціональні можливості та архітектура ELK стеку	17.04.2023 – 20.04.2023	*виконано*
9	Побудова SIEM системи	21.04.2023 – 09.05.2023	*виконано*
10	Огляд функцій SIEM системи та робота з подіями	10.05.2023 – 04.06.2023	*виконано*
11	Оформлення пояснювальної записки	05.06.2023 – 12.06.2023	*виконано*

Завдання видала _____ (підпис) Лариса МИРУТЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Данило ТАБАЧЕНКО (ім'я, прізвище)

Термін подання дипломної роботи до ЕК 12 червня 2022 року

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 68 сторінок, включає в себе зміст, вступ, три розділи дипломної роботи, висновки та список джерел. Крім того, робота містить 1 додаток із загальною кількістю сторінок 5. У пояснювальній записці дипломної роботи міститься 70 рисунків, 1 таблицю та 39 літературних джерел.

Метою роботи є підбір компонентів та налаштування системи управління подіями та інформаційною безпекою для роботи центру оперативної безпеки.

Об'єктом дослідження є процес захисту інформаційної системи підприємства центром оперативної безпеки.

Предметом дослідження є функції та механізми захисту інформаційної системи підприємства центром оперативної безпеки.

Методи дослідження:

- аналіз відкритих джерел;
- аналіз систем захисту центру оперативного захисту підприємства;
- моделювання системи управління подіями та інформаційною безпекою.

Практичною цінністю є вибір і компонування засобів для налаштування системи управління подіями та інформаційною безпекою підприємства.

Ключові слова: центр оперативної безпеки, SIEM-системи, інциденти ІБ, захист від атак, методи реагування на кібератаки, кібератака, кіберзахист.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕННЬ

АС	–	автоматизована система
ЗІ	–	захист інформації
ІБ	–	інформаційна безпека
ПЗ	–	програмне забезпечення
API	–	Application Programming Interface
CISO	–	Chief Information Security Officer
CPU	–	Central Processor Usage
ELK	–	Elasticsearch, Logstash, Kibana
IDS	–	Intrusion Detection System
IOCs	–	Indicators of compromise
IR	–	Incident Response
IPS	–	Intrusion Prevention System
JVM	–	Java Virtual Machine
NIST	–	National Institute of Standards and Technology
RAM	–	Random Access Memory
REST	–	Representational State Transfer
SIEM	–	Security information and event management
SOAR	–	Security Orchestration, Automation and Response
SOCaaS	–	Security Operations Center as a service
TIP	–	Threat Intelligence Platform

ЗМІСТ

ВСТУП

За останні роки кількість кібератак значно зросла, і це стало причиною великих фінансових втрат для підприємств. Згідно з статистикою Check Point Research кількість кібератак в світі у 2022 виросла на 38% в порівнянні з 2021 роком. В звіті ІСЗ вказано що кількість збитків компаній в 2022 році збільшилося з 6,9 млрд доларів до 10,3 млрд доларів. Тенденція зростання кількості атак пов’язана з декількома факторами:

- Зростання кількості людей та компаній, які користуються Інтернетом, тому що збільшується кількість потенційних цілей для зловмисників. Крім того, зростає кількість пристроїв, які підключаються до Інтернету, таких як мобільні телефони, планшети, телевізори та інші "розумні" пристрої, що створює додаткові можливості для злочинців.
- Зростання складності програмного забезпечення, яким користуються компанії. Чим більше функціональності, тим більше вразливостей, що можуть бути використані зловмисниками.
- Війни - держави використовують кіберінструменти для досягнення своїх політичних, економічних та військових цілей. Кібератаки можуть призвести до розколу суспільства, руйнування інфраструктури, викрадення конфіденційної інформації, крадіжки коштів, розкриття та втручання у виборчі процеси.
- Доступність інформації створює умови в яких навіть звичайний школяр може знайти в Інтернеті засоби та інструкції, які розкривають інформацію про вразливості систем та методи здійснення кібератак.
- Нові технології на базі штучного інтелекту стрімко розвиваються і є загальнодоступними, що дозволяє зловмисникам генерувати шкідливий код і фішингові листі більш швидко та автоматизовано.

Умови війни значно збільшують загрозу кібератак і поглиблюють потребу в ефективній кібербезпеці. Кібератаки можуть бути спрямовані на критичну інфраструктуру, включаючи електроенергетичні системи, транспортні мережі,

комунікації та інші сектори, які є життєво важливими для функціонування держави. Згідно інтерв'ю заступника начальника Держспецзв'язку тільки у 2022 році державна команда реагування на комп'ютерні надзвичайні події зареєструвала 2 194 кіберінциденти [2].

Збитки підприємств та держав напряму залежать від швидкості реагування на інциденти. Центр оперативної безпеки відділ забезпечує реагування на кібератаки в режимі реального часу, забезпечуючи захист від атак на всіх рівнях інфраструктури організації.

Центр оперативної безпеки є підрозділом, який відповідає за виявлення, аналіз та реагування на кібератаки, що відбуваються в інфраструктурі компанії. SOC може забезпечувати безпеку в реальному часі, розслідувати події, виявляти нові загрози та розробляти стратегії захисту. Він забезпечує захист від різних видів загроз, включаючи кібератаки, фішинг, віруси, розповсюдження шкідливого програмного забезпечення.

Тож *актуальність роботи* полягає в виборі і компонуванні засобів для налаштування ефективної системи управління подіями та інформаційною безпекою, як одного з найважливіших інструментів в роботі центру оперативної безпеки в процесі реагування на кібератаки.

Метою роботи є підбір компонентів та налаштування системи управління подіями та інформаційною безпекою для роботи центру оперативної безпеки.

Для досягнення зазначеної мети кваліфікаційної роботи поставлено наступні завдання:

- дослідити роботу центру оперативної безпеки;
- провести аналіз засобів для роботи центру оперативної безпеки;
- дослідити механізми роботи та функціонал SIEM систем;
- вибрати і скомпонувати засоби для налаштування системи управління подіями та інформаційною безпекою підприємства.

Об'єктом дослідження є процес захисту інформаційної системи підприємства центром оперативної безпеки.

Предметом дослідження є функції та механізми захисту інформаційної системи підприємства центром оперативної безпеки.

Методи дослідження:

- аналіз відкритих джерел;
- аналіз систем захисту центру оперативного захисту підприємства;
- моделювання системи управління подіями та інформаційною безпекою;

Практична цінність роботи полягає у виборі і компонуванні засобів для налаштування системи управління подіями та інформаційною безпекою підприємства.

РОЗДІЛ 1
ФУНКЦІЇ ТА ЗАСОБИ ЗАХИСТУ ЦЕНТРУ ОПЕРАТИВНОЇ БЕЗПЕКИ

1.1 Функціональні характеристики центру оперативної безпеки

Центр оперативної безпеки – це структурний підрозділ, який використовує людей, процеси і технології для постійного моніторингу і покращення стану інформаційної безпеки компанії запобігаючи, виявляючи, аналізуючи та реагуючи на інциденти кібербезпеки.

Центр безпеки діє як командний пункт, приймаючи дані з усієї інфраструктури організації включаючи її мережі, пристрої, обладнання, сховища даних. SOC це місце, де корелюються всі події зареєстровані в організації. Для кожної з цих подій центр безпеки вирішує, як з ними діяти та чи несуть вони загрозу.

Центр безпеки – це команда спеціалістів з інформаційної безпеки, яка цілодобово та без вихідних контролює всю інфраструктуру компанії та в реальному часі реагує на загрози.

Основні завдання центру безпеки:

- Моніторинг мережі та систем компанії для виявлення кібератак.
- Аналіз виявлених загроз з метою визначення їх потенційного впливу на компанію.
- Реагування на інциденти інформаційної безпеки.
- Забезпечення безпеки клієнтів компанії та зменшення ризику витоку їхніх даних.
- Розробка та впровадження стратегії кібербезпеки компанії.

Центри оперативної безпеки стали необхідною складовою для забезпечення захисту від кібератак. Створення внутрішнього SOC або залучення послуг зовнішнього провайдера є питанням, яке часто виникає перед компаніями. Тому важливо зрозуміти різницю між створенням власного SOC відділу та залученням послуг зовнішньої компанії.

Створення власного SOC відділу це довгий і важкий процес, який включає в себе пошук кваліфікованих кадрів з досвідом роботи, що в умовах високої конкуренції компаній за кадри можу бути дуже складно, створення системи моніторингу та реагування на інциденти. Один з найбільших мінусів цього підходу є висока вартість створення та підтримку відділу.

Багато компаній зараз пропонують послуги центру безпеки як сервісу. Вибираючи цей варіант є багато плюсів:

- Компанії, які не мають достатньо ресурсів та кваліфікації в сфері інформаційної безпеки можуть отримати доступ до високоякісних послуг.
- Компанії надавачі таких послуг швидко пристосовуються до змін на ринку і забезпечують компанії потрібними рішеннями в області кібербезпеки.
- SOCaaS це широкий спектр послуг, який дозволяє компанії забезпечити повну безпеку своїх систем та мережі. Включаючи в себе виявлення та аналіз кібератак, моніторинг безпеки, виявлення потенційних загроз.
- Це швидке рішення для інформаційної безпеки компанії.

Однак у такого підходу є один дуже суттєвий мінус: передача конфіденційних даних сторонній компанії. Це може бути особливо проблематичним для організацій, які зберігають велику кількість конфіденційної інформації про клієнтів або іншу чутливу інформацію. Існує ризик, що стороння компанія може втрутитися в конфіденційні дані підприємства, що може призвести до серйозних наслідків.

Крім того, іншим недоліком є обмежена контрольна можливість за процесом забезпечення кібербезпеки. Підприємство, яке використовує послуги SOC as a service, не може повністю контролювати інфраструктуру та налаштування, які використовує зовнішня компанія. Це може призвести до того, що підприємство не зможе ефективно виявляти та відповідати на кібератаки, які сталися в результаті помилок або недбалості з боку сторонньої компанії.

Саме тому великі компанії створюють власні SOC у складі відділу інформаційної безпеки.

Склад центру оперативної безпеки:

- Менеджер SOC – керівник відділу, керує командою та слідкує за всіма операціями по забезпеченню безпеки. В залежності від організації може доповідати CISO або його заступнику.
- Інженери безпеки – підтримують системи моніторингу та реагування. В залежності від організації можуть керувати та створювати архітектуру. Більша частина роботи включає в себе тестування, рекомендації, впровадження і обслуговування інструментів та технологій безпеки.
- Аналітики безпеки – спеціалісти по реагування на інциденти. Аналітики виявляють, досліджують, пріоритизують загрози. Основне завдання це пом’якшення та стримування загрози або інцидента. В залежності від організацій можуть бути 1, 2 та 3 рівня.

В команду SOC можуть входити і інші спеціалісти, що залежить від розміру організації або сфери в якій працює компанія. В великих компаніях може бути позиція директору по реагуванню на інциденти, який відповідає за обмін інформацією і координацію в реагуванні на інциденти.

1.2 Нормативно правові аспекти роботи центу оперативної безпеки

NIST Cybersecurity Framework – це стандарт кібербезпеки, розроблений Національним інститутом стандартів та технологій (NIST) США. Він містить рекомендації щодо захисту критично важливої інфраструктури та відповідного відновлення роботи після кібератак.

Застосування стандартів NIST Cybersecurity Framework допомагає забезпечити високий рівень безпеки та захисту від кібератак, а також сприяє розробці ефективних заходів з реагування на інциденти в кібербезпеці.

Згідно стандарту кібербезпека складається з 3 основних компонентів (рис. 1.1):

Ядро – набір бажаних заходів із кібербезпеки та результатів. Основні рекомендації допомагають організаціям керувати ризиками кібербезпеки та зменшувати їх у спосіб, який доповнює існуючі процеси кібербезпеки та управління ризиками в організації.

Рівні реалізації інфраструктури допомагають організаціям, надаючи контекст того, як організація бачить управління ризиками кібербезпеки. Рівні скеровують організації до розгляду належного рівня суворості для їхньої програми кібербезпеки та часто використовуються як інструмент спілкування для обговорення схильності до ризику, пріоритету місії та бюджету.

Профілі — це унікальне узгодження організаційних вимог і цілей організації, схильності до ризику та ресурсів із бажаними результатами ядра Framework. Профілі в основному використовуються для визначення та визначення пріоритетів можливостей для покращення кібербезпеки в організації.

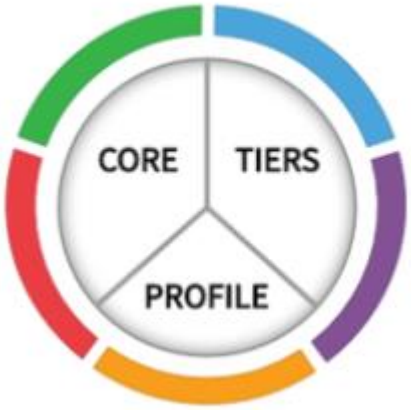

Рисунок 1.1 – Основні компоненти стандарту

Фреймворк складається з 5 основних складових частин (див. рис. 1.2). Кожна з цих складових частин має свої конкретні вимоги та рекомендації щодо захисту від кіберзагроз.

1. Identify.

Передбачає встановлення меж системи, а також ідентифікацію ризиків, які можуть бути пов'язані з кожним із активів. Визначається, які дані потребують захисту, де вони зберігаються, хто має до них доступ, які процеси використовують ці дані, і як вони обробляються. Крім того, на цьому етапі визначається, які активи мають бути захищені, включаючи технічні активи, такі як сервери та мережеві пристрої, і не технічні активи, такі як інтелектуальна власність та репутація. Під час визначення також варто враховувати всіх зацікавлених сторін, які мають доступ до даних та

систем, включаючи власників, співробітників, клієнтів та партнерів. Важливо визначити, які рівні доступу до систем та даних мають різні категорії користувачів.

Ці відомості допомагають SOC відділу розробити ефективні стратегії та технічні рішення для захисту даних та систем від потенційних загроз.

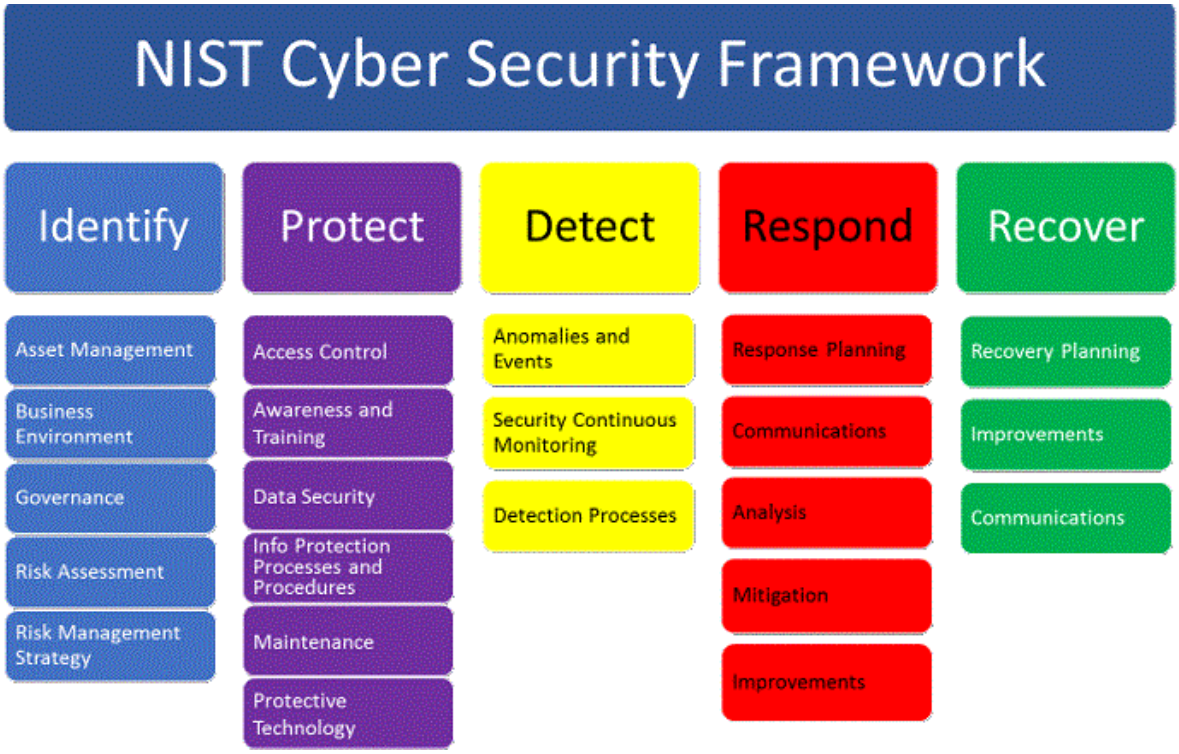

Рисунок 1.2 – NIST Cyber Security Framework

2. Protect.

Впроваджуються політики та процедур для захисту інфраструктури підприємства. Це включає встановлення і налагодження технічних засобів захисту, таких як мережеві фаєрволи, антивірусні програми, системи виявлення та запобігання вторгненням (IDS / IPS), системи управління подіями (SIEM). Також у цьому пункті рекомендується розробка та впровадження процедур контролю доступу, які дозволяють забезпечити необхідний рівень захисту від несанкціонованого доступу до важливих даних та ресурсів підприємства.

Окрім технічних засобів, в цьому пункті рекомендується виконання різних процедур, які допоможуть забезпечити високий рівень безпеки підприємства. Наприклад, це може включати підготовку та проведення регулярних тренувань з кібербезпеки для співробітників, проведення аудиту безпеки, підготовку та впровадження планів захисту в разі кібератаки. Реалізація заходів з цього пункту

допоможе зменшити ризик виникнення кібератак та підвищить рівень захищеності підприємства від них.

3. Detect.

Описується процес виявлення кібератак та інших подій, які можуть вплинути на кібербезпеку, які можуть відбуватися в підприємстві. Для виявлення таких подій використовуються інструменти та засоби, які було встановлено в другому пункті, а саме: IDS/IPS, SIEM, EDR.

Також етап включає рекомендації щодо виявлення аномальних дій користувачів, незвичайних мережевих підключень і інших ознак, які можуть свідчити про можливий кібератаку або інший кіберінцидент. Для досягнення цієї мети, пропонується розробляти та впроваджувати політики та процедури для моніторингу і аналізу подій, а також використовувати інструменти для збору та аналізу логів.

Основна мета пункту виявлення полягає в тому, щоб забезпечити підприємству можливість вчасно виявляти кібератаки і інші кіберінциденти, щоб швидко реагувати на них і зменшувати можливі наслідки. Даний пункт також допомагає забезпечити ефективний моніторинг мережі та систем, що дозволяє оперативно виявляти можливі загрози і запобігати їх поширенню.

4. Response.

Пункт Описує процес реагування на кібератаку після її виявлення, забезпечуючи швидку та ефективну реакцію на події безпеки. Цей пункт охоплює вимоги до швидкості та якості реагування, а також до здатності відновлення діяльності після атаки.

Організація повинна мати плани реагування на інциденти, щоб забезпечити ефективну реакцію на кібератаку. Ці плани повинні бути розроблені на основі ризиків та можливих загроз, які можуть виникнути. Крім того, необхідно підготувати персонал та розробити процедури з управління кризовими ситуаціями, щоб забезпечити швидку та ефективну реакцію на інцидент.

У відповідь на загрозу SOC вживає заходів для обмеження потенційних збитків. Дії можуть включати:

- Розслідування основної причини для визначення технічних вразливостей, які надали хакерам доступ до системи, а також інші чинники такі як неправильна гігієна паролів або погане дотримання політик, які сприяли інциденту.
- Вимкнення скомпрометованих кінцевих точок.
- Ізоляція скомпрометованих областей мережі або перенаправлення мережевого трафіку.
- Призупинення або зупинення скомпрометованих додатків або процесів.
- Видалення пошкоджених або заражених файлів
- Запуск антивірусного програмного забезпечення.
- Блокування скомпрометованих користувачів.

Важливим елементом цього пункту є розслідування інцидентів. Після того, як інцидент був виявлений та зупинений, організація повинна провести детальне розслідування з метою виявлення причин інциденту та вдосконалення систем безпеки для запобігання подібних інцидентів у майбутньому.

5. Recover.

Пункт описує процеси та процедури для відновлення після кібератаки або іншої події, яка призвела до порушення безпеки. Цей пункт забезпечує підтримку нормальної діяльності після інциденту та зменшення впливу на бізнес.

Основні етапи пункту відновлення включають відновлення систем, відновлення даних та відновлення послуг. Ці етапи можуть бути виконані за допомогою резервних копій, збережених даних та інших процедур відновлення.

Для забезпечення ефективного відновлення необхідно зробити наступні кроки:

- Визначення впливу: Визначте вплив інциденту на вашу організацію. Це допоможе вам прийняти правильні рішення щодо відновлення.
- Відновлення систем: Забезпечте відновлення необхідних систем та додатків. Це може бути досягнуто за допомогою резервних копій або інших методів відновлення.
- Відновлення даних: Забезпечте відновлення необхідних даних. Це може бути досягнуто за допомогою резервних копій або інших методів відновлення.

- Відновлення послуг: Забезпечте відновлення необхідних послуг. Це може бути досягнуто за допомогою резервних копій або інших методів відновлення.
- Аналіз та вдосконалення: Проведіть аналіз інциденту та зробіть висновки. Використовуйте ці висновки, щоб вдосконалити процедури відновлення та запобігти подібним інцидентам у майбутньому.

NIST SP 800-61 – документ про обробку інцидентів комп’ютерної безпеки. Оскільки ефективне реагування на інциденти є складним завданням, створення можливостей для успішного реагування на інциденти потребує серйозного планування та ресурсів. Документ допомагає організаціям створити можливості для успішного реагування на інциденти комп'ютерної безпеки для ефективної і результативної обробки інцидентів. У документі представлені рекомендації щодо обробки інцидентів, зокрема щодо аналізу даних, пов'язаних з інцидентами, та визначення належних заходів реагування на кожен інцидент. Ці рекомендації можна виконувати незалежно від конкретних апаратних платформ, операційних систем, протоколів або додатків.

Для SOC відділу NIST SP 800-61 є одним з найважливіших стандартів, оскільки він містить конкретні стандарти та рекомендації щодо організації процесу кібербезпеки та допомагає забезпечити стандартизацію діяльності. Він надає можливість SOC відділу оцінювати свій рівень захищеності від кіберзагроз та розробляти плани для його покращення.

Подія — це будь-яке зафіксоване повідомлення в системі або мережі.

Несприятлива подія — це подія з негативними наслідками. Наприклад: попередній збій у роботі ПО, несанкціонований доступ до даних, несанкціоноване використання підвищених пільг, запуск шкідливого ПО).

Кіберінцидент — це порушення або невигідна загроза порушення політики ІБ, політики допустимого використання або стандартних практик ІБ.

Згідно документу при виробленні процесу управління кіберінцидентами важливо розробити політику, план і процедури реагування на кіберінциденти.

Політика реагування на кіберінциденти повинна бути індивідуально розроблена для кожної конкретної організації і включати в себе такі елементи, як:

1. Утвердження про причетність керівництва компанії в процес реагування на кіберінциденти та розуміння його важливості на всіх рівнях компанії;
2. Цілі і завдання політики;
3. Терміни та визначення для створення єдиної системи понять;
4. Організаційна структура та розподіл ролей, відповідальності, повноцінного та рівня прийняття рішень;
5. Рівні критичності та пріоритезація інцидентів;
6. Метрики ефективності процесу реагування на кіберінциденти;
7. Форми звітності та відправки повідомлень.

План реагування на кіберінциденти повинен відображати формалізований, узгоджений і специфічний для конкретної організації підхід до реагування на кіберінциденти, в якому будуть виражені наступні елементи:

1. Місія, стратегія і план реагування на кіберінциденти;
2. Узгодження плану керівництвом компанії;
3. Загальний підхід компанії до реагування на кіберінциденти;
4. Структура команди реагування на кіберінциденти;
5. Способи взаємодії команд реагування з працівниками компанії та з іншими компаніями;
6. Метрики оцінки можливостей та ефективності функції реагування на кіберінциденти в компанії;
7. План підвищення рівня функції реагування на кіберінциденти в компанії;
8. Взаємозв'язок функцій реагування на кіберінциденти з іншими функціями в компанії.

Процедури реагування на кіберінциденти повинні опиратися на політику і план реагування і містити докладний опис технічних процесів, дій, техніки, чек-листів і форм звітності. Для кожного типу інциденту слід розробити окремі процедури реагування, в яких будуть вивчені специфіка інфраструктури компанії та конкретні дії щодо реагування на певний тип інциденту.

У рамках розробки документів з управління кіберінцидентами слід описати формат і спосіб взаємодії зі сторонніми особами у разі виявлення інциденту:

1. Взаємодія з ЗМІ: слід назначити відповіді щодо взаємодії з ДМІ, розглянути необхідність залучення юридичного департаменту під час спілкування з ДМІ, переглянути формат і обсяг повідомленої інформації про інцидент для зменшення корисної для атакуючих публічної інформації, продумати формат короткого обговорення подробиць інциденту з уповноваженими по взаємодію з СМІ, передбачити способи актуалізації інформації про інцидент для СМІ, проінструктувати співробітників компанії про можливі формати взаємодії з СМІ. Також рекомендується проводити тренувальні інтерв'ю, заздалегідь проробляючи відповіді на питання про те, хто і за чим нападав вашу компанію; коли, як і чому це сталося; наскільки руйнівним був інцидент і як іде його внутрішнє розслідування; якові наслідки інциденту, були чи запущені охоронювана законом інформація (наприклад, персональні дані), як попередній фінансовий збиток від інциденту.

2. Взаємодія з державними органами: в залежності від країни, до компаній можуть застосовуватися різні вимоги за повідомленням органів влади за фактами виявлення інциденту ІБ. Слід призначити відповідь щодо взаємодії з державними органами, яка повинна знати формат взаємодії та бути підготовленим юридично та технічно.

3. Взаємодія з центрами реагування на кіберінциденти: обов’язково надавати інформацію про виниклі кіберінциденти в державних центрах реагування на кіберінциденти або обмінюватися інформацією про виниклі інциденти та отримання допомоги від відчужених або комерційних центрів протидії кібератакам.

4. Взаємодія з інтернет-провайдером: блокування мережевого трафіку (наприклад, у разі DDoS-атаки), збереження та отримання подій мережевих з'єднань.

5. Взаємодія з власником атакуючої IP-адреси: у разі атаки можна взаємодіяти з контактом зовнішнього провайдера або з власником автономної системи.

6. Взаємодія з вендорами: взаємодія з ІБ-вендором може допомогти при виникненні питань при роботі з СЗІ або при вірогідних погано позитивних обробках, а взаємодія з виробником ПО допоможе обмінюватися інформацією про можливі вразливості або нових векторах атак на програмне забезпечення.

7. Взаємодія з третіми особами, запущеними інцидентом: клієнти, контрагенти, постачальники, підрядники можуть бути заблоковані інцидентом, що стався в компанії, або вони можуть повідомити про інцидент, джерелом якого може бути ваша компанія. В обох випадках слід попередити формат взаємодії та обсяг внутрішньої інформації, яка передається.

Документ також включає фактори, які потрібно враховувати при виборі структури команди реагування на інциденти, а саме: потреба в покритті 24/7, бюджет, досвід команди та описує ризики, які необхідно враховувати при передачі процесу реагування на інциденти компанії підрядчику.

1.3. Засоби захисту центру безпеки

Центр безпеки має бути обладнаний різними засобами захисту, щоб забезпечити захист від кібератак та забезпечити надійну захисту даних підприємства.

1. Засоби виявлення вторгнень (IDS) – це програмне або апаратне забезпечення, яке виявляє загрози кібербезпеці компанії, використовуючи такі методи, як аналіз мережевого трафіку та дослідження даних. Це рішення пасивного моніторингу, яке генерує сповіщення для співробітників служби безпеки про необхідність проведення розслідування. IDS можна класифікувати двома способами: За місцем розташування:

- NIDS – встановлення IDS на вузлі входу трафіку в внутрішню мережу організації.
- HIDS – встановлення IDS на конкретному хості для відстеження всіх мережевих контактів цього хоста.

За методом виявлення загроз:

- На основі сигнатур. Засоби виявлення вторгнень на основі сигнатур використовують бібліотеки сигнатур вже відомих загроз для їх ідентифікації.
- На основі поведінки. Засоби виявлення вторгнень на основі поведінки будують модель типової для системи поведінки і сповіщають при будь-яких змінах.

- Гібридна система. Використовує обидва методи для виявлення потенційних загроз.

IDS призначена для виявлення потенційного інциденту і створення сповіщення, що є гарним рішенням для систем з високими потребами в доступності, де блокування підозрілого трафіку може вплинути на роботу системи. Сповіщення аналітика безпеки дозволяє оцінити інцидент і прийняти правильне рішення, щодо подальших дій.

2. Засоби запобігання вторгненням (IPS) – це система активного захисту, така система, як і IDS аналізує трафік і намагається ідентифікувати потенційні загрози з використанням сигнатурного, поведінкового або гібридного аналізу, однак при виявленні загрози вона блокується (див. рис. 1.3). Кібератаки з кожним роком стають все більш швидкими і складними, IPS дозволяє зупинити атаку на ранній стадії без збитків для компанії. Таке рішення ідеально підходить для середовищ, де будь-яка атака може призвести до великих втрат, наприклад для баз даних, які зберігають конфіденційні дані.

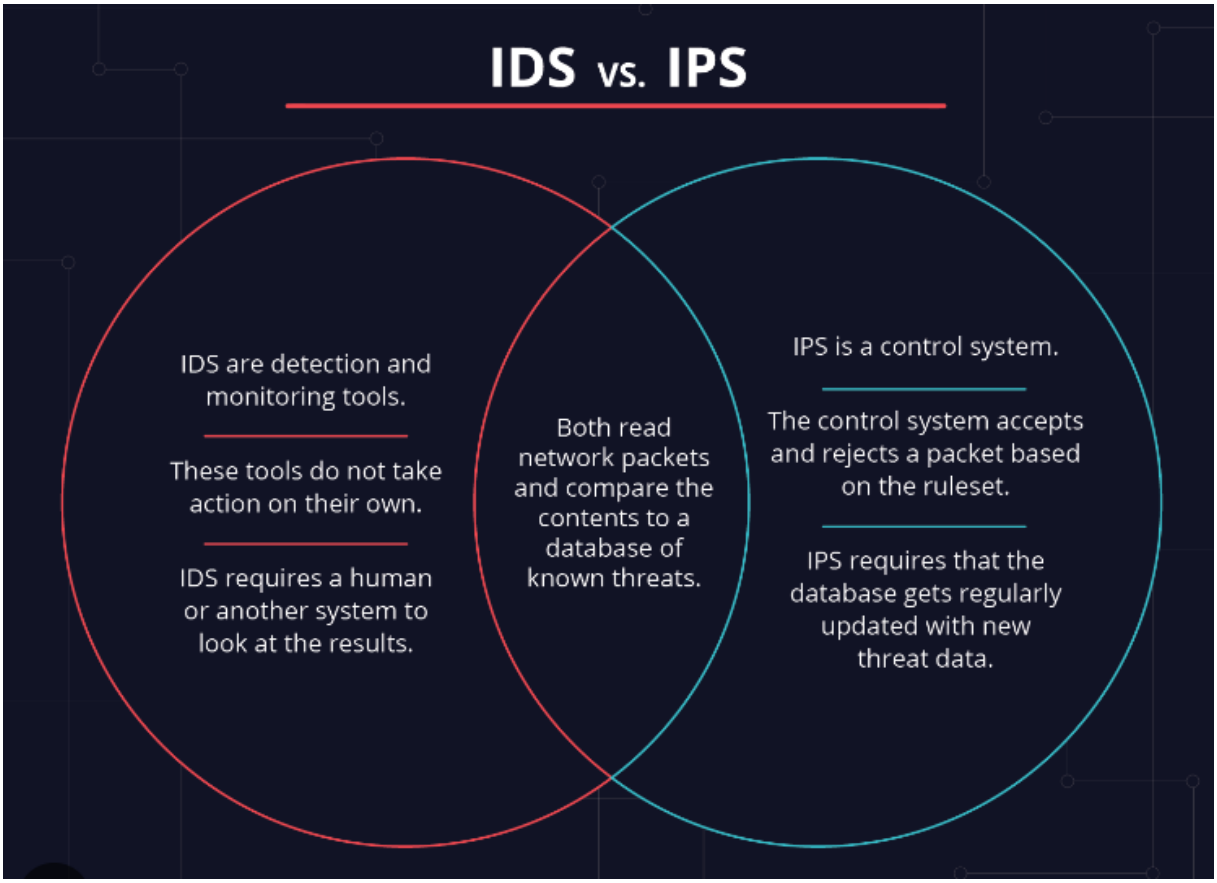

Рисунок 1.3 – Порівняння IDS та IPS

3. Endpoint Detection and Response (EDR) – це рішення для захисту комп'ютерів та серверів від кібератак, яке здатне здійснювати моніторинг та реагування на події на рівні кінцевих точок. EDR забезпечує стійкий захист кінцевих точок від зловмисних дій, включаючи виявлення та ізоляцію загроз, обмеження їх поширення та відновлення роботи системи після нападу. EDR збирає дані про поведінку комп'ютера та виконання процесів, аналізує ці дані на предмет незвичної або підозрілої активності та генерує сповіщення для SOC аналітиків у разі виявлення загроз.

EDR дозволяє створити сповіщення на використання небажаних для організації програм, на підключення до небажаних серверів та на використання підозрілих команд, що можуть свідчити про компрометацію хоста.

Основне значення EDR для SOC полягає в тому, що вона забезпечує глибоку видимість на рівні кінцевих точок, що дозволяє аналітикам SOC виявляти загрози, які можуть обійти інші системи захисту. Виявлення загроз на рівні кінцевих точок також дозволяє ефективно ліквідувати загрози та зменшує ризик їх поширення в системі.

Окрім того, EDR може використовуватися для збору даних та створення детальних звітів про кінцеві точки, що допомагає аналітикам центру оперативної безпеки виявляти та усувати вразливості, які можуть бути використані зловмисниками для здійснення кібератак.

4. Брандмауери – це апаратне або програмне рішення, для контролю та фільтрації мережевого трафіку, згідно з заданими правилами. Види брандмауерів:

- З фільтрацією пакетів - є найстарішим і найпростішим типом брандмауерів. Працюючи на мережевому рівні, вони перевіряють пакет даних на IP-адресу джерела та IP-адресу призначення, протокол, порт джерела та порт призначення на відповідність заздалегідь визначеним правилам, щоб визначити, передавати чи відхиляти пакет. Брандмауери фільтрації пакетів, по суті, не мають стану, відстежуючи кожен пакет незалежно без жодного відстеження встановленого з’єднання або пакетів, які раніше пройшли через це з’єднання. Це робить ці брандмауери дуже обмеженими у своїй здатності захищати від розширених загроз і атак. Брандмауери з фільтрацією пакетів швидкі, дешеві та ефективні. Але безпека,

яку вони забезпечують, дуже проста. Оскільки ці брандмауери не можуть перевіряти вміст пакетів даних, вони не здатні захистити від зловмисних пакетів даних, що надходять із IP-адрес надійних джерел. Оскільки вони працюють без збереження стану, вони також вразливі до атак маршрутизації джерела та атак із використанням крихітних фрагментів.

- Сеансового рівня. Працюючи на рівні сеансу, вони перевіряють встановлені з'єднання і відстежують активні сеанси. Вони дуже схожі на брандмауери з фільтрацією пакетів, оскільки виконують одну перевірку та використовують мінімальні ресурси. Однак вони функціонують на вищому рівні моделі взаємодії відкритих систем. В першу чергу вони визначають безпеку встановленого з'єднання. Коли внутрішній пристрій ініціює з'єднання з сервером, шлюзи на рівні каналу встановлюють віртуальне з'єднання від імені внутрішнього пристрою, щоб приховати особу та IP-адресу внутрішнього користувача. Шлюзи на рівні каналів є економічно ефективними, спрощеними та майже не впливають на продуктивність мережі. Однак їхня нездатність перевіряти вміст пакетів даних робить їх неповним рішенням безпеки. Пакет даних, що містить зловмисне програмне забезпечення, може легко обійти шлюз на рівні каналу, якщо він має законне рукостискання TCP. Саме чому інший тип брандмауера часто налаштовується поверх шлюзів на рівні каналів для додаткового захисту.

- Брандмауери нового покоління поєднують у собі традиційні технології брандмауерів з додатковими функціями, такими як перевірка зашифрованого трафіку, системи запобігання вторгненням, антивірус та багато іншого. Зокрема він включає глибоку перевірку пакетів. У той час як базові брандмауери переглядають лише заголовки пакетів, глибока перевірка пакетів перевіряє дані всередині пакета, дозволяючи користувачам більш ефективно ідентифікувати, класифікувати або зупиняти пакети зі шкідливими даними.

- Брандмауери з збереженням стану працюють шляхом створення таблиці стану з IP-адресою джерела, IP-адресою призначення, портом джерела та портом призначення після встановлення з'єднання. Вони динамічно створюють власні правила, щоб дозволити очікуваний вхідний мережевий трафік, замість того, щоб

покладатися на жорстко закодований набір правил на основі цієї інформації. Вони зручно відкидають пакети даних, які не належать до перевіреного активного з'єднання. Брандмауери з збереженням стану перевіряють законні підключення та IP-адреси джерела та призначення, щоб визначити, які пакети даних можуть пройти. Хоча ці додаткові перевірки забезпечують розширену безпеку, вони споживають багато системних ресурсів і можуть значно сповільнити трафік.

- Брандмауери на рівні додатків також відомі як проксі-брандмауери, реалізуються на прикладному рівні через проксі-пристрій. Замість стороннього доступу до вашої внутрішньої мережі напряму, з'єднання встановлюється через брандмауер проксі. Зовнішній клієнт надсилає запит на брандмауер проксі. Після перевірки автентичності запиту брандмауер проксі пересилає його на один із внутрішніх пристроїв або серверів від імені клієнта. Крім того, внутрішній пристрій може запитувати доступ до веб-сторінки, а проксі-пристрій пересилає запит, приховуючи дані про місцезнаходження внутрішніх пристроїв і мережі. На відміну від брандмауерів фільтрації пакетів, брандмауери проксі-серверів виконують глибоку перевірку стану пакетів, щоб проаналізувати контекст і вміст пакетів даних відповідно до набору визначених користувачем правил. Залежно від результату вони або дозволяють, або відхиляють пакет. Вони захищають ідентифікаційні дані та розташування ваших конфіденційних ресурсів, запобігаючи прямому з'єднанню між внутрішніми системами та зовнішніми мережами. Однак налаштувати їх для досягнення оптимального захисту мережі може бути складно.

5. Поштовий шлюз – це апаратне або програмне рішення, яке є точкою входу і виходу всіх листів підприємства. Використовується для моніторингу всієї пошти організації і призначена для захисту від спаму та фішингу. Шлюз також дозволяє фільтрувати всі листи, по відправникам, вкладенням.

6. Інтернет шлюз – це апаратне або програмне рішення, яке є точкою входу і виходу всього інтернет трафіку підприємства. Використовується для моніторингу інтернет трафіку. Призначений для захисту користувачів від відвідування небезпечних сайтів.

7. Security Information and Event Management (SIEM) – це система, яка забезпечує збір, аналіз та інформації про події в системі інформаційної безпеки. SIEM є важливим компонентом в SOC, оскільки вона дозволяє об'єднувати дані з різних джерел, таких як фаєрволи, системи виявлення, системи захисту від вторгнень і проводити аналіз цих даних для виявлення потенційних загроз та атак на підприємство.

8. Програмні засоби Threat Intelligence – рішення для збору інформації про індикатори компрометації систем, методи атак, про зловмисні угруповання та їх мотиви. Компанії, які займаються розвідкою загроз аналізують кібератаки на підприємства, збирають всі можливі дані і створюють детальні звіти з поетапним поясненням атаки, що дозволяє компаніям захиститися від вже відомих атак. З кожним роком атаки стають все складніші, кількість IOCs та методів збільшується кожний день, таку кількість інформації фізично не можна запам’ятати, тому було створено програмні засоби, які дозволяють ділитися інформацією про загрози. TIP – це програмний засіб, який використовує дані для збору, оброблення, співставлення та візуального представлення інформації о загрозах, атаках і вразливостях.

Основні функції платформи аналізу загроз (див. рис. 1.4):

- Звіти аналізів загроз. Основна мета аналізу загроз – надавати регулярну та актуальну інформацію про атаки, як внутрішні так і глобальні. Платформа має бути пов’язана з кінцевими точками і системами безпеки для моніторингу інфраструктури на наявність загроз.
- Автоматизація робочих процесів. Платформа може автоматично отримувати та оновлювати індикатори. Можливо налаштувати інтеграцію з системами управління інцидентами, щоб видавати автоматичні оповіщення та ініціювати автоматичне виправлення. Платформи нового покоління для аналізу загроз використовують когнітивні технології, щоб відфільтрувати шум і автоматично відображати тільки високопріоритетну інформацію.

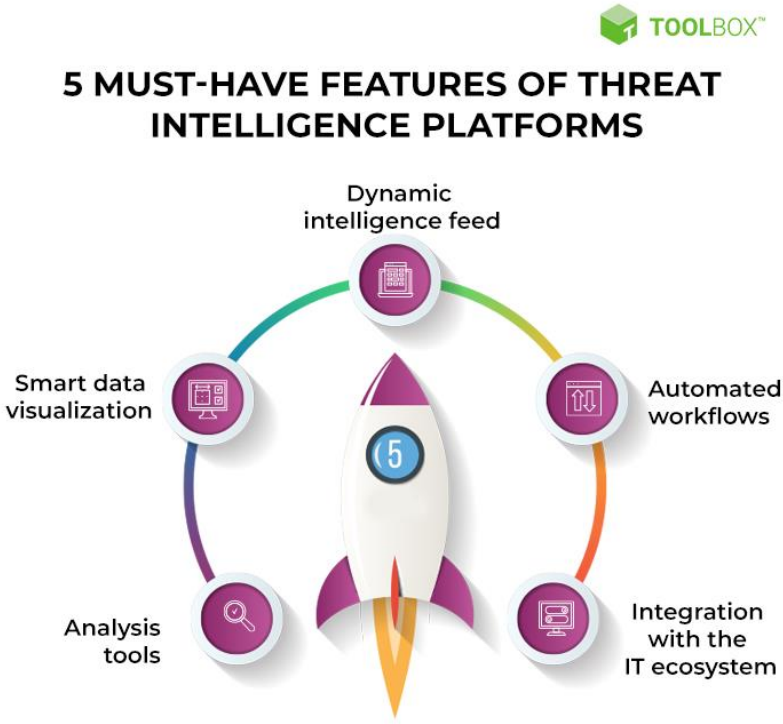

Рисунок 1.4 – Основні функції TIP

- Інтеграція з інфраструктурою. Вибрана платформа обміну інформацією про загрози повинна підтримувати повну інтеграцію з інфраструктурою. Системи повинні передавати внутрішні дані про загрози на платформу, а платформа до центру безпеки. Платформи підтримують гнучкі API, які дозволяють підключити їх майже до будь-якого програмного або апаратного засобу.
- Візуалізація даних. Візуалізація даних – це ключ до правильного аналізу загроз. Дані можуть бути корисними лише тоді, коли представлені розумно та легко для використання. Дані аналізу загроз мають візуалізуватися за допомогою карт, графіків тенденцій, часових шкал, таблиць і діаграм (за потреби), щоб ви могли легко помітити кореляції та провести більш глибокий аналіз.
- Інструменти аналізу. Вбудовані інструменти для аналізу даних дозволяють правильно орієнтуватися в безкінечних потоках інформації. Необхідно враховувати зручність і ефективність інструментів від розробників платформи, так як кожна інтеграція підвищує складність системи.

9. IR платформи – це програмні рішення для структуризації та автоматизації процесу реагування на інциденти.

Функції IR платформ:

- Підтримка робочих процесів аналітиків ІБ. Зручний інтерфейс для ескалації сповіщень ІБ в інциденти з можливістю робити записи, визначати пріоритети загроз та ділитися даними з іншими аналітиками.
- Інтеграція з іншими системами безпеки. IR платформи дозволяють налаштувати інтеграції відповідно до потреб компанії. Можливо експортувати IOCs на платформу обміну інформацією о загрозах.
- Автоматизація. Автоматизація реагування на інциденти за раніше визначеними сценаріями. Сценарії реагування на інциденти можуть бути дуже ефективними для скорочення часу реагування та можуть допомогти заощадити час аналітикам ІБ.

10. Security Orchestration, Automation and Response (SOAR) – комплекс програмних рішень призначений для координування і управління системами безпеки підприємства.

SOAR складається з 3 основних частин (див. рис. 1.5):

- Оркестрація. Машинна координація серії взаємозалежних дій безпеки, включаючи розслідування інцидентів, реагування на них. Оркестрація координує всі інструменти безпеки для того щоб вони працювали злагоджено.
- Автоматизація. Виконання дій безпеки основаних на машинному навчанні з можливістю виявлення, розслідування та усунення кіберзагроз без необхідності ручного втручання людини. Він виконує більшу частину механічної роботи для команди SOC, тому їм більше не потрібно переглядати та вручну обробляти кожне сповіщення, щойно воно надходить. Автоматизація виявляє загрози, сортує потенційні загрози, визначає чи потрібно вживати заходи стосовно інциденту, стримує та вирішує проблему.
- Відповідь. І оркестрація, і автоматизація забезпечують основу функції реагування системи SOAR. За допомогою SOAR організація може керувати, планувати та координувати свою реакцію на загрозу безпеці. Функція автоматизації

SOAR усуває ризик людської помилки. Це робить відповіді точнішими та скорочує час, необхідний для усунення проблем безпеки.

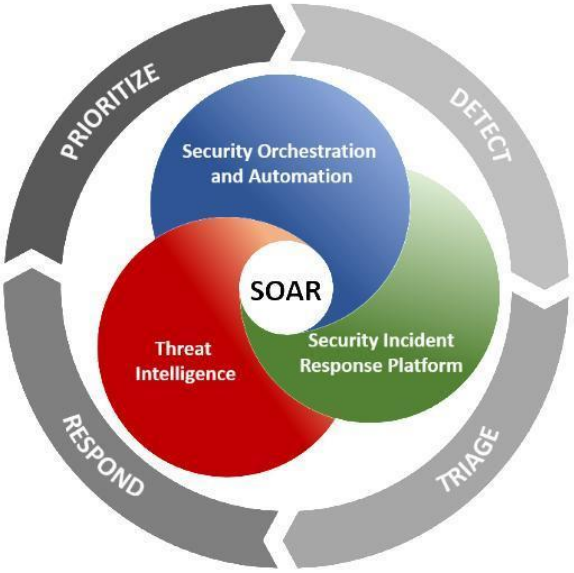

Рисунок 1.5 – Функції SOAR систем

SOAR також може включати платформу управління аналізом загроз. Управління розвідкою загроз дозволяє організаціям краще розуміти глобальний ландшафт загроз, передбачати наступні кроки зловмисників і вживати оперативних заходів для припинення атак.

Існує значна різниця між розвідкою загроз та керуванням розвідкою загроз. У той час як розвідка про загрози – це дані та інформація про загрози, управління розвідкою про загрози – це збір, нормалізація, збагачення та дії щодо даних про потенційних зловмисників та їхні наміри, мотивацію та можливості. Ця інформація може допомогти організаціям приймати швидші та більш обґрунтовані рішення щодо безпеки та, таким чином, бути краще підготовленими до кіберзагроз.

Складові SOAR:

- SIEM;
- EDR;
- DLP;
- TIM;
- системи аналізу поведінки користувачів (UEBA) ;
- брандмауери.

SOAR дозволяє автоматизувати основні процеси центру оперативної безпеки для більш ефективного реагування. Підвищена ефективність допомагає підприємствам зменшити час реагування на інциденти, що зменшує час простою систем і дозволяє швидке локалізувати та зупинити атаку.

Висновки за розділом 1

З ростом кількості кібератак в світі центри оперативної безпеки стали необхідною складовою для забезпечення захисту від кібератак. SOC відіграє важливу роль у виявленні, аналізі та реагуванні на кіберзагрози, що становлять потенційну небезпеку для організації.

NIST SP 800-61, відомий як "Computer Security Incident Handling Guide", надає рекомендації та керівництво з обробки інцидентів інформаційної безпеки. Цей стандарт надає організації чіткий керівництво з планування, виявлення, аналізу та відновлення після інцидентів. Використовуючи цей стандарт підприємства можуть створити власний центр оперативної безпеки, слідуючи теоретичним та практичним рекомендаціям.

Було визначено основні інструменти, необхідні для роботи центру оперативної безпеки. EDR допомагає захистити найслабше місце в будь-якій системі – користувачів. IDI і IPS, допомагають виявляти та запобігати несанкціонованому доступу до мережі та систем. SIEM системи використовуються для збору, аналізу та відображення подій інформаційної безпеки. Security Orchestration, Automation and Response платформи допомагають автоматизувати процеси реагування на інциденти та підвищують ефективність роботи SOC.

Розуміння цих концепцій і технологій є критичним для створення та забезпечення ефективного захисту інформаційної безпеки підприємства.

РОЗДІЛ 2
ОГЛЯД ТА ПОРІВНЯННЯ SIEM СИСТЕМ

2.1 Види та функціональні характеристики SIEM систем

Розвиток SIEM систем можна умовно поділити на 3 етапи:

- Перший етап: в 2000-х роках SIEM система була спробою поєднання системи інформаційної безпеки та системи управління подіями. Через незрілість кібербезпеки, мало програм мали належне журналювання і основними джерелами для подій були системи безпеки, такі як: IDS/IPS, фаєрволи. Основною задачею SIEM було отримання даних, агрегація і відправка сповіщень команді безпеки. Проте локальна обчислювальна потужність для неструктурованих даних була дуже малою, тому для отримання хоч якоїсь інформації про виникнення сповіщення або інцидента могло пройти дуже багато часу.
- Другий етап: Даних становилося ще більше, структуровані бази даних не могли відповідати потребам IT-служб або груп безпеки. Вони не могли встигати за обсягом, різноманітністю чи швидкістю даних, які надходять до них. Тоді компанія Splunk в 2003 році представила світу технологію індексації, завдяки чому можна шукати структуровані дані та не структуровані і конвертувати їх в доступні для пошуку події. Технологія компанії стала проривом, оскільки вона значно спростила організаціям завантажувати, шукати, зберігати, візуалізувати та отримувати статистичні дані з усіх своїх даних, що постійно зростають.
- Третій етап: в SIEM почали інтегрувати нову технологію аналітики поведінки користувачів та суб’єктів. У той момент у світі почалося збільшення атак нульового дня. Індустрія SIEM мала не відставати, намагаючись ще краще аналізувати дані.

На даний момент системи управління подіями та інформаційною безпекою перейшли від використання підходу на основі правил і тепер використовують штучний інтелект для досягнення найвищого рівня безпеки. Незважаючи на те, що сучасні SIEM засновані на штучному інтелекті, вони все ще потребують взаємодії з людиною для реалізації, моніторингу та вжиття належних заходів щодо згенерованих сповіщень.

За реалізацією SIEM системи можна поділити на:

- Хмарна SIEM – система управління подіями та інформаційною безпекою побудована у хмарного провайдера. Цей варіант полегшує витрати на розгортання та не потребує догляду за сервером, він став дуже популярним після розвитку хмарних технологій. Однак він збільшує поверхню атаки, так як дані оброблюються іншою компанією, яка надає послуги хмари.
- Внутрішня SIEM – система впроваджується на власному апаратному забезпеченні. Цей варіант забезпечує максимальну інтеграцію з іншими системами компанії і прибирає ризик зберігання інформації у сторонніх компаній. Однак потребує більш кваліфікованих і коштує більше, що компенсується ефективністю системи.

Основні функції SIEM системи (див. рис. 2.1):

1. Збір подій системи.
2. Зберігання подій.
3. Аналіз подій.
4. Кореляція подій.
5. Відображення подій.
6. Сповіщення про загрози в реальному часі.

Рисунок 2.1 – Основні функції SIEM системи

2.2. Огляд та порівняння SIEM систем

Найпопулярніші SIEM системи:

Splunk – це спеціалізована SIEM платформа для збору, зберігання, аналізу, моніторингу та аналітики інформації. Особливість платформи полягає у роботі з різними джерелами даних, на кшталт віртуального та фізичного хоста, різних IoT-пристроїв, хмар, CRM системи та іншого.

IBM Qradar – здійснює консолідацію даних із журналів подій, що надходять від тисяч пристроїв, кінцевих точок та додатків у мережі. Продукт поєднує необроблені дані з даними минулих періодів та контекстом реального часу за допомогою Sense Analytics, що допомагає знизити шум та забезпечити виявлення інцидентів з високою точністю. Є частиною IBM QRadar Security Intelligence Platform, яке дозволяє покрити майже всі вектори кібербезпеки організації.

ELK – це акронім, який використовується для опису стека, який складається з трьох популярних проектів: Elasticsearch, Logstash і Kibana. Стек ELK, який часто називають Elasticsearch, дає вам можливість агрегувати журнали з усіх ваших систем і програм, аналізувати ці журнали та створювати візуалізації для моніторингу програм та інфраструктури, швидшого усунення несправностей, аналітики безпеки.

LogRhythm SIEM – створює простий для сприйняття опис безпеки, який консолідує дані та дії користувача або хоста в одному поданні, допомагаючи

аналітикам швидко зрозуміти та усунути інциденти безпеки. LogRhythm SIEM оптимізує розслідування інцидентів і реагування на них за допомогою досвіду візуального аналітика, який розповідає історію безпеки про користувача або хост, використовуючи всі доступні дані в SIEM, допомагаючи командам безпеки визначити пріоритети та зосередитися на найважливіших речах.

McAfee Enterprise Security Manager (ESM) – ядро рішення McAfee SIEM забезпечує продуктивність, дієвий інтелект та інтеграцію рішень із швидкістю та масштабом, необхідним для організацій безпеки. Це дозволяє швидко визначати пріоритети, досліджувати та реагувати на приховані загрози та відповідати вимогам відповідності.

На таблиці 2.1 наведено загальний огляд основних переваг та недоліків кожної SIEM системи.

Таблиця 2.1

Порівняння популярних SIEM систем

Система	Плюси	Мінуси
Splunk	Швидка обробка величезної кількості даних. Підтримка індексації будь-яких даних. Зручний інтерфейс. Лідер ринку SIEM систем.	Дуже висока вартість.
IBM QRadar	Система розумного зберігання даних. Функція моментального пошуку. Безкоштовні інтеграційні модулі.	Високі витрати та складність впровадження.
ELK (Elasticsearch, Logstash, Kibana)	Гнучкість та розширюваність. Безкоштовне рішення.	Складність впровадження та конфігурування. Система потребує

Продовження таблиці 2.1

		багато ресурсів для роботи.
LogRhythm SIEM	Готові модулі фільтрації подій. Застосовує машинне навчання на основі ШІ, щоб зменшити помилкові спрацьовування. Має чудові посібники користувача.	Складність конфігурації.
McAfee Enterprise Security Manager (ESM)	Модульне рішення, яке дозволяє охопити більше векторів кібербезпеки.	Погана продуктивність.

2.3. Функціональні можливості та архітектура ELK стеку

ELK – це абревіатура, яка використовується для опису трьох програмних рішень: Elasticsearch, Logstash и Kibana.

Elasticsearch – це система повнотекстового пошуку та аналізу з відкритим вихідним кодом, заснована на пошуковій системі Apache Lucene. Він забезпечує просте розвертання, максимальну надійність і просте управління. Він також пропонує розширені запити для виконання детального аналізу та централізованого зберігання всіх даних. Це корисно для виконання швидкого пошуку документів.

Elasticsearch також дозволяє зберігати, шукати та аналізувати великі обсяги даних. Він в основному використовується в якості базового механізму для додатків, що відповідають вимогам пошуку. Окрім швидкого пошуку, інструмент також пропонує комплексну аналітику та безліч додаткових функцій.

Особливості Elasticsearch:

- Відкритий вихідний код написаний на Java;
- індексує будь-які дані;
- має веб-інтерфейс REST API із виводом JSON;
- повнотекстовий пошук;

- пошук в реальному часі;
- розділене, репліковане сховище документів JSON;
- розподілене сховище документів без схем, засноване на REST та JSON;
- підтримка кількох мов та геолокації.

Logstash – це агрегатор журналів, який збирає дані з різних джерел виведення, фільтрує їх, а потім відправляє дані в Elasticsearch.

Складається із трьох компонентів:

1. Введення – передача подій для їх обробки.
2. Фільтр – набір умов виконання певної дії чи події. Тут можна налаштувати програму для збору подій: редагування значень, додавання та видалення нових параметрів, розбір полів.
3. Вивід – відправка опрацьованих подій.

Переваги Logstash:

- Централізована обробка даних;
- аналіз великої кількості структурованих/неструктурованих даних та подій;
- LogStash пропонує плагіни для підключення до різних типів джерел введення та платформ.

Kibana – це рівень візуалізації, який працює поверх Elasticsearch, надає користувачам можливість аналізувати та візуалізувати дані. Дозволяє шукати дані на рівні полів, за логічними виразами.

Особливості Kibana:

- Інформаційна панель, яка здатна візуалізувати індексовану інформацію;
- пошук індексованої інформації в реальному часі;
- запити до даних і візуалізація результатів в діаграмах, таблицях і картах;
- переваги та недоліки:
- легка візуалізація;
- повністю інтегрований з Elasticsearch;
- інструмент візуалізації;

- пропонує аналіз у реальному часі, діаграми, узагальнення та можливості налагодження;
- забезпечує інтуїтивний і зручний інтерфейс;
- дозволяє обмінюватися знімками журналів, у яких проводився пошук;
- дозволяє зберігати інформаційну панель і керувати кількома інформаційними панелями.

Beats – це легкі агенти, які встановлюються на кінцевих точках для збору різних типів даних для пересилання в стек.

Beats і Logstash працюють над збіркою та обробкою даних, Elasticsearch індексує та зберігає дані, а Kibana надає інтерфейс користувача для запиту даних та їх візуалізації (див. рис. 2.2).

Рисунок 2.2 – Принцип роботи ELK стеку.

Переваги ELK стеку:

- Стек може безпечно та швидко витягувати, аналізувати та візуалізувати дані в режимі реального часу з будь-якого джерела та у будь-якому форматі;
- дозволяє централізовано вести журнал, що допомагає виявляти будь-які проблеми, пов'язані з сервером та додатком, на декількох серверах та зіставляти журнали за певний період часу;
- простий у використанні та налаштуванні, зручний для користувача;
- рентабельний набір програм із відкритим вихідним кодом;
- розгортається у будь-якому масштабі незалежно від технічної інфраструктури компанії;
- стабільне, відмовостійке рішення - при збої кластерних вузлів дані не губляться, а перерозподіляються;

- стек передбачає можливість додання багатьох інтеграцій;
- безкоштовне рішення, з можливістю перейти на платну;
- велика спільнота з базою даних для вирішення будь-яких проблем.

Недоліки:

- Відносно складна внутрішня мови запитів;
- витратне масштабування;
- через використання JVM стек споживає багато ресурсів CPU та RAM, що при дуже високих навантаженнях може призвести до зниження продуктивності;
- коли розміри індексів в Elasticsearch перевищують обмеження сховища даних вузла, індексація починає давати збій, що може призвести до втрати даних;
- встановлення та запуск стеку ELK — далеко не простий процес, і організаціям, які не мають власних необхідних навичок та ресурсів, доведеться інвестувати в програму навчання або найняти інженера з досвідом для управління розгортанням.

Висновки за розділом 2

SIEM системи є важливим компонентом кібербезпеки організації, допомагаючи організаціям ефективно виявляти, аналізувати та реагувати на потенційні загрози безпеки. Розвиток SIEM систем почався з простих рішень, які забезпечували збір та аналіз журналів подій. Проте, з часом функціонал SIEM систем розширювався, включаючи можливості виявлення аномалій, кореляції подій, пов'язаних з безпекою, а також впровадження автоматизованих процедур реагування на інциденти. Сучасні SIEM системи володіють потужними аналітичними можливостями, включаючи машинне навчання та штучний інтелект, для виявлення складних кіберзагроз та забезпечення постійного моніторингу стану безпеки.

ELK є однією з найпопулярніших і простих у освоєнні платформ для аналізу журналів, які використовуються в усьому світі. Незважаючи на те, що ELK добре підходить для роботи з великими даними для великих корпорацій, стек ELK також є дуже цінним набором для невеликих компаній, які використовують невеликі системи.

ELK стек є відкритим програмним забезпеченням, що означає доступність вихідного коду та активну спільноту користувачів. Це дає можливість для власного налаштування та розширення функціональності системи під потреби конкретної організації.

Однією з основних переваг ELK стеку є його масштабованість та гнучкість. Elasticsearch, який використовується для зберігання та індексації даних, може легко масштабуватися горизонтально, що дозволяє оптимально використовувати ресурси при збільшенні обсягу даних.

Logstash забезпечує можливість збору та обробки даних з різних джерел, що спрощує їх інтеграцію у систему. Kibana надає зручний інтерфейс для візуалізації та аналізу даних, дозволяючи користувачам легко здійснювати пошук, фільтрацію та виведення статистики.

На додаток до всіх дивовижних функцій і переваг, які пропонує користувачам стек ELK, він є безкоштовним.

Проте, ELK стек також має свої недоліки. Один з них - висока складність установки та налаштування. Інсталяція та налагодження ELK стеку може бути вимогливим завданням для необізнаних користувачів, особливо у випадку складних конфігурацій або великих обсягів даних. Крім того, підтримка та налаштування ELK стеку також може бути складним завданням, особливо для мало досвідчених адміністраторів.

Загалом, ELK стек є потужним інструментарієм для обробки та аналізу даних. Враховуючи його переваги та недоліки, важливо враховувати специфіку конкретної організації та її потреби у реалізації системи. Правильно налаштований та ефективно використовуваний ELK стек може значно покращити аналіз та виявлення потенційних загроз безпеці, сприяючи високому рівню захищеності інформаційних систем.

РОЗДІЛ 3
ПОБУДОВА SIEM СИСТЕМИ НА БАЗІ СТЕКУ ELK

3.1 Опис запропонованого рішення

У попередніх розділах було детально проаналізовано процеси роботи SIEM систем, що дозволило прийти до висновку, що система управління подіями та інформаційною безпекою один з найважливіших механізмів забезпечення кібербезпеки підприємств. В даній роботі буде сконфігуровано та поєднано засоби для налаштування SIEM системи.

Розроблювана SIEM система буде реалізована на базі ELK стеку. ELK стек підтримує тонке налаштування та багато модулів для програмного розширення системи та для горизонтального масштабування. Сервер та клієнт реалізовано на операційній системі Ubuntu версії 22.04. Для наближення до більш реальних умов було побудовано окрему підмережу, маршрутизатором всередині мережі виступає програмне рішення Pfsense. На рисунку 3.1 наведена схема взаємодії всіх складових підсистеми.

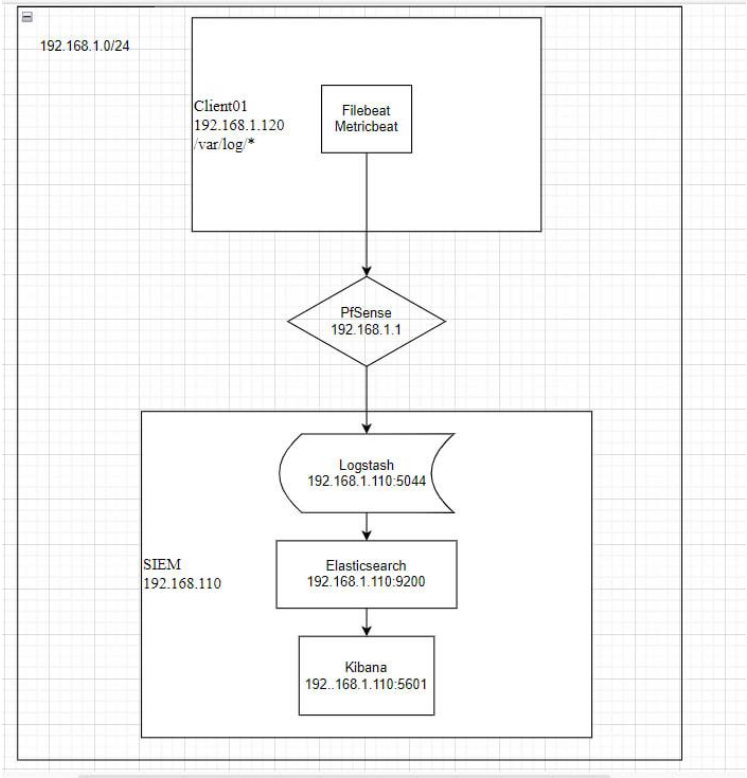

Рисунок 3.1 – Архітектура запропонованого рішення.

PfSense – це фаєрвол та маршрутизатор з відкритим програмним кодом, який має такі корисні функції: управління загрозами, управління навантаженням. В даній роботі рішення застосовується виключно, як маршрутизатор.

3.2 Побудова SIEM системи

Для початку необхідно завантажити офіційний образ PfSense та створити нову віртуальну машину в Virtual Box. Далі створюємо нову внутрішню мережу, наприклад: InternalLan (див. рис. 3.2).

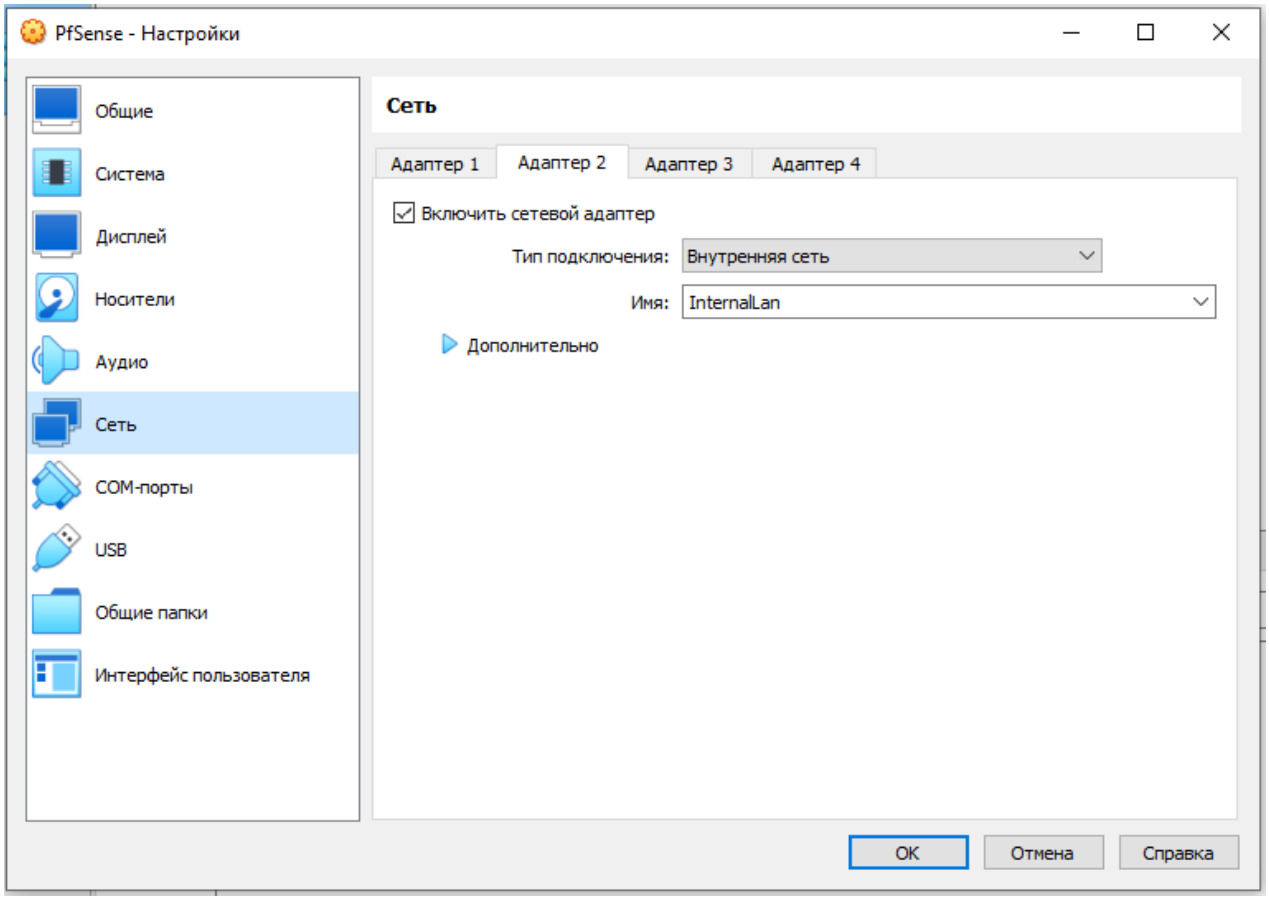

Рисунок 3.2 – Створення нової мережі.

Приймаємо ліцензійну угоду (див. рис. 3.3) і тиснемо встановити (див. рис. 3.4).

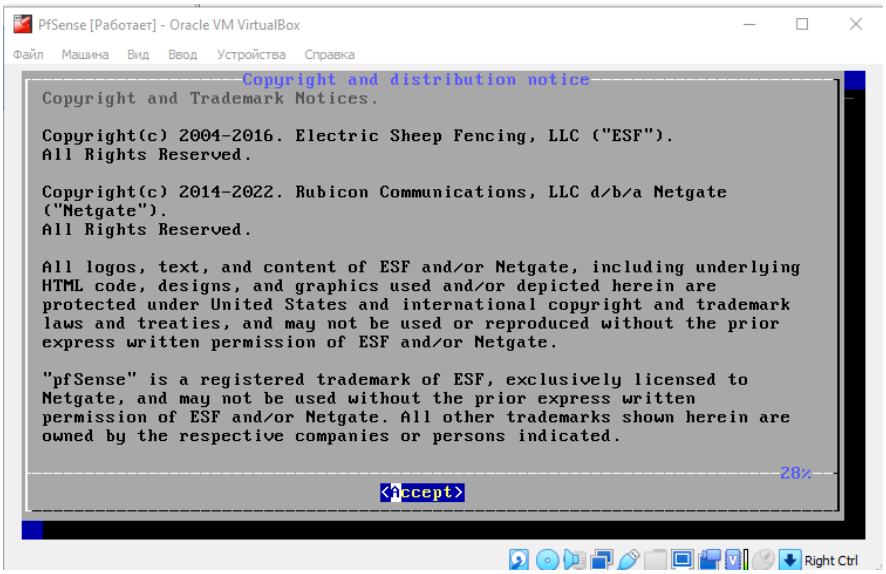

Рисунок 3.3 – Ліцензійна угода.

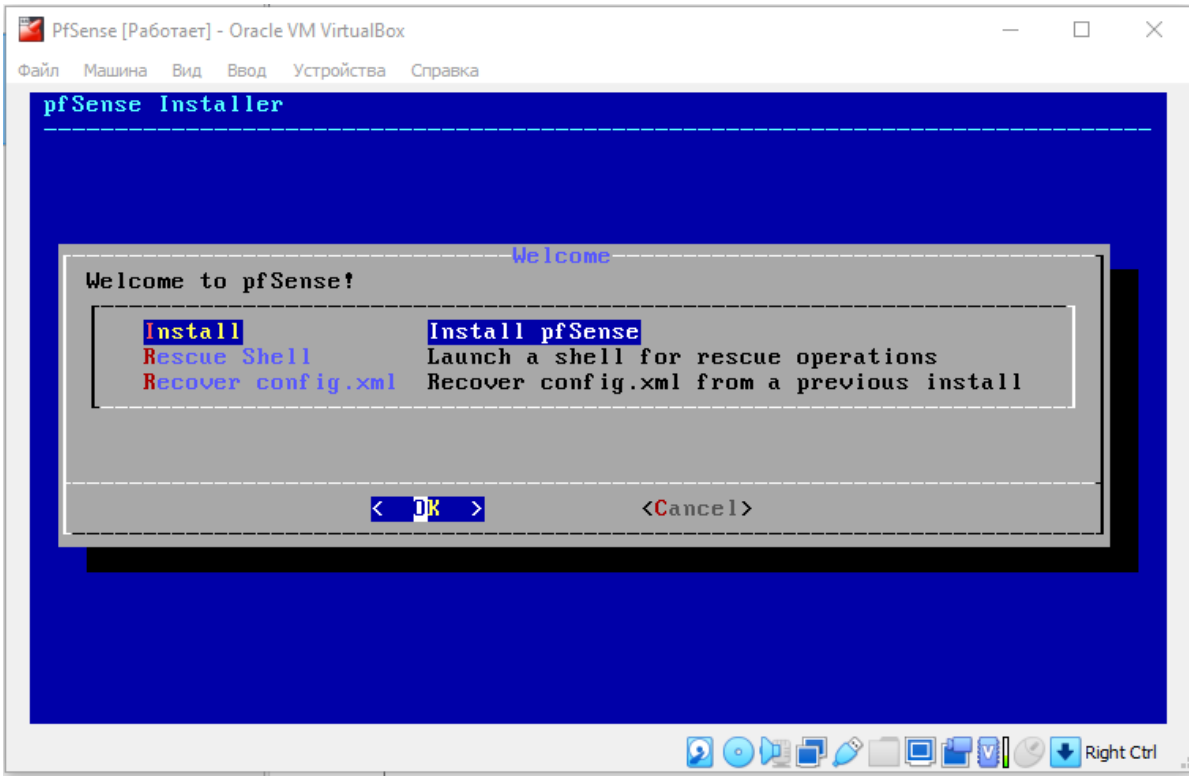

Рисунок 3.4 – Ліцензійна угода.

Вибираємо продовжити зі звичайною розкладкою клавіш (див. рис. 3.5) та автоматичну розмітку диску (див. рис. 3.6).

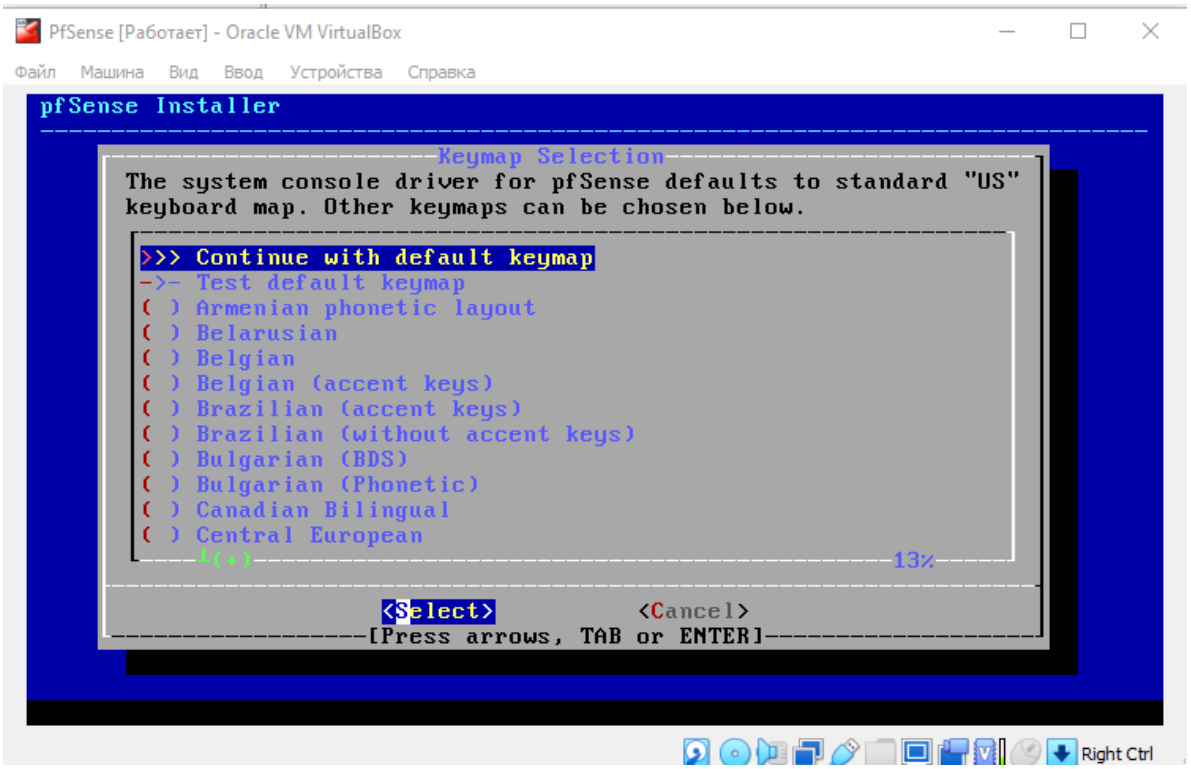

Рисунок 3.5 – Розкладка клавіш.

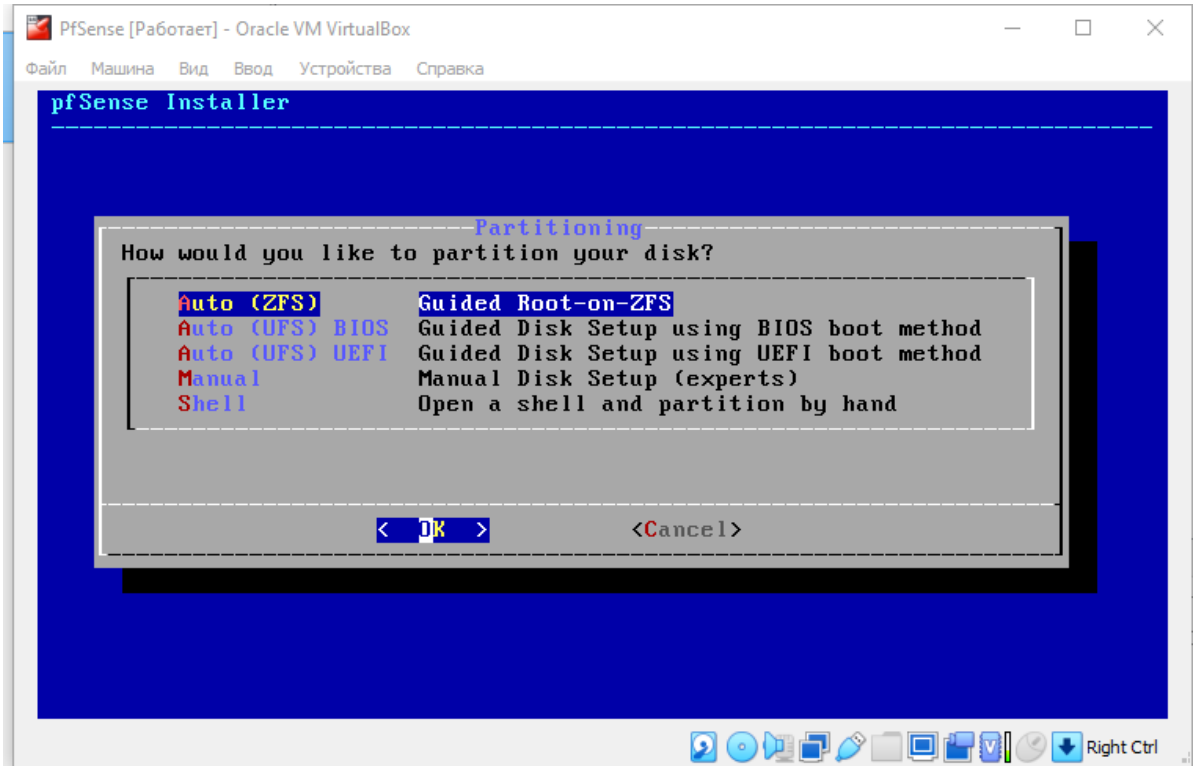

Рисунок 3.6 – Розмітка диску.

Тиснемо встановити (див. рис. 3.7) та вибираємо тип віртуального пристрою за замовчуванням (див. рис. 3.8).

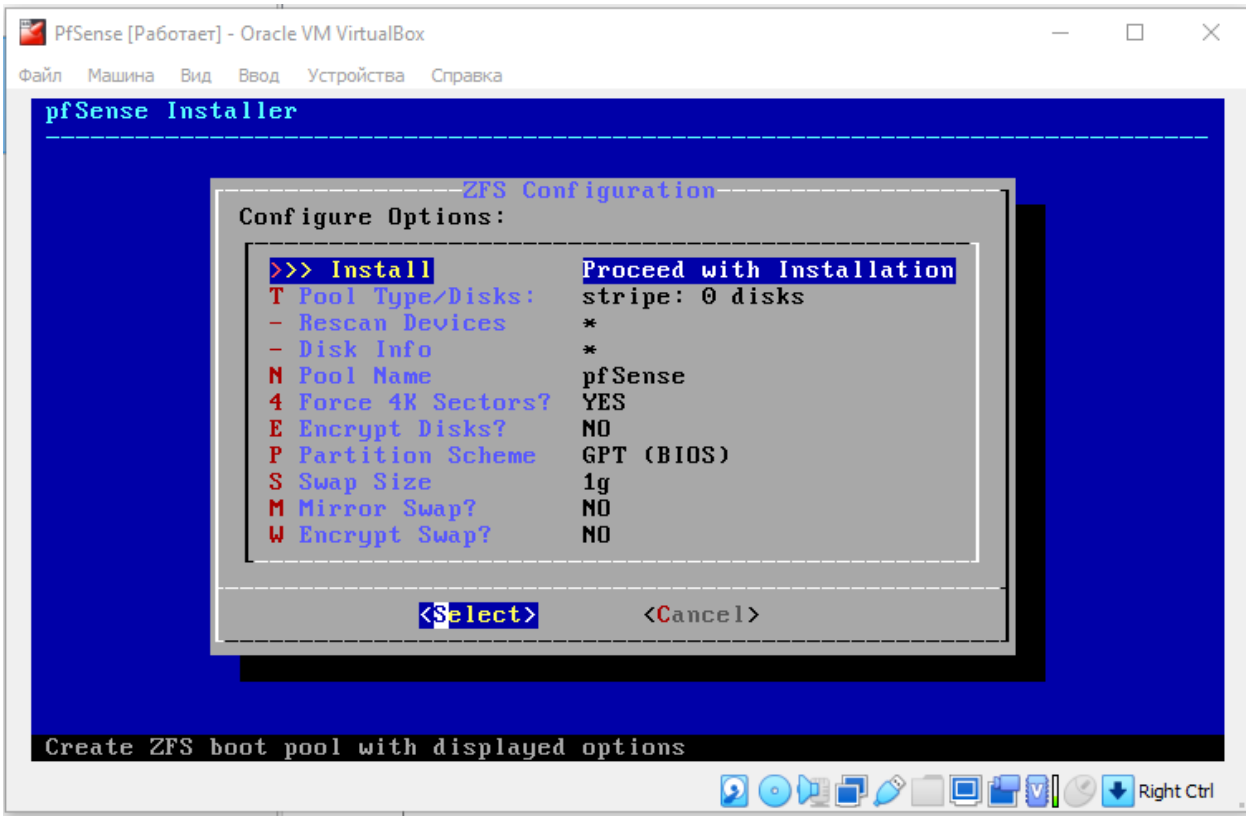

Рисунок 3.7 – Конфігурація ZFS.

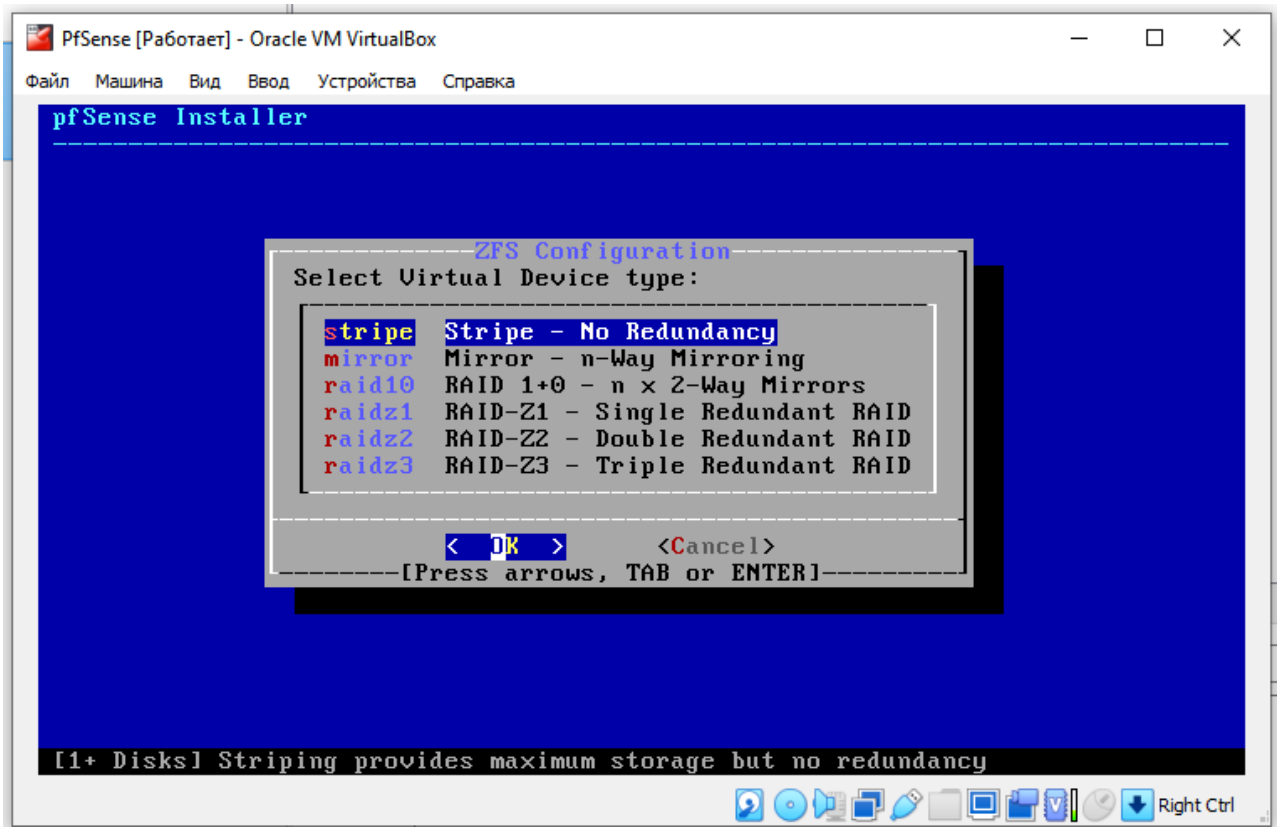

Рисунок 3.8 – Конфігурація типу віртуального пристрою.

Обираємо пункт ada0 (див. рис. 3.9) і тиснемо так (див. рис. 3.10).

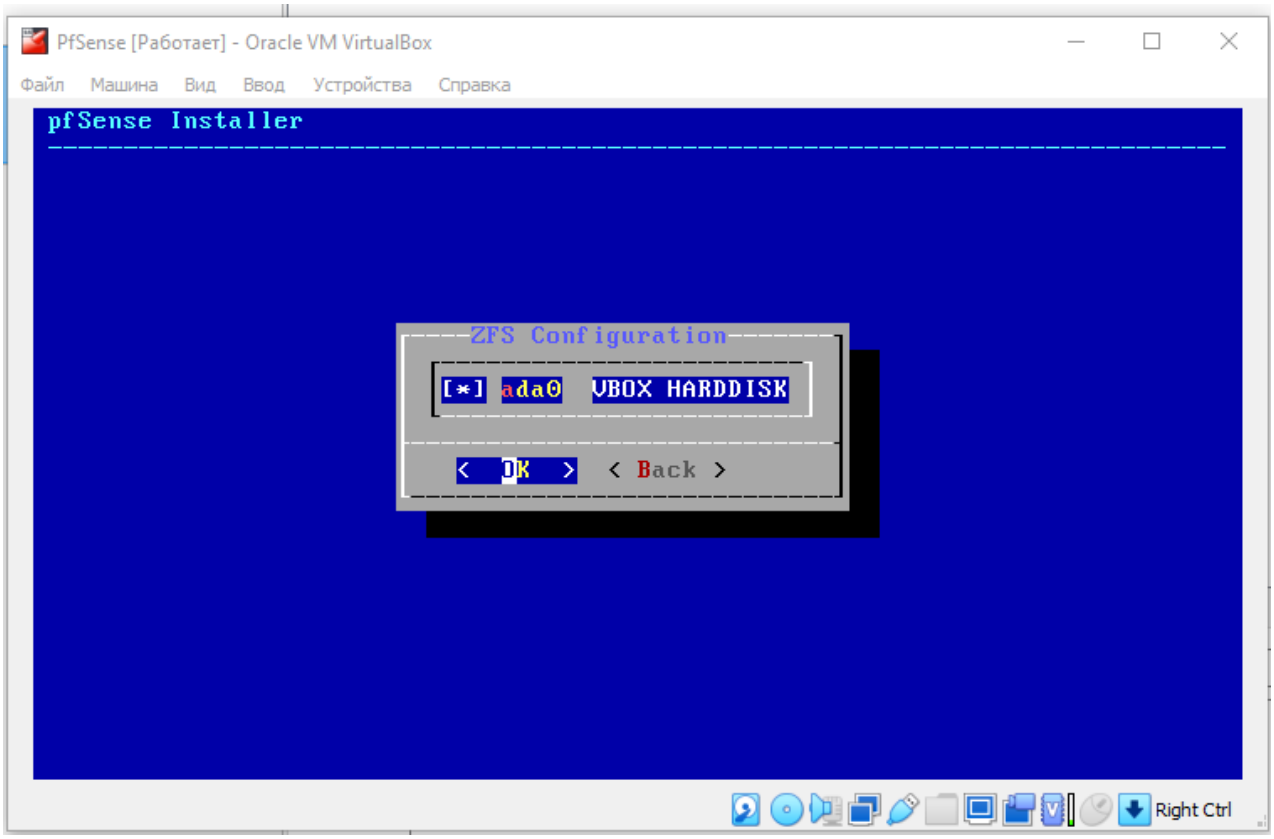

Рисунок 3.9 – Конфігурація жорсткого диску.

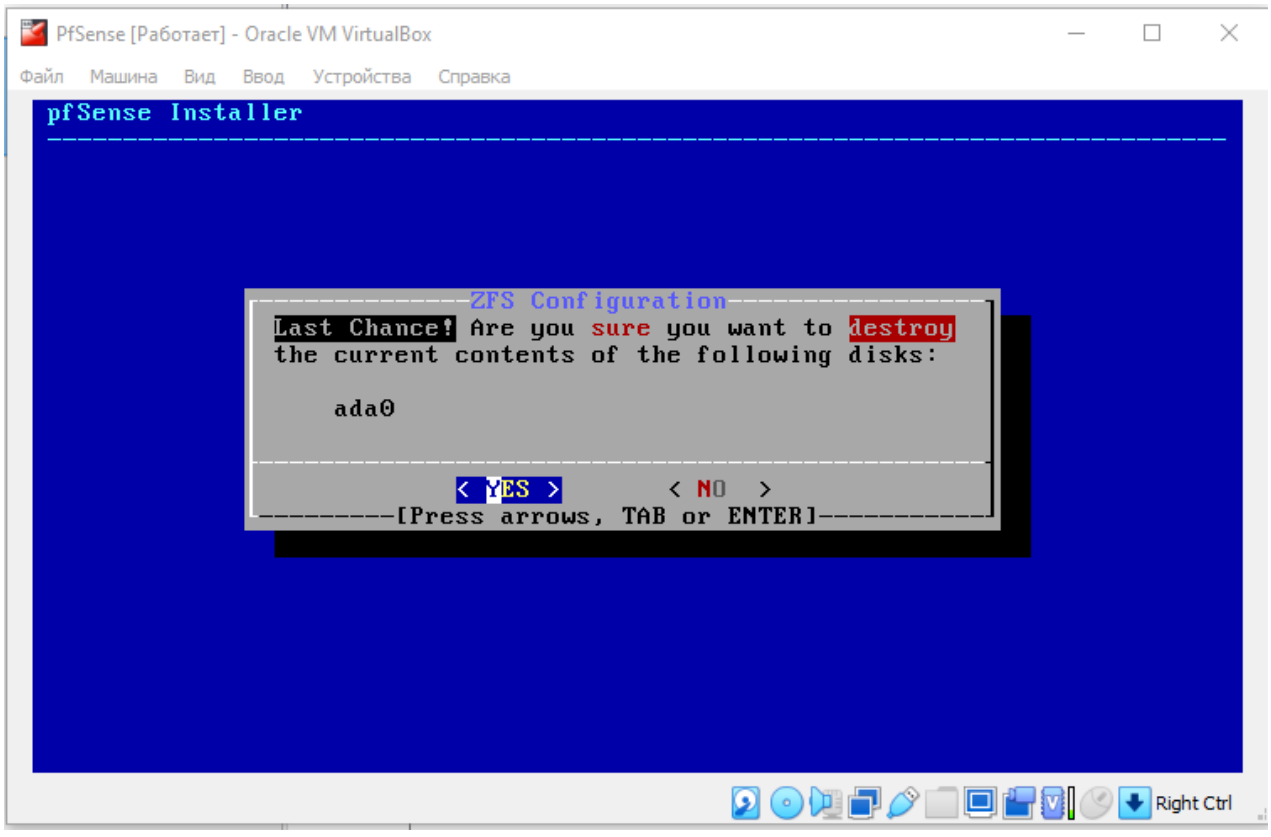

Рисунок 3.10 – Продовження конфігурації диску.

Далі відбувається автоматичний процес встановлення маршрутизатора (див. рис. 3.11) в кінці тиснемо ні (див. рис. 3.12), а потім перезавантажити (див. рис. 3.13).

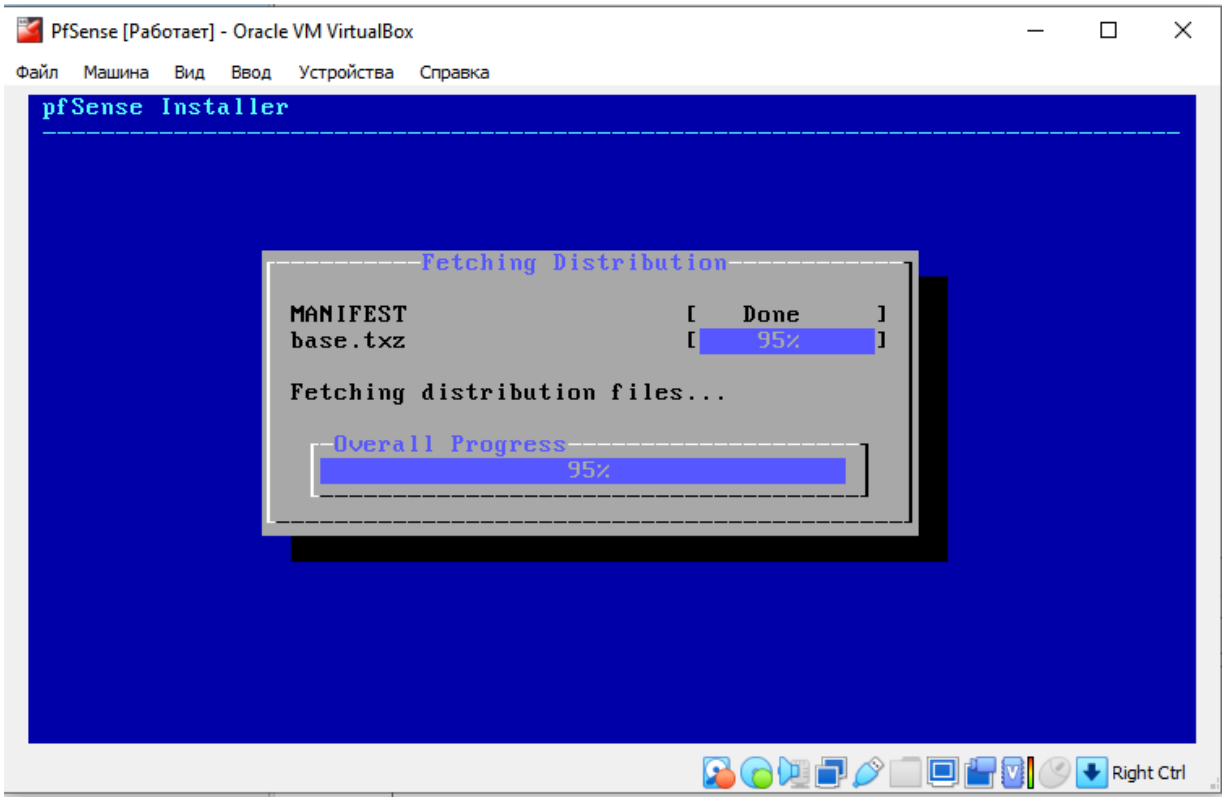

Рисунок 3.11 – Автоматичне налаштування маршрутизатора.

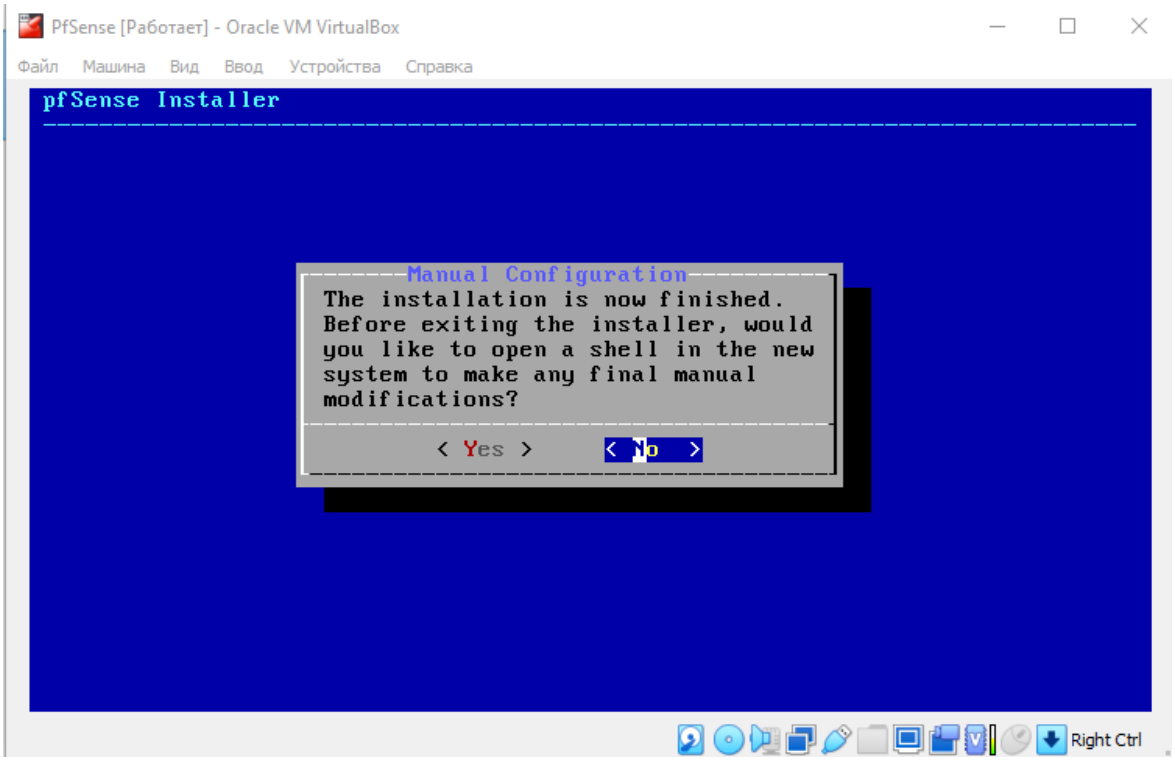

Рисунок 3.12 – Підтвердження в кінці встановлення.

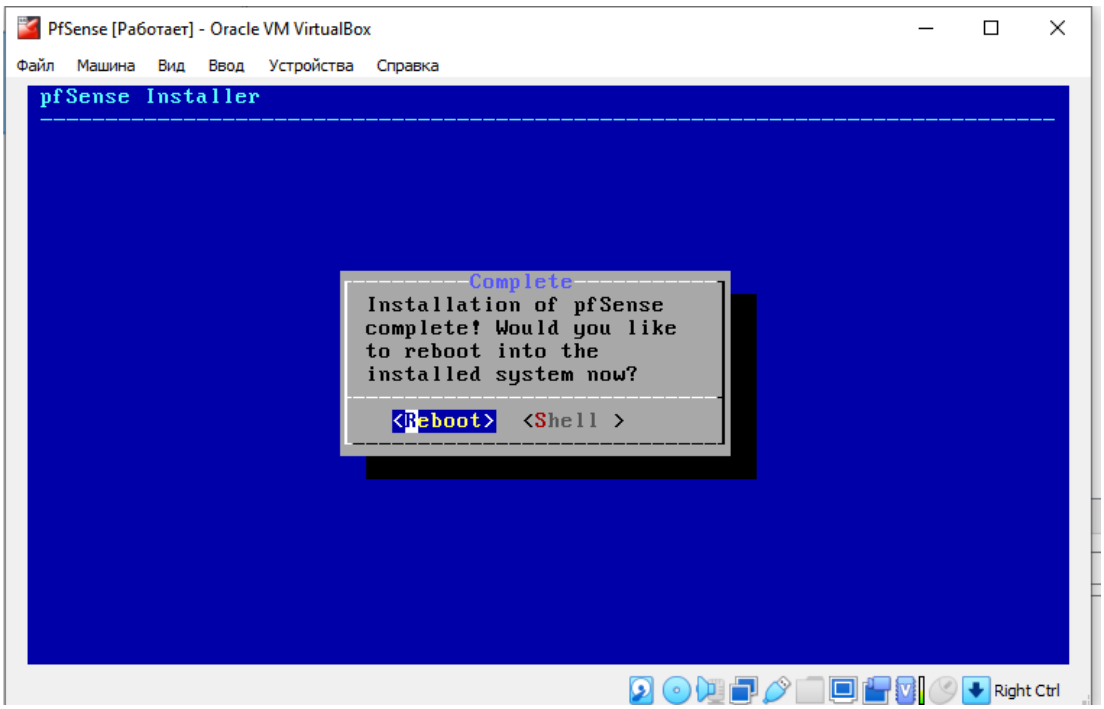

Рисунок 3.13 – Кінець налаштування PfSense.

Після цього маршрутизатор перезавантажується і ми отримуємо доступ до консолі, після завантаження одразу можна побачити IP адресу маршрутизатору та 16 можливих варіантів роботи з PfSense (див. рис. 3.14).

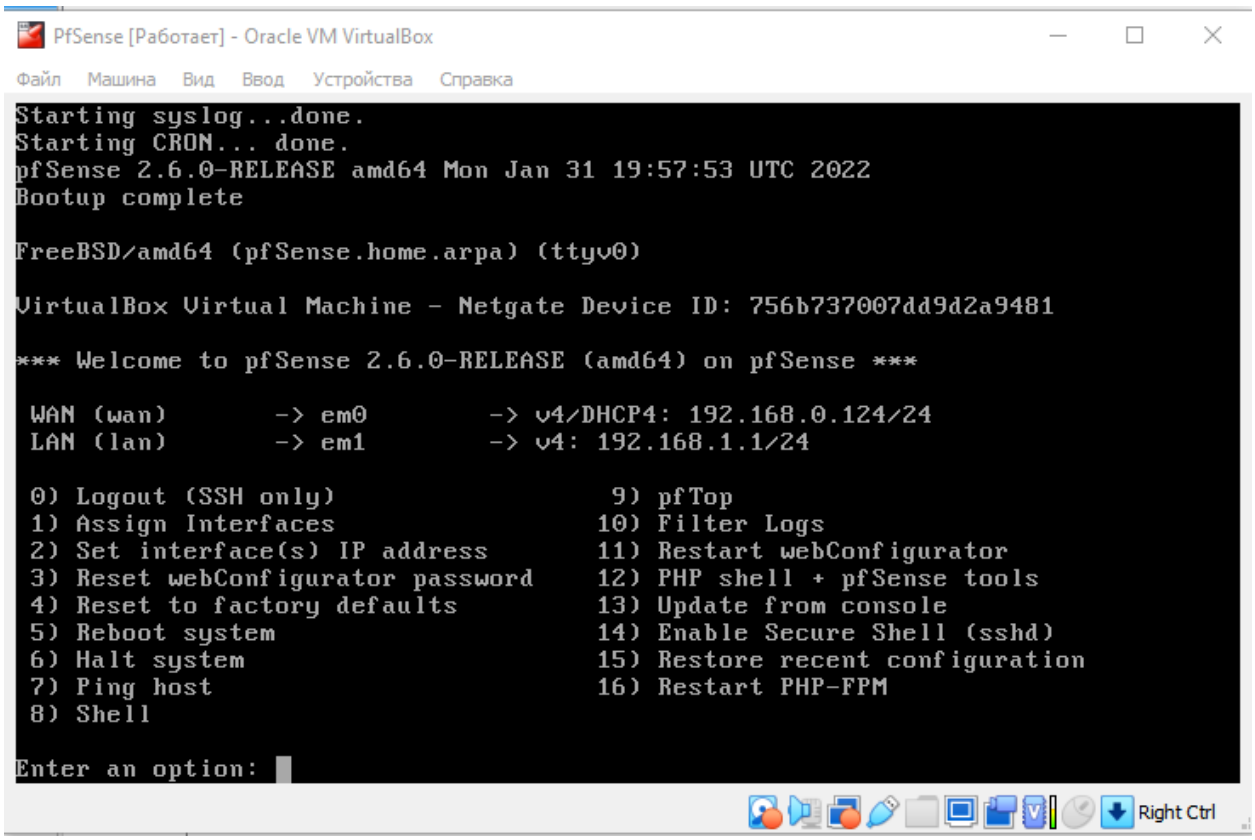

Рисунок 3.14 – PfSense після налаштування.

Сервер та клієнт використовують операційну систему Ubuntu. Після встановлення серверу необхідно назначити йому статичну IP адресу. Для цього заходимо в налаштування утиліти netplan та вказуємо статичну адресу (див. рис. 3.15, 3.16). Після цього за допомогою команди перевіряємо коректність налаштувань та зберігаємо зміни (див. рис. 3.17).

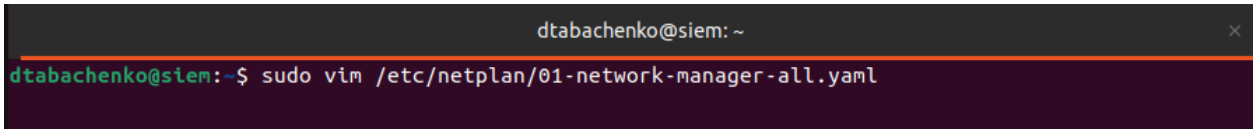

Рисунок 3.15 – Відкриття netplan.

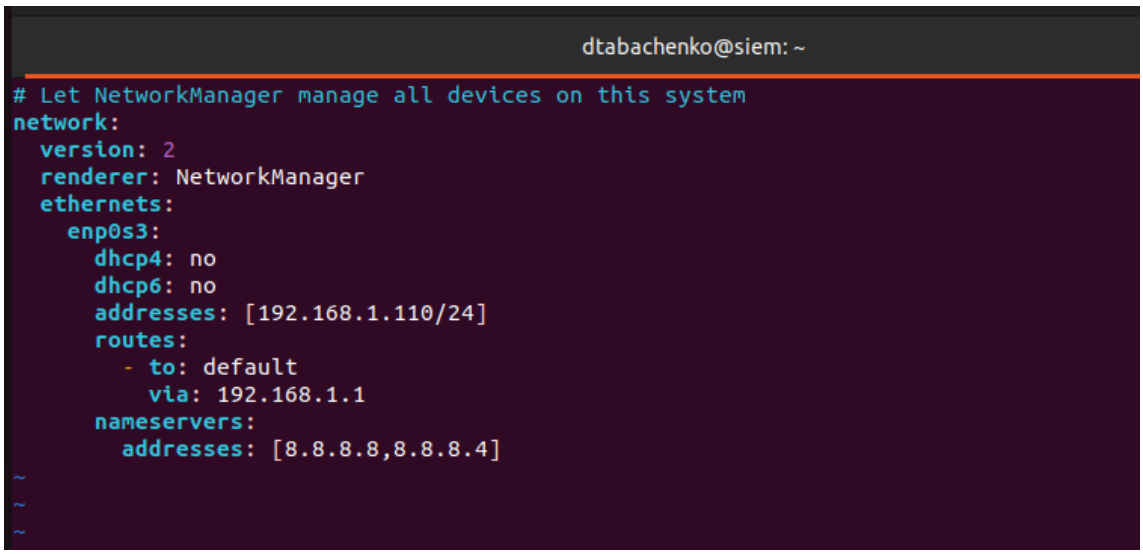

Рисунок 3.16 – Конфігурація netplan.

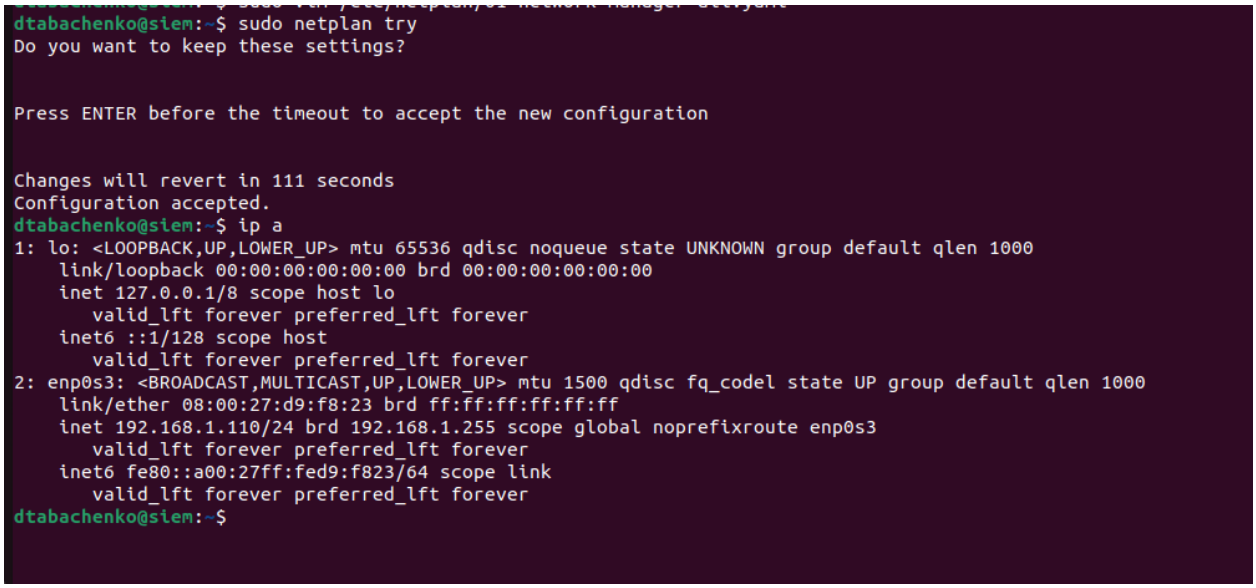

Рисунок 3.17 – Перевірка конфігурації netplan.

Переходимо безпосередньо до встановлення та налаштування ELK на сервері. Для встановлення необхідно додати репозиторії ELK в систему (див. рис. 3.18), оновити пакети в системі та завантажити elasticsearch (див. рис. 3.19).

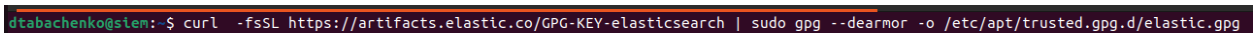

Рисунок 3.18 – Додавання репозиторіїв в систему.

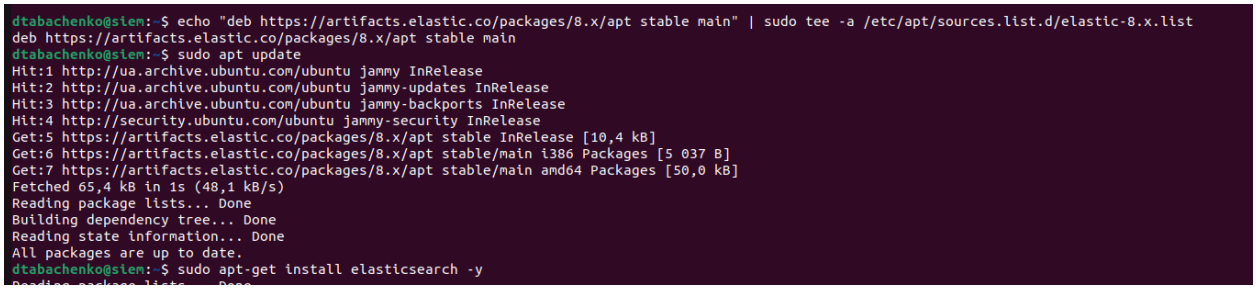

Рисунок 3.19 – Встановлення elasticsearch.

Переходимо до налаштування elasticsearch (див. рис. 3.20) та змінюємо IP адресу серверу elasticsearch (див. рис. 3.21).

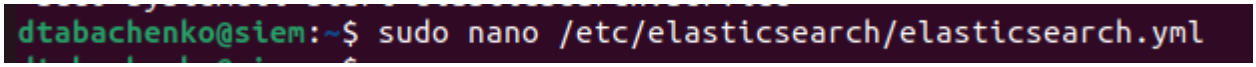

Рисунок 3.20 – Відкриття конфігурації elasticsearch.

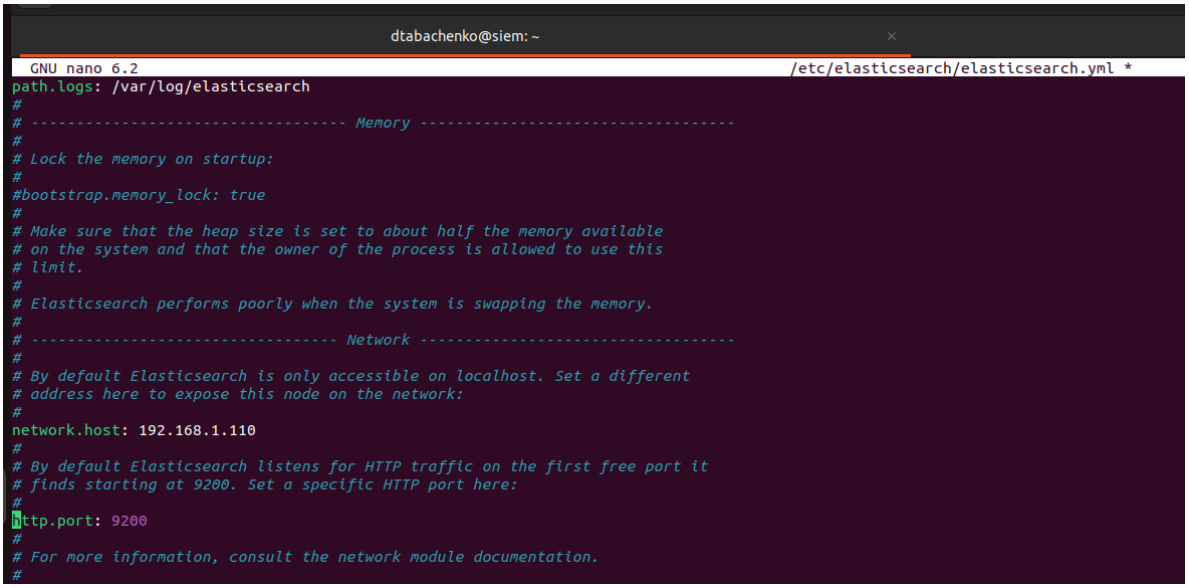

Рисунок 3.21 – Конфігурація elasticsearch.

Запускаємо сервіс, додаємо його в автозапуск та перевіряємо статус (див. рис. 3.22). Elasticsearch запущен та працює.

```
dtabachenko@siem:~$ sudo systemctl start elasticsearch
dtabachenko@siem:~$ sudo systemctl enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/sys
dtabachenko@siem:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enab
     Active: active (running) since Fri 2023-05-05 22:58:19 EEST; 18s ago
       Docs: https://www.elastic.co
   Main PID: 6462 (java)
      Tasks: 82 (limit: 8067)
     Memory: 3.7G
        CPU: 1min 25.419s
     CGroup: /system.slice/elasticsearch.service
             ├─6462 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -D
             ├─6518 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -
             └─6538 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/con

тра 05 22:57:31 siem systemd[1]: Starting Elasticsearch...
тра 05 22:58:19 siem systemd[1]: Started Elasticsearch.
dtabachenko@siem:~$
```

Рисунок 3.22 – Статус роботи elasticsearch.

Починаємо встановлення kibana (див. рис. 3.23) та переходимо в конфігураційний файл (див. рис. 3.24).

```
dtabachenko@siem:~$ sudo apt-get install kibana
```

Рисунок 3.23 – Встановлення kibana.

```
dtabachenko@siem:~$ sudo nano /etc/kibana/kibana.yml
```

Рисунок 3.24 – Перехід до редагування конфігураційного файлу kibana.

В конфігураційному файлі змінюємо IP адресу серверу kibana та серверу elasticsearch (див. рис. 3.25 та 3.26).

```
dtabachenko@siem: ~
 GNU nano 6.2                                  /etc/kibana/kibana.yml *
# ================== System: Kibana Server ==================
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "192.168.1.110"
```

Рисунок 3.25 – Редагування конфігураційного файлу kibana.

```
# ================== System: Elasticsearch ==================
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://192.168.1.110:9200"]
```

Рисунок 3.26 – Редагування конфігураційного файлу kibana.

Запускаємо сервіс, додаємо його в автозапуск та перевіряємо статус (див. рис. 3.27). Kibana запущена та працює.

```
dtabachenko@siem:~$ sudo systemctl start kibana
dtabachenko@siem:~$ sudo systemctl enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /lib/systemd/system/kibana.service.
dtabachenko@siem:~$ sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/lib/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2023-05-05 23:04:28 EEST; 11s ago
       Docs: https://www.elastic.co
   Main PID: 6774 (node)
      Tasks: 11 (limit: 8067)
     Memory: 159.7M
        CPU: 9.825s
     CGroup: /system.slice/kibana.service
             └─6774 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist

тра 05 23:04:28 siem systemd[1]: Started Kibana.
тра 05 23:04:35 siem kibana[6774]: [2023-05-05T23:04:35.626+03:00][INFO ][node] Kibana process configured with roles: [background_tasks, ui]
dtabachenko@siem:~$
```

Рисунок 3.27 – Статус роботи kibana.

Починаємо встановлення logstash (див. рис. 3.28) та створюємо конфігураційний файл, для роботи logstash (див. рис. 3.29). Вказуємо, що logstash повинен приймати події на порт 5044, застосовувати до них фільтр, який буде змінювати час події та повідомлення події, а в кінці відправляти події в elasticsearch з індексом, який буде відповідати версії агенту beat та дати його підключення (див. рис. 3.30).

```
dtabachenko@siem:~$ sudo apt-get install logstash
```

Рисунок 3.28 – Встановлення logstash.

```
root@siem:~# sudo vim /etc/logstash/conf.d/beats.conf
```

Рисунок 3.29 – Перехід до редагування конфігураційного файлу logstash.

```
root@siem: ~
input {
  beats {
    port => 5044
  }
}
filter {
  if [type] == "syslog" {
     grok {
        match => { "message" => "%{SYSLOGLINE}" }
  }
     date {
        match => [ "timestamp", "MMM  d HH:mm:ss", "MMM dd HH:mm:ss" ]
     }
  }
}
output {
  elasticsearch {
    hosts => ["192.168.1.110:9200"]
    index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"
  }
}
~
~
```

Рисунок 3.30 – Конфігураційний файл logstash.

Перевіряємо правильність конфігурації (див. рис. 3.31). Бачимо результат OK це означає, що конфігурація правильна.

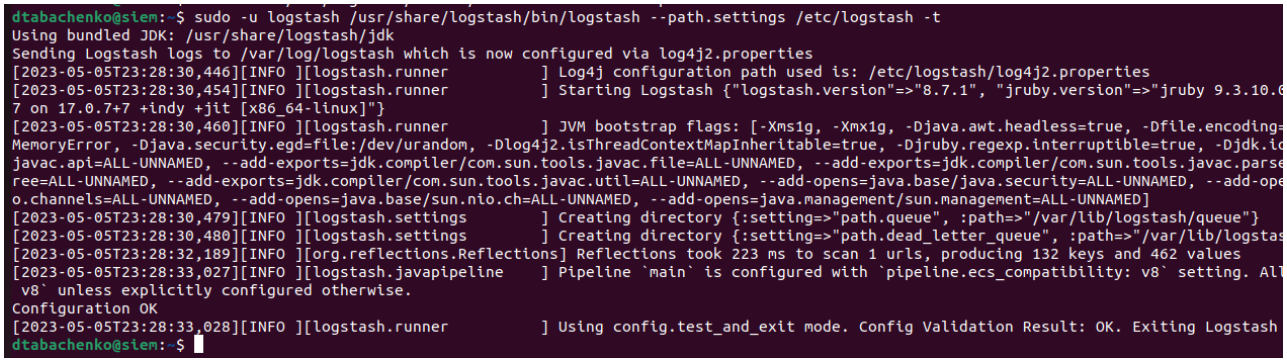

Рисунок 3.31 – Перевірка правильності конфігурації logstash.

Запускаємо сервіс, додаємо його в автозапуск та перевіряємо статус (див. рис. 3.32). Logstash працює.

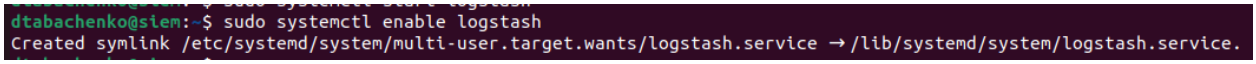

Рисунок 3.32 – Статус роботи logstash.

Після встановлення клієнта призначаємо йому статичну адресу, повторюючи дії, які робили раніше. (див. рис. 3.33–3.35).

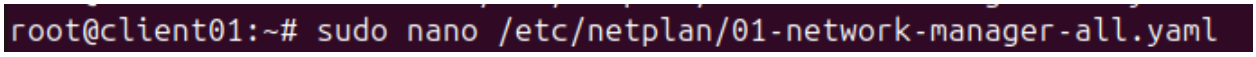

Рисунок 3.33 – Відкриття netplan.

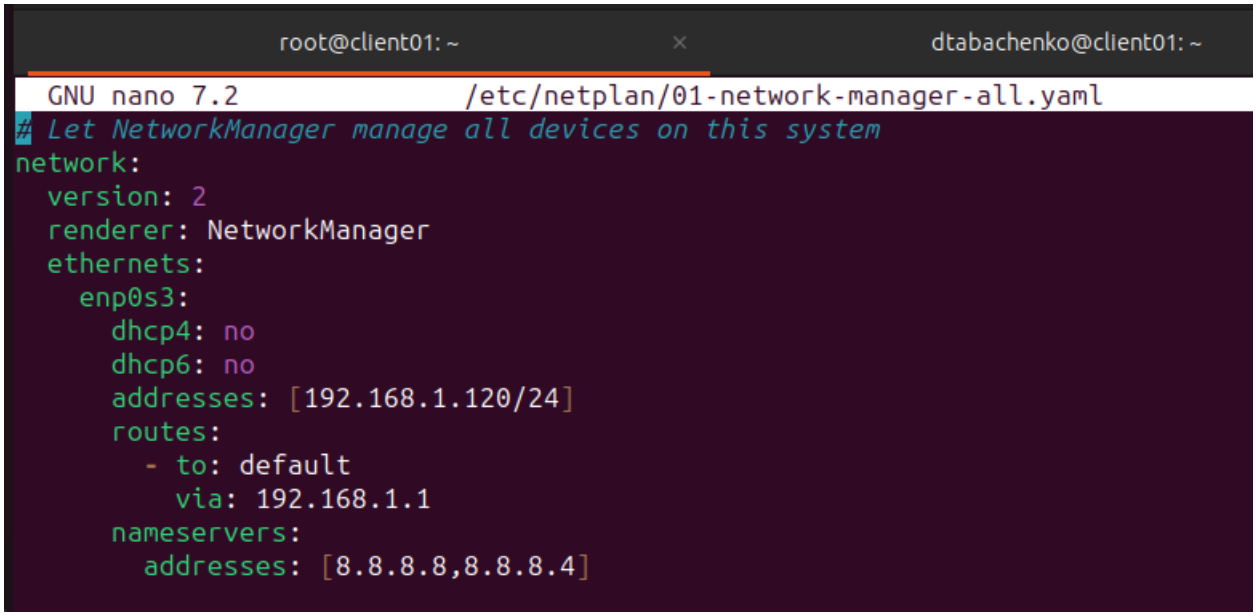

Рисунок 3.34 – Зміна конфігурації netplan.

```
root@client01:~# netplan try
```

Рисунок 3.35 – Перевірка конфігурації netplan та прийняття змін.

Додаємо репозиторій агенту filebeat на клієнт (див. рис. 3.36) і починаємо його встановлення (див. рис. 3.37).

```
root@client01: ~
root@client01:~# curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.7.1-amd64.deb
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 40.5M  100 40.5M    0     0  8081k      0  0:00:05  0:00:05 --:--:-- 8724k
```

Рисунок 3.36 – Додання репозиторію на клієнт.

```
root@client01:~# sudo dpkg -i filebeat-8.7.1-amd64.deb
```

Рисунок 3.37 – Встановлення filebeat.

Після цього змінюємо конфігураційний файл агенту коментуючи абзац, який відповідає за відправку подій в elasticsearch (див. рис. 3.38, 3.39) та редагуємо абзац для відправки подій в logstash. (див. рис. 3.40).

```
root@client01:~# vim /etc/filebeat/filebeat.yml
```

Рисунок 3.38 – Команда для редагування конфігурації агенту.

```
# ================================== Outputs ===================================

# Configure what output to use when sending the data collected by the beat.

# ---------------------------- Elasticsearch Output ----------------------------
#output.elasticsearch:
  # Array of hosts to connect to.
  # hosts: ["localhost:9200"]
```

Рисунок 3.39 – Розділ відправки подій в elasticsearch.

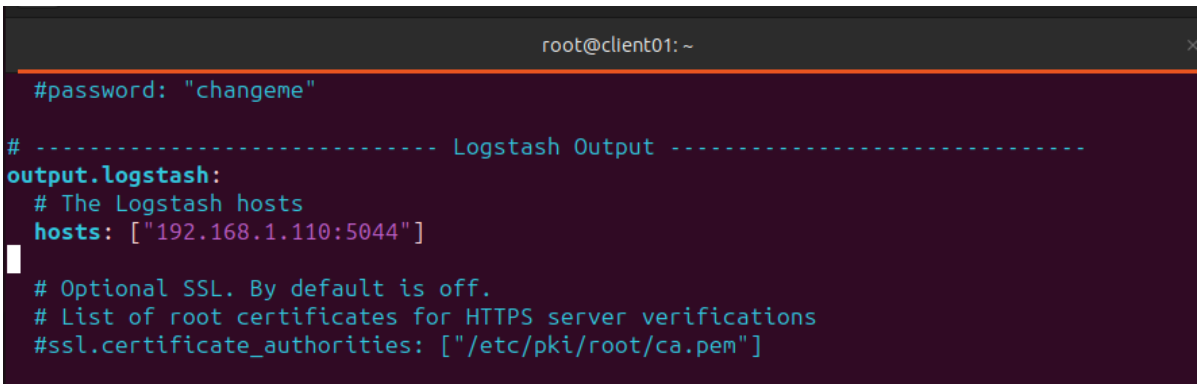

Рисунок 3.40 – Розділ відправки подій в logstash.

Filebeat за замовчуванням не відправляє події на сервер, для відправки подій необхідно в конфігураційному файлі увімкнути відправку подій змінивши значення false на true (див. рис. 3.41).

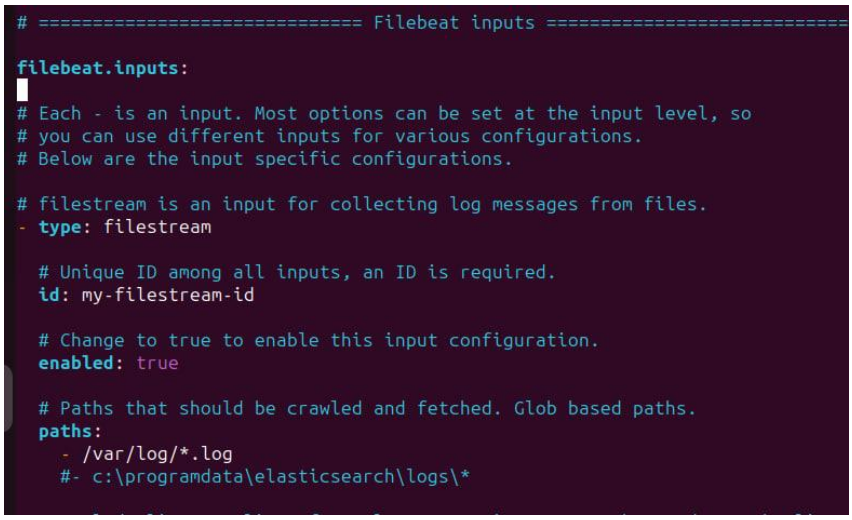

Рисунок 3.41 – Налаштування відправки подій в filebeat.

Тепер необхідно увімкнути модулі filebeat. В filebeat кожен модуль відповідає за відправку різних типів подій. Filebeat підтримує багато різних модулів, які дозволяють зручно та швидко налаштувати відправку подій різних сервісів, таких як: nginx та surikata. В даній роботі було обрано та налаштовано роботу модулів system - відповідає за системні логи та auditd - відповідає за логи аудиту. Файли конфігурації модулів знаходяться за шляхом /etc/filebeat/modules.d. Для ввімкнення модуля необхідно змінити статус модуля в файлі конфігурації змінивши значення false на true (див. рис. 3.42) та ввести команду в консоль (див. рис. 3.43). Повторюємо ті ж самі кроки для ввімкнення модуля auditd (див. рис. 3.44).

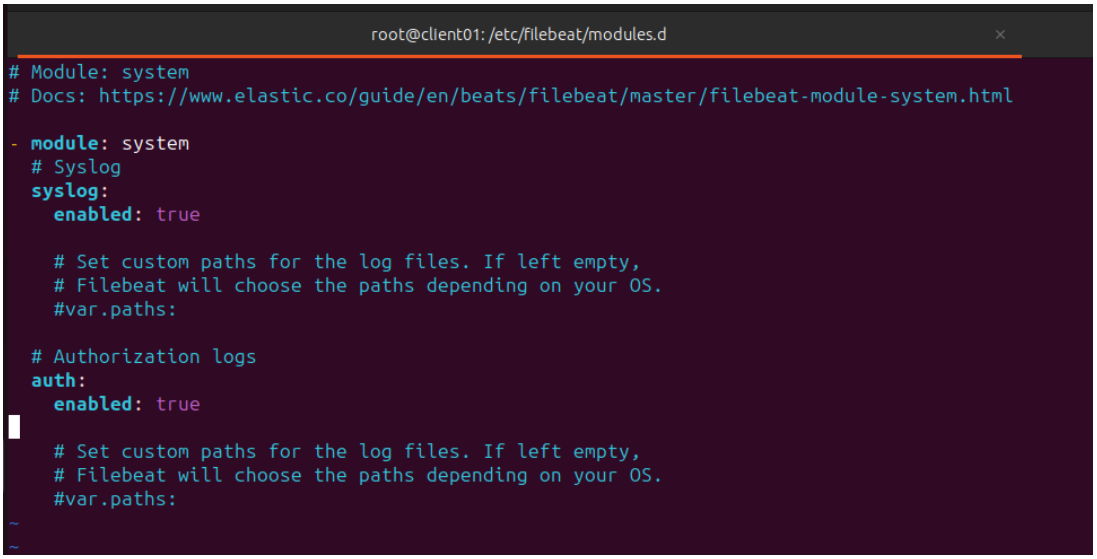

Рисунок 3.42 – Файл конфігурації модуля system.

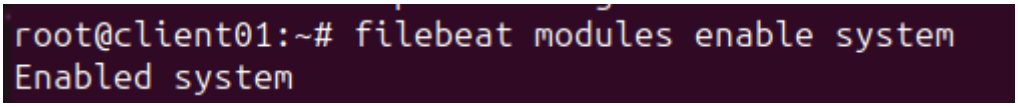

Рисунок 3.43 – Ввімкнення модуля system.

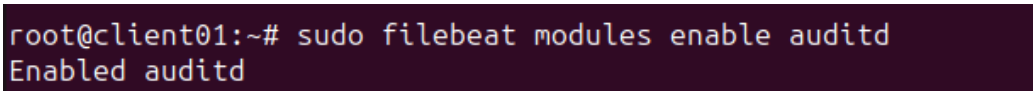

Рисунок 3.44 – Ввімкнення модуля system.

Для перевірки ввімкнених та вимкнених модулів вводимо команду (див. рис. 3.45).

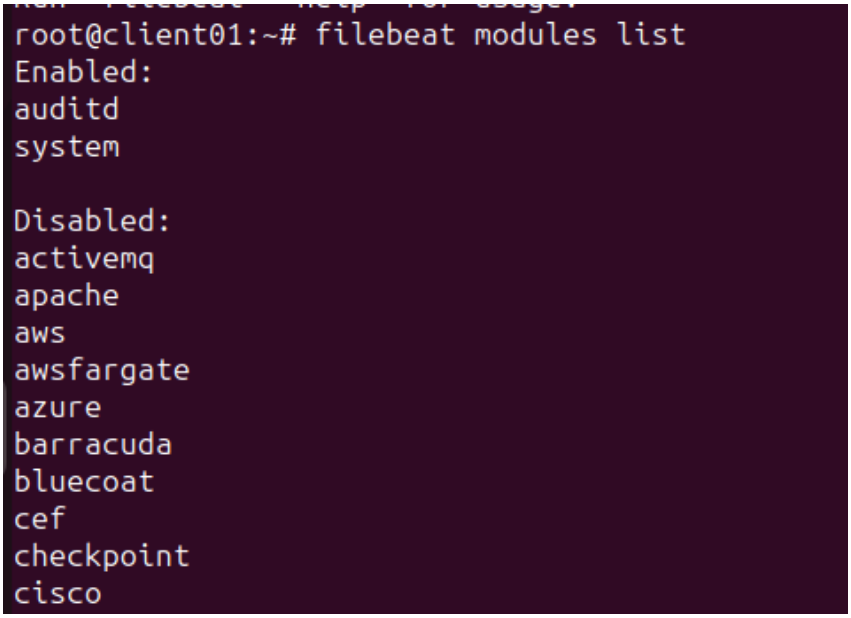

Рисунок 3.45 – Перевірка модулів filebeat.

Далі необхідно завантажити шаблон індексу в Elasticsearch (див. рис. 3.46). Індекси ідентифікуються за назвою. Корисно звертатися до індексу при виконанні в ньому різних операцій. Шаблон індексу застосовується автоматично під час створення нового індексу.

```
root@client01:~# filebeat setup --index-management -E output.logstash.enabled=false -E 'o
utput.elasticsearch.hosts=["192.168.1.110:9200"]'
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling.

Index setup finished.
```

Рисунок 3.46 – Завантаження індексів filebeat в elasticsearch.

Kibana дозволяє візуалізувати дані Filebeat. Для цього необхідно завантажити інформаційні панелі командою. Під час завантаження інформаційних панелей Filebeat підключається до Elasticsearch, перевіряючи інформацію про версію. Для завантаження панелей необхідно увімкнути відправку логів в Elasticsearch (див. рис. 3.47).

```
root@client01:~# sudo filebeat setup -E output.logstash.enabled=false -E output.elasticsearch.hosts=['192.168.1.110:9200'] -E setup.kibana.host=192.168.1.110:5601
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded Ingest pipelines
```

Рисунок 3.47 – Завантаження інформаційних панелей filebeat в elasticsearch.

Запускаємо сервіс, додаємо його в автозапуск, за допомогою команди перевіряємо індекс (див. рис. 3.48) та перевіряємо статус (див. рис. 3.49).

```
root@client01:~# curl -X GET http://192.168.1.110:9200/_cat/indices?v
health status index                           uuid                   pri rep docs.count docs.deleted store.size pri.store.size
yellow open   .ds-filebeat-8.7.1-2023.05.08-000001 j0lb0LuTTyWrPOLA8g7zqQ   1   1          0            0       225b           225b
root@client01:~#
```

Рисунок 3.48 – Перевірка індексів filebeat.

```
root@client01:~# systemctl start filebeat
root@client01:~# systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib/systemd/system/filebeat.service.
root@client01:~# systemctl status filebeat
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
     Loaded: loaded (/lib/systemd/system/filebeat.service; enabled; preset: enabled)
     Active: active (running) since Mon 2023-05-08 20:41:36 EEST; 671ms ago
       Docs: https://www.elastic.co/beats/filebeat
   Main PID: 2720 (filebeat)
      Tasks: 5 (limit: 4581)
     Memory: 32.6M
        CPU: 115ms
     CGroup: /system.slice/filebeat.service
             └─2720 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/s

May 08 20:41:36 client01 systemd[1]: Started filebeat.service - Filebeat sends log files to Logstash or directly to Elastic
May 08 20:41:36 client01 filebeat[2720]: {"log.level":"info","@timestamp":"2023-05-08T20:41:36.767+0300","log.origin":{"fil
May 08 20:41:36 client01 filebeat[2720]: {"log.level":"info","@timestamp":"2023-05-08T20:41:36.768+0300","log.origin":{"fil
lines 1-14/14 (END)
```

Рисунок 3.49 – Статус роботи filebeat.

Додаємо репозиторій агенту metricbeat на клієнт і починаємо його встановлення (див. рис. 3.50). Аналогічно до налаштування filebeat вмикаємо відправку логів в logstash (див. рис. 3.51)

```
root@client01:~# curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-8.7.1-amd64.deb
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 46.7M  100 46.7M    0     0  7552k      0  0:00:06  0:00:06 --:--:-- 9559k
root@client01:~# sudo dpkg -i metricbeat-8.7.1-amd64.deb
```

Рисунок 3.50 – Встановлення metricbeat.

```
root@client01: ~

# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.1.110:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

Рисунок 3.51 – Конфігурація metricbeat.

Аналогічно до налаштувань filebeat завантажуємо індекси та інформаційні панелі (див. рис. 3.52). Після цього вмикаємо автозапуск та запускаємо сервіс.

```
root@client01:~# metricbeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["192.168.1.110:9200"]'
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling.

Index setup finished.
root@client01:~# metricbeat setup -E output.logstash.enabled=false -E output.elasticsearch.hosts=['192.168.1.110:9200'] -E setup.kibana.host=192.168.1.110:5601
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
root@client01:~#
```

Рисунок 3.52 – Завантаження індексів та інформаційних панелей metricbeat в elasticsearch.

3.3 Огляд функцій SIEM системи та робота з подіями

Заходимо в kibana та тиснемо “Explore on my own”. Після цього нам стає доступний веб інтерфейс сервісу. Kibana має 4 розділи, кожен з яких відповідає за функціонал різного типу.

Розділи Kibana:

1. Аналітика – містить один з найголовніших підрозділів Discover в якому SOC аналітики можуть шукати події, а також інформаційні панелі (див. рис. 3.53).

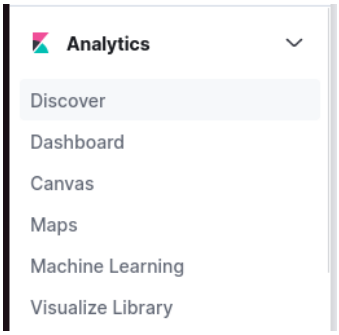

Рисунок 3.53 – Розділ Analytics.

2. Observability – здебільшого містить інформацію про інфраструктуру, яка підключена до кластеру ELK, час роботи клієнтів, їх статус (див. рис. 3.54, 3.55).

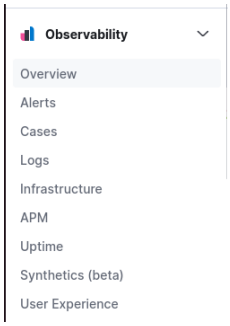

Рисунок 3.54 – Розділ Observability.

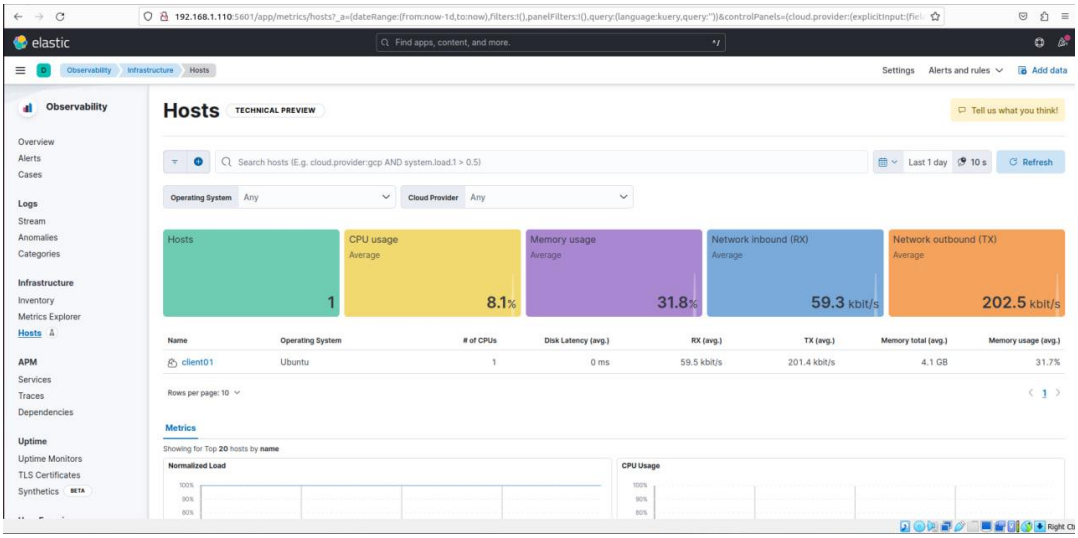

Рисунок 3.55 – Розділ огляду підключених клієнтів.

3. Security – тут можливо налаштувати сповіщення на події, які відбуваються в системі, можна переглядати статистику по сповіщенням та створювати інформаційні панелі для аналізу цих даних (див. рис. 3.56).

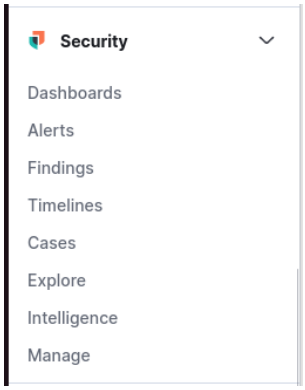

Рисунок 3.56 – Розділ Security.

4. Management – розділ для управління стеком. Тут можливо додавати інтеграції з детальним описом дій, які потрібно виконати. Окремий підрозділ виділено для Fleet – утиліта для централізованого управління агентами та для OSquery – утиліта, яка дозволяє виконувати команди з веб консолі kibana на кінцевих точках (див. рис. 3.57).

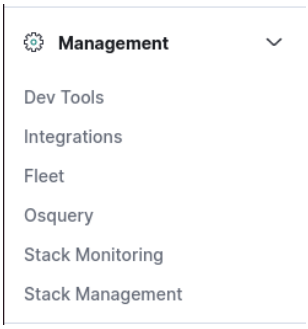

Рисунок 3.57 – Розділ Management.

Відкриваємо розділ discover і перевіряємо наявність логів (див. рис. 3.58). Отже, агенти налаштовані правильно і передають логи. Зліва наведена інформація про поля, які є в подіях. Також є можливість змінювати джерело подій для відображення подій тільки з одного агента (див. рис. 3.59).

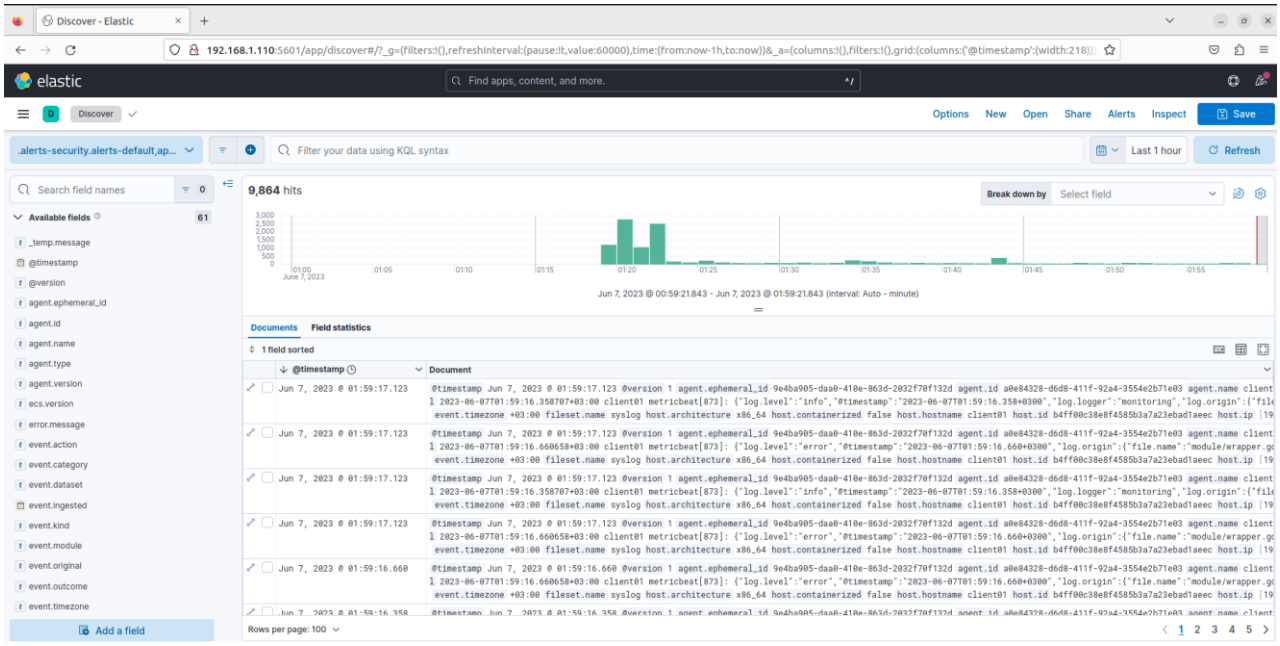

Рисунок 3.58 – Розділ Discover.

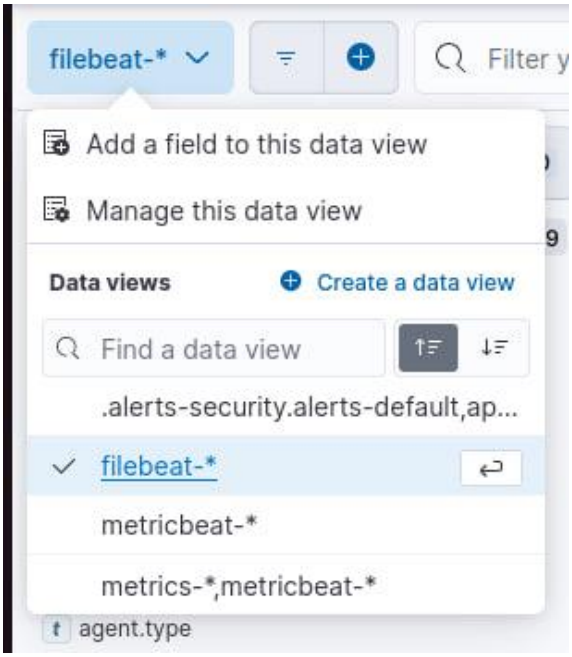

Рисунок 3.59 – Меню джерел подій.

Спробуємо згенерувати події, для цього робимо невдалі спроби підключення по ssh на кінцевій точці (див. рис. 3.60). Спробуємо знайти події по ключовим словам, використовуючи назву сервісу sshd (див. рис. 3.61).

```
root@client01:~# ssh dtabachenko@192.168.1.120
The authenticity of host '192.168.1.120 (192.168.1.120)' can't be established.
ED25519 key fingerprint is SHA256:l0dz2H4a//ZWriWHx/kyHoNXFUTs+tJ7iboQifcPXGI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.120' (ED25519) to the list of known hosts.
dtabachenko@192.168.1.120's password:
Permission denied, please try again.
dtabachenko@192.168.1.120's password:
ePermission denied, please try again.
dtabachenko@192.168.1.120's password:
dtabachenko@192.168.1.120: Permission denied (publickey,password).
root@client01:~# ssh dtabachenko@192.168.1.120
dtabachenko@192.168.1.120's password:
Permission denied, please try again.
dtabachenko@192.168.1.120's password:
Permission denied, please try again.
dtabachenko@192.168.1.120's password:
dtabachenko@192.168.1.120: Permission denied (publickey,password).
root@client01:~#
```

Рисунок 3.60 – Генерація подій.

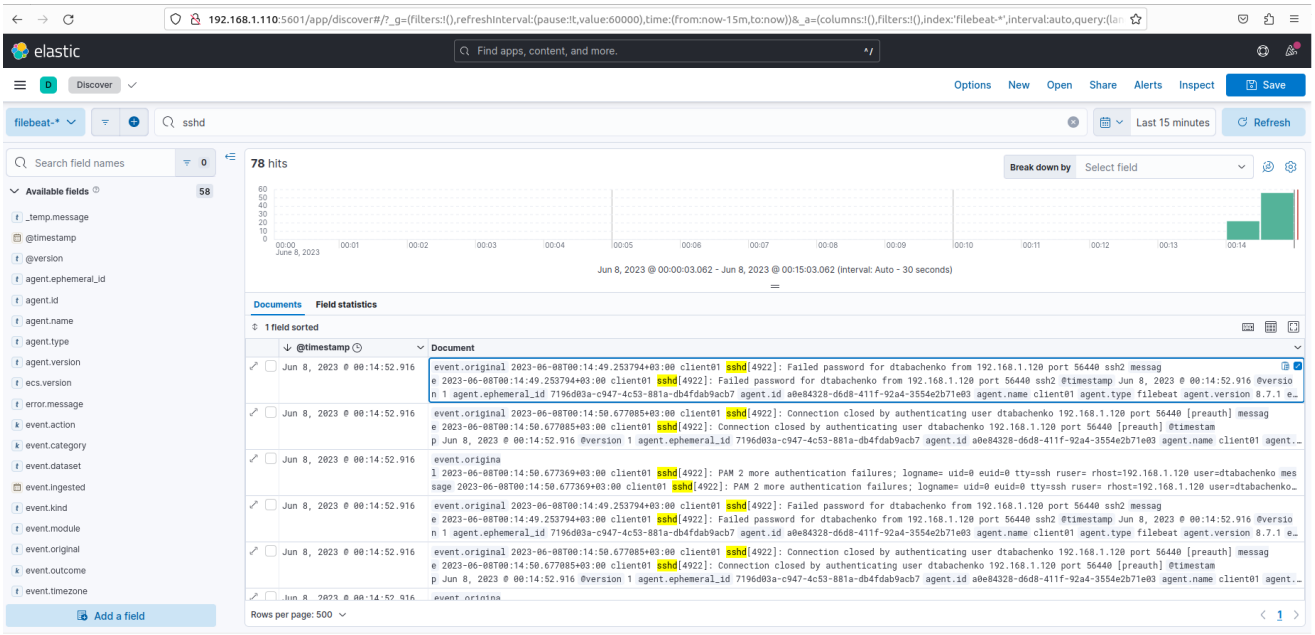

Рисунок 3.61 – Пошук по ключовим словам.

Для кращого читання подія розгортаємо його (див. рис. 3.62), в події є інформація про назву індексу, час події, тип агенту, оригінальна подія з клієнту про невдалу спробу входу, назва кінцевої точки, тип операційної системи, її архітектура, шлях папки на кінцевій точці в якій зберігається подія (див. додаток А).

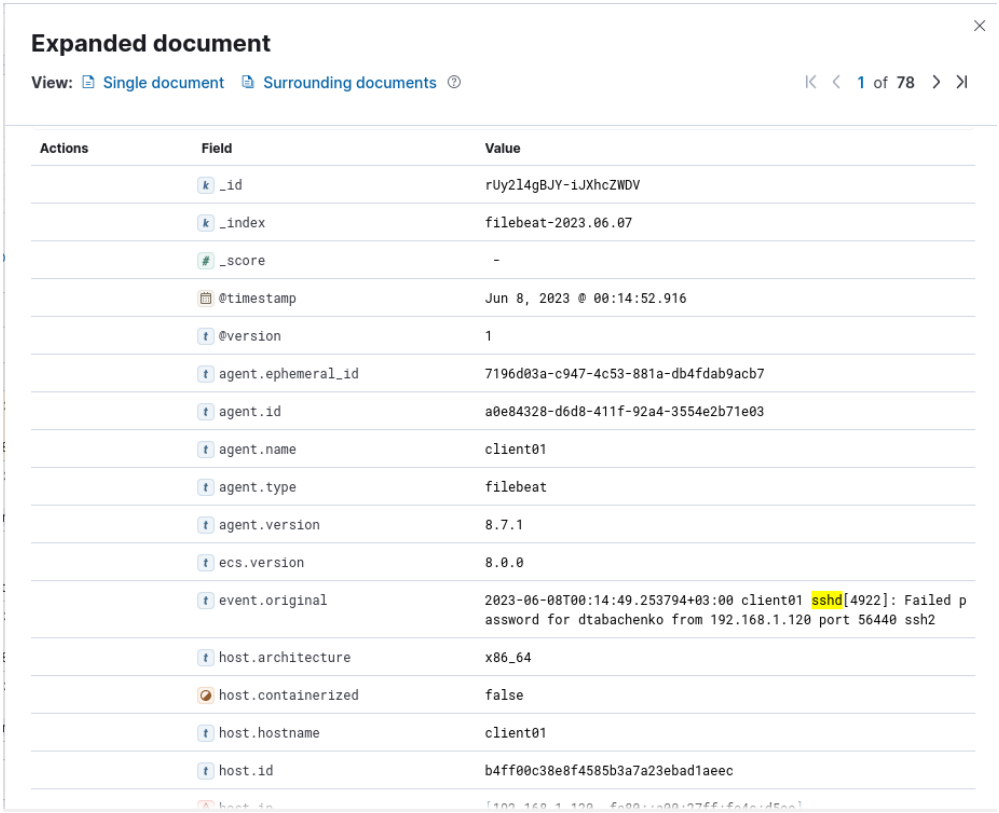

Рисунок 3.62 – Невдала спроба підключення по ssh протоколу.

Після успішного підключення агенту metricbeat в розділі Observability відкривається можливість слідкувати за метриками кінцевої точки, такими як: завантаження процесору, кількість пам’яті, що використовується, мережеве навантаження (див. рис. 3.63).

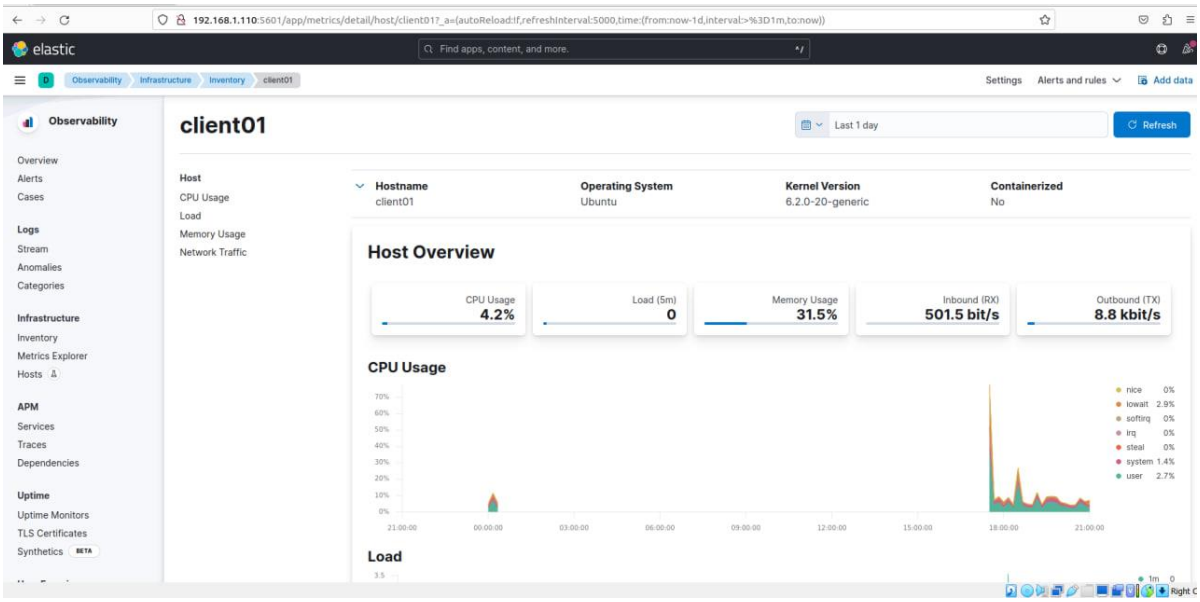

Рисунок 3.63 – Перевірка метрик клієнта.

Висновки за розділом 3

У даній роботі була сконфігуровано систему управління подіями та інформаційною безпекою на базі ELK. Реалізація SIEM системи на базі ELK стеку має декілька переваг. Elasticsearch використовується для зберігання та індексації великого обсягу журналів та подій. Logstash забезпечує потокову обробку та нормалізацію даних з різних джерел. Kibana надає інтуїтивно зрозумілий інтерфейс для візуалізації та аналізу даних. Розглянуто основні функції цієї системи та їх потенційні переваги для забезпечення кібербезпеки.

Основні функції SIEM системи на базі ELK включають збір, аналіз, виявлення і реагування на події, пов'язані з кібербезпекою. Збір даних здійснюється шляхом збору подій з різних джерел, таких як сервери, мережеві пристрої, додатки. Після збору дані проходять процес аналізу, що включає виявлення аномалій, ідентифікацію загроз та пошук кореляцій між різними подіями. Результати аналізу можуть бути візуалізовані за допомогою графіків, діаграм та інших інструментів Kibana. У разі виявлення підозрілих дій або загроз SIEM система може працювати налагодженими правилами та автоматичними процедурами, включаючи відправку сповіщень адміністраторам або активування заходів захисту.

Правильне налаштування та ефективне використання SIEM системи на базі ELK може значно покращити реагування на кібератаки та забезпечити високий рівень безпеки інформаційних систем.

Узагальнюючи, реалізація SIEM системи на базі ELK є потужним інструментом для забезпечення кібербезпеки. Вона дозволяє виявляти та аналізувати підозрілу активність, реагувати на потенційні загрози та створювати звіти для моніторингу та аудиту безпеки. Продуктивність, масштабованість та гнучкість ELK стеку роблять його відмінним вибором для реалізації SIEM системи.

ВИСНОВКИ

У кваліфікаційній роботі було вибрано і скомпоновано засоби для налаштування системи управління подіями та інформаційною безпекою, як однієї з найважливіших систем для центру оперативної безпеки.

У першому розділі було проведено аналіз функцій центру оперативної безпеки. Аналіз складався з дослідження нормативно-правової бази в галузі інформаційної безпеки та реагуванні на інциденти, огляд функцій, типів та складу центру оперативної безпеки, а також засобів захисту, які використовуються. Розглядалися наступні засоби захисту:

- Засоби виявлення вторгнень.
- Засоби запобігання вторгненням.
- EDR.
- Брандмауери.
- Поштові шлюзи.
- Інтернет шлюзи.
- Програмні засоби Threat Intelligence.
- IR платформи.
- SIEM системи.
- SOAR системи.

У другій частині роботи було розглянуто види та функціональні особливості SIEM систем. Також проведено аналіз популярних SIEM систем на ринку. Також проведено детальний огляд ELK стеку, його функціонал, архітектуру та особливості роботи.

У третій частині кваліфікаційної роботи на основі проаналізованих у першому та другому розділах даних було створено архітектуру, в якій PfSense виступає в якості маршрутизатора і дві віртуальні машини в якості клієнта та сервера SIEM системи. Було сконфігуровано систему управління подіями та інформаційною безпекою на базі ELK (Elasticsearch, Logstash, Kibana). Реалізація SIEM системи на базі ELK стеку має

декілька переваг. Elasticsearch використовується для зберігання та індексації великого обсягу журналів та подій. Logstash забезпечує потокову обробку та нормалізацію даних з різних джерел. Kibana надає інтуїтивно зрозумілий інтерфейс для візуалізації та аналізу даних. Beat агенти: metricbeat, filebeat з модулями system, auditd. Також проведено огляд сконфігурованої системи та перевірено правильність налаштування шляхом створення невдалих спроб логіну по протоколу ssh на клієнті і пошуку на сервері та налаштовано функції для відстеження стану сервера та клієнта: завантаженість процесора, використання оперативної пам’яті, використання диску, мережеве навантаження.

Таким чином, всі завдання, які були поставлені відповідно до мети кваліфікаційної роботи були виконані в повному обсязі, а саме:

- досліджено роботу центру оперативної безпеки для виявлення особливостей функціонування.;
- проведено аналіз засобів захисту центру оперативної безпеки для підбору його компонентів;
- досліджено механізми роботи та функціонал SIEM систем для моделювання та конфігурації SIEM системи;
- підібрано компоненти та проведено практичне налаштування SIEM системи для відслідковування стану інфраструктури організації та пошуку подій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Data Breach [Електронний ресурс]. – Режим доступу: https://www.ibm.com/reports/data-breach

2. Готовність України до нових викликів. Кібербезпека і зв’язок [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/news/gotovnist-ukrayini-do-novikh-viklikiv-kiberbezpeka-i-zv-yazok

3. Готовність України до нових викликів. Кібербезпека і зв’язок [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/news/gotovnist-ukrayini-do-novikh-viklikiv-kiberbezpeka-i-zv-yazok

4. У 2022 році в Україні зареєстрували 2194 кіберінциденти — Держспецзв’язку [Електронний ресурс]. – Режим доступу: https://suspilne.media/397220-u-2022-roci-v-ukraini-zareestruvali-2194-kiberincidenti-derzspeczvazku/

5. Cybercrime Losses Exceeded $10 Billion in 2022: FBI [Електронний ресурс]. – Режим доступу: https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi

6. 2022_IC3Report [Електронний ресурс]. – Режим доступу: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

7. What is a Security Operations Center (SOC) [Електронний ресурс]. – Режим доступу: https://www.ibm.com/topics/security-operations-center

8. 63 Terrifying Cyber Security Statistics from 2022 [Електронний ресурс]. – Режим доступу: https://www.tekspace.com.au/blog/cyber-security-stats-2022.

9. РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/9600/1/11.pdf

10. Security Operations Center (SOC)? [Електронний ресурс]. – Режим доступу: https://www.trellix.com/en-us/security-awareness/operations/what-is-soc.html

11. Cyberframework [Електронний ресурс]. – Режим доступу: https://www.nist.gov/cyberframework

12. Cybersecurity Framework Components [Електронний ресурс]. – Режим доступу: https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

13. NIST.SP.800-61r2 [Електронний ресурс]. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

14. Installation Walkthrough [Електронний ресурс]. – Режим доступу: https://docs.netgate.com/pfsense/en/latest/install/install-walkthrough.html

15. What is IDS and IPS? [Електронний ресурс. – Режим доступу: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

16. What Is Endpoint Detection and Response (EDR)? [Електронний ресурс]. – Режим доступу: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html

17. What is a Firewall? [Електронний ресурс]. – Режим доступу: https://www.forcepoint.com/cyber-edu/firewall

18. What is a Firewall? The Different Firewall Types & Architectures [Електронний ресурс]. – Режим доступу: https://www.compuquip.com/blog/types-firewall-architectures

19. What Are the Basic Types of Firewalls? [Електронний ресурс]. – Режим доступу: https://www.parallels.com/blogs/ras/types-of-firewalls/

20. Що таке Endpoint Detection and Response? Топ-3 найкращих EDR рішень [Електронний ресурс]. – Режим доступу: https://ua.softlist.com.ua/articles/chto-takoe-endpoint-detection/

21. Security Information and Event Management (SIEM) [Електронний ресурс]. – Режим доступу: https://itglobal.com/ru-ru/company/glossary/security-information-and-event-management-siem/

22. Security Information and Event Management (SIEM) [Електронний ресурс]. – Режим доступу: https://itglobal.com/ru-ru/company/glossary/security-information-and-event-management-siem/

23. What Is ELK Stack [Електронний ресурс]. – Режим доступу: https://aws.amazon.com/what-is/elk-stack/?nc1=h_ls

24. Documentation [Електронний ресурс]. – Режим доступу: https://docs.splunk.com/Documentation

25. QRadar [Електронний ресурс]. – Режим доступу: https://www.ibm.com/docs/en/qradar

26. Elastic Security for SIEM & security analytics [Електронний ресурс]. – https://www.elastic.co/security/siem

27. LogRhythm Enterprise SIEM [Електронний ресурс]. – https://docs.logrhythm.com/docs/enterprise

28. SOAR (Security Orchestration, Automation and Response) [Електронний ресурс]. – Режим доступу: https://encyclopedia.kaspersky.ru/glossary/security-orchestration-automation-and-response-soar/

29. What Is SOAR? [Електронний ресурс]. – Режим доступу: https://www.trellix.com/en-us/security-awareness/operations/what-is-soar.html

30. SPLUNK [Електронний ресурс]. – Режим доступу: https://www.mogroup.com.ua/?p=607

31. What is Splunk? [Електронний ресурс]. – Режим доступу: https://www.knowledgehut.com/blog/database/what-is-splunk

32. Installing Elasticsearch [Електронний ресурс]. – Режим доступу: https://www.elastic.co/guide/en/elasticsearch/reference/current/install-elasticsearch.html

33. NXLog Documentation [Електронний ресурс]. – Режим доступу: https://docs.nxlog.co/userguide/integrate/mcafee-esm.html

34. Install Kibana with Debian package [Електронний ресурс]. – Режим доступу: https://www.elastic.co/guide/en/kibana/current/deb.html

35. Installing Logstash [Електронний ресурс]. – Режим доступу: https://www.elastic.co/guide/en/logstash/current/installing-logstash.html

36. Top 10 Threat Intelligence Platforms in 2022 [Електронний ресурс]. – Режим доступу: https://www.spiceworks.com/it-security/vulnerability-management/articles/best-threat-intelligence-platforms/

37. What Is a Secure Email Gateway (SEG)? [Електронний ресурс]. – Режим доступу: https://www.proofpoint.com/us/threat-reference/email-gateway

38. Incident Response Platform: The Road to Automating IR [Електронний ресурс]. – Режим доступу: https://www.cynet.com/incident-response-services/incident-response-platform-the-road-to-automating-ir/

39. Metasploitable [Електронний ресурс]. – Режим доступу: https://sourceforge.net/projects/metasploitable/

ДОДАТОК А

Невдала спроба входу по протоколу ssh


```
{
 "_index": "filebeat-2023.06.07",
 "_id": "rUy2l4gBJY-iJXhcZWDV",
 "_version": 1,
 "_score": 0,
 "_source": {
  "ecs": {
   "version": "8.0.0"
  },
  "agent": {
   "name": "client01",
   "id": "a0e84328-d6d8-411f-92a4-3554e2b71e03",
   "type": "filebeat",
   "version": "8.7.1",
   "ephemeral_id": "7196d03a-c947-4c53-881a-db4fdab9acb7"
  },
  "@version": "1",
  "host": {
   "id": "b4ff00c38e8f4585b3a7a23ebad1aeec",
   "name": "client01",
   "ip": [
    "192.168.1.120",
    "fe80::a00:27ff:fe4c:d5ee"
   ],
   "hostname": "client01",
   "mac": [
    "08-00-27-4C-D5-EE"
   ],
   "architecture": "x86_64",
   "containerized": false,
   "os": {
    "codename": "lunar",
    "platform": "ubuntu",
    "name": "Ubuntu",
    "version": "23.04 (Lunar Lobster)",
    "type": "linux",
    "kernel": "6.2.0-20-generic",
    "family": "debian"
   }
  },
  "message": "2023-06-08T00:14:49.253794+03:00 client01 sshd[4922]: Failed password for dtabachenko from 192.168.1.120 port 56440 ssh2",
  "log": {
   "offset": 26146,
   "file": {
    "path": "/var/log/auth.log"
   }
```

Продовження додатку А


```
      },
        "tags": [
          "beats_input_codec_plain_applied"
        ],
        "@timestamp": "2023-06-07T21:14:52.916Z",
        "event": {
          "original": "2023-06-08T00:14:49.253794+03:00 client01 sshd[4922]: Failed password for
dtabachenko from 192.168.1.120 port 56440 ssh2"
        },
        "input": {
          "type": "filestream"
        }
      },
      "fields": {
        "agent.version.keyword": [
          "8.7.1"
        ],
        "host.architecture.keyword": [
          "x86_64"
        ],
        "host.name.keyword": [
          "client01"
        ],
        "host.hostname": [
          "client01"
        ],
        "host.mac": [
          "08-00-27-4C-D5-EE"
        ],
        "ecs.version.keyword": [
          "8.0.0"
        ],
        "host.ip.keyword": [
          "192.168.1.120",
          "fe80::a00:27ff:fe4c:d5ee"
        ],
        "host.os.version": [
          "23.04 (Lunar Lobster)"
        ],
        "host.os.name": [
          "Ubuntu"
        ],
        "host.id.keyword": [
          "b4ff00c38e8f4585b3a7a23ebad1aeec"
        ],
        "agent.name": [
          "client01"
        ],
        "host.name": [
          "client01"
```

Продовження додатку А


```
        ],
        "host.os.version.keyword": [
          "23.04 (Lunar Lobster)"
        ],
        "event.original": [
          "2023-06-08T00:14:49.253794+03:00 client01 sshd[4922]: Failed password for dtabachenko
from 192.168.1.120 port 56440 ssh2"
        ],
        "host.os.type": [
          "linux"
        ],
        "agent.id.keyword": [
          "a0e84328-d6d8-411f-92a4-3554e2b71e03"
        ],
        "input.type": [
          "filestream"
        ],
        "@version.keyword": [
          "1"
        ],
        "log.offset": [
          26146
        ],
        "tags": [
          "beats_input_codec_plain_applied"
        ],
        "host.architecture": [
          "x86_64"
        ],
        "agent.id": [
          "a0e84328-d6d8-411f-92a4-3554e2b71e03"
        ],
        "host.containerized": [
          false
        ],
        "ecs.version": [
          "8.0.0"
        ],
        "message.keyword": [
          "2023-06-08T00:14:49.253794+03:00 client01 sshd[4922]: Failed password for dtabachenko
from 192.168.1.120 port 56440 ssh2"
        ],
        "host.hostname.keyword": [
          "client01"
        ],
        "agent.version": [
          "8.7.1"
        ],
        "host.os.family": [
          "debian"
```

Продовження додатку А


```
],
"input.type.keyword": [
  "filestream"
],
"tags.keyword": [
  "beats_input_codec_plain_applied"
],
"host.ip": [
  "192.168.1.120",
  "fe80::a00:27ff:fe4c:d5ee"
],
"agent.type": [
  "filebeat"
],
"host.os.kernel.keyword": [
  "6.2.0-20-generic"
],
"host.os.kernel": [
  "6.2.0-20-generic"
],
"@version": [
  "1"
],
"host.os.name.keyword": [
  "Ubuntu"
],
"host.id": [
  "b4ff00c38e8f4585b3a7a23ebad1aeec"
],
"log.file.path.keyword": [
  "/var/log/auth.log"
],
"agent.type.keyword": [
  "filebeat"
],
"agent.ephemeral_id.keyword": [
  "7196d03a-c947-4c53-881a-db4fdab9acb7"
],
"host.os.codename.keyword": [
  "lunar"
],
"host.mac.keyword": [
  "08-00-27-4C-D5-EE"
],
"agent.name.keyword": [
  "client01"
],
"host.os.codename": [
  "lunar"
],
```

Продовження додатку А


```
        "message": [
          "2023-06-08T00:14:49.253794+03:00 client01 sshd[4922]: Failed password for dtabachenko
from 192.168.1.120 port 56440 ssh2"
        ],
        "host.os.family.keyword": [
          "debian"
        ],
        "host.os.type.keyword": [
          "linux"
        ],
        "@timestamp": [
          "2023-06-07T21:14:52.916Z"
        ],
        "host.os.platform.keyword": [
          "ubuntu"
        ],
        "host.os.platform": [
          "ubuntu"
        ],
        "log.file.path": [
          "/var/log/auth.log"
        ],
        "event.original.keyword": [
          "2023-06-08T00:14:49.253794+03:00 client01 sshd[4922]: Failed password for dtabachenko
from 192.168.1.120 port 56440 ssh2"
        ],
        "agent.ephemeral_id": [
          "7196d03a-c947-4c53-881a-db4fdab9acb7"
        ]
      }
    }
```