Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Метод та засіб моніторингу безпеки в комп'ютерній мережі засобами SIEM

ПОЯСНЮВАЛЬНА ЗАПИСКА

Виконав студент 2 курсу, групи 1КІ—22м
спеціальності 123 — Комп'ютерна інженерія
Волос О.П.
Керівник к.т.н., доц. каф. ОТ
Савицька Л.А.
"07" 12 2023 р.
Опонент к.ф—м.н., доцент кафедри МБІС
Шиян А.А.
"08" 12 2023 р.

Допущено до захисту
зав. Каф ОТ, дтн., проф.
Азаров О.Д.
"11" 12 2023 р.

ВНТУ 2023

ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

Освітній рівень — магістр

Спеціальність — 123 Комп'ютерна інженерія

Освітньо-професійна програма — Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри обчислювальної техніки, дтн., проф.

О.Д. Азаров

"26" 09 2023 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ

студенту **Волосу Олександру Павловичу**

1 Тема роботи «Метод та засіб моніторингу безпеки в комп'ютерній мережі засобами SIEM» керівник роботи Савицька Людмила Анатоліївна к.т.н., доцент, затверджено наказом вищого навчального закладу від **18.09.2023** року № **247**

2 Строк подання студентом роботи **10.12.2023**.

3 Вихідні дані до роботи: система Wazuh SIEM, середовище ELK Stack

4 Зміст розрахунково—пояснювальної записки (перелік питань, які потрібно розробити): вступ, аналіз стану моніторингу безпеки в КМ, організація безпекового моніторингу мережі, метод інтеграції SIEM в середовищі роботи та запуск агентів, дослідження методу інтеграції системи SIEM та її агентів в середовищі ELK STACK, економічна частина.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): технічне завдання, алгоритм інтеграції системи Wazuh SIEM та запуску агентів, лістинг налаштування.

6 Консультанти розділів роботи приведені в таблиці 1.

Таблиця 1— Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1—4	Савицька Людмила Анатоліївна к.т.н., доцент		
5	Небава Микола Іванович, професор		

7 Дата видачі завдання **19.09.2023** .

8 Календарний план виконання МКР приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів МКР	Строк виконання	Підпис
1	Постановка задачі	26.09.23	
2	Огляд існуючих рішень	28.09.23	
3	Розробка структурної схеми	05.10.23-20.10.23	
4	Вибір ПЗ для моделювання	20.10.23 - 30.10.23	
5	Моделювання роботи	31.10.23 - 12.11.23	
6	Розрахунок економічної частини	15.11.23 - 20.11.23	
7	Оформлення пояснювальної записки та ілюстративного матеріалу	26.11.23 - 26.11.23	
8	Виконання магістерської кваліфікаційної роботи	28.11.23-26.11.23	

Продовження таблиці 2

9	Перевірка якості виконання магістерської кваліфікаційної роботи та усунення недоліків	05.12.23	
10	Підписи супроводжувальних документів у керівника, опонента, нормоконтролера	06.12.23 – 08.12.23	
11	Перевірка «антиплагіат»	08.12.23	
12	Попередній захист	08.11.23	

Студент Волос Олександр Павлович

Керівник к.т.н., доц. Савицька Людмила Анатоліївна

АНОТАЦІЯ

УДК 621.374.415

Волос О.П. Метод та засіб моніторингу безпеки в комп’ютерній мережі засобами SIEM

Магістерська кваліфікаційна робота зі спеціальності «Комп'ютерна інженерія» — Вінниця: ВНТУ 2023р. 96 стор., 45 — рис., 16 — табл., 20 — літ. — українською мовою

Дана магістерська кваліфікаційна робота присвячена дослідженню, аналізу та вдосконаленню методів та засобів моніторингу безпеки в комп’ютерних мережах. У цій роботі засоби і методи моніторингу безпеки мережі розробляються на основі агентів системи SIEM (система управління інформацією про моніторинг мережі) з удосконаленням процесу нормування даних від журналів безпеки. Причому, для прискорення процесів реагування на загрози мережевої безпеки комп’ютерної мережі досліджується робота SIEM з точки зору тріади SIEM—EDR—NDR.

Дослідження ґрунтуються на досвіді роботи іноземних компаній та вітчизняних банківських мереж.

Ключові слова: SIEM, ELK Stack, Wazuh, КМ у центрах SOC, агенти безпеки, Тріада SIEM—EDR—NDR, вразливості та загрози.

ANNOTATION

UDC 621.374.415

Volos O.P. Method and means of monitoring security in a computer network by means of SIEM

Master's thesis in the specialty "Computer Engineering" — Vinnytsia: VNTU, 2023. 96 p., 45 — fig., 16 — table, 20 — lit. — In ukrainian

This Master's paper is devoted to research, analysis and improvement of methods and means of security monitoring in computer networks. In this work, network security monitoring tools and methods are developed based on agents of the SIEM system (network monitoring information management system) with the improvement of the data normalization process from security logs. Moreover, in order to speed up the processes of responding to network security threats of the computer network, the work of SIEM is studied from the point of view of the SIEM—EDR—NDR triad.

Research is based on the experience of foreign companies and domestic banking networks.

Keywords: SIEM, ELK Stack, Wazuh, KM in SOC centers, security agents, SIEM—EDR—NDR triad, vulnerabilities and threats.

ЗМІСТ

ВСТУП

Актуальність теми дослідження моніторингу безпеки в комп'ютерній мережі (КМ) стає все більш актуальним і важливим у всьому світі. Протягом лише 2021 року світова економіка зазнала значних втрат через кібератаки на загальну суму 6 трлн. Доларів [1]. Україна не вийшла з-під цієї загрози, ба навіть зазнала її ще більше. За даними аналізу, проведеного компанією Microsoft у 2021 році, майже 20% світових кібератак спрямовані на Україну, що робить нашу країну другою за кількістю кібератак у світі, випереджаючи багатонаціональні корпорації [2]. Це великий виклик, оскільки з 2014 року Україна веде гібридну війну, включаючи і кібернетичний фронт.

З початком відкритої війни росії проти України в лютому 2022 року атаки ще більш загострилися. Лише впродовж перших 400 днів війни на Україну було скоєно понад 3000 потужних кібератак: DDoS атаки, атаки шкідливим програмним забезпеченням (ПЗ), ботнети, фішингові розсилки тощо [3].

Ураховуючи значні втрати моніторинг безпеки в КМ є одним із головних пріоритетів у системі національної безпеки. Отже, для відповіді на ці зростаючі загрози Україна вживає такі контрзаходи:

— працює Національний координаційний центр з безпеки [4], який курує заходи щодо кібербезпеки на національному рівні;

— працюють державний центр CERT-UA (Computer Emergency Response Team) та регіональні центри CSIRT (Computer Security Incident Response Team), які відповідають за забезпечення захисту інформації та комп'ютерних мереж від несанкціонованих доступів та кібератак [5];

— активно ведуть дії кібервійська [6], яка містять спецпідрозділи і фахівців для ведення операцій з кібербезпеки;

— з метою нормативно-правового регулювання, у 2021 році прийнята нова Стратегія кібербезпеки України, яка має на меті створення безпечного кіберпростору та забезпечення безпеки в цьому важливому сегменті [7].

Всі ці заходи мають на меті забезпечити постійний моніторинг безпеки в КМ, аналіз вторгнень у мережу та виявлення атак в режимі real_time. Враховуючи нові виклики, що виникають у зв'язку з повною цифровою трансформацією країни, створюються можливості для досягнення цих завдань:

— розвиток новітніх організаційно—технічних моделей, що сприяють ефективному захисту комп’ютерних мереж та даних;

— впровадження інноваційних інструментів для оперативного виявлення та запобігання атак, і це допомагає реагувати на загрози вчасно та ефективно;

— підтримка досліджень і розробок у галузі кібербезпеки, спрямованих на розвиток новітніх ІТ-технологій та штучного інтелекту (ШІ).

Отже, тематика дослідження є актуальною, водночас існує реальна потреба у подальшому вдосконаленні методів і засобів для постійного і надійного моніторингу безпеки в комп’ютерних мережах.

Метою дослідження є прискорення процесів реагування на загрози мережевої безпеки завдяки вдосконаленому процесу обробки журналів подій у методі інтеграції SIEM та її агентів в середовище.

Запропонований підхід має потенціал упорядковувати і систематизувати хаотичні та розкидані дані про події у комп’ютерній мережі. Це дозволить конвертувати цю інформацію в зручний та легко зрозумілий формат, представленням у вигляді діаграм і графіків. Такий підхід сприяє оперативному виявленню можливих загроз та надає адміністраторам системи інструменти для їх швидкого усунення.

Для досягнення поставленої в роботі мети необхідно виконати такі завдання:

— дослідити методи, засоби та новітній підхід до використання схеми побудови системи моніторингу безпеки в КМ засобами SIEM на базі відомих стандартів ISO;

— дослідити новітній підхід щодо моніторингу безпеки в комп'ютерних мережах, зокрема, в парадигмі тріади SIEM—EDR—NDR;

— дослідити новітній підхід щодо розробки неперервного ефективного моніторингу безпеки в комп'ютерних мережах у центрах SOC;

— запропонувати альтернативний метод інтеграції SIEM та її агентів в середовище;

— запропонувати альтернативний процесу обробки журналів подій;

— експериментально перевірити роботу методу інтеграції системи SIEM та її агентів в середовищі ELK STACK.

Об'єктом дослідження є процеси моніторингу безпеки в комп'ютерній мережі.

Предметом дослідження є методи та засоби моніторингу безпеки в комп'ютерній мережі за допомогою можливостей SIEM.

Наукова новизна полягає в поліпшенні операційних інструментів для керування мережевою безпекою за допомогою SIEM, зокрема:

— вдосконалено метод інтеграції SIEM та її агентів в середовище за рахунок безпекового моніторингу в парадигмі тріади SIEM-EDR-NDR;

— удосконаленні процесу обробки журналів в системі SIEM за рахунок оптимізованої роботи централізованих хабів агентів та «пісочниці» в EDR.

Практична цінність полягає у впровадженні альтернативних методів моніторингу безпеки в комп'ютерних мережах засобами SIEM, зокрема:

— реалізації архітектурного плану безпекового моніторингу взаємодії компонентів SIEM-EDR-NDR;

— реалізації алгоритму інтеграції системи Wazuh SIEM та запуску агентів;

— інтеграції системи Wazuh SIEM в середовище ELK Stack;

— візуалізації для адміністратора результатів роботи роботи процесу обробки журналів від агента і SIEM.

Матеріали роботи опубліковувалися відображено у Міжнародному науково-технічного журналу “Інформаційні технології та комп’ютерна інженерія” [1]:

Метод та засіб моніторингу безпеки в комп’ютерні мережі засобами SIEM [Текст] / Л.А. Савицька, Т.І. Коробейнікова, О.П. Волос, М. Г. Тарновський // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 2. – С. 52-61

1 АКТУАЛЬНИЙ СТАН ПИТАННЯ У ГАЛУЗІ МОНІТОРИНГУ БЕЗПЕКИ КМ

У першому розділі магістерської роботи розглядається концепція побудови системи моніторингу безпеки в комп'ютерних мережах, методи та засоби, сучасні підходи керування безпекою (Security Operations Center — SOC), а також ідея системного моніторингу мережі в парадигмі тріади SIEM-EDR-NDR.

1.1 Схема системи моніторингу безпеки в комп'ютерних мережах

1.1.1 Стандартний план робіт

Відповідно до стандарту ISO/IEC 27005 [10], рекомендується виконувати підготовку моніторингу безпеки в КМ за таким планом (рис. 1.1):

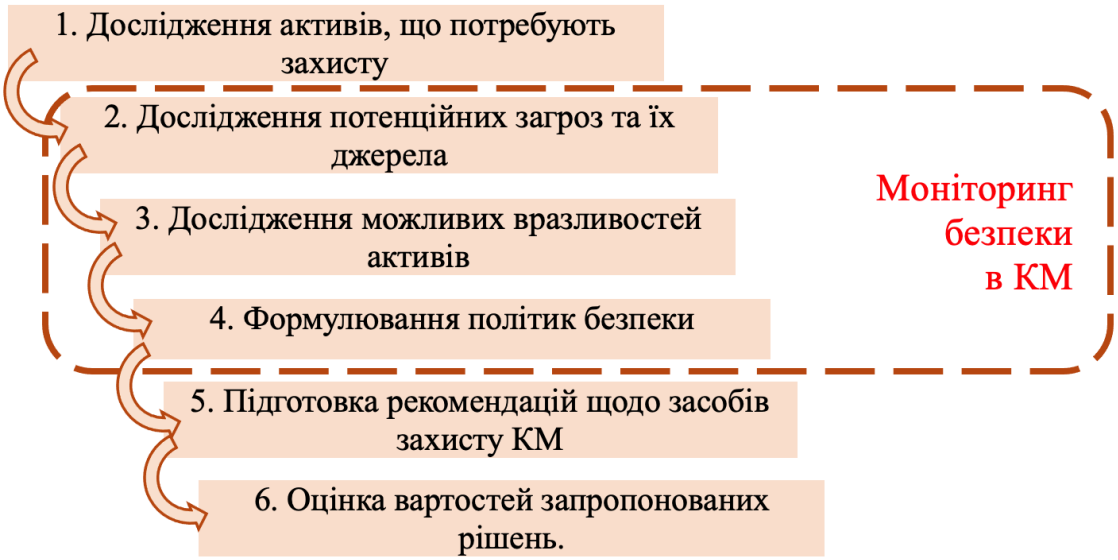


Рисунок 1.1 — Узагальнений план моніторингу безпеки в КМ

Дослідження потенційних загроз, дослідження можливих вразливостей активів та формування політик безпеки — це ті пункти плану, що становлять інтерес дослідження і де присутній моніторинг безпеки в КМ.

1.1.2 Експертний огляд ресурсів, які вимагають захисту

За визначенням, активами вважаються всі ресурси, які мають цінність для компанії і вимагають захисту [11] (рис. 2.1).

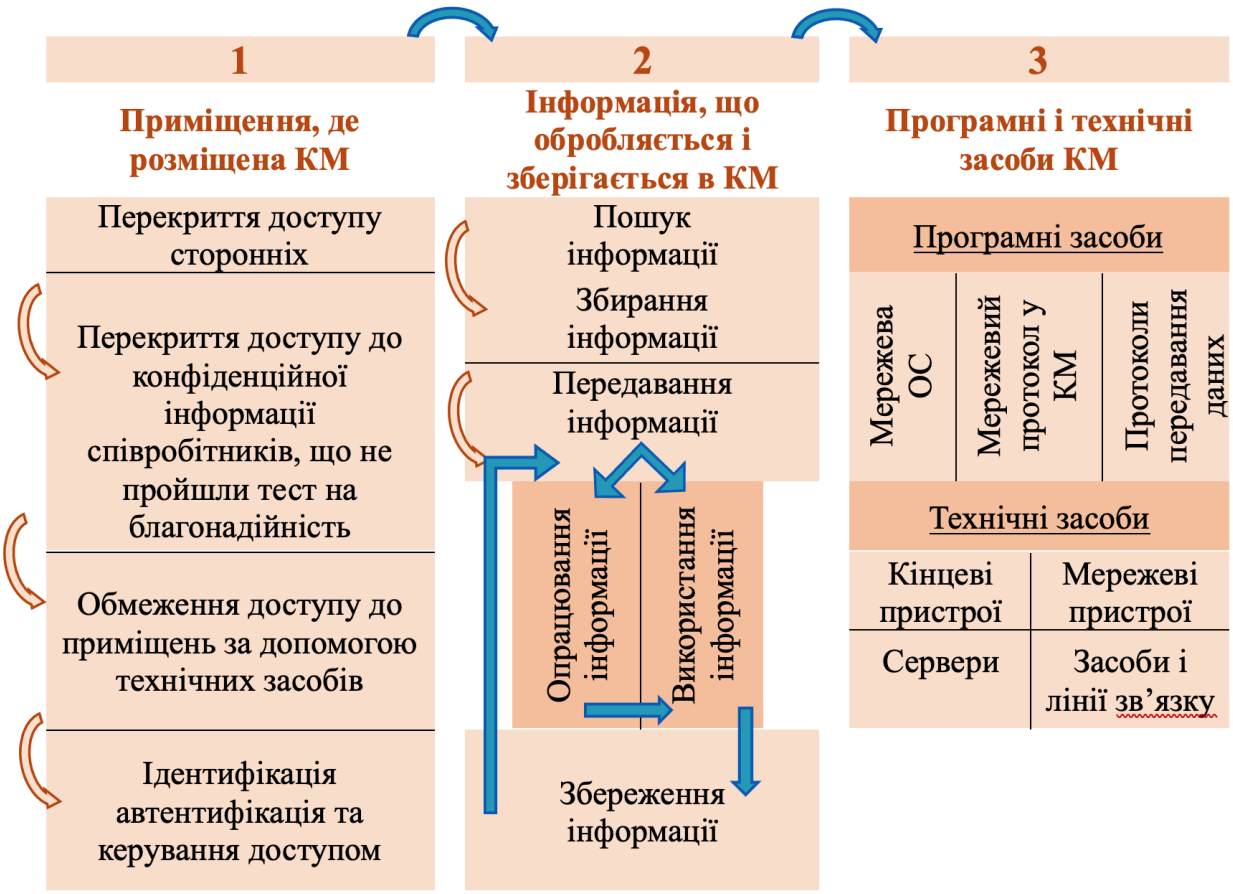


Рисунок 1.2 — Узагальнена схема дослідження активів під час моніторингу безпеки в КМ

Серед таких активів можна відзначити: приміщення, в якому розміщена КМ; інформація, яку тут обробляють і зберігають; засоби комп'ютерних мереж: програмне, технічне обладнання (сервери, мережеві та кінцеві пристрої, засоби зв'язку і т. д.) [12].

Усі ці активи повинні бути ідентифіковані і облікові. Фахівці проводять експертну оцінку відносної цінності цих активів (низька, середня, висока) з

урахуванням можливих втрат або пошкоджень. На рисунку 1.2 показана схема дослідження активів під час моніторингу безпеки в інформаційній КМ. Згідно із завданням магістерської роботи тут обмежуємось такими активами, як інформація та програмні засоби.

1.1.3 Аналіз можливих загроз і джерел їх виникнення

Ккіберзагроза є потенційно небезпечним явищем чи фактором, що становить ризик для активів мережі та загалом для інформаційної безпеки (ІБ) компанії [13]. ІБ містить заходи, спрямовані на забезпечення захищеності від потенційних загроз [13]. Загроза може завдати шкоди активам. Важливо ідентифікувати і випадкові, і навмисні загрози та визначити їх джерела.

Типові загрози ІБ можуть бути класифіковані за різними ознаками [14]: за аспектом, який вони спрямовані порушити; за місцем походження загроз; за рівнем впливу на КМ; за природою виникнення.

За відношенням до аспектів, який можна порушити, загрози такі [14]:

— загрози конфіденційності: це ситуації, коли інформація стає доступною тим, хто не має відповідних повноважень. Це означає несанкціонований доступ до інформаці;

— загрози цілісності: це загрози, пов'язані з можливістю неправомірної зміни даних в системі. Це може означати модифікацію інформації без належних дозволів;

— загрози доступності: це ситуації, коли відбуваються дії, які ускладнюють або навіть блокують доступ до інформаційних ресурсів. Тобто, це може включати в себе дії, спрямовані на заважання нормальному функціонуванню системи або ускладнення доступу до неї.

За локалізацією джерела загроз, їх можна поділити на [14]:

— внутрішні загрози: це джерела загроз, які знаходяться всередині компанії або організації;

— зовнішні загрози: це джерела загроз, які знаходяться поза межами компанії або організації;

За розмірами завданої шкоди, загрози поділяються на:

— загальні загрози: це загрози, які можуть заподіяти шкоду об'єкту безпеки в цілому, охоплюючи всю систему або організацію;

— локальні загрози: це загрози, які можуть призвести до шкоди окремих частин об'єктів безпеки;

— приватні загрози: це загрози, які можуть заподіяти шкоду конкретним властивостям або ресурсам КМ.

За ступенем впливу на КМ [14], загрози поділяються на:

— пасивні загрози: це загрози, які не змінюють структуру або вміст інформації. Однак вони можуть призвести до незаконного доступу до інформації без її зміни або викриття;

— активні загрози: це загрози, які змінюють структуру або вміст інформації: модифікація, видалення або вставка додаткової інформації.

За природою виникнення загрози, загрози можна розмежувати так [14]:

— природні (об'єктивні) загрози: це загрози, що виникають внаслідок впливу об'єктивних фізичних процесів або природних стихійних явищ, які не залежать від волі людини;

— штучні (суб'єктивні) загрози: це загрози, які спричинені впливом людини на КМ.

Джерелами загроз можуть бути суб'єкти (особи), об'єктивні прояви (конкуренти або злочинці). Джерела загроз призначені для отримання доступу до даних, їх модифікації і завдання прямої матеріальної шкоди. Необхідно позначити кожний актив у відповідності до видів загроз. Результатом аналітичної обробки цієї інформації є схема загальної класифікації загроз під час моніторингу інформаційної КМ (див. рис. 1.3).

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В ПРОЦЕСАХ МОНІТОРИНГУ КМ

ЗА АСПЕКТОМ	ЗА РОЗМІЩЕННЯМ ДЖЕРЕЛА ЗАГРОЗ	ЗА СТУПЕНЕМ ВПЛИВУ НА КМ	ЗА ПРИРОДОЮ ВИНИКНЕННЯ
Загроза конфіденційності	Внутрішні	Активні	Природні (об'єктивні)
Загроза цілісності	Зовнішні	Пасивні	Штучні (суб'єктивні)
Загроза доступності	За розміром шкоди, що завдається		
	Загальні		
	Локальні		
	Приватні		

Рисунок 1.3 –Схема загальної класифікації загроз під час моніторингу КМ

1.1.4 Дослідження вразливостей активів

Дослідження вразливостей активів є важливою частиною процесу моніторингу безпеки КМ. Уразливість в цьому контексті означає недолік або слабкість в активі або засобах захисту, яка може бути використана загрозами [10]. Серед типових вразливостей КМ можна виділити такі:

— людський фактор: це уразливість, пов'язана з недостатньою увагою або недбалістю користувачів системи щодо безпеки інформації;

— вразливості операційних систем (ОС): це слабкі місця в ОС, які можуть бути використані для несанкціонованого доступу або атак;

— віддалений доступ: ця уразливість виникає при наявності можливості віддаленого доступу до системи, особливо якщо цей доступ не захищений від несанкціонованого використання;

— зовнішні мережеві підключення: вразливості можуть виникати при зовнішніх з'єднаннях з мережею, особливо якщо не вживаються належні заходи захисту;

— засоби захисту та моніторингу: недоліки тут можуть створювати можливості для атак і несанкціонованого доступу;

— програмне забезпечення (ПЗ): вразливості в ПЗ можуть бути використані для атак на систему або для зламу безпеки КМ.

Ця різноманітність вразливостей покладає особливі вимоги на системи моніторингу безпеки в КМ. Поняття політики безпеки є ключовим в під час моніторингу безпеки КМ. Після аналізу активів, потенційних загроз і вразливостей активів, формулюються політики інформаційної безпеки (ІБ).

Згідно зі стандартом ISO/IEC 27002 [15], політика ІБ є комплексом нормативних, організаційних та експлуатаційних документів, які охоплюють всі аспекти організації, керування та контролю ІБ та експлуатації засобів захисту. Цей комплекс складається з документів трьох рівнів.

На першому рівні розробляється основний системоутворюючий документ — "Концепція інформаційної безпеки", який визначає цілі і принципи системи захисту інформації в КМ, а також вимоги і загальні правила керування інформаційною безпекою в мережі.

Документи другого рівня розробляються на основі "Концепції" і містять:

— порядок поводження з інформацією, основні правила дій користувачів і їх відповідальність;

— технічні вимоги до програмно—апаратних засобів захисту, включаючи системне ПЗ.

На основі документів другого рівня розробляються виконавчі документи третього рівня, які містять:

— конкретизовані та розширені посадові інструкції;

— експлуатаційні документи.

Отже, основною метою забезпечення ІБ є захист інформації від випадкових або навмисних втручань. Водночас ІБ також спрямована на забезпечення неперервності бізнес—процесів.

В таблиці 1.1 наведено принципи побудови системи ІБ:

— генеральний підхід: Система захисту інформації повинна охоплювати організаційні заходи, технічні та програмні засоби, щоб бути комплексною;

— інтегральний підхід: Всі заходи і засоби захисту повинні бути взаємопов'язані, узгоджені та забезпечувати цілісність системи;

— структурна ієрархія: Важливе використання багаторівневого захисту, щоб мати додаткові рівні безпеки;

— усеосяжність: Система захисту повинна охоплювати всі активи, всі вузли та кінцеві пристрої КМ, включаючи прилади BYOD (Bring Your Own Device)

— забезпечення надійності: Механізми захисту повинні бути настільки надійними, щоб вартість зламу була вищою, ніж цінність інформації, яку зловмисник намагається отримати;

— контроль на всіх рівнях: Контроль повноважень при доступі до інформації повинен охоплювати всі рівні контролю, включаючи інформацію, програмне забезпечення, апаратне забезпечення та персонал;

— цикл Демінга "PDCA" (Plan-Do-Check-Act): Цей цикл моделі передбачає обов'язкові етапи:

— планування цілей та політики інформаційної безпеки (Plan);

— реалізація і впровадження заходів інформаційної безпеки (Do);

— оцінка, контроль, моніторинг та аналіз функціонування інформаційної безпеки (Check) ;

— покращення, удосконалення та розвиток системи інформаційної безпеки (Act).

Під час формування принципів політики інформаційної безпеки (ІБ), важливо враховувати основні вимоги до інформації відповідно до моделі CIA (Confidentiality-Integrity-Availability):

— конфіденційність (Confidentiality): Цей принцип означає, що інформація повинна бути доступна лише санкціонованим особам і суб'єктам. Заборонено несанкціонований доступ до конфіденційної інформації;

— цілісність (Integrity): Цей принцип вимагає, щоб інформація залишалася незмінною і не піддавалася несанкціонованій модифікації або знищенню. Система повинна запобігати будь-яким несанкціонованим змінам в інформації;

— доступність (Availability): Цей принцип стверджує, що законні користувачі повинні мати можливість отримувати необхідну інформацію вчасно та без перешкод. Система повинна гарантувати доступ до інформації для тих, хто має на це право.

Таблиця 1.1 — Принципи побудови системи інформаційної безпеки

Генеральний підхід	СЗ інформації повинна бути комплексною, охоплювати організаційні заходи, технічні та програмні засоби.
Системний підхід	Всі заходи і засоби захисту повинні бути пов’язані, узгоджені і забезпечувати цілісність системи.
Структурна ієрархія	Згідно із завданням тут повинен бути реалізований принцип поглибленого багаторівневого захисту .
Усеосяжність	Система захисту повинна охоплювати всі активи, всі вузли та кінцеві пристрої КМ, у тому числі BYOD.
Забезпечення надійності	Повинні бути створені такі механізми захисту, щоб вартість зламу її була дорожчою за інформацію, яку зловмисник прагне поцупити.
Контроль на всіх рівнях	Контроль повноважень будь—якого звернення до інформації повинен охоплювати всі рівні контролю: інформацію, ПЗ, апаратуру, персонал.
Цикл Демінга «PDCA»	Цикл моделі «PDCA» передбачає обов’язкові етапи: 1) Встановлення цілей та політик СЗ (Plan); 2) Реалізацію і впровадження СЗ (Do); 3) Оцінку, контроль, моніторинг і аналіз (Check);

У таблиці 1.1 вказані основні загальноприйняті принципи побудови системи ІБ [16]. Примітка: в таблиці 1.1 використані такі скорочення: СЗ — система захисту; BYOD — Bring Your Own Device, особисті мобільні пристрої, яким дозволений доступ до КМ; PDCA — Plan-Do-Check-Act, модель безперервного поліпшення процесів.

Для виконання політик інформаційної безпеки на підприємстві реалізується відповідна низка заходів. Ці заходи включають в себе розробку і впровадження правил і процедур для забезпечення конфіденційності, цілісності і доступності інформації, встановлення відповідних технічних засобів захисту, навчання персоналу з питань інформаційної безпеки, а також постійний моніторинг і аналіз з метою виявлення і вирішення потенційних загроз

1.2. Поняття, методи та засоби моніторингу безпеки в комп’ютерних мережах

1.2.1 Загальна інформація

Засоби моніторингу безпеки в комп’ютерних мережах є важливою складовою інформаційної безпеки в сучасному світі, де загрози постійно зростають. Ці засоби допомагають виявляти, аналізувати та відстежувати потенційні загрози в

КСМ. Нижче наведено інформацію про основні засоби.

SIEM (Security Information and Event Management): SIEM—системи збирають, аналізують та інтерпретують дані про події та інформацію щодо безпеки з різних джерел, щоб виявляти аномалії та потенційні загрози. Вони допомагають в реальному часі виявляти та реагувати на інциденти безпеки.

EDR (Endpoint Detection and Response): EDR—рішення спеціалізуються на моніторингу кінцевих точок (пристроїв) у мережі. Вони дозволяють виявляти та реагувати на загрози, які можуть виникнути на комп'ютерах та інших пристроях.

NDR (Network Detection and Response): NDR—рішення спеціалізуються на виявленні загроз у мережевому рівні. Вони аналізують трафік мережі, щоб виявити незвичайні або підозрілі активності.

IDS/IPS (Intrusion Detection System/Intrusion Prevention System): Ці системи виявляють та запобігають несанкціонованому доступу та атакам у мережі.

Firewall (Брандмауер): Брандмауери контролюють трафік мережі та фільтрують небезпечний трафік, що може викликати загрози безпеці.

Антивірусні та антималware рішення: Ці програми виявляють та блокують віруси, шкідливі програми та загрози для безпеки.

Системи ведення журналів (Log Management): Вони збирають, агрегують та аналізують журнали подій (Sec_Event_Logs) з різних джерел для виявлення аномалій та інцидентів безпеки.

Засоби моніторингу мережевої безпеки допомагають організаціям виявляти, реагувати та захищати свої мережі та системи від кіберзагроз. Вони стають надзвичайно важливими в сучасному цифровому світі для забезпечення безпеки даних та інфраструктури.

1.2.2 Методи ідентифікації та аутентифікації

Визначають, як система перевіряє особу та дійсність її ідентичності. Ідентифікація означає представлення системі певної інформації про користувача, яка дозволяє встановити його ідентичність. Автентифікація, зі свого боку, визначає, чи є ця інформація правильною та дійсною [14]. Ці процеси ідентифікації та аутентифікації містять:

— перевірку інформації, яку надає користувач (такі як паролі та протоколи аутентифікації);

— перевірку власності користувача, що може включати модулі пам'яті та PIN—коди карток;

— перевірку особи користувача, включаючи використання біометричних даних.

1.2.3 Засоби керування доступом

Контроль та керування правом доступу убезпечують незаконне проникнення на об’єкти захисту та несанкціоноване використання ресурсів.

— розрізняють кілька рівнів контролю доступу [14]: Контроль доступу при вході в систему;

— контроль доступу до окремих об’єктів (файлів, папок, баз даних тощо);

— контроль доступу до окремих пристроїв системи.

Моделі керування доступом поділяються на [16]: дискреційне управління; обов’язковий (мандатний) метод керування; рольова модель.

Дискреційний контроль [14] (DAC — Discretionary Access Control). Передбачає право адміністратора об’єкта визначати та контролювати всіх, хто має доступ до системи, ґрунтуючись на ідентифікаційній інформації про суб’єктів (ключі доступу), допущених до контрольованої системи.

Мандатний контроль [14] (MAC — Mandatory Access Control). Є найбільш обмежувальною формою доступу, оскільки надає контроль та керування системою лише адміністратору. Тут користувачам не дозволяється підвищувати рівень доступу до ресурсів, встановлений адміністратором.

Модель рольового керування [4] (RBAC — Role—Based Access Control). Передбачає розподіл функцій персоналу з урахуванням типу діяльності. Тут достатньо встановити ступінь допуску для ролі, яку виконує типовий користувач ресурсу.

1.2.4 Засоби захисту від шкідливого ПЗ

Інформація, яку обробляє комп'ютер, може бути піддана різним видам загроз, включаючи атаки від шкідливого програмного забезпечення (ШПЗ):

— знищення інформації та/або її носія: це означає фізичне або логічне видалення інформації або руйнування носія інформації;

— несанкціоноване отримання конфіденційної інформації: ця загроза полягає в тому, що хакери намагаються отримати доступ до конфіденційних даних без дозволу;

— модифікація інформації: це включає в себе внесення змін до існуючої інформації, з метою спотворення або підробки даних;

— створення помилкових повідомлень: це може бути використано для введення користувачів в оману або розповсюдження дезінформації;

— блокування доступу до інформації або ресурсів системи: ця загроза полягає в тому, що зловмисники намагаються заблокувати доступ до системи або її ресурсів;

— несанкціоноване використання інформаційних ресурсів системи: це включає в себе використання ресурсів системи без дозволу або зловживання їхнім використанням.

Для боротьби з вірусами використовують антивірусні програми, такі як McAfee, Norton, TrendMicro та інші. Проти шкідливого ПЗ застосовують програми—сканери, такі як Advanced IP Scanner, Wireshark, Solarwinds, Tripwire, Nessus, Vulnerability Manger Plus, Splunk та інші.

1.2.5 Засоби контролю цілісності

Засоби контролю цілісності інформації ґрунтуються на алгоритмах, які використовуються для перевірки цілісності даних і програмного середовища:

— контроль цілісності наборів даних: забезпечує перевірку, що дані не були змінені або пошкоджені під час передачі або зберігання;

— контроль цілісності програмного середовища: Цей аспект допомагає виявити, чи було внесено зміни до програмного середовища, що може вказувати на потенційні загрози безпеці.

Додатково, для забезпечення безпеки використовується електронно—цифровий підпис (ЕЦП). За допомогою математично обґрунтованих алгоритмів, обчислюється унікальний підпис для конкретного повідомлення, який автор генерує за допомогою свого індивідуального ключа. ЕЦП залежить від кожного символу у повідомленні, що робить неможливим зміну або підміну без зміни значення ЕЦП.

Технологія ЕЦП використовується для підтвердження таких параметрів:

– дійсності електронного документа: підтвердження, що документ є дійсним і не був змінений;

– цілісності документа: виявлення будь—яких змін або пошкоджень документа;

– авторства документа: підтвердження, що документ був створений автором, який стверджує, що він його створив.

Українською найпоширенішою програмою для ЕЦП є ISpro.

Запропонований підхід має потенціал упорядковувати і систематизувати хаотичні та розкидані дані про події у комп’ютерній мережі. Це дозволить конвертувати цю інформацію в зручний та легко зрозумілий формат, представленням у вигляді діаграм і графіків. Такий підхід сприяє оперативному виявленню можливих загроз та надає адміністраторам системи інструменти для їх швидкого усунення.

Для досягнення поставленої в роботі мети необхідно виконати такі завдання:

— дослідити методи, засоби та новітній підхід до використання схеми побудови системи моніторингу безпеки в КМ засобами SIEM на базі відомих стандартів ISO;

— дослідити новітній підхід щодо моніторингу безпеки в комп’ютерних мережах, зокрема, в парадигмі тріади SIEM—EDR—NDR;

— дослідити новітній підхід щодо розробки неперервного ефективного моніторингу безпеки в комп’ютерних мережах у центрах SOC;

— запропонувати альтернативний метод інтеграції SIEM та її агентів в середовище;

— запропонувати альтернативний процесу обробки журналів подій;

— експериментально перевірити роботу методу інтеграції системи SIEM та її агентів в середовищі ELK STACK.

2 ОРГАНІЗАЦІЯ БЕЗПЕКОВОГО МОНІТОРИНГУ МЕРЕЖІ

У другому розділі магістерської роботи визначені завдання для компонентів тріади SIEM—EDR—NDR, проведено аналіз ролі, концепції та процесів кожного елемента окремо, висунуті пропозиції щодо поліпшень існуючих відомих процесів, і введено функцію агентів для оптимізації цих процесів. Зокрема, розглянуто відомий процес нормалізації журналів подій та його вдосконалений варіант, а також розглянуто відомий принцип функціонування EDR—систем та його вдосконалений варіант з запропонованими змінами.

2.1 Взаємодія складових SIEM—EDR—NDR

Компоненти SIEM—EDR—NDR взаємодіють та вирішують завдання спільно, формуючи єдиний функціональний блок (SOC—тріаду) [17]. SIEM створює централізоване інформаційне вікно для аналітиків, щоб корелювати зібрані дані в середовищі, в т.ч. від EDR і NDR, та дозволяє командам забезпечення безпеки відокремлювати системні попередження та проводити аналіз потенційних загроз. SIEM забезпечує всебічний погляд на безпеку і використовує механізми з різних джерел, включаючи кінцеві точки, спеціальні програми, хмарні служби та інші джерела даних. Ці журнали збираються у різних форматах і піддаються аналізу для забезпечення їх кореляції та ефективного аналізу, що вказує на покращені можливості раннього виявлення і, отже, на досягнення головної мети SIEM — скорочення «часу перебування» до моменту виявлення.

EDR надає інформацію про зловмисну активність на кінцевих точках організації в рамках SOC—тріади. Виявляє, реагує на різні типи зловмисного ПЗ, а також забезпечує докладний огляд та повну видимість пристроїв у мережі. Можливості NDR доповнюють засоби EDR, усуваючи прогалини агентів EDR, і розширюють аналіз журналу SIEM, асоціюючи виявлені загрози з мережевою активністю та надаючи їм необхідний контекст.

Отже, комбінація цих рішень у складі SOC—тріади забезпечує неперевершену видимість та автоматичність реагування в умовах кібератаки.

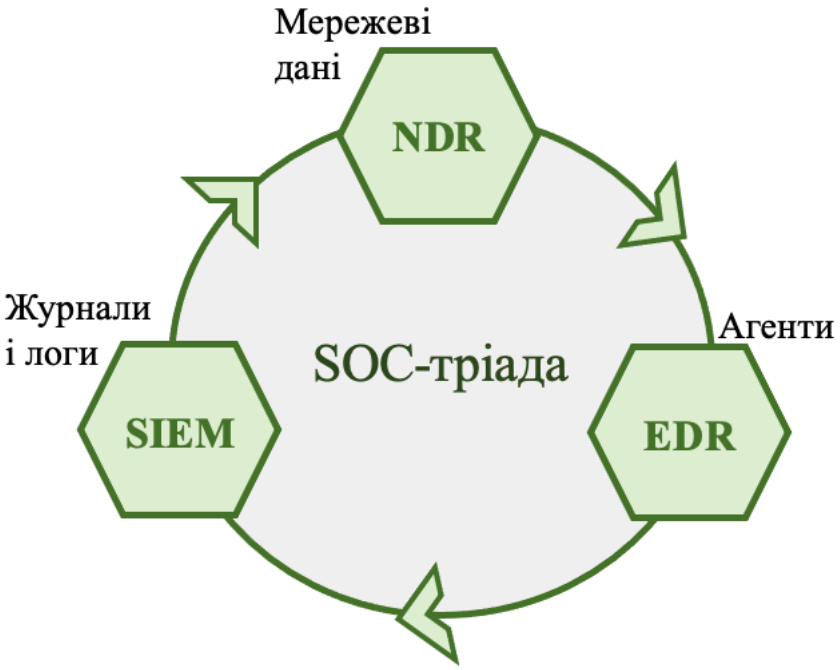


Рисунок 2.1 — SOC—тріада

Тобто разом всі ці рішення, які схематично зображенні на рис. 2.1, забезпечують повну видимість та безпеку системи.

2.2 Формування задач складових SIEM у тріаді SIEM—EDR—NDR

Засоби, які виявляють потенційні загрози — це системи управління інформацією про безпеку та події ІБ (SIEM). SIEM є інфраструктурою, яка акумулює журнали подій від засобів безпеки. Дозволяє розпізнавати та інтегрувати різноманітні «формати» журналів подій із різних джерел, щоб швидко знаходити інформацію у цих журналах подій та зберігати її.

2.2.1 Відомий процес нормалізації журналів

Процес нормалізації журналів подій відомий та продемонстрований на рисунку 2.2.

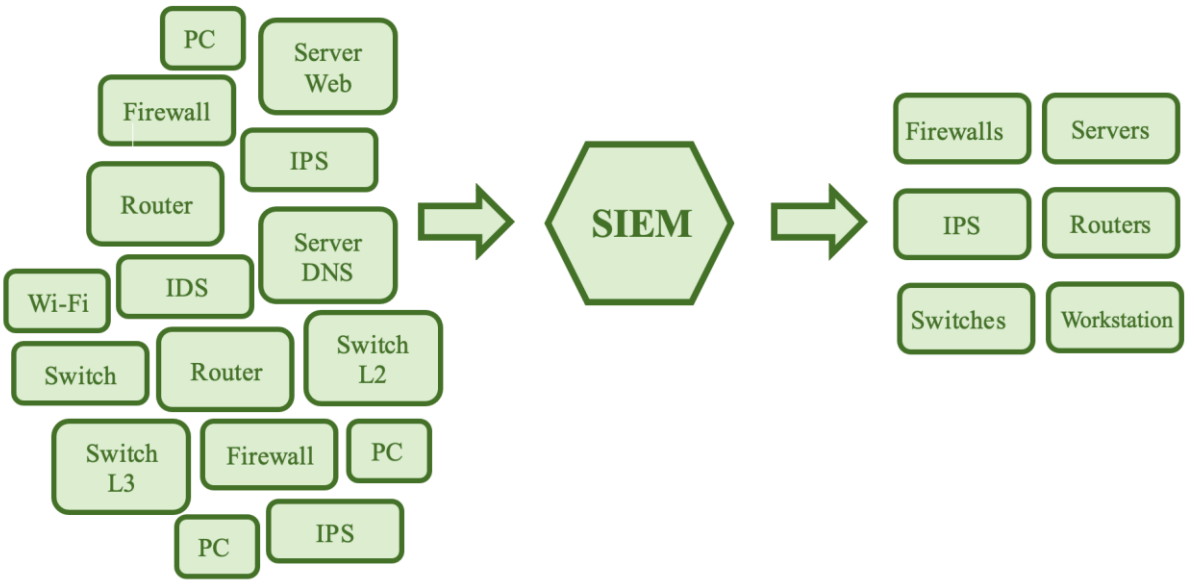


Рисунок 2.2 — Відомий процес нормалізації журналів подій

Система SIEM має здатність виконувати різноманітні функції: проводити таксономію (класифікацію отриманих даних за типами та категоріями) і здійснювати кореляцію (пов'язувати здавалося б розрізнені події між собою). Крім того, вона може надсилати повідомлення відповідальним особам про виявлені підозрілі події в журналах.

Функціонал SIEM на прикладі компанії середнього розміру (близько 1000 співробітників, їх робочі ПК, інформація та бізнес-системи зберігаються та працюють на серверах):

— антивірусні рішення, які призначені для уникнення активності шкідливого коду зловмисного ПЗ на кінцевих точках, у локальному та web—трафіку, а також в електронній пошті;

— засоби захисту від експлойтів, які здатні виявляти та запобігати негативному впливу встановленого прикладного чи системного ПЗ;

— системи управління та контролю обліковими записами, які реалізують централізоване керування обліковими записами користувачів та адміністраторів IT—систем;

— засоби захисту від витоку даних, які спрямовані на запобігання несанкціонованій передачі цінної інформації з порушенням установлених у компанії;

— мережеві брандмауери, які регулюють вхідний та вихідний мережевий трафік як в локальній, так і в інтернет—мережі;

— системи виявлення та/або запобігання мережевим вторгненням призначені для аналізу мережевого трафіку з метою виявлення ознак атаки на пристрої через мережу за допомогою експлойтів;

— «Пісочниці» (засоби ізольованого виконання програм) дозволяють запускати сумнівний файл в ізольованому віртуальному середовищі, призначеному для виявлення аномалій;

— сканери вразливостей застосовуються для аналізу різних IT—систем, отримуючи дані про використовувані версії ПЗ для застосування відомих вразливостей, що застосовуються до зазначених версій;

— системи ресурсів—приманок для зловмисників (honeypots і honeynets) створюються як імітаційні системи інформаційних ресурсів, аналогічні реальним системам компанії, але не містять жодної цінної інформації. Атакуючі, потрапивши в таку пастку, намагаються використовувати свій інструментарій для атаки, і їхні дії ретельно журналюються та аналізуються фахівцями з безпеки інформації;

— засоби управління портативними пристроями (MDM — Mobile Device Management) — це програми контролю та захисту портативних пристроїв співробітників (BYOD). Встановивши такий інструмент, співробітник отримує можливість контрольованого та безпечного віддаленого доступу до IT—ресурсів організації, наприклад, підключивши робочу пошту на свій смартфон.

2.2.2 Вдосконалений процес нормалізації журналів подій

Розглянемо, як функціонує система SIEM, яка користь від її впровадження та які завдання вона виконує.

Перше завдання SIEM — отримати дані від джерела. Це може бути як «активне» джерело, здатне передавати дані у SIEM, достатньо вказати мережеву адресу приймача (так званий менеджер), або «пасивне», до якого SIEM—система повинна самостійно звертатися (так званий агент). Отримавши дані від джерела, SIEM—система перетворює їх у єдиний, придатний для подальшого використання формат — це процес нормалізації.

Далі SIEM—система виконує таксономію, класифікуючи вже нормалізовані повідомлення відповідно до їхнього змісту: яка подія вказує на успішну мережеву комунікацію, яка — на вхід користувача на ПК, а яка — на спрацювання антивіруса. Таким чином, отримуємо не лише набір записів, а послідовність подій (Sec_Event_Logs) із конкретним змістом та часом виникнення. Тепер ми можемо зрозуміти, як взаємодіяли події та встановити можливий зв'язок між ними. В цьому контексті важливу роль відіграє основний механізм SIEM—системи — кореляція. Кореляція в SIEM — це встановлення взаємозв'язку між подіями, які відповідають конкретним умовам (правилам кореляції).

За результатами застосування правил кореляції у SIEM формується інцидент ІБ. В такому випадку фахівець, що працюєз SIEM, має ефективно знаходити серед попередніх інцидентів та подій, що зберігаються в системі SIEM. Отже, ключові завдання системи SIEM такі:

— збір журналів з усіх наявних засобів захисту;

— нормалізація отриманих даних;

— таксономія нормалізованих даних;

— кореляція класифікованих подій (Sec_Event_Logs);

— створення інциденту та забезпечення інструментів для проведення розслідування;

— збереження інформації про події та інциденти протягом значного періоду (принаймні 6 місяців);

— швидкий пошук за даними, які зберігаються в SIEM.

Враховуючи ці аспекти, пропонується удосконалити схему відомого процесу нормалізації журналів подій (рисунок 2.3).

Нова концепція схеми відрізняється від існуючих за такими параметрами:

- вона була ретельно розглянута та уточнена, з докладно визначеними складовими процесу нормалізації журналів подій;
- в ній визначено роль агентів між джерелом даних та SIEM—системою;
- тут представлені ключові етапи обробки даних в межах SIEM—системи.

2.3 Формування задач складових EDR у тріаді SIEM—EDR—NDR

Кожен кінцевий пристрій, який підключений до мережі, є «входом» до конфіденційної інформації. Тому важливо враховувати основні принципи розробки ефективної стратегії кіберзахисту кінцевих пристроїв у мережі:

— захист повинен виявляти і ліквідовувати всі етапи атаки. А саме, ефективний захист від вторгнень містить:

— засоби перевірки поштових додатків (електронна пошта залишається основним «засобом поширення зловмисних кодів» на пристроях користувачів);

— засоби захисту від завантаження небажаних. Тут працює технологія, яка аналізує весь вхідний та вихідний трафік і надає захист браузера, щоб блокувати такі загрози перед їх запуском на кінцевому пристрої;

— потужний захист самого кінцевого пристрою, із службами контролю та додатків, а також сам пристрій.

— механізм реагування та розслідування інцидентів має демонструвати конкретні результати, має мати можливість ізолювати кінцевий пристрій для ефективного вивчення інциденту, зупиняти поширення вірусів та відновлювати пристрій за допомогою його незараженої копії;

— система не повинна впливати на бізнес—процеси, тобто заходи безпеки не повинні заважати нормальному функціонуванню бізнес—процесів та швидкому обміну даними в мережі;

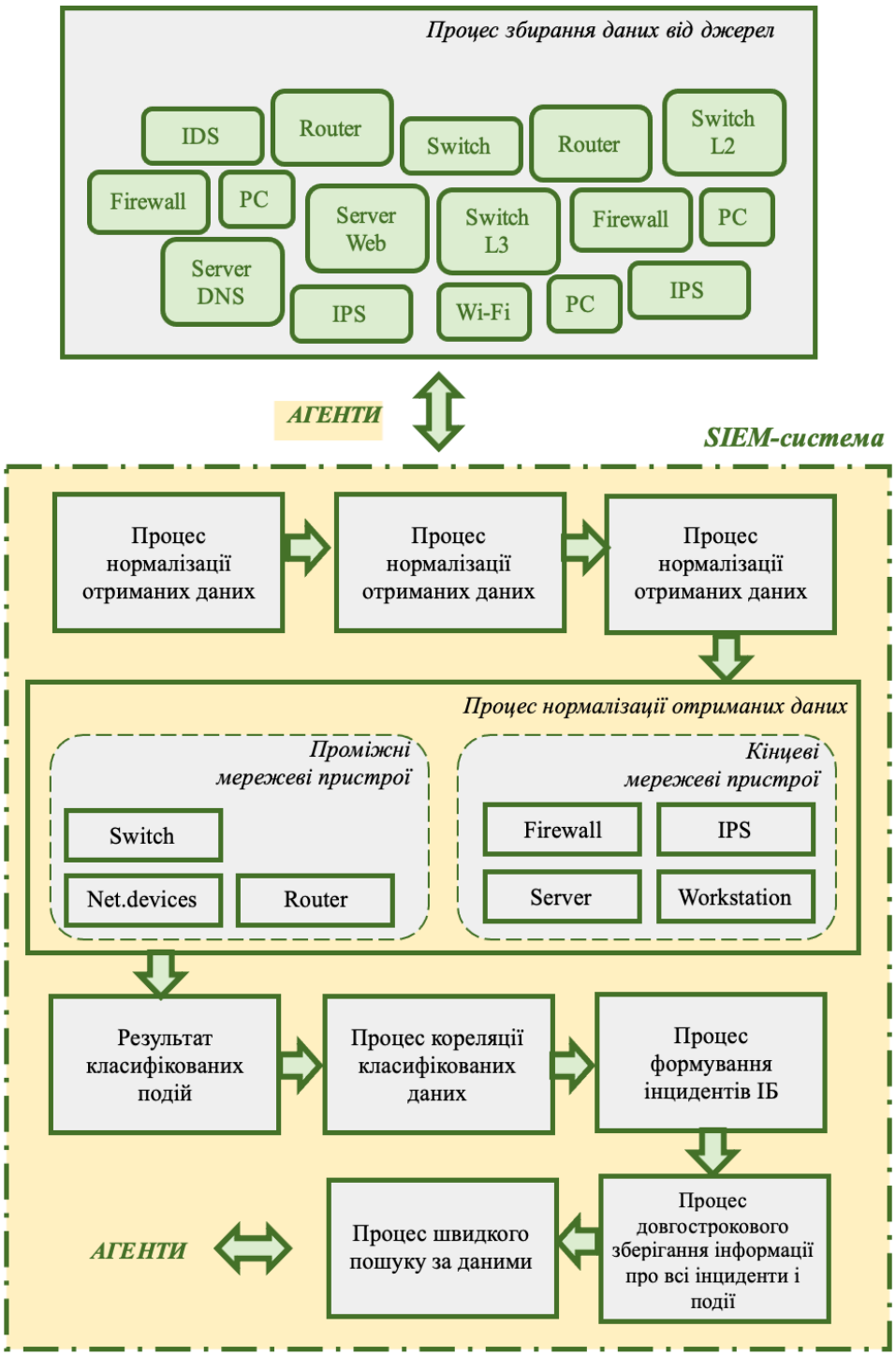


Рисунок 2.3 — Вдосконалений процес нормалізації журналів подій

— централізоване управління кібербезпекою. Отже, політики адміністрування та сам протокол безпеки повинні включати заходи забезпечення безпеки всіх компонентів мережі підприємства, об'єднуючи всі кінцеві пристрої (BYOD). Кожен такий пристрій повинен відповідати вимогам доступу до мережі, що передбачає автоматизацію їхнього кіберзахисту.

Загалом, для дотримання політик безпеки кінцевих пристроїв ураховуючи зростання загроз, необхідно застосовувати:

— мережеві екрани для різних типів пристроїв;

— антивіруси для електронної пошти;

— моніторинг, фільтрацію та захист web—трафіку;

— управління безпекою та захисні рішення для MDM;

— контроль роботи додатків;

— шифрування;

— виявлення вторгнень.

EDR є інтегрованою системою безпеки кінцевої точки, об'єднує постійний моніторинг у реальному часі та збір даних із функціями автоматизованого реагування та аналізу на основі правил. Важливо відзначити, що EDR доповнюють, а не замінюють попередні засоби безпеки, інтегруються з ними для створення більш ефективної та комплексної системи захисту.

Інструментарій EDR складається із трьох основних компонентів:

— агенти збору даних. Моніторинг кінцевих точок та збір даних (процеси, підключення, обсяг активності та передача даних) і передавання цієї інформації у центральну БД.

— автоматизована відповідь. Заздалегідь налаштовані правила в рішенні EDR спроможні виявляти вхідні дані, що вказують на відомий тип порушення безпеки, та запускати автоматизовану реакцію, наприклад, вихід із системи кінцевого користувача чи висилання сповіщення співробітнику.

— аналіз та криміналістика. Аналіз в реальному часі та швидка діагностики загроз, застосуваввння інструментів криміналістики для виявлення загроз чи проведення пост—аналізу атаки.

Безпека системи EDR забезпечує інтегроване централізоване середовище для збору, кореляції та аналізу даних кінцевих точок, а також для координації сповіщень і реагування на активні загрози (рис. 2.4).

EDR операційно взаємодіють за допомогою агентів, які встановлюються на локальних пристроях. З метою полегшення управління ними вони централізовано об'єднуються через центральний хаб. Кілька агентів приєднуються до цього централізованого хабу, і кожен постійно моніторить пристрій та надає інформацію для подальшого аналізу.

Дані, отримані з різних кінцевих точок, транслюються до централізованого хабу для проведення обробки та аналізу, часто використовуючи машинне навчання. Розроблені під час цього процесу статистичні моделі використовуються для часу аналізу вхідних даних з кінцевих точок та виявлення потенційних загроз.

У випадку виявлення загрози система EDR генерує сповіщення та надсилає його IT—адміністраторам чи команді кібербезпеки через інтерфейс користувача, які, здійснюють ізоляцію (переміщення в пісочницю) або вилучення шкідливих файлів, і так усувають потенційну загрозу. Саме так і пропонується вдосконалити схему відомого принципу функціонування EDR—системи (рис. 2.5).

Методи виявлення потенційних загроз в EDR:

— аналіз сигнатур — порівняння сигнатур мережевого трафіку із базою даних відомих сигнатур зловмисного програмного забезпечення;

— аналіз поведінки — поріг прийняття поведінки кінцевої точки порівнюється для виявлення випадків аномальної активності;

— аналіз пісочниці — потенційно небезпечні файли ізолюються в безпечному середовищі (пісочниці), і їхнє взаємодію спостерігається, уникаючи можливих негативних впливів на кінцеву точку;

— відповідність білого/чорного списків — дії кінцевих точок порівнюються із наперед визначеним списком IP—адрес у білому та чорному списках для контролю дозволеного/забороненого мережевого трафіку.

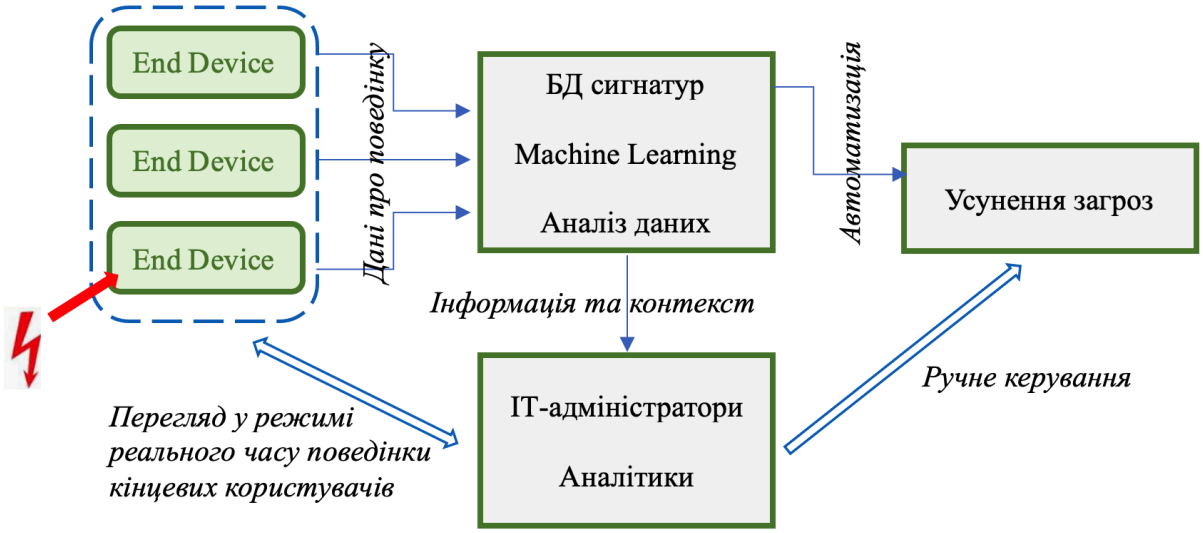


Рисунок 2.4 — Відома схема роботи EDR—систем

2.4 Формування задач складових NDR у тріаді SIEM—EDR—NDR

Як важливий елемент мережевої безпеки, система NDR (мережеве виявлення та реагування) містить технології мережевої безпеки для автоматизованого контролю, виявлення, аналізу та реагування на кіберзагрози.

Засоби NDR, які реалізовані для аналізу мережевого трафіку, включають IDS/IPS і розширений аналіз загроз, що надає змогу командам забезпечення безпеки спостерігати за мережевим трафіком в реальному часі та швидко реагувати на потенційнізагрози.

У зв'язку з розширенням розподілених мереж, інструменти безпеки на основі сигнатур, такі як IDS/IPS, стають недостатніми для ефективного забезпечення безпеки підприємств. Рішення NDR використовують розширену поведінкову аналітику, машинне навчання та штучний інтелект для забезпечення додаткового рівня захисту в локальних і хмарних середовищах. Важливо відзначити, що

рішення NDR не замінюють, а доповнюють попередні засоби моніторингу та аналізу мережі, утворюючи єдину повноцінну систему.

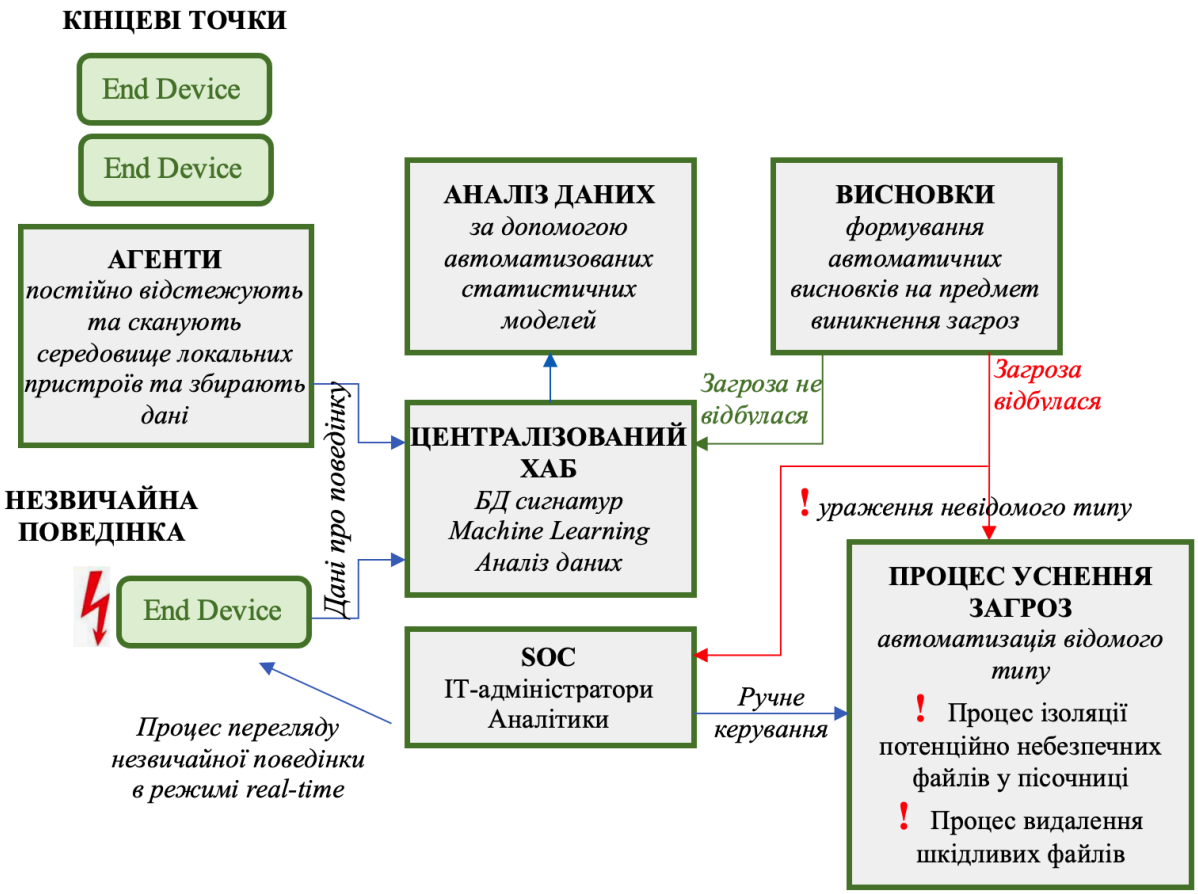


Рисунок 2.5 — Вдосконалений принцип роботи EDR—системи

Рішення NDR можуть відстежувати транспортні потоки в обох напрямках (північ—південь та схід—захід, як внутрішні, так і зовнішні) за допомогою стратегічно розташованих датчиків. Це забезпечує глибоку видимість мережі, що підтримує функції NDR як:

— виявлення кіберінцидентів: виявлення засобами машинного навчання, і аналіз даних на предмет аномалій, підозрілого або зловмисного трафіку.

— розслідування: відстежування мережевого трафіку та виділення шаблонів, які можуть свідчити про аномальні або підозрілі підключення. Ця інформація використовується для автоматизованих відповідей самим NDR та

надається аналітикам SOC для полегшення їхньої діяльності з розслідування інцидентів;

— управління розвідкою: здатність використовувати дані про загрози зсередини та ззовні організації для виявлення потенційних загроз у мережевому трафіку, що може передаватись іншим рішенням безпеки в рамках конвергентної архітектури безпеки;

— створення каналу: NDR забезпечує аналітикам SOC картину поточного стан безпеки мережі. NDR створює канал сповіщень системи безпеки, який вказує на підозрілий і потенційно шкідливий мережевий трафік.

— запобігання загрозам: NDR можуть автоматично та завчасно діяти для запобігання успіху кібератак (блокування підозрілого трафіку до досягнення його місця призначення та переривання атаки).

Ефективні рішення NDR демонструють ряд переваг:

— розширена видимість загроз: групи безпеки можуть відслідковувати загрози, в т.ч. вторгнення та сторонні активності в мережі на локальному рівні та у хмарному середовищі;

— зменшення помилкових спрацьовувань: акцентування уваги на реальних вторгненнях;

— швидше запобігання або зупинка вторгнення: NDR використовує штучний інтелект і машинне навчання для роботи в режимі реального часу, розпізнавання та зупинки загроз зі швидкістю мережевого зв'язку;

— повна візуалізація атак: завдяки інформації про план вторгнень та детальному графіку загроз у мережі, служби безпеки можуть оперативно зрозуміти масштаб атаки та визначити пріоритетність ресурсів.

Рішення NDR постійно аналізують та корелюють значні обсяги мережевого трафіку та подій безпеки (Sec_Event_Logs) між різними активами та переходами. Інструменти NDR засновано на штучному інтелекті, який постійно самонавчається та адаптується для автоматичного виявлення еволюціонуючих та складних загроз.

У випадку виявлення атаки рішення NDR забезпечують всебічний криміналістичний аналіз хронології атаки, починаючи від ініціювання проникнення та стороннім переміщеннями в мережі, а також автоматично запускають процеси для запобігання майбутнім атакам.

3 МЕТОД ІНТЕГРАЦІЇ SIEM В СЕРЕДОВИЩЕ РОБОТИ ТА ЗАПУСК АГЕНТІВ

У третьому розділі планується розгляд організації підходу щодо розробки неперервного ефективного моніторингу безпеки в мережі у Ситуаційних центрах інформаційної безпеки. Необхідно обґрунтувати доцільність моніторингу безпеки в мережі у парадигмі тріади SIEM-EDR-NDR, та його відображенні у методі інтеграції SIEM в ELK Stack та запускові агентів. Для реалізації методу необхідний алгоритм інтеграції системи Wazuh SIEM та запуску агентів. Для практичного застосування методу необхідно описати апаратні та програмні компоненти.

3.1 Підхід щодо розробки неперервного ефективного моніторингу безпеки в КМ у центрах SOC

Для забезпечення ефективного та стійкого моніторингу безпеки інформаційних систем у критичних об'єктах можна впровадити спеціалізовані центри та залучити кваліфікованих фахівців з кібербезпеки, зокрема, такі як центри SOC (Security Operations Center) або Ситуаційні центри інформаційної безпеки. Ці структури орієнтовані на постійний моніторинг та аналіз систем захисту інформації в критичних об'єктах.

Одним з ключових аспектів їхньої роботи є виявлення аномалій та потенційних загроз, зокрема, виявлення вірусів, які можуть експлуатувати вразливості в операційних системах та програмному забезпеченні. Важливо підкреслити, що зловмисники можуть використовувати ці вразливості таким чином, що дії вірусу стають маскованими та важко виявляються засобами антивірусного програмного забезпечення. Таким чином, центри та фахівці з кібербезпеки використовують різноманітні методи та інструменти для детектування та реагування на подібні загрози, щоб забезпечити найвищий рівень безпеки для інформаційних ресурсів критичних об'єктів.

Співробітники центрів SOC володіють важливим завданням — вчасно виявляти аномальні події та несправжні дії, що можуть становити загрозу для інформаційної безпеки КМ (критичних об'єктів). Серед потенційних аномалій, які зацікавлені виявити співробітники, можуть бути такі:

— несподівана зміна кількості змінених файлів: велика кількість файлів, які були змінені за короткий період, може свідчити про потенційно шкідливі дії;

— нетиповий обсяг трафіку: надзвичайно великий обсяг трафіку до різних ресурсів може бути ознакою DDoS—атаки, що вимагає уваги фахівців;

— велике споживання ресурсів: занадто велике споживання системних ресурсів може вказувати на несанкціонований доступ або інші аномалії.

Центри SOC, або Центри Операцій Безпеки, виконують комплекс завдань для забезпечення безпеки КМ:

— постійний моніторинг та виявлення аномалій: вони безперервно відстежують події та вторгнення в КМ та КСМ, аналізуючи їх для виявлення потенційних загроз;

— запобігання кіберзагрозам: розробляють та впроваджують заходи, спрямовані на запобігання можливим кіберзагрозам, прагнучи забезпечити безпеку ще до їхньої активізації;

— сканування та моніторинг вразливостей: проводять постійне сканування та моніторинг для виявлення вразливостей у системах та аналізують інциденти для постійного вдосконалення заходів безпеки;

— ефективна реакція на інциденти: реагують на підтверджені інциденти негайно, надаючи відповідну реакцію для усунення загрози. Важливо розрізняти помилкові спрацьовування та фокусуватися на справжніх загрозах для максимально ефективного захисту інформаційних ресурсів.

3.2 Моніторинг безпеки в КМ в парадигмі тріади SIEM—EDR—NDR

З метою вдосконалення функціонування центрів SOC, провідна аналітична компанія Gartner представила концепцію SOC Visibility Triad. Цей інноваційний підхід є мережево-орієнтованою структурою, спроектованою для ефективного виявлення, реагування та управління інформацією щодо моніторингу безпеки в комп'ютерних мережах. Завдяки цій новій технології компанії можуть досягти підвищеного рівня захисту своїх інформаційних ресурсів.

Коли всі три ключові компоненти тріади SOC взаємодіють, команди SOC отримують повний обсяг перегляду кібермережі, що значно поліпшує ефективність моніторингу. SOC Visibility Triad складається з трьох відокремлених компонентів: SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response) і NDR (Network Detection and Response). Кожен із цих компонентів взаємодіє, доповнюючи один одного, та формує інтегровану та комплексну систему кібербезпеки.

У цій новій парадигмі тріади, система SIEM відповідає за виявлення, реєстрацію, ідентифікацію та аналіз повідомлень про кібербезпеку, які впливають на мережу. Це здійснюється в режимі реального часу за допомогою збору та аналізу даних з різних джерел у мережі. Такий підхід забезпечує повний моніторинг кібермережі і дозволяє центру SOC швидко реагувати на кіберзагрози та проводити їх докладний аналіз.

Коли SIEM використовується ізольовано, без інтеграції EDR і NDR, існує ймовірність упущення експлойтів та вразливостей, які не фіксуються у журналах SIEM, і це може створити так звані "сліпі зони". Для повного охоплення потенційних загроз необхідно використовувати комплексний підхід.

EDR спрямовується на збір та аналіз даних з кінцевих точок і може автоматично реагувати на загрози на цих точках. Проте, EDR сам по собі не є

достатньою гарантією повного захисту, оскільки не контролює рух зловмисного трафіку та охоплює лише обмежену частину мережевої інфраструктури.

NDR взаємодіє з усіма трьома компонентами центру SOC, надаючи повний обсяг інформації про стан мережі та захищаючи її від можливих внутрішніх та зовнішніх атак. Значущою перевагою NDR є можливість ефективно захищати мережу від зловмисників, які переміщаються в ній, ускладнюючи їм завдання нанесення шкоди після вторгнення. Дозволяючи командам SOC оперативно аналізувати дані мережі з різних точок зору, NDR обмежує час, протягом якого зловмисник може залишатися в мережі, і зменшує загрозу вторгнення. Такий комплексний підхід є ефективним засобом забезпечення повного кіберзахисту.

3.3 Метод інтеграції SIEM та її агентів в середовище

У цій частині нашої роботи розглянемо метод інтеграції системи SIEM в ELK Stack. ELK Stack та, зокрема, роботу обробки журналів подій від агента і SIEM, який є квінтесенцією із трьох потужних інструментів: Elasticsearch, Logstash і Kibana, які використовуються взаємодіючи для обробки та аналізу даних. Процесу обробки журналів подій дозволяє переглядати журнали з різних систем і програм, аналізувати їх та створювати візуалізації для моніторингу програм та інфраструктури. Також це сприяє швидкому виявленню загроз, проведенню аналізу безпеки, та інтеграції агентів.

Зокрема, у цьому дослідженні ми вибрали конкретну систему Wazuh SIEM. Wazuh об'єднує різні функції в єдину архітектурну систему, яка складається з агента та платформи, і забезпечує безпеку кінцевих точок, виявлення загроз, операції безпеки та хмарну безпеку.

У рамках цього дослідження ми розглядаємо можливість використання агента FileBeat та Wazuh Agent під час роботи процесу обробки журналів подій. FileBeat агент працює, збираючи log—повідомлення з log—файлів і передаючи їх в ELK Stack для індексації. Wazuh Agent, з свого боку, активно працює на кінцевих

точках, які користувач хоче відстежувати. Він взаємодіє з системою Wazuh SIEM майже в режимі реального часу через зашифрований та автентифікований канал.

На рис. 3.1 зображено структурну схему методу інтеграції Wazuh SIEM та запуску агентів FileBeat та Wazuh Agent із застосуванням процесу обробки журналів подій та вдосконаленим принципом роботи EDR.

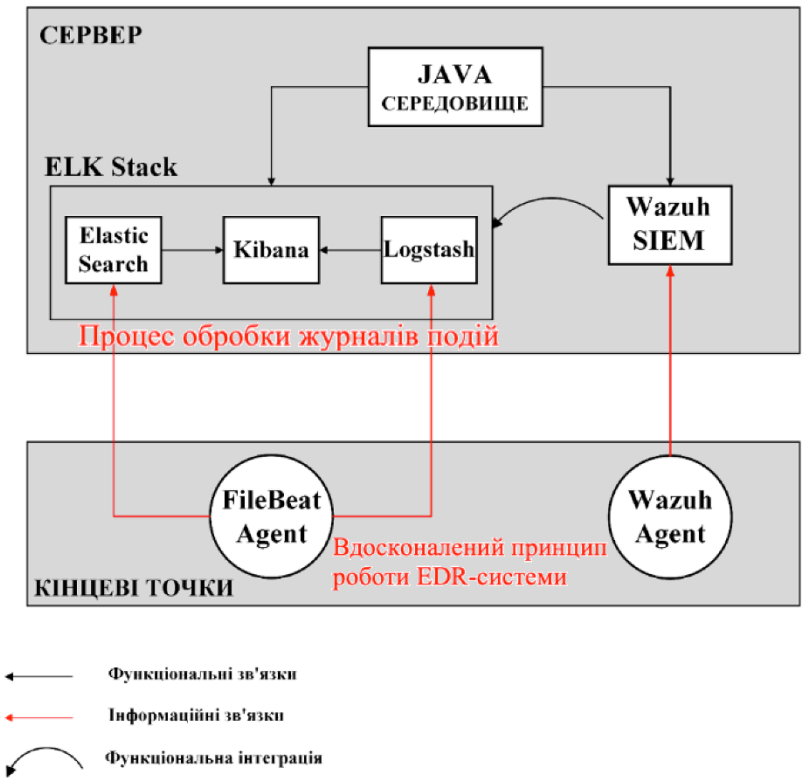


Рисунок 3.1 — Структурна схема методу інтеграції SIEM в ELK Stack та запуску агентів

3.4 Алгоритм інтеграції системи Wazuh SIEM та запуску агентів

Процеси інтеграції системи Wazuh SIEM та запуску агентів можна визначити за наступним алгоритмом, який подано відповідно до схеми на рис. 3.2.:

— встановлення та налаштування ОС Ubuntu 20.04 на Oracle VM VirtualBox: для забезпечення правильної роботи подальших процесів інтеграції;

— налаштування двонапрямленої передачі файлів та спільного Буфера: щоб забезпечити зручність обміну даними;

— встановлення Java на ОС Ubuntu: для забезпечення запуску різноманітних компонентів;

— налаштування змінних середовища JAVA_HOME: щоб визначити шлях до встановленого середовища Java та забезпечити правильну роботу з іншими програмами;

— встановлення, ралаштування та тестування ELK Stack 8 на ОС Ubuntu: протестуємо його для визначення ефективності та правильності конфігурації;

— встановлення та налаштування агента Filebeat на ОС Ubuntu: для забезпечення збору та передачі log—повідомлень у ELK Stack;

— встановлення системи Wazuh SIEM: для забезпечення повноцінного контролю над безпекою;

— інтеграція Wazuh SIEM в середовище ELK Stack: для оптимізації процесів моніторингу та аналізу;

— встановлення та демонстрація роботи Wazuh Agent на ОС Windows та Wazuh SIEM: для повного охоплення функціональності.

3.5 Використані апаратні та програмні компоненти

Для налагодження та формування віртуальних мереж та середовища використовується різноманітна сукупність апаратних і програмних компонентів, що детально розглядаються та перелічені в таблиці 3.1. Важливо відзначити, що правильний вибір цих компонентів є ключовим етапом у розробці ефективного та оптимального віртуального середовища.

Зокрема, до апаратних компонентів можуть входити сервери, мережеві комутатори, маршрутизатори та інші пристрої, які забезпечують необхідні обчислювальні та комунікаційні ресурси. У контексті програмних компонентів

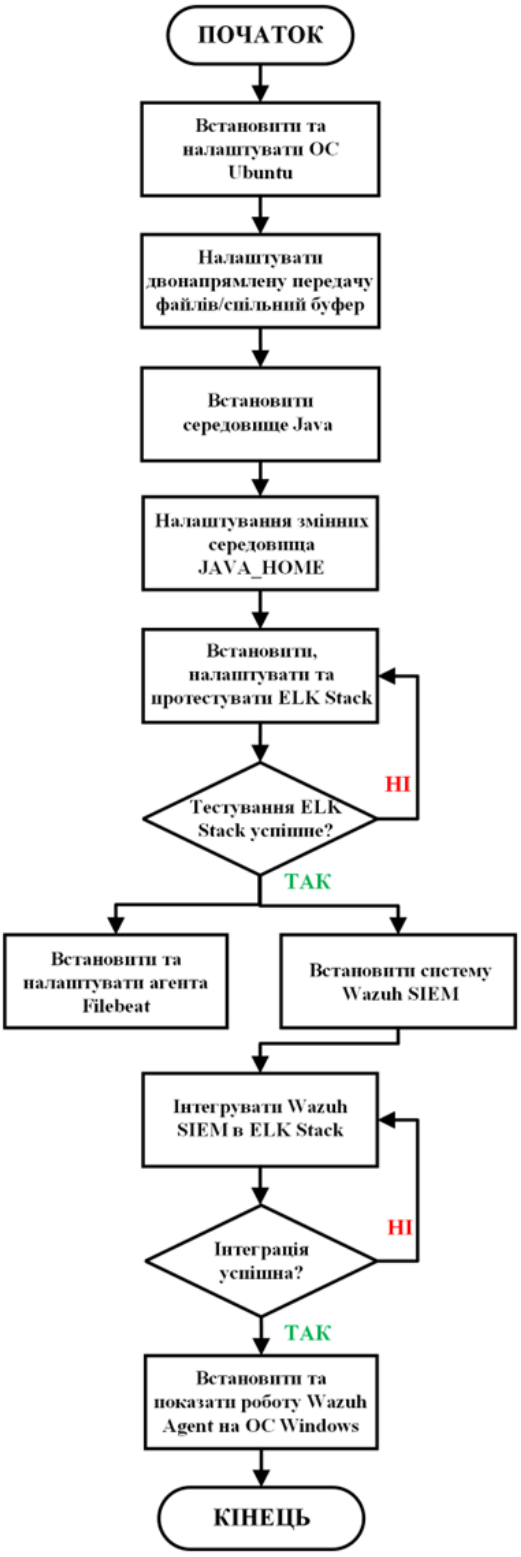


Рисунок 3.1 — Алгоритм процесу інтеграції системи Wazuh SIEM

можуть використовуватися віртуалізаційні платформи, гіпервізори, програмні інструменти для управління віртуальними мережами та інші рішення,спрямовані на оптимізацію роботи віртуального середовища.

Важливим аспектом є також належне налаштування і взаємодія всіх цих компонентів для забезпечення найвищого рівня продуктивності та ефективності віртуальної мережі. Такий підхід дозволяє створити стійке та динамічне середовище, що задовольняє всі потреби проекту та користувачів.

Для створення віртуальних мережі і середовища використана низка апаратних та програмних компонентів, які наведені в таблиці 3.1.

Таблиця 3.1 — Апаратні та програмні компоненти

	Операційна система	Відкриті порти	Реалізовані програми
Сервер	Ubuntu 20.04	Elasticsearch: 9200 TCP Kibana: 5601 TCP Logstash: 5044 TCP Filebeat: 5044 TCP Wazuh SIEM: 55000/TCP	ELK Stack 8 Filebeat Wazuh SIEM
Кінцеві точки	Ubuntu 20.04 Windows 10	Filebeat: 5044 TCP Wazuh Agent: 1514 TCP	Filebeat Wazuh Agent

Для оптимальної роботи системи було визначено конфігурацію операційної системи та портів, які використовуються для забезпечення взаємодії різних програм. На сервері, який працює на Ubuntu 20.04, відкриті порти для Elasticsearch (9200 TCP), Kibana (5601 TCP), Logstash (5044 TCP), Filebeat (5044 TCP) та Wazuh SIEM (55000/TCP). Це надає можливість ефективної комунікації та обміну даними між цими компонентами ELK Stack 8, Filebeat та Wazuh SIEM.

Щодо кінцевих точок, які включають Ubuntu 20.04 та Windows 10, визначені відкриті порти для Filebeat (5044 TCP) та Wazuh Agent (1514 TCP). Це необхідно для забезпечення збору та передачі log—повідомлень з цих кінцевих точок до центральної системи моніторингу та аналізу. Така конфігурація забезпечує надійність та безпеку обміну інформацією в рамках встановленого віртуального середовища.

4 ДОСЛІДЖЕННЯ МЕТОДУ ІНТЕГРАЦІЇ СИСТЕМИ SIEM ТА РОБОТИ АГЕНТІВ В СЕРЕДОВИЩІ ELK STACK

У четвертому розділі планується розглядати процеси дослідження та реалізації системи SIEM та агентів та аналізувати результати роботи агента і системи SIEM.

4.1 Розгортання кросплатформеної ОС на віртуальній машині та розробка спільного буферу

В першу чергу створили віртуальну машину, виділивши 4048 МБ для оперативної пам'яті та 16 МБ для відеопам'яті. Завантажили образ Ubuntu 20.04 вагою 40 ГБ безпосередньо з офіційного сайту та інтегрували його у віртуальну машину. Окремо використали вбудований оптичний привід Oracle VM VirtualBox для спільного буфера, який має об'єм понад 50 МБ.

Після запуску віртуальної машини виконали інсталяцію Ubuntu 20.04, під час якої визначили мову клавіатури, регіон та обрали параметри запуску програм. Вибрали "Normal Installation" для повного встановлення офісного програмного забезпечення. Після цього здійснили реєстрацію та створили пароль. Після завершення встановлення віртуальна машина перезавантажилась для належного функціонування.

Для налаштування спільного буфера та двонапрямленої передачі вибирали оптичний привід VBoxGuestAdditions.iso та активували дозвіл «двонапрямлений» у конфігураціях віртуальної машини.

Після цього в операційній системі з'являється файл VBox_GAs_7.0.8, який потрібно запустити та дочекатись повного встановлення. Застосування цього налаштування є обов'язковим, оскільки воно сприяє полегшенню подальших дій та встановленню програм, забезпечуючи оптимальні умови для ефективної роботи віртуального середовища.

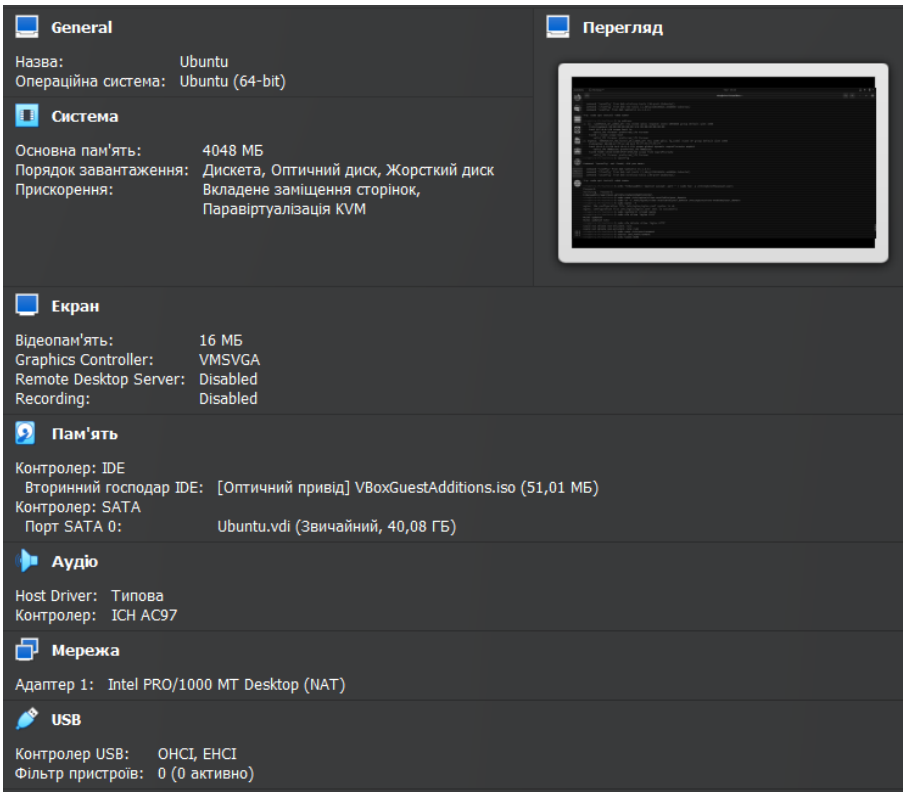


Рисунок 4.1 — Налаштування віртуальної машини

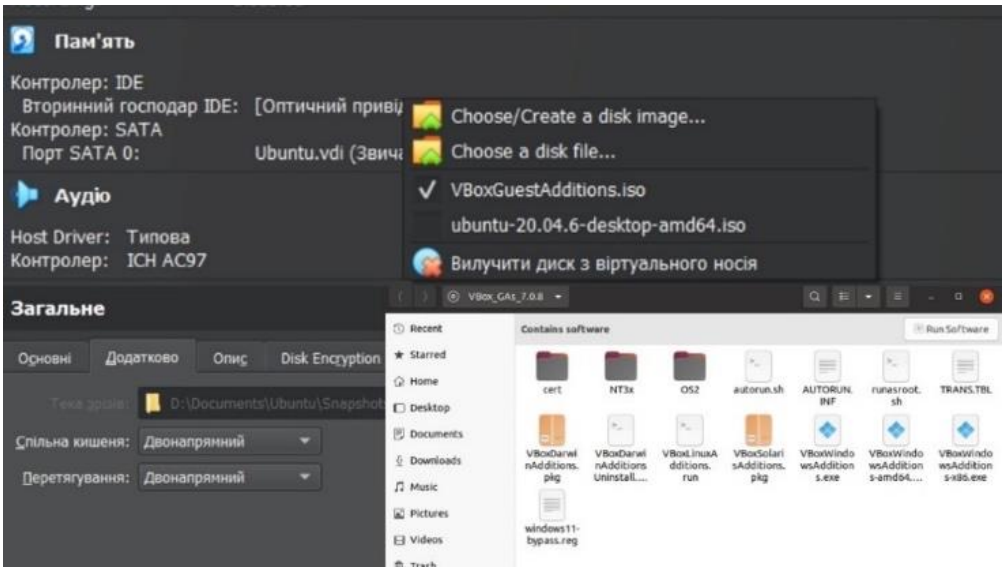


Рисунок 4.2 — Налаштування спільного буферу та двонапрямленої передачі

4.2 Встановлення та налаштування середовища програмування в межах віртуалізованої ОС

Перед тим як встановлювати середовища програмування Java, було виконано встановлення пакету apt—transport—https, що дозволяє забезпечити доступ до репозиторію через протокол HTTPS. Виконаємо встановлення OpenJDK 11 на ОС Ubuntu (рис. 4.4), та перевіримо актуальну версію Java.

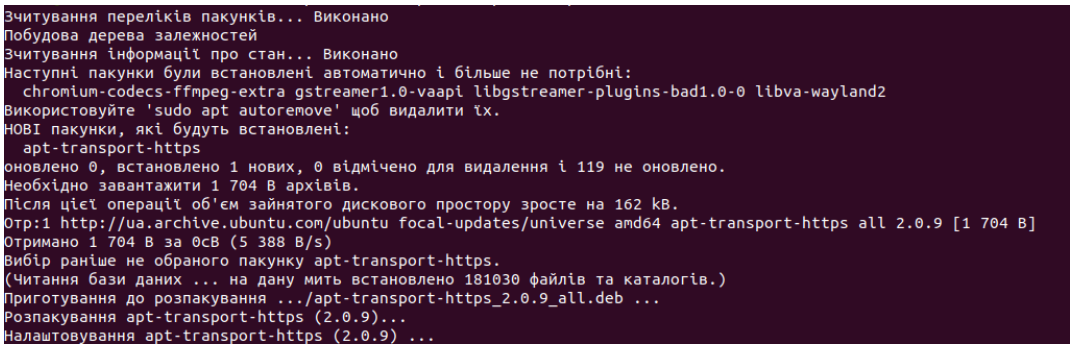


Рисунок 4.3 — Встановлення пакету доступу сховища через HTTPS

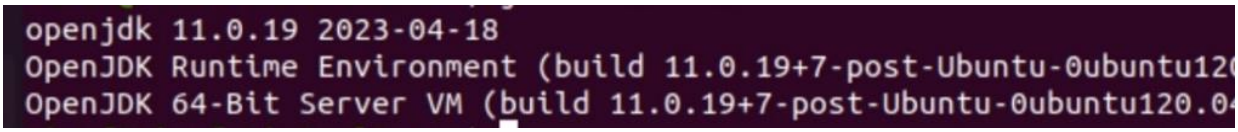


Рисунок 4.4 — Встановлення OpenJDK 11

Рисунок 4.5 — Конфігурація nano файлу

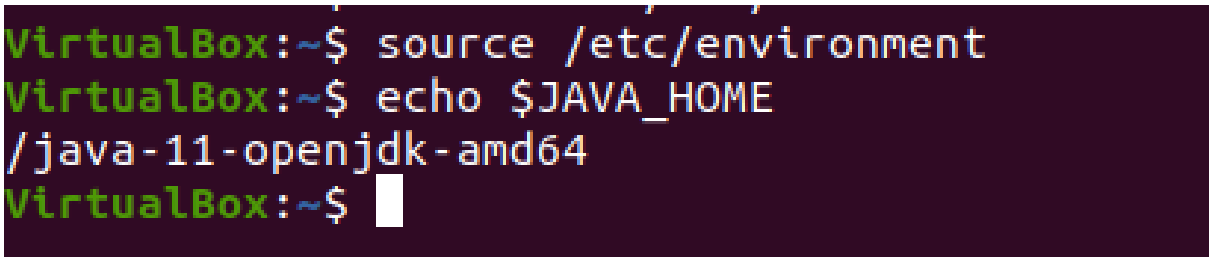


Рисунок 4.6 — Змінна середовища та перевірка коректності встановлення

Для визначення змінної середовища слід відкрити файл «/etc/environment» у редакторі nano, де вводиться команда «JAVA_HOME="/usr/lib/jvm/java—11—openjdk—amd64» для правильного функціонування середовища. Після цього ми завантажуємо змінну середовища за допомогою «source /etc/environment» та перевіряємо правильність встановлення. Таким чином, оточення Java налаштовано і готове до подальшої роботи.

4.3 Конфігурування середовища ELK Stack 8

Перше, що робиться, — це встановлення ElastickSearch. Ми завантажуємо та встановлюємо відкритий ключ підпису (див. рис. 4.7). Після цього ми виконуємо саме встановлення ElasticSearch за допомогою команд, які представлені на Рис 4.8, і запускаємо систему. На заключному етапі ми перевіряємо статус системи ElasticSearch, щоб впевнитися, що вона активна та працює нормально.

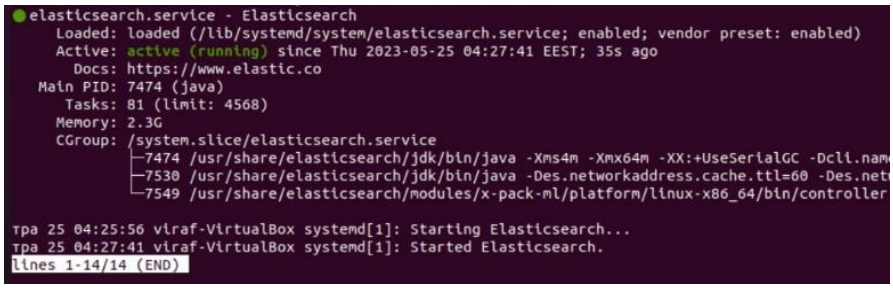


Рисунок 4.7 — Встановлення Elasticsearch; запуск, увімкнення та перевірка роботи системи

Рисунок 4.8 — Встановлення відкритого ключа підпису

Налаштування Elasticsearch проводиться в текстовому редакторі nano, в файлі «/etc/elasticsearch/elasticsearch.yml». Перший етап включає перехід до секції «Network», де необхідно розкоментувати рядок поблизу network.host і замінити свій системний IP на network.host: 0.0.0.0. Також важливо додати новий рядок discovery.seed_hosts: [ ] у секцію «Discovery», як показано на рис. 4.9. На другому етапі ми переходимо до початку автоматичної конфігурації безпеки, де замінюємо значення true на false, згідно з рис. 4.10. Після внесення змін у файл конфігурації, необхідно перезавантажити систему за допомогою команди: sudo systemctl restart elasticsearch.

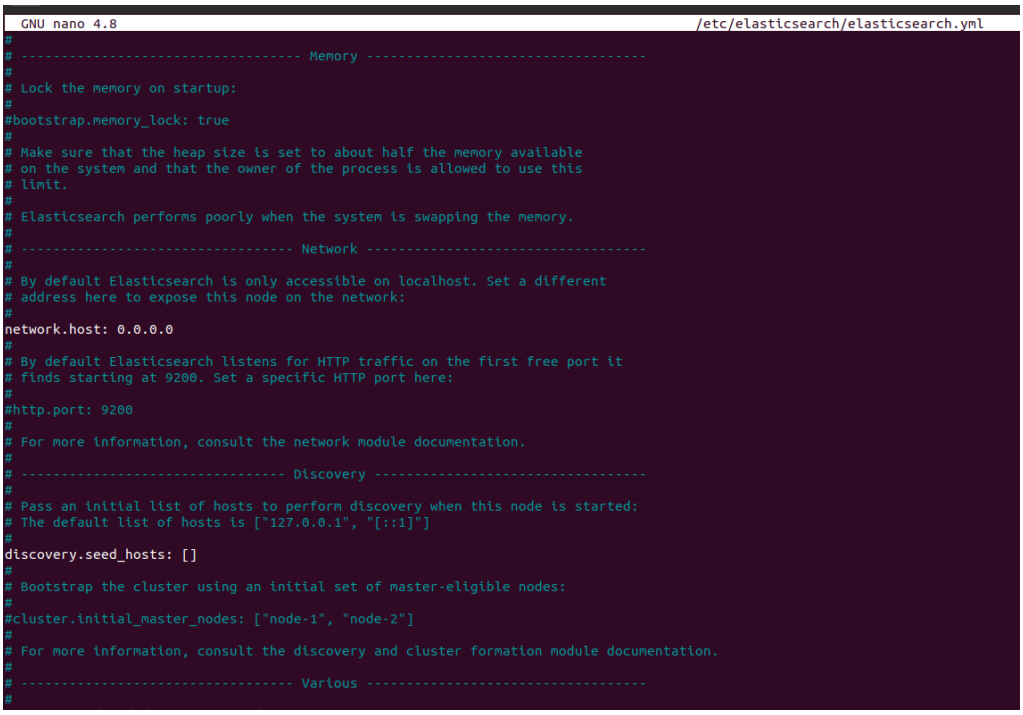


Рисунок 4.9 — Конфігурація nano файлу

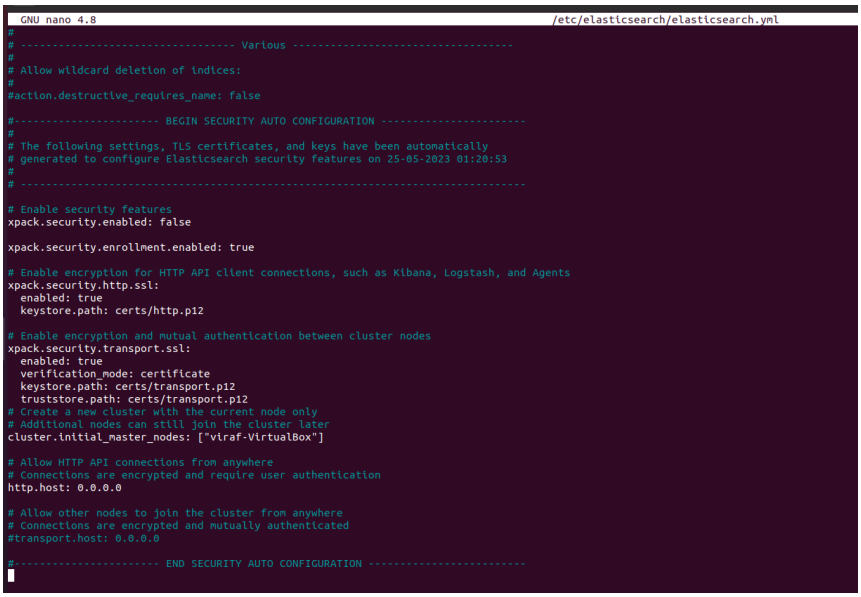


Рисунок 4.10 — Автоматична конфігурація безпеки системи

Переконаймось у правильному функціонуванні Elasticsearch, використовуючи команду curl та відправляючи HTTP—запит. Як показано на рис. 4.11 у командному рядку, доступ вказаний правильно. Також перевіримо доступ через браузер, відкривши http://10.0.2.15:9200. Elasticsearch працює коректно, і ми можемо перейти до наступних етапів налаштування.

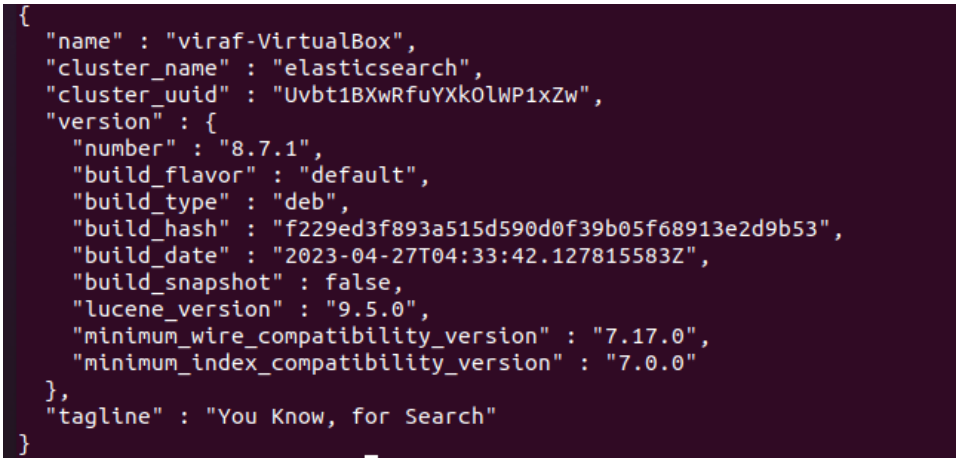


Рисунок 4.11 — Перевірка роботи Elasticsearch в командному рядку

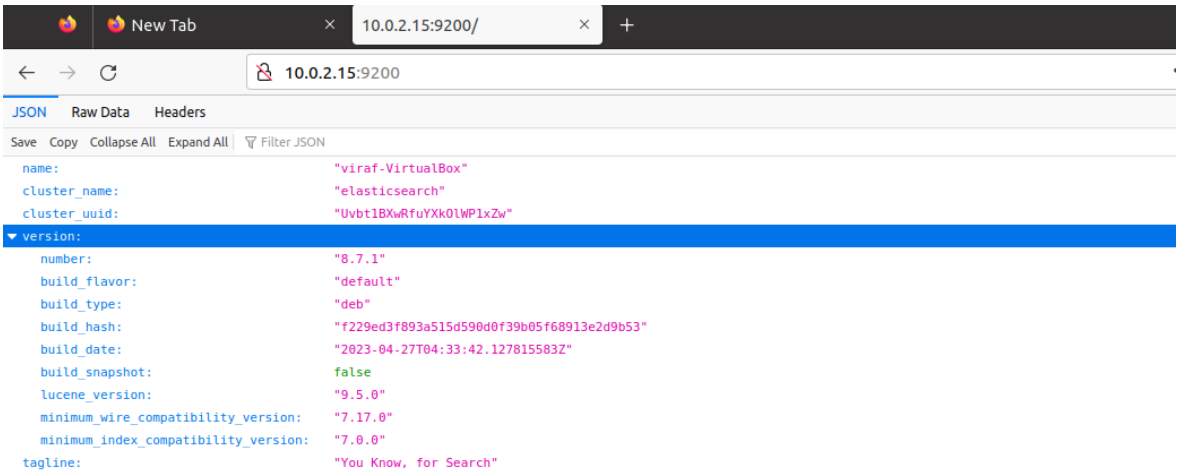


Рисунок 4.12 — Перевірка роботи Elasticsearch в браузері

Переходимо до процесу встановлення Logstash — інструменту, який збирає дані з різних джерел. Зібрані дані піддаються аналізу у Kibana та зберігаються у Elasticsearch. Виконуючи аналогічний алгоритм, який використовували з Elasticsearch, ми встановлюємо, запускаємо та активуємо службу Logstash. Далі ми перевіряємо статус служби за допомогою знайомої команди sudo systemctl status logstash. Результат показує, що Logstash активний і працює коректно. На даному етапі жодних змін у файлі nano не вносимо.

Рисунок 4.13 — Повне встановлення та налаштування Logstash

Центральний елемент — Kibana. Kibana представляє собою інтерфейс користувача з графічною оболонкою для аналізу та інтерпретації зібраних журнальних файлів. Цей інструмент дозволяє проводити налаштування, конфігурацію та інтеграцію різних систем, агентів та програмного забезпечення. Дотримуючись відомого алгоритму, ми встановлюємо, запускаємо та активуємо

службу Kibana. Перевіряємо статус служби, як показано на рис. 4.14, і бачимо, що вона активна та працює належним чином.

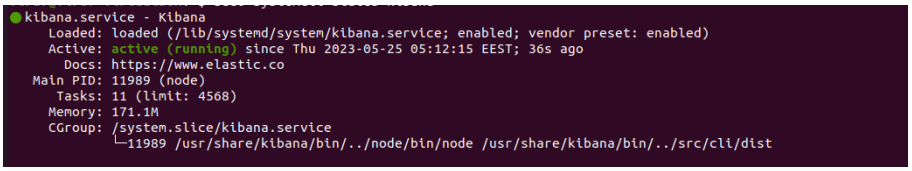


Рисунок 4.14 — Встановлення служби Kibana

Конфігурація Kibana проводиться шляхом редагування файлу «/etc/kibana/kibana.yml» за допомогою текстового редактора nano: server.port: 5601, server.host: "localhost", elasticsearch.hosts: ["http://localhost:9200"]. Здійснюється заміна server.host: "localhost" на server.host: "0.0.0.0", що індикує призначення будь—якої IP—адреси. Після внесення змін у файл конфігурації виконується перезавантаження Kibana.

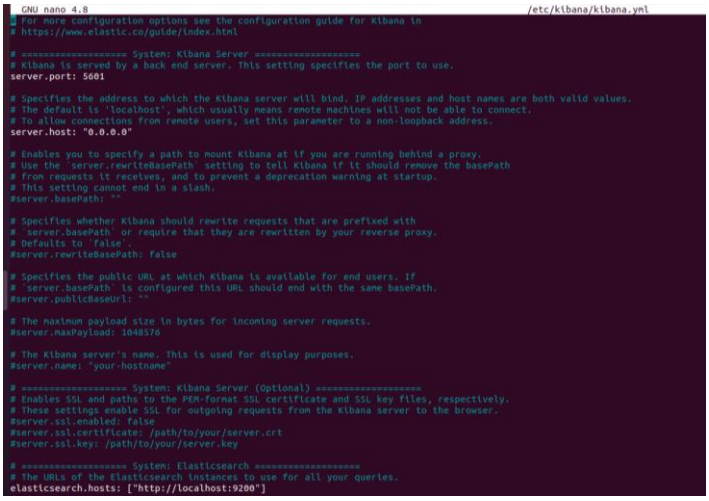


Рисунок 4.15 — Конфігурація nano файлу Kibana

Проведемо випробування Kibana. Для отримання доступу до середовища використаємо веб—браузер і перейдемо за наступною веб—адресою:

http://10.0.2.15:5601. Відкривається саме середовище Elastic, в якому будуть моніторитися всі зміни та дія агента.

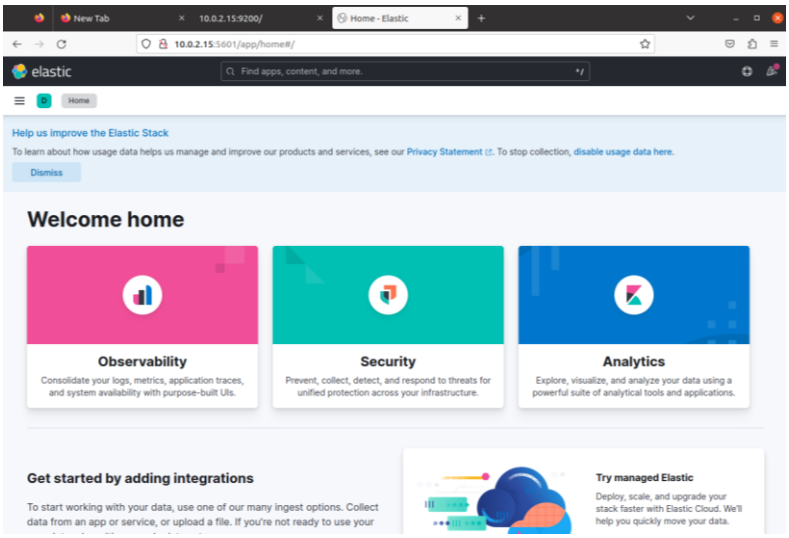


Рисунок 4.16 — Середовище Elastic

Filebeat представляє собою легкий агент або плагін, що використовується для збору та передачі файлів журналів. Цей агент є найбільш поширеним серед інших агентів Elastic Beats. Однією з ключових переваг цього агента є його здатність автоматично пристосовуватися до навантаження при переповненні служби Logstash даними. Здійснимо завантаження цього агента на операційну систему, використовуючи команду, зазначену на рис. 4.17.

Filebeat, за замовчуванням, передає дані до Elasticsearch, але його також можна налаштувати для надсилання інформації про події (Sec_Event_Logs) до Logstash.

Для внесення необхідних змін у конфігураційний файл, який розташований за адресою /etc/filebeat/filebeat.yml, необхідно закоментувати рядки в розділі "Elasticsearch Output": # output.elasticsearch, # Array of hosts to connect to, # hosts: ["localhost:9200"]. В той же час рядки в розділі "Logstash Output" повинні бути розкоментовані: output.logstash, hosts: ["localhost:5044"].

```
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей
Зчитування інформації про стан... Виконано
Наступні пакунки були встановлені автоматично і більше не потрібні:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libgstreamer-plugins-bad1.0-0 libva-wayland2
Використовуйте 'sudo apt autoremove' щоб видалити їх.
НОВІ пакунки, які будуть встановлені:
  filebeat
оновлено 0, встановлено 1 нових, 0 відмічено для видалення і 117 не оновлено.
Необхідно завантажити 42,5 MB архівів.
Після цієї операції об'єм зайнятого дискового простору зросте на 157 MB.
Отр:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 filebeat amd64 8.7.1 [42,5 MB]
Отримано 42,5 MB за 8сВ (5 581 kB/s)
Вибір раніше не обраного пакунку filebeat.
(Читання бази даних ... на дану мить встановлено 244670 файлів та каталогів.)
Приготування до розпакування .../filebeat_8.7.1_amd64.deb ...
Розпакування filebeat (8.7.1)...
Налаштовування filebeat (8.7.1) ...
Обробка тригерів systemd (245.4-4ubuntu3.20)...
```

Рисунок 4.17 — Завантаження агента Filebeat

```
# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

# ================================== Outputs ===================================

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

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

  # 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"

# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["localhost: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 4.18 — Конфігурування nano файлу Filebeat

За внесеними конфігураційними змінами зберігаємо відредагований файл та активуємо системний модуль Filebeat. Після чого завантажуємо необхідний шаблон індексу для забезпечення правильної функціональності агента Filebeat. Далі, використовуючи стандартний алгоритм, проводимо процес встановлення, запуску та активації агента Filebeat. Для перевірки його стану використовуємо вже знайому команду sudo systemctl status filebeat.

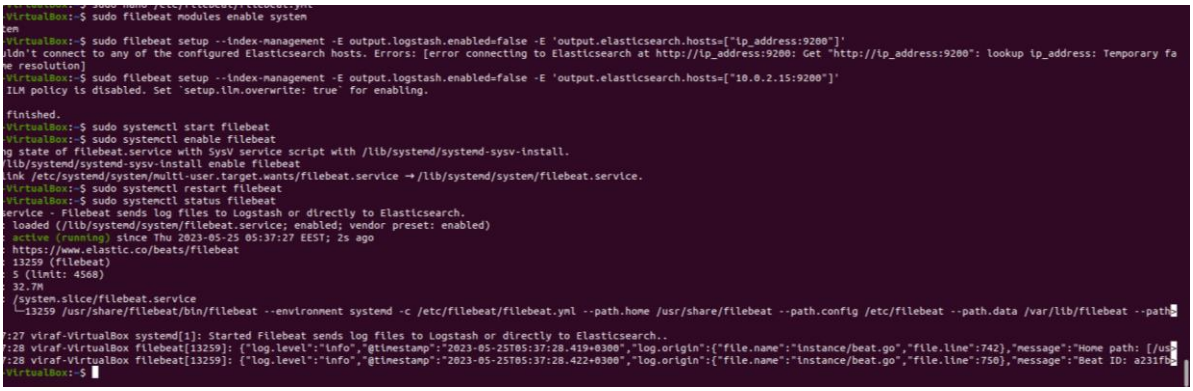


Рисунок 4.19 — Встановлення агента Filebeat

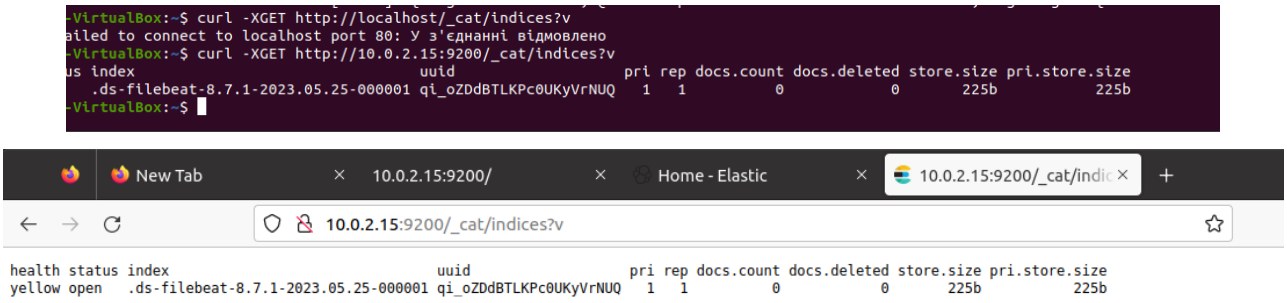


Рисунок 4.20 — Робота агента Filebeat

Перевіряємо наявність даних в Elasticsearch, які були передані агентом, щодо поточного стану системи. Для цього використовуємо посилання: http://10.0.2.15:9200/_cat/indices?v. Стан системи, її ефективність та кількість оброблених файлів є індикаторами успішної роботи агента.

4.5 Конфігурування та налаштування системи Wazuh SIEM

Перехід до розгортання та активації системи Wazuh SIEM виконується відповідно до документації [18], що ілюструється зображеннями 4.21—4.23. Очевидно, що система наразі активна і працює відповідно.

Wazuh SIEM (Security Information and Event Management) — це інтегрована система безпеки, яка надає комплексний підхід до моніторингу та управління подіями в інформаційних системах. SIEM спроектована для виявлення потенційних

загроз, аналізування подій (Sec_Event_Logs) і реагування на інциденти безпеки в реальному часі.

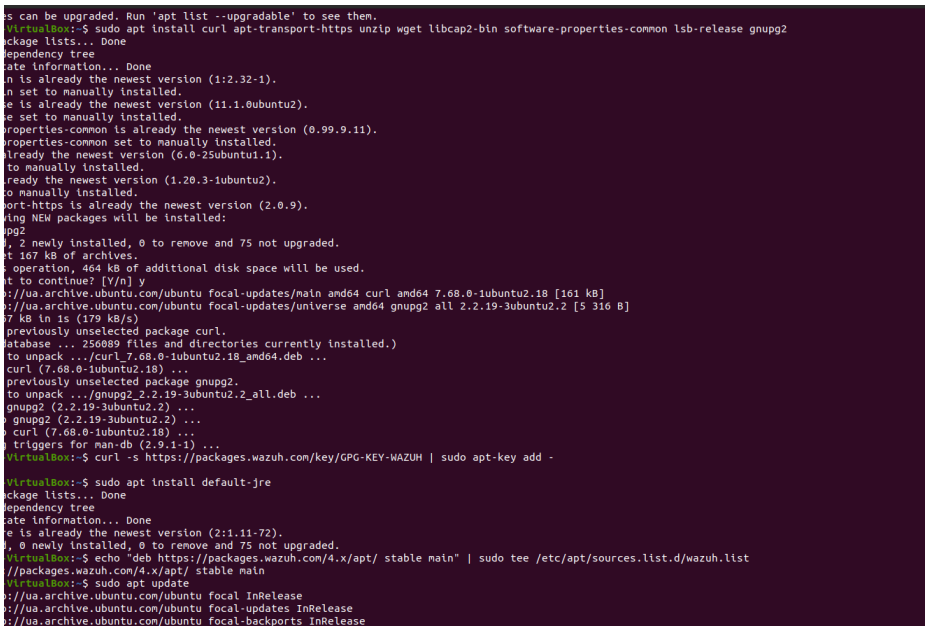


Рисунок 4.21— Встановлення Wazuh SIEM

Wazuh є відкритою платформою, яка об'єднує агентів, розгорнуті на кінцевих точках мережі, і центральний сервер для обробки та аналізу зібраних даних. Основні функції Wazuh SIEM включають моніторинг log—файлів, виявлення аномалій, реагування на інциденти, аудит безпеки та інші аспекти кібербезпеки.

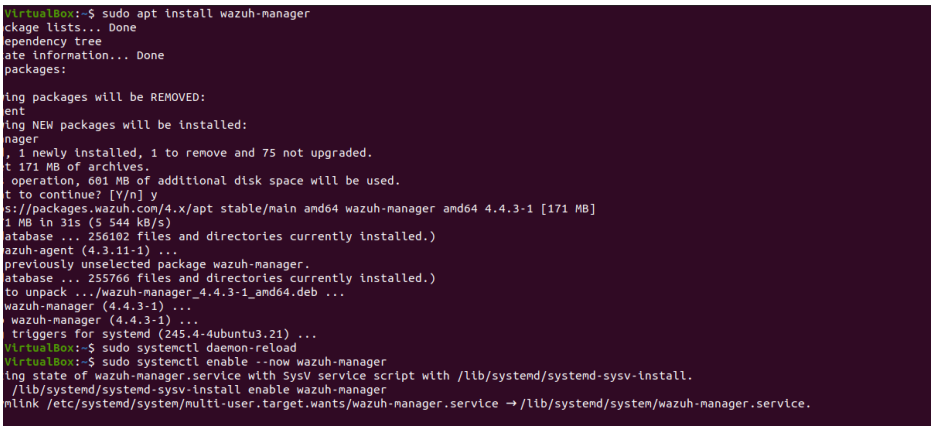


Рисунок 4.22 — Активація Wazuh SIEM

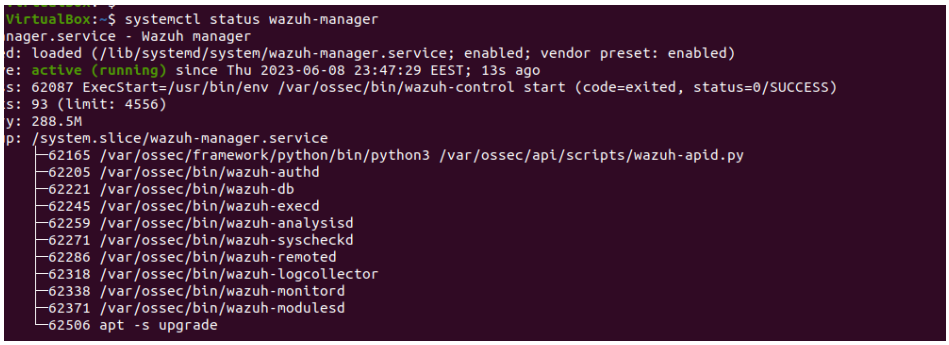


Рисунок 4.23 — Перевірка статусу Wazuh SIEM

4.6 Інтеграція системи Wazuh SIEM в середовище ELK Stack

Wazuh також володіє іншими елементами, такими як агенти для збору даних з кінцевих точок, інтеграція з ELK Stack (Elasticsearch, Logstash, Kibana) для зручного аналізу та візуалізації даних, а також елементи для виявлення вразливостей та забезпечення безпеки хмарних обчислень. Загалом Wazuh SIEM допомагає організаціям створювати ефективну систему кібербезпеки для виявлення та вирішення потенційних загроз. За допомогою директорії домашнього каталогу «/usr/share/kibana» здійснимо встановлення плагіну Kibana для Wazuh за допомогою наступної команди: sudo —u kibana /usr/share/kibana/bin/kibana—plugin install https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana—4.1.5_7.10.0—1.zip

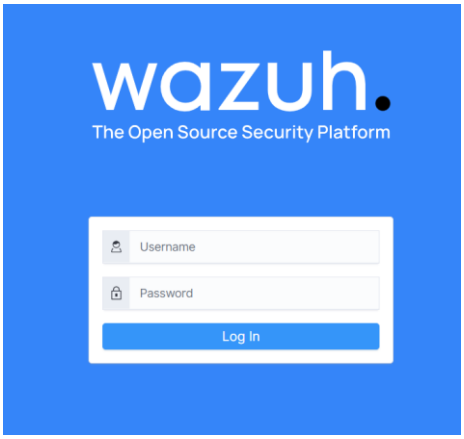


Рисунок 4.24 — Сторінка реєстрації Wazuh SIEM

Таким чином, відбулося інтегрування системи Wazuh SIEM у середовище ELK Stack. Це дозволяє звертатися до головної сторінки системи, використовуючи посилання «https://10.0.2.15», і підтверджує успішність виконаних дій.

4.7 Встановлення Wazuh Agent на ОС Windows та перевірка його роботи і системи Wazuh SIEM

Після успішної реєстрації користувача переходимо на основну сторінку Wazuh, де нам негайно пропонується додати нового агента за допомогою докладних інструкцій з щодо його встановлення. Відповідно до наведених інструкцій ми обираємо операційну систему Windows для кінцевої точки та отримуємо індивідуальний код агента з унікальним паролем для використання в консолі Windows PowerShell.

Шляхом використання команди NET START WazuhSvc ми активуємо функціонування агента Wazuh. За результатами виконання команди вбачаємо, що агент успішно запущено.

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

PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.11-1.msi -OutFile
${env:tmp}\wazuh-agent-4.3.11.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.11.msi /q WAZUH_MANAGER='qavxh6926dwv.cloud
.wazuh.com' WAZUH_REGISTRATION_SERVER='qavxh6926dwv.cloud.wazuh.com' WAZUH_REGISTRATION_PASSWORD='EbsjtJjnGTgCslQHkXM5zO
L2uxSCFsFq' WAZUH_AGENT_GROUP='default'
```

Рисунок 4.25 — Код Wazuh Agent для Windows

```
PS C:\WINDOWS\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\WINDOWS\system32>
```

Рисунок 4.26 — Запуск Wazuh Agent для Windows

Перейдемо до системи Wazuh SIEM і проводимо перевірку функціонування агента. На екрані відображається панель, що демонструє активність та інформацію про наш Wazuh Agent для Windows, таку як його ім'я, IP—адресу, ОС кінцевої точки та його поточний статус в системі.

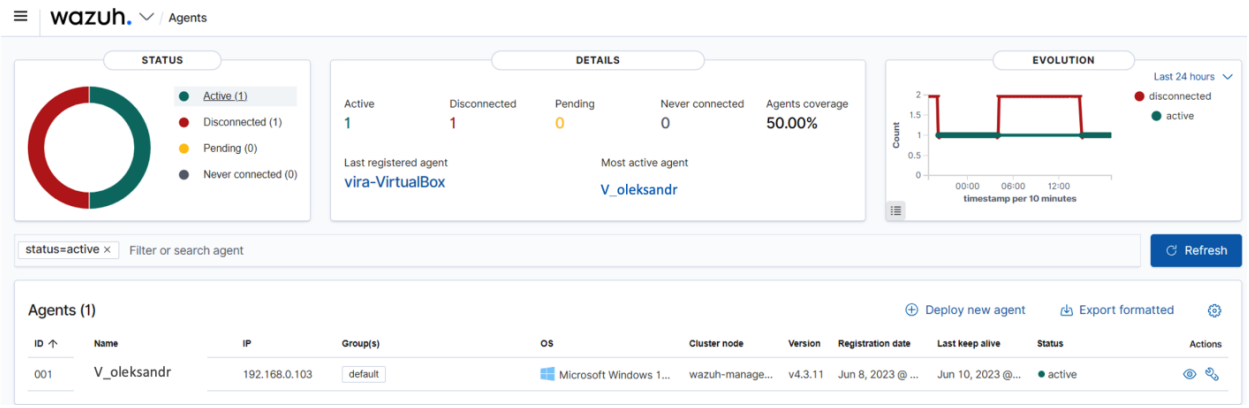


Рисунок 4.27 — Панель Wazuh SIEM для агентів

Вся інформація, яку передає агент, обробляється системою Wazuh SIEM, яка проводить нормалізацію, класифікацію та структурує дані згідно з відповідними аналітичними панелями. На рис. 4.28 є загальна аналітична панель, що надає інформацію про події безпеки, системні журнали подій, контроль цілісності інформації, останні сканування системи для виявлення вразливостей, інформацію про вторгнення та кібератаки, а також стан мережі.

4.8 Результати роботи процесу обробки журналів від агента і SIEM

По кожному конкретному виду інформації система надає деталізовані інформаційні панелі. Розглянемо їх детально.

4.8.1 Панель подій безпеки (Sec_Event_Logs)

Панель подій безпеки Sec_Event_Logs (рис. 4.29, 4.30). повідомляє про стан процесу аутентифікації користувача, виявлення можливих атак, присутність пошкоджених файлів, а також визначає рівень небезпеки, представлений числовою шкалою від 1 до 13 і так далі.

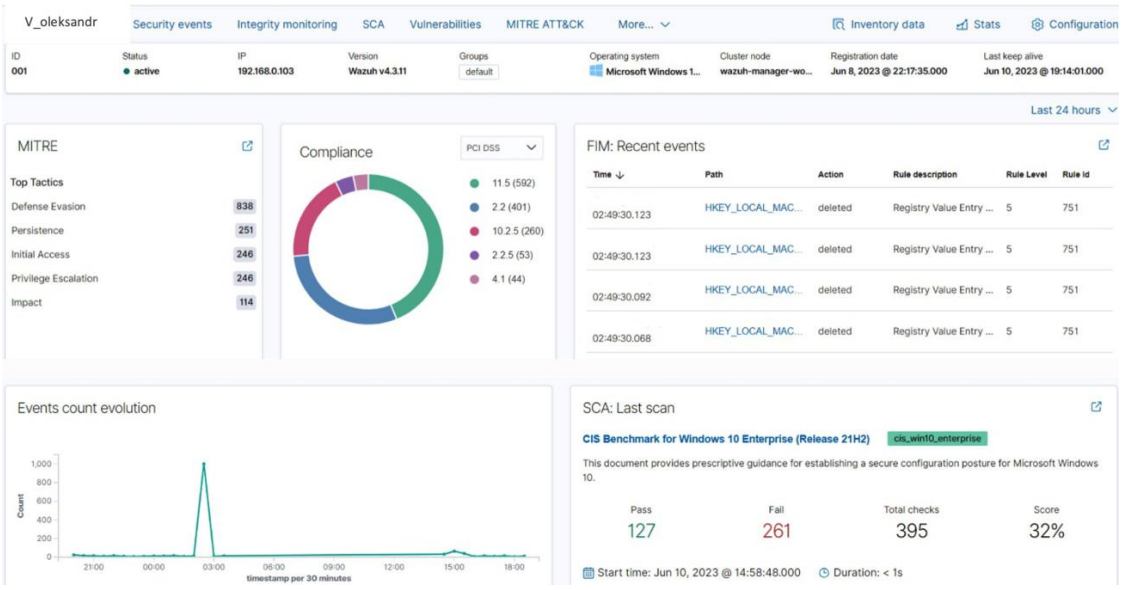


Рисунок 4.28 — Загальна аналітична панель

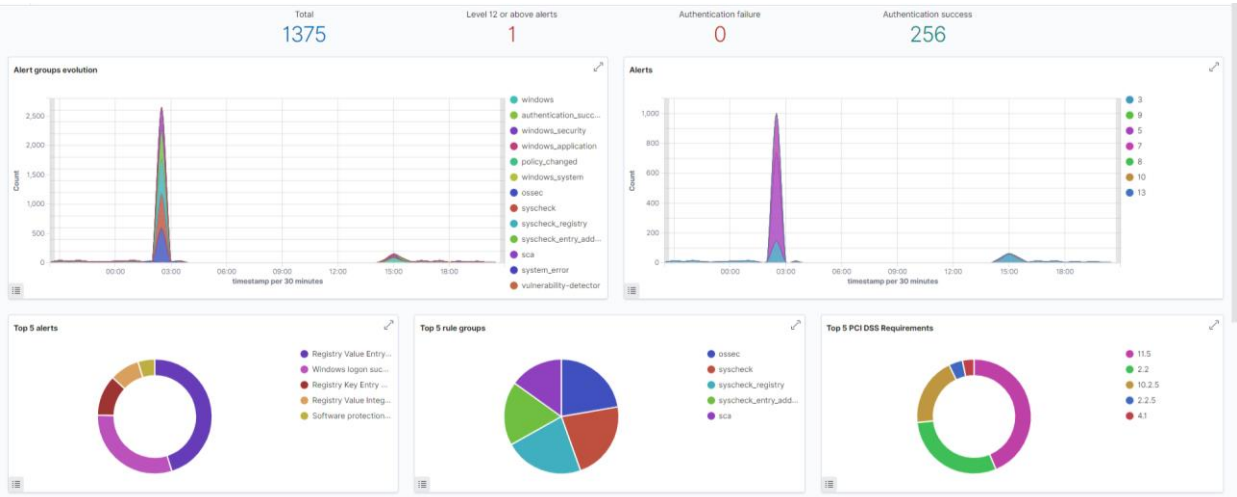
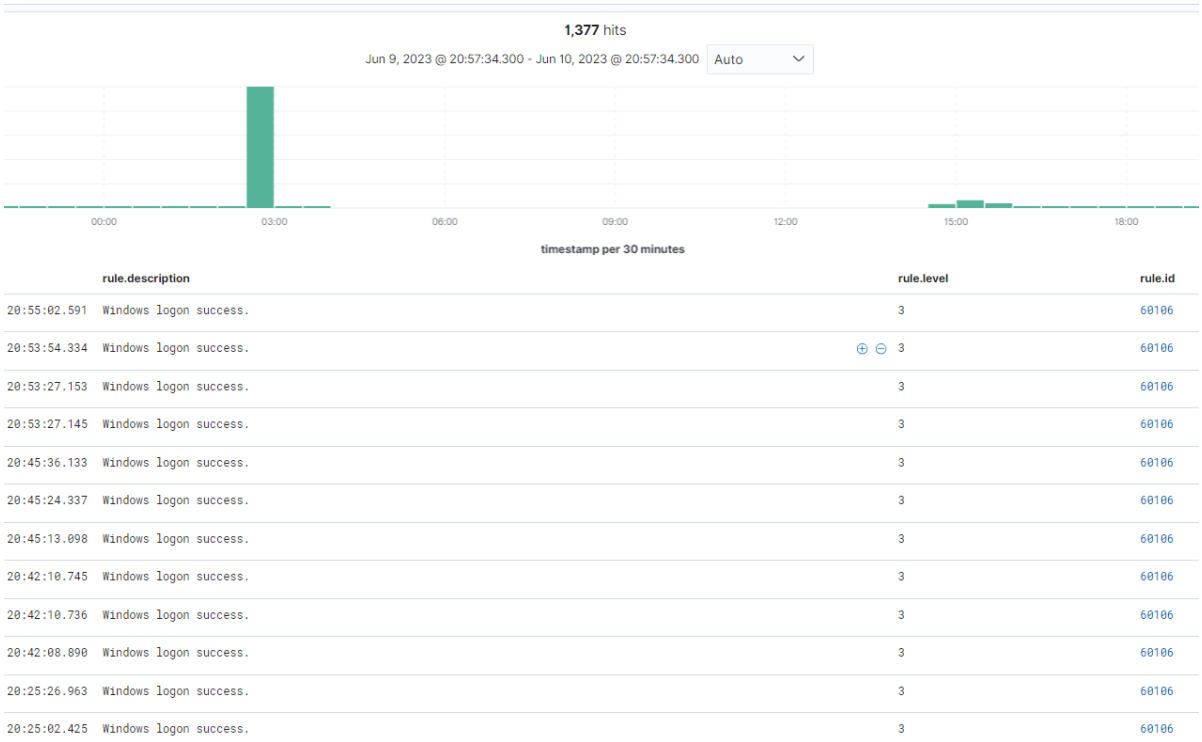


Рисунок 4.28 — Діаграми подій безпеки (Sec_Event_Logs)



	rule.description	rule.level	rule.id
20:55:02.591	Windows logon success.	3	60106
20:53:54.334	Windows logon success.	3	60106
20:53:27.153	Windows logon success.	3	60106
20:53:27.145	Windows logon success.	3	60106
20:45:36.133	Windows logon success.	3	60106
20:45:24.337	Windows logon success.	3	60106
20:45:13.098	Windows logon success.	3	60106
20:42:10.745	Windows logon success.	3	60106
20:42:10.736	Windows logon success.	3	60106
20:42:08.890	Windows logon success.	3	60106
20:25:26.963	Windows logon success.	3	60106
20:25:02.425	Windows logon success.	3	60106

Рисунок 4.29 — Перелік подій безпеки (Sec_Event_Logs)

4.8.2 Панель контролю цілісності інформації та журнал безпеки (Sec_Logs)

Панель моніторингу цілісності даних та журналу подій (Sec_Event_Logs) (див. рис. 4.31, 4.32) повідомляє стан про активність користувачів та відображає інформацію щодо додавання, зміни та видалення файлів, а також їхню цілісність.

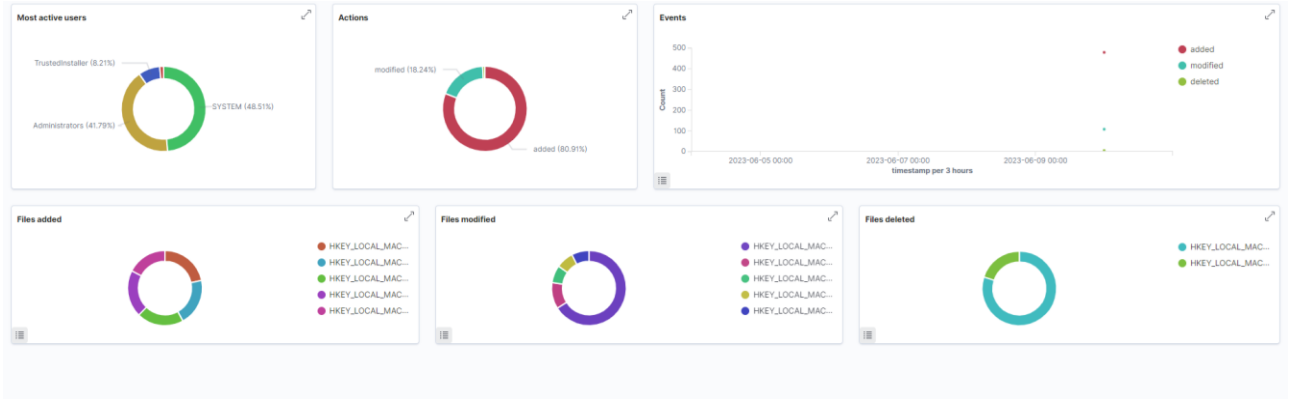
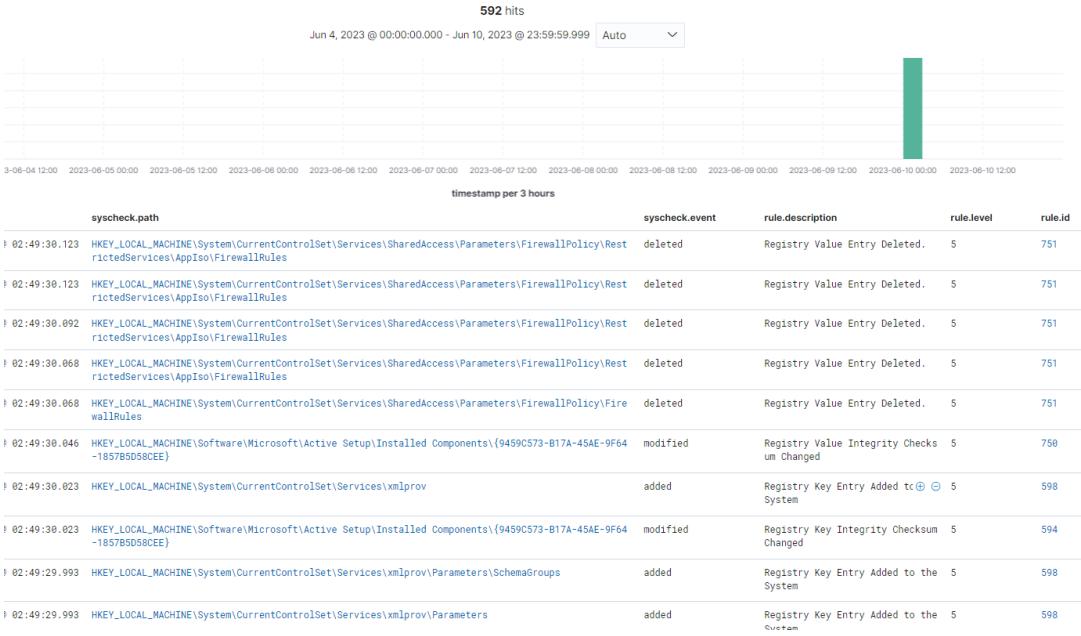


Рисунок 4.31 — Діаграма цілісності інформації та журналів подій

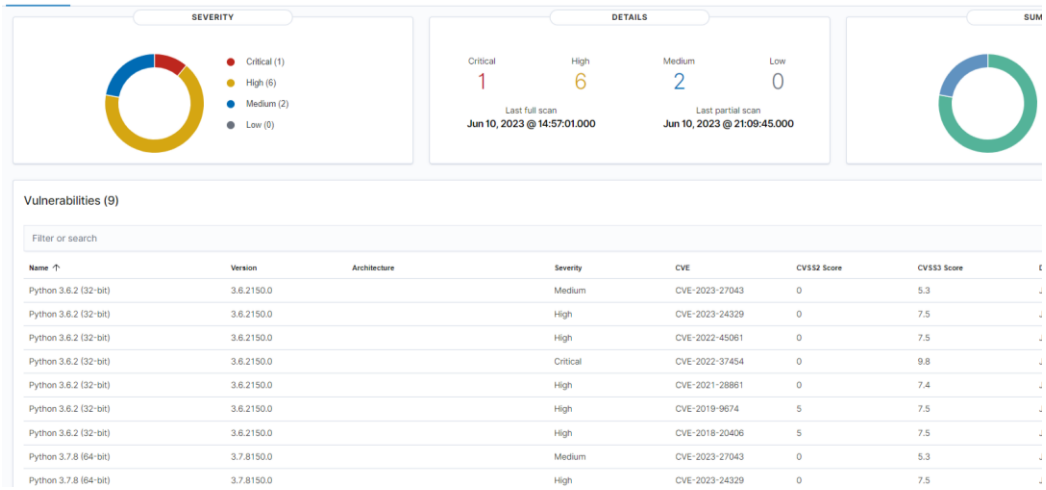
4.8.3 Панель останніх сканувань системи стосовно вразливостей

Аналітична панель, яка відображає останні сканування системи на предмет вразливостей (див. рис. 4.33), надає інформацію щодо поточних вразливостей в системі та файлах, класифікуючи їх за рівнями небезпеки.



	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
02:49:30.123	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules	deleted	Registry Value Entry Deleted.	5	751
02:49:30.123	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules	deleted	Registry Value Entry Deleted.	5	751
02:49:30.092	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules	deleted	Registry Value Entry Deleted.	5	751
02:49:30.068	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules	deleted	Registry Value Entry Deleted.	5	751
02:49:30.068	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules	deleted	Registry Value Entry Deleted.	5	751
02:49:30.046	HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{9459C573-B17A-45AE-9F64-1857B5D58CEE}	modified	Registry Value Integrity Checksum Changed	5	750
02:49:30.023	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\xmlprov	added	Registry Key Entry Added to System	5	598
02:49:30.023	HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{9459C573-B17A-45AE-9F64-1857B5D58CEE}	modified	Registry Key Integrity Checksum Changed	5	594
02:49:29.993	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\xmlprov\Parameters\SchemaGroups	added	Registry Key Entry Added to the System	5	598
02:49:29.993	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\xmlprov\Parameters	added	Registry Key Entry Added to the System	5	598

Рисунок 4.32 — Журнал безпеки (Sec_Logs)



Name	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score
Python 3.6.2 (32-bit)	3.6.2150.0		Medium	CVE-2023-27043	0	5.3
Python 3.6.2 (32-bit)	3.6.2150.0		High	CVE-2023-24329	0	7.5
Python 3.6.2 (32-bit)	3.6.2150.0		High	CVE-2022-45061	0	7.5
Python 3.6.2 (32-bit)	3.6.2150.0		Critical	CVE-2022-37454	0	9.8
Python 3.6.2 (32-bit)	3.6.2150.0		High	CVE-2021-28861	0	7.4
Python 3.6.2 (32-bit)	3.6.2150.0		High	CVE-2019-9674	5	7.5
Python 3.6.2 (32-bit)	3.6.2150.0		High	CVE-2018-20406	5	7.5
Python 3.7.8 (64-bit)	3.7.8150.0		Medium	CVE-2023-27043	0	5.3
Python 3.7.8 (64-bit)	3.7.8150.0		High	CVE-2023-24329	0	7.5

Рисунок 4.33 — Сканер вразливостей

4.8.4 Панель вторгнення і кібератак

Панель інформації про стан мережі (рис. 4.34) надає інформацію про IP—адреси та з’єднання з мережею Ethernet чи Wi—Fi. А також інформацію про вид процесору кінцевої точки, кількість ядер та об’єм пам’яті.

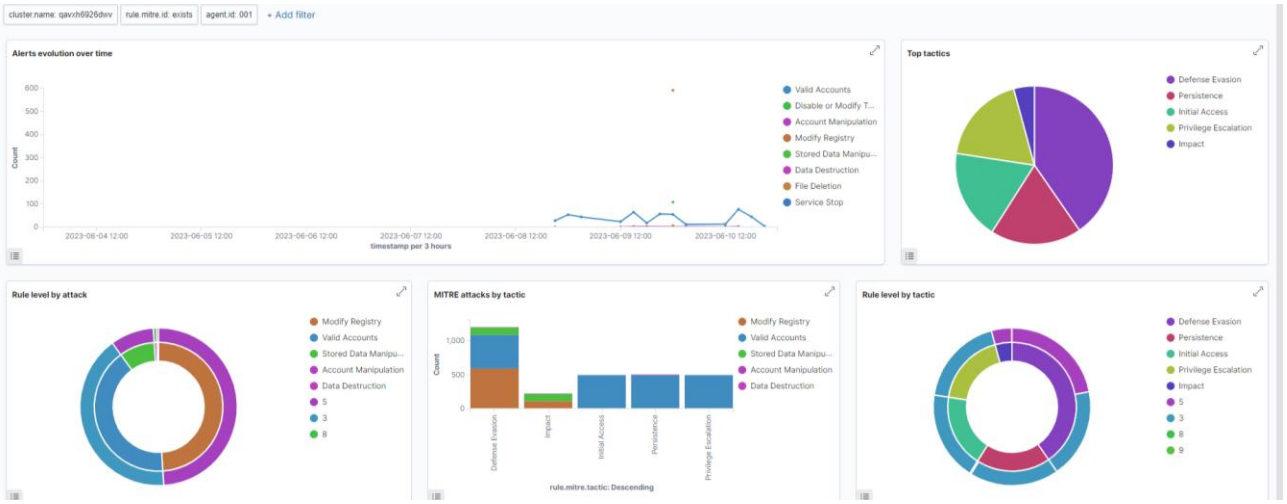


Рисунок 4.34 — Діаграма видів кібератак та рекомендації

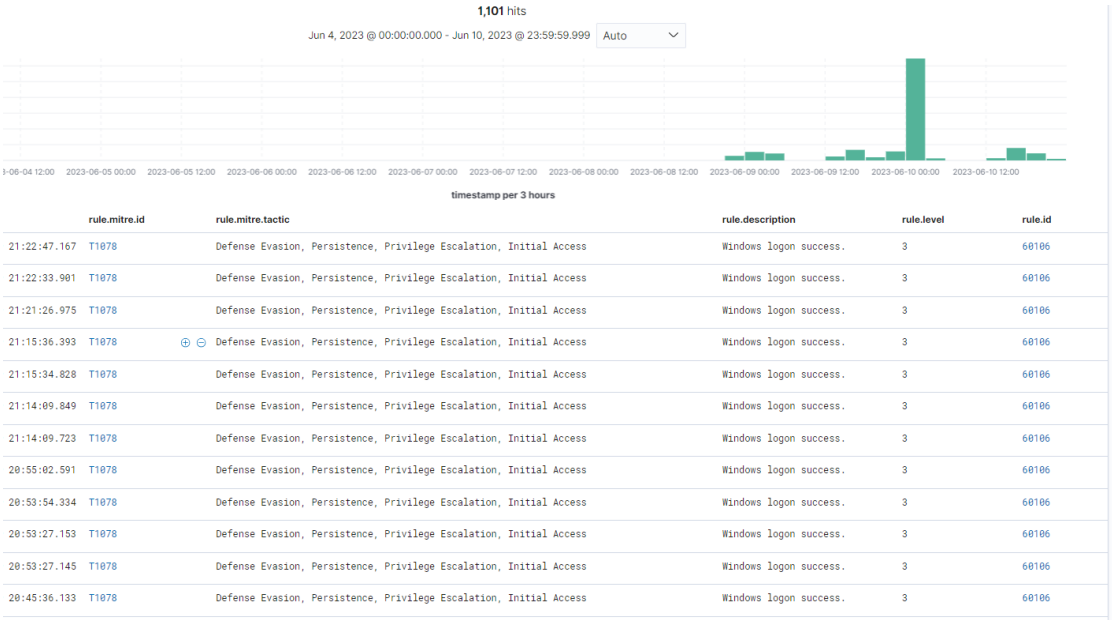


Рисунок 4.35 — Журнал кібератак

4.8.5 Панель інформації

Вибір системи Wazuh SIEM для подальшого дослідження, що базується на результаті аналізу ринку систем SIEM:

— ретельний аналіз та опрацювання алгоритму реалізації віртуального середовища ELK Stack та інтеграції з ним системи Wazuh SIEM;

— успішна установка, налаштування та запуск агентів Filebeat та Wazuh на операційній системі Ubuntu;

— отримання значущих результатів у вигляді інформаційних аналітичних панелей, які надає система SIEM адміністратору, таких як загальна аналітична панель, панелі про події безпеки, про вторгнення і кібератаки, контроль цілісності інформації, останнє сканування системи на предмет вразливостей, журнал безпеки (Sec_Logs) та інформація про стан мережі.

У випадку відсутності SIEM адміністратор мусив би отримувати всю цю інформацію від різних джерел і програм захисту, але завдяки SIEM ця інформація зручно представлена в структурованій та систематизованій формі на аналітичних панелях. Це важливо, оскільки в умовах великого обсягу подій адміністратору складно ефективно проаналізувати їх, виявити найнебезпечніші та вчасно реагувати на загрози. Таким чином, система SIEM виявляється вкрай важливою для забезпечення ефективності адміністрування та захисту інформаційно-комунікаційних мереж.

5 ЕКОНОМІЧНА ЧАСТИНА

Метою даного розділу є проведення технологічного аудиту, в даному випадку програмного алгоритму інтеграції системи SIEM у віртуальне середовище та запуску агентів. Особливістю розробки є прискорення процесів реагування на загрози мережевої безпеки завдяки вдосконаленому процесу обробки журналів в системі SIEM та оптимізованій моделі роботи EDR.

Аналогом може бути комутатор Cisco Catalyst 2960—X 48 GigE PoE 370W, який використовує аналогічний алгоритм за ціною 114 701,00 грн. або адаптивна безпека Fortinet FortiSOAR для SOC—команд — 73 313,00 грн. Для проведення комерційного та технологічного аудиту залучають не менше 3—х незалежних експертів. Оцінювання науково—технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням 5—бальної системи оцінювання за 12—ма критеріями, у відповідності із табл. 5.1.

За даними таблиці 5.2 можна зробити висновок щодо рівня комерційного потенціалу даної розробки. Для цього доцільно скористатись рекомендаціями, наведеними в таблиці безпеки інформаційних технологій 5.3.

Таблиця 5.1 — Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Бали (за 5—ти бальною шкалою)					
Кри-терій	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздат—ність продукту в реальних умовах

Продовження таблиці 5.1

Ринкові переваги					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни
4	Технічні та споживчі властивості продукту значно	Технічні та споживчі властивості продукту трохи гірші,	Технічні та споживчі властивості продукту на рівні	Технічні та споживчі властивості продукту трохи кращі,	Технічні та споживчі властивості продукту значно
5	Експлуатаційні витрати значно вищі, ніж в .	Експлуатаційні витрати дещо вищі, ніж в .	Експлуатаційні витрати на рівні експлуатаційних .	Експлуатаційні витрати трохи нижчі, ніж в .	Експлуатаційні витрати значно нижчі, ніж в .
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною
7	Активна конкуренція великих ком-	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практик на здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реа-	Необхідно наймати фахівців або витрачати значні кошти та	Необхідне незначне навчання фахівців та збільшення їх	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так із комерційної
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї .	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування

Продовження табл. 5.1

10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово—	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно ви-
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності	Термін реалізації ідеї від 3—х до 5—ти років. Термін окупності інвестицій	Термін реалізації ідеї менше 3—х років. Термін окупності	Термін реалізації ідеї менше 3—х років. Термін окупності
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних доку-	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію	Відсутні будь—які регламентні обмеження на виробництво та реалізацію продукту

Усі дані по кожному параметру занесено в таблиці 5.2

Таблиця 5.2 — Результати оцінювання комерційного потенціалу розробки

Критерії оцінювання	ПІБ експертів		
	Експерт 1	Експерт 2	Експерт 3
	Бали		
Технічна здійсненність концепції	3	4	4
Наявність аналогів на ринку	3	3	4
Цінова політика	4	4	4
Технічні та споживчі властивості виробу	4	3	3
Експлуатаційні витрати	4	4	3
Ринок збуту	4	3	4

Продовження табл. 5.2

Конкурентоспроможність	3	4	3
Фахівці з технічної і комерційної реалізації	4	3	4
Фінансування	4	4	3
Матеріально—технічна база	3	3	3
Термін реалізації ідеї	4	4	3
Супровідна документація	3	2	4
Сума	43	41	42
Середньоарифметична сума балів	(43+41+42) / 3 = 42		

Таблиця 5.3 — Рівні комерційного потенціалу розробки

Середньоарифметична сума балів, розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0—10	Низький
11—20	Нижче середнього
21—30	Середній
31—40	Вище середнього
41—48	Високий

Як видно з таблиці, рівень комерційного потенціалу розроблюваного нового програмного продукту є високим, що досягається за рахунок того, що особливістю розробки є прискорення процесів реагування на загрози мережевої безпеки завдяки вдосконаленому процесу обробки журналів в системі SIEM та оптимізованій моделі роботи EDR.

5.1 Прогнозування витрат на виконання науково—дослідної (дослідно—конструкторської) роботи

Основна заробітна плата розробників, яка розраховується за формулою:

$$З_о = \frac{M}{T_р} \cdot t, \qquad (5.1)$$

де М — місячний посадовий оклад конкретного розробника (дослідника), грн.;

$Т_р$ — число робочих днів за місяць, 23 днів;

t — число днів роботи розробника (дослідника).

Результати розрахунків зведемо до таблиці 5.5.

Таблиця 5.4 — Основна заробітна плата розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник проекту	28000	1217,39	34	41391,304
Програміст	27000	1173,91	34	39913,043
Всього				81304,35

Так як в даному випадку розробляється програмний продукт, то розробник виступає одночасно і основним робітником, і тестувальником розроблюваного програмного продукту.

Додаткова заробітна плата розробників, які брати участь в розробці обладнання/програмного продукту.

Додаткову заробітну плату прийнято розраховувати як 11 % від основної заробітної плати розробників та робітників:

$$З_д = З_о \cdot 11\ \% / 100\ \% \qquad (5.2)$$

$$З_д = (81304{,}35 \cdot 11\ \% / 100\ \%) = 8943{,}48 \ \text{(грн.)}$$

5.2 Нарахування на заробітну плату розробників.

Згідно діючого законодавства нарахування на заробітну плату складають 22 % від суми основної та додаткової заробітної плати.

$$Н_з = (З_о + З_д) \cdot 22\ \% / 100\% \quad (5.3)$$

$$Н_з = (81304{,}35 + 8943{,}48) \cdot 22\ \% / 100\ \% = 19854{,}52 \text{ (грн.)}$$

Оскільки для розроблювального пристрою не потрібно витрачати матеріали та комплектуючи, то витрати на матеріали і комплектуючі дорівнюють нулю.

5.3 Амортизація обладнання, яке використовувалось для проведення розробки

Амортизація обладнання, що використовувалось для розробки в спрощеному вигляді розраховується за формулою:

$$A = \frac{Ц}{Тв} \cdot \frac{t_{вик}}{12} \text{ [грн.].} \quad (5.4)$$

де Ц — балансова вартість обладнання, грн.;

Т — термін корисного використання обладнання згідно податкового законодавства, років

$t_{вик}$ — термін використання під час розробки, місяців

Розрахуємо, для прикладу, амортизаційні витрати на комп’ютер балансова вартість якого становить 37000 грн., термін його корисного використання згідно податкового законодавства — 2 роки, а термін його фактичного використання — 1,48 міс.

$$A_{обл} = \frac{37000}{2} \times \frac{1{,}48}{12} = 2278{,}986 \text{ грн.}$$

Аналогічно визначаємо амортизаційні витрати на інше обладнання та

приміщення. Розрахунки заносимо до таблиці 5.5. Так як вартість ліцензійної ОС та спеціалізованих ліцензійних нематеріальних ресурсів менше 20000 грн, то даний нематеріальний актив не амортизується, а його вартість включається у вартість розробки повністю, $В_{нем.ак.}$ = 4843 грн.

Таблиця 5.5 — Амортизаційні відрахування на матеріальні та нематеріальні ресурси для розробників

Найменування обладнання	Балансова вартість, грн.	Строк корисного використання, років	Термін використання обладнання, місяців	Амортиза—ційні відрахуван—ня, грн.
Комп'ютер та комп'ютерна периферія	37000	2	1,48	2278,986
Офісне обладнання (меблі)	23500	4	1,48	723,732
Приміщення	1300000	20	1,48	8007,246
Всього				11009,96

Тарифи на електроенергію для непобутових споживачів (промислових підприємств) відрізняються від тарифів на електроенергію для населення. При цьому тарифи на розподіл електроенергії у різних постачальників (енергорозподільних компаній), будуть різними. Крім того, розмір тарифу залежить від класу напруги (1—й або 2—й клас). Тарифи на розподіл електроенергії для всіх енергорозподільних компаній встановлює Національна комісія з регулювання енергетики і комунальних послуг (НКРЕКП). Витрати на силову електроенергію розраховуються за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п, \quad (5.5)$$

де В — вартість 1 кВт—години електроенергії для 1 класу підприємства, В = 6,2 грн./кВт;

П — встановлена потужність обладнання, кВт. П = 0,4 кВт;

Ф — фактична кількість годин роботи обладнання, годин.

$К_п$ — коефіцієнт використання потужності, $К_п$ = 0,9.

$$В_е = 0,9 \cdot 0,4 \cdot 8 \cdot 34 \cdot 6,2 = 607,104 \text{ (грн.)}$$

5.4 Інші витрати та загальновиробничі витрати.

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (5.6)$$

де $Н_{ів}$ — норма нарахування за статтею «Інші витрати».

$$І_в = 81304,35 * 50\% / 100\% = 40652,17 \text{ (грн.)}$$

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково—технічну інформацію та рекламу та ін. Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників:

$$Н_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (5.7)$$

де $Н_{нзв}$ — норма нарахування за статтею «Накладні (загальновиробничі) витрати».

$$Н_{нзв} = 81304,35 * 110\ \% / 100\ \% = 89435 \text{ (грн.)}$$

5.4 Витрати на проведення науково—дослідної роботи

Сума всіх попередніх статей витрат дає загальні витрати на проведення науково—дослідної роботи:

$$В_{заг} = 81304,35+8943,48+19854,52+11009,96+4843+607,10+40652,17+$$

$$+89435 = 256649,37 \text{ грн.}$$

5.5 Розрахунок загальних витрат на науково—дослідну (науково—технічну) роботу та оформлення її результатів.

Загальні витрати на завершення науково—дослідної (науково—технічної) роботи та оформлення її результатів розраховуються за формулою:

$$ЗВ = \frac{В_{заг}}{\eta} \text{ (грн)}, \qquad (5.8)$$

де η — коефіцієнт, який характеризує етап (стадію) виконання науково—дослідної роботи.

Так, якщо науково—технічна розробка знаходиться на стадії: науково—дослідних робіт, то η=0,1; технічного проектування, то η=0,2; розробки конструкторської документації, то η=0,3; розробки технологій, то η=0,4; розробки дослідного зразка, то η=0,5; розробки промислового зразка, то η=0,7; впровадження, то η=0,9. Оберемо η = 0,5, так як розробка, на даний момент, знаходиться на стадії дослідного зразка:

$$ЗВ = 256649,37 / 0,5 = 513299 \text{ грн.}$$

5.6 Розрахунок економічної ефективності науково—технічної розробки за її можливої комерціалізації потенційним інвестором

В ринкових умовах узагальнювальним позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково—технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку. Саме зростання чистого прибутку забезпечить потенційному інвестору надходження додаткових коштів, дозволить покращити фінансові результати його діяльності, підвищить конкурентоспроможність та може позитивно вплинути на ухвалення рішення щодо комерціалізації цієї розробки.

Для того, щоб розрахувати можливе зростання чистого прибутку у потенційного інвестора від можливого впровадження науково—технічної розробки необхідно:

— вказати, з якого часу можуть бути впроваджені результати науково—технічної розробки;

— зазначити, протягом скількох років після впровадження цієї науково—технічної розробки очікуються основні позитивні результати для потенційного інвестора (наприклад, протягом 3—х років після її впровадження);

— кількісно оцінити величину існуючого та майбутнього попиту на цю або аналогічні чи подібні науково—технічні розробки та назвати основних суб’єктів (зацікавлених осіб) цього попиту; визначити ціну реалізації на ринку науково—технічних розробок з аналогічними чи подібними функціями.

При розрахунку економічної ефективності потрібно обов’язково враховувати зміну вартості грошей у часі, оскільки від вкладення інвестицій до отримання прибутку минає чимало часу. При оцінюванні ефективності інноваційних проектів передбачається розрахунок таких важливих показників:

— абсолютного економічного ефекту (чистого дисконтованого доходу);

— внутрішньої економічної дохідності (внутрішньої норми дохідності);

— терміну окупності (дисконтованого терміну окупності).

Аналізуючи напрямки проведення науково—технічних розробок, розрахунок економічної ефективності науково—технічної розробки за її можливої комерціалізації потенційним інвестором можна об’єднати, враховуючи визначені ситуації з відповідними умовами.

Розробка чи суттєве вдосконалення програмного засобу (програмного забезпечення, програмного продукту) для використання масовим споживачем.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

$$\Delta П_i = (\pm \Delta Ц_0 \cdot N + Ц_0 \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \qquad (5.9)$$

де $\pm\Delta Ц_о$ — зміна вартості програмного продукту (зростання чи зниження) від впровадження результатів науково—технічної розробки в аналізовані періоди часу;

N — кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково—технічної розробки;

$Ц_о$ — основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки, $Ц_о = Ц_б \pm \Delta Ц_о$;

Цб — вартість програмного продукту у році до впровадження результатів розробки;

ΔN — збільшення кількості споживачів продукту, в аналізовані періоди часу, від покращення його певних характеристик;

λ — коефіцієнт, який враховує сплату податку на додану вартість. Ставка податку на додану вартість дорівнює 20%, а коефіцієнт λ = 0,8333.

р — коефіцієнт, який враховує рентабельність продукту;

ϑ — ставка податку на прибуток, у 2023 році ϑ =18%.

Припустимо, що при прогнозованій ціні 15500 грн. за одиницю виробу, термін збільшення прибутку складе 3 роки. Після завершення розробки і її

вдосконалення, можна буде підняти її ціну на 1000 грн. Кількість одиниць реалізованої продукції також збільшиться: протягом першого року — на 1000 шт., протягом другого року — на 1300 шт., протягом третього року на 1500 шт. До моменту впровадження результатів наукової розробки реалізації продукту не було:

$$\Delta П_1 = (0*1000 + (15500 + 1000)*1000)* 0{,}8333* 0{,}28) * (1 — 0{,}18) = 2965666{,}548 \text{ грн.}$$

$$\Delta П_2 = (0*1000 + (15500 + 1000)*(1000+1300)* 0{,}8333* 0{,}28) * (1 — 0{,}18) = 7261099{,}710 \text{ грн.}$$

$$\Delta П_3 = (0*1000 + (15500 + 1000)*(1000+1300+1500)* 0{,}8333* 0{,}28) * (1 — 0{,}18) = 11996599{,}520 \text{ грн.}$$

Отже, комерційний ефект від реалізації результатів розробки за три роки складе 22223365,78 грн.

5.6.2 Розрахунок ефективності вкладених інвестицій та періоду їх окупності.

Розраховуємо приведену вартість збільшення всіх чистих прибутків ПП, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково—технічної розробки:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (5.10)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої науково—дослідної (науково—технічної) роботи, грн;

Т – період часу, протягом якою виявляються результати впровадженої науково—дослідної (науково—технічної) роботи, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ = 0,05…0,15;

t — період часу (в роках).

Збільшення прибутку ми отримаємо, починаючи з першого року:

ПП = (2965666,548/(1+0,1)[1])+(7261099,710/(1+0,1)[2])+(11996599,520/

/(1+0,1)[3]) = 2696060,50 + 6000908,851 + 9013222,78 = 17710192,13 грн.

Далі розраховують величину початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково—технічної розробки. Для цього можна використати формулу:

$$PV = k_{інв} * ЗВ, \quad (5.11)$$

де $k_{інв}$ — коефіцієнт, що враховує витрати інвестора на впровадження науково—технічної розробки та її комерціалізацію. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{інв}$=2...5, але може бути і більшим;

ЗВ — загальні витрати на проведення науково—технічної розробки та оформлення її результатів, грн.

$$PV = 2 * 513299 = 1026597,49 \text{ грн.}$$

Тоді абсолютний економічний ефект $Е_{абс}$ або чистий приведений дохід (NPV, Net Present Value) для потенційного інвестора від можливого впровадження та комерціалізації науково—технічної розробки становитиме:

$$Е_{абс} = ПП — PV, \quad (5.12)$$

$$Е_{абс} = 17710192,13 — 1026597,49 = 16683594,64 \text{ грн.}$$

Оскільки $E_{абс} > 0$ то вкладання коштів на виконання та впровадження результатів даної науково—дослідної (науково—технічної) роботи може бути доцільним.

Для остаточного прийняття рішення з цього питання необхідно розра—хувати внутрішню економічну дохідність або показник внутрішньої но—рми дохідності (IRR, Internal Rate of Return) вкладених інвестицій та порівняти її з так званою бар'єрною ставкою дисконтування, яка визначає ту мінімальну внутрішню економічну дохідність, нижче якої інвестиції в будь—яку науково—технічну розробку вкладати буде економічно недоцільно.

Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $E_в$. Для цього використаємо формулу:

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{5.13}$$

$T_ж$ – життєвий цикл наукової розробки, роки.

$$E_в = \sqrt[3]{(1 + 16683594{,}64/1026597{,}49} \text{ — } 1 = 1{,}584$$

Визначимо мінімальну ставку дисконтування, яка у загальному вигляді визначається за формулою:

$$\tau = d + f, \tag{5.14}$$

де d — середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні d = (0,09…0,14);

f – показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,5).

$$\tau_{\min} = 0{,}14 + 0{,}05 = 0{,}19.$$

Так як $E_в > \tau_{min}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій за формулою:

$$T_{ок} = \frac{1}{E_в}, \tag{5.15}$$

$$T_{ок} = 1 / 1{,}584 = 0{,}63 \text{ р.}$$

Оскільки $T_{ок}$ < 3—х років, а саме термін окупності рівний 0,63 роки, то фінансування даної наукової розробки є доцільним.

Економічна частина даної роботи містить розрахунок витрат на розробку нового програмного продукту, сума яких складає 513299 гривень. Було спрогнозовано орієнтовану величину витрат по кожній з статей витрат. Також розраховано чистий прибуток, який може отримати виробник від реалізації нового технічного рішення, розраховано період окупності витрат для інвестора та економічний ефект при використанні даної розробки. В результаті аналізу розрахунків можна зробити висновок, що розроблений програмний продукт за ціною дешевший за аналог і є висококонкурентоспроможним. Період окупності складе близько 0,63 роки.

ВИСНОВКИ

Потреба у аналізі та удосконаленні методів та засобів неперервного моніторингу безпеки в комп'ютерних мережах засобами SIEM стала підставою для написання даної магістерської роботи.

У даній роботі досягнута поставлена мета, яка дозволяє прискорення процесів реагування на загрози мережевої безпеки завдяки вдосконаленому процесу обробки журналів подій у методі інтеграції SIEM та її агентів в середовище. У підсумку це дозволяє упорядковувати та класифікувати хаотичні неосяжні потоки інформації про події в мережі та перетворити у зручну візуально прийнятну інформацію для оперативного усунення загроз адміністратором системи.

Зокрема, в даній роботі виконані такі завдання:

— виконано дослідження методів, засобів та новітніх підходів до використання схеми побудови системи моніторингу безпеки в КМ засобами SIEM на базі відомих стандартів ISO;

— виконано дослідження новітнього підходу щодо моніторингу безпеки в комп'ютерних мережах, зокрема, в парадигмі тріади SIEM—EDR—NDR;

— виконано дослідження новітнього підхід щодо розробки неперервного ефективного моніторингу безпеки в комп'ютерних мережах у центрах SOC;

— вапропоновано альтернативний метод інтеграції SIEM та її агентів в середовище;

— вапропоновано альтернативний процесу обробки журналів подій;

— веревірено експериментально роботу методу інтеграції системи SIEM та її агентів в середовищі ELK STACK.

Наукова новизна полягає в удосконаленні в поліпшенні операційних інструментів для керування мережевою безпекою за допомогою SIEM, зокрема:

— вдосконалено метод інтеграції SIEM та її агентів в середовище за рахунок безпекового моніторингу в парадигмі тріади SIEM—EDR—NDR;

— удосконаленні процесу обробки журналів в системі SIEM за рахунок оптимізованої роботи централізованих хабів агентів та «пісочниці» в EDR.

Практична цінність полягає у впровадженні альтернативних методів моніторингу безпеки в комп'ютерних мережах засобами SIEM, зокрема:

— реалізації архітектурного плану безпекового моніторингу взаємодії компонентів SIEM—EDR—NDR;

— реалізації алгоритму інтеграції системи Wazuh SIEM та запуску агентів;

— інтеграції системи Wazuh SIEM в середовище ELK Stack;

— візуалізації для адміністратора результатів роботи роботи процесу обробки журналів від агента і SIEM.

Особистий внесок студента полягає у розширенні методологічної бази моніторингу мережевої безпеки за допомогою інструментів SIEM. Цей внесок може стати стимулом для більш широкого впровадження в Україні передових та ефективних систем захисту, подібних до SIEM, EDR і NDR.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Метод та засіб моніторингу безпеки в комп'ютерні мережі засобами SIEM [Текст] / Л.А. Савицька, Т.І. Коробейнікова, О.П. Волос, М. Г. Тарновський // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 2. – С. 52-61

2. Кібербезпека бізнесу в умовах нестабільності [Електронний ресурс] // PwC Україна. — 2022. — Режим доступу до ресурсу: https://www.pwc.com/ua/uk/publications/2022/cybersecurity—uncertainty—state.html

3. Як змінилися російські кібератаки під час війни [Електронний ресурс] // Укрінформ. — 2023. — Режим доступу до ресурсу: https://www.ukrinform.ua/rubric—technology/3518528—ak—zminilisa—rosijski—kiberataki—pid—cas—vijni.html

4. Про Національний координаційний центр кібербезпеки [Електронний ресурс] // Верховна Рада України. — 2016. — Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/242/2016#Text

5. Про CERT—UA [Електронний ресурс] // Державна служба спеціального зв'язку та захисту інформації України. — 2023. — Режим доступу до ресурсу: https://cert.gov.ua

6. Військова кібербезпека [Електронний ресурс] // Міністерство оборони України. — 2023. — Режим доступу до ресурсу: https://www.mil.gov.ua/ukbs

7. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 [Електронний ресурс] // Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". — 2021. — Режим доступу до ресурсу: https://www.president.gov.ua/documents/4472021—40013

8. Miller D. Security Information and Event Management (SIEM) — Implementation Guide / David R. Miller. CRC Press, 2020.

9. Stallings W. Effective Cybersecurity Using Security Information and Event Management (SIEM): A Complete Guidebook / W. Stallings, A. Moro. Wiley, 2021.

10. Щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Ел. ресурс] // Документ v0365500—11. — 2011. — Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0365500—11

11. Pitis Andrei. SIEM: Trends and Best Practices for Operations and Development / Andrei Pitis, Apress: 2020.

12. Top SIEM Use Cases for Correlation and SIEM Alerts Best Practices [Електронний ресурс] // DNSstuff. — 2020. — Режим доступу до ресурсу: https://www.dnsstuff.com/common—siem—alerts.

13. Про засади інформаційної безпеки України [Електронний ресурс] // Проект Закону України від 28.05.2014 № 4949 (Одержаний ВР України). — 2014. — Режим доступу до ресурсу: https://ips.ligazakon.net/document/JG3TH00A.

14. Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats, 2020 — 242p.

15. Класифікація загроз інформаційній безпеці [Електронний ресурс] // Інформаційна безпеки особистості. — 2020. — Режим доступу до ресурсу: https://web.archive.org/web/20201029231318/https://sites.google.com/site/infobezosob/klasifikacia—zagroz—informacijnij—bezpeci

16. Гребенюк А. М. Основи управління інформаційною безпекою [Ел. ресурс] / А. М. Гребенюк, Л. В. Рибальченко. — 2020. — Режим доступу: https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1I%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3I%D0%91%20.pdf

17. What is the SOC visibility triad? [Електронний ресурс] // SOC visibility triad Режим доступу до ресурсу: https://www.nomios.be/en/resources/what—is—the—soc—visibility—triad/

18. Ubuntu from packages [Електронний ресурс] // Wazuh Inc.. — 2023. — Режим доступу до ресурсу: https://documentation.wazuh.com/3.12/installation—

guide/installingwazuhmanager/linux/ubuntu/wazuh_server_packages_ubuntu.html#wazuh—server—packages—ubuntu

19. How to Manage Packages with APT on Ubuntu [Електронний ресурс] // Wazuh Inc.. — 2023. — Режим доступу до ресурсу: https://www.howtoforge.com/how—to—manage—packages—with—apt—on—ubuntu/

20. Ubuntu [Електронний ресурс] Режим доступу до ресурсу: https://linuxconfig.org/list—installed—packages—on—ubuntu—18—04—bionic—beaver—linux

ДОДАТОК А

Технічне завдання

Міністерство освіти і науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп’ютерної інженерії

Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

проф., д.т.н.. Азаров О.Д

"29" вересня 2023 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

“ Метод та засіб моніторингу безпеки в комп’ютерній мережі засобами SIEM ”

08—54.МКР.002.00.000 ПЗ

Науковий керівник: доцент к.т.н.

_____ Савицька Л.А.

Студент групи 1КІ—22м

_____ Волос О.П.

ВНТУ 2023

1 Підстава для виконання магістерської кваліфікаційної роботи (МКР)

1.1 Моніторинг безпеки в комп'ютерній мережі (КМ) стає все більш актуальним і важливим у всьому світі. Протягом лише 2021 року світова економіка зазнала значних втрат через кібератаки на загальну суму 6 трлн. доларів. Україна не вийшла з—під цієї загрози, ба навіть зазнала її ще більше. За даними аналізу, проведеного компанією Microsoft у 2021 році, майже 20% світових кібератак спрямовані на Україну, що робить нашу країну другою за кількістю кібератак у світі, випереджаючи багатонаціональні корпорації. Це великий виклик, оскільки з 2014 року Україна веде гібридну війну, включаючи і кібернетичний фронт.

1.2 Наказ про затвердження теми МКР.

2 Мета МКР і призначення розробки

2.1 Мета роботи — прискорення процесів реагування на загрози мережевої безпеки завдяки вдосконаленому процесу обробки журналів подій у методі інтеграції SIEM та її агентів в середовище.

2.2 Призначення розробки — розширення методологічної бази моніторингу мережевої безпеки за допомогою інструментів SIEM

3 Вихідні дані для виконання МКР

3.1 Огляд методів, засобів та новітніх підходів до використання схеми побудови системи моніторингу безпеки в КМ засобами SIEM на базі відомих стандартів ISO.

3.2 Вивчення методів, засобів та новітніх підходів до використання схеми побудови системи моніторингу безпеки в КМ засобами SIEM на базі відомих стандартів ISO.

3.3 Дослідження новітнього підходу щодо моніторингу безпеки в комп'ютерних мережах, зокрема, в парадигмі тріади SIEM—EDR—NDR.

3.4 Проведення перевірки та аналізу отриманих результатів.

3.5 Виконання економічних розрахунків для оцінки доцільності впровадження нової розробки.

4 Вимоги до виконання МКР

Головна вимога — підвищення безпеки комп'ютерної мережі та зменшення часу реагування на загрозу засобами SIEM.

5 Етапи МКР та очікувані результати

Етапи роботи та очікувані результати приведено в Таблиці А.1.

Таблиця А.1 — Етапи МКР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Огляд і аналіз актуального стану питаня у галузі моніторингу безпеки у КМ			Аналітичний огляд літературних джерел, задачі досліджень, розділ 1 ПЗ
2	Дослідження методів організації безпекового моніторингу мережі			Розділ 2
3	Інтеграція SIEM в середовище роботи та запуску агентів			Розділ 3
4	Дослідження методу інтеграції системи SIEM та роботи агентів в середовищі ELK STACK			Розділ 4

Продовження таблиці А.1

5	Підготовка економічної частини			Розділ 5
6	Опублікування результатів досліджень			Стаття
7	Оформлення пояснювальної записки, графічного матеріалу і презентації			Пояснювальна записка, графічний матеріал і презентація
8	Підготовка супроводжуючих документів, їх підписування, проходження нормоконтролю та тесту на плагіат			Оформлені документи

6 Матеріали, що подаються до захисту МКР

До захисту подаються: пояснювальна записка МКР, графічні і ілюстративні матеріали, протокол попереднього захисту МКР на кафедрі, відгук наукового керівника, відгук опонента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами.

7 Порядок контролю виконання та захисту МКР

Виконання етапів графічної та розрахункової документації МКР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

8 Вимоги до оформлювання та порядок виконання МКР

8.1 При оформлюванні МКР використовуються:

— ДСТУ 3008 : 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— ГОСТ 2.104—2006 «Едина система конструкторської документації. Основні написи»;

— методичні вказівки до виконання магістерських кваліфікаційних робіт зі спеціальності 123 — «Комп'ютерна інженерія»;

— Документами на які посилаються у вище вказаних.

8.2 Порядок виконання МКР викладено в «Положення про кваліфікаційні роботи на другому (магістерському) рівні вищої освіти СУЯ ВНТУ—03.02.02—П.001.01:21».

ДОДАТОК Б

Коди встановлення програм

Лістинг Б.1 Встановлення та налаштування ELK—Stack

```
sudo apt install apt—transport—https
sudo apt install openjdk—11—jdk
java ——version
sudo nano /etc/environment
JAVA_HOME="/usr/lib/jvm/java—11—openjdk—amd64"
source /etc/environment
echo $JAVA_HOME
/usr/lib/jvm/java—11—openjdk—amd64
wget —qO — https://artifacts.elastic.co/GPG—KEY—elasticsearch | sudo gpg
——dearmor —o /usr/share/keyrings/elasticsearch—keyring.gpg
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
sudo apt—get update
sudo apt—get install elasticsearch
sudo systemctl start elasticsearch
sudo systemctl enable elasticsearch
sudo systemctl status elasticsearch
sudo nano /etc/elasticsearch/elasticsearch.yml
sudo systemctl restart elasticsearch
curl —X GET "localhost:9200"
sudo apt—get install logstash
sudo systemctl start logstash
```

```
sudo systemctl enable logstash
sudo systemctl status logstash
sudo apt—get install kibana
sudo systemctl start kibana
sudo systemctl enable kibana
sudo systemctl status kibana
sudo nano /etc/kibana/kibana.yml
sudo systemctl restart kibana
```

Лістинг Б.2 Встановлення та налаштування агента FileBeat

```
sudo apt—get install filebeat
sudo nano /etc/filebeat/filebeat.yml
sudo filebeat modules enable system
sudo filebeat setup ——index—management —E output.logstash.enabled=false
—E 'output.elasticsearch.hosts=["ip_address:9200"]'
sudo systemctl start filebeat
sudo systemctl enable filebeat
sudo systemctl restart filebeat
sudo systemctl status filebeat
curl —XGET http://ip_address:9200/_cat/indices?v
```

Лістинг Б.3 Встановлення системи Wazuh SIEM

```
curl —s https://packages.wazuh.com/key/GPG—KEY—WAZUH | sudo apt—
key add —
echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee
/etc/apt/sources.list.d/wazuh.list
```

```
sudo apt update
sudo apt install wazuh—manager
sudo systemctl daemon—reload
sudo systemctl enable ——now wazuh—manager
systemctl status wazuh—manager
```

Лістинг Б.4 Інтеграція системи Wazuh SIEM в середовище ELK Stack

```
sudo —u kibana /usr/share/kibana/bin/kibana—plugin install
https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana—4.1.5_7.10.0—1.zip
```

Лістинг Б.5 Встановлення Wazuh Agent на ОС Windows

```
Invoke—WebRequest —Uri https://packages.wazuh.com/4.x/windows/wazuh—
agent—4.3.11—1.msi —OutFile ${env:tmp}\wazuh—agent—4.3.11.msi;
msiexec.exe /i ${env:tmp}\wazuh—agent—4.3.11.msi /q
WAZUH_MANAGER='qavxh6926dwv.cloud.wazuh.com'
WAZUH_REGISTRATION_SERVER='qavxh6926dwv.cloud.wazuh.com'
WAZUH_REGISTRATION_PASSWORD='EbsjtJjnGTgCslQHkXM5zOL2uxS
CFsFq' WAZUH_AGENT_GROUP='default'
NET START WazuhSvc
```

ДОДАТОК В

Алгоритму інтеграції системи Wazuh SIEM та запуску агентів

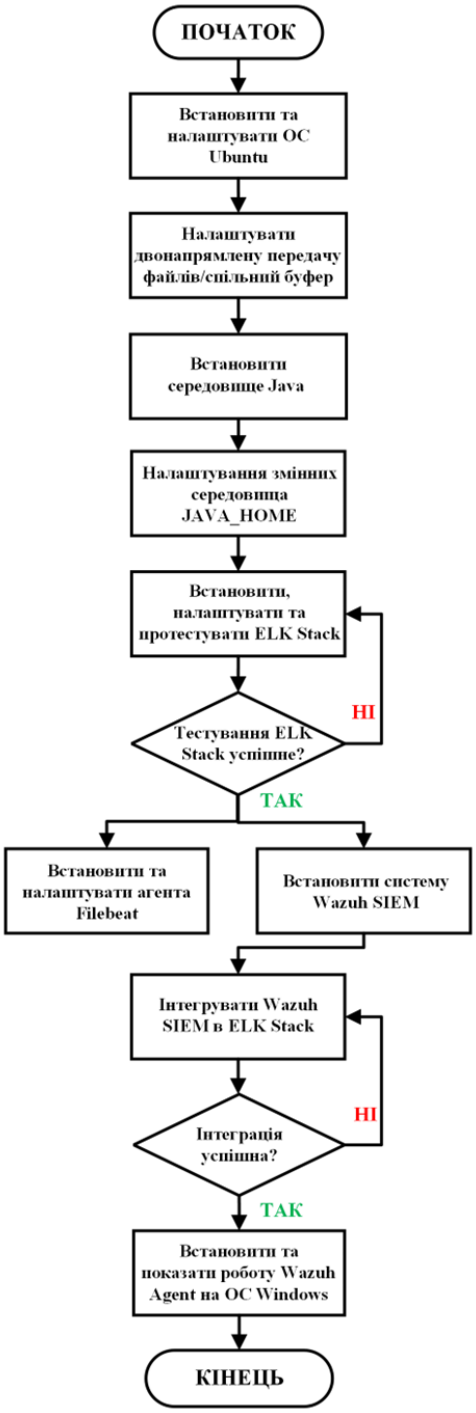


Рисунок В.1 — Алгоритму інтеграції системи Wazuh SIEM та запуску агентів

ДОДАТОК Г

Інструкція із встановлення Wazuh Agent на ОС Windows

Відповідно до наведених інструкцій ми обираємо операційну систему Windows для кінцевої точки та отримуємо індивідуальний код агента з унікальним паролем для використання в консолі Windows PowerShell.

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

PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.11-1.msi -OutFile
${env:tmp}\wazuh-agent-4.3.11.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.11.msi /q WAZUH_MANAGER='qavxh6926dwv.cloud
.wazuh.com' WAZUH_REGISTRATION_SERVER='qavxh6926dwv.cloud.wazuh.com' WAZUH_REGISTRATION_PASSWORD='EbsjtJjnGTgCslQHkXM5zO
L2uxSCFsFq' WAZUH_AGENT_GROUP='default'
```

Рисунок Г.1 — Код Wazuh Agent для Windows

Шляхом використання команди NET START WazuhSvc ми активуємо функціонування агента Wazuh. За результатами виконання команди вбачаємо, що агент успішно запущено.

```
PS C:\WINDOWS\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\WINDOWS\system32>
```

Рисунок Г.2 — Запуск Wazuh Agent для Windows

ДОДАТОК Д

Результати перевірки функціонування Wazuh Agent

Перейдемо до системи Wazuh SIEM і проводимо перевірку функціонування агента. На екрані відображається панель, що демонструє активність та інформацію про наш Wazuh Agent для Windows, таку як його ім'я, IP—адресу, ОС кінцевої точки та його поточний статус в системі.

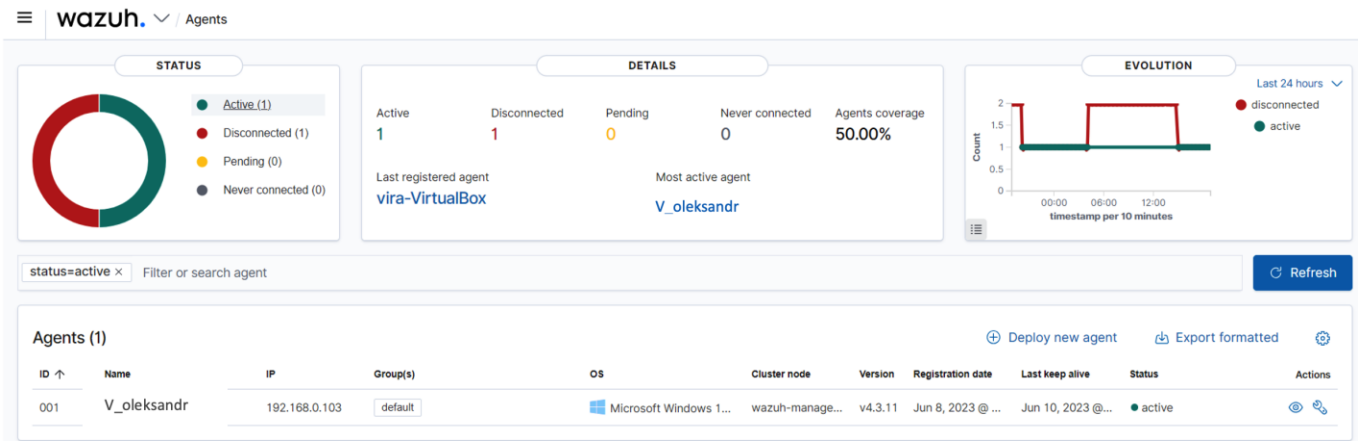


Рисунок Д.1 — Панель Wazuh SIEM для агентів

Вся інформація, яку передає агент, обробляється системою Wazuh SIEM, яка проводить нормалізацію, класифікацію та структурує дані згідно з відповідними аналітичними панелями. На рис. Д.2 є загальна аналітична панель, що надає інформацію про події безпеки, системні журнали подій, контроль цілісності інформації, останні сканування системи для виявлення вразливостей, інформацію про вторгнення та кібератаки, а також стан мережі.

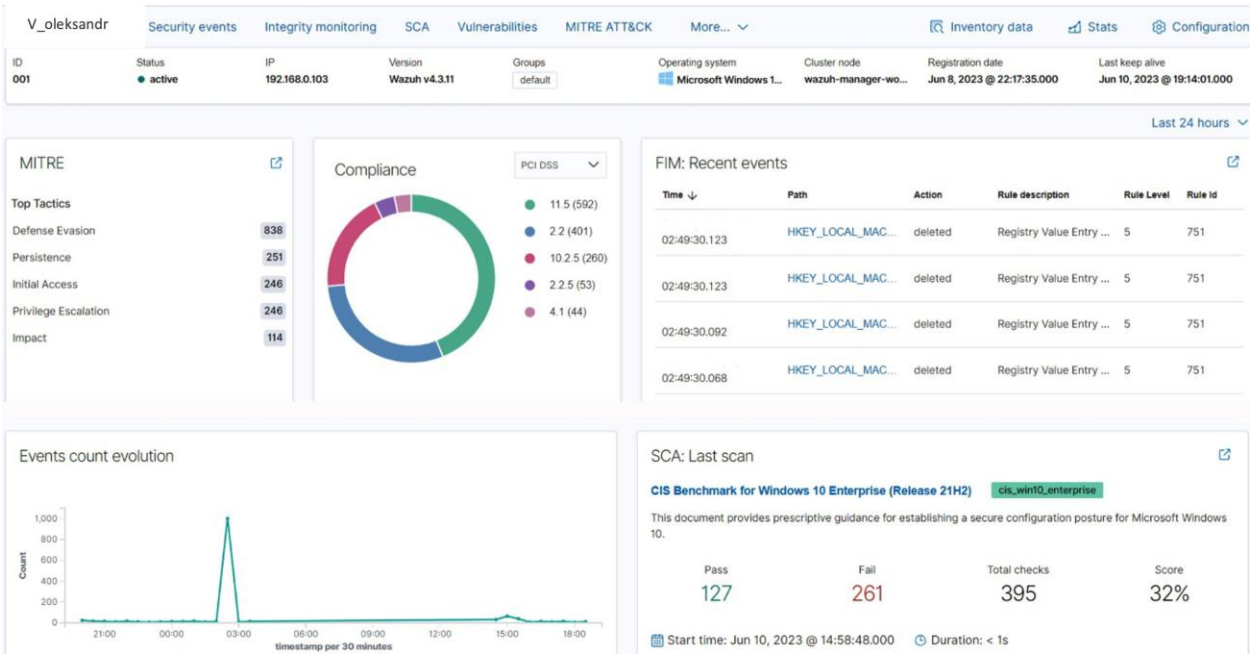


Рисунок Д.2 — Загальна аналітична панель

ДОДАТОК Е

Протокол перевірки роботи на текстові запозичення

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Метод та засіб моніторингу безпеки в комп'ютерній мережі засобами SIEM

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 95,8% Схожість 4,2%

Аналіз звіту подібності (відмітити потрібне):

✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.

☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Волос О. П.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Савицька Л. А.
(підпис) (прізвище, ініціали)