Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Вітмановського Вадима Олегович

на здобуття ступеня вищої освіти Бакалавра

Система виявлення несанкціонованого доступу до заборонених ресурсів з корпоративної мережі

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ. 2102140.21.02.03 ПЗ

Виконав студент 4 курсу група КБ-21-2 Вадим ВІТМАНОВСЬКИЙ
Керівник канд. техн. наук, доцент Юрій КЛЬОЦ
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

16 06 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Вітмановському Вадиму Олеговичу

1 Тема роботи Система виявлення несанкціонованого доступу до заборонених ресурсів з корпоративної мережі

Керівник роботи Кльоц Юрій Павлович

Затверджено наказом ректора університету від 7 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру 17.06.2025

3 Вихідні дані до роботи Розробити ефективну систему виявлення несанкціонованого доступу до заборонених ресурсів у корпоративній мережі.Дослідити предметно область що стосується загроз інформаційної безпеки , пов'язаних шы використанням VPN, анонімних мереж TOR та проксі-серверів як засобів обходу мережевих обмежень.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз предметної області та постановка задачі,проектування та розгортання системи моніторингу на базі Wazuh,налаштування власних правил для фіксації потенційно небезпечної активності ,тестування та оцінка ефективності

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
«Діаграма архітектури Wazuh», «Типова кластерна архітектура Wazuh», «Загальний вигляд системи після тестування інцидентів»

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студент _____ Вадим ВІТМАНОВСЬКИЙ

Керівник кваліфікаційної роботи _____ Юрій КЛЬОЦ

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система виявлення несанкціонованого доступу до заборонених ресурсів з корпоративної мереж.

Автор роботи: Вітмановський Вадим Олегович.

Керівник роботи: Кльоц Юрій Павлович.

Пояснювальна записка: 60 с., 1 додаток, 23 рисунків, 2 таблиці, 41 джерел.

Графічна частина: 3 плакати.

ВИЯВЛЕННЯ ЗАГРОЗ, СИСТЕМИ ВИЯВЛЕННЯ ІНЦИДЕНТІВ, КІБЕРБЕЗПЕКА, SIEM, IDS/IPS, КОРПОРАТИВНІ МЕРЕЖІ, ЗАБОРОНЕНІ РЕСУРСИ, ПОЛІТИКИ ДОСТУПУ, ЛОГУВАННЯ, АНАЛІЗ ПОВЕДІНКИ.

У даній кваліфікаційній роботі розглянуто питання виявлення несанкціонованого доступу до заборонених ресурсів у корпоративних мережах. Проведено аналіз сучасних систем інформаційної безпеки, зокрема SIEM, IDS/IPS, DPI та UEBA, які дозволяють виявляти спроби обходу політик доступу з використанням VPN, TOR, проксі та інших методів. На основі визначених критеріїв ефективності було обґрунтовано вибір SIEM-системи Wazuh як найбільш оптимального рішення. Робота містить детальний опис процесу розгортання, налаштування та тестування системи в умовах імітації загроз, а також оцінку її ефективності для виявлення аномальної активності користувачів. Отримані результати можуть бути використані фахівцями з кібербезпеки, адміністраторами корпоративних мереж та розробниками систем захисту.

08.06.2025 _____

ABSTRACT

Theme of qualification work: System for detecting unauthorized access to prohibited resources from corporate networks.

Author of the work: Vadym Olehovych Vitmanovskyi.

Supervisor: Klots Yurii Pavlovych.

Explanatory note: 60 p., 1 appendices, 23 figures,2 tables,41 references.

Graphic part: 3 posters.

THREAT DETECTION, INCIDENT RESPONSE SYSTEMS, CYBERSECURITY, SIEM, IDS/IPS, CORPORATE NETWORKS, RESTRICTED RESOURCES, ACCESS POLICIES, LOGGING, BEHAVIORAL ANALYSIS.

This qualification paper addresses the issue of detecting unauthorized access to restricted resources within corporate networks. It presents an analysis of modern cybersecurity systems, including SIEM, IDS/IPS, DPI, and UEBA technologies, which enable the detection of policy violations through the use of VPNs, TOR, proxies, and other evasion techniques. Based on established evaluation criteria, the Wazuh SIEM system was selected as the optimal solution. The paper includes a detailed description of the deployment, configuration, and testing process of the system under simulated threat conditions, along with an assessment of its effectiveness in identifying anomalous user activity. The results may be useful for cybersecurity professionals, network administrators, and developers of security systems.

08.06.2025 

ЗМІСТ

Вступ

У сучасному цифровому середовищі, де інформація є одним із найцінніших ресурсів, питання забезпечення кібербезпеки корпоративних мереж набуває особливої актуальності. Щоденно організації стикаються з викликами, пов’язаними з витоком даних, зловмисною активністю, порушенням політик доступу та спробами обходу систем захисту. Однією з критичних загроз для інформаційної безпеки є несанкціонований доступ користувачів до заборонених ресурсів — як зовнішніх, так і внутрішніх, що виходять за межі дозволеного кола взаємодії в межах корпоративної інфраструктури.

Сучасні користувачі мають у своєму розпорядженні широкий спектр технологій, які дозволяють обходити обмеження доступу, зокрема використання VPN-сервісів, анонімних проксі-серверів, мережі TOR, тунелювання через нестандартні порти або DNS-запити. Такі дії унеможливлюють ефективний моніторинг трафіку, знижують рівень прозорості мережевих процесів та ускладнюють завдання систем інформаційної безпеки щодо виявлення і реагування на інциденти.

У зв’язку з цим виникає необхідність у впровадженні інтелектуальних систем виявлення, які здатні не лише фіксувати факти доступу до заборонених ресурсів, а й аналізувати поведінку користувачів, корелювати події з різних джерел, ідентифікувати нетипову активність та формувати сповіщення у реальному часі. Найбільш ефективним рішенням у цьому напрямі є застосування платформ класу SIEM у поєднанні з IDS/IPS-інструментами та компонентами поведінкового аналізу.

Практична частина роботи включає моделювання сценаріїв порушень, налаштування системи для їх виявлення, а також оцінку результатів функціонування обраної системи.

1 АНАЛІЗ ЗАГРОЗ ТА ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ДОСТУПУ В КОРПОРАТИВНИХ МЕРЕЖАХ

1.1 Технології забезпечення несанкціонованого доступу до заборонених ресурсів

Використання VPN та проксі-серверів є одними з найпоширеніших методів обходу обмежень, накладених корпоративними мережами або державними фільтрами. Ці технології дозволяють користувачам змінювати своє мережеве розташування та отримувати доступ до заблокованих ресурсів, маскуючи свою активність.

VPN (Virtual Private Network) створює зашифрований тунель між пристроєм користувача та віддаленим сервером, через який проходить весь інтернет-трафік. Це означає, що всі дані, які користувач передає та отримує, шифруються за допомогою криптографічних алгоритмів, що робить їх недоступними для перегляду навіть адміністратору мережі. Коли користувач підключається до VPN, його реальна IP-адреса змінюється на адресу VPN-сервера, що дозволяє обійти блокування на основі геолокації або списків заборонених IP-адрес. Деякі провайдери VPN також використовують технології стелс-режиму, які маскують VPN-трафік під звичайні HTTPS-з'єднання, роблячи його непомітним для систем виявлення [1].

Окрім класичних VPN, існують і альтернативні методи тунелювання трафіку, такі як SoftEther VPN, WireGuard та OpenVPN. SoftEther VPN підтримує мультипротокольне з'єднання, що дозволяє працювати навіть у середовищах, де заблоковано традиційні VPN-протоколи. WireGuard, є сучасною, високопродуктивною VPN-технологією, що забезпечує швидку та ефективну передачу даних при мінімальних затратах. OpenVPN залишається одним із найбільш універсальних рішень завдяки відкритому коду та можливості використання різних методів шифрування.

Проксі-сервери діють за дещо іншим принципом, ніж VPN. Вони виступають посередниками між пристроєм користувача та запитуваними ресурсами, перенаправляючи інтернет-трафік через себе. Це дозволяє користувачу змінити свою IP-адресу, що може допомогти в обході мережевих обмежень.

Найпоширенішими видами проксі є HTTP-проксі, SOCKS-проксі та анонімні проксі. HTTP-проксі обробляє лише веб-трафік, працюючи на рівні браузера, тоді як SOCKS-проксі може обробляти всі види інтернет-з'єднань, включаючи потокове відео, VoIP-з'єднання та ігровий трафік. Анонімні проксі приховують не лише IP-адресу, а й сам факт використання проксі, що робить їх ефективними для збереження конфіденційності [2].

Важливим аспектом використання проксі є кешування даних. Деякі проксі-сервери можуть зберігати копії популярних веб-сторінок, що зменшує навантаження на мережу та прискорює завантаження контенту. Ця функція часто використовується в корпоративних мережах для оптимізації інтернет-трафіку, однак вона також може бути застосована для обходу обмежень, коли кешована версія сторінки зберігається навіть після її блокування в реальному часі.

Анонімні мережі, такі як Tor (The Onion Router) та I2P (Invisible Internet Project), є потужними інструментами для забезпечення конфіденційності, обходу цензури та отримання доступу до заблокованих ресурсів. Вони використовують методи багатошарової маршрутизації та децентралізації, що значно ускладнює моніторинг активності користувачів.

Tor працює за принципом "цибулевої маршрутизації" (onion routing) рисунок 1.1 [26], що означає, що інтернет-запити проходять через випадкові сервери (ноди) всередині мережі. Кожен з цих серверів розшифровує лише один рівень маршруту, не знаючи ні відправника, ні кінцевого отримувача запиту. Це забезпечує високий рівень анонімності, оскільки жоден вузол не має повної інформації про передані дані. Крім того, Tor дозволяє отримати доступ до прихованих сайтів із доменом .onion, які не індексуються звичайними

пошуковими системами та не прив’язані до стандартної DNS-системи. Ці ресурси використовуються не лише журналістами, активістами та правозахисниками, а й користувачами, які прагнуть обійти цензуру.У звичайних мережах ваш трафік проходить через провайдера безпосередньо до запитуваного сервера, що залишає сліди і надає можливість для відстеження. У разі Tor, маршрутизація через вузли з шифруванням забезпечує анонімність, роблячи складним або практично неможливим відстеження користувацького трафіку. [4]

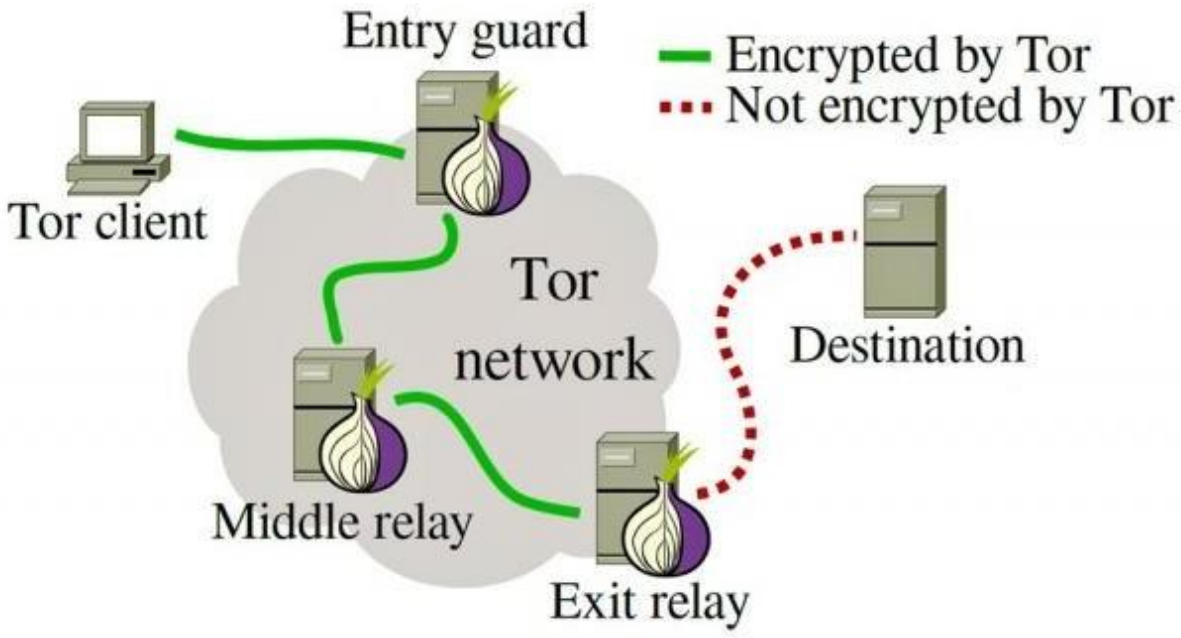


Рисунок 1.1 – Принцип роботи Tor

Мережа I2P (Invisible Internet Project) створена для безпечного внутрішнього обміну даними та зв’язку. Вона працює за принципом "часникової маршрутизації" (garlic routing), де декілька повідомлень групуються в один пакет, перш ніж бути переданими по мережі. Це ускладнює аналіз трафіку, оскільки навіть якщо один пакет буде перехоплений, він не міститиме повної інформації про відправника.

На відміну від традиційного інтернету, де запити спрямовуються напряму від клієнта до сервера, I2P використовує кілька віртуальних тунелів, які шифрують трафік між різними учасниками мережі. Кожен користувач I2P одночасно є і клієнтом, і ретранслятором трафіку для інших учасників, що підвищує рівень децентралізації та захисту. Ця структура робить I2P стійкою до блокувань і спроб виявлення активності.

I2P використовується для анонімного хостингу сайтів, відомих як eepsites, які мають домен ".i2p" і доступні лише в межах самої мережі. Це дозволяє створювати веб-ресурси, які неможливо заблокувати через традиційні механізми цензури, такі як DNS-фільтрація. Також I2P широко застосовується для захищеного спілкування, включаючи pfшифровані чати, що робить її корисною для користувачів, які прагнуть уникнути спостереження.

Ще однією важливою сферою використання є P2P-файлообмін, де I2P забезпечує безпечну передачу даних без ризику розкриття IP-адреси. Наприклад, такі сервіси, як I2PSnark (аналог BitTorrent) або I2P-Bote (анонімна електронна пошта), дозволяють обмінюватися файлами та повідомленнями без централізованого контролю. Через свою децентралізовану структуру I2P є більш стійкою до блокувань, оскільки не має відомих вихідних вузлів, як у випадку з Tor [5].

Обидві технології широко застосовуються для захисту приватності та обходу мережевих обмежень. Tor дозволяє анонімно переглядати веб-сайти та отримувати доступ до заблокованих ресурсів через випадкову маршрутизацію трафіку, тоді як I2P створює окрему захищену мережу для комунікації та обміну даними без можливості відстеження місцезнаходження користувача.

Використання цих мереж допомагає уникати контролю з боку провайдерів і корпоративних систем безпеки, забезпечуючи безпечний і зашифрований зв’язок у режимі реального часу. Крім того, завдяки активному розвитку та адаптації до сучасних викликів безпеки, Tor та I2P залишаються одними з найефективніших

інструментів для користувачів, які прагнуть забезпечити конфіденційність своїх даних в інтернеті [6].

Тунелювання трафіку через нестандартні порти є важливим методом забезпечення безпеки та конфіденційності в мережах, а також засобом обходу мережевих обмежень. Цей процес передбачає передачу даних через порти, які зазвичай не використовуються для конкретних сервісів, що допомагає уникнути блокування або фільтрації трафіку. Основна думка полягає в тому, що дані,які передаються між двома вузлами мережі, пересилаються через незахищену мережузапакованими в зашифрований пакет – таким чином вони захищені від прослуховуванняй модифікації. Водночас,зберігається прозорість мережі, тобто кінцеві вузли не знають про наявність тунелю та застосовують його, як звичайний канал зв'язку рисунок 1.2 [25].

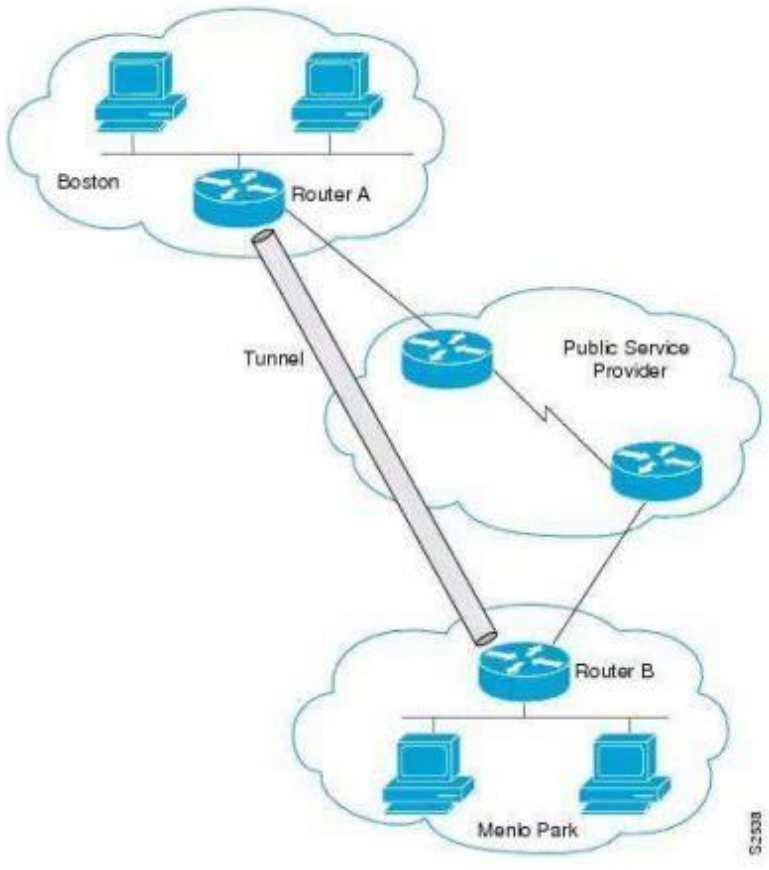


Рисунок 1.2 – Схема взаємодії мереж через тунель

Основний принцип тунелювання полягає в інкапсуляції одного мережевого протоколу в пакети іншого. Це дозволяє передавати дані через несумісні мережі або створювати безпечні шляхи через недовірені мережі. Наприклад, використовуючи SSH-тунелювання, можна перенаправляти трафік через захищене з'єднання, забезпечуючи безпечний доступ до внутрішніх ресурсів або обхід мережевих обмежень [7].

Тунелювання через нестандартні порти також використовується для обходу мережевих обмежень. Деякі організації або країни можуть блокувати доступ до певних сервісів, обмежуючи трафік на стандартних портах. У таких випадках перенаправлення трафіку через нестандартні порти може допомогти обійти ці обмеження та забезпечити доступ до необхідних ресурсів.

Використання тунелювання стає все більш важливішим у галузі кібербезпеки через зростання віддаленої роботи та потребу в безпечних з'єднаннях через публічні мережі. Процес інкапсуляції передбачає додавання додаткового заголовка до оригінального пакета, що містить необхідну інформацію для процесу тунелювання. Це дозволяє інкапсульованому пакету проходити через публічну мережу, залишаючись захищеним і безпечним [8].

Неправильне налаштування або використання тунелів може призвести до потенційних ризиків, таких як несанкціонований доступ або витік даних. Тому перед впровадженням тунелювання рекомендується ретельно оцінити потреби та можливі наслідки для мережевої безпеки.

Тунелювання трафіку через нестандартні порти є потужним інструментом для забезпечення безпеки, конфіденційності та доступу до обмежених ресурсів. Правильне впровадження та управління цією технологією може значно підвищити ефективність та безпеку мережевих з'єднань.

Одним з ключових інструментів, що дозволяє користувачам обходити обмеження корпоративної мережі та приховувати несанкціонований доступ до заборонених ресурсів, є використання шифрування трафіку. Суть даного методу полягає у перетворенні переданих даних у такий вигляд, який неможливо

прочитати або інтерпретувати без відповідного ключа дешифрування. Це унеможливлює або значно ускладнює спроби мережевого моніторингу, аналізу або блокування такого трафіку з боку систем контролю.

Сучасні технології шифрування працюють на декількох рівнях мережевої моделі, дозволяючи реалізовувати як повне шифрування сесії (end-to-end encryption), так і шифрування окремих елементів трафіку. Найбільш розповсюдженим є протокол HTTPS (HTTP Secure), що використовує TLS (Transport Layer Security) для створення захищеного каналу передачі даних. Завдяки HTTPS користувач може отримувати доступ до вебресурсів, при цьому навіть системи глибокого аналізу пакетів (Deep Packet Inspection, DPI) не можуть побачити вміст запитів чи відповідей.

Проте HTTPS — лише базовий рівень шифрування. Для обходу жорсткіших фільтрів користувачі можуть вдаватися до використання VPN(Virtual Private Network), який створює захищене тунельне з'єднання між пристроєм користувача та віддаленим сервером. Усі дані, що проходять через цей тунель, повністю зашифровані, і маршрутизація трафіку здійснюється ззовні корпоративної мережі. Таким чином, усі звернення до заборонених сайтів виглядають для системи як звичайний зв’язок із VPN-сервером, без можливості побачити, що відбувається всередині.

Іншим методом є SSH-тунелювання, коли зашифрований канал створюється за допомогою протоколу SSH. Цей підхід дозволяє не лише захищено адмініструвати сервери, але й пересилати трафік інших програм через створений захищений канал. Таким чином, звичайні HTTP або навіть нестандартні порти можуть бути перенаправлені через зашифрований тунель.

Окремо слід відзначити використання мережевих протоколів із вбудованим шифруванням та маскуванням трафіку, як-от Tor, I2P або Obfs4. Tor, наприклад, використовує багаторівневе шифрування (onion routing), що дозволяє приховати не лише зміст трафіку, але й маршрут передачі, включно з IP-адресою відправника. Протоколи обфускації, такі як Obfs4, здатні змінювати структуру

трафіку так, щоб він не виглядав як зашифрований або як трафік певного типу, а нагадував нешкідливі запити до вебсайтів або навіть звичайні DNS-запити.

Ще один напрям — використання протоколу QUIC, який працює поверх UDP і вбудовує TLS безпосередньо в транспортний рівень. Цей протокол ускладнює фільтрацію, бо не покладається на традиційні TCP-порти й має менше метаданих у відкритому доступі.

Завдяки широкому використанню шифрування, сучасні засоби контролю корпоративного трафіку втрачають змогу проводити ефективний контент-аналіз. Навіть системи DPI при наявності повноцінного TLS або VPN-трафіку можуть лише визначити обсяг переданих даних, частоту запитів або кінцеву IP-адресу, але не зміст звернень. Це створює серйозну загрозу інформаційній безпеці організації, оскільки шкідливе ПЗ, витік конфіденційних даних або доступ до заборонених ресурсів можуть бути приховані під виглядом легітимного зашифрованого трафіку.

У підсумку, шифрування трафіку є потужним інструментом в арсеналі обхідних технік користувачів і зловмисників. Щоб уникнути цього потрібні комплексні підходи, зокрема поведінковий аналіз, контроль активності на кінцевих пристроях (Endpoint Detection and Response, EDR) та інтеграція систем виявлення аномалій.

1.2 Технології виявлення несанкціонованого доступу до заборонених ресурсів

Зі зростанням складності технік обходу корпоративної безпеки зростає і потреба у вдосконалених технологіях виявлення несанкціонованого доступу до заборонених ресурсів. Традиційні фаєрволи та списки блокування вже не здатні ефективно стримувати зловмисні дії користувачів або витік інформації, особливо в умовах широкого використання шифрування, VPN, Tor і тунелювання через

нестандартні порти. Тому в сучасних корпоративних мережах застосовуються більш гнучкі, інтелектуальні й багаторівневі системи контролю трафіку.

Системи IDS (Intrusion Detection System) і IPS (Intrusion Prevention System) є одними з основних інструментів для виявлення підозрілої активності в мережі. IDS здійснює моніторинг трафіку в реальному часі та порівнює його з відомими шаблонами атак, сигнатурами або аномаліями. IPS, на відміну від IDS, не лише виявляє загрозу, а й автоматично блокує потенційно небезпечний трафік.

IPS або система запобігання вторгненням працює шляхом виявлення аномальної активності, повідомлення про таку активність і спроб запобігти таким загрозам. Як правило, IPS знаходиться відразу за брандмауером. Цей тип систем є надзвичайно корисним для виявлення проблем, пов'язаних зі стратегіями безпеки, виявлення несанкціонованого доступу та ідентифікації загроз.

Запобігання цим активностям відбувається в IPS шляхом змінення змісту атаки або реконфігурації брандмауерів . Деякі користувачі сприймають IPS як розширення IDS, головним чином тому, що вони відповідають за моніторинг мережі.ьної поведінки користувача або системи.

IDS та IPS функціонують для досягнення одної мети - захисту структури мережі. У більшості випадків ці системи виявляють дивну активність, порівнюючи її зі стандартними (нормальними) характеристиками поведінки. Окрім незалежної роботи, IPS та IDS можуть бути інтегровані між собою. Більше того, брандмауери також можуть співпрацювати з IPS/IDS для кращого захисту системи. Така співпраця називається UTM або NGFW. Сучасні підприємства більше орієнтовані на роботу онлайн, ніж раніше. Існує дуже багато компаній, які перейшли на цей режим під час пандемії і продовжують дотримуватись цього шляху, що вимагає більшого трафіку і більшої кількості точок доступу в цілому. Ручний аналіз і моніторинг загроз стали майже непотрібними завдяки хмарним середовищам. Крім того, кібербезпека також покращує механізми роботи з різноманітними ризиками, і ці підходи також повинні бути впроваджені.Принцим роботи IPS/IDS зображений на рисунку 1.3 [11]

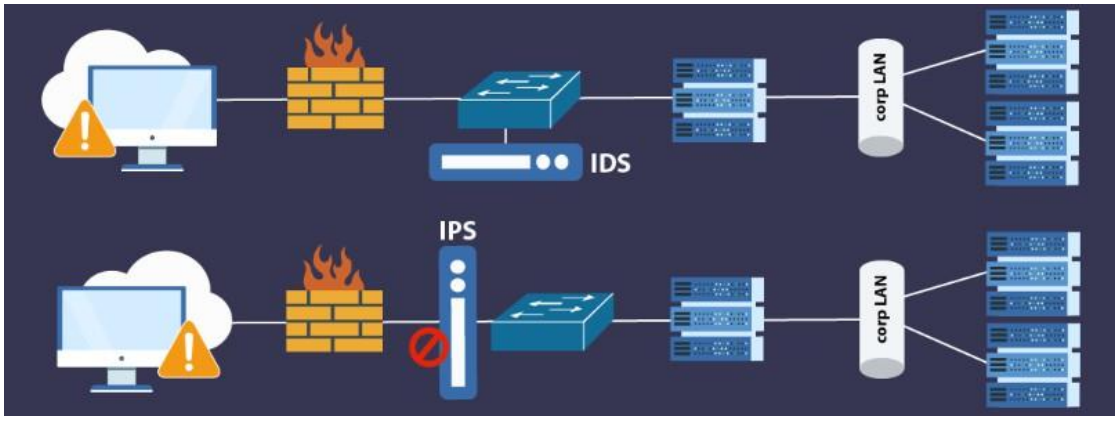


Рисунок 1.3 принцип роботи IPS/IDS

Тожі IPS, і IDS невід'ємні від світу кібербезпеки та ідеальнопасуютьдля підприємств. Автоматизація більшості процесів робить виявлення загроз значно легшим та результативнішим,ніж раніше. Просто потрібно не забувайти оновлювати систему щоразу, коли виникає потреба ,і система буде ще більше захищена від нових небезпек.

SIEM-системи (Security Information and Event Management) є потужною технологією, що відіграє ключову роль у виявленні несанкціонованого доступу до заборонених ресурсів в інформаційних системах.

Їхня основна функція полягає в централізованому зборі, аналізі та кореляції подій безпеки з різноманітних джерел, таких як мережеве обладнання, сервери, операційні системи, бази даних, прикладні програми та системи виявлення вторгнень. Об'єднуючи журнали подій та дані про безпеку в єдину платформу, SIEM-системи забезпечують цілісне представлення стану безпеки організації в реальному часі.

Для виявлення несанкціонованого доступу SIEM-системи використовують складні механізми аналізу. Вони здатні ідентифікувати підозрілу активність, аномальну поведінку користувачів, нетипові шаблони трафіку та інші індикатори компрометації, які можуть свідчити про спроби проникнення або вже здійснений нелегітимний доступ до конфіденційних даних чи критично важливих систем.

Наприклад, система може виявити численні невдалі спроби входу в обліковий запис, доступ до файлів у неробочий час, незвичайні обсяги передачі даних або спроби отримати доступ до ресурсів, на які користувач не має прав [12].

Коли SIEM-система виявляє подію або комбінацію подій, що відповідають визначеним правилам безпеки або аномальній поведінці, вона генерує сповіщення. Ці сповіщення надають інформацію про потенційний інцидент безпеки, включаючи джерело події, ціль, час виникнення та рівень серйозності. Це дозволяє командам безпеки оперативно реагувати на загрози, проводити подальше розслідування та вживати необхідних заходів для блокування несанкціонованого доступу та мінімізації потенційного збитку. Таким чином, SIEM-системи є незамінним інструментом для забезпечення інформаційної безпеки та захисту від внутрішніх і зовнішніх загроз.

SIEM-системи є важливим інструментом для виявлення несанкціонованого доступу, але аналіз поведінки користувачів (UBA)), пропонує інший, але комплементарний підхід до виявлення загроз, зокрема несанкціонованого доступу до заборонених ресурсів. Замість того, щоб концентруватися на подіях та журналах, як це роблять SIEM-системи, UBA/UEBA зосереджується на поведінці користувачів та інших сутностей в інформаційній системі, таких як пристрої, програми та сервери.

Основна ідея UBA/UEBA полягає у встановленні базових профілів нормальної поведінки для кожного користувача та сутності. Це досягається шляхом безперервного збору та аналізу даних про їхню діяльність, включаючи час входу в систему, ресурси, до яких вони звертаються, обсяги переданих даних, використовувані пристрої та географічне розташування. Для аналізу цих великих обсягів даних UBA/UEBA-системи використовують алгоритми машинного навчання та статистичний аналіз.

Після встановлення базових ліній поведінки, UBA/UEBA-системи в реальному часі відстежують будь-які відхилення від цих норм. Нетипова активність, яка може свідчити про несанкціонований доступ, включає в себе

спроби доступу до заборонених ресурсів, вхід в систему з незвичайних місць або в неробочий час, різке збільшення обсягу завантажених або переданих даних, використання невідомих пристроїв або облікових записів.

На відміну від SIEM-систем, які часто покладаються на заздалегідь визначені правила для виявлення загроз, UBA/UEBA здатні виявляти аномалії, які не відповідають відомим шаблонам атак. Це робить їх особливо ефективними у виявленні внутрішніх загроз, скомпрометованих облікових записів та складних цільових атак, де зловмисники можуть намагатися діяти непомітно, використовуючи легітимні облікові дані.

Коли UBA/UEBA-система виявляє аномальну поведінку, вона генерує сповіщення, надаючи контекстну інформацію про потенційну загрозу. Це дозволяє службам безпеки краще розуміти ризики та приймати обґрунтовані рішення щодо реагування на інциденти. Таким чином, UBA/UEBA є цінним доповненням до традиційних засобів безпеки, забезпечуючи додатковий рівень захисту від несанкціонованого доступу та інших кіберзагроз шляхом розуміння та аналізу поведінки користувачів та сутностей в інформаційному середовищі.

Deep Packet Inspection (DPI) є потужною технологією аналізу мережевого трафіку, яка забезпечує глибокий рівень контролю та розуміння даних, що передаються мережею. На відміну від традиційних методів перевірки пакетів, які обмежуються аналізом заголовків (наприклад, IP-адреси, порти), DPI здатна заглиблюватися у вміст кожного пакета даних. Це дозволяє не лише ідентифікувати протоколи та програми, що використовуються, але й аналізувати фактичні дані, які передаються.

У контексті виявлення несанкціонованого доступу до заборонених ресурсів, DPI відіграє важливу роль, надаючи можливість виявляти спроби обходу контролів доступу або передачу забороненого контенту. Оскільки DPI аналізує сам пакет, він може ідентифікувати шкідливе пз, спроби SQL-ін'єкцій, передачу конфіденційної інформації без якісного шифрування або використання протоколів, заборонених політиками безпеки.

Наприклад, якщо користувач намагається завантажити заборонений файл через веб-браузер, DPI може ідентифікувати сигнатури цього файлу у вмісті пакетів, навіть якщо спроба маскується під легітимний трафік. Аналогічно, спроби отримати доступ до захищеної бази даних шляхом вставки шкідливого SQL-запиту можуть бути виявлені шляхом аналізу вмісту пакетів, що містять ці запити.

Крім того, DPI може використовуватися для забезпечення дотримання політик використання мережі, запобігаючи несанкціонованому доступу до певних веб-сайтів або сервісів. Шляхом аналізу URL-адрес та вмісту HTTP-запитів, DPI може блокувати доступ до ресурсів, які вважаються небажаними або небезпечними.

Однак, варто зазначити, що використання DPI викликає певні питання щодо конфіденційності, оскільки передбачає аналіз вмісту комунікацій користувачів. Тому, при впровадженні DPI, організації повинні враховувати законодавчі вимоги та етичні аспекти, забезпечуючи прозорість та мінімізуючи вплив на приватність користувачів [14].

Незважаючи на це, DPI залишається цінною технологією для виявлення та запобігання несанкціонованому доступу до заборонених ресурсів, надаючи глибокий рівень видимості мережевого трафіку та дозволяючи виявляти загрози, які можуть бути непомітними для менш глибоких методів аналізу.

Також важливими хоча різними технологіями для виявлення несанкціонованого доступу є DNS-аналіз та Моніторинг на кінцевих пристроях (Endpoint Monitoring)

DNS-аналіз зосереджується на системі доменних імен (DNS), яка є своєрідною "телефонною книгою" інтернету, що перетворює зрозумілі для людини доменні імена на IP-адреси, необхідні для встановлення з'єднання. Зловмисники часто використовують DNS для різних шкідливих цілей, включаючи Command and Control (C2) зв'язок зі скомпрометованими системами,

перенаправлення трафіку на фішингові сайти або розповсюдження шкідливого програмного забезпечення.

DNS-аналіз передбачає моніторинг DNS-запитів, що надходять з мережі організації, та відповідей, які повертаються від DNS-серверів. Виявляючи незвичайні або шкідливі DNS-запити, можна ідентифікувати потенційні загрози. Наприклад, запити до відомих шкідливих доменів, доменів, що нещодавно були зареєстровані та мають підозрілу репутацію, або велика кількість невдалих DNS-запитів можуть бути індикаторами компрометації [15].

Крім того, DNS-аналіз може виявити спроби DNS-туннелювання, коли зловмисники маскують шкідливий трафік під звичайні DNS-запити та відповіді, щоб обійти традиційні засоби захисту. Аналізуючи розмір, частоту та структуру DNS-пакетів, можна виявити аномалії, що свідчать про таку активність.

Моніторинг на кінцевих пристроях (Endpoint Monitoring), з іншого боку, фокусується на діяльності, що відбувається безпосередньо на комп'ютерах користувачів, серверах та інших кінцевих точках мережі. Цей підхід забезпечує глибоку видимість процесів, файлової системи, реєстру, мережевих підключень та іншої активності, що відбувається на окремих пристроях.

Завдяки моніторингу кінцевих точок можна виявляти спроби несанкціонованого доступу до локальних ресурсів, запуск шкідливого програмного забезпечення, підозрілі зміни конфігурації, незвичайну активність облікових записів та інші дії, які можуть свідчити про компрометацію або порушення політик безпеки.

Сучасні рішення для моніторингу кінцевих точок, часто відомі як EDR (Endpoint Detection and Response), використовують розширені методи аналізу поведінки, машинного навчання та бази знань про загрози для виявлення складних атак, які можуть не залишати слідів у мережевому трафіку або журналах подій. Вони також надають можливості для реагування на виявлені інциденти, такі як ізоляція уражених пристроїв, видалення шкідливих файлів та блокування шкідливих процесів.

DNS-аналіз та моніторинг на кінцевих пристроях, є важливими складовими багаторівневої стратегії безпеки. DNS-аналіз забезпечує раннє виявлення загроз на рівні мережевої інфраструктури, тоді як моніторинг кінцевих точок надає детальну інформацію про діяльність, що відбувається безпосередньо на пристроях, дозволяючи виявляти та реагувати на загрози, які могли проникнути в мережу. Їхнє комбіноване використання значно підвищує здатність організації виявляти та запобігати несанкціонованому доступу до заборонених ресурсів.

Таким чином, сучасна корпоративна мережа стикається з різноманітними методами обходу систем обмеження доступу. Користувачі можуть застосовувати як технічні інструменти для маскування трафіку, так і більш складні технології, що ускладнюють виявлення їхніх дій. У відповідь на це впроваджуються багатоетапні системи виявлення та аналізу, які охоплюють як мережеву інфраструктуру, так і поведінку користувачів. Для кращого розуміння взаємозв’язку між технологіями доступу до заборонених ресурсів та способами виявлення обходу наведено таблиці 1.1

Таблиця 1.1 технології та виявлення та доступу до заборонених ресурсів

Методи доступу / Технології протидії	Фаєрвол (Firewall)	IDS/IPS	DPI	SIEM	DNS-аналіз	UBA/ UEBA	EDR
1	2	3	4	5	6	7	8
Використання VPN	+/-	+	+	+	+	+	+
Проксі-сервери	+	+	+	+	+	+	+
Анонімні мережі (Tor, I2P)	-	+	+	+	+	+	+

Кінець таблиці 1.1

1	2	3	4	5	6	7	8
Тунелювання через нестандартні порти	-	+	+	+	-	+	+/-
Шифрування трафіку (HTTPS, SSH, TLS)	-	+/-	+/-	+	-	+	+/-
DNS-тунелювання	-	+	+	+	+	+	-

1.3 Постановка задачі

У сучасному цифровому середовищі, де більшість підприємств активно використовують мережеву інфраструктуру для виконання повсякденних операцій, питання контролю інформаційних потоків стає критично важливим. Одним із серйозних викликів, з яким стикаються IT-відділи та служби кібербезпеки, є несанкціонований доступ до заборонених ресурсів зсередини корпоративної мережі. Це може включати спроби відвідування сайтів, що порушують політику компанії, використання сторонніх інструментів обходу фільтрації (VPN, проксі-серверів, анонімних мереж), завантаження забороненого контенту або підключення до зовнішніх сервісів, які становлять загрозу для безпеки підприємства.

Такі дії, навіть якщо вони виконуються не зі зловмисною метою, можуть призвести до серйозних наслідків. По-перше, порушення політик доступу може

спричинити витік конфіденційної інформації або компрометацію внутрішніх даних. По-друге, використання сторонніх засобів для обходу обмежень унеможливлює централізований контроль та моніторинг, що вкрай необхідно для дотримання стандартів інформаційної безпеки. І по-третє, зростає ризик зараження внутрішньої мережі шкідливим програмним забезпеченням або відкриття каналів зв’язку з потенційно небезпечними зовнішніми вузлами.

З огляду на ці загрози, актуальним завданням є створення такої системи, яка дозволила б виявляти і реагувати на спроби несанкціонованого доступу до заборонених ресурсів у режимі реального часу. Це повинна бути система, яка поєднує сучасні технології аналізу мережевого трафіку, машинного навчання та поведінкової аналітики для комплексного моніторингу активності користувачів і автоматичного виявлення порушень політик безпеки.

Під час розробки такої системи необхідно вирішити низку наукових і практичних задач. Насамперед, слід провести глибокий аналіз сучасних підходів до виявлення аномалій у трафіку, технологій IDS/IPS, SIEM, DPI, а також засобів моніторингу поведінки користувачів (UEBA). Важливо не лише порівняти їх за критеріями точності, швидкості реагування, масштабованості та інтеграції, а й оцінити їхню ефективність саме в контексті виявлення доступу до заборонених ресурсів, зокрема із застосуванням методів шифрування та обфускації трафіку.

Наступним кроком є вибір найбільш релевантної системи, яка відповідатиме вимогам корпоративної мережі за технічними, функціональними та економічними параметрами. Це передбачає як технічне розгортання вибраного рішення, так і його адаптацію до особливостей інфраструктури, з урахуванням чинної архітектури мережі, політик доступу, ролей користувачів тощо. Особливу увагу слід приділити етапу налаштування сигнатур або правил виявлення загроз, створенню алгоритмів кореляції подій та сценаріїв інцидентів безпеки.

Далі необхідно реалізувати моделювання типових загроз, які найчастіше зустрічаються в корпоративному середовищі. Це можуть бути спроби підключення до VPN-серверів, використання TOR або проксі, тунелювання

трафіку через нестандартні порти, звернення до ресурсів, що перебувають у чорному списку компанії. На основі цього проводиться тестування системи в умовах, максимально наближених до реального робочого середовища. Метою цього етапу є перевірка здатності системи своєчасно виявляти та ідентифікувати порушення, а також оцінка її надійності, точності та рівня хибнопозитивних спрацьовувань.

Завершальним етапом є аналіз отриманих результатів, формування висновків щодо ефективності розробленого рішення, а також підготовка рекомендацій для його впровадження в реальних корпоративних середовищах. Таким чином, результатом даної роботи має стати дієвий програмно-апаратний або програмний комплекс, що здатен виявляти несанкціоновані дії користувачів щодо доступу до заборонених ресурсів та забезпечити прозорий контроль за дотриманням політик інформаційної безпеки у внутрішній мережі підприємства.

2 ОГЛЯД, ПОРІВНЯННЯ ТА ОБҐРУНТУВАННЯ ВИБОРУ СИСТЕМИ

2.1 Аналіз систем виявлення несанкціонованого доступу до заборонених ресурсів з виходом на перелік критеріїв порівняння.

В умовах зростання кількості кіберзагроз та поширення інструментів для обходу обмежень у корпоративних мережах особливої актуальності набуває задача виявлення несанкціонованого доступу до заборонених ресурсів. Користувачі можуть свідомо або неусвідомлено використовувати інструменти типу VPN, TOR, HTTP/HTTPS проксі, DNS-тунелі, SSH-тунелі або нестандартні порти для обходу корпоративних політик доступу. Це становить загрозу як для інформаційної безпеки організації, так і для виконання внутрішніх регламентів, стандартів (наприклад, ISO/IEC 27001) та юридичних вимог. Для виявлення таких дій необхідно використовувати спеціалізовані системи, які здатні працювати як на мережевому, так і на хостовому рівні, виявляти аномалії, сигнатури відомих загроз, корелювати події та аналізувати поведінку користувачів [16].

До найбільш поширених типів таких систем належать IDS/IPS, SIEM, DPI, UEBA та EDR-рішення. Їх застосування може бути ізольованим або інтегрованим, що дає змогу формувати багаторівневу систему виявлення загроз.

IDS (Intrusion Detection System) та IPS (Intrusion Prevention System) є класичними інструментами контролю трафіку. Вони дозволяють здійснювати глибокий аналіз пакетів даних, виявляти підозрілі шаблони трафіку або поведінкові відхилення. Snort і Suricata — найпопулярніші представники цього класу. Snort використовує сигнатурний метод, тоді як Suricata також підтримує потоковий аналіз, а також роботу з TLS/SSL-сесіями, що дозволяє виявляти використання VPN-протоколів чи обфускації трафіку. Наприклад, Suricata може зафіксувати використання WireGuard або OpenVPN через аналіз специфічних параметрів handshake-процесів або портів.

SIEM-системи (Security Information and Event Management), такі як Wazuh, Splunk або ArcSight, дозволяють об'єднувати дані з різних джерел — логів

операційної системи, журналів доступу, фаєрволів, мережевих пристроїв — у єдину інформаційну систему. Це забезпечує можливість глибокого аналізу і кореляції подій, створення звітів, побудови графіків і таймлайнів. Наприклад, Wazuh, який також має функції HIDS, може виявляти запуск TOR, підключення до невідомих VPN-серверів, використання проксі або нестандартних портів на підставі системних логів та запуску процесів [17].

Системи DPI (Deep Packet Inspection) — менш поширені через вимоги до обчислювальних ресурсів, проте надзвичайно ефективні в складних середовищах. DPI дозволяє аналізувати тіло мережевого пакету, включно з метаданими TLS-з'єднань, типом запитів, DNS-іменами, ентропією вмісту. Це дає змогу виявляти проксі, TOR або DNS-тунелювання навіть при наявності шифрування. DPI часто використовується в продуктах Fortinet, Palo Alto, Cisco Firepower тощо [18].

UEBA (User and Entity Behavior Analytics) є новітнім підходом, що базується на аналізі поведінки користувача. Системи цього типу будують профіль «нормальної» активності кожного облікового запису або пристрою. В разі відхилення — наприклад, якщо офісний працівник, який раніше використовував лише браузер і пошту, починає регулярно встановлювати з'єднання з TOR-серверами — система генерує інцидент. UEBA часто використовується як модуль у великих SIEM-рішеннях або як окрема платформа [19].

Останньою складовою є EDR-системи (Endpoint Detection and Response), які здійснюють постійний моніторинг кінцевих точок. Вони дозволяють виявити запуск VPN-клієнта, зміну конфігурацій маршрутизатора, підключення нестандартного пристрою або використання нестандартного DNS. Приклади — OSSEC, CrowdStrike Falcon, Microsoft Defender for Endpoint. На рисунку 2.1 представлено типову схему взаємодії між компонентами IDS/IPS та SIEM [27]

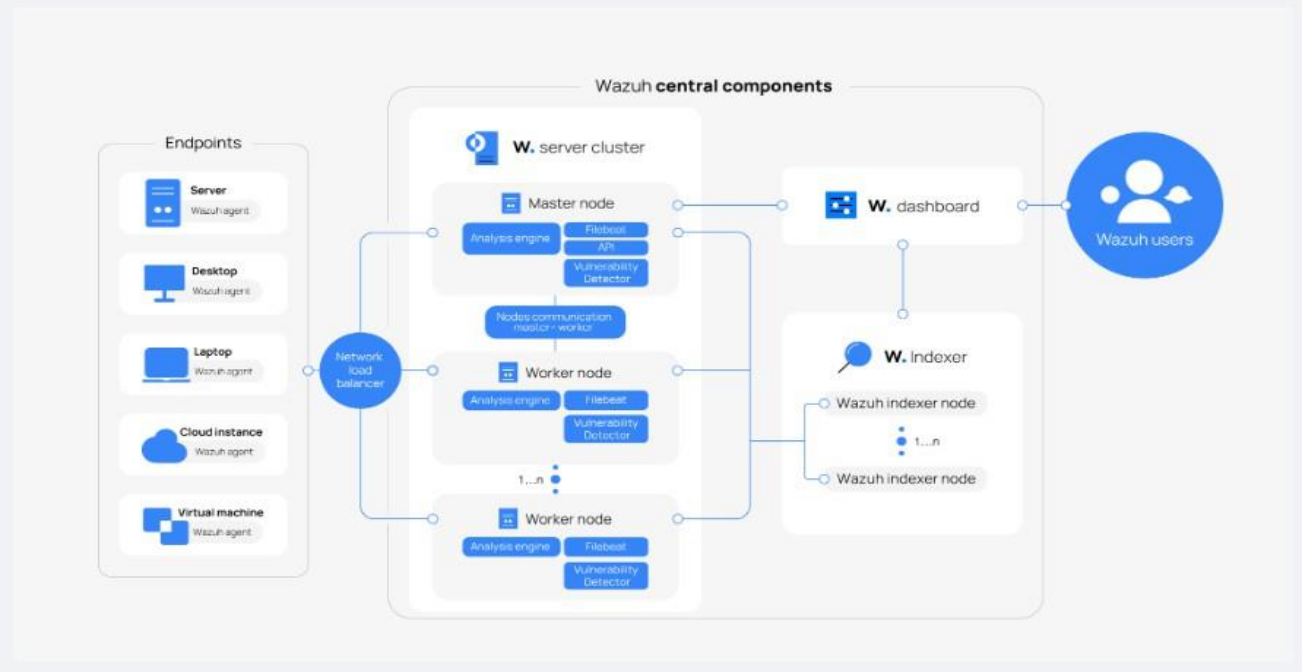


Рисунок 2.1 — Діаграма архітектури Wazuh

Таким чином, ефективне виявлення несанкціонованого доступу не може базуватись на єдиному інструменті. Найбільш надійні рішення комбінують функціонал кількох підходів, зокрема SIEM для аналітики, IDS/IPS для мережевого виявлення, EDR для моніторингу дій користувачів та UEBA для оцінки поведінкових відхилень. У наступному підрозділі буде здійснено вибір конкретної системи для впровадження в межах цієї роботи на основі визначених функціональних критеріїв.

Таблиця 2.1 Основні характеристики і порівняння систем

Тип системи	Приклад	Виявлення VPN	Виявлення TOR	Підтримка логів	Аналіз поведінки	Реакція
1	2	3	4	5	6	7
IDS/IPS	Snort, Suricata	Так	Так	Ні	Ні	Так/ні
SIEM	Wazuh, Splunk	Так	Так	Так	Обмежно	Так

Кінець таблиці 2.1

1	2	3	4	5	6	7
DPI	nDPI, Palo Alto NGFW	Так	Так	Обмежено	Ні	Так
UEBA	Securonix, Exabeam	Частково	Частково	Так	Так	Ні
EDR	OSSEC, CrowdStrike	Частково	Частково	Частково	Так	Так

Таким чином, для виявлення несанкціонованого доступу до заборонених ресурсів доцільно використовувати комбінацію SIEM+IDS+EDR, що дозволяє досягти балансу між глибиною аналізу, точністю виявлення та швидкістю реагування. Особливо ефективною є інтеграція SIEM-рішення, такого як Wazuh, із Snort або Suricata та модулем поведінкового аналізу. Це забезпечує повноцінне покриття як мережевого, так і прикладного рівня виявлення загроз.

На основі проведеного аналізу можна сформувати перелік ключових критеріїв, які будуть використані для обґрунтування вибору систем виявлення несанкціонованого доступу до заборонених ресурсів:

- Повнота покриття (види загроз, які система здатна виявляти);
- швидкість виявлення та реакції;
- простота впровадження та налаштування;
- масштабованість;
- вартість (наявність безкоштовної версії) ;
- підтримка поведінкового аналізу;
- можливість інтеграції з іншими системами;

Ці критерії дозволять обґрунтовано обрати оптимальне рішення для подальшого практичного впровадження у межах корпоративної мережі.

2.2 Обґрунтування вибору систем виявлення несанкціонованого доступу до заборонених ресурсів.

Аналіз існуючих систем виявлення несанкціонованого доступу до заборонених ресурсів показав, що жоден окремий клас систем — IDS/IPS, SIEM, DPI, UEBA чи EDR — не може повністю забезпечити ефективний та всебічний моніторинг усіх типів порушень. Особливо актуально це в умовах, коли порушники активно використовують шифрування, нестандартні протоколи, анонімізатори та інші методи обходу мережевих обмежень. Тому обґрунтування вибору має ґрунтуватися не лише на аналізі функціональності, а й на гнучкості системи, її здатності до інтеграції, адаптації до потреб конкретного середовища та глибини аналітики.

Серед проаналізованих систем найкращим кандидатом на впровадження в межах даної кваліфікаційної роботи є платформа Wazuh. Це система рішення з відкритим кодом, що включає в себе функціональність SIEM, HIDS (Host-based Intrusion Detection System), засобів аналізу подій, моніторингу цілісності файлів та аналітики поведінки. Перевага Wazuh полягає в її гнучкій архітектурі: вона підтримує встановлення як у вигляді централізованої платформи для моніторингу всієї інфраструктури, так і у вигляді окремих агентів на хостах для детального контролю кінцевих точок [20].

Wazuh має вбудовані механізми для інтеграції з системами мережевого аналізу, такими як Suricata або Zeek, що дозволяє об'єднати мережеву та хостову аналітику в одному середовищі. Це відкриває можливість детектувати, з одного боку, зовнішні спроби проникнення або вихід на сторонні сервери, а з іншого — аномалії у поведінці користувача, запуск заборонених додатків, спроби тунелювання трафіку або використання VPN-клієнтів [21].

Важливою перевагою Wazuh є її сумісність з indexer та dashboard. dashboard відповідає за швидке індексування великих обсягів даних журналів, а indexer — за зручну візуалізацію інформації, створення панелей моніторингу (dashboard),

побудову звітів, часових ліній подій та графіків. Таким чином, адміністратор отримує повноцінне середовище для роботи з подіями безпеки в режимі реального часу.

У контексті виявлення саме несанкціонованого доступу до заборонених ресурсів Wazuh забезпечує ефективну обробку таких сценаріїв:

- виявлення запуску VPN-клієнтів, таких як OpenVPN, WireGuard, SoftEther, на основі моніторингу процесів (auditd, osquery) або аналізу логів;
- виявлення запуску TOR-браузера або клієнта на основі сигнатур процесів та бібліотек, які використовує Tor;
- моніторинг звернень до анонімних проксі або DNS-запитів до підозрілих доменів (через інтеграцію з Threat Intelligence базами);
- фіксація змін у файлах конфігурації мережевих інтерфейсів (що може свідчити про спробу ручного тунелювання);
- автоматичне генерування сповіщень про порушення, запис у журнал безпеки та виконання контрдій (відправка email, блокування IP, запуск скриптів тощо) [22].

Додатковою перевагою є активна спільнота Wazuh, яка забезпечує постійну підтримку, оновлення правил безпеки, шаблони дашбордів, а також відкриті репозиторії з прикладами інтеграцій. Оскільки система підтримує API, вона може використовуватись як база для побудови кастомних рішень.

Попри наявність комерційних альтернатив, таких як Splunk або IBM QRadar, саме Wazuh виявляється оптимальним вибором для цілей даної роботи. Це рішення поєднує глибоку функціональність, підтримку мережевих і хостових подій, адаптивність і доступність без ліцензійних обмежень. Крім того, воно дозволяє гнучко масштабувати систему від однієї станції до централізованої інфраструктури [23].

Інтеграція Wazuh з системами моніторингу, зокрема filebeat, дає змогу реалізувати багатошарову систему виявлення, яка буде реагувати на відхилення поведінки користувачів, нетипові з'єднання, сигнатури VPN-трафіку, та запуск

заборонених додатків. Такий підхід відповідає концепції Zero Trust і дозволяє забезпечити відповідність сучасним вимогам кібербезпеки.

Відтак, зважаючи на аналіз функціональних можливостей, гнучкість, адаптованість до умов корпоративного середовища, доступність, потужну документацію та спільноту підтримки, система Wazuh обрана як базова платформа для подальшого впровадження, налаштування та тестування у межах корпоративної мережі.

2.3 Висновки

Результати аналітичного етапу дослідження підтвердили, що у сучасних умовах постійного зростання кіберзагроз та активного використання технологій обходу фільтрації доступу (таких як VPN, проксі, TOR, DNS-тунелі), організаціям необхідно впроваджувати багаторівневі системи виявлення несанкціонованого доступу до заборонених ресурсів. Одновимірні рішення — наприклад, лише IDS/IPS або фаєрвол — уже не здатні самостійно забезпечити надійний захист. Тому оптимальним підходом є інтеграція декількох технологій безпеки, які спільно забезпечують як глибокий аналіз трафіку, так і виявлення підозрілої активності на рівні кінцевих точок та користувачів.

У рамках аналізу були розглянуті п’ять основних класів систем: IDS/IPS, SIEM, DPI, UEBA та EDR. Кожен із них має свої сильні сторони. IDS/IPS дозволяють виявляти шаблони мережевого трафіку, SIEM — обробляти і корелювати події з великої кількості джерел, DPI — аналізувати зміст трафіку, UEBA — виявляти аномалії в поведінці користувачів, а EDR — здійснювати моніторинг дій на кінцевих пристроях. Проте жодна з цих систем у відриві від інших не забезпечує повного охоплення необхідних задач у сфері контролю доступу [20][29].

На підставі порівняння систем за ключовими критеріями (функціональність, масштабованість, доступність, інтеграційність, підтримка поведінкового аналізу, ефективність виявлення загроз) було прийнято обґрунтоване рішення обрати для подальшого впровадження SIEM-систему Wazuh. Цей вибір обумовлений не лише її багатофункціональністю та відкритістю коду, але й високою гнучкістю у налаштуванні, активною спільнотою користувачів і наявністю повноцінної документації.

Wazuh дозволяє ефективно виявляти спроби обходу фільтрації: запуск VPN-клієнтів, використання TOR, нетипову мережеву активність, зміну конфігурацій тощо. Інтеграція з Suricata або Zeek дозволяє розширити можливості системи за рахунок глибокого аналізу мережевого трафіку, а використання Elasticsearch і Kibana забезпечує високий рівень візуалізації, інтерпретації та взаємодії з даними [30].

У контексті масштабованості, особливої уваги заслуговує здатність розгортання Wazuh в кластерному режимі. Це дозволяє досягти високої доступності системи, розподілити навантаження між декількома вузлами та забезпечити стабільну роботу навіть у великих інфраструктурах. На рисунку 2.2 подано архітектуру кластерної моделі Wazuh [28]:

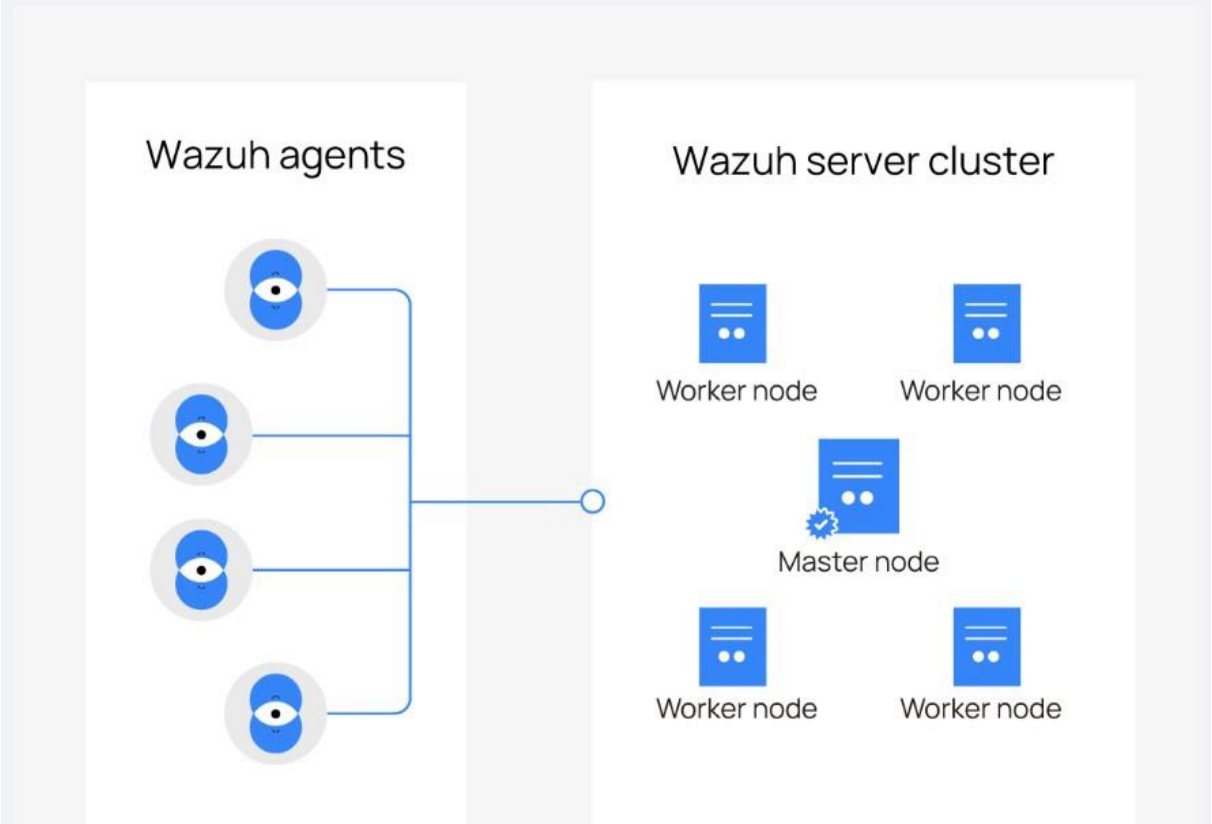


Рисунок 2.2 – Типова кластерна архітектура Wazuh

Ця схема наочно демонструє, як компоненти системи (агенти, сервери, індексатори, панелі управління) можуть працювати у взаємодії, забезпечуючи надійний і масштабований захист. Кластерна модель особливо актуальна для організацій, які прагнуть побудувати безперервну систему безпеки із резервуванням та автоматичним балансуванням навантаження.

Таким чином, можна зробити висновок, що обрана система Wazuh є повноцінним рішенням, здатним забезпечити виявлення несанкціонованого доступу до заборонених ресурсів на високому рівні ефективності. Її функціональність дозволяє не лише контролювати мережеву та системну активність, а й будувати гнучкі правила виявлення, формувати звіти, автоматизовувати реагування та масштабувати рішення залежно від потреб. У наступному розділі буде здійснено практичне розгортання системи, її налаштування, тестування та аналіз результатів.

3 РЕАЛІЗАЦІЯ , НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ПОРУШЕНЬ МЕРЕЖЕВОЇ ПОЛІТИКИ

3.1 Розгортання системи Wazuh

На даному етапі було реалізовано повне розгортання системи виявлення несанкціонованого доступу до заборонених ресурсів з корпоративної мережі на основі SIEM-платформи Wazuh. Це сучасне рішення дозволяє об’єднувати функціональність збору логів, аналізу поведінки, виявлення вторгнень і візуалізації подій у єдиному середовищі.

Розгортання системи передбачало підготовку серверного середовища, завантаження та інсталяцію основних компонентів, налаштування служби агентів та підключення інтерфейсу візуалізації. Усі дії виконувались поетапно, з фіксацією результатів для подальшого документування.

Передусім було створено тестове серверне середовище з операційною системою Ubuntu Server 22.04 LTS [31]. Це один із рекомендованих дистрибутивів для стабільної роботи Wazuh. Систему було розгорнуто у віртуальній машині за допомогою VirtualBox [32], що дозволило ізолювати процес розгортання від основної операційної системи та зберегти гнучкість у налаштуванні мережі.

Після встановлення ОС були виконані базові дії рисунок 3.1:

- оновлення системи sudo apt update && sudo apt upgrade -y;
- встановлення мережевих утиліт sudo apt install curl wget net-tools;

Ці кроки дозволяють уникнути потенційних конфліктів версій пакетів і забезпечити стабільну базу для подальших дій.

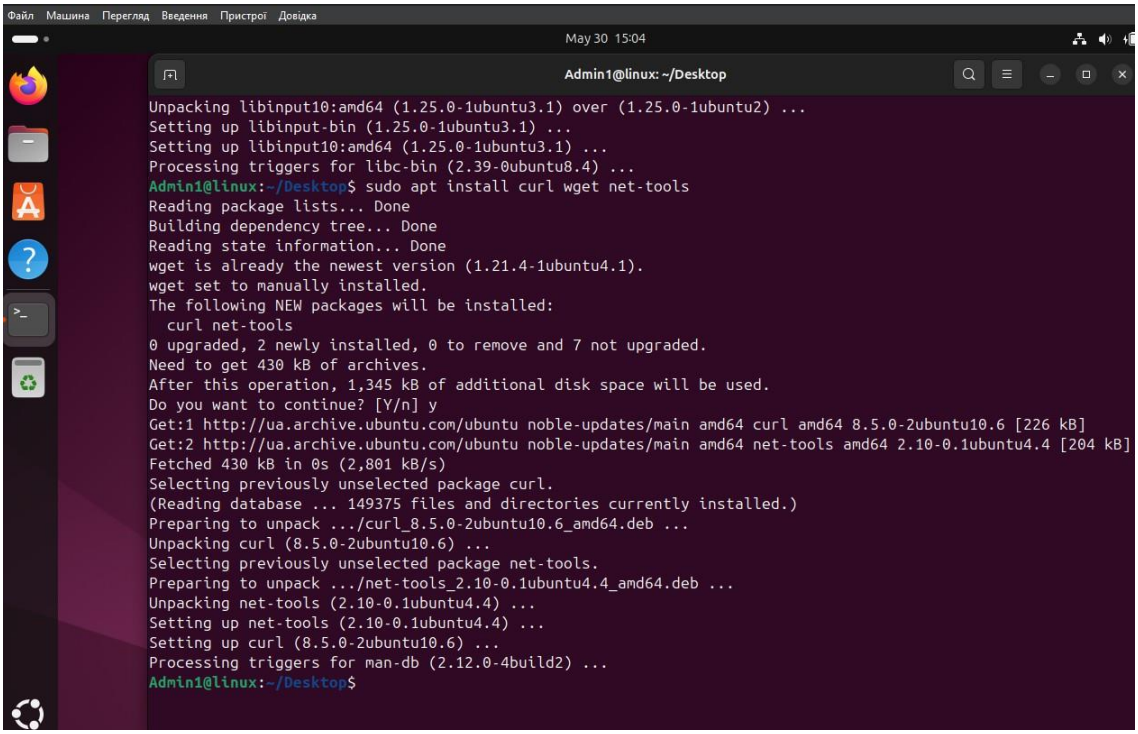


Рисунок 3.1 — Консоль Ubuntu з результатами оновлення системи

Для розгортання однонодової (single-node) конфігурації було використано офіційний інсталяційний скрипт, який автоматично завантажує та налаштовує всі необхідні компоненти [33] (Wazuh Manager, wazuh-indexer wazuh-dashboard, filebeat):

Завантаження інсталятора:

- curl -sO https://packages.wazuh.com/4.7.5-1/wazuh-install.sh

Надання прав на виконання:

- chmod +x wazuh-install.sh Запуск

автоматичного встановлення:

- sudo ./wazuh-install.sh -a -i рисунок 3.2

Ключ -a означає повну автоматизацію інсталяції всіх компонентів у рамках одного хосту. У процесі встановлення система кілька разів перевіряє залежності, доступність мережі, стан служби wazuh-dashboard, та автоматично налаштовує порти і конфігураційні файли.

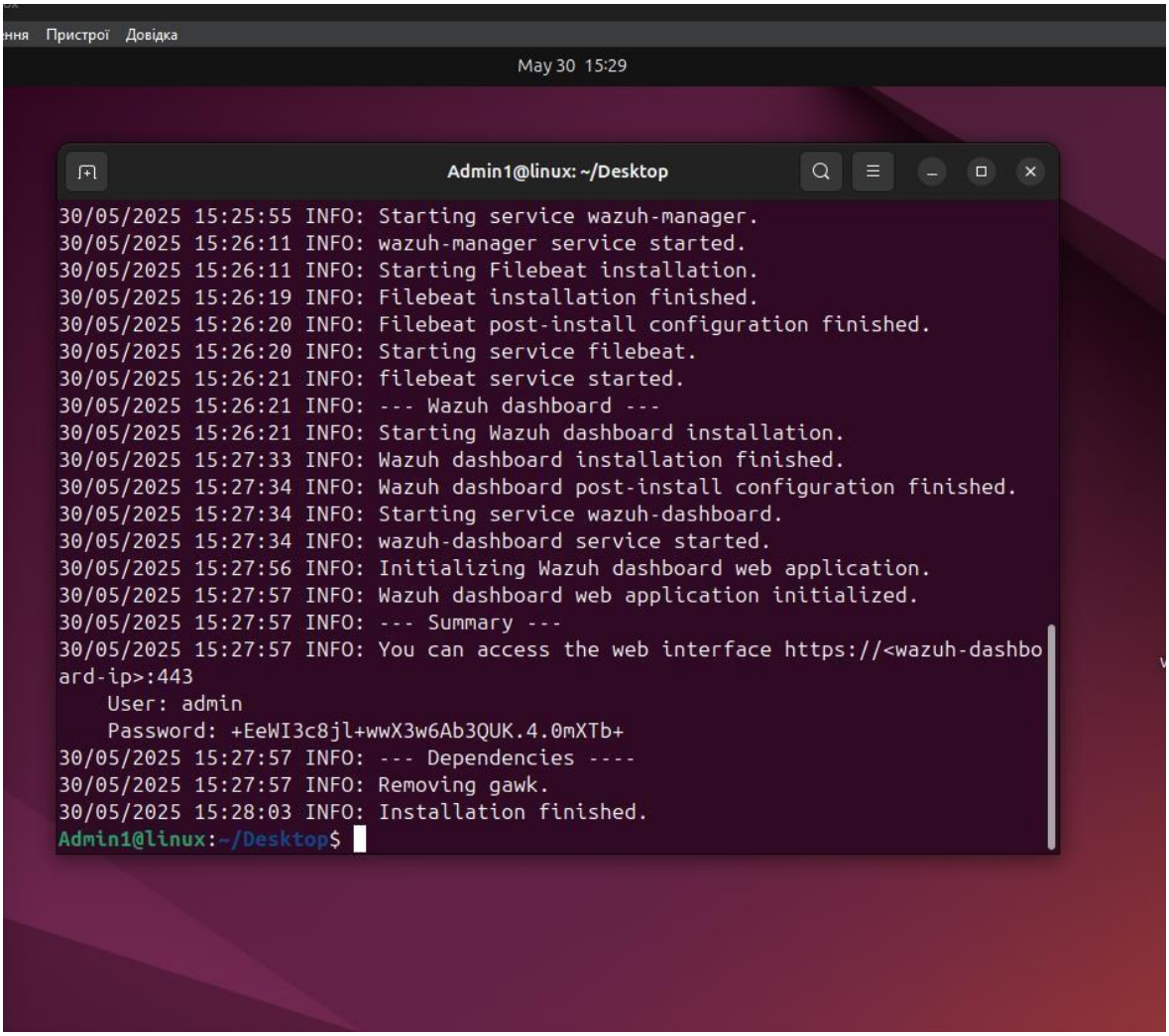


Рисунок 3.2 — Запуск інсталяційного скрипту wazuh-install.sh

Після успішного встановлення було надано доступ до веб-інтерфейсу Wazuh Dashboard:

- Ім'я користувача: admin
- Пароль:+EeWI3c8jl+wwX3w6Ab3QUK.4.0mXTb+

Після завершення автоматичної інсталяції системи необхідно перевірити, чи коректно працюють основні служби, від яких залежить стабільність та функціональність Wazuh. Починаючи з останніх версій (4.3 і вище), Wazuh більше не використовує окремі компоненти Elasticsearch і Kibana. Натомість застосовуються власні компоненти: wazuh-indexer (для зберігання та пошуку подій) і wazuh-dashboard (для візуалізації та адміністрування) [34]. Для перевірки стану служб у системі використовуються наступні команди:

- sudo systemctl status wazuh-manager
- sudo systemctl status wazuh-indexer
- sudo systemctl status wazuh-dashboardsc
- sudo systemctl status filebeat

У результаті виконання команд користувач має переконатися, що всі служби знаходяться у стані active (running) рисунок 3.3, 3.4, 3.5, 3.6. Це підтверджує, що менеджер подій, індексатор, візуальний інтерфейс та засіб транспортування логів працюють належним чином.

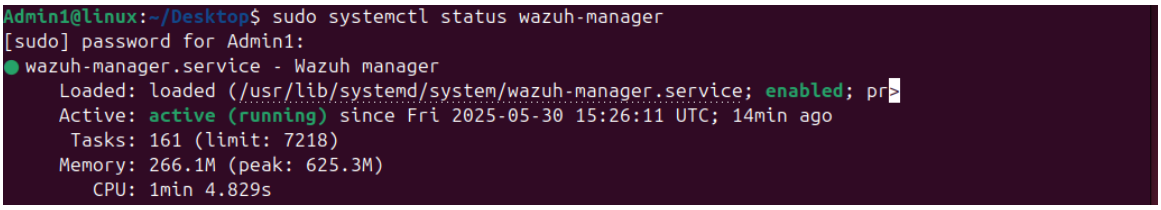


Рисунок 3.3 Статус служби wazuh-manager

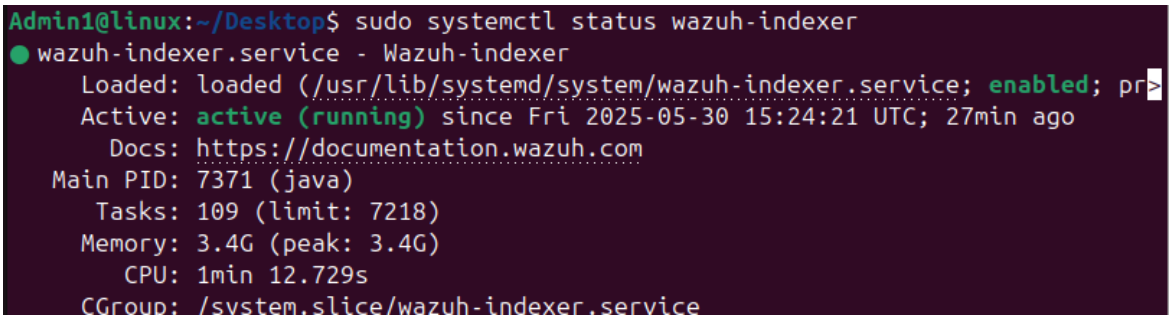


Рисунок 3.4 Статус служби wazuh-indexer

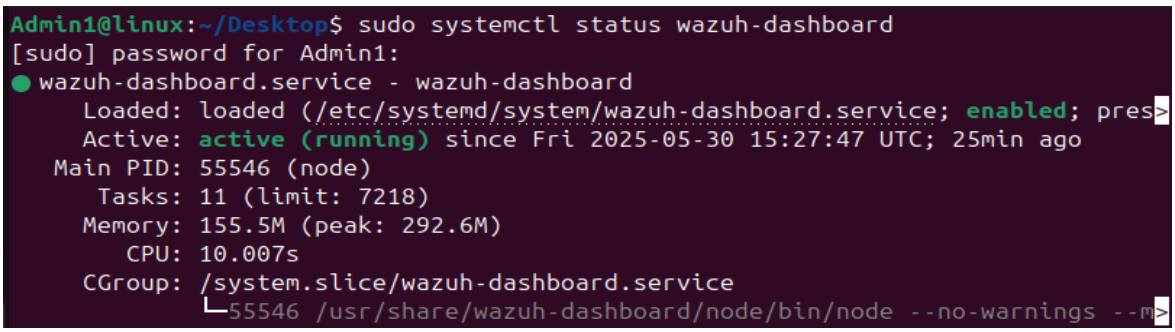


Рисунок 3.5 Статус служби wazuh-dashboard

```
Admin1@linux:~/Desktop$ sudo systemctl status filebeat
[sudo] password for Admin1:
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasti>
     Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; preset:>
     Active: active (running) since Fri 2025-05-30 15:27:45 UTC; 26min ago
       Docs: https://www.elastic.co/products/beats/filebeat
   Main PID: 55356 (filebeat)
      Tasks: 11 (limit: 7218)
     Memory: 22.6M (peak: 23.3M)
        CPU: 441ms
     CGroup: /system.slice/filebeat.service
             └─55356 /usr/share/filebeat/bin/filebeat --environment systemd -c >
```

Рисунок 3.6 Статус служби filebeat

Із версії 4.3 Wazuh використовує власну панель Wazuh Dashboard, яка відкривається у браузері.За допомогою посилання https://localhost переходим у веб-інтерфейс wazuh та за допомогою логіна і пароля який отримали раніше входим в систему рисунок 3.7.

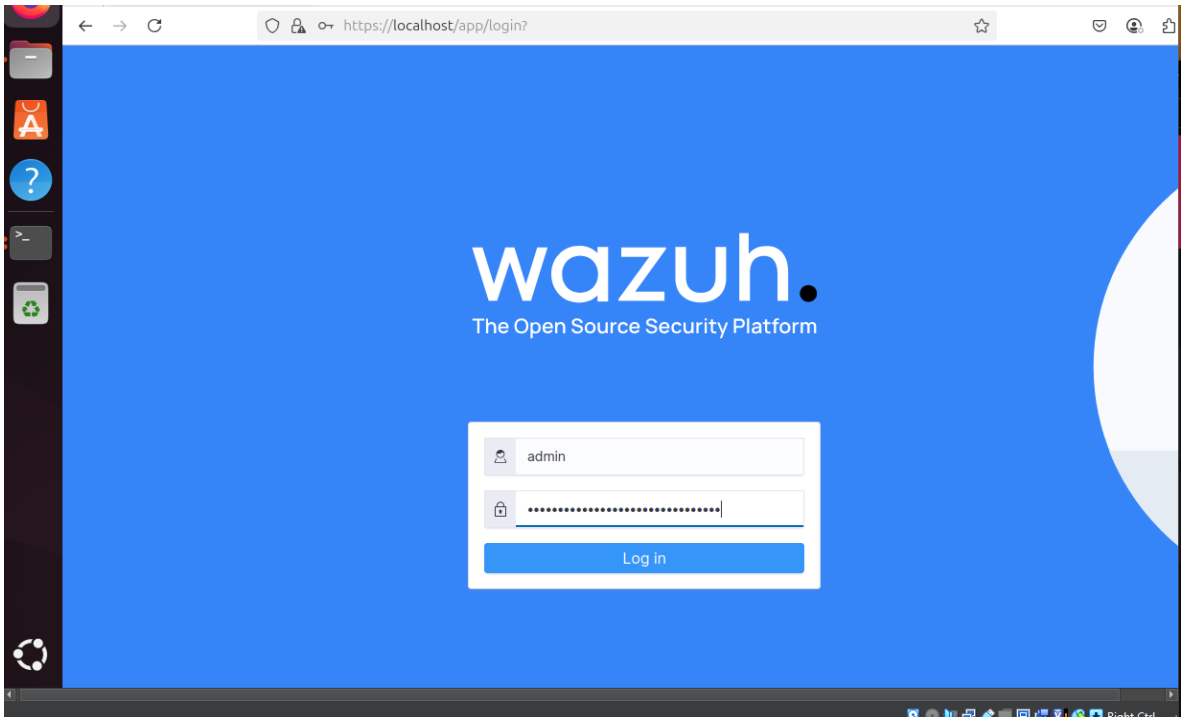


Рисунок 3.7 вікно авторизації wazuh

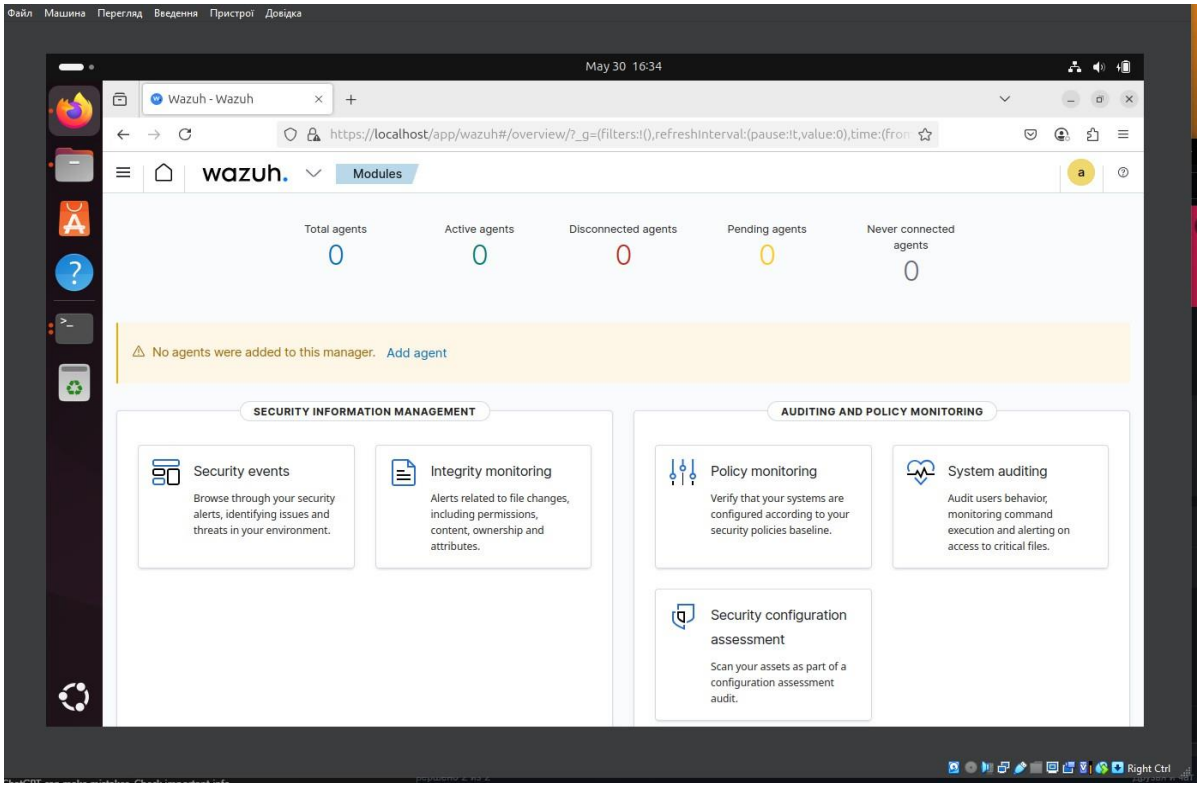


Рисунок 3.8 Інтерфейс Wazuh Dashboard після входу

Для повноцінного моніторингу системи необхідно встановити агента на клієнтський хост — той, на якому буде здійснюватись виявлення підозрілої активності (запуск VPN, TOR тощо).

```
****************************************
* Wazuh v4.7.5 Agent manager.          *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: a

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: lanos
   * The IP Address of the new agent: 192.168.0.100
Confirm adding it?(y/n): y
```

Рисунок 3.9 Створення агента і генерація ключа в manage_agents

Для забезпечення зв'язку між Wazuh Manager та агентом, встановленим на Windows-машині, необхідно було коректно вказати адресу Manager та ввести ключ аутентифікації.

На Рисунку 3.10 – Вікно налаштувань Wazuh Agent на Windows відображено інтерфейс Wazuh Agent на операційній системі Windows. У полі "Manager IP" було вказано IP-адресу Wazuh Manager – 192.168.0.106. Ця адреса є точкою входу для агента, що дозволяє йому встановлювати з'єднання з центральним сервером.

Крім того, для встановлення довіреного та безпечного з'єднання, у відповідне поле було вставлено унікальний ключ аутентифікації. Цей ключ був попередньо згенерований на Wazuh Manager під час додавання нового агента, забезпечуючи, що лише авторизовані агенти можуть підключатися до Manager [35].

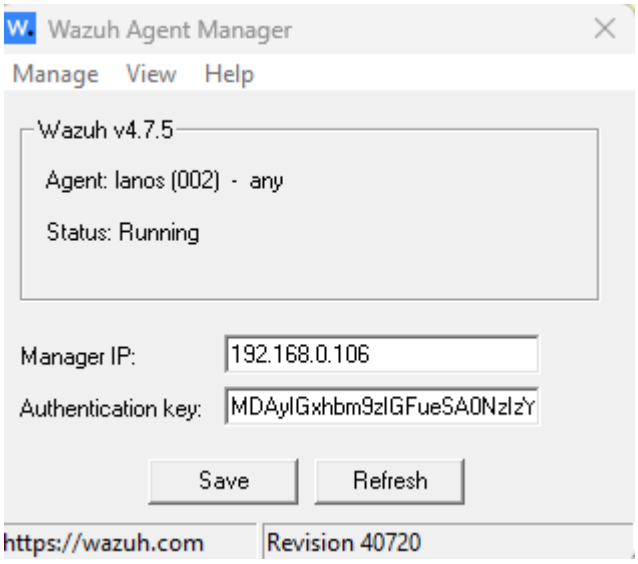


Рисунок 3.10 Вікно активації Wazuh agenta на windows

Після введення цих даних та збереження налаштувань, Wazuh Agent успішно встановив зв'язок з Wazuh Manager, перейшовши у статус "Running" на локальній машині та згодом відобразившись як "Active" у веб-інтерфейсі Wazuh Dashboard. Це підтвердило успішну інтеграцію Windows-хоста в систему моніторингу безпеки Wazuh.

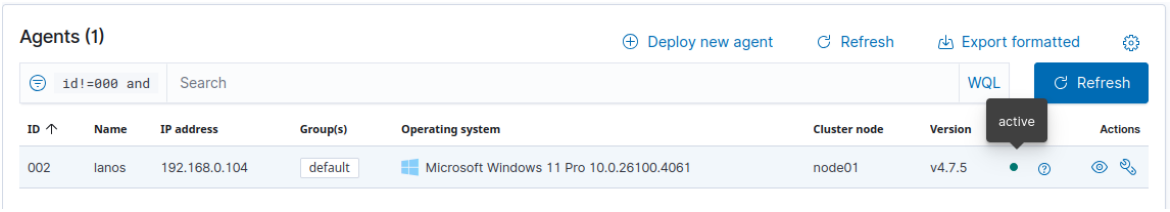


Рисунок 3.11 Успішно змінений статус на active

3.2 Налаштування системи Wazuh

Після розгортання SIEM-системи Wazuh та підключення агентів, наступним етапом стало налаштування правил виявлення інцидентів, пов'язаних із несанкціонованим доступом до заборонених ресурсів. Зокрема, увагу було зосереджено на визначенні типових ознак використання VPN-клієнтів, анонімізаторів типу TOR, а також проксі-серверів. Такі інструменти часто застосовуються для обходу внутрішніх політик безпеки, тому їх своєчасне виявлення є критичним завданням [36].

Wazuh підтримує декілька способів виявлення аномальної активності — через аналіз логів, поведінкові патерни, активність мережевих портів та запуск системних процесів. Основним механізмом є правила безпеки, які задаються у вигляді XML-структур у файлі local_rules.xml.

За замовчуванням, система Wazuh містить лише базові шаблони, тому для розширення функціональності було створено набір власних (локальних) правил, які спрацьовують при фіксації ознак використання заборонених засобів обходу мережевої фільтрації.Розміщення файлу з локальними правилами:

- /var/ossec/etc/rules/local_rules.xml

Після чого було відкрито для редагування за допопомогою sudo nano рисунок 3.12. На цьому етапі також перевіряється, чи є в системі доступ до файлу, чи він не пошкоджений, і чи структура XML збережена коректно. Порушення синтаксису можуть призвести до того, що менеджер Wazuh не зможе стартувати.

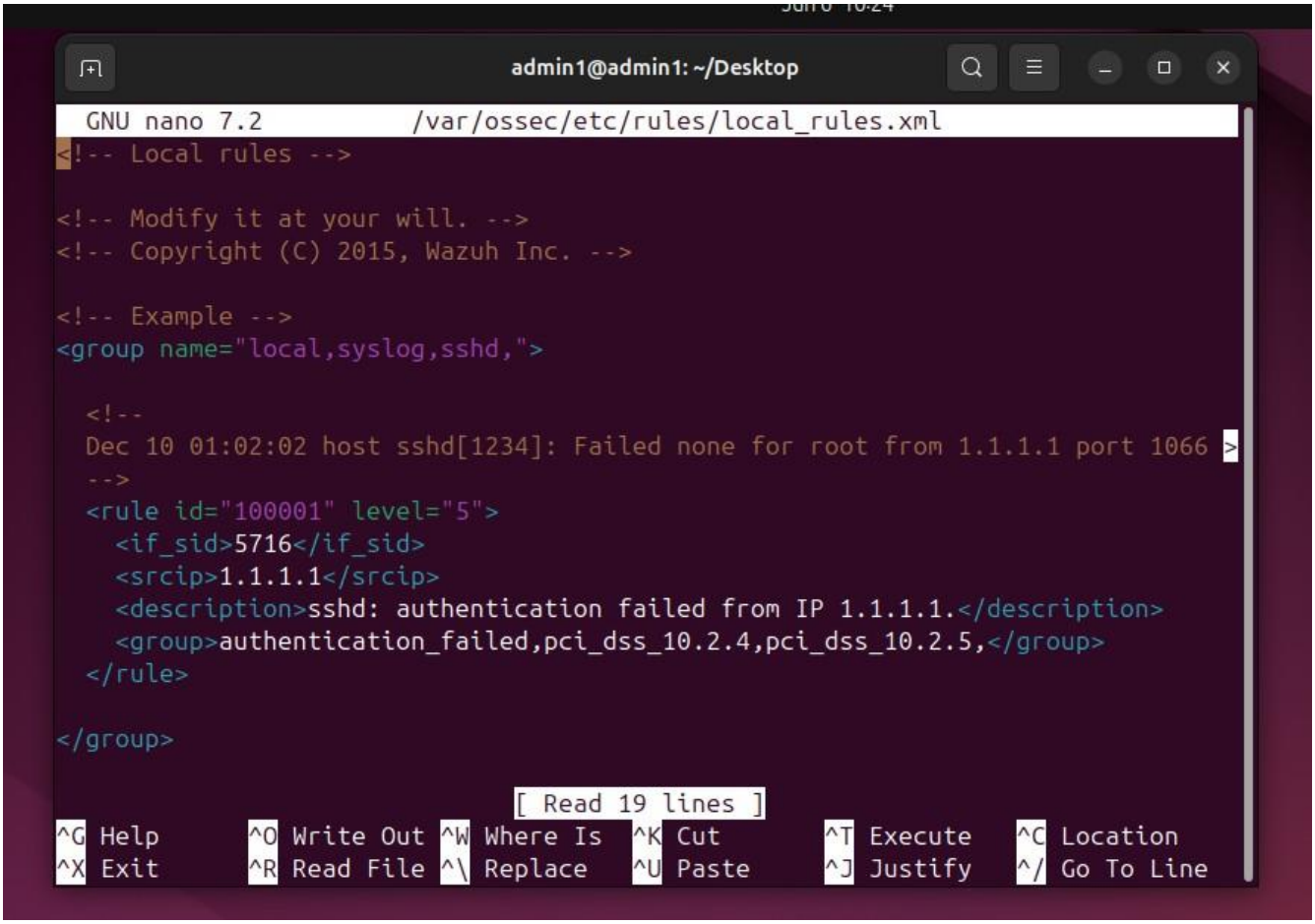


Рисунок 3.12 Відкритий файл local_rules.xml для додавання правил

VPN є одним із найрозповсюдженіших інструментів для обходу мережевих обмежень. Наприклад, OpenVPN запускає власний процес (openvpn), використовує специфічні порти (1194/UDP за замовчуванням) і створює лог-записи при ініціалізації з'єднання. Для реалізації поставлених задач спочатку було відкрито вказаний файл, у якому зафіксовано базову структуру правил безпеки у форматі XML. Усі локальні правила повинні бути обгорнуті в теги <rules>...</rules>, а кожне окреме правило має чітку структуру з визначеними елементами: унікальний ідентифікатор id, рівень критичності level, опис події <description>, ключове слово для пошуку відповідності <match>, а також класифікаційну групу <group>, яка дозволяє впорядкувати події. Було створено

три окремі правила, кожне з яких відповідає за виявлення певного типу активності, що порушує політику безпеки.

Перше правило орієнтоване на виявлення використання VPN-сервісів, зокрема OpenVPN, який є одним із найпоширеніших у корпоративному середовищі. Сигнатурою для цього правила є ключове слово openvpn, що може міститись у назві запущеного процесу, логах, командах чи конфігураційних файлах. Система реагує на появу цього слова у вхідних даних, що дозволяє швидко зафіксувати факт запуску VPN-клієнта. Рівень критичності для цього правила встановлено на рівні 7, що відповідає високій загрозі з точки зору контролю доступу.

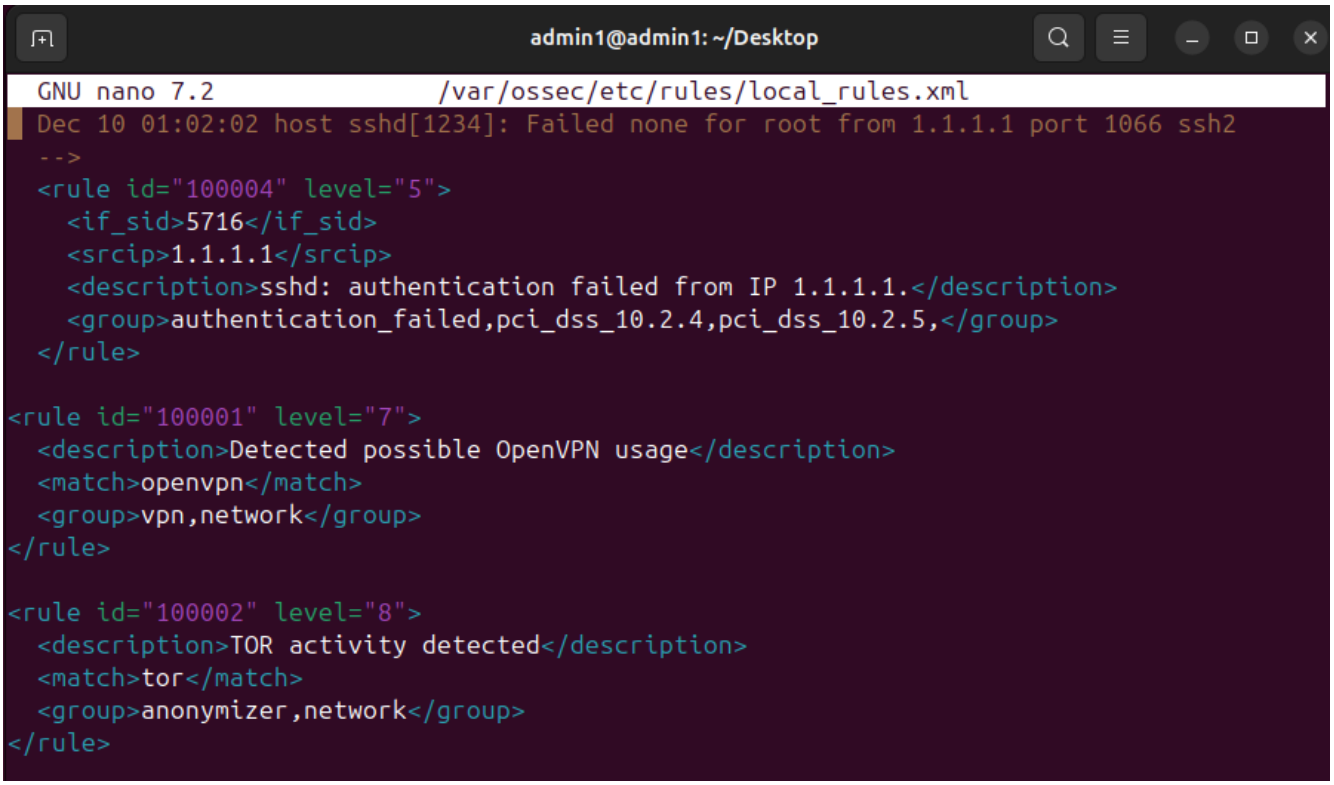
Для того, щоб Wazuh міг виявити подібну активність, до local_rules.xml було додано правило рисунок 3.13. Після додавання правила файл було збережено і перезапущено менеджер подій за допомогою sudo systemctl restart wazuh-manager

```
 GNU nano 7.2          /var/ossec/etc/rules/local_rules.xml
 Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066
 -->
 <rule id="100004" level="5">
   <if_sid>5716</if_sid>
   <srcip>1.1.1.1</srcip>
   <description>sshd: authentication failed from IP 1.1.1.1.</description>
   <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
 </rule>

<rule id="100001" level="7">
 <description>Detected possible OpenVPN usage</description>
 <match>openvpn</match>
 <group>vpn,network</group>
</rule>

<rule id="100002" level="8">
```

Рисунок 3.13 Додане правило для OpenVPN

Наступне правило було присвячене виявленню активності, пов'язаної з використанням TOR-мережі [37]. TOR, або The Onion Router, є анонімізаційною мережею, що забезпечує високий рівень конфіденційності, водночас значно

ускладнюючи завдання адміністратора системи щодо контролю за трафіком. У контексті корпоративної мережі така активність розцінюється як потенційно небезпечна. Для цього правила також використано ключове слово — tor, а рівень критичності підвищено до 8, що свідчить про пріоритетність реагування на подібні інциденти. До local_rules.xml було додано правило рисунок 3.14




```
<rule id="100004" level="5">
  <if_sid>5716</if_sid>
  <srcip>1.1.1.1</srcip>
  <description>sshd: authentication failed from IP 1.1.1.1.</description>
  <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>

<rule id="100001" level="7">
  <description>Detected possible OpenVPN usage</description>
  <match>openvpn</match>
  <group>vpn,network</group>
</rule>

<rule id="100002" level="8">
  <description>TOR activity detected</description>
  <match>tor</match>
  <group>anonymizer,network</group>
</rule>
```

Рисунок 3.14 Додане правило для TOR-мережі

Третє правило охоплює використання проксі-серверів, які часто застосовуються як менш очевидний, але не менш ефективний спосіб обійти обмеження. У даному випадку — ключове слово proxy, яке дозволяє виявляти не лише конкретні процеси, але й конфігураційні файли або частини логів, де згадується налаштування або використання проксі. Для цього правила встановлено рівень критичності 6, що відповідає середньому ступеню загрози рисунок3.14.

```
<rule id="100001" level="7">
  <description>Detected possible OpenVPN usage</description>
  <match>openvpn</match>
  <group>vpn,network</group>
</rule>

<rule id="100002" level="8">
  <description>TOR activity detected</description>
  <match>tor</match>
  <group>anonymizer,network</group>
</rule>

<rule id="100003" level="6">
  <description>Detected possible proxy usage</description>
  <match>proxy</match>
  <group>proxy,network</group>
```

Рисунок 3.15 Додане правило для Proxi

Після збереження змін у конфігураційному файлі було виконано перезапуск служби менеджера Wazuh для застосування нових правил:sudo systemctl restart wazuh-managerУ ході перевірки працездатності правил було змодельовано кілька тестових сценаріїв: запуск OpenVPN, відкриття TOR-браузера та використання утиліти proxychains. У результаті цих дій система автоматично створила відповідні події, які були зафіксовані у веб-інтерфейсі Wazuh Dashboard в розділі Security Events. Для зручності фільтрації спрацювань було використано ключовий запит rule.description: *VPN* OR *TOR* OR *proxy*Події були коректно оброблені, і кожне правило спрацювало відповідно до свого призначення. Таким чином, система успішно виконує моніторинг і фіксацію спроб використання механізмів обходу мережевого контролю. Це дозволяє підвищити загальний рівень кібербезпеки в організації, а також забезпечує основу для створення системи сповіщень або автоматичних відповідей на подібні інциденти в майбутньому.

Застосовані правила є універсальними, легко адаптуються під нові умови або розширення системи безпеки, що робить запропоноване рішення гнучким і ефективним. У наступному підрозділі буде розглянуто, як саме виглядають

результати роботи налаштованої системи та як їх аналізувати з точки зору адміністратора безпеки.

3.3 Опис роботи системи

Після налаштування системи правил у Wazuh, згідно з визначеними критеріями безпеки, було виконано тестування її роботи з метою перевірки, як система реагує на реальні події, що відповідають умовам виявлення порушень. Для цього було змодельовано декілька типових сценаріїв, які імітують поведінку користувача, що намагається обійти обмеження доступу до заборонених інтернет-ресурсів.

Зокрема, з боку клієнтського вузла було виконано запуск OpenVPN, відкрито TOR-браузер та здійснено з'єднання через проксі-сервер із використанням утиліти proxychains. Усі ці дії спричиняли появу подій у системі, які були оброблені Wazuh відповідно до раніше налаштованих локальних правил. Це продемонструвало коректність функціонування створених сигнатур та ефективність системи у виявленні порушень безпеки.

Веб-інтерфейс Wazuh Dashboard надає можливість візуалізації усіх зафіксованих подій в логах системи підключеного агента. Для цього було здійснено вхід до панелі адміністрування, де через розділ Security Events було застосовано фільтрацію результатів за допомогою запиту:

- rule.description: *VPN* OR *TOR* OR *proxy*

У результаті система вивела список спрацювань, де кожна подія містила детальну інформацію: опис події, ідентифікатор правила, рівень загрози, назву агента (тобто хоста, де було зафіксовано подію), а також мітку часу, що дозволяє точно ідентифікувати момент порушення [39].

Наприклад, при запуску OpenVPN на клієнтській машині з'явилась подія з описом "Detected possible OpenVPN usage", що відповідає правилу з

ідентифікатором 100001. У структурі події зазначено, що ключове слово openvpn було виявлено у системному журналі агента, а рівень загрози системою був визначений як 7. Аналогічно, при запуску TOR-браузера було зафіксовано спрацювання правила з ідентифікатором 100002, що підтверджує правильну роботу сигнатури на ключове слово tor.

Проксі-активність, змодельована за допомогою proxychains, також була виявлена та зафіксована системою. Подія містила відповідний опис “Detected possible proxy usage”, що дозволило швидко ідентифікувати інцидент. Оскільки всі події також потрапляють до історії журналів подій та можуть бути експортовані або передані до зовнішніх систем (наприклад, SIEM-платформ), це відкриває можливості для масштабного моніторингу, аналітики та автоматизації реагування.

Таким чином, налаштована система Wazuh успішно виконує свої функції в частині моніторингу, виявлення та реєстрації критичних подій, пов’язаних із використанням анонімізаторів та сервісів обходу фільтрації трафіку. Завдяки налаштованим правилам події ідентифікуються точно, оперативно потрапляють до інтерфейсу адміністратора, та можуть слугувати основою для подальших дій — зокрема сповіщення, блокування або ведення статистики порушень у динаміці.

3.4 Тестування системи

З метою перевірки ефективності реалізованої системи виявлення несанкціонованого доступу до заборонених ресурсів було проведено тестування, в межах якого оцінювалась здатність Wazuh фіксувати порушення встановлених політик безпеки. Особливу увагу зосереджено на виявленні активності, пов’язаної з використанням VPN-клієнтів, анонімізаторів TOR та проксі-серверів — найбільш розповсюджених засобів обходу корпоративних обмежень [40].

У результаті моніторингу системою Wazuh було зафіксовано події, що вказують на використання сервісу VPN. Зокрема, у розділі Security Events інтерфейсу Wazuh Dashboard з'явилась подія з описом "Detected possible OpenVPN usage". Подія містила деталі щодо часу, агента, рівня небезпеки та класифікації інциденту. Це свідчить про те, що система змогла виявити факт використання VPN-з'єднання відповідно до встановлених правил.Ця подія ілюструє здатність системи виявити запуск VPN-з'єднання, що підтверджується на рисунку 3.14.

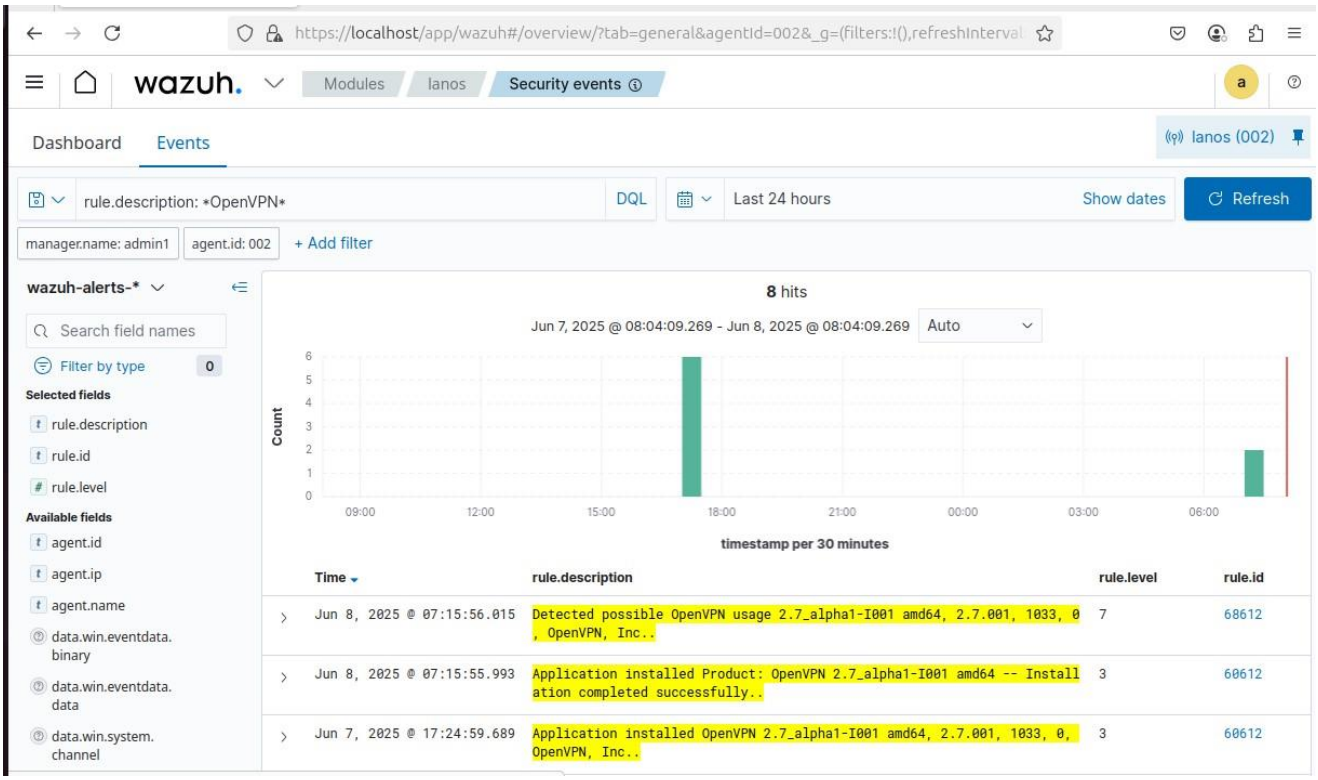


Рисунок 3.16 Виявлення використання OpenVPN у Wazuh Dashboard

Крім моніторингу стандартних мережевих підключень, система безпеки також успішно зафіксувала ознаки використання мережі TOR. На панелі моніторингу (Dashboard) системи Wazuh чітко відображено подію з описом "TOR activity detected". Завдяки налаштованому користувацькому правилу, ця подія була класифікована як інцидент високого рівня загрози, отримавши рівень 8. Це підкреслює її потенційну небезпеку та потребу в негайній увазі з боку фахівців з безпеки.

Виявлення таких спроб використання анонімізаторів, як TOR, є критично важливим для забезпечення прозорості та контролю над мережевим трафіком у корпоративному середовищі. Це дозволяє ідентифікувати потенційні загрози, такі як обхід політик безпеки, витік конфіденційної інформації або зв'язок зі шкідливими ресурсами. Своєчасне виявлення та реагування на подібні інциденти є ключовим компонентом ефективної стратегії кібербезпеки організації4.

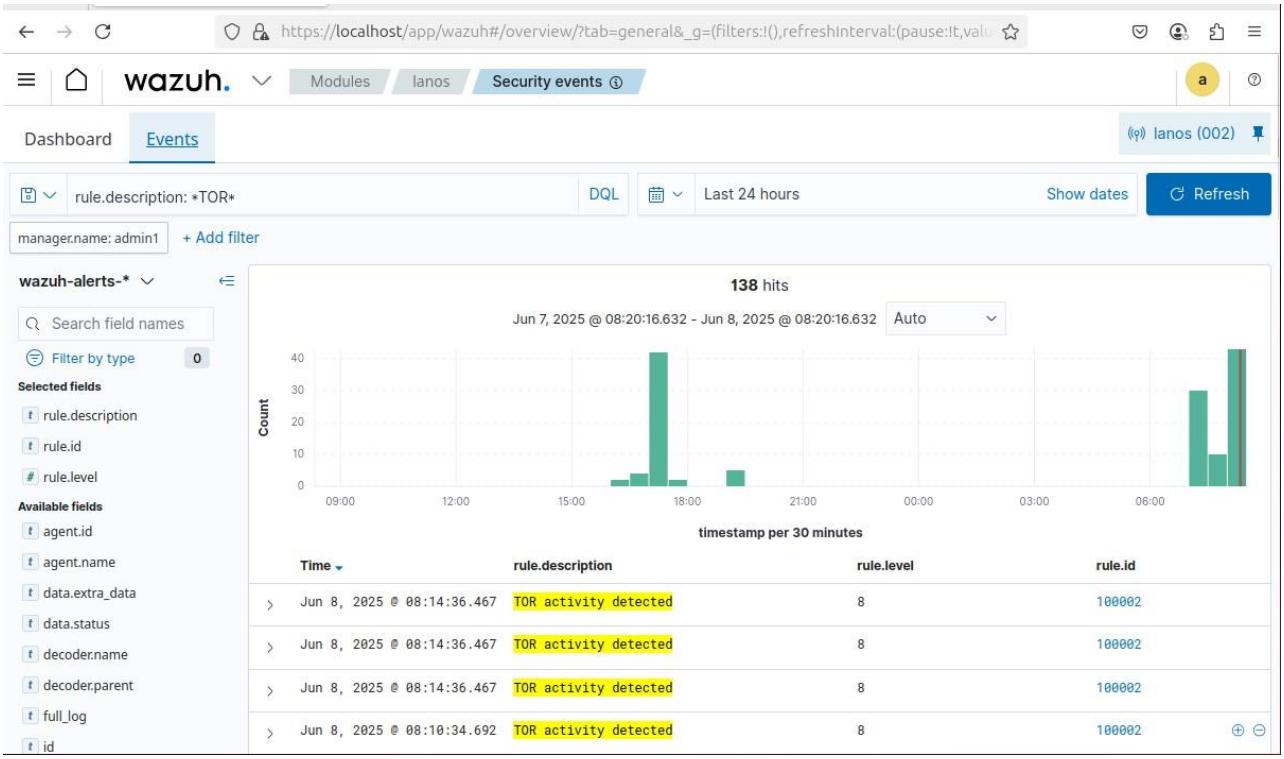


Рисунок 3.17 Виявлення використання TOR у Wazuh Dashboard

Крім активного моніторингу мережі та виявлення прихованих підключень, система безпеки продемонструвала свою ефективність, успішно ідентифікувавши спробу використання проксі-сервера. Це виявлення є значущим, оскільки застосування проксі-сервісів, які перенаправляють інтернет-трафік через проміжний сервер, також розцінюється як порушення встановлених корпоративних правил доступу та політик безпеки. Такі дії можуть мати на меті приховати реальне джерело трафіку, обійти корпоративні файрволи, фільтри контенту або отримати доступ до заборонених ресурсів.

На панелі керування Wazuh, у розділі подій безпеки (Security Events), була чітко відображена подія з описом “Detected possible proxy usage”. Цей алерт супроводжувався відповідними технічними деталями, що дозволяють адміністраторам безпеки швидко ідентифікувати джерело та контекст події. Завдяки правильно налаштованим правилам (зокрема, правилу з ID 100003 та рівнем загрози 6), система автоматично класифікувала цю активність.

Таке виявлення є яскравим свідченням того, що навіть найпростіші спроби перенаправлення трафіку через проксі-сервери не залишаються поза увагою системи моніторингу. Wazuh демонструє здатність виявляти такі дії на рівні операційної системи, відстежуючи виконання команд та інші системні події. Це забезпечує додатковий рівень прозорості та контролю, дозволяючи оперативно реагувати на будь-які спроби обходу встановлених політик безпеки та підтримувати цілісність корпоративної мережі. Здатність системи фіксувати подібні аномалії на ранніх етапах є критично важливою для мінімізації потенційних ризиків та захисту конфіденційних даних.

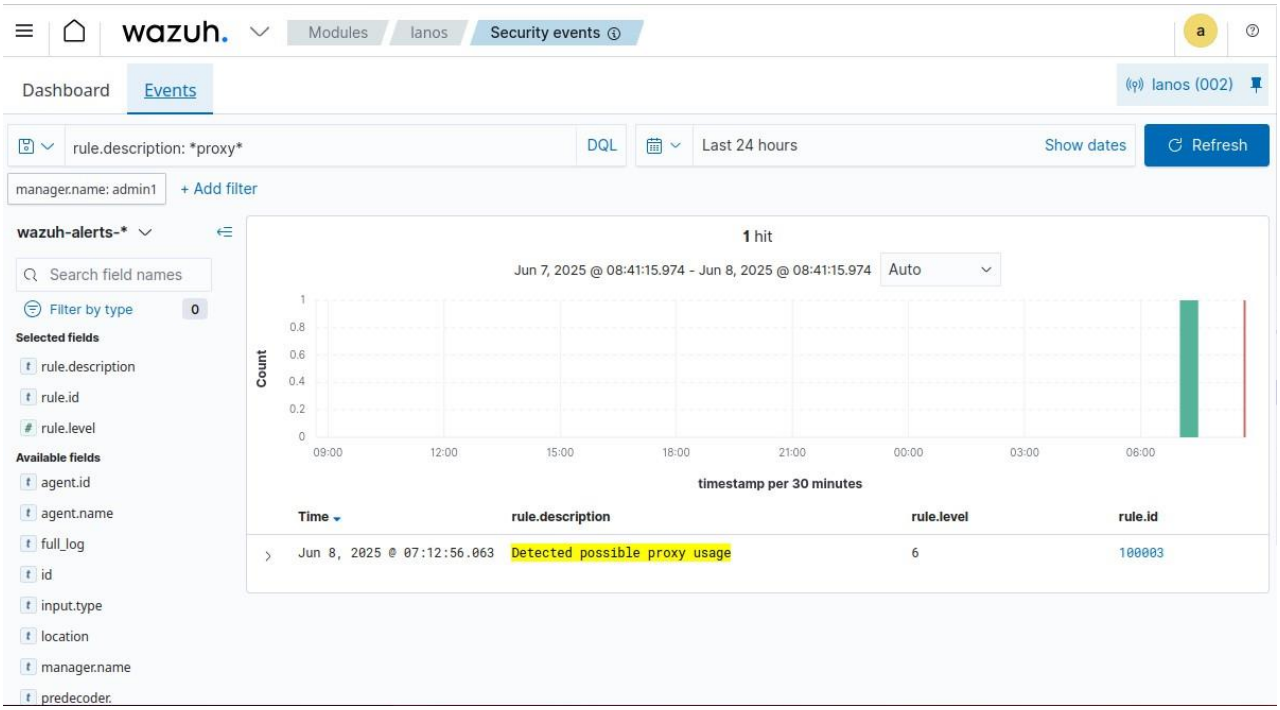


Рисунок 3.18 Виявлення використання proxy Wazuh Dashboard

Усі виявлені події також були доступні для аналізу через пошуковий інтерфейс Dashboard. Для фільтрації використовувалась текстова умова rule.description: *VPN* OR *TOR* OR *proxy*, яка дозволяє зручно переглядати інциденти за категоріями. Завдяки чіткому групуванню правил за типом загрози адміністратор має змогу оперативно ідентифікувати характер порушення, його джерело, а також ініціювати подальші заходи — зокрема обмеження доступу, сповіщення чи додатковий аудит.

Загалом результати тестування підтвердили, що реалізована система працює коректно: усі типи небажаної активності було виявлено, зафіксовано й подано в інтерфейсі моніторингу без затримок. Це демонструє, що створені правила виявлення є достатньо чутливими, а архітектура Wazuh дозволяє реалізувати ефективний механізм виявлення порушень у реальному часі.

3.5 Висновок

У результаті реалізації третього розділу дипломної роботи було проведено повний цикл практичної роботи з впровадження, налаштування та тестування системи виявлення несанкціонованого доступу до заборонених ресурсів на основі SIEM-рішення Wazuh. Цей етап дозволив перевірити на практиці доцільність і функціональність обраного підходу до моніторингу та забезпечення інформаційної безпеки в межах корпоративної мережі.

Було успішно розгорнуто ключові компоненти системи: менеджер подій, індексатор, веб-інтерфейс (Wazuh Dashboard), а також агенти на клієнтських вузлах. Встановлення системи відбувалось із дотриманням офіційних технічних вимог, що забезпечило стабільну роботу усіх сервісів у тестовому середовищі. Після розгортання особливу увагу було приділено налаштуванню локальних правил безпеки, що дозволяють фіксувати спроби обійти мережеві обмеження за допомогою VPN, TOR та проксі-серверів.

Власноруч створені правила у файлі local_rules.xml показали високу ефективність у виявленні ключових ознак несанкціонованої активності. Кожне правило було чітко структуроване, прив'язане до унікального ідентифікатора та класифіковане за групами. Система показала здатність оперативно обробляти події, формувати відповідні записи та відображати їх у веб-інтерфейсі адміністратора з усією необхідною інформацією — датою, джерелом, рівнем загрози та текстовим описом [41].

Тестування системи на базі контрольованих сценаріїв дозволило перевірити як саму логіку виявлення, так і стабільність усієї архітектури Wazuh. Усі події були успішно зафіксовані та проаналізовані. Використання ключових фраз у правилах забезпечило достатню чутливість без надмірної генерації хибнопозитивних спрацювань. У розділі Security Events інтерфейсу Wazuh події були автоматично класифіковані відповідно до закладених сигнатур, що підтвердило практичну ефективність реалізованого рішення.т

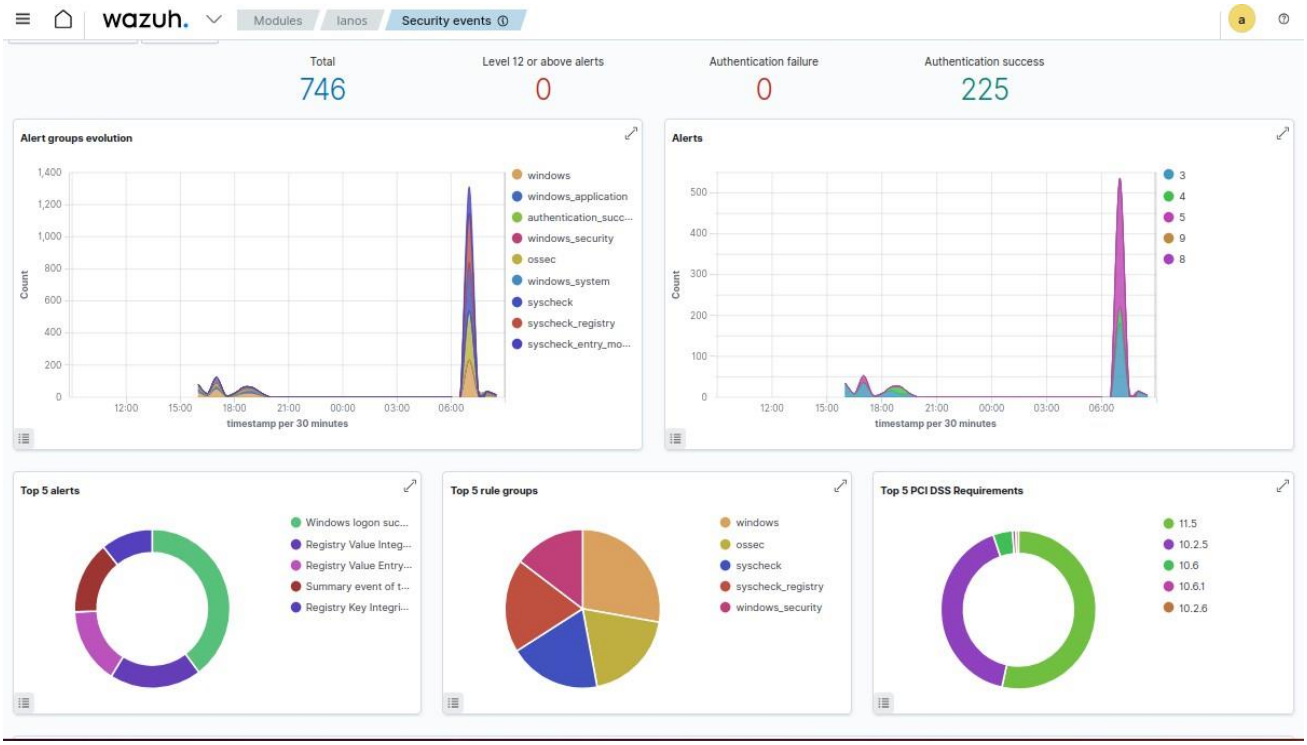


Рисунок 3.19 Загальний вигляд системи після тестування інцидентів

Окремо варто відзначити зручність та інтуїтивність роботи з інтерфейсом Wazuh. Можливість швидкого фільтрування подій за ключовими словами, групами або рівнем загрози значно спрощує аналітичну роботу адміністратора. Це особливо важливо у випадках, коли обсяг подій великий, а оперативність прийняття рішень є критичною. Структура подій у вигляді розгорнутих JSON-об’єктів дозволяє отримати максимум технічної інформації для подальшого розслідування.

Загальний результат практичного етапу підтвердив, що система Wazuh є дієвим інструментом для моніторингу і виявлення несанкціонованої активності в межах локальної мережі. Її відкритий код, гнучкість налаштування, підтримка візуалізації та здатність до масштабування роблять цю систему придатною як для невеликих організацій, так і для великих корпоративних інфраструктур. Виявлені події дозволяють не лише реагувати на факти порушень, а й формувати аналітичні звіти, створювати політики безпеки та виявляти нові вектори загроз.

Таким чином, результати третього розділу свідчать про повну реалізацію поставлених цілей: налаштування Wazuh, створення системи виявлення інцидентів, перевірка її працездатності та демонстрація здатності до адаптації під специфіку корпоративного середовища. Отриманий результат може бути основою для впровадження автоматизованих механізмів реагування, інтеграції з іншими системами та подальшого розвитку напрямку кіберзахисту.

ВИСНОВКИ

Захист інформаційних ресурсів у сучасних корпоративних мережах потребує не лише обмеження доступу, а й постійного моніторингу активності користувачів з метою виявлення порушень. У сучасних умовах, коли більшість загроз здійснюються не лише ззовні, а й зсередини мережі, особливого значення набуває виявлення спроб обійти встановлені політики безпеки. Це стосується, зокрема, використання VPN-сервісів, TOR-мереж і проксі-рішень для несанкціонованого доступу до заборонених або контрольованих інтернет-ресурсів.

Побудова ефективної системи виявлення таких порушень потребує комплексного підходу: від вибору технічного рішення до глибокої інтеграції з внутрішніми процесами контролю. Практична реалізація на базі відкритої системи Wazuh довела, що з використанням гнучкого й масштабованого інструментарію можна створити повноцінну систему виявлення інцидентів безпеки з можливістю налаштування під конкретні потреби організації. Власноруч створені правила виявлення активності, пов’язаної з анонімізаційними сервісами, дозволили продемонструвати, що навіть у рамках обмежених ресурсів можливо забезпечити високий рівень контролю над внутрішнім трафіком.

Інтеграція системи моніторингу з візуальним інтерфейсом адміністрування дозволила спростити процес аналізу, класифікації та фільтрації подій. Отримані результати свідчать про точність виявлення, стабільність роботи та простоту масштабування реалізованого рішення. Важливо також відзначити, що впровадження подібного підходу не вимагає дорогого ліцензованого програмного забезпечення — вся система може функціонувати на основі безкоштовних і відкритих компонентів, зберігаючи при цьому високу ефективність.

Проведене тестування підтвердило практичну здатність системи фіксувати критичні події, пов’язані з порушенням мережевої політики, та оперативно передавати їх для аналізу. Події, що стосуються використання VPN, TOR і проксі, були виявлені та класифіковані відповідно до рівня загрози, що створює передумови для побудови не лише пасивної, а й активної моделі реагування на інциденти.

У підсумку можна зазначити, що побудована система має високий потенціал для практичного використання в організаціях різного масштабу. Вона забезпечує гнучкість, адаптивність, можливість подальшого розширення та інтеграції з зовнішніми аналітичними платформами, а також є ефективним інструментом у забезпеченні контролю, звітності та попередження інцидентів інформаційної безпеки. Такий підхід сприяє формуванню стійкої та керованої мережевої інфраструктури, де кожна спроба порушення фіксується, аналізується та не залишається поза увагою.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Все про VPN: сервери, VPN-підключення, шифрування, обхід блокувань. Vpnunlimited. URL:https://www.vpnunlimited.com/ua/help/more-about-vpn(дата звернення: 06.05.2025).

2. Проксі для обходу блокувань – принципи та важливість. Mediacom. URL: https://mediacom.com.ua/proksi-dlya-obxodu-blokuvan-yak-tse-pratsyue-ta-chomu-tse-vazhlivo/ (дата звернення: 08.05.2025).

3. Чим відрізняється проксі-сервер від VPN?. URL: https://nordvpn.com/uk/blog/proksi-proty-vpn/. (дата звернення: 01.06.2025).

4. Що таке Tor і як він забезпечує анонімність?. URL: https://foxminded.ua/shcho-take-tor/ (дата звернення: 03.06.2025).

5. Alternative networks – privacy guides. URL: https://www.privacyguides.org/en/alternative-networks/ (дата звернення: 04.06.2025).

6. Anonymizing networks: tor vs I2P | infosec institute. URL: https://www.infosecinstitute.com/resources/general-security/anonymizing-networks-tor-vs-i2p/ (дата звернення: 04.06.2025).

7. Тунелі SSH: налаштування та практичні приклади використання. URL: https://alexhost.com/uk/faq/tuneli-ssh-nalashtuvannya-ta-praktychni-pryklady-vykorystannya (дата звернення: 04.06.2025).

8. Що таке Tunneling - Терміни та визначення в кібербезпеці. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/tunneling?utm_source=chatgpt.com (дата звернення: 04.06.2025).

9. Що таке HTTPS і навіщо він потрібен. URL: https://frontend.lviv.ua/shho-take-https-i-navishho-vin-potriben10 (дата звернення: 04.06.2025).

10. TCP/IP. URL: https://oxorona.com/tcp-ip (дата звернення: 04.06.2025).

11. Що таке ips/ids і де застосовується. URL: https://www.hostzealot.com.ua//blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya (дата звернення: 04.06.2025).

12. Системи SIEM: Що це таке, як працюють і чому вони важливі?. URL: https://cyberset.com.ua/network/attacks-vs-defense/siem-systems/ (дата звернення: 05.06.2025).

13. Аналіз поведінки користувачів та суб'єктів (UEBA). URL: https://iitd.ua/analiz-povedinki-koristuvachiv-ta-subyektiv-ueba/ (дата звернення: 05.06.2025).

14. Глибока перевірка пакетів (DPI). URL: https://www.techtarget.com/searchnetworking/definition/deep-packet-inspection-DPI (дата звернення: 05.06.2025).

15. Аналіз протоколу DNS over HTTPS. URL:https://conf.ztu.edu.ua/wp-content/uploads/2020/05/88-1.pdf(дата звернення: 05.06.2025).

16. Roesch, M. (1999). *Snort – Lightweight Intrusion Detection for Networks. URL: https://www.snort.org/](https://www.snort.org/ (дата звернення: 05.06.2025).

17. Wazuh Documentation. Open source SIEM and XDR. URL: https://documentation.wazuh.com (дата звернення: 05.06.2025).

18. Palo Alto Networks. Understanding Deep Packet Inspection. URL: https://www.paloaltonetworks.com/resources (дата звернення: 05.06.2025).

19. Gartner. UEBA Market Guide 2023. URL: https://www.gartner.com/en (дата звернення: 05.06.2025).

20. Wazuh Documentation. SIEM & XDR Platform. URL: https://documentation.wazuh.com (дата звернення: 05.06.2025).

21. Suricata IDS. Open source threat detection engine. URL: https://suricata.io (дата звернення: 05.06.2025).

22. SANS Institute. Detecting DNS Tunneling. URL: https://www.sans.org/white-papers/367 (дата звернення: 06.06.2025).

23. Splunk Documentation. Security Information and Event Management. URL: https://www.splunk.com (дата звернення: 06.06.2025).

24. Tor Project – Technical Overview. URL: https://www.torproject.org (дата звернення: 06.06.2025).

25. Віртуальні тунелі. URL: https://openarchive.nure.ua/server/api/core/bitstreams/fa7d0cb3-011f-45d9-b304-9f97eeafee97/content (дата звернення: 06.06.2025).

26. Tor upgrades to make anonymous publishing safer. URL: https://theconversation.com/tor-upgrades-to-make-anonymous-publishing-safer-73641 (дата звернення: 06.06.2025).

27. Архітектура Wazuh. URL: https://documentation.wazuh.com/current/getting-started/architecture.html (дата звернення: 06.06.2025).

28. Wazuh Cluster Overview. URL: https://documentation.wazuh.com/current/user-manual/wazuh-server-cluster/architecture-overview.html (дата звернення: 06.06.2025).

29. Gartner – SIEM and Threat Detection Platforms Market Guide. URL: https://www.gartner.com (дата звернення: 06.06.2025).

30. Suricata IDS. URL: https://suricata.io (дата звернення: 06.06.2025).

31. Ubuntu 22.04.5 LTS (Jammy Jellyfish). URL: https://releases.ubuntu.com/jammy/ (date of access: 06.06.2025)

32. Virtual box download. URL: https://www.virtualbox.org/ дата звернення: 06.06.2025).

33. Офіційна документація Wazuh: тестування декодерів і правил. URL: https://documentation.wazuh.com/current/user-manual/ruleset/ (дата звернення: 06.06.2025).

34. Реалізація SIEM рішення на основі Wazuh із прикладом Active Response. URL: https://www.researchgate.net/publication/378672896 (дата звернення: 07.06.2025).

35. Стаття про інтеграцію Wazuh із TheHive і threat intelligence. URL: https://thesai.org/Downloads/Volume15No9/Paper_23-SIEM_Threat_Intelligence_Protecting_Applications.pdf (дата звернення: 07.06.2025).

36. Дослідження ефективності Wazuh в хмарних середовищах. URL: https://americaspg.com/article/pdf/ (дата звернення: 07.06.2025).

37. Блог Wazuh: моніторинг мережевих пристроїв (MikroTik). URL: https://thesai.org/Downloads/Volume15No9/Paper_23-SIEM_Threat_Intelligence_Protecting_Applications.pdf (дата звернення: 07.06.2025).

38. Кейс стаді Університету Чичестера: швидка та проста налаштування Wazuh. URL: https://wazuh.com/uploads/2024/07/case-study-university-of-chichester.pdf (дата звернення: 07.06.2025).

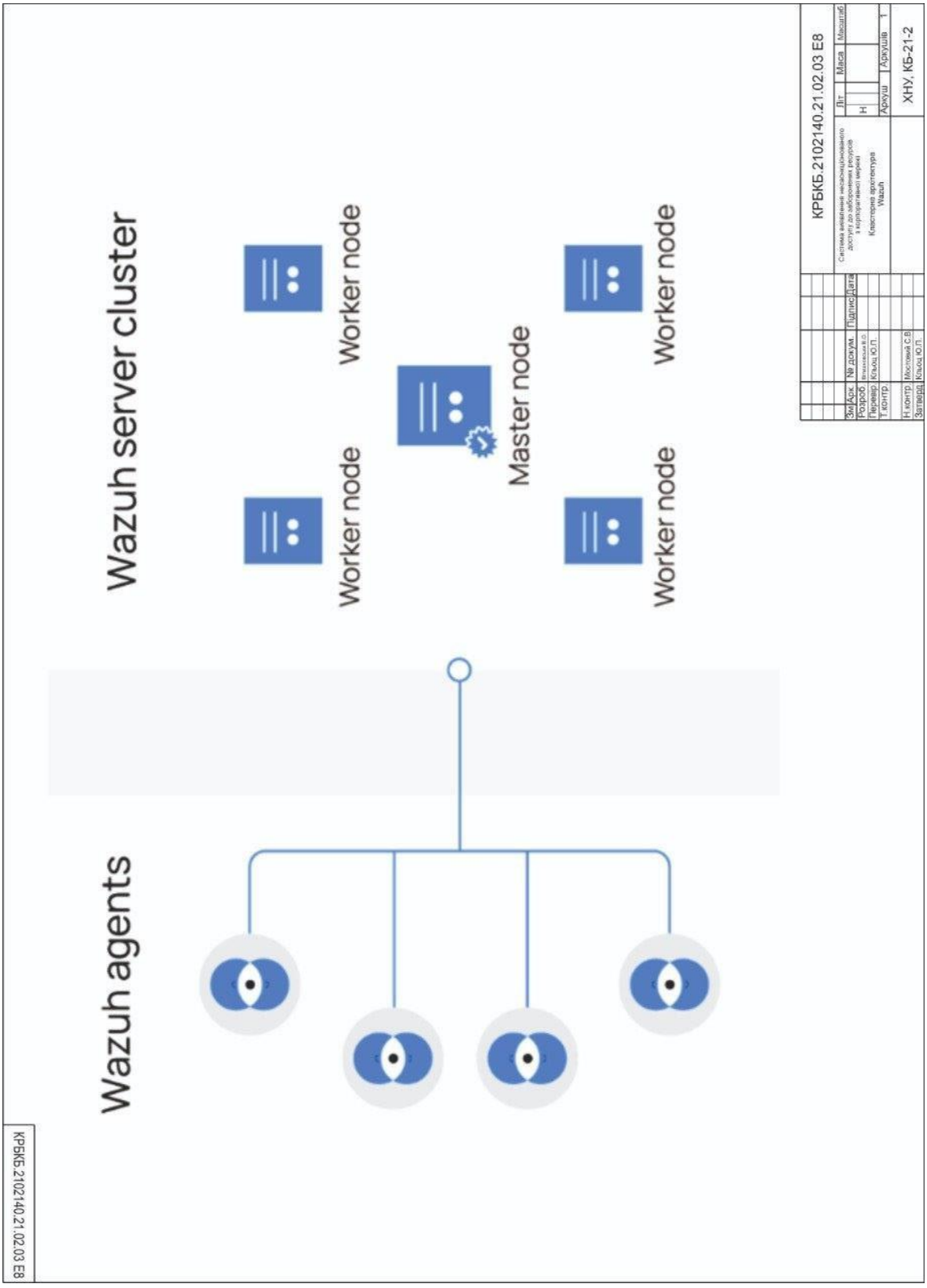
39. Блог Wazuh: відстеження підключень OpenVPN із GeoIP. URL: https://wazuh.com/uploads/2024/07/case-study-university-of-chichester.pdf (дата звернення: 07.06.2025).

40. Порівняльне дослідження SIEM рішень: Wazuh vs. інші платформи. URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone (дата звернення: 08.06.2025).

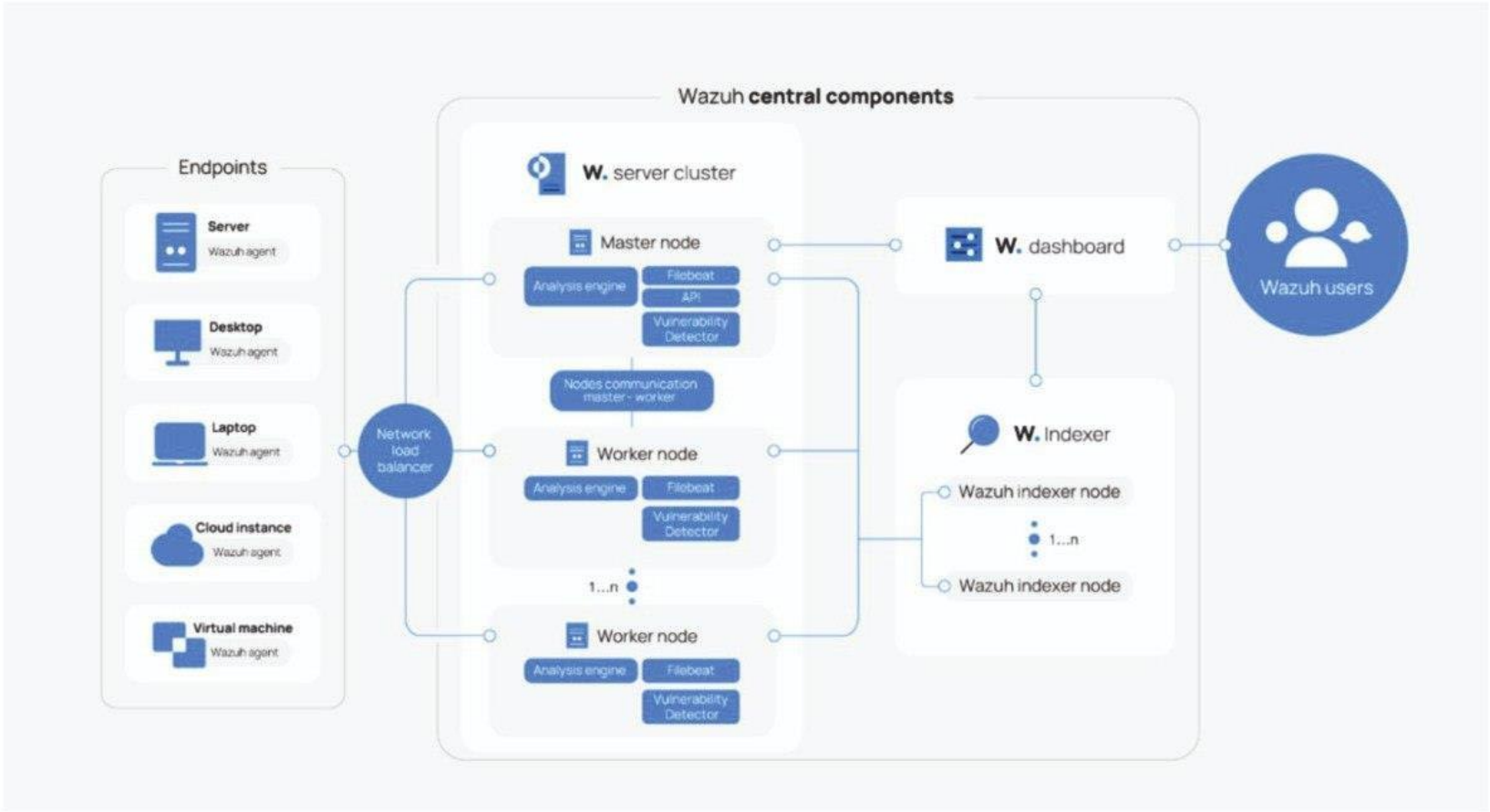
41. Груповий форум Wazuh: тестування правил через wazuh-logtest (Google Groups). URL: https://groups.google.com/g/wazuh/c/EmiOirZp4L8 (дата звернення: 08.06.2025).

Додаток А

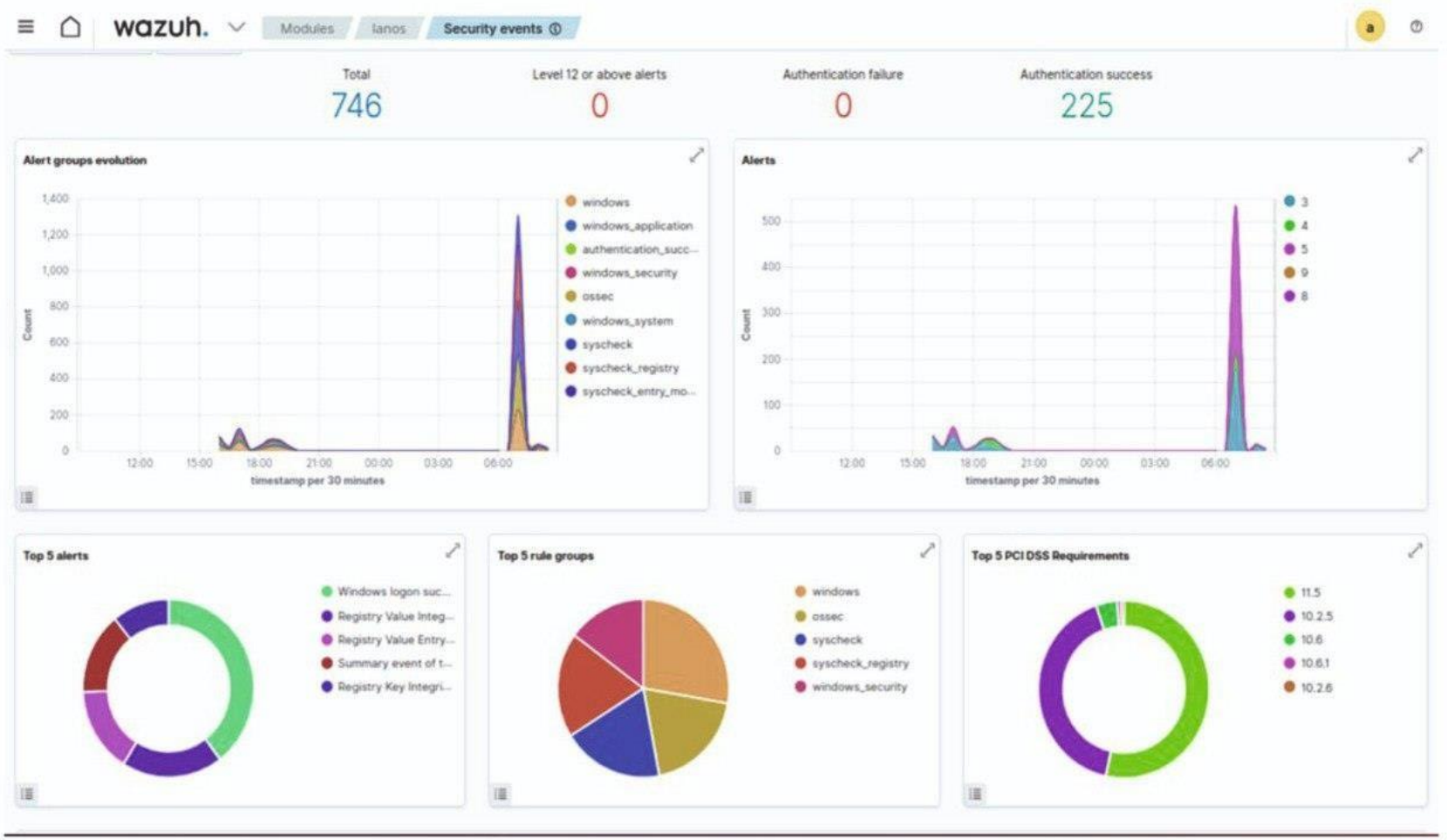
Копії графічної частини



КРБКБ.2102140.21.02.03 Е8



					КРБКБ.2102140.21.02.03 Е8			
Зм.	Арк.	№ докум.	Підпис	Дата	Система виявлення несанкціонованого доступу до заборонених ресурсів з корпоративної мережі	Літ.	Маса	Масштаб
Розроб.		Вітковський В.О.						
Перевір.		Кльоц Ю.П.			Діаграма архітектури Wazuh			
Т.контр.						Аркуш	Аркушів	1
Н.контр.		Мостовий С.В.				ХНУ, КБ-21-2		
Затверд.		Кльоц Ю.П.						



					КРБКБ.2102140.21.02.03 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Система виявлення несанкціонованого доступу до заборонених ресурсів з корпоративної мережі	Літ	Маса	Масштаб
Розроб.		Вітковський В.О.				Н		
Перевір.		Кільоц Ю.П.			Загальний вигляд системи після тестування інцидентів			
Т.контр.						Аркуш	Аркушів	1
Н.контр.		Мостовий С.В.				ХНУ, КБ-21-2		
Затверд.		Кільоц Ю.П.						

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Вітмановського Вадима Олеговича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-21-2

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

08.06.25
дата

підпис

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 12%**

	Document		Sum coincidence on the DB	
ID: 244615 Title: Система виявлення несанкціонованого доступу до заборонених ресурсів з корпоративної мережі Added in a DB: 2025-06-10 Authors: Вітмановський Вадим Олегович Heads: Кльоц Ю.П. Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	66997	461	590 (1%)	7 (2%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Вітмановський Вадим Олегович

Співавтор:

Назва: Система виявлення несанкціонованого доступу до заборонених ресурсів з корпоративної мережі

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:1.4%

Коефіцієнт подібності 2:0.3%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-10 16:00:22.0

Після аналізу Звіту подібності констатую наступне:

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

11.06.2025р.

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система виявлення несанкціонованого доступу до заборонених ресурсів з корпоративної мережі

Автор: Вітмановський Вадим Олегович

Спеціальність: 125 – Кібербезпека

Освітня програма: Кібербезпека

Науковий керівник: Юрій КЛЬОЦ, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 98,6%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 99%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Юрій КЛЬОЦ

Гарант ОП _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студентка Вітмановський Вадим Олегович

Тема Система виявлення несанкціонованого доступу до заборонених ресурсів з корпоративної мереж

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки 60.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі, відповідно до поставленого завдання, розглянуто питання виявлення несанкціонованого доступу до заборонених ресурсів у межах корпоративних мереж. Проведено дослідження сучасних інструментів інформаційної безпеки, зокрема систем виявлення атак та аномальної активності: SIEM, IDS/IPS, DPI та UEBA. Обґрунтовано вибір SIEM-системи Wazuh як найбільш придатного рішення за критеріями ефективності. Реалізовано її розгортання та налаштування в умовах імітації потенційних загроз, а також здійснено оцінку можливостей системи щодо виявлення аномальної активності користувачів. Запропоновані рішення можуть бути адаптовані до потреб фахівців з кібербезпеки та адміністраторів корпоративних мереж для підвищення рівня захищеності інформаційної інфраструктури.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі повністю виконано поставлене завдання як у теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У розділі 1 розглянуто актуальні виклики, пов'язані з виявленням несанкціонованого доступу до заборонених ресурсів у корпоративних мережах. Проаналізовано сучасні загрози, пов'язані з використанням VPN, TOR, проксі-серверів, а також підкреслено зростання внутрішніх ризиків, що зумовлюють необхідність глибшого моніторингу користувацької активності.

У розділі 2 досліджено функціональні можливості провідних засобів контролю безпеки, таких як SIEM, IDS/IPS, DPI та UEBA. На основі порівняльного аналізу обґрунтовано вибір SIEM-системи Wazuh як оптимального безкоштовного рішення. Детально описано процес її налаштування, створення користувацьких правил для виявлення аномальної активності, пов'язаної з анонімізаційними сервісами. Реалізовано інтеграцію системи з візуальним інтерфейсом адміністрування, що спростило класифікацію та аналіз подій.

У розділі 3 здійснено імітацію загроз і тестування працездатності впровадженої системи в умовах обмежених ресурсів. Продемонстровано здатність Wazuh ефективно фіксувати порушення політик доступу, зокрема спроби обходу заборон через VPN і TOR, а також передавати дані для оперативного реагування. Робота підтверджує, що навіть за мінімальних витрат можливо реалізувати масштабовану, адаптивну систему безпеки, придатну для використання в реальних корпоративних умовах.

4. Позитивні сторони роботи Кваліфікаційна робота демонструє достатній рівень розуміння актуальних викликів у сфері інформаційної безпеки корпоративних мереж, зокрема в контексті виявлення несанкціонованого доступу до заборонених ресурсів через VPN, TOR і проксі. Автором проведено глибокий огляд сучасних рішень, зокрема SIEM, IDS/IPS, DPI, UEBA, із фокусом на їхню роль у виявленні аномальної

активності. Практична частина відзначається вдалою реалізацією SIEM-системи Wazuh, яка налаштована під специфіку завдань моніторингу та виявлення загроз у внутрішньому трафіку. Створення власних правил виявлення та інтеграція з інтерфейсом візуального адміністрування демонструють навички практичного проєктування гнучких систем захисту. Робота має прикладне значення для фахівців з кібербезпеки, системних адміністраторів та розробників захисних рішень

5. Негативні сторони роботи У роботі недостатньо детально розкрито технічні особливості інфраструктури, в якій впроваджувалась SIEM-система, зокрема бракує структурованого опису мережевого середовища, що ускладнює оцінку масштабованості та сумісності запропонованого рішення з іншими типами мереж. Також обмежено увагу приділено порівнянню альтернативних SIEM-рішень, вибір Wazuh обґрунтовано на загальному рівні без глибшого аналізу переваг і недоліків у контексті конкретного сценарію використання. Крім того, хоча в роботі продемонстровано налаштування користувацьких правил, їх ефективність оцінюється переважно описово, без докладної кількісної аналітики

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота справляє позитивне загальне враження. Вона демонструє системний підхід до вирішення актуального завдання виявлення несанкціонованого доступу в корпоративних мережах та застосування сучасних рішень у сфері інформаційної безпеки. Матеріал роботи викладено логічно, послідовно та з урахуванням реальних викликів, пов'язаних із використанням VPN, TOR і проксі-сервісів для обходу обмежень. Практична частина реалізована на основі відкритої SIEM-платформи Wazuh, що дозволяє демонструвати не лише технічну обґрунтованість рішення, а й його доступність для широкого кола організацій. Водночас деякі аспекти потребують глибшої деталізації, опис об'єкта захисту та порівняльний аналіз альтернатив. Попри це, робота має прикладну цінність і може бути використана як основа для впровадження рішень моніторингу в реальних умовах. Загалом кваліфікаційна робота відповідає вимогам до бакалаврського рівня і заслуговує позитивної оцінки.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні сторони кваліфікаційної роботи, а також негативні сторони, які не зменшують практичну цінність отриманих результатів і загальну якість роботи, рекомендованою оцінкою є «задовільно»

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Нічепорук Андрій Олександрович
кандидат технічних наук, доцент кафедри комп'ютерної інженерії та інформаційних систем

« 12 » 06 2025. (підпис)