

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

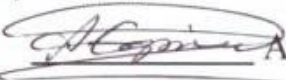
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack»

Виконав: студент 4-го курсу групи КБ-21-2
спеціальності 125 «Кібербезпека»

 Віталій ГНАТЮК

Керівник: завідувач кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

 Андрій ЄФІМЕНКО

Рецензент: професор кафедри комп'ютерної інженерії та
кібербезпеки, доктор технічних наук, доцент

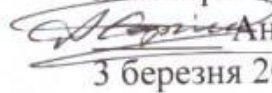
 Володимир ВОРОТНИКОВ

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій ЄФІМЕНКО
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Гнатюк Віталій Олександрович

Тема роботи: «Проект підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack»

затверджена Наказом університету від 3 березня 2025 р. № 80/с

Термін здачі студентом закінченої роботи 20 червня 2025 р.

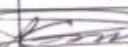
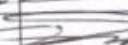
Вихідні дані роботи:

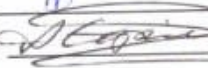
Об'єктом дослідження є процес проектування підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack. Предметом дослідження є технологія проектування підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack.

Обладнання та програмне забезпечення:

1. Мережевий емулятор GNS3;
2. SIEM-рішення The Elastic Stack;
3. Операційна система Linux Ubuntu Server;
4. Операційна система Kali Linux;
5. Операційна система Linux Ubuntu
6. Операційна система Windows 10

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 25.04.2025	 25.04.2025
2	Єфіменко А.А.	 16.05.2025	 16.05.2025
3	Єфіменко А.А.	 05.06.2025	 05.06.2025

Студент  Віталій Гнатюк
Керівник  Андрій Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	02.03.2025-06.03.2025	
2	Аналіз літературних джерел	07.03.2025-27.03.2025	
3	Аналіз об'єкта дослідження	28.03.2025-06.04.2025	
4	Аналіз аналогів	07.04.2025-12.04.2025	
5	Вибір обладнання та програмного забезпечення	13.04.2025-23.04.2025	
6	Розробка архітектури підсистеми моніторингу	24.04.2025-08.05.2025	
7	Інсталяція та конфігурація ELK Stack	09.05.2025-16.05.2025	
8	Налагодження збору та обробки подій безпеки	17.05.2025-22.05.2025	
9	Тестування системи	23.05.2025-28.05.2025	
10	Написання пояснювальної записки	29.05.2025-13.06.2025	
11	Отримання відгуку та рецензії на кваліфікаційну роботу	13.06.2025-19.06.2025	
12	Захист	24.06.2025	

Студент  Віталій Гнатюк

Керівник  Андрій Єфіменко

АНОТАЦІЯ

Кваліфікаційна робота бакалавра представлена у вигляді проєкту підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack.

Мета і завдання роботи. Метою роботи є проєктування підсистеми моніторингу подій інформаційної безпеки в мережі з використанням рішень The Elastic Stack

Досягнення поставленої мети передбачає виконання наступних завдань:

- Дослідження основ функціонування підсистеми моніторингу подій інформаційної безпеки та вимог до неї;
- Огляд можливостей The Elastic Stack та альтернативних рішень;
- Розробка архітектури підсистеми SIEM на основі ELK;
- Налаштування системи моніторингу подій на базі рішення The Elastic Stack;
- Проведення тестування та аналіз результатів для покращення системи;
- Оцінка ефективності підсистеми при виявленні інцидентів інформаційної безпеки;

Об'єктом дослідження є процес проєктування підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack.

Предметом дослідження є технологія проєктування підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack

Пояснювальна записка до випускної кваліфікаційної роботи складається зі вступу, трьох розділів, висновку, списку використаної літератури та додатків.

Текстова частина викладена на 91 сторінці друкованого тексту.

Пояснювальна записка має список використаних джерел, який містить 21 найменувань і займає 2 сторінки. Робота містить 3 таблиці та 84 рисунка. Загальний обсяг роботи – 96 сторінок.

Ключові слова: ELK, МОНІТОРИНГ ПОДІЙ, ІНФОРМАЦІЙНА БЕЗПЕКА, КОМП'ЮТЕРНА МЕРЕЖА, ЗАХИСТ, SIEM СИСТЕМА.

					ККІК.КР.Б – 125 – 5 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми моніторингу по- дій інформаційної безпеки в мережі — на базі рішень The Elastic Stack	Лім.	Арк.	Аркушів
Розроб.		Гнатюк В. О.		18.06.25			4	96
Керівник		Єфіменко А. А.		18.06.25				
Реценз.		Воротніков В. В.		18.06.25				
Н. контр.		Єфіменко А. А.		18.06.25				
Затверд.		Єфіменко А. А.		18.06.25				
						ФІКТ, Гр. КБ-21-2		

ANNOTATION

The bachelor's qualification work is presented in the form of a project for a subsystem for monitoring information security events in a network based on The Elastic Stack solutions.

Purpose and objectives of the work. The purpose of the work is to design a subsystem for monitoring information security events in a network using The Elastic Stack solutions

Achieving the set goal involves performing the following tasks:

- Research into the basics of the functioning of the subsystem for monitoring information security events and requirements for it;
- Review of the capabilities of The Elastic Stack and alternative solutions;
- Development of the architecture of the SIEM subsystem based on ELK;
- Configuring the event monitoring system based on The Elastic Stack solution;
- Conducting testing and analyzing the results to improve the system;
- Assessing the effectiveness of the subsystem in detecting information security incidents;

The object of the study is the process of designing a subsystem for monitoring information security events in a network based on The Elastic Stack solutions.

The subject of the study is the technology of designing a subsystem for monitoring information security events in the network based on The Elastic Stack solutions.

The explanatory note to the final qualification work consists of an introduction, three sections, a conclusion, a list of used literature and appendices.

The text part is set out on 91 pages of printed text.

The explanatory note has a list of used sources, which contains 21 items and occupies 2 pages. The work contains 3 tables and 84 figures. The total volume of the work is 96 pages.

Keywords: ELK, EVENT MONITORING, INFORMATION SECURITY, COMPUTER NETWORK, PROTECTION, SIEM SYSTEM.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ МОНІТОРИНГУ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	10
1.1 Архітектура та принципи функціонування SIEM-систем.....	10
1.2 Що таке The Elastic Stack і які його функціональні можливості.....	21
1.3 Огляд наявних альтернативних SIEM рішень	24
Висновки до першого розділу	44
РОЗДІЛ 2 ПРОЄКТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ ПОДІЙ НА БАЗІ THE ELASTIC STACK.....	45
2.1 Проєктування системи	45
2.2. Проєктування служб та сервісів	49
2.3 Аналіз рішення The Elastic Stack та допоміжного програмного забезпечення.....	51
2.4 Аналіз типових атак на систему моніторингу	52
Висновки до другого розділу	59
РОЗДІЛ 3 ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ СПРОЄКТОВАНОЇ СИСТЕМИ	60
3.1. Побудова та налагодження спроектованої системи	60
3.3. Тестування спроектованої системи	72
3.3. Налаштування захисту	85
Висновки до третього розділу.....	88
ВИСНОВКИ.....	89
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	90
ДОДАТКИ.....	92

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SIEM – Security information and event

ELK – Elasticsearch, Logstash, Kibana

IP – Internet Protocol

UDP – User Datagram Protocol

ОС – Операційна система

IPS – Intrusion Prevention System

IDS – Intrusion Detection System

DHCP – Dynamic Host Configuration Protocol

OSPF – Open Shortest Path First

DNS – Domain Name System

ІІІ – Штучний інтелект

UEBA – User and Entity Behavior Analytics

GNS3 – Graphical Network Simulator-3

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В умовах постійного розвитку інформаційних систем та все більшого їх впровадження в різні аспекти повсякденного життя, постає питання безпеки даних та моніторингу подій. Системи моніторингу подій безпеки дозволяють не лише виявляти інциденти в режимі реального часу, але й аналізувати причини їх виникнення, а також здійснювати прогнозування потенційних загроз. У цьому контексті інтеграція різних рішень для моніторингу, таких як The Elastic Stack, набуває особливої актуальності.

Тема роботи є актуальною через зростаючий попит на економічно вигідні, надійні та масштабовані рішення у сфері моніторингу подій безпеки.

Метою кваліфікаційної роботи є розробка проєкту підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack, що надасть можливість керувати та моніторити подіями та інцидентами інформаційної безпеки, підвищить рівень захищеності мережної інфраструктури організації, збільшить швидкість виявлення та реагування на загрози.

У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack. Проєкт включає в себе розробку архітектури системи, інтеграцію з іншими рішеннями безпеки та налаштування з метою забезпечення ефективного механізму виявлення та реагування на кіберзагрози.

Мета і завдання роботи. Метою роботи є проєктування підсистеми моніторингу подій інформаційної безпеки в мережі з використанням рішень The Elastic Stack.

Досягнення поставленої мети передбачає виконання наступних завдань:

- Дослідження основ функціонування підсистеми моніторингу подій інформаційної безпеки та вимог до неї;
- Огляд можливостей The Elastic Stack та альтернативних рішень;
- Розробка архітектури підсистеми SIEM на основі ELK;
- Налаштування системи моніторингу подій на базі рішення The Elastic Stack;
- Проведення тестування та аналіз результатів для покращення системи;

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

– Оцінка ефективності підсистеми при виявленні інцидентів інформаційної безпеки;

Об’єктом дослідження є процес проєктування підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack.

Предметом дослідження є технологія проєктування підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ МОНІТОРИНГУ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Архітектура та принципи функціонування SIEM-систем

Говорячи про SIEM варто уявляти складний механізм, де кожна деталь виконує чітко визначену функцію, і злагоджена робота кожного елемента гарантує справність усієї системи. Якщо хоча б один елемент вийде зладу, це може призвести до збою в роботі всієї системи. Архітектура[9] SIEM може мати різноманітну будову, але базова складова містить шість основних частин:

1. Пристрій-джерело даних.
2. Збір логів.
3. Парсинг/Нормалізація журналів подій.
4. Кореляція даних.
5. Збір логів.
6. Моніторинг подій.

Пристрій-джерело даних – це вихідна точка, з якої генеруються дані про події.

Збір логів – це компонент, який відповідає за збір логів з різних пристроїв-джерел.

Парсинг/Нормалізація журналів подій – це етап під час якого зібрані логи обробляються та перетворюються у стандартизований формат для подальшого аналізу.

Кореляція даних – це процес відбувається аналіз нормалізованих даних на відповідність заздалегідь визначеним правилам для виявлення підозрілої активності.

Зберігання журналів – це місце, де зберігаються всі зібрані та оброблені журнали для історичного аналізу та відповідності регуляторним вимогам.

Моніторинг подій – це компонент забезпечує можливість моніторингу подій у реальному часі та зручного пошуку та отримання даних для розслідувань.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Кожна з цих частин може функціонувати самостійно, але без їхньої тісної взаємодії SIEM не зможе ефективно виконувати свої завдання з моніторингу та управління безпекою.

Загальна схема архітектури SIEM-системи наведена на рисунку 1.1.1

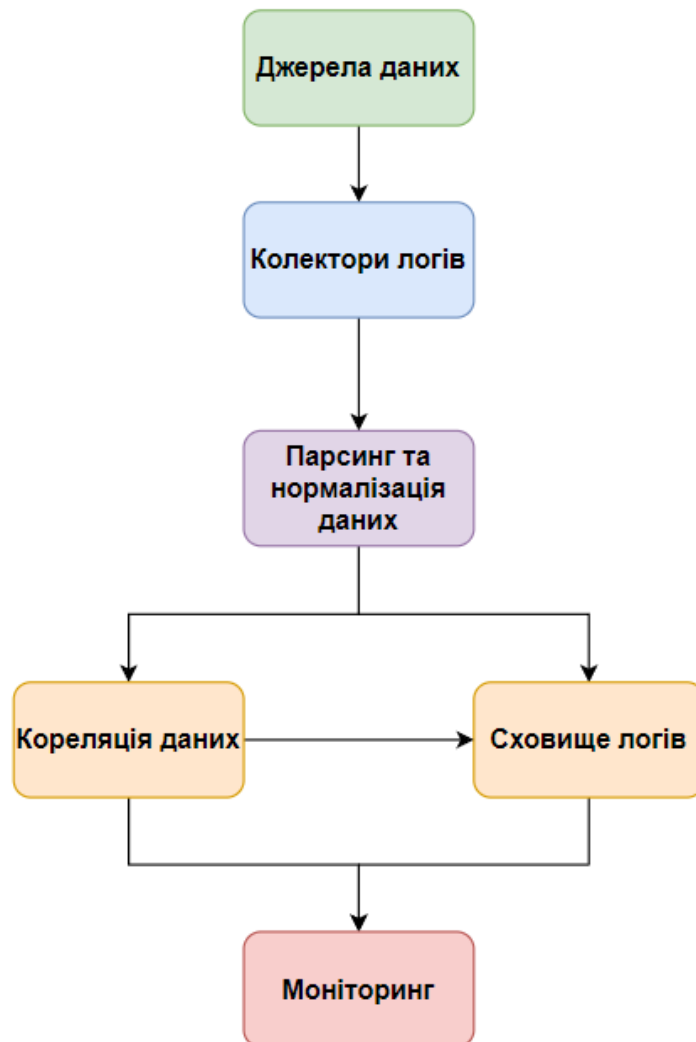


Рисунок 1.1.1 – Загальна схема архітектури SIEM-систем

Обсяг журналів цифрової активності часто залишається непомітним для звичайного користувача. Проста дія, така як відкриття браузера та перевірка електронної пошти, ініціює створення логів на безлічі пристроїв: від комп'ютера користувача до маршрутизаторів, міжмережевих екранів, комутаторів і самого вебсайту. Кожен із цих елементів фіксує певні події, створюючи записи, що документують

рух користувача мережею. Обсяг цих журналів величезний, і хоча не всі з них будуть корисними для аналізу, певні фрагменти можуть мати критичне значення для виявлення інцидентів безпеки чи розслідувань.

В основі будь-якої SIEM-системи[11] стоїть поняття пристрою-джерела. Хоча він і не є частиною самої SIEM, саме цей елемент визначає, звідки система отримує дані. Пристрій-джерело – це будь-який елемент інфраструктури, що генерує журнали: фізичні пристрої, програмне забезпечення або сторонні сервіси. Наприклад, це можуть бути сервери, мережеве обладнання, додатки або сервіси, які продукують дані, що містять інформацію про дії користувачів, події в системі та мережеву активність. Без таких джерел даних SIEM не зможе виконувати свої функції, залишаючись лише інструментом без наповнення.

На етапі впровадження SIEM важливо точно і чітко визначити, з яких джерел буде здійснюватися збір інформації. Це рішення має прийматися ще до початку активного розгортання системи, оскільки від нього залежить ефективність усієї подальшої роботи. Якщо структура джерел визначена правильно, це забезпечить стабільну і масштабовану роботу SIEM-рішення, зменшить кількість помилок та спростить налаштування збору, обробки і зберігання журналів у майбутньому.

Після того як стало зрозуміло, які саме пристрої та додатки присутні в IT-інфраструктурі, виникає наступне завдання це визначити, які журнали подій необхідні для ефективної роботи SIEM-системи. Основна мета отримати саме ті логи, які сприятимуть підвищенню рівня безпеки та забезпечать можливість вчасно виявляти і аналізувати проблеми в мережі. У деяких випадках збір та зберігання журналів зумовлений також вимогами нормативних актів і стандартів, що регламентують збереження інформації протягом встановленого періоду.

Втім, необхідно враховувати, що не кожен журнал подій є однаково корисним. Часто можна почути думку, що збирати слід усе, аби мати повну картину подій у мережі. Це частково вірно, але на практиці значно важливіше знайти правильний баланс між загальним обсягом даних і можливістю ефективно їх опрацьовувати. Надмірна кількість логів, особливо на початковому етапі впровадження SIEM, може призвести до перевантаження як інфраструктури, так і спеціалістів,

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

відповідальних за аналіз подій. Велика кількість непотрібної або малозначущої інформації ускладнює виявлення справді важливих інцидентів безпеки.

Крім обмежень у продуктивності, більшість адміністраторів стикаються з обмеженим обсягом сховищ і обчислювальних потужностей. Тому на ранніх етапах необхідно чітко визначити пріоритети: які саме типи журналів справді потрібні і з яких джерел вони мають надходити. Наприклад, потрібно зважити, чи є сенс зберігати журнали DNS-запитів лише для можливого використання в рідкісних сценаріях інцидентів. Хоча технічно така можливість існує, її доцільність слід обґрунтовувати виходячи з вартості зберігання та навантаження на систему.

Наступним кроком після визначення джерел є оцінка обсягів ресурсів[11], необхідних для обробки та зберігання отриманих даних. При цьому потрібно враховувати важливість кожного джерела з точки зору безпеки, орієнтовну кількість логів, які генерує кожен пристрій, частоту їх надходження, а також стан мережевого з'єднання між джерелом та SIEM. Крім того, варто визначити, чи потрібно отримувати дані в режимі реального часу, чи буде достатньо періодичної обробки.

Загальна оцінка необхідних ресурсів завжди матиме похибку, оскільки кількість подій у мережі може суттєво змінюватися залежно від часу доби, кількості активних користувачів або позаштатних ситуацій. Тому рекомендується закладати певний резерв на випадок раптового зростання навантаження. У ситуаціях на кшталт встановлення шкідливого ПЗ або DDoS-атаки обсяги журналів можуть різко зрости, і до цього потрібно бути готовим заздалегідь.

Наступним важливим етапом у роботі з журналами пристроїв та додатків є їх доставка від джерел до системи моніторингу подій інформаційної безпеки. Хоча конкретні механізми збору логів можуть відрізнятися залежно від типу впровадженої системи, в основі цього процесу лежать два принципових підходи: у першому випадку пристрій-джерело самостійно надсилає логи до SIEM, так званий метод «push», а в другому збором даних займається сама SIEM система, яка під'єднується до джерела і самостійно отримує потрібну інформацію, метод «pull». Обидва методи є ефективними, однак мають свої особливості.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Метод «push» вирізняється простотою налаштування з боку SIEM, оскільки основна конфігурація виконується на самому пристрої-джерелі. Класичним прикладом є надсилання логів через syslog, коли достатньо вказати IP-адресу або DNS-ім'я сервера-приймача, і пристрій починає передавати дані автоматично. Такий підхід зручний, оскільки забезпечує передачу логів відразу після їх генерації. Проте він має і суттєві недоліки. Зокрема, при використанні протоколу UDP, який часто застосовується у syslog, виникає ризик втрати даних через ненадійність доставки, особливо у випадку перевантаження мережі. Крім того, якщо на стороні приймача не налаштований контроль доступу, зловмисник або неправильно сконфігуроване джерело можуть переповнити SIEM-систему надмірною або хибною інформацією, що ускладнить виявлення справжніх інцидентів.

Натомість метод «pull» передбачає, що SIEM самостійно встановлює з'єднання з джерелом логів і здійснює їх читання, наприклад, з текстових файлів або баз даних. На відміну від «push», тут передача даних не завжди здійснюється у режимі реального часу. Часто вона виконується із затримкою, відповідно до налаштованих інтервалів, які можуть становити як кілька секунд, так і кілька годин. Проте цей метод забезпечує більший контроль з боку SIEM, дозволяючи гнучко планувати завантаження системи та встановлювати графіки збору.

Більшість сучасних SIEM-рішень мають вбудовані механізми для інтеграції з поширеними системами і застосунками[12]. Наприклад, існують готові сценарії збору логів з бази даних Oracle, достатньо лише надати облікові дані для доступу, і SIEM виконає автентифікацію та збір у штатному режимі. Однак у випадках, коли йдеться про власноруч розроблені додатки, для яких не передбачено стандартних засобів інтеграції, адміністратору доведеться самостійно вирішити, як подавати дані до SIEM. Один з варіантів, перетворення логів у зрозумілий формат, наприклад, syslog, який потім може бути переданий до SIEM як текстовий потік. Інший, більш складний шлях полягає у створенні спеціального механізму збору, який зможе читати нестандартні логи, аналізувати їх структуру і транслювати у формат, який підтримується SIEM. Такий підхід дозволяє досягти максимальної точності та

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

повноти інформації, але вимагає глибокого розуміння внутрішньої структури як логів, так і можливостей обробки на стороні SIEM.

Реальні мережні середовища зазвичай включають пристрої та системи різних типів, що змушує адміністраторів комбінувати методи збору. Наприклад, Cisco ASA може надсилати логи через syslog, Snort IDS може записувати події у базу MySQL, а Windows Server робити запис до журналів подій. У таких умовах часто доводиться одночасно використовувати як «push», так і «pull» механізми, при цьому оптимізуючи конфігурацію з метою зменшення кількості інструментів збору. Важливо, щоб обрана структура дозволяла гнучко адаптуватися до нових джерел логів, забезпечуючи надійне та своєчасне надходження всієї необхідної інформації до SIEM.

Після успішного збору журналів подій з різних джерел наступним ключовим етапом є їх нормалізація. Хоча всі ці журнали вже надходять до централізованої системи обробки подій, зокрема до SIEM-рішення, у початковому вигляді вони зберігаються у власних, неструктурованих форматах. Відповідно, без додаткової обробки їх зміст є складним для інтерпретації та автоматичного аналізу. Саме тому виникає необхідність у приведенні всієї вхідної інформації до певної заздалегідь визначеної структури. Даний процес має назву нормалізація.

Нормалізацією[19] називають процес стандартизації форматів журналів подій, що надходять із різних джерел, з метою приведення їх до спільного уніфікованого формату. Основною метою цього процесу є забезпечення цілісного та однорідного представлення подій, що дозволяє SIEM-системі проводити повноцінну аналітику незалежно від типу пристрою, програмного забезпечення чи виробника, з якого походять ці події.

У реальній практиці різні пристрої або програмні рішення можуть записувати однакові за суттю події у кардинально різних форматах. Наприклад, факт успішної автентифікації користувача в операційній системі Windows може відображатися як подія з певним кодом та описом у журналі подій, тоді як аналогічна дія у маршрутизаторі Cisco буде фіксуватися у вигляді syslog-повідомлення зі своїм унікальним

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

синтаксисом. Без нормалізації SIEM не зможе коректно зіставити ці події між собою та визначати їх як одну й ту ж дію.

Результатом нормалізації є перетворення всіх подій у стандартизований набір полів, який є спільним для всіх джерел. Наприклад, незалежно від формату оригінального повідомлення, подія успішного входу користувача буде зведена до спільної структури з такими полями, як тип події, ім'я користувача, IP-адреса джерела, час події тощо. Завдяки цьому подальший аналіз, кореляція та побудова аналітичних запитів відбуваються у межах єдиного формату даних.

Крім спрощення процесу обробки даних, нормалізація значно підвищує ефективність побудови правил виявлення інцидентів інформаційної безпеки. За умов наявності уніфікованого формату даних створення універсальних правил кореляції, які одночасно охоплюють події з різних джерел, стає можливим і зручним. Це, своєю чергою, забезпечує більшу гнучкість у реагуванні на інциденти, зменшує кількість хибнопозитивних спрацьовувань та сприяє формуванню цілісної картини подій у мережевому середовищі.

Таким чином, нормалізація є критично важливим етапом функціонування SIEM-системи, що забезпечує узгодженість даних, спрощує їх обробку, покращує точність виявлення загроз і дозволяє ефективно реалізовувати механізми кореляційного аналізу в умовах багатоджерельного середовища.

Після того, як журнали подій з різних джерел були нормалізовані, настає черга правил та кореляцій[19]. Вони розширюють можливості нормалізації подій з різних джерел, дозволяючи генерувати сповіщення у SIEM на основі виявлення специфічних умов у цих журналах. Метод написання правил для SIEM може починатися досить просто, але швидко стати надзвичайно складним. Зазвичай правила пишуться з використанням булевої логіки для визначення відповідності певним умовам та аналізу збігів за шаблонами у полях даних.

Наприклад, якщо ви хочете отримувати сповіщення про кожен вхід до сервера з обліковими даними локального адміністратора, SIEM дозволяє створити єдине правило. Замість того, щоб мати декілька окремих правил для різних типів серверних операційних систем, які б шукали специфічні імена користувачів, SIEM

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

може використовувати свою внутрішню логіку для спрацьовування правила на основі кількох змінних. Це значно спрощує управління правилами та підвищує їхню універсальність.

Основна функція кореляцій полягає в зіставленні кількох стандартних подій з різних джерел у єдину, корельовану подію. Кореляція подій здійснюється для спрощення процедур реагування на інциденти у вашому середовищі. Вона представляє оператору одну подію, яка була викликана низкою окремих подій, що надходять з різних пристроїв-джерел.

Таким чином, замість того, щоб переглядати журнали, намагаючись знайти окремі події та їх взаємозв'язки, можна використовувати вбудовану логіку SIEM для об'єднання мережевих подій у корельовану подію. Для цього потрібно написати правило, що спрацьовує на основі певних подій. Логіка для такого корельованого правила буде залежати від конкретної SIEM-системи, що використовується.

Після отримання даних про події постає питання що робити з цим масивом інформації. І тут здійснюється перехід на етап збереження логів[11].

Організація ефективного та надійного зберігання великого обсягу журналів подій, що надходять з різних джерел є одним із ключових завдань систем управління подіями інформаційної безпеки. Збереження логів у структурованому вигляді є необхідною умовою для забезпечення довготривалого утримання даних, виконання запитів та аналітики інцидентів безпеки. Вибір методу зберігання безпосередньо впливає на продуктивність системи, швидкість обробки запитів, можливості масштабування та зручність доступу до інформації.

Одним із найпоширеніших способів зберігання є використання бази даних. У цьому випадку журнали подій зберігаються у вигляді записів у таблицях, організованих відповідно до структури, яку підтримує конкретне SIEM-рішення. Такий підхід дозволяє здійснювати ефективний пошук, агрегацію, сортування та аналіз даних за допомогою стандартних механізмів роботи з базами даних. Крім того, доступ до журналів через мову запитів дозволяє інтегрувати SIEM з іншими системами або створювати власні інструменти для аналізу. У разі, якщо SIEM-система реалізована як апаратно-програмний комплекс, адміністрування бази даних зазвичай не

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

вимагається, оскільки ці процеси приховані від користувача. Натомість у випадку самостійного розгортання системи необхідно забезпечити кваліфіковане адміністрування бази даних, що може ускладнити експлуатацію без відповідного досвіду.

Альтернативним підходом є зберігання журналів у вигляді простих текстових файлів. Цей метод передбачає збереження логів у звичайному текстовому форматі з розділенням полів за допомогою ком або табуляцій. Такий формат є простим у реалізації, зручним для ручного перегляду та доступним для обробки за допомогою зовнішніх програмних засобів. Проте продуктивність цього методу знижується при роботі з великими обсягами даних, а обмежені можливості масштабування унеможливають його ефективне використання у великих інфраструктурах. Незважаючи на це, у невеликих системах або в середовищах з низькою інтенсивністю подій зберігання у текстових файлах може залишатися доцільним.

Ще одним способом зберігання є використання бінарних файлів, які зазвичай реалізовані у вигляді власного, закритого формату, що використовується конкретно SIEM-системою. Такі файли не призначені для ручного перегляду або обробки сторонніми засобами, однак забезпечують високу швидкість запису й читання, а також оптимальне використання простору на носії. Подібна реалізація забезпечує максимальну продуктивність, але створює залежність від конкретного програмного забезпечення SIEM. Дані, збережені у бінарному форматі, можуть бути недоступними без використання рідного інструментарію, що ускладнює аналіз подій або їх міграцію до іншої системи.

Таким чином, вибір формату зберігання логів у SIEM-системі залежить від особливостей конкретного середовища, обсягу даних, вимог до швидкодії, а також потреб у доступності інформації для зовнішніх інструментів. Найбільш універсальним підходом залишається використання бази даних, однак за певних умов можуть застосовуватись і альтернативні методи, зокрема текстові або бінарні формати, кожен з яких має свої переваги й обмеження.

Завершальним етапом побудови SIEM-системи[12] є організація ефективної взаємодії з даними, що зберігаються в системі. Після збору журналів з різноманіт-

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

них джерел, їх обробки, аналізу та збереження, виникає потреба у створенні зручного та функціонального інтерфейсу для подальшого використання цієї інформації. Без належного механізму доступу до логів та подій навіть найточніший аналіз залишиться неефективним, адже результати не будуть використані для прийняття рішень або реагування на інциденти.

Сучасні SIEM-рішення зазвичай надають користувачу інтерфейсну консоль, яка може бути реалізована як веб-застосунок або як настільна програма, встановлена на окремій робочій станції. Ця консоль виконує функції не лише відображення даних, а й забезпечує управління всіма компонентами системи SIEM. Вона є основним інструментом аналітика чи адміністратора для моніторингу, аналізу, створення правил кореляції, візуалізації даних і формування звітів.

Завдяки уніфікованому інтерфейсу, SIEM надає централізований огляд стану безпеки всієї інформаційної інфраструктури. На відміну від традиційного підходу, коли фахівець повинен переглядати журнали окремо на кожному пристрої, SIEM дозволяє працювати з подіями у стандартизованому форматі. Це стало можливим завдяки процесу нормалізації даних, в результаті якого логи, отримані з різних джерел, набувають єдиної структури та спільного формату представлення. Як наслідок, значно спрощується аналіз і прискорюється виявлення аномальних або потенційно небезпечних подій.

Консоль управління дозволяє не лише переглядати вже наявні події, але й створювати спеціалізовані правила та алгоритми для виявлення інцидентів, що відповідають заданим умовам. Це можуть бути складні запити або шаблони, які використовують внутрішню мову запитів системи для вилучення важливої інформації зі збережених даних. Таким чином, інтерфейс SIEM фактично виконує функцію доступу до великої бази даних подій безпеки, забезпечуючи як оперативну роботу з поточними подіями, так і можливість аналізу історичних даних.

На рисунку 1.1.2 наведені функції SIEM-системи, які виконуються вище згаданими складовими системи.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

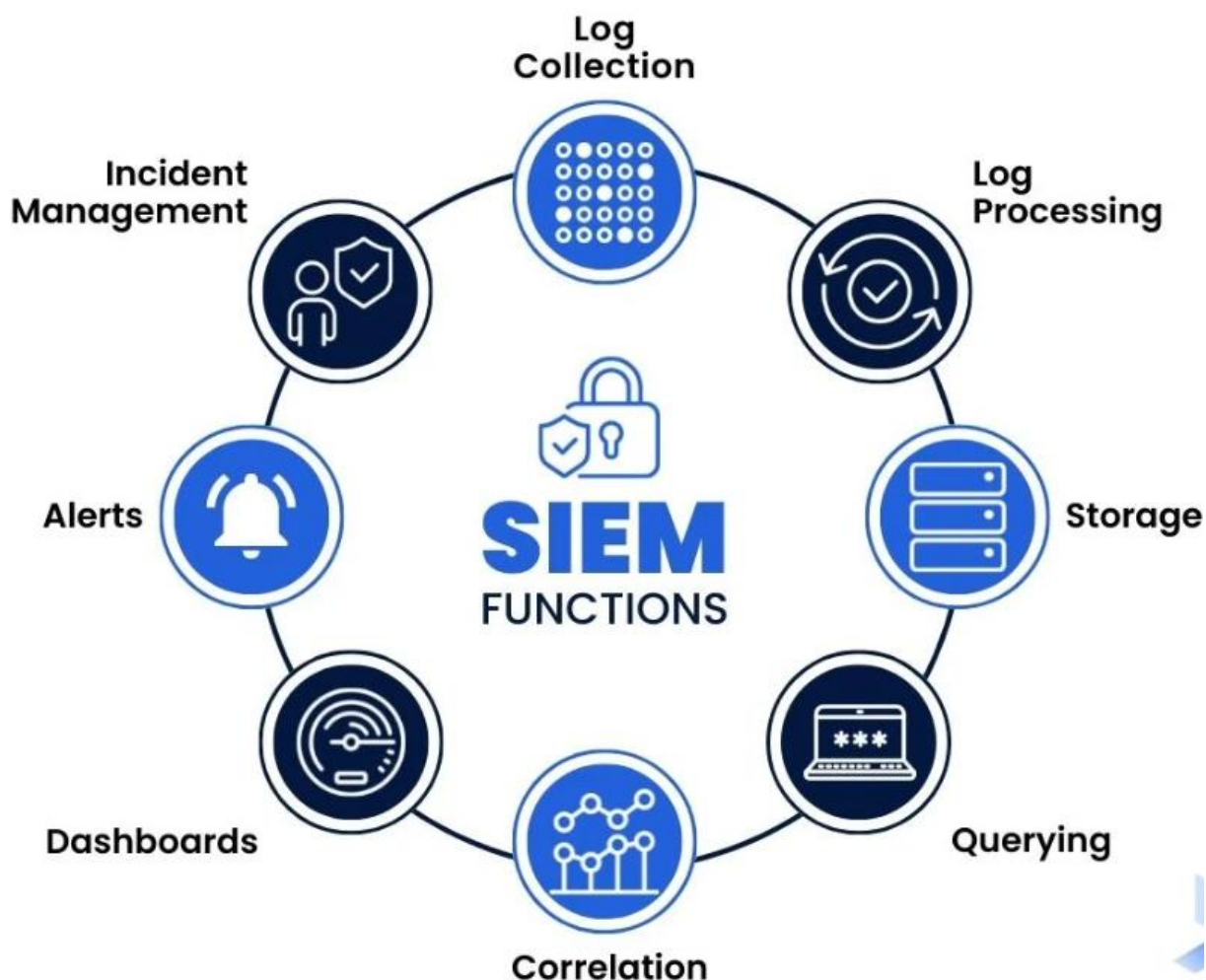


Рисунок 1.1.2 – Функції SIEM

Кожна SIEM-система складається з функціональних компонентів, що можуть функціонувати незалежно один від одного, проте лише їх узгоджена взаємодія дозволяє досягти високої ефективності системи в цілому. Важливо розуміти призначення кожного модуля, його місце в архітектурі SIEM, а також способи налагодження їх взаємодії. Такий підхід дозволяє не лише ефективно експлуатувати систему, а й своєчасно виявляти та усувати проблеми, що можуть виникати у процесі її роботи.

Таким чином, моніторинг у SIEM є не просто інструментом перегляду подій, а ключовим елементом управління безпекою інформаційної системи. Завдяки комплексному підходу, що включає збір, нормалізацію, зберігання та інтерпретацію даних, SIEM стає потужним засобом забезпечення інформаційної безпеки в організації.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2 Що таке The Elastic Stack і які його функціональні можливості

ELK Stack[4] це колекція інструментів які застосовують для збору, аналізу, та візуалізації даних. Він був розроблений компанією Elastic. Ці інструменти часто використовуються для моніторингу мереж, аналізу журналів пошуку необхідної інформації в великих об'ємах даних.

Назва ELK є об'єднанням перших літер трьох головних інструментів: Elasticsearch, Logstash та Kibana. Elasticsearch є пошуково-аналітичною системою, яка забезпечує зберігання даних у вигляді JSON файлів. Він відповідає за індексування та швидкий пошук по структурованим і неструктурованим даним.

Elasticsearch[3] підтримує реплікацію та балансування навантаження, що робить його стійким до відмов.

Logstash[3] використовується для збору, обробки та трансформації даних. Даний інструмент підтримує різні джерела даних, такі як файли журналів, бази даних або API, та дозволяє фільтрувати, обробляти і пересилати дані в Elasticsearch або інші системи. Він є гнучким у налаштуванні, що робить його ідеальним для різноманітних сценаріїв обробки даних.

Kibana[3] надає можливість візуалізації даних і створення інформаційних панелей. Завдяки йому можна створювати графіки, діаграми, карти та інші візуалізації для аналізу даних. Kibana також підтримує інтерактивні функції для пошуку і аналізу, що дозволяє користувачам глибше досліджувати свої дані.

Історія ELK почалася з розробки Elasticsearch, який був випущений 2010 році Шай Баном. Першою версією стала пошукова платформа з відкритим кодом, що працювала на базі Lucene. Elasticsearch швидко завоював популярність завдяки своїй продуктивності, масштабованості та простоті у використанні. Компанія Elastic, заснована у 2012 році, почала активно розвивати продукт і випускати нові версії, додаючи підтримку агрегатів, реплікацію та інтеграцію з іншими інструментами.

Logstash був створений як окремий проєкт Джорданом Сіссерманом у 2009 році. Спочатку він був призначений для збору й обробки логів, але згодом еволюціонував у потужний інструмент для роботи з даними з різних джерел. У 2013 році

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Logstash приєднався до екосистеми Elastic, що дозволило йому інтегруватися з Elasticsearch та іншими компонентами.

Kibana з'явилася у 2013 році як інструмент для візуалізації даних, що зберігаються в Elasticsearch. Вона забезпечила зручний інтерфейс для створення графіків і панелей моніторингу. У 2015 році Elastic включила Kibana у свій офіційний стек, зробивши її невід'ємною частиною ELK.

Ключовими етапами розвитку ELK стали випуски нових версій із значними оновленнями. Elasticsearch отримав підтримку security features, таких як керування доступом і шифрування, а також потужні механізми машинного навчання для виявлення аномалій. Logstash додав підтримку безлічі плагінів, що розширили його можливості обробки та передачі даних. Kibana отримала інтеграцію з Elastic Stack Security, Canvas для створення кастомних візуалізацій та Lens для спрощеного аналізу даних.

На сьогодні ELK[4] є одним із найпопулярніших стеків для роботи з великими даними, а компанія Elastic продовжує інвестувати в його розвиток, додаючи нові функції та інтеграції. ELK Stack має широкий спектр можливостей. Він дозволяє збирати та аналізувати журнали серверів, додатків та мережевих пристроїв, що допомагає ідентифікувати проблеми та несправності в системах. Його функціонал моніторингу інфраструктури дає змогу створювати метрики продуктивності серверів, баз даних і додатків, а також виявляти аномалії та прогнозувати можливі збої. Завдяки можливості створення інтерактивних панелей, ELK забезпечує зручну візуалізацію ключових метрик, аналіз трендів і кореляцій між різними параметрами.

Він також дозволяє здійснювати швидкий повнотекстовий пошук по великих обсягах даних із використанням складних запитів, фільтрів і агрегацій. Гнучкість інтеграції робить його сумісним з іншими інструментами, такими як Beats, Fluentd і Prometheus, а також дає змогу налаштовувати пайплайни для специфічних типів даних.

Архітектура ELK забезпечує масштабованість через розподіл даних між вузлами, що дозволяє горизонтально масштабувати систему. Elasticsearch надає

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

реплікацію даних для запобігання втратам у разі збоїв вузлів, а потужні механізми індексування забезпечують високу продуктивність і швидкий доступ до даних.

ELK Stack застосовують в різних галузях. У фінансовій сфері його використовують для аналізу транзакцій і виявлення шахрайства. У розробці програмного забезпечення він допомагає моніторити продуктивність додатків. У сфері кібербезпеки стек сприяє виявленню аномалій і аналізу інцидентів, а в електронній комерції аналізу поведінки користувачів і оптимізації бізнеспроцесів.

Переваги Elastic Stack:

- Відкритий код і гнучка архітектура для налаштування під будь-які потреби.
- Масштабованість. Підтримка від стартапів до великих підприємств.
- Миттєвий аналіз даних завдяки Elasticsearch.
- Активна спільнота, велика кількість плагінів та інтеграцій.
- Різні варіанти розгортання: локально, в хмарі або гібридно.
- Базові функції доступні безкоштовно.

Недоліки Elastic Stack:

- Вимагає часу на освоєння KQL, EQL та архітектури.
- Комерційні функції та хмарне розгортання можуть бути дорогими.
- Високі потреби у CPU, RAM і диску.
- Деякі SIEM-можливості потребують додаткової інтеграції.

Elastic Stack[2] є надзвичайно потужним і гнучким рішенням для аналізу даних, що робить його популярним вибором для побудови SIEM-систем. Elastic Security є агресивним гравцем на ринку SIEM/XDR, пропонуючи сучасний, хмарно-орієнтований підхід до безпеки, який інтегрується з можливостями моніторингу та спостережуваності.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3 Огляд наявних альтернативних SIEM рішень

ІТ-системи, бізнес-процеси та операційна діяльність сучасних організацій генерують значні обсяги інформації. Для прийняття ефективних рішень, забезпечення належного рівня безпеки та підвищення продуктивності важливо аналізувати та контролювати ці дані.

Серед відомих SIEM рішень можна виділити наступні:

1. ManageEngine Log360
2. Logmanager
3. SolarWinds Security Event Manager
4. Microsoft Sentinel
5. LogRhythm SIEM
6. Datadog Cloud SIEM
7. ArcSight Enterprise Security Manager
8. Splunk Enterprise
9. IBM Security QRadar SIEM
10. FortiSIEM

В таблиці 1.3.1. Наведено короткі характеристики кожного з цих рішень.

Таблиця 1.3.1

Коротка характеристика SIEM рішень

№	Назва	Платформа розгортання	Ліцензія	Джерела даних	Підтримка аналітики загроз	Спрямування
1	ManageEngine Log360	Локально /Хмара	Платна	Syslog сервери, Мережеві пристрої, інші.	Вбудована аналітика загроз	Середній бізнес

Продовження таблиці 1.3.1

2	Logmanager	Локально	Платна	ОС, Мере- жеві при- строї, Системи безпеки	Обмежена	Малі/се- редні компанії
3	SolarWinds Security Event Manager	Локально	Платна	Мере- жеві при- строї, ОС	Вбудована кореляція подій	Великі компанії / хмарні системи
4	Microsoft Sentinel	Хмара(Azure)	Платна	Microsoft про- дукти	Вбудована аналітика загроз, за- снована на експертизі Microsoft, з підтримкою машинного навчання	Середній та вели- кий біз- нес
5	LogRhythm SIEM	Локально	Платна	Мере- жеві при- строї, Сервери та опера- ційні си- стеми	Вбудована кореляція подій	Середній та вели- кий біз- нес

6	Datadog Cloud SIEM	Хмара	Платна	Microsoft Azure, Пристрої безпеки	Вбудована система аналітики загроз	DevOps/ Cloud Security
7	ArcSight Enterprise Security Manager	Локально	Платна	Хмарні сервіси, ОС, Ме-режеві пристрої	Кореляція подій	Для великих орга-нізацій / підприємств
8	Splunk Enterprise	Локально /Хмара	Платна	Будь-які структу-ровані дані	Наявні сис-теми штуч-ного інтеле-кту та ма-шинного навчання	Середній та вели-кий біз-нес
9	IBM Security QRadar SIEM	Локально /Хмара	Платна	Широ-кий спектр	Кореляція подій	Корпора-ції, дер-жавні ус-танови
10	FortiSIEM	Локально /Хмара	Платна	Мережні дані, пристрої Fortinet	Автомати-зований аналіз	Користу-вачі Fortinet
11	Elastic Stack	Локально	Безко-што-вна/ Платна	Широ-кий спектр	Вбудована кореляція	Невеликі компанії

ManageEngine Log360 – це комплексне SIEM рішення, призначене для вирішення широкого спектру безпекових проблем. Воно об'єднує можливості групи інструментів які входять до ManageEngine, задля забезпечення повної видимості мережі та її комплексного захисту.

Основні можливості та функції ManageEngine Log360.

- Управління журналами логування. Збирає, агрегує та зберігає журнали подій з різних джерел, включаючи мережеві пристрої, сервери, файлові сервери, бази даних, веб-сервери, Microsoft 365, Exchange сервери, Active Directory та хмарні платформи. Це дозволяє отримати централізоване сховище для всіх даних журналів.
- Виявлення та аналіз загроз. Виявляє, розслідує та нейтралізує загрози безпеки за допомогою передового аналізу журналів. Може здійснювати аналіз поведінки користувачів та об'єктів використовуючи машинне навчання для виявлення аномалій у їх поведінці, що дозволяє ідентифікувати приховані загрози, такі як витік даних або компрометація облікових записів.
- Аналіз загроз та розвідка. Використовує оновлювані канали загроз для блокування шкідливих IP-адрес, доменів та URL-адрес.
- Пошук загроз. Дозволяє виявляти шкідливих акторів та потенційні атаки, які могли пройти повз початкові засоби захисту.
- Моніторинг даркнету. Виявляє приховані загрози та конфіденційні дані, що були скомпрометовані в даркнеті, надаючи ранні попередження про витоки облікових даних.
- Аудит безпеки. Аудит Active Directory, моніторинг усіх змін в Active Directory, включаючи входи, блокування, зміни користувачів та груп, зміни дозволів, доступ до файлів тощо. Аудит хмарних середовищ відстеження та аналіз подій у публічних хмарах таких як AWS та Azure, надаючи звіти про активність користувачів та зміни в мережевих групах безпеки, віртуальних мережах, DNS-зонах, віртуальних машинах та інших ресурсах.
- Звіти про відповідність стандартам. Надає великий набір попередньо налаштованих звітів, які допомагають відповідати нормативним вимогам, таким як

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

PCI DSS, GDPR, FISMA, HIPAA, SOX та GLBA. Можливість створення власних звітів.

Також дана система має інтегровані можливості запобігання витоку даних та безпеки хмарних додатків забезпечують ефективний захист конфіденційної інформації та контроль доступу до хмарних сервісів. Система управління інцидентами дозволяє своєчасно виявляти, розслідувати, реагувати та нейтралізувати інциденти безпеки, доповнюючись функціями сповіщення в реальному часі через електронну пошту, SMS або інші канали. Користувачі можуть створювати власні правила кореляції для виявлення складних загроз, а всі ці можливості доступні через єдиний, інтуїтивно зрозумілий інтерфейс, що значно спрощує управління IT-безпекою.

Узагальнені переваги ManageEngine Log360:

- **Комплексність.** Об'єднує різноманітні інструменти безпеки в одне рішення, що дозволяє отримати повну картину безпеки мережі.
- **Повна видимість.** Забезпечує глибоку видимість подій у мережі, серверах, додатках, Active Directory та хмарних середовищах.
- **Автоматизація.** Автоматизує збір журналів, аналіз даних та генерацію звітів, заощаджуючи час та ресурси.
- **Виявлення загроз у реальному часі.** Швидко виявляє вторгнення та аномалії, попереджаючи про них у реальному часі.
- **Відповідність стандартам.** Допомагає забезпечити відповідність різним нормативним вимогам за допомогою готових звітів та аудиту.
- **Масштабованість.** Підходить для бізнесу будь-якого розміру, від малого до великого підприємства.
- **Простота використання.** Незважаючи на складність функціоналу, продукт має інтуїтивно зрозумілий інтерфейс.

Хоча ManageEngine Log360 є потужним і багатофункціональним SIEM-рішенням, воно має деякі недоліки, які можуть бути важливими для потенційних користувачів. Ось основні з них:

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

- Необхідність потужного обладнання. Для безперебійної та швидкої роботи Log360 потрібне потужне обладнання з достатньою кількістю оперативної пам'яті та процесорної потужності.
- Високі вимоги до сховища. Log360 збирає великі обсяги журналів, що вимагає значних обсягів сховища для зберігання даних.
- Проблеми з продуктивністю. За відгуками користувачів може система може повільно працювати навіть на системах з достатнім обсягом пам'яті та потужним процесором.
- Ціна. Хоча ManageEngine зазвичай вважається більш доступним у порівнянні з деякими конкурентами, для деяких компаній ціна Log360 може бути високою, особливо залежно від необхідного функціоналу та обсягів даних.

Важливо зазначити, що багато з цих недоліків є типовими для комплексних SIEM-рішень.

Logmanager – це програмне рішення, яке використовується для централізованого збору, зберігання, аналізу та управління логами з різних джерел у мережевій інфраструктурі. Воно може бути частиною SIEM-рішень або існувати як окремий інструмент для забезпечення прозорості, відповідності стандартам безпеки та виявлення інцидентів.

Основні функції Logmanager:

- Централізований збір логів. Збирає події з різних джерел: серверів, мережевого обладнання, систем безпеки, додатків, баз даних, операційних систем тощо.
- Нормалізація та уніфікація логів. Приводить логи з різних форматів до єдиного вигляду для полегшеного аналізу.
- Зберігання даних. Забезпечує довгострокове зберігання логів з можливістю пошуку, фільтрації, експорту. Часто передбачено шифрування, контроль доступу та управління політиками зберігання.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

- Аналіз і кореляція подій. Виявляє аномальні або небезпечні події шляхом аналізу взаємозв'язків між подіями з різних джерел. У SIEM-рішеннях цей компонент часто інтегровано з інструментами для виявлення загроз.
- Створення звітів і аудит. Формує звіти для внутрішнього контролю або для проходження аудитів.
- Сповіщення в реальному часі. Надсилає повідомлення про критичні події або підозрілу активність за допомогою email, SMS або інших каналів.

Як і будь яка інша система Logmanager має свої переваги та недоліки:

Переваги Logmanager:

- Підвищення рівня безпеки через моніторинг подій у режимі реального часу.
- Спрощення аналізу інцидентів та виявлення загроз.
- Відповідність вимогам регуляторів.
- Зменшення часу на пошук та усунення проблем.

Недоліки:

- Може вимагати значних обчислювальних ресурсів особливо при великому обсязі логів.
- Не всі рішення підтримують автоматичну кореляцію подій.
- Вартість комерційних продуктів може бути високою.
- Потрібне належне налаштування для ефективного використання.

SolarWinds Security Event Manager або SEM – це комерційне SIEM-рішення, розроблене для централізованого моніторингу подій безпеки, управління логами, виявлення загроз та автоматизації реагування на інциденти. Його основна мета допомогти організаціям швидко виявляти підозрілу активність, контроль відповідності нормативам та зменшувати час реагування на інциденти.

SolarWinds SEM має наступні можливості:

- Централізоване збирання та нормалізація логів. SEM збирає журнали подій з різних джерел: серверів, мережевого обладнання, систем безпеки, додатків

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

і баз даних. Всі логи автоматично нормалізуються для полегшення подальшого аналізу.

- Реальний час і кореляція подій. Система постійно аналізує події у реальному часі та застосовує вбудовані правила кореляції для виявлення потенційних інцидентів безпеки.
- Автоматизоване реагування на інциденти. SEM дозволяє налаштувати автоматичні дії у відповідь на певні події або загрози, що пришвидшує нейтралізацію інцидентів.
- Готові політики комплаєнсу. Продукт має шаблони та звіти для відповідності таким стандартам, як HIPAA, PCI DSS, SOX, GDPR, NIST тощо. Це спрощує аудит і внутрішній контроль.
- Гнучка аналітика та візуалізація. SEM має вбудовані панелі моніторингу (дашборди), інструменти для фільтрації та пошуку подій, що дає змогу швидко аналізувати ситуації та проводити розслідування.
- USB Device Monitoring. Окрема функція, яка дозволяє відстежувати та контролювати використання USB-накопичувачів у мережі, що є зручним для запобігання витоку даних.

Перевагами SolarWinds Security Event Manager можна вважати наступні:

- Інтуїтивний інтерфейс із простими в налаштуванні правилами та дашбордами.
- Високий рівень автоматизації — зниження навантаження на команду безпеки.
- Потужна система виявлення інцидентів у реальному часі.
- Велика кількість шаблонів звітів та політик відповідності.
- Вбудовані механізми контролю доступу до зовнішніх пристроїв

Недоліки та обмеження:

- Ціна. SEM належить до комерційних рішень з доволі високою вартістю ліцензії.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

- Вимоги до ресурсів. Може вимагати продуктивного обладнання для обробки великого потоку логів.
- Обмежені можливості масштабування у порівнянні з рішеннями рівня enterprise-класу.
- Обмежений функціонал кастомізації.

SolarWinds SEM добре підходить для середніх організацій та компаній, які потребують швидкого впровадження SIEM-рішення з широкими можливостями без складної конфігурації. Особливо корисний для ІТ-відділів, що прагнуть покрити вимоги аудиту та забезпечити базовий захист від внутрішніх і зовнішніх загроз.

Microsoft Sentinel – це хмарна платформа класу SIEM та SOAR, яка допомагає організаціям збирати, виявляти, розслідувати та реагувати на загрози безпеки в масштабах підприємства. Він розроблений для забезпечення повного огляду безпеки в гібридних та мультихмарних середовищах, використовуючи можливості штучного інтелекту та машинного навчання.

Microsoft Sentinel може збирати журнали подій і телеметрію з великої кількості джерел, серед яких сервіси Microsoft, хмарні платформи AWS і GCP, локальні середовища такі, як Windows, Linux-сервери, мережеві пристрої, антивіруси, IDS/IPS, бази даних, а також сторонні ІТ-рішення. Завдяки хмарній архітектурі, Sentinel забезпечує масштабовану обробку великих обсягів даних без потреби в локальній інфраструктурі.

Для виявлення загроз Sentinel використовує потужну аналітику: система включає набір готових правил на основі експертизи Microsoft у сфері безпеки, а також можливість створювати власні запити за допомогою мови KQL. Використання машинного навчання та UEBA дозволяє виявляти аномалії в поведінці користувачів і об'єктів, знижуючи кількість помилкових спрацювань. Дані збагачуються завдяки інтеграції з каналами розвідки загроз, а співставлення із MITRE ATT&CK допомагає краще розуміти природу атак.

Для розслідування інцидентів Sentinel надає зручний візуальний граф, що відображає взаємозв'язки між сутностями, подіями та сповіщеннями, допомагаючи

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

аналітикам швидко зрозуміти масштаб інциденту. Функція загрозоорієнтованого пошуку дозволяє проводити поглиблений аналіз за межами стандартних сценаріїв. Реагування на загрози автоматизується завдяки інтеграції з Azure Logic Apps, що дає змогу створювати плейбуки для автоматичних дій. Крім того, автоматичні правила можуть закривати інциденти з низьким пріоритетом або передавати їх відповідальним спеціалістам.

Загалом, Microsoft Sentinel є провідним хмарним SIEM-рішенням, яке активно розвивається і пропонує потужні можливості для захисту сучасних, розподілених IT-інфраструктур.

LogRhythm SIEM є однією з провідних платформ у галузі кібербезпеки, призначеною для централізованого збору, аналізу та управління подіями безпеки та інформацією з усієї IT-інфраструктури організації. Вона допомагає організаціям виявляти, розслідувати та реагувати на кіберзагрози, а також забезпечувати відповідність нормативним вимогам.

Після нещодавнього злиття компаній LogRhythm та Exabeam об'єднана організація продовжує функціонувати під брендом Exabeam, однак рішення LogRhythm SIEM залишається ключовим елементом портфеля. Це об'єднання має на меті поєднати переваги обох платформ: зокрема, потужний механізм збору даних LogRhythm і передову поведінкову аналітику Exabeam на основі ШІ.

LogRhythm SIEM забезпечує повноцінний цикл моніторингу, виявлення та реагування на кіберзагрози. Система збирає та нормалізує журнальні записи, дані про мережевий трафік, кінцеві точки та інші контекстуальні події з понад 950 джерел, включаючи сервери, мережеву інфраструктуру, фаєрволи, хмарні сервіси та сторонні продукти. Зібрані дані приводяться до уніфікованого формату й збагачуються додатковими атрибутами такими як, геолокація, інформація про пристрої, користувачів, що робить їх зручними для глибокого аналізу.

Система реалізує багаторівневий підхід до виявлення загроз. Кореляційний механізм із понад тисячею готових правил дозволяє виявляти шаблони підозрілої активності, а вбудована аналітика поведінки користувачів і об'єктів на основі машинного навчання допомагає виявляти відхилення від нормальної поведінки, що

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

може свідчити про інсайдерські загрози чи компрометацію. Додатково LogRhythm використовує мережевий трафік для виявлення аномалій і інтегрується з каналами розвідки загроз для виявлення відомих індикаторів компрометації. Уся аналітика підсилюється пріоритезацією сповіщень за рівнем ризику, що дозволяє зосередитися на найнебезпечніших загрозах.

Для ефективного реагування LogRhythm має розвинені можливості автоматизації завдяки інструментам SOAR. Система підтримує автоматичні дії у відповідь, контекстуалізацію інцидентів, а також візуалізацію зв'язків між подіями у вигляді інтерактивних діаграм. Можливості проактивного пошуку загроз (Threat Hunting) дозволяють аналітикам виявляти приховані загрози без прив'язки до заздалегідь визначених правил.

Крім того, LogRhythm виконує функції централізованого управління журналами з довгостроковим зберіганням і швидким пошуком. Це важливо як для розслідування інцидентів, так і для аудиту. Платформа підтримує відповідність таким стандартам, як PCI DSS, HIPAA, GDPR, SOX, NIST, забезпечуючи готові звіти для аудитів і регуляторів. У комплексі LogRhythm SIEM виступає як гнучке, масштабоване рішення для організацій, які шукають баланс між надійним збором даних і сучасною аналітикою загроз.

Переваги LogRhythm SIEM:

- Комплексність. Об'єднує SIEM, UEBA, NTA та SOAR в єдину платформу.
- Якість збору даних. Високоточне збирання, нормалізація та інтерпретація з понад 950 джерел.
- Ефективне виявлення загроз. Поєднання кореляцій, ML та Threat Intelligence.
- Автоматизація реагування. Широкі можливості SOAR для зменшення ручної роботи.
- Підтримка комплаєнсу. Готові звіти для PCI DSS, GDPR, NIST та інших стандартів.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

- Зменшення MTTD/MTTR. Прискорення виявлення й реагування на інциденти.

Недоліки:

- Високі вимоги до ресурсів: Особливо для локальних інсталяцій.
- Крива навчання: Повне використання функцій потребує досвіду.
- Інтеграційні складності: Деякі специфічні джерела можуть потребувати ручного налаштування.
- Ціна: Значна інвестиція для організацій середнього бізнесу.

LogRhythm SIEM – це потужне, надійне рішення, особливо для тих, хто шукає глибоку інтеграцію, автоматизацію й гнучкість в операціях безпеки.

Datadog Cloud SIEM – це компонент комплексної платформи Datadog, яка спеціалізується на забезпеченні безпеки хмарних додатків та інфраструктури. На відміну від традиційних SIEM-систем, які часто є локальними та потребують значних ресурсів для підтримки, Datadog Cloud SIEM розроблений для хмарних середовищ, що дозволяє швидко виявляти загрози в реальному часі.

Datadog Cloud SIEM забезпечує централізований збір, нормалізацію та аналіз безпекових подій, інтегруючись з іншими продуктами Datadog, такими як моніторинг інфраструктури, APM та лог-менеджмент. Це дає змогу користувачам отримувати уніфіковану панель керування для повної видимості та контролю над подіями безпеки.

Платформа підтримує понад 600 вбудованих інтеграцій, що дозволяє збирати журнали та телеметрію з широкого спектру джерел: хмарних, сервісів Microsoft, мережевих пристроїв, серверів, контейнерів, додатків, баз даних та інших інструментів безпеки. Зібрані логи автоматично нормалізуються та збагачуються додатковими метаданими, наприклад, інформацією про інфраструктуру, користувачів чи геолокацію, що суттєво полегшує аналіз.

Для виявлення загроз у реальному часі Datadog Cloud SIEM використовує попередньо налаштовані правила, які охоплюють типові шаблони атак. При цьому користувачі можуть створювати власні правила на основі запитів, побудованих за

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

мовою Datadog. Аналіз загроз доповнюється даними з інших модулів – метрик, траєкторій, інфраструктурного моніторингу, що дозволяє отримати повну картину інциденту. Хоч Datadog не є класичним UEBA-рішенням, його можливості дозволяють виявляти поведінкові аномалії, що можуть вказувати на інсайдерську активність чи компрометацію акаунтів. Інтеграція з фреймворком MITRE ATT&CK дає змогу зіставляти сигнали безпеки з тактиками та техніками реальних злоумисників.

При виявленні загрози система генерує сигнал безпеки, що містить усю релевантну інформацію для розслідування. Аналітики можуть досліджувати події, переглядаючи повний контекст – логи, інфраструктурні залежності, часові зв'язки. Автоматизація реагування реалізується через Workflows, які дозволяють запускати сценарії реагування – від надсилання сповіщень до ізоляції хостів чи блокування IP-адрес. Інтеграція з Jira, ServiceNow та іншими системами управління інцидентами підтримує оперативну взаємодію команд. Вбудовані інструменти для управління кейсами допомагають координувати розслідування та фіксувати прогрес.

Datadog Cloud SIEM також підтримує відповідність регуляторним вимогам, таким як PCI DSS, HIPAA та GDPR, завдяки надійному збору та зберіганню логів, а також можливості створення аудиторських звітів.

Переваги Datadog Cloud SIEM:

- Хмарна архітектура – не потребує власного обладнання, легко масштабується.
- Інтеграція з екосистемою Datadog – працює в єдиному інтерфейсі з іншими модулями.
- Швидке впровадження – завдяки великій кількості готових інтеграцій.
- Контекст та видимість – пов'язує події безпеки з метриками,логами й трасами додатків.
- Гнучке ціноутворення – модель “pay-as-you-go”, оплата за фактичне використання.
- Автоматизація – пришвидшує реагування, знижує потребу в ручних діях.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Недоліки Datadog Cloud SIEM:

- Ціна – висока вартість при великому обсязі даних, складність у прогнозуванні витрат.
- Фокус на хмарі – краще підходить для хмарних/гібридних середовищ, ніж для локальних.
- Крива навчання – потреба у знаннях мови запитів (подібної до KQL) для складного аналізу.
- Обмежене позиціонування – поступається традиційним SIEM у forensic-аналізі чи складному UEBA.

Datadog Cloud SIEM є чудовим вибором для організацій, які вже використовують Datadog для моніторингу або активно розгортають свою інфраструктуру в хмарі. Він пропонує сучасний підхід до SIEM, поєднуючи моніторинг безпеки з повною спостережуваністю, що дозволяє командам швидше виявляти, розслідувати та реагувати на загрози в динамічних хмарних середовищах.

ArcSight Enterprise Security Manager або ESM – це потужна, масштабована та комплексна платформа класу SIEM, розроблена для виявлення, аналізу, розслідування та реагування на кіберзагрози в реальному часі. Історично ArcSight була одним з першопрохідців у галузі SIEM, і хоча вона пройшла через кілька змін власності, її основні принципи та можливості залишаються ключовими.

ArcSight ESM орієнтована на великі організації з високими вимогами до інформаційної безпеки та складною IT-інфраструктурою. Вона забезпечує глибокий контроль, потужну аналітику та здатність до масштабованого оброблення подій безпеки в режимі реального часу.

ArcSight збирає журнальні дані з практично будь-яких джерел, включаючи мережеві пристрої, сервери, кінцеві точки, хмарні сервіси та програми. Застосування SmartConnectors дозволяє нормалізувати ці дані до уніфікованого формату CEF, що забезпечує ефективний та стандартизований аналіз. Крім того, події збагачуються контекстуальною інформацією, що покращує точність виявлення загроз.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Ключовим елементом ArcSight є потужний механізм кореляції подій, здатний обробляти понад 100 тисяч подій на секунду. Система підтримує попередньо визначені правила кореляції та дозволяє створювати гнучкі власні правила. Модуль динамічного оцінювання ризиків допомагає фокусувати увагу аналітиків на найважливіших загрозах.

Інтеграція з UEBA-модулем забезпечує виявлення аномалій у поведінці користувачів за допомогою машинного навчання, а джерела threat intelligence дозволяють оперативно ідентифікувати відомі індикатори компрометації. Система також підтримує співставлення з MITRE ATT&CK для кращого розуміння тактик зломисників.

Для реагування на інциденти ArcSight надає вбудовану систему керування інцидентами та інтеграцію з SOAR-рішеннями, що дозволяє автоматизувати типові дії: ізоляцію хостів, блокування адрес, створення тікетів або надсилання сповіщень. Інструменти для активного пошуку загроз дозволяють здійснювати поглиблений аналіз та розслідування складних атак, які не були виявлені автоматично.

Платформа також має широкі можливості звітності та дотримання регуляторних вимог. Вона включає велику кількість готових звітів для стандартів типу PCI DSS, HIPAA чи GDPR, а також підтримує створення власних дашбордів та аналітичних панелей. Забезпечується тривале й надійне зберігання журналів для потреб аудиту та цифрової криміналістики.

Переваги ArcSight ESM:

- Надійність та зрілість – перевірене рішення з багаторічною історією на ринку SIEM.
- Потужний механізм кореляції – виявляє складні та багатоступеневі атаки.
- Глибока кастомізація – гнучке налаштування правил, інтеграцій та звітів.
- Масштабованість – підходить для великих корпоративних середовищ.
- Комплексність – інтеграція з SOAR, UEBA, NTA; повний функціонал SIEM.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

- Підтримка гібридних середовищ – працює локально, у хмарі та в гібриді.

Недоліки ArcSight ESM:

- Складність впровадження та управління – потребує експертизи, часу та ресурсів.
- Висока вартість – дороге ліцензування, обслуговування та навчання персоналу.
- Вимоги до ресурсів – потребує потужного апаратного забезпечення.
- Крива навчання – новим користувачам може бути важко освоїти платформу.
- Інтерфейс користувача – застарілий, менш інтуїтивний за сучасні рішення.
- Швидкість пошуку – може бути повільною при великих обсягах даних.
- Гнучкість у хмарі – менш оптимізований для хмарних сервісів

ArcSight ESM залишається потужним вибором для великих підприємств, які мають необхідні ресурси та експертизу для його розгортання та ефективного використання. Він надає глибокий контроль над безпекою та є одним з найпотужніших інструментів для виявлення та реагування на складні кіберзагрози.

Splunk Enterprise – це потужне та масштабоване рішення для забезпечення інформаційної безпеки, яке дає змогу ефективно збирати, аналізувати та використовувати дані з величезної кількості джерел. Система підтримує агрегацію інформації з мережевих пристроїв, серверів, хмарних сервісів, систем управління ідентифікацією, кінцевих точок, баз даних, а також працює з неструктурованими логами. Її архітектура дозволяє обробляти петабайти даних, що робить її придатною для підприємств будь-якого масштабу.

Завдяки гнучкій мові SPL можна створювати складні правила кореляції. Система підтримує UEBA для виявлення аномалій у поведінці користувачів та систем, інтегрується з різноманітними джерелами розвідки загроз, а також має вбудовану

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

підтримку фреймворку MITRE ATT&CK. Адаптивні правила дозволяють зменшити кількість хибних спрацювань.

Інструменти розслідування та реагування включають централізовану панель інцидентів, інтерактивні дашборди, глибокий пошук, а також тісну інтеграцію зі Splunk SOAR. Це дозволяє автоматизувати реагування, наприклад, ізоляцію систем чи блокування IP-адрес. Інструменти пошуку загроз допомагають виявляти приховані атаки, які могли залишитися поза увагою стандартної аналітики.

Для відповідності вимогам Splunk Enterprise пропонує готові звіти, підтримку різноманітних стандартів безпеки, налаштовувані дашборди для керівників, а також механізми тривалого зберігання логів для аудиту та цифрової криміналістики.

Переваги Splunk Enterprise:

- Найкращий у галузі збір даних з будь-яких машинних джерел
- Потужний пошук і аналітика на базі мови SPL
- Висока гнучкість та кастомізація правил, дашбордів і звітів
- Масштабованість для підтримки великих обсягів даних
- Розвинена екосистема додатків через Splunkbase
- Активна спільнота користувачів і підтримка

Недоліки Splunk Enterprise:

- Висока вартість і модель ліцензування за обсягом даних
- Значні вимоги до апаратних ресурсів
- Складність освоєння мови SPL та потреба у фахівцях
- Складне впровадження та підтримка

Незважаючи на високу вартість та складність, Splunk Enterprise залишається одним з найбільш потужних, гнучких та масштабованих SIEM-рішень, яке обирають великі підприємства та організації з високими вимогами до кібербезпеки та необхідністю глибокого аналізу машинних даних.

IBM Security QRadar SIEM є однією з провідних інтегрованих платформ безпеки, призначених для збору, аналізу та управління подіями безпеки, а також для

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

виявлення, розслідування та реагування на кіберзагрози. Вона орієнтована на великі та середні підприємства, державні установи та постачальників керованих послуг безпеки.

QRadar об'єднує функції SIEM, управління журналами, мережевий аналіз, аналіз поведінки користувачів та розвідку загроз в єдину архітектуру, надаючи комплексний огляд безпеки всієї IT-інфраструктури.

IBM Security QRadar забезпечує всебічний збір даних із широкого спектра джерел, включаючи журнали, мережеві потоки, пакети, інформацію про вразливості та активи. Усі зібрані дані автоматично нормалізуються й збагачуються контекстом, що дозволяє значно покращити точність аналізу. Завдяки потужному механізму кореляції QRadar здатен у реальному часі виявляти складні загрози, інсайдерську активність і порушення політик. У рішенні доступні як попередньо налаштовані, так і повністю настроювані правила, а також функціонал UEBA для виявлення поведінкових аномалій. Аналіз мережевого трафіку, включаючи рівень 7, дозволяє виявляти підозрілу активність, а інтеграція з розвідкою загроз надає актуальні індикатори компрометації.

QRadar автоматично об'єднує пов'язані події в інциденти (Offenses) і розставляє пріоритети залежно від рівня ризику. Інтерфейс розслідування інцидентів дозволяє бачити повну картину атаки, включаючи контекст і часову шкалу. Пошук загроз можливий за допомогою гнучких інструментів аналізу, а інтеграція з QRadar SOAR забезпечує автоматизацію реагування на інциденти: від блокування IP до створення тікетів. Продукт також тісно взаємодіє з іншими рішеннями IBM Security, формуючи єдину екосистему безпеки.

Також дана система пропонує велику кількість готових звітів для демонстрації відповідності різним стандартам, можливість створення кастомних дашбордів і забезпечує довготривале зберігання логів для аудиту й аналітики.

Переваги IBM Security QRadar SIEM:

- Комплексність та інтеграція функцій SIEM, UEBA, NTA, TI, SOAR.
- Висока ефективність виявлення загроз завдяки кореляції, AI та TI.
- Глибока видимість мережі через аналіз потоків і пакетів.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

- Пріоритезація інцидентів через агрегування подій у порушення.
- Надійність і масштабованість для великих корпоративних середовищ.
- Підтримка локальних, хмарних та гібридних розгортань.

Недоліки IBM Security QRadar SIEM:

- Складність впровадження та адміністрування.
- Висока вартість ліцензування, підтримки та навчання.
- Крива навчання для користувачів і адміністраторів.
- Високі вимоги до апаратних ресурсів при локальному розгортанні.

Загалом, IBM Security QRadar SIEM є одним з лідерів ринку SIEM, який надає повний спектр можливостей для кібербезпеки великих та складних організацій, що прагнуть комплексного моніторингу, виявлення загроз та ефективного реагування.

FortiSIEM від Fortinet є SIEM рішенням з розширеними функціями, розроблене для забезпечення комплексної видимості, аналітики безпеки та управління інцидентами в сучасних, складних IT-інфраструктурах, що охоплюють локальні мережі, хмарні середовища, IoT та OT. Він спрямований на об'єднання операцій безпеки та мережевих операцій для більш ефективного виявлення та реагування на загрози.

FortiSIEM забезпечує централізований збір логів та телеметрії з великої кількості джерел, включаючи як пристрої Fortinet, так і стороннє обладнання, сервери, бази даних, хмарні сервіси та системи IAM. Зібрані дані проходять нормалізацію та збагачуються контекстною інформацією, що суттєво спрощує подальший аналіз.

Основою аналітики FortiSIEM є кореляція подій у реальному часі, яка дозволяє виявляти багаторівневі загрози та аномалії. За допомогою механізмів UEBA створюються поведінкові профілі користувачів і пристроїв, що дає змогу виявляти інсайдерські загрози або зломи облікових записів. Система інтегрується з FortiGuard і сторонніми джерелами розвідки загроз для автоматичного виявлення відомих ІОС. Використання CMDB дозволяє зіставляти події безпеки з конкрет-

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

ними активами, а підтримка MITRE ATT&CK зіставляти загрози з відомими тактиками атак. Пріоритезація сповіщень базується на оцінці ризиків, що дозволяє командам безпеки зосередитися на найбільш критичних інцидентах.

FortiSIEM також виконує функції SOAR-системи, забезпечуючи централізоване управління інцидентами з можливістю перегляду повного контексту подій. Завдяки інтеграції з FortiSOAR можливе автоматизоване реагування: блокування IP-адрес, ізоляція систем, надсилання сповіщень або створення тікетів у зовнішніх системах. Інструменти для проактивного пошуку загроз дають змогу аналітикам виявляти приховані атаки поза межами наявних правил.

Окремою перевагою є здатність FortiSIEM поєднувати функції безпеки з моніторингом доступності та продуктивності мережі й інфраструктури. Це дозволяє забезпечити ефективну взаємодію команд SOC і NOC та оперативно реагувати як на загрози, так і на збої в роботі систем.

Платформа також має розвинену систему звітності: включає готові шаблони для відповідності вимогам стандартів (наприклад, PCI DSS, HIPAA, GDPR, SOX, NIST) і дозволяє створювати власні дашборди та аналітичні звіти для оцінки ефективності заходів безпеки.

Переваги FortiSIEM:

- Інтеграція з Fortinet, безшовна робота з FortiGate, FortiAnalyzer та іншими продуктами екосистеми.
- Поєднання безпеки й моніторингу продуктивності в одній платформі.
- Гнучкість розгортання, підтримка фізичних, віртуальних, хмарних і гібридних середовищ.
- Потужний кореляційний механізм, UEBA та розвідка загроз.
- Ефективна робота у великих корпоративних мережах.

Недоліки FortiSIEM:

- Складність налаштування: інтеграція з багатьма джерелами вимагає досвіду.
- Потрібен час для повного освоєння функцій.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

- Залежність від Fortinet, найкраща ефективність у зв'язці з власними продуктами Fortinet.
- Рішення вимагає значних інвестицій, хоч і має конкурентне ціноутворення.

FortiSIEM є чудовим вибором для організацій, які шукають інтегроване рішення SIEM, особливо якщо вони вже є користувачами екосистеми Fortinet. Він надає комплексний підхід до безпеки та операційної видимості, що допомагає організаціям ефективно керувати ризиками та реагувати на загрози.

Після аналізу SIEM-рішень стає очевидним, що кожна з цих платформ має свої унікальні переваги та недоліки. Керуючись дослідженими характеристиками кожного з них для дослідження було обрано Elastic Stack тому що, дане рішення пропонує ідеальне поєднання гнучкості, потужності та доступності, що робить його оптимальним вибором для дослідження та розробки в контексті кваліфікаційної роботи з побудови підсистеми моніторингу подій інформаційної безпеки.

Висновки до першого розділу

В першому розділі було розглянуто особливості моніторингу подій інформаційної безпеки, розглянуто SIEM-рішення The Elastic Stack його альтернативи та їх переваги і недоліки.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

РОЗДІЛ 2 ПРОЄКТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ ПОДІЙ НА БАЗІ THE ELASTIC STACK

2.1 Проєктування системи

Для дослідження в даній роботі була розглянута модель корпоративної мережі, на базі якої було проведено тестування особливостей та можливостей підсистеми моніторингу подій інформаційної безпеки в мережі на базі рішень The Elastic Stack. Мережа спроектована таким чином, щоб забезпечити гнучкість у розгортанні, розширенні та модифікації її структури відповідно до потреб тестування.

Модель мережі складається з базового набору серверів і робочих станцій, до яких можуть бути додані інші вузли, пристрої та сервіси для емулявання реальних сценаріїв. Такий підхід дозволяє створити умови, наближені до реального середовища, що є важливим фактором для ефективної перевірки роботи SIEM-системи.

The Elastic Stack – це потужний інструмент для збору, обробки, аналізу та візуалізації логів з різних джерел. Його модульна структура, яка включає такі основні компоненти, як Filebeat, Logstash, Elasticsearch, Kibana, забезпечує масштабованість і можливість інтеграції з різноманітними частинами мережі. Завдяки цьому Elastic Stack здатен обробляти великі обсяги подій без втрати продуктивності.

На рисунку 2.1.1. Зображено схему моделі мережі мережної інфраструктури організації.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

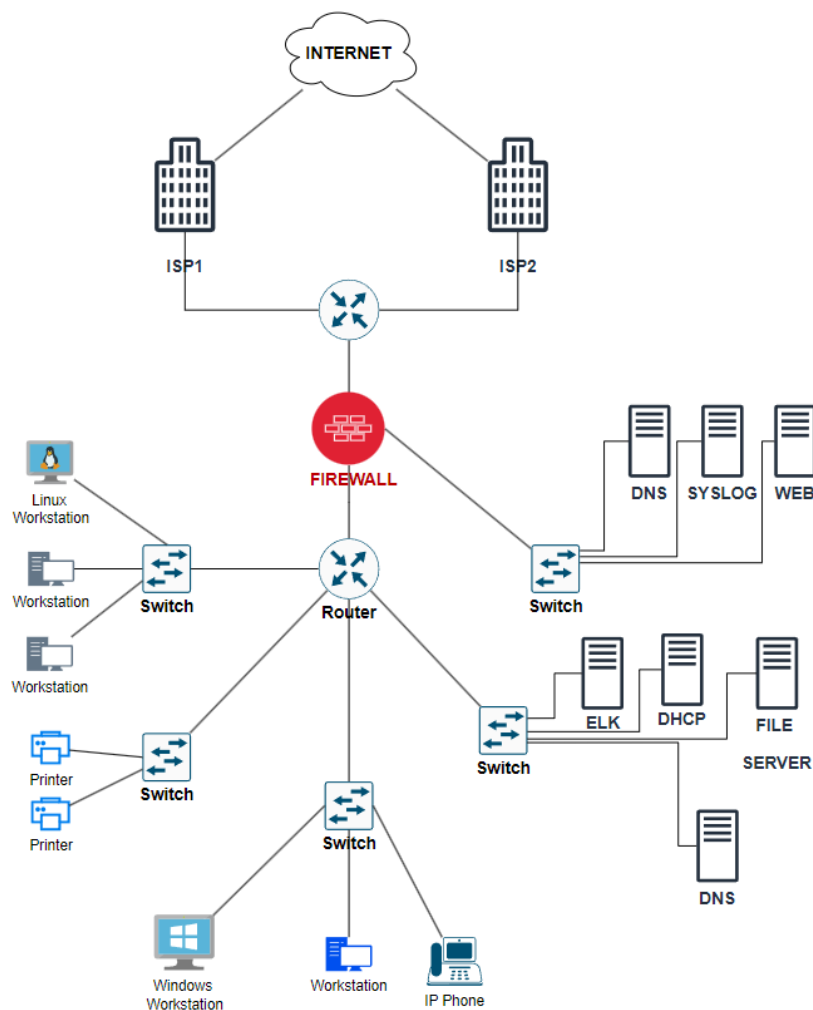


Рисунок 2.1.1 – Схема моделі мережної інфраструктури організації

Модель мережі включає підключення до Інтернету через двох провайдерів, що забезпечує відмовостійкість. Трафік фільтрується за допомогою Firewall, що є ключовим елементом безпеки. За Firewall знаходиться Router, який керує маршрутизацією всередині корпоративної мережі.

Мережа складається з набору серверів і робочих станцій, до яких можуть бути додані інші вузли, пристрої та сервіси для емулявання реальних сценаріїв. Такий підхід дозволяє створити умови, наближені до реального середовища, що є важливим фактором для ефективної перевірки роботи SIEM-системи.

До маршрутизатора підключено декілька комутаторів, які розділяють мережеву інфраструктуру на різні підмережі. До цих комутаторів підключені робочі станції, принтери та IP телефони. Серверна частина мережі, що включає DNS, SYSLOG, WEB, ELK, DHCP, FILE SERVER, також взаємодіє з маршрутизатором

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

через ці комутатори, забезпечуючи розподілене функціонування усіх сервісів. Для зручності деякі сервери було винесено до DMZ.

В розробленій мережі окрему роль відіграють сервери журналювання, сервери DNS, DHCP та інші інфраструктурні компоненти, які створюють типову корпоративну екосистему. Це дозволяє не лише відстежувати події інформаційної безпеки, а й тестувати реакцію системи на інциденти, налаштовувати кореляційні правила та будувати дашборди для візуального контролю.

Таким чином, обрана модель корпоративної мережі, відображена на рисунку 2.1.1, дозволяє повноцінно протестувати функціональні можливості ELK як системи моніторингу подій ІБ у різних умовах та масштабах. Вона слугує базовою платформою для подальших досліджень і практичних експериментів у сфері кібербезпеки.

В даній роботі буде розгорнуто віртуальну модель мережі організації в середовищі GNS3. Для побудови мережі буде використано маршрутизатори та комутатори Cisco, віртуальні машини, запуск яких буде здійснено за допомогою VirtualBox.

Компоненти використані для розробки проєкту:

- GNS3
- VirtualBox
- Linux Ubuntu Server
- Linux Lubuntu
- Kali Linux
- Cisco Router
- Cisco Switch

GNS3 – це програмний емулятор мереж, який дозволяє створювати віртуальні комп’ютерні мережі для навчання та тестування технологій.

VirtualBox – це інструмент віртуалізації, який використовують для розгортання операційних систем робочих станцій та серверів як віртуальні машини.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Linux Ubuntu Server – це є спеціалізованим дистрибутивом Linux який орієнтований на стабільну та безпечну роботу в серверному середовищі. Ця система є безкоштовною, має відкритий вихідний код і підтримується компанією Canonical. Ubuntu Server забезпечує високу сумісність із сучасними програмними рішеннями, включаючи системи віртуалізації, контейнери, засоби моніторингу, бази даних та інші серверні сервіси.

Linux Lubuntu – це легкий варіант операційної системи Ubuntu, створений спеціально для менш потужних або старіших комп'ютерів. Вона використовує LXQt як графічне середовище, що робить систему швидкою та економною до ресурсів.

Kali Linux – це спеціалізований дистрибутив Linux, створений для тестування на проникнення, аналізу безпеки та цифрової криміналістики. Його розробкою займається компанія Offensive Security, і він базується на Debian, що забезпечує сумісність з широким спектром програмного забезпечення та стабільну основу для роботи. Kali містить попередньо встановлений набір інструментів, що охоплюють різні аспекти інформаційної безпеки: сканування мереж, тестування вебдодатків, злом паролів, аналіз вразливостей, перехоплення трафіку та інші напрямки.

Cisco Router – це мережевий пристрій, призначений для маршрутизації трафіку між різними мережами. Пристрої цього типу широко використовуються в корпоративних та телекомунікаційних інфраструктурах завдяки високій продуктивності, масштабованості та надійності. Cisco Router підтримує розширені функції маршрутизації, фільтрації трафіку, створення VPN-з'єднань і реалізації політик безпеки. Завдяки операційній системі Cisco IOS, маршрутизатори забезпечують гнучкість у налаштуванні та інтеграції з іншими елементами мережі, що робить їх ключовими компонентами у побудові захищених та ефективних мережевих рішень.

Cisco Switch – це комутаційний пристрій, який виконує функції пересилання кадрів між пристроями в межах однієї LAN. Комутатори Cisco вирізняються високою продуктивністю, низькою затримкою та широкими можливостями керування. Вони підтримують розділення мережі на VLAN, контроль доступу, моніторинг тра-

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

фіку та інші функції, необхідні для забезпечення безпеки та стабільної роботи мережевої інфраструктури. Завдяки надійності та гнучким можливостям конфігурації, Cisco Switch є невід'ємним елементом сучасних мережевих середовищ.

2.2. Проектування служб та сервісів

Проектування служб та сервісів є важливим етапом побудови системи моніторингу подій. Саме на даному етапі визначається логіка взаємодії компонентів, спосіб обробки даних та механізми взаємозв'язку між вузлами. У цьому підрозділі розглядаються ключові функціональні елементи, які забезпечують повноцінну та безперебійну роботу системи: від збору подій на кінцевих пристроях до їх зберігання, аналізу та візуалізації.

Служби збору логів у запропонованій архітектурі реалізуються за допомогою агентів, які встановлюються на робочих станціях або серверах. Вони відповідають за збір різних типів логів, включаючи системні повідомлення ядра, журнали доступу, логи аутентифікації та прикладні події. Це дозволяє охопити усі критично важливі аспекти роботи системи, які можуть містити ознаки потенційних загроз або інцидентів інформаційної безпеки.

Однак не всі пристрої мережі дозволяють встановлення агентів. У випадку мережевого обладнання або інших спеціалізованих пристроїв, збір подій здійснюється за допомогою стандартних мережевих протоколів, які не потребують втручання у роботу пристрою. До таких протоколів належать:

- SNMP
- Syslog
- NetFlow

SNMP – це протокол який дозволяє отримувати інформацію про стан інтерфейсів, завантаження, кількість помилок тощо.

Syslog – це протокол системного журналювання, що спрощує передачу інформації від пристроїв в мережі до syslog сервера.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

NetFlow – це мережевий протокол розроблений для пристроїв від компанії Cisco. Він широко застосовується для збору даних про інтернет трафік який проходить по мережевих пристроях, що допомагає відстежувати інформацію про продуктивність мережі.

Для передачі подій до центрального вузла обробки використовуються стандартні транспортні механізми, зокрема Beats-протокол та syslog. Передача даних відбувається через мережеві з'єднання із використанням захищених каналів, що забезпечує цілісність інформації та захист від перехоплення. Передбачено можливість використання TLS для шифрування трафіку між агентами та приймальними вузлами, що підвищує рівень безпеки системи.

Обробка отриманих логів реалізується за допомогою компонента Logstash, який виступає посередником між агентами збору та базою даних. Він виконує попередню фільтрацію, нормалізацію даних та додавання структурованих метаданих, що полегшує подальший аналіз. Крім того, у Logstash налаштовуються пайплайни, які дозволяють визначити маршрутизацію подій залежно від їхнього типу або вмісту.

Зберігання оброблених подій здійснюється в Elasticsearch — високопродуктивному пошуковому рушії, оптимізованому для роботи з великими обсягами структурованих логів. Тут реалізовано поділ на індекси за категоріями подій, що забезпечує швидкий доступ до потрібних даних.

Для доступу до інформації використовується Kibana — інтерфейс візуалізації, що дозволяє створювати інформативні дашборди, здійснювати пошук по логах, виявляти аномальні дії та проводити аналіз подій у зручному графічному вигляді. Інструмент дозволяє не лише переглядати дані, а й формувати динамічні запити, будувати графіки та гістограми, що значно спрощує процес моніторингу та реагування.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

2.3 Аналіз рішення The Elastic Stack та допоміжного програмного забезпечення

The Elastic Stack є потужним набором інструментів з відкритим вихідним кодом для пошуку, аналізу та візуалізації даних у реальному часі. Його гнучкість та масштабованість дозволяють створювати комплексні рішення для моніторингу, аналізу логів, безпеки та бізнес-аналітики.

Основою стеку є чотири ключові компоненти:

- Elasticsearch;
- Logstash;
- Kibana;
- Beats;

Elasticsearch – це пошуковий та аналітичний рушій, що забезпечує зберігання, індексацію та швидкий пошук великих обсягів даних.

Logstash – це елемент обробки даних, який отримує дані з безлічі джерел одночасно, трансформує їх та відправляє до сховища, такого як Elasticsearch.

Kibana – це веб-інтерфейс для візуалізації даних з Elasticsearch. Дозволяє користувачам створювати інтерактивні дашборди, графіки та діаграми для аналізу даних.

Beats – це сімейство легких агентів, які встановлюються на кінцевих системах для збору різноманітних типів даних та їх подальшої передачі до Elasticsearch або Logstash.

Інтеграція стеку The Elastic Stack із системою виявлення та запобігання вторгненням Snort є важливим етапом у побудові централізованої системи моніторингу подій інформаційної безпеки. Така взаємодія забезпечує можливість отримання, збереження, обробки та візуалізації даних про мережевий трафік та загрози, виявлені системою Snort. У результаті реалізується цілісний підхід до аналізу подій безпеки, що включає як мережевий рівень, так і системні або прикладні журнали.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Ключовим елементом даної інтеграції є компонент Filebeat — легкий агент збору логів, який встановлюється на сервер, де розгорнуто Snort. Filebeat конфігурується на моніторинг лог-файлів, що створюються системою виявлення вторгнень, та на передачу отриманих подій у систему Elastic Stack. Передача може здійснюватися безпосередньо до Elasticsearch або з використанням Logstash як проміжного етапу для попередньої обробки даних.

Snort – це потужна система виявлення та запобігання вторгнень, яка надає можливість аналізувати мережевий трафік в режимі реального часу задля виявлення аномальної активності та вчасного реагування на атаки.

На рисунку 2.3.1. можна побачити схему зв'язку між Snort та ELK.

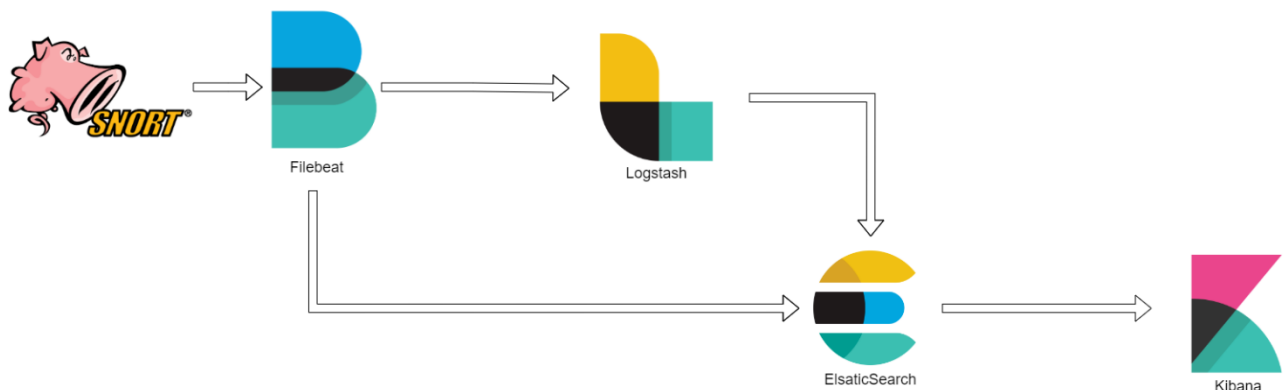


Рисунок 2.3.1 – Схема можливої роботи системи із Snort

Крім того, за допомогою надбудови Elastalert до ELK можна налаштувати автоматичне оповіщення у разі виявлення Snort аномальної активності або потенційних атак, що забезпечує оперативну реакцію на загрози в режимі реального часу.

2.4 Аналіз типових атак на систему моніторингу

Системи моніторингу інформаційної безпеки відіграють ключову роль при виявленні та запобіганні кіберзагрозам. Для забезпечення їх надійної роботи необхідно розуміти, які типи атак становлять найбільшу загрозу, а також шляхи їх реалізації. Серед найбільш поширених атак варто виділити наступні:

- Spoofing
- Port Scanning
- UDP Flood

Дослідження цих атак дозволяє виявити потенційні вразливості, скоригувати правила виявлення інцидентів безпеки та реалізувати ефективні заходи реагування.

Першою в нашому аналізі буде атака Spoofing, що характеризується підміною ідентифікаторів в мережевих пакетах з метою обходу систем захисту.

Суть Spoofing атаки полягає в імітації надійного джерела. Зловмисник намагається видати себе за довірену систему або користувача, з метою отримання доступу до закрити даних чи функціоналу. Таке підроблення адрес дозволяє зловмиснику приховати свою справжню ідентичність та обійти механізми аутентифікації або авторизації, що створює значну загрозу для безпеки мережі.

Існують різні види Spoofing-атак, серед яких найбільш поширеними є:

- IP-spoofing
- ARP-spoofing
- DNS-spoofing

Атаку IP Spoofing можна поділити на зовнішню та внутрішню.

При зовнішній зловмисник надсилає на внутрішню мережу пакети, у яких підроблено IP-адресу відправника, підставляючи внутрішню IP-адресу. Оскільки такі адреси згідно з RFC 1918 не повинні з'являтися в інтернеті, отримання подібних пакетів ззовні є ознакою атаки. У цьому випадку граничний міжмережевий екран має відкинути такий пакет і повідомити про подію систему SIEM для подальшого аналізу.

Внутрішній IP Spoofing відбувається, коли з локальної мережі надсилається пакет із підробленою публічною IP-адресою відправника. Оскільки цей пакет походить із приватної мережі, наявність у ньому публічної адреси є ненормальною і свідчить про потенційно шкідливу активність. У цьому випадку застосовується фільтрація, яка блокує відправлення такого трафіку й передає інформацію до SIEM. Така ситуація вказує на наявність зловмисника вже всередині мережі, причому зазвичай це не користувач, а скомпрометована система, яка використовується для атак на зовнішні ресурси.

ARP-spoofing полягає у підміні MAC-адрес у локальній мережі, що дозволяє перехоплювати або змінювати трафік між пристроями, а DNS-spoofing – у зміні

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

адреси DNS-сервера, що спричиняє перенаправлення користувача на фальшиві сайти.

На рисунках 2.4.1 – 2.4.3 можна побачити схеми Spoofing атак

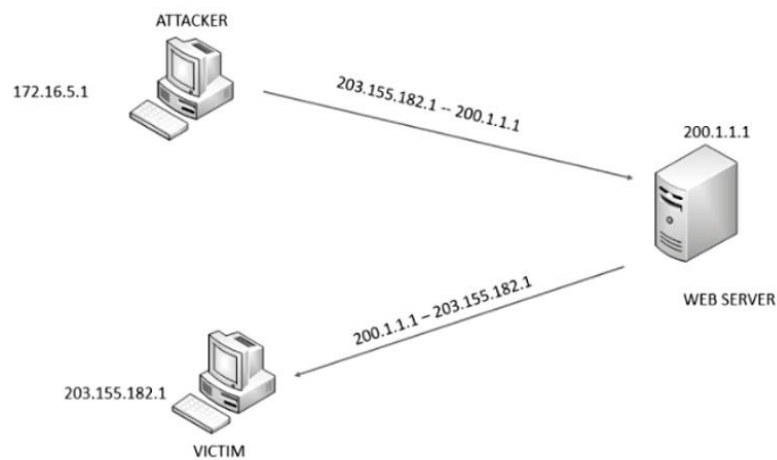


Рисунок 2.4.1 – Схема IP Spoofing атаки

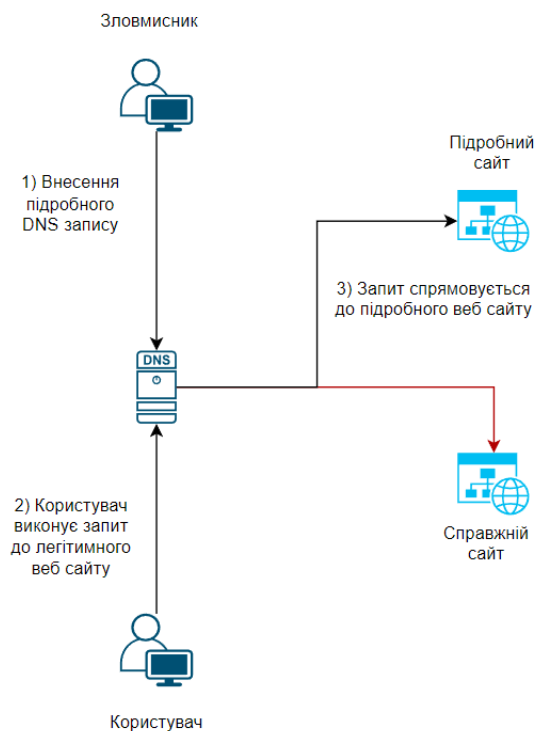


Рисунок 2.4.2 – Схема DNS Spoofing атаки

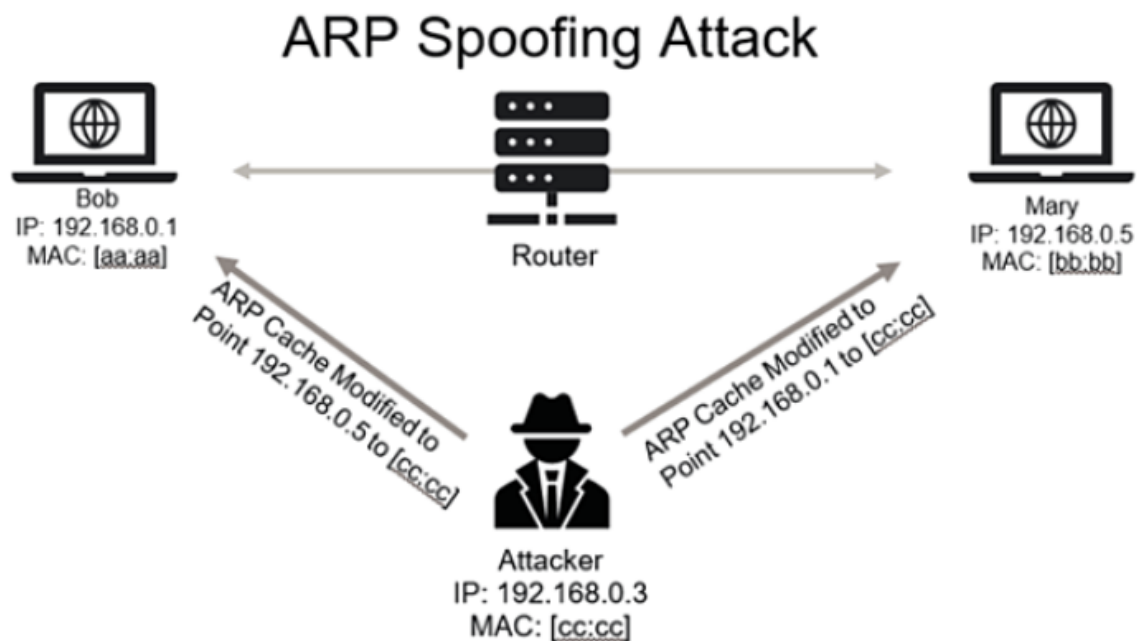


Рисунок 2.4.3 – Схема ARP Spoofing атаки

Наслідки Spoofing-атак можуть бути дуже серйозними: від витоку конфіденційної інформації до порушення роботи мережі і навіть повного контролю над ураженими пристроями. Через це для забезпечення безпеки мережевої інфраструктури необхідно своєчасно виявляти та блокувати подібні атаки.

Для виявлення Spoofing-атак у системах моніторингу інформаційної безпеки застосовують різні методи. Це може бути аналіз аномалій мережевого трафіку, виявлення невідповідностей між IP-адресами і MAC-адресами, перевірка TTL пакетів та інші поведінкові індикатори. Крім того, у таких інструментах, як Snort, можна налаштовувати спеціальні сигнатури та правила для виявлення типових ознак Spoofing. Elastic Stack, у свою чергу, дозволяє агрегувати, індексувати та візуалізувати мережеві логи, що значно полегшує виявлення підозрілої активності.

Окрім Spoofing, для оцінки безпеки систем моніторингу важливо розглянути і таку техніку, як Port Scanning, що дозволяє зловмисникам визначити відкриті сервіси та вразливі точки у мережі.

Port Scanning – це метод, який широко застосовується для виявлення відкритих або слабо захищених точок у мережевій інфраструктурі. Така атака дозволяє кіберзлочинцям визначити, які порти на комп'ютерах або серверах доступні, які

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

сервіси на них працюють, та оцінити потенційні вразливості. Крім того, сканування портів може допомогти виявити наявність мережевих захисних засобів, таких як міжмережеві екрани чи системи виявлення вторгнень.

На рисунку 2.4.4 наведено схему атаки Port Scanning.

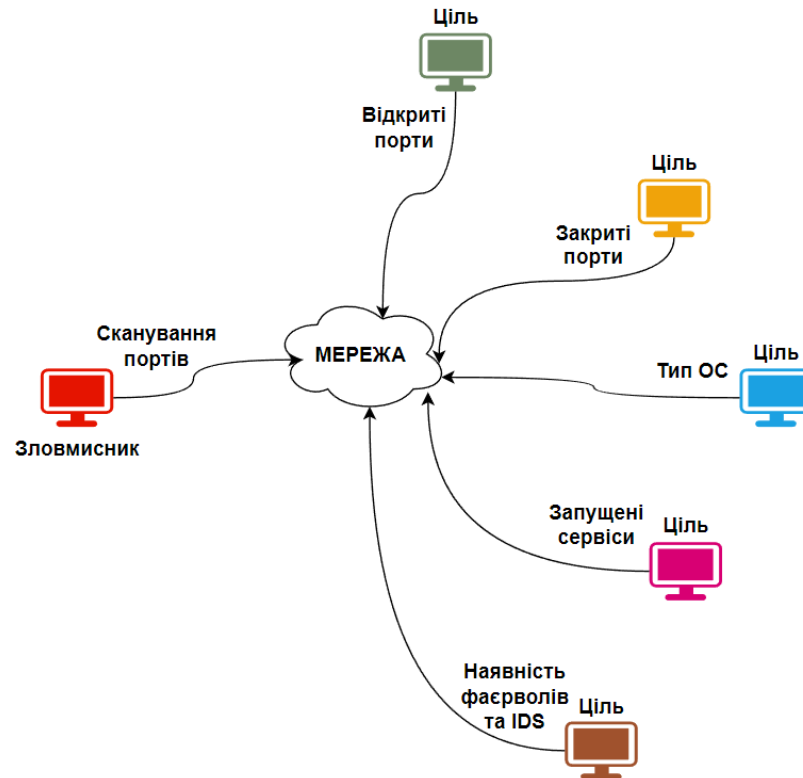


Рисунок 2.4.4 – Схема атаки Port-Scanning

Для того щоб зрозуміти як працює port scanning потрібно розібратися що таке порт.

Порт – це умовна точка в комп’ютерній системі, через яку відбувається обмін інформацією між програмами або між пристроями в мережі. Для зручності та стандартизації кожному порту призначається числовий ідентифікатор у діапазоні від 0 до 65 535.

Порти поділяються на кілька категорій:

Порти 0–1023 (well-known ports) – це "добре відомі порти", зарезервовані для основних інтернет-протоколів і сервісів.

Порти 1024–49 151 (registered ports) – "zareєстровані порти", які можуть використовуватись прикладними програмами.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

Порти 49 152–65 535 (dynamic/private ports) – "динамічні або приватні порти", які можуть використовуватись будь-якими програмами без попередньої реєстрації.

Передача даних через порти здійснюється за допомогою таких протоколів:

TCP – надійний протокол, який забезпечує контроль доставки даних.

UDP – швидкий, але менш надійний протокол, що використовується для передавання даних з мінімальними затримками.

Приклади стандартних портів:

Порт 20 (TCP) – використовується для передавання даних у протоколі FTP.

Порт 21 (TCP) – керуючий порт для FTP-з'єднань.

Порт 22 (TCP) – протокол SSH, що забезпечує безпечний віддалений доступ до системи.

Порт 23 (TCP) – протокол Telnet, який дозволяє встановлювати текстові з'єднання без шифрування.

Порт 53 (UDP) – використовується системою доменних імен (DNS).

Порт 80 (TCP) – використовується для доступу до вебсторінок через протокол HTTP.

Порт 443 (TCP) – застосовується для захищених веб-з'єднань через HTTPS.

Сканування портів полягає в надсиланні запитів на різні порти цільового пристрою та аналізі відповідей. Залежно від відповіді можна визначити:

- Чи порт відкритий, закритий або фільтрується.
- Який сервіс працює на порту.
- Чи потребує сервіс автентифікації.
- Чи дозволений анонімний доступ.
- Версії програмного забезпечення, що працює.

Хакери можуть використовувати такі методи сканування:

TCP SYN scan – найпоширеніший метод, який надсилає SYN-пакет і аналізує відповідь.

UDP scan – надсилає UDP-пакети для виявлення служб, що працюють на цьому протоколі.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

Xmas, Null, FIN scan – спеціалізовані методи, які використовуються для обходу фаєрволів або IDS.

Сканування портів застосовується не лише зловмисниками, але й адміністраторами безпеки для виявлення та усунення вразливостей у власних системах. Для цього використовуються спеціалізовані інструменти:

Nmap – один із найпотужніших сканерів портів з широким функціоналом.

Netcat – універсальний інструмент для роботи з мережею.

IP Scanner – використовується для виявлення активних пристроїв у мережі.

Сканування портів є як ефективним методом атак, так і необхідним інструментом у сфері захисту інформації. Його своєчасне виявлення та правильне використання дозволяє суттєво покращити рівень кіберзахисту організацій.

Серед можливих атак на систему також варто виділити UDP Flood атаку.

UDP-флуд атака є формою розподіленої атаки на відмову в обслуговуванні, так званий DDoS, що ґрунтується на масовій відправці UDP-пакетів до цільової системи з метою її перевантаження. Через те, що UDP є безз'єднальним протоколом, який не вимагає встановлення з'єднання, система змушена реагувати на кожен отриманий пакет, не знаючи заздалегідь, чи є надійним його джерело. Це створює додаткове навантаження, особливо коли пакети спрямовуються на випадкові порти, і система має перевірити наявність відповідних служб. Якщо жодна служба не прослуховує порт, то генерується ICMP-повідомлення про недоступність, що ще більше виснажує ресурси. У результаті, система може втратити здатність обробляти законні запити, що призводить до часткового або повного збою в її роботі.

На рисунку 2.4.5 зображено схему UDP Flood атаки.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

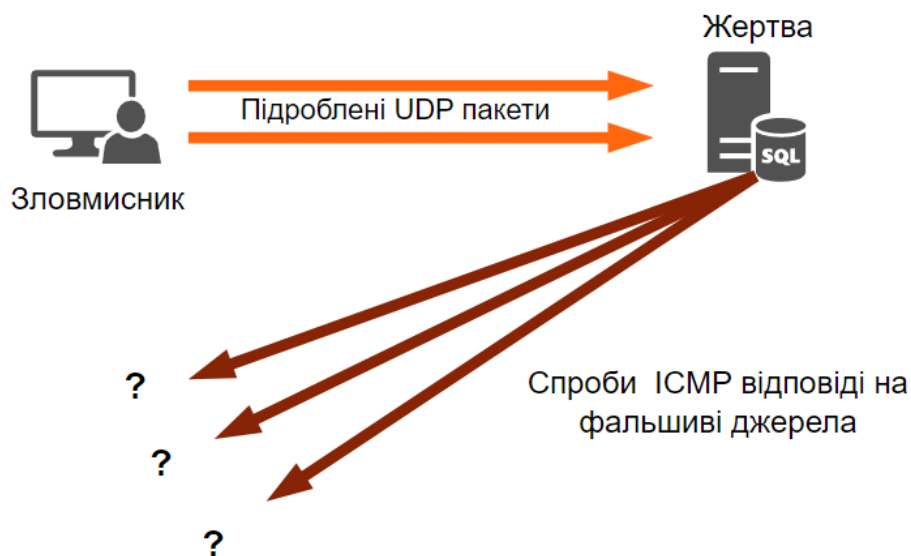


Рисунок 2.4.5 – Схема UDP Flood атаки

Захист від UDP-флуд атак базується на поєднанні технічних і організаційних заходів. Одним із основних методів є обмеження швидкості обробки запитів, яке допомагає уникнути перевантаження шляхом регулювання кількості запитів, що обробляються за певний період часу. Також ефективним є використання систем виявлення та запобігання вторгненням, які аналізують трафік у реальному часі, виявляють характерні ознаки атаки та можуть автоматично блокувати підозрілий потік даних. Також задля зменшення ризиків можна вимкнути UDP-сервіси, які не використовуються в роботі мережі, що зменшить кількість можливих точок для атак. Регулярні аудити безпеки дозволяють вчасно виявляти потенційні вразливості, а розгортання комплексних DDoS-захисних рішень, що включають механізми машинного навчання, дає змогу виявляти та блокувати аномальний трафік ще до того, як він завдасть шкоди.

Висновки до другого розділу

У другому розділі було проаналізовано процес проєктування підсистеми моніторингу подій інформаційної безпеки на базі рішень The Elastic Satch. Розглянуто ключові технології та протоколи, що забезпечують функціонування системи. Особливу увагу приділено системі Snort та прикладам атак на систему які можна виявити з її допомогою.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ СПРОЄКТОВАНОЇ СИСТЕМИ

3.1. Побудова та налагодження спроектованої системи

Для практичної побудови, налагодження та тестування роботи спроектованої підсистеми моніторингу подій інформаційної безпеки було створено модельний приклад мережі. З огляду на обмежені фізичні ресурси машини, на якій здійснюється розгортання, мережева архітектура реалізована у спрощеному вигляді. Такий підхід дозволяє зберегти основну функціональність системи, продемонструвати її ключові можливості та забезпечити умови для моделювання типових сценаріїв взаємодії компонентів SIEM-рішення. Спрощена модель водночас зберігає логічну структуру, наближену до реального середовища, що дозволяє провести базову оцінку ефективності побудованої системи.

На рисунку 3.1.1 зображено модельний приклад мережі.

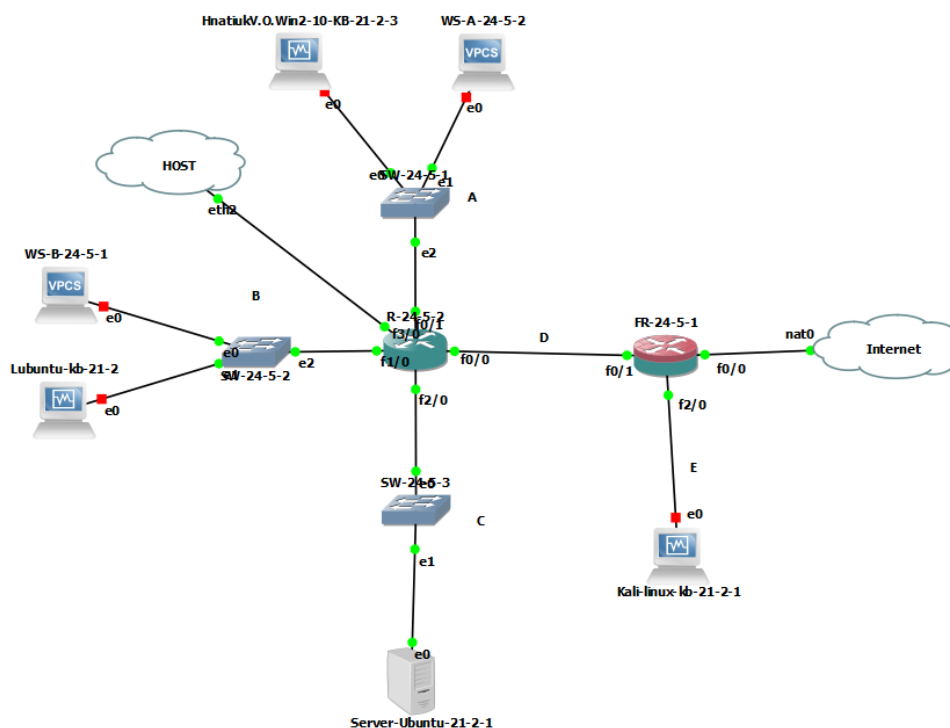


Рисунок 3.1.1 – Схема архітектури модельного прикладу мережі

Мережа складається з декількох підмереж, зв'язок між яким забезпечується протоколом OSPF.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Загалом використовуються 2 маршрутизатора та 3 комутатора. Проєкт налічує 3 підмережі. Таблиця підмереж та призначення IP-адрес представлені в додатку А

Перш завсе налаштовуємо мережеві пристрої. Нижче, на рисунках 3.1.1 – 3.1.2., наведено приклад базового налаштування необхідного для збору даних та моніторингу.

```
FR-24-5-1(config)#logging host 192.168.2.2 transport udp port 514
FR-24-5-1(config)#logging trap debugging
FR-24-5-1(config)#logging facility local1
FR-24-5-1(config)#logging console debugging
FR-24-5-1(config)#logging buffered debugging
FR-24-5-1(config)#logging on
```

Рисунок 3.1.2 – Налаштування логування подій

```
R-24-5-2(config)#flow record MyNetFlow
R-24-5-2(config-flow-record)#description NetFlow record
R-24-5-2(config-flow-record)#description NetFlow record
R-24-5-2(config-flow-record)#match ipv4 ttl
R-24-5-2(config-flow-record)#match ipv4 tos
R-24-5-2(config-flow-record)#match ipv4 protocol
R-24-5-2(config-flow-record)#match ipv4 source address
R-24-5-2(config-flow-record)#match ipv4 destination address
R-24-5-2(config-flow-record)#match transport source-port
R-24-5-2(config-flow-record)#match transport destination-port
R-24-5-2(config-flow-record)#collect counter bytes
R-24-5-2(config-flow-record)#collect counter packets
R-24-5-2(config-flow-record)#collect timestamp sys-uptime first
R-24-5-2(config-flow-record)#collect timestamp sys-uptime last
R-24-5-2(config-flow-record)#
R-24-5-2(config-flow-record)#flow exporter NETFLOWtoELK
R-24-5-2(config-flow-exporter)#destination 192.168.2.2
R-24-5-2(config-flow-exporter)#transport udp 2055
R-24-5-2(config-flow-exporter)#template data timeout 60
R-24-5-2(config-flow-exporter)#flow monitor FLOW-MONITOR
R-24-5-2(config-flow-monitor)#exporter NETFLOWtoELK
R-24-5-2(config-flow-monitor)#cache timeout active 300
R-24-5-2(config-flow-monitor)#cache timeout update 60
R-24-5-2(config-flow-monitor)#record MyNetFlow
R-24-5-2(config-flow-monitor)#exit
R-24-5-2(config)#int f0/0
R-24-5-2(config-if)#ip flow monitor FLOW-MONITOR input
R-24-5-2(config-if)#ip flow monitor FLOW-MONITOR output
R-24-5-2(config-if)#exit
R-24-5-2(config)#
```

Рисунок 3.1.3 – Налаштування NetFlow

Після проведеного налаштування мережевих пристроїв було проведено встановлення та налагодження основних компонентів системи. На рисунках 3.1.4 -

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

3.1.17. показано налаштування сервера, встановлення необхідних для системи пакетів та їх базове налаштування.

```
vitadmin@server-ubuntu2121:~$ sudo apt install openjdk-11-jdk -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  openjdk-11-jdk-headless openjdk-11-jre openjdk-11-jre-headless
Suggested packages:
```

Рисунок 3.1.4 – Встановлення пакетів java на сервер

```
vitadmin@server-ubuntu2121:~$ sudo apt-get install nginx
Reading package lists... Done
```

Рисунок 3.1.5 – Встановлення nginx

```
vitadmin@server-ubuntu2121:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
File '/usr/share/keyrings/elasticsearch-keyring.gpg' exists. Overwrite? (y/N) y
vitadmin@server-ubuntu2121:~$
```

Рисунок 3.1.6 – Встановлення елементів ELK

```
vitadmin@server-ubuntu2121:~$ echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" |
sudo tee /etc/apt/sources.list.d/elastic-8.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main
vitadmin@server-ubuntu2121:~$
```

Рисунок 3.1.7 – Встановлення елементів ELK

```
vitadmin@server-ubuntu2121:~$ sudo apt-get install elasticsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 636 MB of archives.
After this operation, 1,210 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch arch amd64 8.17.1 [636 MB]
46% [1 elasticsearch 363 MB/636 MB 57%] 2,197 kB/s 2min 4s
```

Рисунок 3.1.8 – Встановлення елементів ELK

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

```
vitadmin@server-ubuntu2121:~$ sudo systemctl start elasticsearch
[sudo] password for vitadmin:

vitadmin@server-ubuntu2121:~$ sudo systemctl enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
vitadmin@server-ubuntu2121:~$
```

Рисунок 3.1.9 – Встановлення елементів ELK

```
vitadmin@server-ubuntu2121:~$ sudo apt-get install logstash -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
```

Рисунок 3.1.10 – Встановлення елементів ELK

```
vitadmin@server-ubuntu2121:~$ sudo systemctl start logstash
vitadmin@server-ubuntu2121:~$ sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /lib/systemd/system/logstash.service.
vitadmin@server-ubuntu2121:~$
```

Рисунок 3.1.11 – Встановлення елементів ELK

```
sudo: apt-get: command not found
vitadmin@server-ubuntu2121:~$ sudo apt-get install kibana
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
```

Рисунок 3.1.12 – Встановлення елементів ELK

```
vitadmin@server-ubuntu2121:~$ sudo systemctl start kibana
vitadmin@server-ubuntu2121:~$ sudo systemctl enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /lib/systemd/system/kibana.service.
vitadmin@server-ubuntu2121:~$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/lib/systemd/system/kibana.service; enabled; vendor preset: enabled)
```

Рисунок 3.1.13 – Встановлення елементів ELK

```

vitadmin@server-ubuntu2121: ~
GNU nano 6.2 /etc/kibana/kibana.yml *
# For more configuration options see the configuration guide for Kibana in
# https://www.elastic.co/guide/index.html

# ===== 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
# The default is 'localhost', which usually means remote machines will not be able
# To allow connections from remote users, set this parameter to a non-loopback
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^_ Replace   ^U Paste     ^J Justify   ^_ Go To Line

```

Рисунок 3.1.14 – Налаштування Kibana

```

vitadmin@server-ubuntu2121:~$ sudo apt update && sudo apt install snort
[sudo] password for vitadmin:
Hit:1 http://ua.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://ua.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://ua.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Get:5 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]

```

Рисунок 3.1.15 – Встановлення Snort

```

Server-Ubuntu-21-2-1 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
Activities  Terminal  Jun 9 09:49

vitadmin@server-ubuntu2121: ~
GNU nano 6.2 /etc/snort/snort.conf *

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 195.24.5.0/30

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

```

Рисунок 3.1.16 – Приклад налаштування Snort

```
alert tcp any any -> any any (msg:"Possible PORT SCAN"; flags:S; threshold:type both, track by_src,
alert ip !$HOME_NET any -> $HOME_NET any (msg:"Possible IP Spoofing"; sid:1002001; rev:1;)
alert udp any any -> $HOME_NET any (msg:" UDP Flood"; detection_filter:track by_src, count 10, seco
```

Рисунок 3.1.17 – Приклад користувацьких правил Snort

На рисунках 3.1.18 – 3.1.30 Показано встановлення та налагодження необхідних компонентів на робочих станціях.

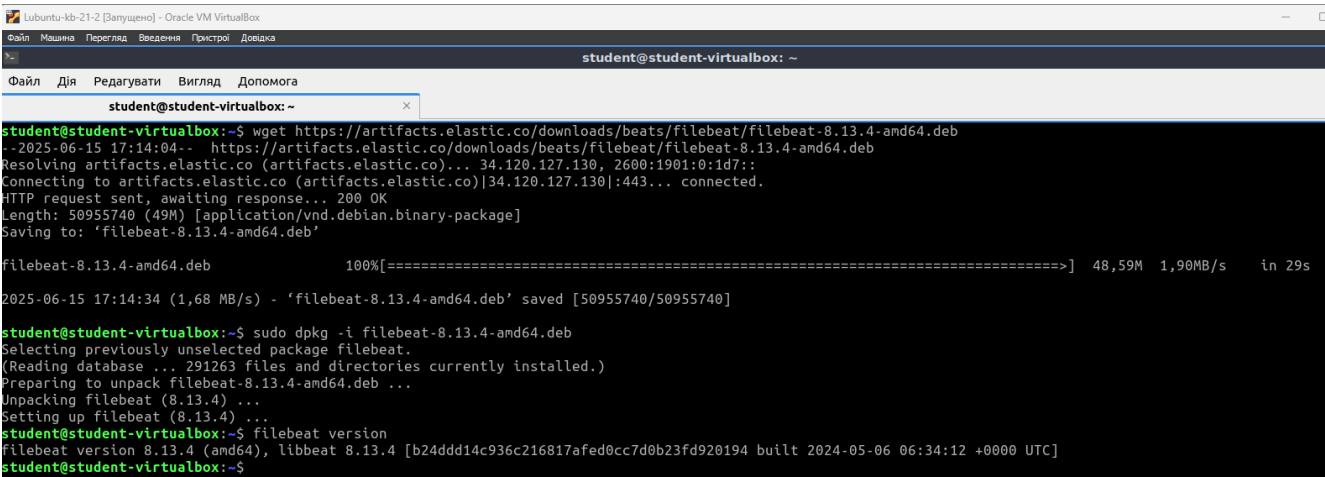


Рисунок 3.1.18 – Встановлення filebeat на робочу станцію Lubuntu ОС

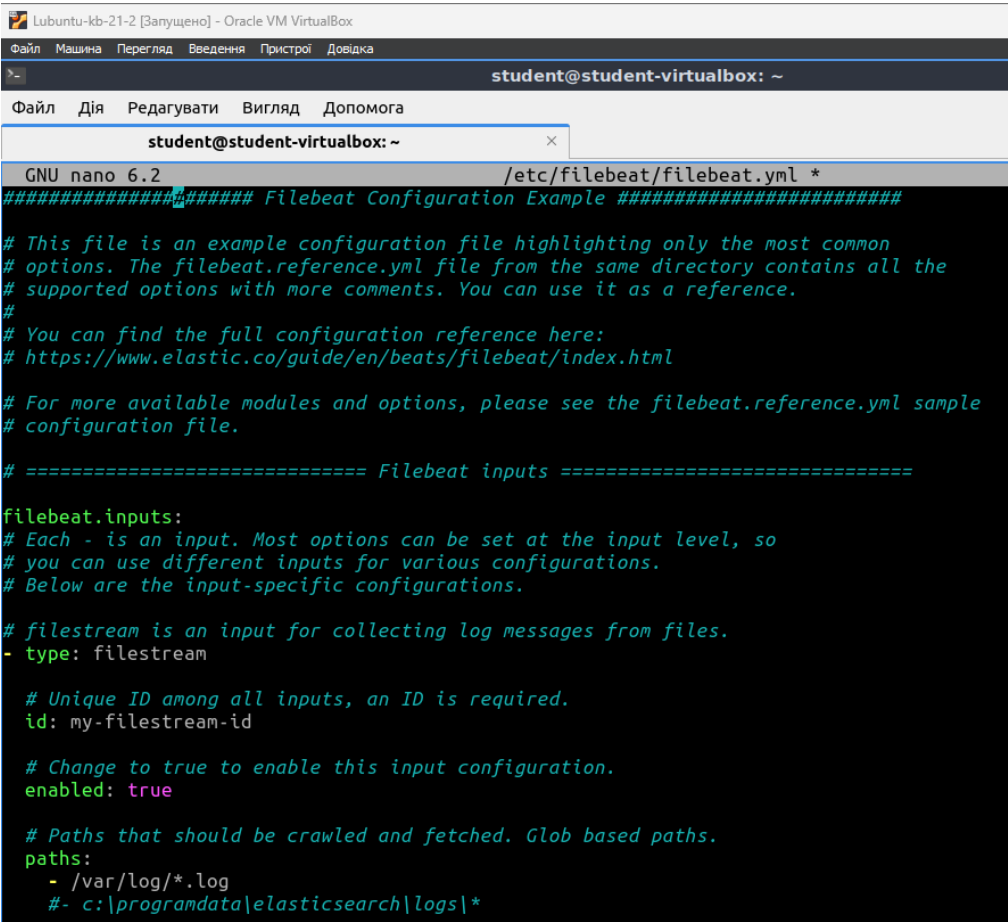


Рисунок 3.1.19 – Налаштування filebeat на робочій станції Lubuntu ОС

```

student@student-virtualbox: ~
GNU nano 6.2 /etc/filebeat/filebeat.yml *
# ----- Logstash Output -----
output.logstash:
# The Logstash hosts
hosts: ["http:192.168.2.2:5044"]

# 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 3.1.20. Налаштування filebeat на робочій станції Lubuntu OS

```

Lubuntu-kb-21-2 [Запущено] - Oracle VM VirtualBox
student@student-virtualbox: ~
student@student-virtualbox: ~
student@student-virtualbox:~$ wget https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-8.14.0-amd64.deb
--2025-06-17 15:08:32-- https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-8.14.0-amd64.deb
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:1901:0:1d7::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 54864866 (52M) [application/vnd.debian.binary-package]
Saving to: 'metricbeat-8.14.0-amd64.deb'

metricbeat-8.14.0-amd64.deb 100%[=====] 52,32M 1,74MB/s in 45s

2025-06-17 15:09:18 (1,16 MB/s) - 'metricbeat-8.14.0-amd64.deb' saved [54864866/54864866]

student@student-virtualbox:~$ sudo dpkg -i metricbeat-8.14.0-amd64.deb
Selecting previously unselected package metricbeat.
(Reading database ... 293485 files and directories currently installed.)
Preparing to unpack metricbeat-8.14.0-amd64.deb ...
Unpacking metricbeat (8.14.0) ...
Setting up metricbeat (8.14.0) ...
student@student-virtualbox:~$

```

Рисунок 3.1.21 – Встановлення metricbeat на робочій станції Lubuntu OS

```

student@student-virtualbox: ~
GNU nano 6.2 /etc/metricbeat/metricbeat.yml *
#username: "elastic"
#password: "changeme"

# ----- Logstash Output -----
output.logstash:
# The Logstash hosts
hosts: ["192.168.2.2:5044"]

```

Рисунок 3.1.22 – Налаштування metricbeat на робочій станції Lubuntu OS

```

Lubuntu-kb-21-2 [Занущено] - Oracle VM VirtualBox
student@student-virtualbox: ~
student@student-virtualbox: ~
student@student-virtualbox:~$ wget https://artifacts.elastic.co/downloads/beats/p
packetbeat/packetbeat-8.14.0-amd64.deb
--2025-06-17 15:10:36-- https://artifacts.elastic.co/downloads/beats/packetbeat/
packetbeat-8.14.0-amd64.deb
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:190
1:0:1d7::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 35194760 (34M) [application/vnd.debian.binary-package]
Saving to: 'packetbeat-8.14.0-amd64.deb'

packetbeat-8.14.0-am 83%[=====>] 28,10M 1,75MB/s eta 3s ^
ketbeat-8.14.0-amd64 87%[=====>] 29,23M 1,99MB/s eta 2s ^
tbeat-8.14.0-amd64.d 89%[=====>] 30,06M 1,85MB/s eta 2s ^
beat-8.14.0-amd64.de 90%[=====>] 30,24M 1,75MB/s eta 2s ^
packetbeat-8.14.0-am 100%[=====>] 33,56M 1,91MB/s in 16s

2025-06-17 15:10:52 (2,16 MB/s) - 'packetbeat-8.14.0-amd64.deb' saved [35194760/3
5194760]

student@student-virtualbox:~$ sudo dpkg -i packetbeat-8.14.0-amd64.deb
Selecting previously unselected package packetbeat.
(Reading database ... 294757 files and directories currently installed.)
Preparing to unpack packetbeat-8.14.0-amd64.deb ...
Unpacking packetbeat (8.14.0) ...
Setting up packetbeat (8.14.0) ...

```

Рисунок 3.1.23 – Встановлення packetbeat на робочій станції Lubuntu ОС

```

student@student-virtualbox: ~
GNU nano 6.2 /etc/packetbeat/packetbeat.yml *
# Pipeline to route events to protocol pipelines.
#pipeline: "packetbeat-{{[agent.version]}}-routing"

# ----- Logstash Output -----
output.logstash:
# The Logstash hosts
hosts: ["192.168.2.2:5044"]

# 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"

# ===== Processors =====

```

Рисунок 3.1.24 – Налаштування metricbeat на робочій станції Lubuntu ОС

```

Hnatiuk V.O. Win2-10-KB-21-2-3 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

Select Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cd 'C:\Program Files\Winlogbeat'
PS C:\Program Files\Winlogbeat> .\install-service-winlogbeat.ps1

Status      Name            DisplayName
-----
Stopped     winlogbeat      winlogbeat

PS C:\Program Files\Winlogbeat>

```

Рисунок 3.1.25 – Встановлення Winlogbeat на робочій станції з Windows ОС

```

Hnatiuk V.O. Win2-10-KB-21-2-3 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

Administrator: Windows PowerShell

PS C:\Program Files\Winlogbeat> Get-WinEvent -ListLog * | Format-List -Property LogName

LogName : Windows PowerShell
LogName : System
LogName : Security
LogName : Key Management Service
LogName : Internet Explorer
LogName : HardwareEvents
LogName : Application
LogName : Windows Networking Vpn Plugin Platform/OperationalVerbose
LogName : Windows Networking Vpn Plugin Platform/Operational
LogName : SMSApi
LogName : Setup
LogName : OpenSSH/Operational
LogName : OpenSSH/Admin
LogName : Network Isolation Operational
LogName : Microsoft-WindowsPhone-Connectivity-WiFiConnSvc-Channel

```

Рисунок 3.1.26 – Перегляд списку назв подій

```
winlogbeat.yml: Блокнот
Файл Редагування Формат Вигляд Довідка
# ignore_older, level, event_id, or provider keys. Please visit the
# documentation for the complete details of each option.
# https://go.es.io/WinlogbeatConfig

winlogbeat.event_logs:
- name: Application
  tags: ["win-app-event"]
  ignore_older: 72h
- name: System
  tags: ["win-system-event"]
  level: critical, error, warning
- name: Security
  tags: ["win-security-event"]
  level: critical, error, warning
- name: Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
- name: Microsoft-Windows-Sysmon/Operational
- name: Windows PowerShell
  event_id: 400, 403, 600, 800
- name: Microsoft-Windows-PowerShell/Operational
  event_id: 4103, 4104, 4105, 4106
- name: ForwardedEvents
  tags: [forwarded]
```

Рисунок 3.1.27 – Налаштування Winlogbeat на робочій станції з Windows ОС

```
# ===== 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: ["https://192.168.2.2:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "changeme"

  # Pipeline to route events to security, sysmon, or powershell pipelines.
  pipeline: "winlogbeat-%[agent.version]}-routing"
  index: "%[agent.name]}-winlogbeat-%{yyyy.MM.dd}"
```

Рисунок 3.1.28 – Налаштування Winlogbeat на робочій станції з Windows ОС

```
Administrator: C:\Program Files\PowerShell\7\pwsh.exe
PowerShell 7.5.1
PS C:\Windows\System32> cd 'C:\Program Files\Metricbeat\'
PS C:\Program Files\Metricbeat> .\install-service-metricbeat.ps1

Status      Name      DisplayName
-----
Stopped     metricbeat      metricbeat

PS C:\Program Files\Metricbeat>
```

Рисунок 3.1.29 – Інсталяція Metricbeat на робочій станції з Windows ОС

```

Administrator: C:\Program Files\PowerShell\7\powershell.exe
PS C:\> cd 'C:\Program Files\Packetbeat\'
PS C:\Program Files\Packetbeat> .\install-service-packetbeat.ps1

Status      Name            DisplayName
-----
Stopped     packetbeat      packetbeat

PS C:\Program Files\Packetbeat>

```

Рисунок 3.1.30 – Інсталяція Packetbeat на робочій станції з Windows ОС

Для збору інформації з певних джерел в мережі було застосовано logstash. На рисунках 3.1.31 – 3.1.34 наведено приклади конфігурацій logstash.

```

GNU nano 6.2 /etc/logstash/conf.d/beats.conf
input {
  beats {
    port => 5044
  }
}

filter {
  if [agent][type] == "metricbeat" {
    mutate { add_tag => ["from_metricbeat"] }
  }
  if [agent][type] == "filebeat" {
    mutate { add_tag => ["from_filebeat"] }
  }
  if [agent][type] == "packetbeat" {
    mutate { add_tag => ["from_packetbeat"]}
  }
}

output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "beats-lubuntu-%{+YYYY.MM.dd}"
  }
}

```

Рисунок 3.1.31. Приклад конфігураційного файлу logstash для отримання даних з Beat-агентів

```

vitadmin@server-ubuntu2121: ~
GNU nano 6.2 /etc/logstash/conf.d/snort-port-scan.conf
input {
  file {
    path => "/var/log/snort/alert"
    start_position => "beginning"
    sincedb_path => "/dev/null"
    codec => plain
  }
}

filter {
}

output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "snort-%{+YYYY.MM.dd}"
  }
  stdout { codec => rubydebug }
}

```

Рисунок 3.1.32 – Приклад конфігурації Logstash для приймання повідомлень від Snort

```

vitadmin@server-ubuntu2121: ~
GNU nano 6.2 /etc/logstash/conf.d/netflow.conf
input {
  udp {
    port => 2055
    codec => netflow {
      versions => [5, 9]
    }
    type => "netflow"
  }
}

filter {}

output {
  if [type] == "netflow" {
    elasticsearch {
      hosts => ["http://localhost:9200"]
      index => "netflow-%{+YYYY.MM.dd}"
    }
    stdout {
      codec => rubydebug
    }
  }
}

```

Рисунок 3.1.33 – Приклад конфігурації Logstash для взаємодії з NetFlow

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

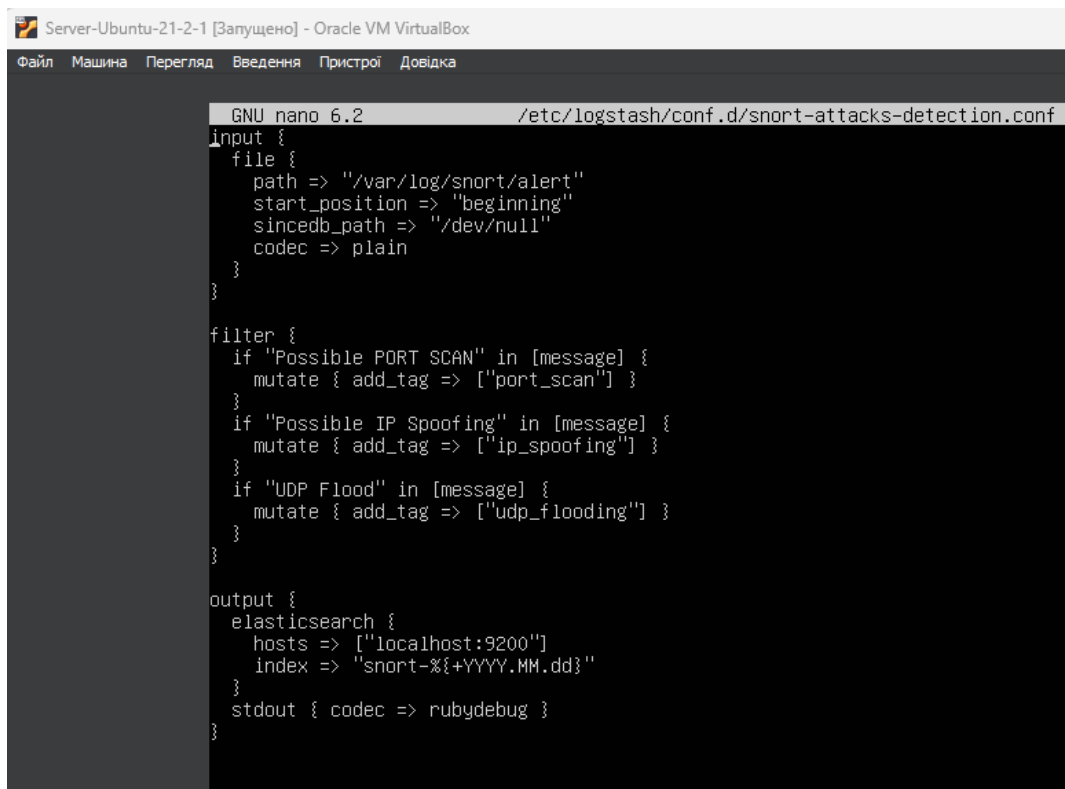


Рисунок 3.1.34 – Приклад конфігурації logstash для отримання даних про різні атаки

3.3. Тестування спроектованої системи

Проводимо тестування роботи системи та її компонентів.

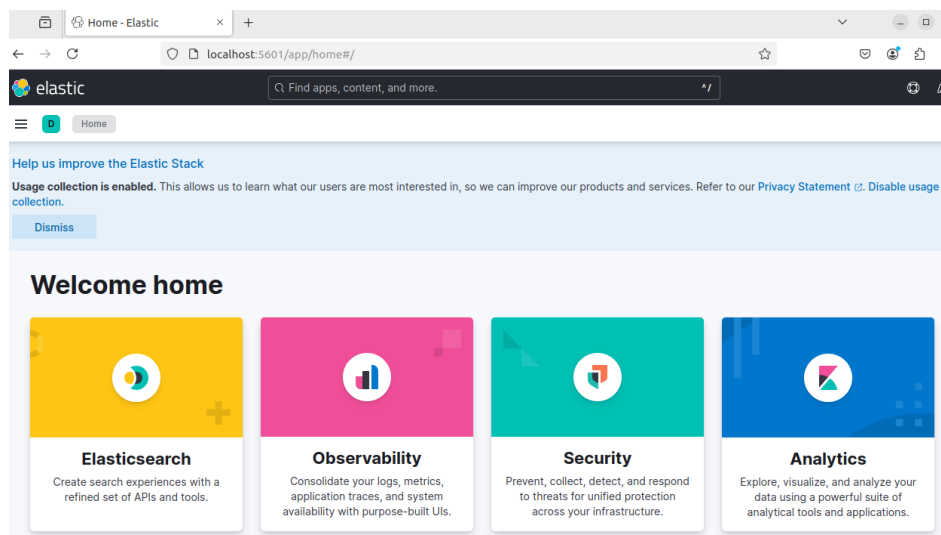


Рисунок 3.2.1 – Вхід в Kibana

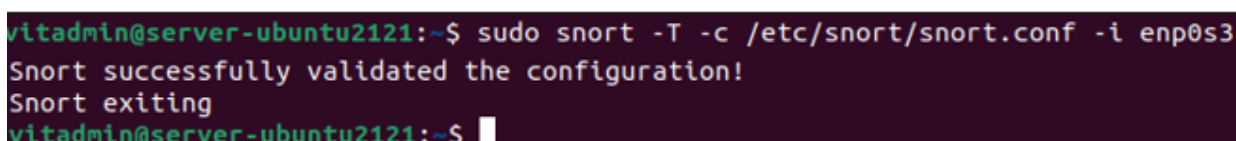


Рисунок 3.2.2 – Перевірка конфігурації Snort

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

```

vitadmin@server-ubuntu2121:~$ sudo snort -v -i enp0s3
Running in packet dump mode

--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet

--== Initialization Complete ==--

    ,'-
o"  )~
    '""

-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.

Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Commencing packet processing (pid=3800)

WARNING: No preprocessors configured for policy 0.
02/02-02:02:47.940152 10.0.2.15 -> 8.8.8.8
ICMP TTL:64 TOS:0x0 ID:29308 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:1 Seq:1 ECHO
+++++

```

Рисунок 3.2.3 – Перевірка роботи Snort

```

vitadmin@server-ubuntu2121:~$ sudo tail -f /var/log/snort/alert
02/02-03:44:05.686449  [**] [1:1000001:1] ICMP Echo Request Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 8.8.8.8
02/02-03:44:05.740545  [**] [1:1000001:1] ICMP Echo Request Detected [**] [Priority: 0] {ICMP} 8.8.8.8 -> 10.0.2.15
02/02-03:44:53.068999  [**] [1:1000001:1] ICMP Echo Request Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 8.8.8.8
02/02-03:44:53.176295  [**] [1:1000001:1] ICMP Echo Request Detected [**] [Priority: 0] {ICMP} 8.8.8.8 -> 10.0.2.15
02/02-03:44:54.070054  [**] [1:1000001:1] ICMP Echo Request Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 8.8.8.8
02/02-03:44:54.109204  [**] [1:1000001:1] ICMP Echo Request Detected [**] [Priority: 0] {ICMP} 8.8.8.8 -> 10.0.2.15
02/02-03:44:55.071599  [**] [1:1000001:1] ICMP Echo Request Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 8.8.8.8
02/02-03:44:55.110926  [**] [1:1000001:1] ICMP Echo Request Detected [**] [Priority: 0] {ICMP} 8.8.8.8 -> 10.0.2.15
02/02-03:44:56.072579  [**] [1:1000001:1] ICMP Echo Request Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 8.8.8.8
02/02-03:44:56.115699  [**] [1:1000001:1] ICMP Echo Request Detected [**] [Priority: 0] {ICMP} 8.8.8.8 -> 10.0.2.15

```

Рисунок 3.2.4 – Перегляд повідомлень Snort

Для перевірки взаємодії системи разом із Snort було проведено декілька атак. Після проведення збору даних було здійснено вхід в Kibana де було протестовано можливості графічного представлення даних.

		Гнатюк В. О.			<i>ККІКБ.КР.Б – 125 – 05 – ПЗ</i>	Арк.
		Єфіменко А. А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

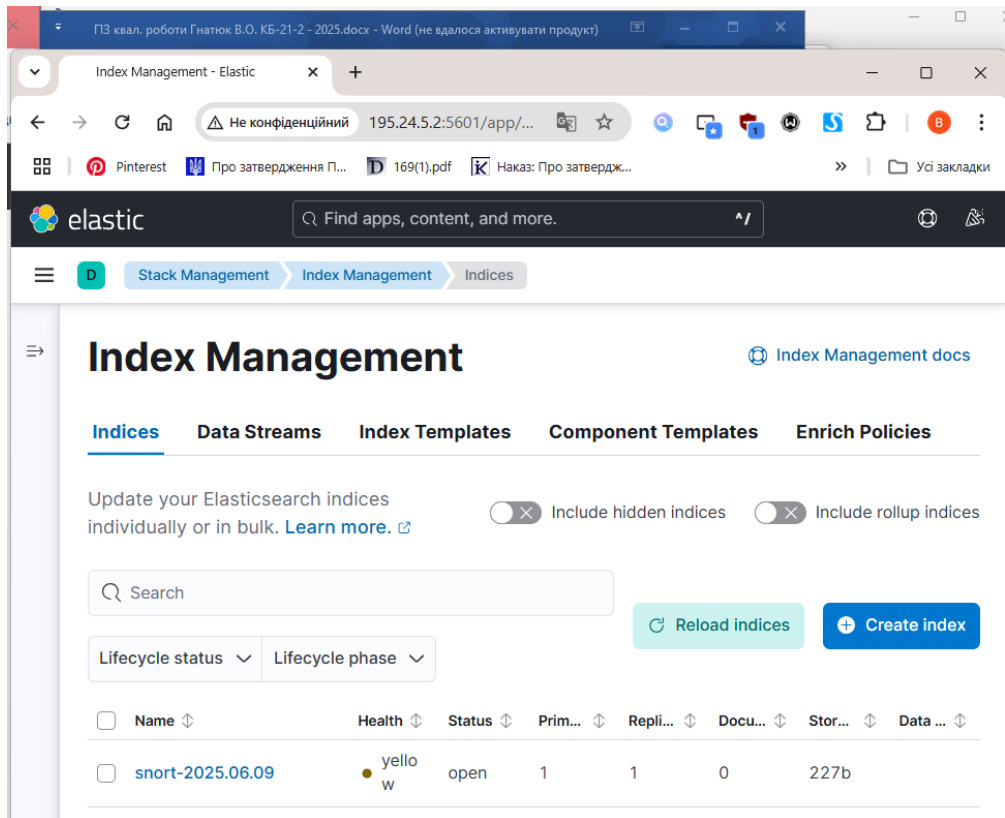


Рисунок 3.2.5 – Перегляд автоматично створеного індексу при атаці Port Scanning

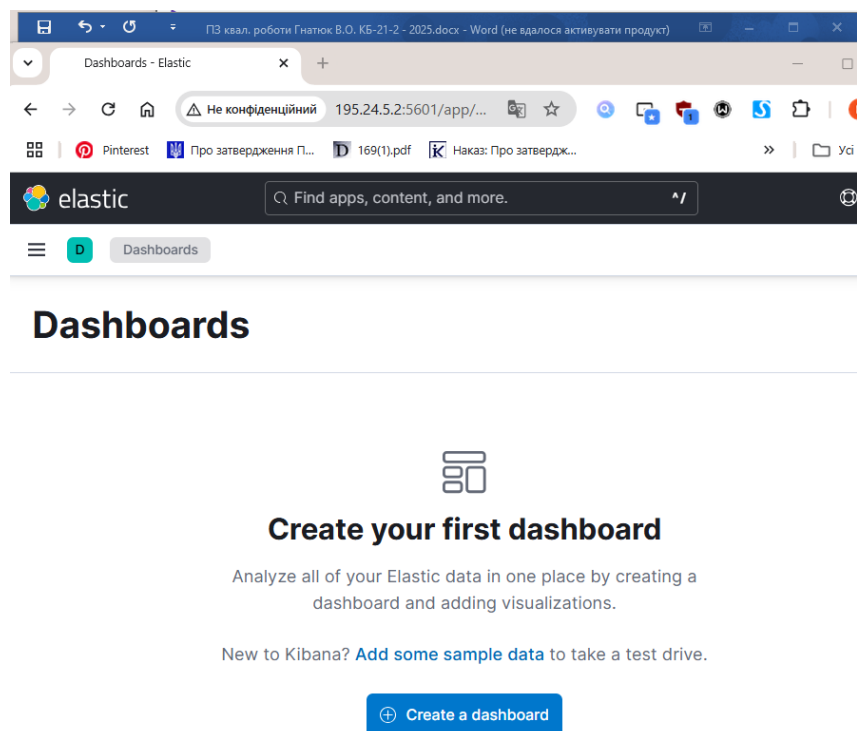


Рисунок 3.2.6 – Приклад створення дашборда

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

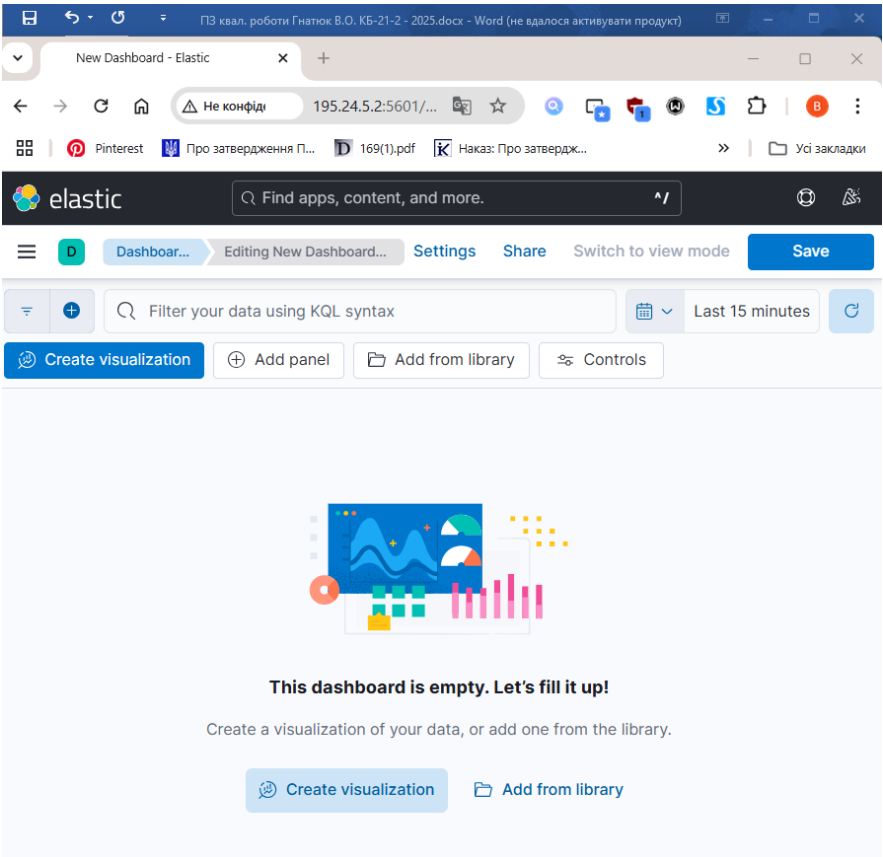


Рисунок 3.2.7 – Приклад створення дашборда

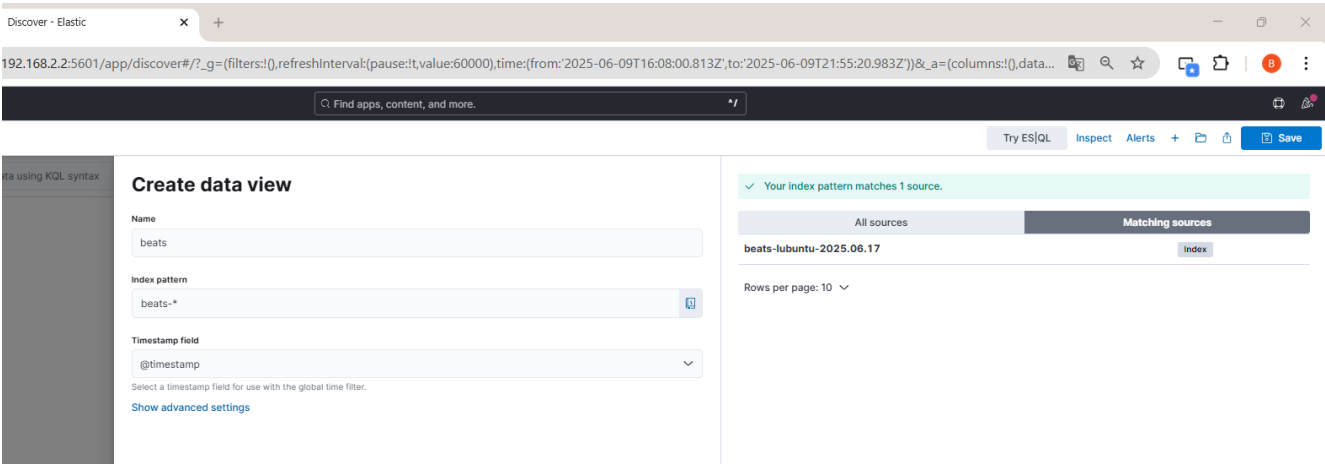


Рисунок 3.2.8 – Створення представлення даних

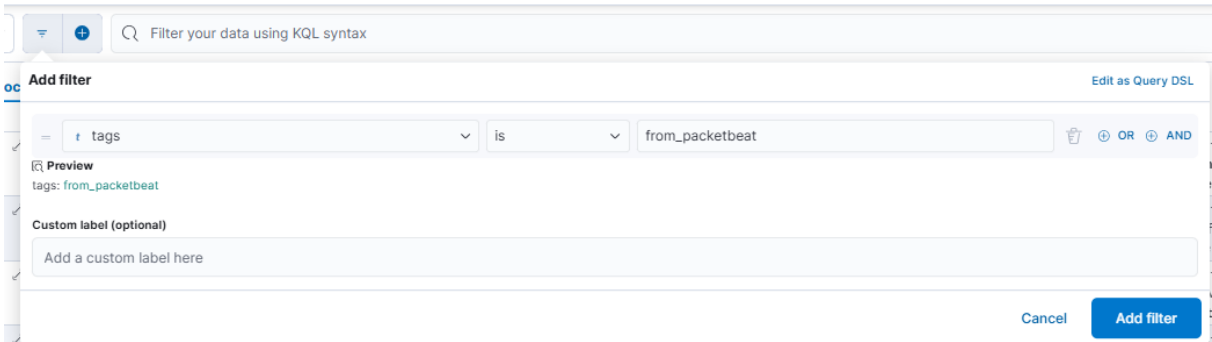
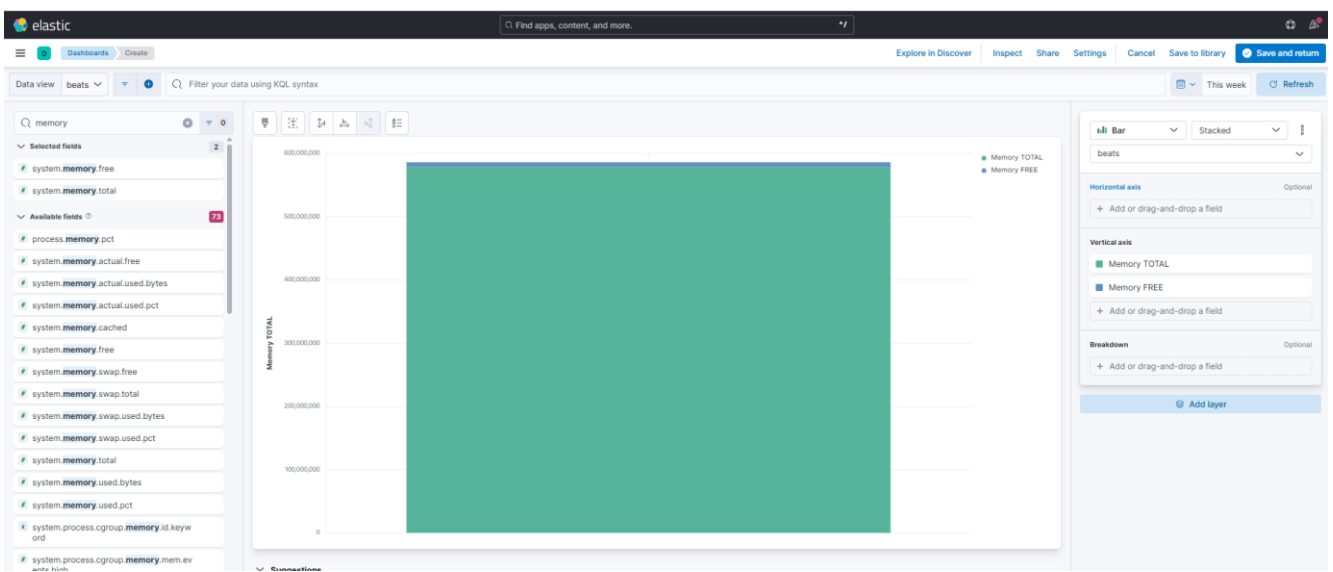
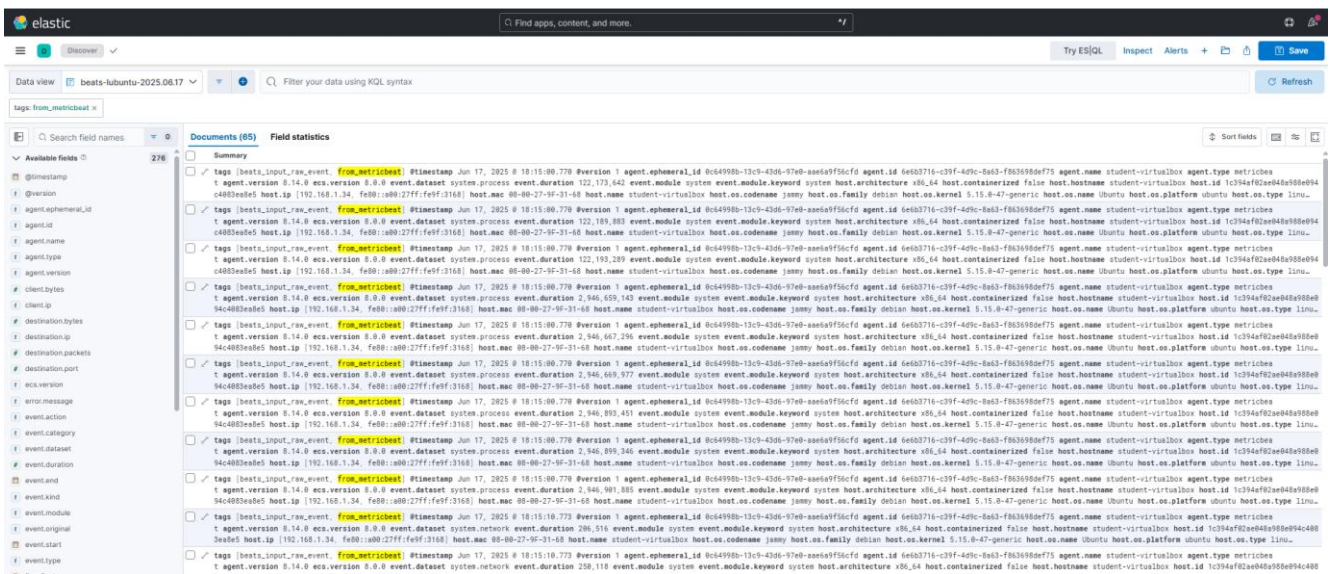
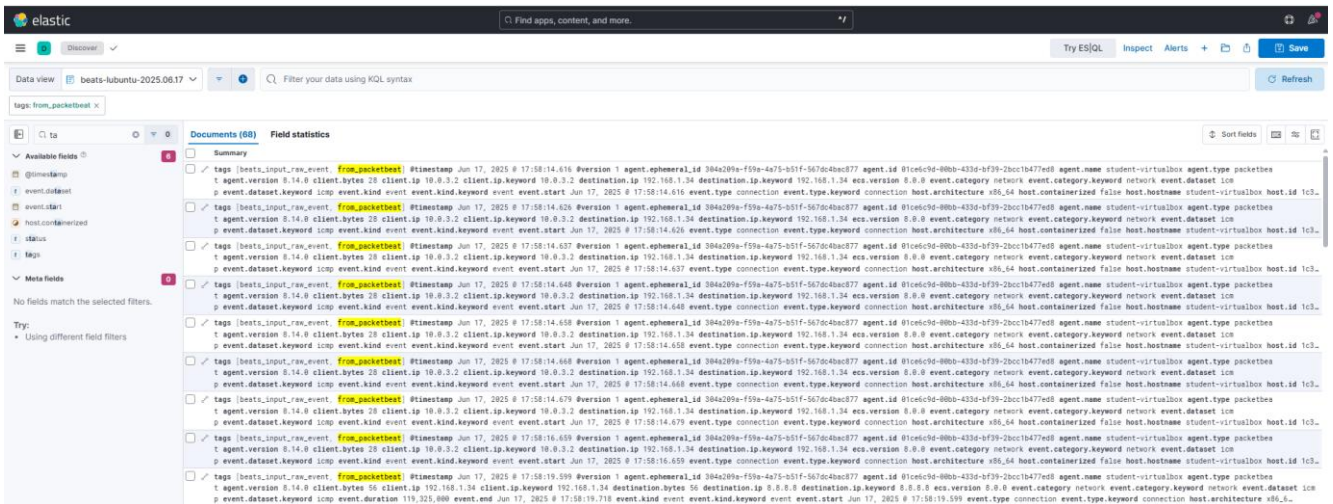


Рисунок 3.2.9 – Перевірка використання тегу

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				75
Змн.	Арк.	№ докум.	Підпис	Дата		



		Гнатюк В. О.			<i>ККИКБ.КР.Б – 125 – 05 – ПЗ</i>	<i>Арк.</i>
		Єфіменко А. А.				76
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		

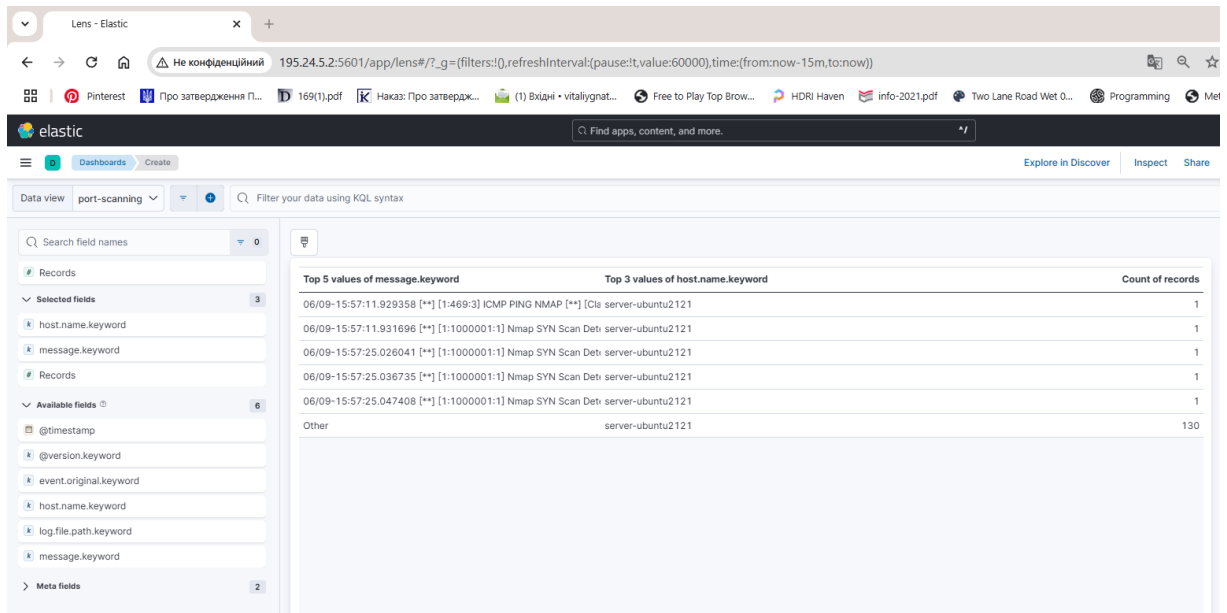


Рисунок 3.2.13 – Створення діаграми у вигляді таблиці

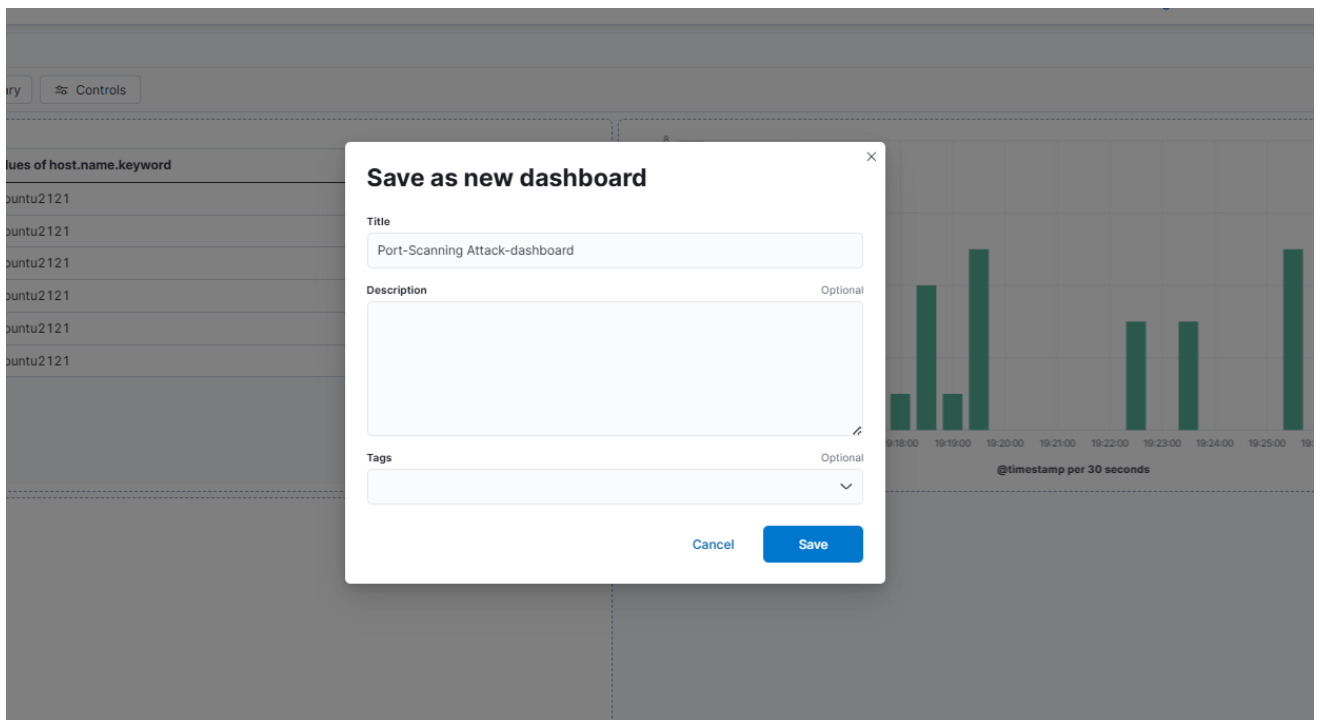


Рисунок 3.2.14 – Збереження дашборда

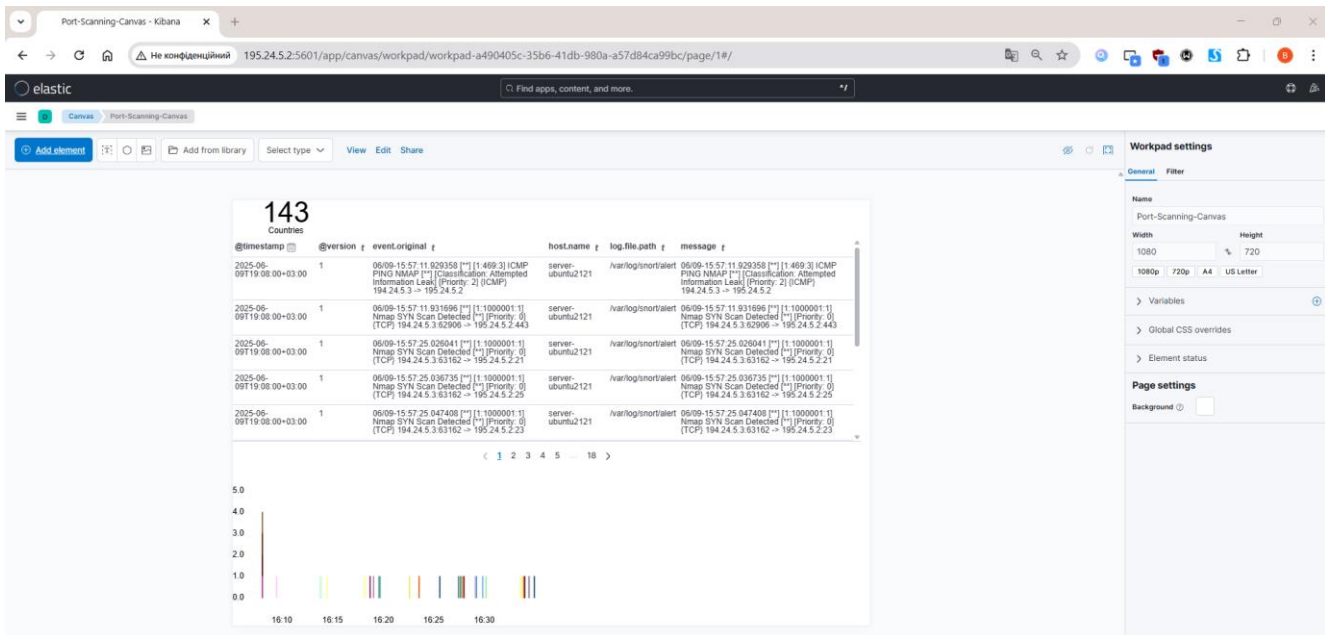


Рисунок 3.2.15 – Перегляд робочої панелі

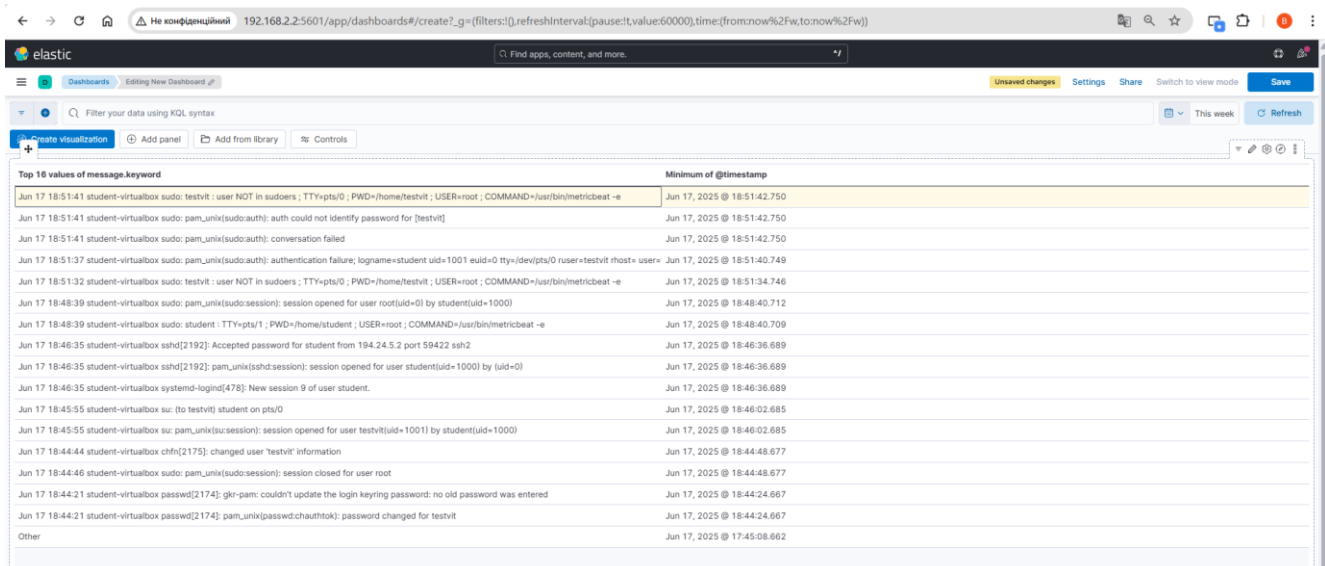


Рисунок 3.2.16 – Перегляд даних отриманих від filebeat

Далі моделюємо атаку на систему з машини порушника. В результаті в системі моніторингу фіксуються аномальні події. Це дозволяє перевірити ефективність налаштувань обробки подібного роду атак у середовищі Elastic Stack.

```

Kali-linux-kb-21-2 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
(kali♦ kali)-[~]
$ sudo nmap -sS -p 1-100 -T4 195.24.5.2
Starting Nmap 7.94 ( https://nmap.org ) at 2025-06-09 11:57 EDT
Nmap scan report for 195.24.5.2
Host is up (0.56s latency).
Not shown: 98 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds
(kali♦ kali)-[~]
$

```

Рисунок 3.2.17 – Проведення сканування портів

```

Kali-linux-kb-21-2 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
(kali♦ kali)-[~]
$ sudo hping3 -a 1.2.3.4 -S -p 80 195.24.5.2
[sudo] password for kali:
HPING 195.24.5.2 (eth0 195.24.5.2): S set, 40 headers + 0 data bytes
^C
--- 195.24.5.2 hping statistic ---
15 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(kali♦ kali)-[~]
$

```

Рисунок 3.2.18 – Проведення IP Spoofing атаки

```

vitadmin@server-ubuntu2121: ~
vitadmin@server-ubuntu2121:~$ sudo tail /var/log/snort/alert
06/09-18:16:41.403110  [**] [1:1002001:1] [SPOOFING] Suspicious external IP traffic [**] [Priority: 0] (TCP) 194.24.5.5:49787 -> 195.24.5.2:22
06/09-18:16:41.532057  [**] [1:1002001:1] [SPOOFING] Suspicious external IP traffic [**] [Priority: 0] (TCP) 194.24.5.5:49787 -> 195.24.5.2:22
06/09-18:16:41.599978  [**] [1:1002001:1] [SPOOFING] Suspicious external IP traffic [**] [Priority: 0] (TCP) 194.24.5.5:49787 -> 195.24.5.2:22
06/09-18:16:41.642239  [**] [1:1002001:1] [SPOOFING] Suspicious external IP traffic [**] [Priority: 0] (TCP) 194.24.5.5:49787 -> 195.24.5.2:22
06/09-18:16:41.865636  [**] [1:1002001:1] [SPOOFING] Suspicious external IP traffic [**] [Priority: 0] (TCP) 194.24.5.5:49787 -> 195.24.5.2:22
06/09-18:16:41.994130  [**] [1:1002001:1] [SPOOFING] Suspicious external IP traffic [**] [Priority: 0] (TCP) 194.24.5.5:49787 -> 195.24.5.2:22
06/09-18:16:42.069324  [**] [1:1002001:1] [SPOOFING] Suspicious external IP traffic [**] [Priority: 0] (TCP) 194.24.5.5:49787 -> 195.24.5.2:22
06/09-18:16:42.166381  [**] [1:1002001:1] [SPOOFING] Suspicious external IP traffic [**] [Priority: 0] (TCP) 194.24.5.5:49787 -> 195.24.5.2:22
06/09-18:16:42.467851  [**] [1:1002001:1] [SPOOFING] Suspicious external IP traffic [**] [Priority: 0] (TCP) 194.24.5.5:49787 -> 195.24.5.2:22
06/09-18:16:42.576439  [**] [1:1002001:1] [SPOOFING] Suspicious external IP traffic [**] [Priority: 0] (TCP) 194.24.5.5:49787 -> 195.24.5.2:22
vitadmin@server-ubuntu2121:~$

```

Рисунок 3.2.19 – Виявлення атаки в Snort

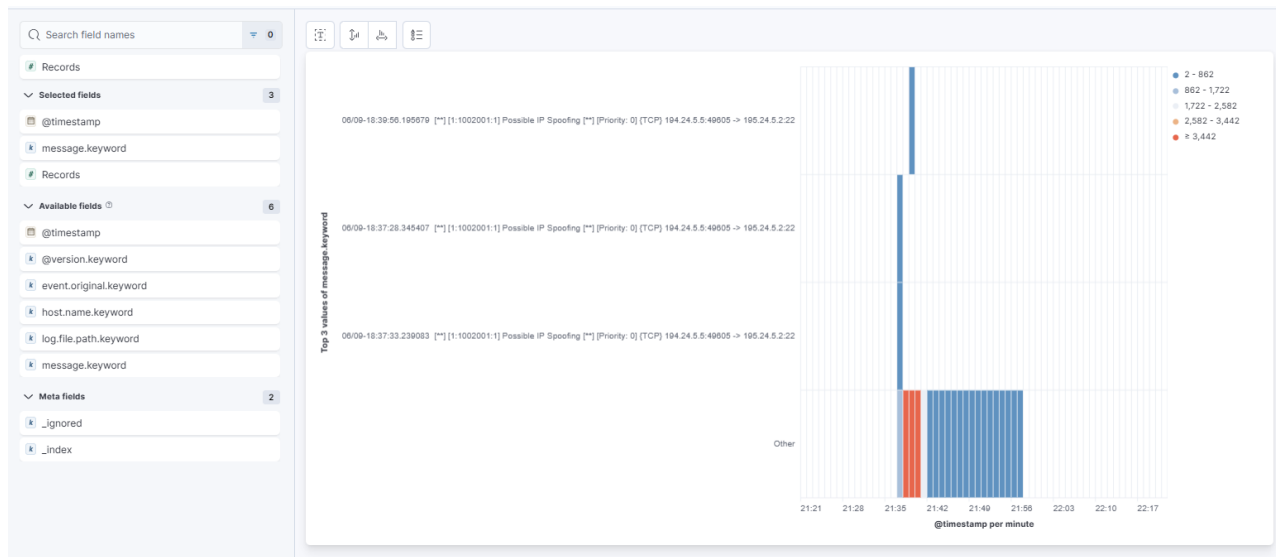


Рисунок 3.2.20 – Приклад створення діаграми з даними про IP Spoofing

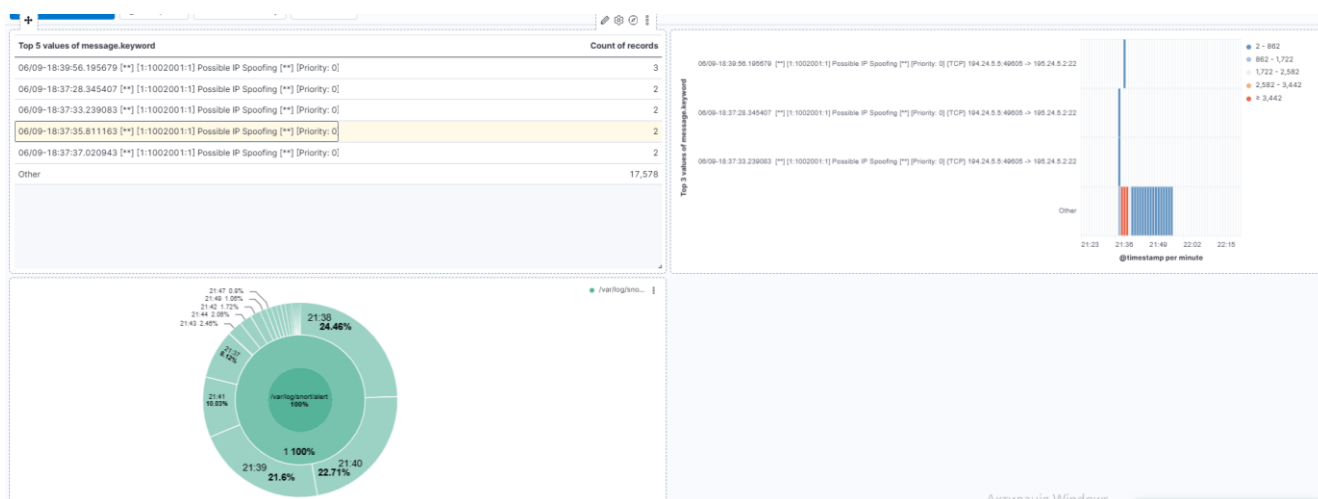


Рисунок 3.2.21 – Приклад створення дашборду з даними про IP Spoofing

Далі на рисунках 3.2.22 – 3.2.29. можна побачити приклад створення правил в Kibana для виявлення атак. Для показаного правила умови спрацювання формулюємо на основі високої кількості однотипних повідомлення, що надходять за короткий проміжок часу. Визначаємо порогові значення для кількості подій та обмежуємо час спостереження, щоб уникнути хибних спрацьовувань. Після збереження правила перевіряємо його роботу.

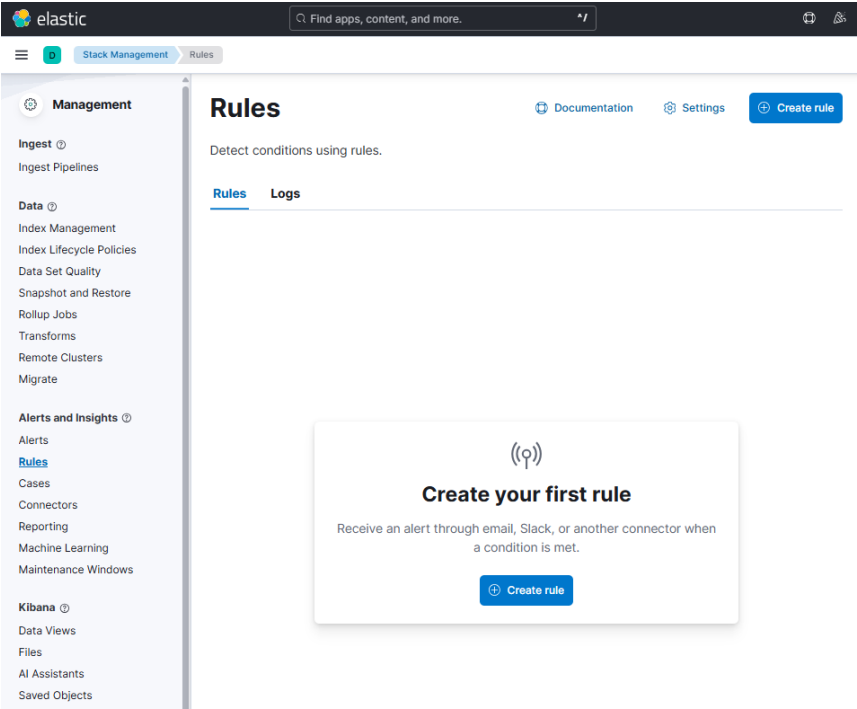


Рисунок 3.2.22 – Створення правила в Kibana

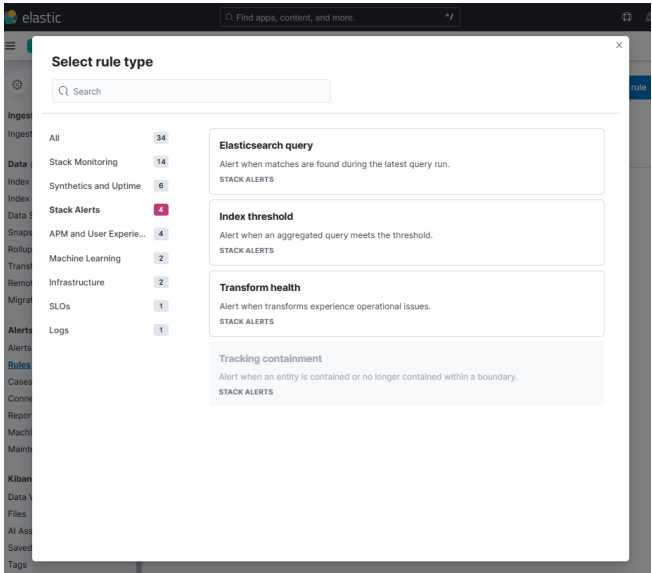


Рисунок 3.2.23 – Вибір типу правила

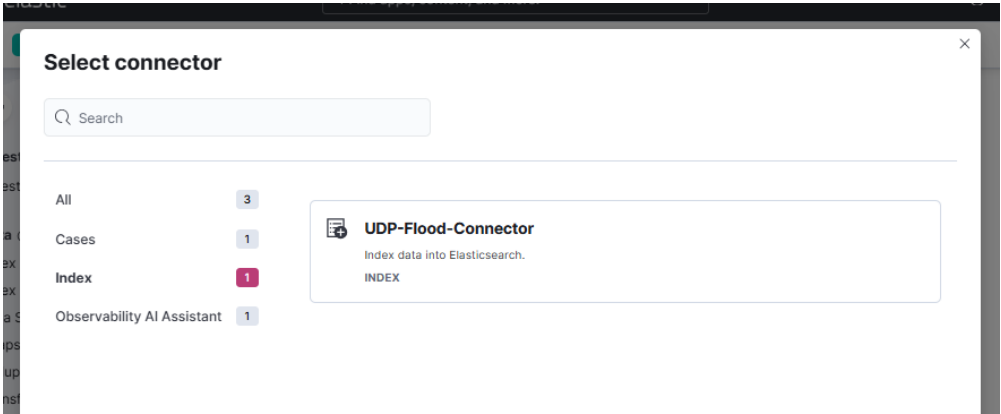


Рисунок 3.2.24 – Вибір конектора

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

Edit filter

Edit as Query DSL

tags

is

udp_flooding

OR

AND

Preview

tags: udp_flooding

Custom label (optional)

Add a custom label here

Cancel

Update filter

Рисунок 3.2.25 – Налаштування правила

1 Rule definition

Elasticsearch query

Alert when matches are found during the latest query run.

View documentation

KQL or Lucene

Use KQL or Lucene to define a text-based query.

Select a data view

DATA VIEW UDP-Flooding

Define your query

Filter your data using KQL syntax

tags: udp_flooding

Set the group, threshold, and time window

WHEN count()

OVER all documents

IS ABOVE 1000

FOR THE LAST 5 hours

Set the number of documents to send

SIZE 100

Exclude matches from previous runs

Add more fields to alert details

host.name

Test query

Copy query

Query matched 366 documents in the last 5h.

Rule schedule

Set the frequency to check the alert conditions

Every

1

minute

Rule scope

Select the applications to associate the corresponding role privilege

Role visibility

Logs

Advanced options

2 Actions

UDP-Flood-Connector

Index

Run when query matched

Add action

3 Rule details

Rule name and tags

Define a name and tags for your rule.

Rule name

UDP-FloodRule

Рисунок 3.2.28 – Налаштування правила

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

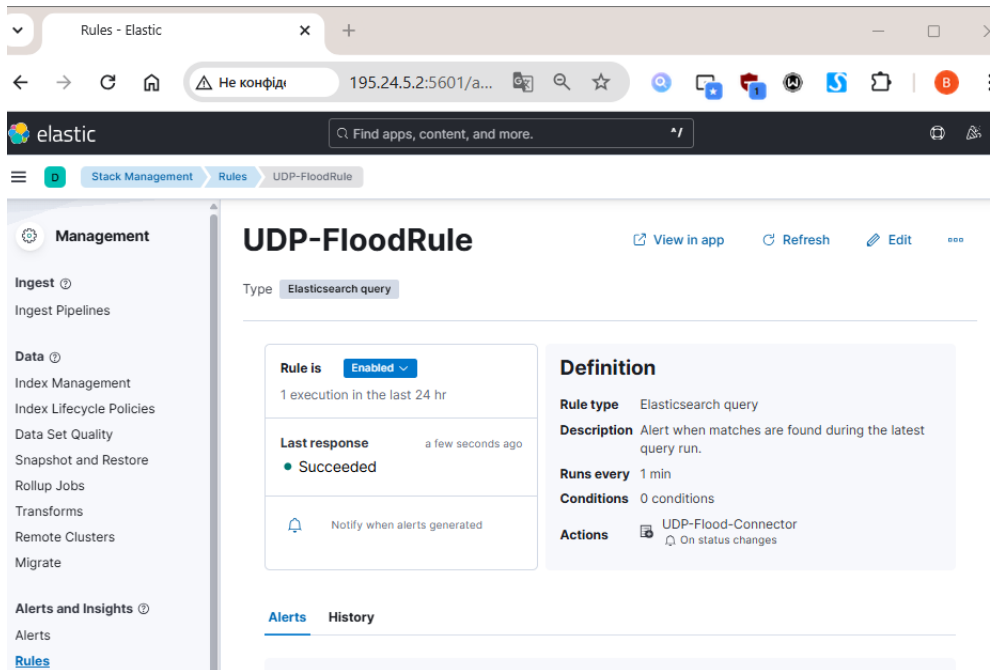


Рисунок 3.2.29. Перегляд створеного правила

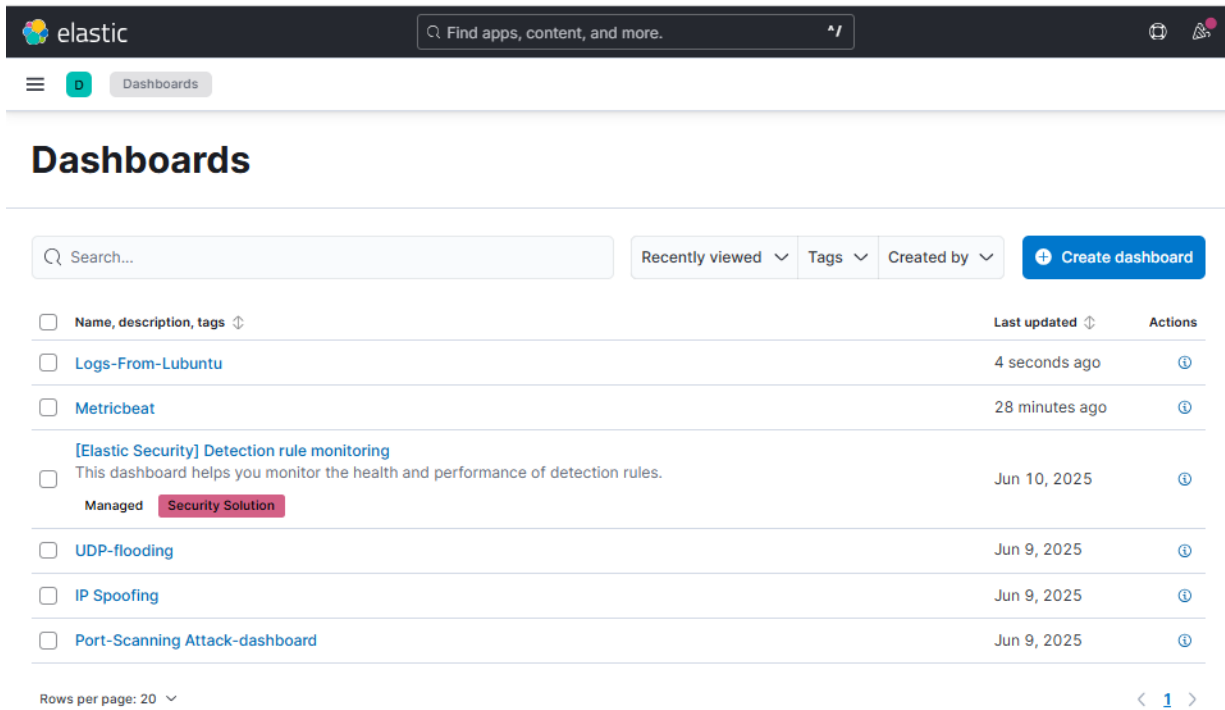


Рисунок 3.2.30 – Перегляд створених дашбордів

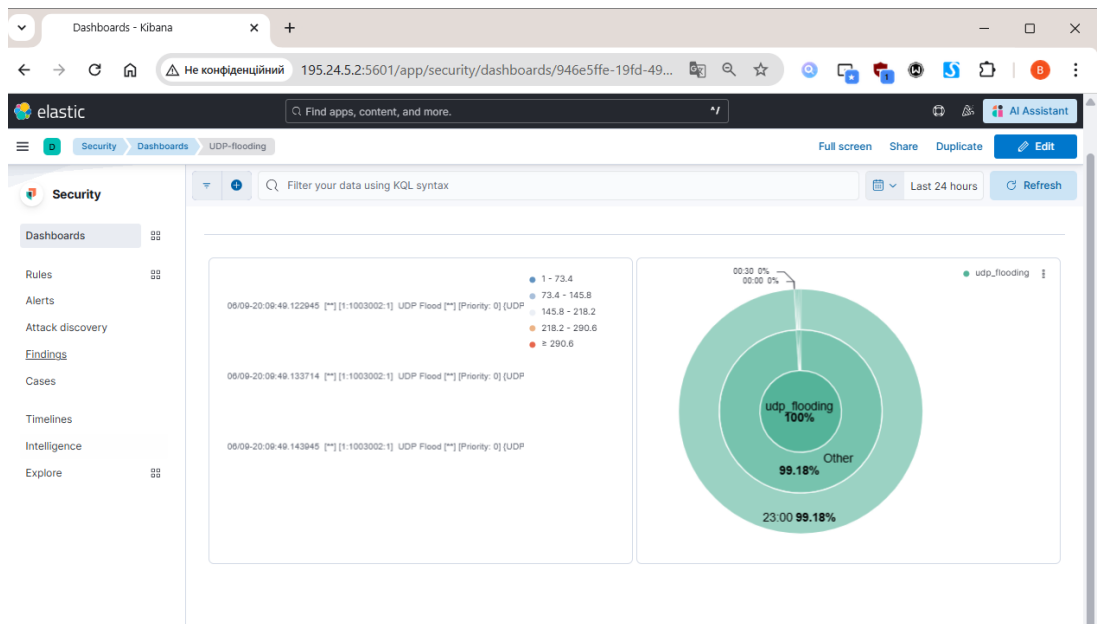


Рисунок 3.2.31 – Перегляд вручну створеного дашборду

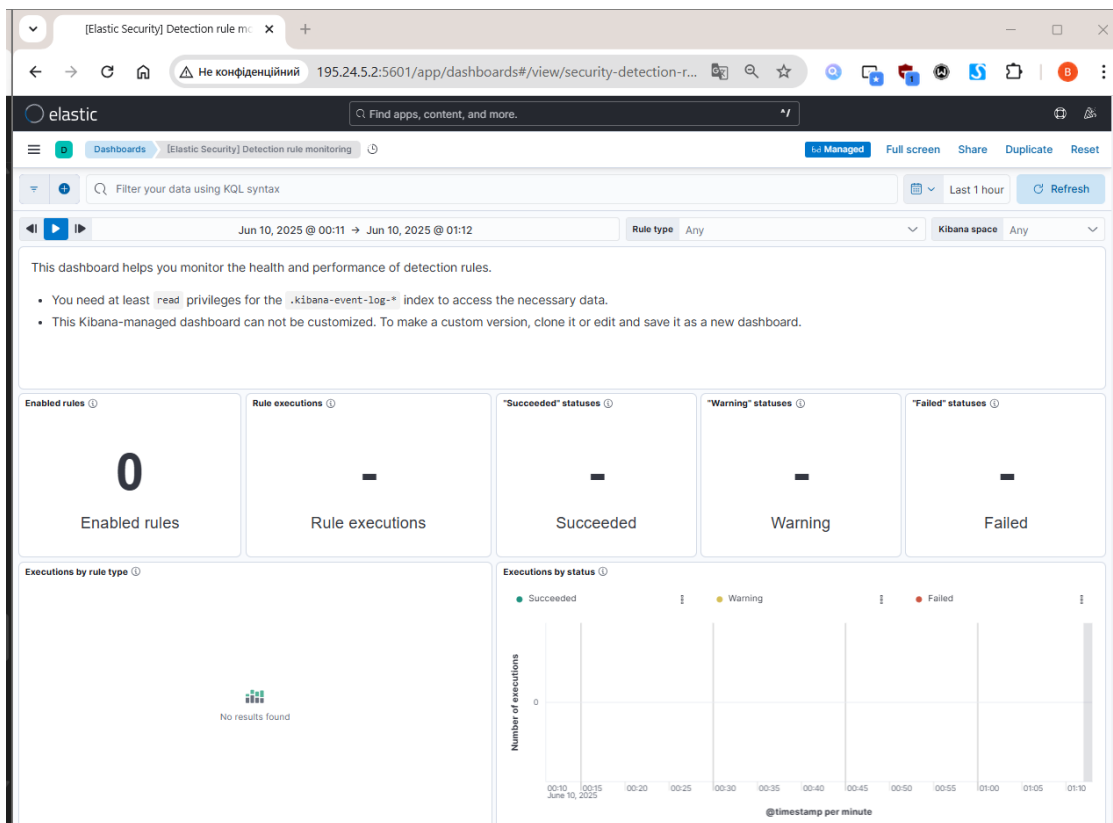


Рисунок 3.2.32. Перегляд автоматично створеного дашборду

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

Index Management

[Index Management docs](#)

[Indices](#) [Data Streams](#) [Index Templates](#) [Component Templates](#) [Enrich Policies](#)

Update your Elasticsearch indices individually or in bulk. [Learn more.](#)

☐ Include hidden indices ☐ Include rollup indices

Search

Lifecycle status

Lifecycle phase

Reload indices

Create index

Name	Health	Status	Primar...	Replic...	Docu...	Stora...	Data s...
beats-lubuntu-2025.06.17	yellow	open	1	1	3 422	3.04mb	
filebeat-lubuntu-2025.06.17	yellow	open	1	1	25 281	6.96mb	
netflow-2002.03.01	yellow	open	1	1	6	33.96kb	
snort-2025.06.09	yellow	open	1	1	19 160	3.08mb	
udp-flooding	yellow	open	1	1	5	20.48kb	

Rows per page: 10

<

1

>

Рис. 3.2.33. Перегляд створених індексів

3.3. Налаштування захисту

Після аналізу результатів атак переходимо до налаштування захисту. Вносимо відповідні зміни до конфігурації брандмауера та систем виявлення вторгнень. Після впровадження захисних заходів повторюємо атаки, щоб переконатися в ефективності налаштувань.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

```
Server-Ubuntu-21-2-1 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
vitadmin@server-ubuntu2121:~$ sudo ufw enable
[sudo] password for vitadmin:
Firewall is active and enabled on system startup
vitadmin@server-ubuntu2121:~$ sudo ufw allow 22/tcp
Rule added
Rule added (v6)
vitadmin@server-ubuntu2121:~$ sudo ufw allow 80/tcp
Rule added
Rule added (v6)
vitadmin@server-ubuntu2121:~$ sudo ufw allow 443/tcp
Rule added
Rule added (v6)
vitadmin@server-ubuntu2121:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
vitadmin@server-ubuntu2121:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
vitadmin@server-ubuntu2121:~$ _
```

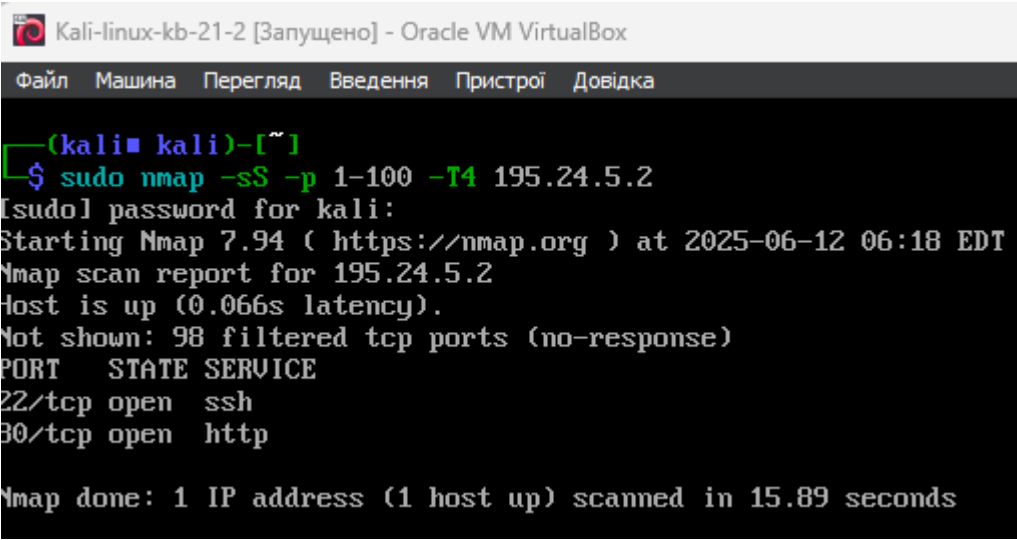
Рисунок 3.3.1 – Налаштування фаєрволу для захисту від атак

```
Server-Ubuntu-21-2-1 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
GNU nano 6.2 /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse lookup)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1
```

Рисунок 3.3.2. – Налаштування захисту від спуфінгу

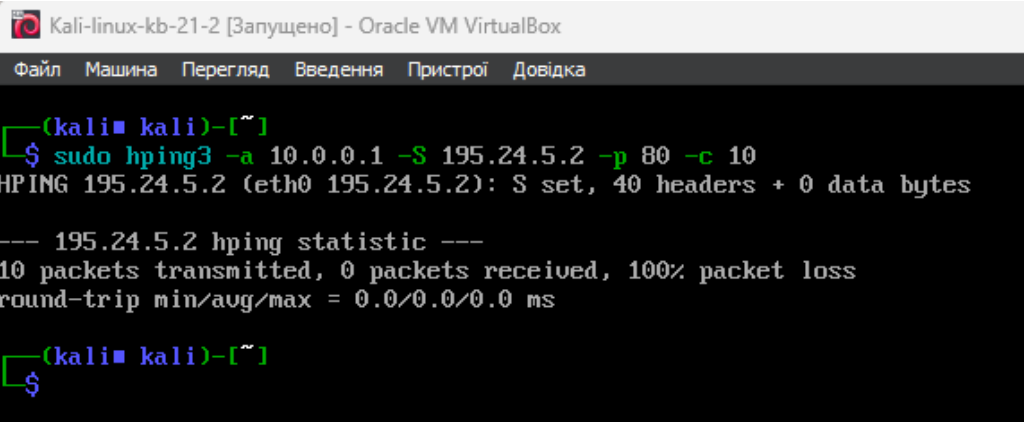
```
Server-Ubuntu-21-2-1 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
vitadmin@server-ubuntu2121:~$ sudo nft add table inet filter
vitadmin@server-ubuntu2121:~$ sudo nft add chain inet filter input {type filter hook input priority
0 \; }
vitadmin@server-ubuntu2121:~$ sudo nft add rule inet filter input ip protocol udp limit rate 20/second burst 40 packets accept
vitadmin@server-ubuntu2121:~$ sudo nft add rule inet filter input ip protocol udp drop
vitadmin@server-ubuntu2121:~$ _
```

Рисунок 3.3.3 – Налаштування захисту від UDP Flood



```
(kali~ kali)-[~]
$ sudo nmap -sS -p 1-100 -T4 195.24.5.2
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2025-06-12 06:18 EDT
Nmap scan report for 195.24.5.2
Host is up (0.066s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 15.89 seconds
```

Рисунок 3.3.4 – Повторне проведення атаки Port Scanning

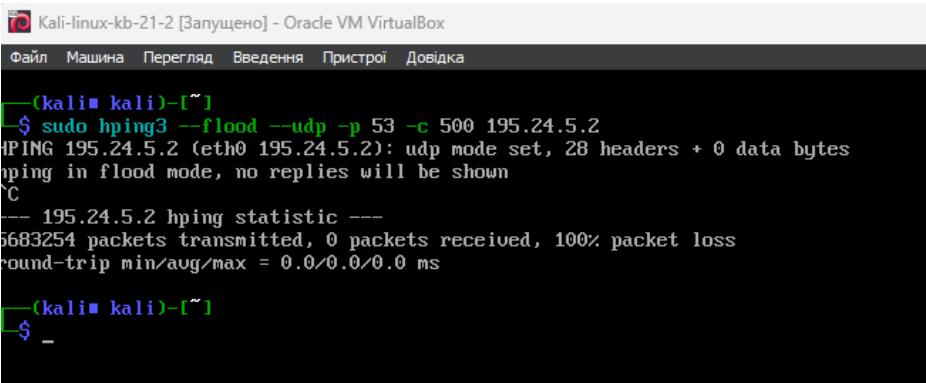


```
(kali~ kali)-[~]
$ sudo hping3 -a 10.0.0.1 -S 195.24.5.2 -p 80 -c 10
HPING 195.24.5.2 (eth0 195.24.5.2): S set, 40 headers + 0 data bytes

--- 195.24.5.2 hping statistic ---
10 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali~ kali)-[~]
$
```

Рисунок 3.3.5 – Повторне проведення атаки IP Spoofing



```
(kali~ kali)-[~]
$ sudo hping3 --flood --udp -p 53 -c 500 195.24.5.2
HPING 195.24.5.2 (eth0 195.24.5.2): udp mode set, 28 headers + 0 data bytes
ping in flood mode, no replies will be shown
^C
--- 195.24.5.2 hping statistic ---
6683254 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali~ kali)-[~]
$ _
```

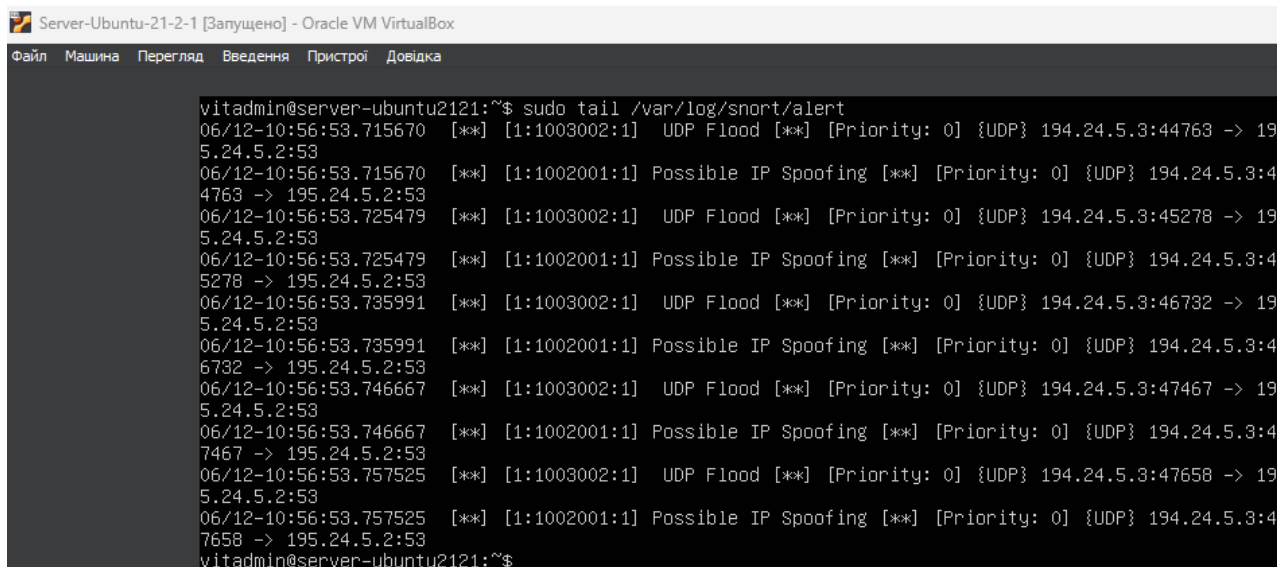
Рисунок 3.3.6 – Повторне проведення атаки UDP Flood

```

vitadmin@server-ubuntu2121:~$ sudo tail /var/log/snort/alert
06/12-10:40:51.297012  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {TCP} 10.0.0.1:293
8 -> 195.24.5.2:80
06/12-10:40:52.315711  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {TCP} 10.0.0.1:293
9 -> 195.24.5.2:80
06/12-10:40:53.299823  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {TCP} 10.0.0.1:294
0 -> 195.24.5.2:80
06/12-10:40:54.349337  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {TCP} 10.0.0.1:294
1 -> 195.24.5.2:80
06/12-10:40:55.315071  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {TCP} 10.0.0.1:294
2 -> 195.24.5.2:80
06/12-10:40:56.323773  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {TCP} 10.0.0.1:294
3 -> 195.24.5.2:80
06/12-10:40:57.312755  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {TCP} 10.0.0.1:294
4 -> 195.24.5.2:80
06/12-10:40:58.317646  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {TCP} 10.0.0.1:294
5 -> 195.24.5.2:80
06/12-10:40:59.319041  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {TCP} 10.0.0.1:294
6 -> 195.24.5.2:80
06/12-10:41:00.321754  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {TCP} 10.0.0.1:294
7 -> 195.24.5.2:80
vitadmin@server-ubuntu2121:~$ _

```

Рисунок 3.3.7 – Повідомлення про атаку



```

Server-Ubuntu-21-2-1 [Занущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

vitadmin@server-ubuntu2121:~$ sudo tail /var/log/snort/alert
06/12-10:56:53.715670  [**] [1:1003002:1]  UDP Flood [**] [Priority: 0] {UDP} 194.24.5.3:44763 -> 19
5.24.5.2:53
06/12-10:56:53.715670  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {UDP} 194.24.5.3:4
4763 -> 195.24.5.2:53
06/12-10:56:53.725479  [**] [1:1003002:1]  UDP Flood [**] [Priority: 0] {UDP} 194.24.5.3:45278 -> 19
5.24.5.2:53
06/12-10:56:53.725479  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {UDP} 194.24.5.3:4
5278 -> 195.24.5.2:53
06/12-10:56:53.735991  [**] [1:1003002:1]  UDP Flood [**] [Priority: 0] {UDP} 194.24.5.3:46732 -> 19
5.24.5.2:53
06/12-10:56:53.735991  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {UDP} 194.24.5.3:4
6732 -> 195.24.5.2:53
06/12-10:56:53.746667  [**] [1:1003002:1]  UDP Flood [**] [Priority: 0] {UDP} 194.24.5.3:47467 -> 19
5.24.5.2:53
06/12-10:56:53.746667  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {UDP} 194.24.5.3:4
7467 -> 195.24.5.2:53
06/12-10:56:53.757525  [**] [1:1003002:1]  UDP Flood [**] [Priority: 0] {UDP} 194.24.5.3:47658 -> 19
5.24.5.2:53
06/12-10:56:53.757525  [**] [1:1002001:1] Possible IP Spoofing [**] [Priority: 0] {UDP} 194.24.5.3:4
7658 -> 195.24.5.2:53
vitadmin@server-ubuntu2121:~$

```

Рисунок 3.3.8 – Повідомлення про атаку

Висновки до третього розділу

В третьому розділі було досліджено на практиці процес побудови, налагодження та тестування системи моніторингу подій.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		88

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було спроектовано та налаштовано підсистему моніторингу подій інформаційної безпеки.

В першому розділі було розглянуто особливості моніторингу подій інформаційної безпеки, розглянуто SIEM-рішення The Elastic Stack, його альтернативи та їх переваги і недоліки.

У другому розділі було проаналізовано процес проектування підсистеми моніторингу подій інформаційної безпеки на базі рішень The Elastic Stack. Розглянуто ключові технології та протоколи, що забезпечують функціонування системи. Окрему увагу приділено системі Snort та прикладам атак на систему які можна виявити з її допомогою.

В третьому розділі було досліджено на практиці процес побудови, налагодження та тестування системи моніторингу подій.

Проведена робота показала доцільність використання комплексу рішень Elastic Stack у поєднанні з IDS/IPS системами для організації ефективного моніторингу подій інформаційної безпеки в комп'ютерних мережах. Отримані знання та практичні навички можуть бути застосовані для створення надійних і масштабованих рішень у сфері інформаційної безпеки.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		89

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Події інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: <https://www.theknowledgeacademy.com/blog/security-event-vs-incident/>
2. Is Elastic Stack (ELK) the Best SIEM Tool? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.bitlyft.com/resources/is-elastic-stack-elk-the-best-siem-tool>
3. What is ELK Stack? [Електронний ресурс] – Режим доступу до ресурсу: <https://aws.amazon.com/what-is/elk-stack/>
4. ELK Stack для чого він використовується [Електронний ресурс] – Режим доступу до ресурсу: <https://freehost.com.ua/ukr/faq/wiki/chto-takoe-elk-stack/>
5. What Is A Port Scan? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.fortinet.com/resources/cyberglossary/what-is-port-scan>
6. IP Spoofing [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/IP_address_spoofing
7. UDP Flood DDoS attack [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/>
8. Spoof Attacks [Електронний ресурс] – Режим доступу до ресурсу: <https://us.norton.com/blog/malware/what-is-ip-spoofing>
9. Applied Network Security / Артур Селмон, Варун Левек, Майкл Маклафферті – Packt Publishing Ltd., 2017 336 с.
10. The-Essential-Guide-to-SIEM [Електронний ресурс] – Режим доступу до ресурсу: <https://www.exclusive-networks.com/ie/wp-content/uploads/sites/19/2021/07/The-Essential-Guide-to-SIEM.pdf>
11. Security Information and Event Management (SIEM) Implementation / Аллен Гарпер, Кріс Бласк, Шон Гарріс – McGraw-Hill, 2010 – 464 с.
12. Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases: A condensed field guide for the Security Operations team / Don Murdoch – CreateSpace Independent Publishing Platform

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

- 13.What is SIEM? A Beginner’s Guide [Електронний ресурс] – Режим доступу до ресурсу: <https://www.varonis.com/blog/what-is-siem>
- 14.What is security information and event management [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/think/topics/siem>
- 15.Getting Started with Elastic Stack 8.0: Run powerful and scalable data platforms to search, observe, and secure your organization / Asjad Athick – Next, 2019 – 474 с.
- 16.Netflow Configuration [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/iosxr/cisco8000/netflow/70x/configuration/guide/b-netflow-config-guide-cisco8k-r70x/b-netflow-cisco-8k-r70x_chapter_01.html
- 17.Ingestion tools [Електронний ресурс] – Режим доступу до ресурсу: <https://www.elastic.co/docs/reference/ingestion-tools/>
- 18.Snort For Dummies / Чарлі Скотт, Паул Вулфб, Берт Хейс – For Dummies, 2004 – 385 с.
- 19.Mastering SIEM / Kris Hermans – Independently published, 2023 – 134 с.
- 20.IDS and IPS with Snort 3 1st edition / Ashley Thomas Packt Publishing Ltd, 2024 – 262 с.
- 21.What is NetFlow? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/think/topics/netflow>

ДОДАТКИ

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

Адресація підмереж

Таблиця А.1

Схема IP-адресації

Канал/Підмережа	IP-адреса
A	192.168.1.0/27
B	192.168.1.32/27
C	192.168.2.0/30
D	192.168.3.0/30
E	194.24.5.0/28

Таблиця А.2

Розподіл IP-адрес

Пристрій	Інтер-фейс	IP-адреса	Маска	Префікс
FR-24-5-1	f0/0	DHCP		
	f0/1	192.168.3.1	255.255.255.252	/30
	f1/0	194.24.5.2	255.255.255.240	/28
	f2/0	195.24.5.1	255.255.255.240	/28
R-24-5-2	f0/0	192.168.3.2	255.255.255.252	/30
	f0/1	192.168.1.1	255.255.255.224	/27
	f1/0	192.168.1.33	255.255.255.224	/27
	f2/0	192.168.2.1	255.255.255.252	/30
Lubuntu-kb-21-2-1	e0	DHCP		
Windows	e0	DHCP		
Server-Ubuntu-21-2-1	e0	192.168.2.2	255.255.255.252	/30
Kali-linux-kb-21-2-1	e0	194.24.5.2	255.255.255.240	/28

Конфігураційні файли пристроїв спрєктованої системи

Конфігурація FR-24-5-1	ip cef
FR-24-5-1#show run	no ip domain lookup
Building configuration...	ip domain name hnatiuk.com
Current configuration : 6404 bytes	ip name-server 8.8.8.8
version 12.4	multilink bundle-name authenticated
service timestamps debug datetime msec	username admin privilege 15 secret 5
service timestamps log datetime msec	\$1\$Noty\$H4Uq5ARuvQAcaSRELHafd0
no service password-encryption	archive
hostname FR-24-5-1	log config
boot-start-marker	hidekeys
boot-end-marker	ip tcp synwait-time 5
logging buffered 4096	ip ssh time-out 60
enable secret 5	ip ssh version 2
\$1\$pDAU\$fWwvqD7lfOHSsEFYFhtjC1	interface FastEthernet0/0
no aaa new-model	ip address dhcp
memory-size iomem 5	ip flow monitor FLOW-MONITOR input
flow record MyNetFlow	ip flow monitor FLOW-MONITOR output
description NetFlow record	ip nat outside
match ipv4 tos	ip virtual-reassembly
match ipv4 ttl	duplex auto
match ipv4 protocol	speed auto
match ipv4 source address	interface FastEthernet0/1
match ipv4 destination address	ip address 192.168.3.1 255.255.255.252
match transport source-port	ip flow monitor FLOW-MONITOR input
match transport destination-port	ip flow monitor FLOW-MONITOR output
collect timestamp sys-uptime last	ip nat inside
collect timestamp sys-uptime first	ip virtual-reassembly
collect counter packets	duplex auto
collect counter bytes	speed auto
flow exporter NETFLOWtoELK	interface FastEthernet1/0
destination 192.168.2.2	no ip address
transport udp 2055	shutdown
template data timeout 60	duplex auto
flow monitor FLOW-MONITOR	speed auto
record MyNetFlow	interface FastEthernet2/0
exporter NETFLOWtoELK	ip address 195.24.5.1 255.255.255.240
cache timeout active 60	duplex auto
cache timeout update 30	speed auto
no ip icmp rate-limit unreachable	router ospf 5

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				94
Змн.	Арк.	№ докум.	Підпис	Дата		

```

log-adjacency-changes
passive-interface default
no passive-interface FastEthernet0/0
no passive-interface FastEthernet0/1
no passive-interface FastEthernet2/0
network 192.168.3.0 0.0.0.3 area 0
network 195.24.5.0 0.0.0.15 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip nat inside source list 1 interface
FastEthernet0/0 overload
logging trap debugging
logging facility local1
logging 192.168.2.2
access-list 1 permit 192.168.1.0 0.0.0.31
access-list 1 permit 192.168.1.32 0.0.0.31

access-list 1 permit 192.168.2.0 0.0.0.7
control-plane
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
exec-timeout 30 0
logging synchronous
login local
transport input ssh
line vty 5 15
exec-timeout 30 0
logging synchronous
login local
transport input ssh
ntp server 109.205.49.8
ntp server 91.189.237.182
end

```

```

FR-24-5-1#
Конфігурація R-24-5-2
R-24-5-2#show run
Building configuration...
Current configuration : 6781 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-24-5-2
boot-start-marker
boot-end-marker
logging buffered 4096
enable
secret
no aaa new-model
memory-size iomem 5
flow record MyNetFlow
description NetFlow record
match ipv4 tos
match ipv4 ttl
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
flow exporter NETFLOWtoELK
destination 192.168.2.2
transport udp 2055
template data timeout 60
flow monitor FLOW-MONITOR
record MyNetFlow
exporter NETFLOWtoELK
cache timeout active 300
cache timeout update 60
no ip icmp rate-limit unreachable
ip cef
no ip dhcp use vrf connected

```

5

\$1\$EHc6\$GA7EwnQKHwtWDB1eVuZgo.

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А. А.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.33
ip dhcp pool A-DHCP
    network 192.168.1.0 255.255.255.224
    default-router 192.168.1.1
    dns-server 192.168.2.2 8.8.8.8
ip dhcp pool B-DHCP
    network 192.168.1.32 255.255.255.224
    default-router 192.168.1.33
    dns-server 192.168.2.2 8.8.8.8
no ip domain lookup
ip domain name hnatiuk.com
ip name-server 8.8.8.8
multilink bundle-name authenticated
username admin privilege 15 secret 5
$1$EMK$wXV4ZmbAqOPQRVfXxYm2b0
archive
    log config
    hidekeys
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
interface FastEthernet0/0
    ip address 192.168.3.2 255.255.255.252
    ip flow monitor FLOW-MONITOR input
    ip flow monitor FLOW-MONITOR output
    duplex auto
    speed auto
interface FastEthernet0/1
    ip address 192.168.1.1 255.255.255.224
    duplex auto
    speed auto
interface FastEthernet1/0
    ip address 192.168.1.33 255.255.255.224
    duplex auto
    speed auto
interface FastEthernet2/0
    ip address 192.168.2.1 255.255.255.248
    duplex auto
    speed auto
interface FastEthernet3/0
    ip address 194.24.5.1 255.255.255.240
    duplex auto
    speed auto
router ospf 5
    log-adjacency-changes
    passive-interface default
    no passive-interface FastEthernet0/0
    no passive-interface FastEthernet0/1
    no passive-interface FastEthernet1/0
    no passive-interface FastEthernet2/0
    no passive-interface FastEthernet3/0
    network 192.168.1.0 0.0.0.15 area 0
    network 192.168.1.32 0.0.0.15 area 0
    network 192.168.2.0 0.0.0.7 area 0
    network 192.168.3.0 0.0.0.3 area 0
    network 194.24.5.0 0.0.0.15 area 0
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.3.1
no cdp log mismatch duplex
control-plane
line con 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
    login local
line aux 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line vty 0 4
    exec-timeout 30 0
    logging synchronous
    login local
    transport input ssh
line vty 5 15
    exec-timeout 30 0
    logging synchronous
    login local
    transport input ssh
ntp server 109.205.49.8
ntp server 91.189.237.182
end
R-24-5-2#

```

		Гнатюк В. О.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А. А.				96
Змн.	Арк.	№ докум.	Підпис	Дата		