

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА
ЗАХИСТУ
ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія виявлення та реагування на інциденти інформаційної безпеки з
використанням платформи Wazuh»

зі спеціальності

125 Кібербезпека та захист інформації

(код, найменування спеціальності)

освітньо-професійної
програми

Інформаційна та кібернетична безпека

(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання
ідей, результатів і текстів інших авторів мають посилання на відповідне
джерело

_____ Богдан ПЕДОСЕНКО

(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61

ПЕДОСЕНКО Богдан

(прізвище, ім'я)

Керівник

доктор філософії, ПЕДЧЕНКО Євгеній

(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент

(науковий ступінь, вчене звання, прізвище, ім'я)

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**

Кафедра Систем та технологій кібербезпеки

Ступінь вищої освіти Магістр

Спеціальність 125 Кібербезпека та захист інформації

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ

Завідувач кафедри

Систем та технологій
кібербезпеки

Галина ГАЙДУР

“___” жовтня 2025 року

**З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

ПЕДОСЕНКО Богдану Володимировичу

(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія виявлення та реагування на
інциденти інформаційної безпеки з використанням платформи Wazuh»

керівник кваліфікаційної роботи ПЕДЧЕНКО Євгеній, доктор філософії

(прізвище, ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-
комунікаційних технологій від «_____» жовтня 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 25.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи
рішення Wazuh;

наукова та технічна література, експлуатаційна документація, нормативні
документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які
потрібно розробити)

1. Аналіз проблеми виявлення та реагування на інциденти інформаційної
безпеки в корпоративних інформаційних системах.

2. Аналіз методів та засобів виявлення та реагування на інциденти

Інформаційної безпеки на базі платформи Wazuh.

3. Розроблення варіанта технології виявлення та реагування на інциденти інформаційної безпеки на базі платформи Wazuh.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми забезпечення безпечної роботи гібридних працівників організації.	01.10.2025 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	12.10.2025 р.	
3.	Аналіз методів і засобів виявлення та реагування на інциденти інформаційної безпеки на базі платформи Wazuh.	27.10.2024 р.	
4.	Розроблення варіанта технології виявлення та реагування на інциденти інформаційної безпеки на базі платформи Wazuh.	03.11.2025 р.	
5.	Розроблення рекомендацій щодо впровадження технології Wazuh у корпоративне середовище.	15.11.2025 р.	
6.	Оформлення результатів дослідження.	26.11.2025 р.	
7.	Подання роботи на плагіат. Підготовка доповіді до захисту.	25.12.2025 р.	

Здобувач вищої освіти

(підпис)

Богдан ПЕДОСЕНКО

(ім'я, прізвище)

Керівник кваліфікаційної роботи

(підпис)

Євгеній ПЕДЧЕНКО

(ім'я, прізвище)

ВІДГУК РЕЦЕНЗЕНТА на кваліфікаційну роботу

здобувача ПЕДОСЕНКА Богдана

на тему: «Технологія виявлення та реагування на інциденти інформаційної безпеки з використанням платформи Wazuh»

Актуальність: Сучасні IT-інфраструктури стикаються зі зростаючою кількістю кіберзагроз, що потребує ефективних засобів моніторингу та оперативного реагування. Поширення хмарних сервісів, віддаленої роботи та розподілених систем збільшує ризики компрометації інформаційних ресурсів. Платформа Wazuh, як сучасне open-source SIEM/XDR-рішення, забезпечує можливість централізованого контролю безпеки, аналізу подій та автоматизованого реагування. Використання даної технології сприяє підвищенню кіберстійкості організацій, що зумовлює актуальність обраної теми.

Позитивні сторони:

1. На основі проведеного аналізу в роботі чітко сформульовано проблему забезпечення виявлення та реагування на інциденти інформаційної безпеки в корпоративних інформаційних системах..
2. Детально досліджено методи та засоби виявлення й реагування на інциденти інформаційної безпеки на базі платформи Wazuh. Робота показує призначення, можливості, архітектуру Wazuh та її ключові компоненти (Manager, Agent, Indexer, Dashboard).
3. Розглянуто технологічні механізми збору, обробки, кореляції подій безпеки та інтеграції Wazuh із зовнішніми джерелами даних (фасерволи, IDS/IPS, хмарні сервіси), що демонструє комплексне розуміння функціонування системи.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У роботі бракує прикладу практичного застосування розробленої технології виявлення та реагування на інциденти на прикладі конкретної організації.
2. Механізми реагування та побудова архітектури системи могли б бути продемонстровані у вигляді повноцінного кейсу, наприклад, із моделюванням конкретних інцидентів, їх кореляцією, спрацьовуванням правил та наступним реагуванням (Active Response, SIEM Alerts)

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку “добре”, а здобувач(ка) **ПЕДОСЕНКО Богдан** – присвоєння кваліфікації магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь,
вчене звання)

(підпис)

(ім'я, прізвище)

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

**ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**

Направляється здобувач ПЕДОСЕНКО Богдан до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія виявлення та реагування на інциденти інформаційної безпеки з
використанням платформи Wazuh».
Кваліфікаційна робота і рецензія додаються.

Директор інституту

(підпис)

Євгенія ІВАНЧЕНКО
(ім'я, прізвище)

Висновок керівника кваліфікаційної роботи

Здобувач ПЕДОСЕНКО Богдан обрав тему роботи, метою якої було дослідити технологію виявлення та реагування на інциденти інформаційної безпеки та розробити рекомендації щодо її реалізації на базі платформи Wazuh. Перелік використаних джерел свідчить про вміння здобувачем працювати з науковою літературою та застосовувати отримані знання у дослідженні. Під час виконання кваліфікаційної роботи здобувач продемонстрував достатню теоретичну та практичну підготовку, уміння самостійно аналізувати інформацію та робити обґрунтовані висновки. Роботу виконував сумлінно, акуратно та вчасно.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ПЕДОСЕНКО Богдан на оцінку «добре» та присвоїти йому кваліфікацію *магістр з кібербезпеки* за освітньо-професійною програмою «Інформаційна та кібернетична безпека».

Керівник кваліфікаційної роботи

(підпис)

“ ”

Євгеній ПЕДЧЕНКО
(ім'я, прізвище)

2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач ПЕДОСЕНКО Богдан допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

(підпис)

Галина ГАЙДУР
(ім'я, прізвище)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 67 сторінок, 42 рисунки, 2 таблиці, 19 джерел.

Об'єкт дослідження — процеси виявлення та реагування на інциденти інформаційної безпеки в корпоративних інформаційних системах.

Предмет дослідження — технологія виявлення та реагування на інциденти інформаційної безпеки на базі платформи Wazuh.

Мета роботи — розробити технологію виявлення та реагування на інциденти інформаційної безпеки з використанням платформи Wazuh та надати рекомендації щодо її впровадження в корпоративне середовище.

Методи дослідження — аналіз наукової літератури, вивчення експлуатаційної документації, порівняння міжнародних стандартів, моделювання сценаріїв інцидентів, практичне налаштування компонентів Wazuh.

Платформа Wazuh є сучасним рішенням у сфері кібербезпеки, що поєднує функціонал SIEM, IDS/IPS, механізми кореляції подій та автоматизованого реагування. Вона дозволяє здійснювати централізований моніторинг безпеки, збір логів, аналіз подій та реалізацію сценаріїв реагування на інциденти.

У роботі проаналізовано сучасні загрози корпоративним інформаційним системам, досліджено підходи до виявлення та реагування на інциденти, порівняно можливості Wazuh з іншими SIEM-рішеннями (Splunk, ELK, AlienVault). Розкрито архітектуру Wazuh, її основні компоненти (Manager, Agent, Indexer, Dashboard), механізми інтеграції з зовнішніми джерелами (Firewall, IDS/IPS, Cloud), а також реалізовано сценарії реагування (Active Response, SIEM Alerts).

На основі проведених досліджень запропоновано варіант технології виявлення та реагування на інциденти безпеки на базі Wazuh та розроблено рекомендації для фахівців з кібербезпеки щодо її впровадження.

Галузь використання — кібербезпека корпоративних інформаційних ресурсів.

Ключові слова: інформаційна безпека, інциденти, реагування, SIEM, Wazuh, корпоративні системи.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, ГІБРИДНА РОБОТА, SASE,
ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОЇ РОБОТИ ГІБРИДНИХ
ПРАЦІВНИКІВ

ABSTRACT

Text part of the qualification work: 67 pages, 42 figures, 2 table, 19 sources.

Object of research – detection and response to information security incidents in corporate information systems.

Subject of research – the technology for detecting and responding to information security incidents based on the Wazuh platform.

The aim of research – to develop a procedure for applying the Wazuh platform to detect and respond to information security incidents in corporate systems and to formulate recommendations for its implementation.

Research methods – study of the literature on this topic, analysis of operational documentation, international standards and their comparison, modeling of incident scenarios and practical configuration of Wazuh components.

The Wazuh platform is a modern cybersecurity solution that integrates SIEM functionality, intrusion detection and prevention, log analysis, and automated response mechanisms. It enables centralized security monitoring, event correlation, and active response to threats in real time.

The paper analyzes the problem of detecting and responding to information security incidents in corporate environments, defines its purpose and objectives. A comparison of Wazuh with other SIEM solutions (Splunk, ELK, AlienVault) is carried out. The architecture and core components of Wazuh (Manager, Agent, Indexer, Dashboard) are examined, along with its integration with external data sources (firewalls, IDS/IPS, cloud services). Incident response scenarios are implemented using Active Response and SIEM alerts.

Based on the research carried out in the work, a technology for detecting and responding to information security incidents using Wazuh is proposed. Recommendations for cybersecurity specialists on the use of Wazuh in corporate environments are developed.

Field of application – cybersecurity of information resources of the organization.

Keywords: information security, incident detection, incident response, SIEM, Wazuh, corporate systems.

INFORMATION RESOURCES OF THE ORGANIZATION, HYBRID
WORK, SASE, TECHNOLOGY FOR ENSURING THE SECURE WORK OF
HYBRID WORKE

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	9
ВСТУП	10
1 АНАЛІЗ ПРОБЛЕМИ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ	12
1.1 Проблема забезпечення інформаційної безпеки в корпоративних інформаційних системах	12
1.2 Аналіз сучасних загроз безпеці корпоративних інформаційних систем	15
1.3 Підходи до систем виявлення та реагування на інциденти інформаційної безпеки	22
1.4 Порівняння можливостей Wazuh з іншими SIEM-рішеннями (Splunk, ELK, AlienVault)	27
2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА БАЗІ WAZUH	33
2.1 Призначення, можливості та архітектура платформи Wazuh	33
2.2 Основні компоненти системи Wazuh: Manager, Agent, Indexer, Dashboard	38
2.3 Механізми збору, обробки та кореляції подій безпеки в системі Wazuh	42
2.4 Інтеграція Wazuh із зовнішніми джерелами даних (Firewalls, IDS/IPS, Cloud-сервіси).....	45
2.5 Механізми реагування на інциденти: правила, дії, автоматизація (Active Response).....	51
3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА БАЗІ ПЛАТФОРМИ WAZUH	54
3.1 Розроблення архітектури системи виявлення та реагування інформаційної безпеки на базі Wazuh	54
3.2 Налаштування збору логів і кореляції подій з використанням Wazuh Agent.....	60
3.3 Реалізація сценаріїв реагування на інциденти безпеки (Active Response, SIEM Alerts).....	66
3.4 Розроблення рекомендацій щодо впровадження технології Wazuh у корпоративне середовище	73

ВИСНОВКИ	75
ПЕРЕЛІК ПОСИЛАНЬ	77
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)	79

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп'ютер

API – Application Programming Interface

APT – Advanced Persistent Threat

DDoS – Distributed Denial of Service

DNS – Domain Name System

EDR – Endpoint Detection and Response

IaaS – Infrastructure as a Service

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

SIEM – Security Information and Event Management

SOAR – Security Orchestration Automation and Response

SOC – Security Operations Center

UEBA – User and Entity Behavior Analytic

TCO – Total Cost of Ownership

CSIRT – Computer Security Incident Response Team

BYOD – Bring Your Own Device

DBIR – Data Breach Investigations Report

ВСТУП

Актуальність дослідження. У сучасному цифровому середовищі корпоративні інформаційні системи постійно зазнають впливу з боку кіберзагроз, які стають дедалі складнішими, масовішими та витонченішими. Традиційні засоби захисту, орієнтовані на периметр мережі, вже не здатні ефективно протистояти атакам, що здійснюються через хмарні сервіси, віддалені підключення, мобільні пристрої та внутрішні вразливості.

У зв'язку з цим особливої актуальності набуває впровадження інтегрованих рішень, здатних забезпечити централізований моніторинг, виявлення та реагування на інциденти інформаційної безпеки в реальному часі. Одним із таких рішень є платформа Wazuh, яка поєднує функціонал SIEM, IDS/IPS, засоби кореляції подій, моніторинг цілісності файлів, контроль доступу та механізми автоматизованого реагування.

Застосування Wazuh дозволяє організаціям не лише виявляти загрози на ранніх етапах, а й оперативно реагувати на них, зменшуючи ризики втрати даних, порушення бізнес-процесів та репутаційних втрат. У контексті зростаючої кількості інцидентів безпеки, дана технологія є перспективною для побудови ефективної системи кіберзахисту.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження технології виявлення та реагування на інциденти інформаційної безпеки в корпоративних інформаційних системах на базі платформи Wazuh.

Об'єкт дослідження – процеси виявлення та реагування на інциденти інформаційної безпеки в корпоративних інформаційних системах.

Предмет дослідження – технологія виявлення та реагування на інциденти інформаційної безпеки на базі платформи Wazuh.

Мета роботи – розробити порядок застосування технології виявлення та реагування на інциденти інформаційної безпеки з використанням платформи Wazuh та рекомендації щодо її реалізації.

Наукові завдання:

- дослідити сутність проблеми виявлення та реагування на інциденти інформаційної безпеки в корпоративних системах;
- проаналізувати сучасні загрози та підходи до забезпечення кіберзахисту;
- порівняти можливості платформи Wazuh з іншими SIEM-рішеннями;
- дослідити архітектуру, функціональні компоненти та механізми роботи Wazuh;
- розробити варіант технології виявлення та реагування на інциденти безпеки на базі Wazuh;
- сформулювати рекомендації щодо впровадження платформи Wazuh у корпоративне середовище.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання інцидентів та практичне налаштування компонентів Wazuh.

Практичне значення одержаних результатів – запропоновано технологію виявлення та реагування на інциденти інформаційної безпеки на базі Wazuh, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації у корпоративних інформаційних системах.

1 АНАЛІЗ ПРОБЛЕМИ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1 Проблема забезпечення інформаційно безпеки в корпоративних інформаційних системах

Сучасні корпоративні інформаційні системи являють собою складні динамічні екосистеми, у яких поєднуються гібридні інфраструктури, хмарні сервіси, розподілені додатки, мобільні платформи та численні інтерфейси взаємодії з бізнес-партнерами і сторонніми сервісами. Поєднання цих технологічних характеристик із посиленням цифрової трансформації бізнес-процесів створює нову якість проблем в інформаційній безпеці: захист перестає бути локальною задачею і перетворюється на проблему системного менеджменту, яка вимагає поєднання технічних, організаційних і процесних рішень. Це загальне положення становить вихідну тезу для аналізу проблеми забезпечення ІБ у корпоративних системах. [1]

Архітектурні та технологічні чинники проблеми

По-перше, розширення площини атаки як системна властивість. Сучасні організації використовують мультихмарні та гібридні моделі, платформені інтеграції (API), мікросервісну архітектуру та масове підключення кінцевих пристроїв — кожна така складова додає нові точки входу, які необхідно контролювати. У результаті відбувається істотне ускладнення моделей доступу і міжсистемної довіри: межі периметра розмиваються, і контроль довіри має ґрунтуватися не на локальній прив'язці, а на контексті та непрямих атрибутах (принципи Zero Trust). Наслідком цієї технологічної еволюції є збільшення складності моніторингу та аналізу подій, оскільки кореляція подій відбувається на рівні багатьох різномірних джерел телеметрії. [2]

По-друге, поява нових сценаріїв атак, пов'язаних із автоматизацією та інструментами масштабу. Ворог використовує автоматичні сканери, бот-мережі, оркестровані кампанії, інструменти для купівлі/продажу облікових даних та сервіси «ransomware-as-a-service». Це сприяє збільшенню швидкості та масовості атак, водночас роблячи їх більш «тонкими» — з меншим шумом і високою ймовірністю обходу відомих сигнатурних детекторів. Сам по собі цей тренд не руйнує базові принципи захисту, але змінює вимоги до інструментарію: потрібні платформи здатні в

режимі реального часу корелювати події, виявляти поведінкові аномалії і виконувати автоматичні відповіді на підозрілі ланцюги дій. [1, 2]

Інформаційна ентропія і проблема агрегування даних

Кількісний аспект проблеми полягає у зростанні обсягів генерованої телеметрії. Журнали ОС, мережеві потоки, події безпеки додатків, сигнали кінцевих точок, результати сканувань вразливостей і дані хмарної телеметрії формують багатовимірні масиви, що перевищують можливості ручного аналізу. Цей феномен назвемо інформаційною ентропією середовища: в умовах великого потоку подій важливість кожного окремого повідомлення знижується без контекстуальної обробки. Наслідок — традиційні підходи до моніторингу (розрізнені інструменти, локальні алерти) виявляються недостатньо ефективними, і виникає потреба в централізованих механізмах нормалізації, індексування й кореляції подій. Саме необхідність побудови масштабованих індексаторів та механізмів автоматичної фільтрації формує вимогу до архітектури SIEM/XDR-рішень. [3]

Організаційні фактори: процеси, ролі, людський фактор

Організаційна складова проблеми має дві взаємопов'язані площини. З одного боку, брак уніфікованих процесів і процедур (відсутність стандартизованих playbook-ів реагування, нечетка відповідальність за ролі в SOC/CSIRT) призводить до повільного та непослідовного реагування на інциденти. NIST у своїх останніх рекомендаціях окреслює необхідність інтеграції процесів виявлення, аналізу, реагування та відновлення у єдину лінію життєвого циклу інциденту (prepare → detect → analyze → contain → eradicate → recover → lessons learned). Недостатня зрілість процесів робить організації вразливими навіть там, де технічні засоби присутні. [3]

З іншого боку, людський фактор залишається джерелом більшості початкових помилок: неправильно встановлені права доступу, пропущені оновлення, необачні дії користувачів або адміністраторів. При цьому роль людини подвійна: вона і джерело ризику, і ресурс, здатний суттєво мінімізувати цей ризик при належному навчанні та процесному супроводі. Як показують останні великі огляди порушень, велика частина інцидентів має вадою на рівні операційної практики або помилки конфігурації — а не лише наявністю нульових днів у софті. [2]

Фрагментація інструментів та її операційні наслідки

У типовому корпоративному середовищі набір рішень з безпеки формується

еволюційно: антивірусні підсистеми, EDR-агенти, мережеві монітори, IDS/IPS, хмарні монітори, системи управління вразливостями та локальні лог-сервера. Така фрагментація призводить до кількох системних проблем: дублювання сигналів, відсутність єдиного контексту для кореляції, велика кількість хибних спрацьовувань, та недостатня оперативність реагування. Наслідок — підвищений MTTD (mean time to detect) і MTTR (mean time to respond), що безпосередньо збільшує потенційні наслідки інциденту для бізнесу. Рішення: побудова інтегрованої платформи, що забезпечує централізоване збирання, нормалізацію та консистентну інтерпретацію подій. [3]

Нормативно-правові та відповідальні вимоги як каталізатор проблем

Регуляторні вимоги (зокрема GDPR, секторні стандарти та контрактні вимоги постачальників послуг) накладають додаткові технічні й організаційні зобов'язання. Відповідність вимогам означає не лише ведення логів, але й їх збереження у відповідному вигляді, забезпечення цілісності доказової бази, своєчасне повідомлення зацікавлених сторін та здатність демонструвати процес реагування при аудиті. Недотримання цих вимог створює не лише фінансові та репутаційні ризики, а й ставить під загрозу безперервність бізнес-операцій. Отже, вимоги регуляторів підсилюють потребу в надійних механізмах моніторингу та IR-процесах. [1]

Технічні наслідки: потреба в ранньому виявленні та автоматизації реагування

Поєднання архітектурної складності, обсягу подій та нестачі кадрів у SOC створює умови, коли людський аналіз у реальному часі стає неефективним. Для зменшення цього розриву необхідні інструменти автоматизації — від простих правил кореляції до складних SOAR-процесів, що дозволяють виконувати попередню фільтрацію, пріоритизацію та навіть автоматичне блокування на основі визначених сценаріїв. Важливо, щоб автоматизація не була «чорною скринькою», а інтегрувалася в процеси людського контролю (human-in-the-loop) та залишала повний аудит для подальшого розслідування. [3]

Проблема забезпечення інформаційної безпеки в корпоративних системах має системний та мультидисциплінарний характер. Вона виникає не лише через наявність окремих технічних вразливостей, а як результат поєднання архітектурної складності, інформаційної ентропії, фрагментації інструментів, людського чинника та нормативно-правових вимог. Практична імплікація для організацій — необхідність

переходу від локальних, ізольованих рішень до концепції централізованого управління інцидентами, яка включає збір та нормалізацію телеметрії, кореляцію подій, поведінковий аналіз, інтегровані процеси IR та засоби автоматизації реагування.

1.2 Аналіз сучасних загроз безпеці корпоративних інформаційних систем

Сучасний ландшафт загроз для корпоративних інформаційних систем характеризується суттєвим збільшенням кількості атак, їх технологічною складністю та швидкістю поширення. За даними глобальних аналітичних звітів ENISA Threat Landscape 2025 [1] та Verizon DBIR 2025 [2], простежується кілька домінантних тенденцій, які суттєво впливають на рівень кіберризиків для організацій незалежно від масштабу їхньої IT-інфраструктури. Характерною ознакою поточного періоду є зростання експлуатації вразливостей та індустріалізація соціальної інженерії, які дедалі частіше комбінуються у рамках складних багатоступеневих атак.

Однією з ключових тенденцій є збільшення ролі експлуатації відомих та невідомих (zero-day) вразливостей як початкових векторів доступу. Звіт Verizon DBIR 2025 фіксує значне зростання кількості інцидентів, де саме вразливості стали першим елементом атаки, — частка таких випадків досягла приблизно 20 %, що становить зростання на 34 % у порівнянні з попереднім роком [2]. Особливо тривожною є ситуація з пристроями периферійної інфраструктури (edge devices) та VPN-шлюзами, вразливості яких стали об'єктом масової експлуатації: їх частка збільшилася з 3 % до 22 %. Це свідчить про те, що атаки дедалі частіше спрямовуються на компоненти, які традиційно мають слабший контроль оновлень і недостатній рівень журналювання.

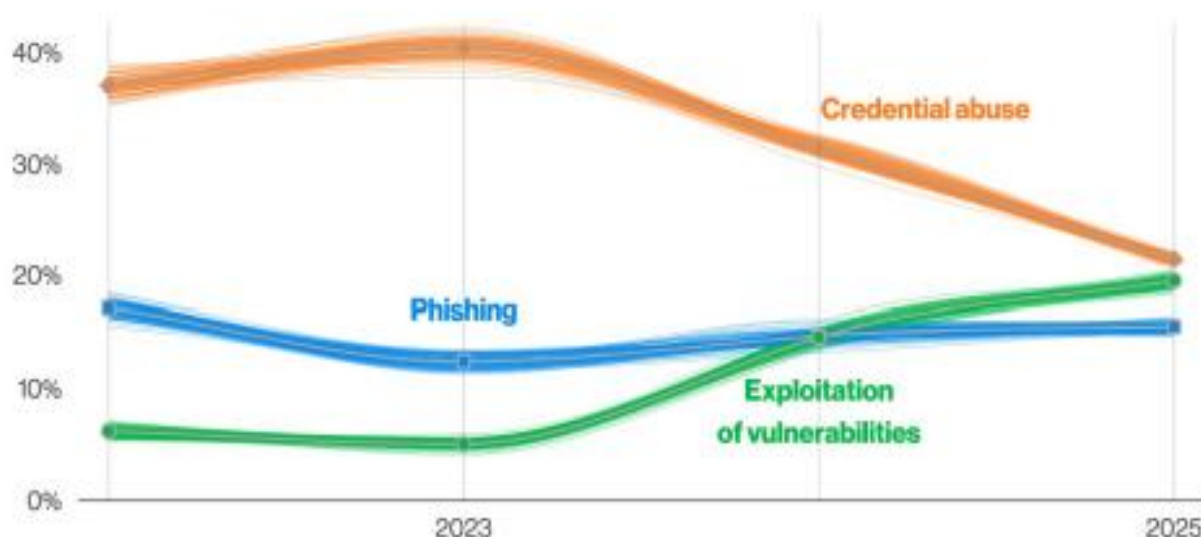


Рис. 1.1 – Відомі початкові вектори доступу з плином часу при порушеннях, що не пов'язані з помилками та зловживанням

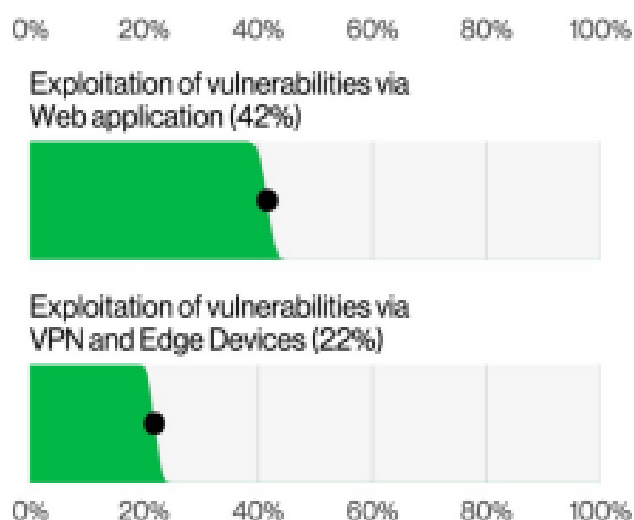


Рис. 1.2 – Вибір переліків векторів використання вразливостей що не пов'язані з помилками та зловживанням

Не менш вагому роль у сучасних атаках відіграє фактор людини. ENISA зазначає, що фішинг та інші форми соціальної інженерії залишаються найпоширенішими способами початкового проникнення в корпоративні системи — майже 60 % виявлених інцидентів починалися саме з фішингових повідомлень [1]. Водночас індустріалізація цього методу через платформи Phishing-as-a-Service (PhaaS) зробила його доступним навіть для зловмисників із мінімальною технічною компетенцією. Такі інструменти дають змогу автоматизувати розсилки, створювати фальшиві сторінки авторизації та обходити багатофакторну автентифікацію через техніки «людина-посередина» (AiTM).

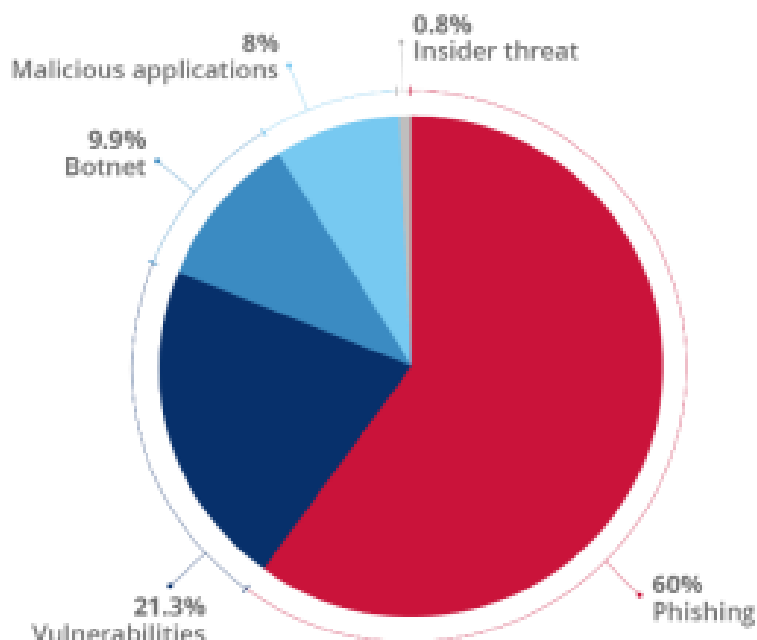


Рис. 1.3 – Відсоткове відношення початкових векторів інфекції

Значну увагу фахівців привертає також проблема залежності від третіх сторін та ланцюгів постачання. За оцінкою DBIR 2025, частка інцидентів, у яких була задіяна третя сторона, зросла з приблизно 15 % до майже 30 % [2]. Компрометація одного постачальника чи хмарного сервісу може мати каскадний ефект, спричиняючи збої або витоки відразу у десятках організацій. Такі сценарії демонструють, що управління ризиками ланцюга постачання (supply chain risk management) стає обов’язковою складовою корпоративної безпеки. Це підтверджується рекомендаціями міжнародних стандартів, зокрема NIST SP 800-61 Rev.3 [3], які підкреслюють необхідність контролю безпеки не лише всередині організації, а й серед партнерів і підрядників.



Рис. 1.4 – Участь третіх сторін у порушеннях

Окремою складовою сучасних загроз є стрімке поширення інфостілерів та масова компрометація облікових даних. DBIR відзначає, що близько 46 % пристроїв, на яких були виявлені викрадені корпоративні логіни, належали до категорії неменеджованих (BYOD), що значно підвищує ризик змішування особистих і службових облікових записів [2]. Кореляційний аналіз показав, що у понад 50 % атак типу ransomware застосовувалися саме викрадені облікові дані, а майже 40 % компрометованих компаній мали корпоративні облікові записи у відкритих дампах інфостілерів. Така тенденція свідчить про необхідність суворішого контролю кінцевих пристроїв, впровадження MDM/EDR та політик, що обмежують використання BYOD у середовищах з підвищеним рівнем ризику.

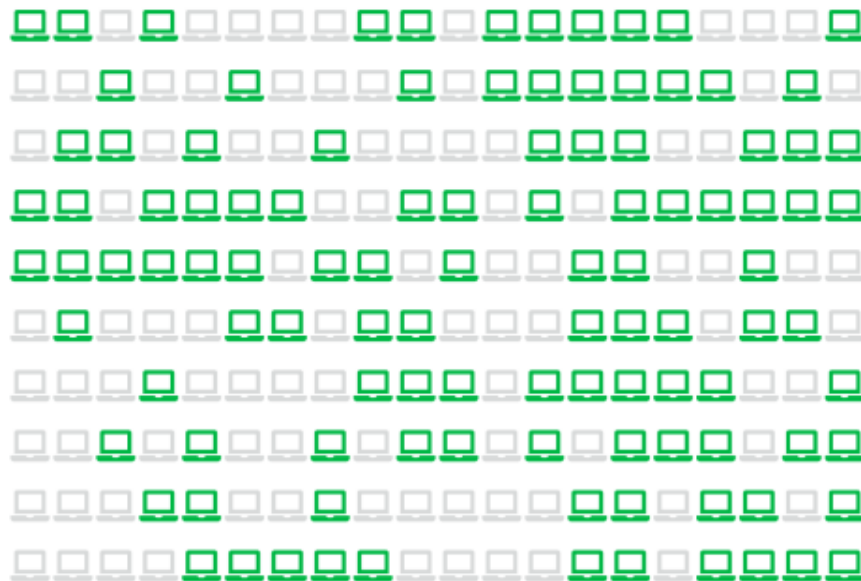


Рис. 1.5 – Відсоток некерованих пристроїв із корпоративними логінами в журналах infostealer (кожен гліф становить 0,5%)

Водночас ENISA підкреслює суттєве зростання кількості атак на мобільні платформи: у 2024–2025 роках частка мобільних загроз у ЄС досягла 42,4 %, що робить цей сегмент найбільш ураженим у порівнянні з іншими платформами [1]. Поширення шпигунського ПЗ для Android, атак, спрямованих на месенджери, та використання вразливостей у телекомунікаційних протоколах створюють нову площину ризиків для корпоративних систем, особливо у моделях гнучкої роботи та дистанційного доступу.

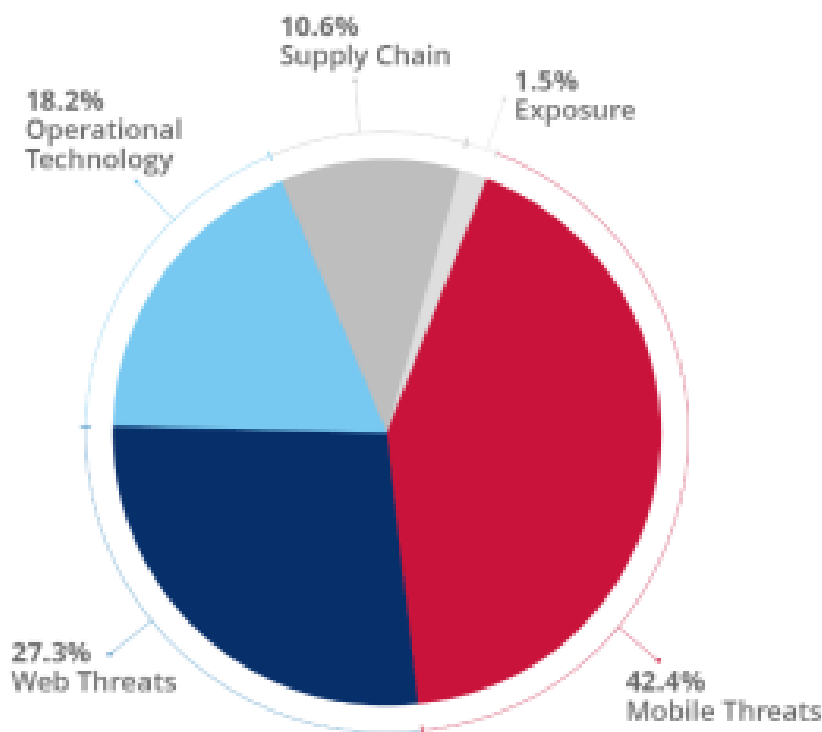


Рис. 1.6 – Розподіл загроз.

Ще однією визначальною тенденцією є значний розвиток операцій державних АРТ-груп, які дедалі частіше поєднують експлуатацію zero-day, атаки на ланцюги постачання та техніки прихованого доступу. За даними DBIR, діяльність таких груп у 2024–2025 роках набула суттєвої інтенсивності, а частка шпигунських операцій досягла 17 %, що істотно перевищує аналогічні показники попередніх років [2]. Більшість цих атак були спрямовані на телекомунікаційні, виробничі та логістичні сектори, які мають критичне значення для державної інфраструктури. Цей тренд підкреслює важливість багаторівневого захисту та впровадження підходів Zero Trust, які дозволяють знизити ризик непомітної компрометації.

Не менш суттєвим є розвиток і трансформація екосистеми ransomware. Згідно з DBIR, частка атак із використанням ransomware у структурі загальних порушень безпеки досягла 44 %, збільшившись майже на третину порівняно з попереднім роком [2]. Хоча середній розмір викупу зменшився до близько 115 тис. доларів США, загальний рівень збитків залишається високим, особливо для малих та середніх підприємств, де ransomware фігурує приблизно в 88 % усіх інцидентів. Зменшення викупів пояснюється як посиленням відмови компаній платити (до 64 %), так і

конкуренцією всередині ринку RaaS-послуг, але це не зменшує загальної небезпеки таких атак.

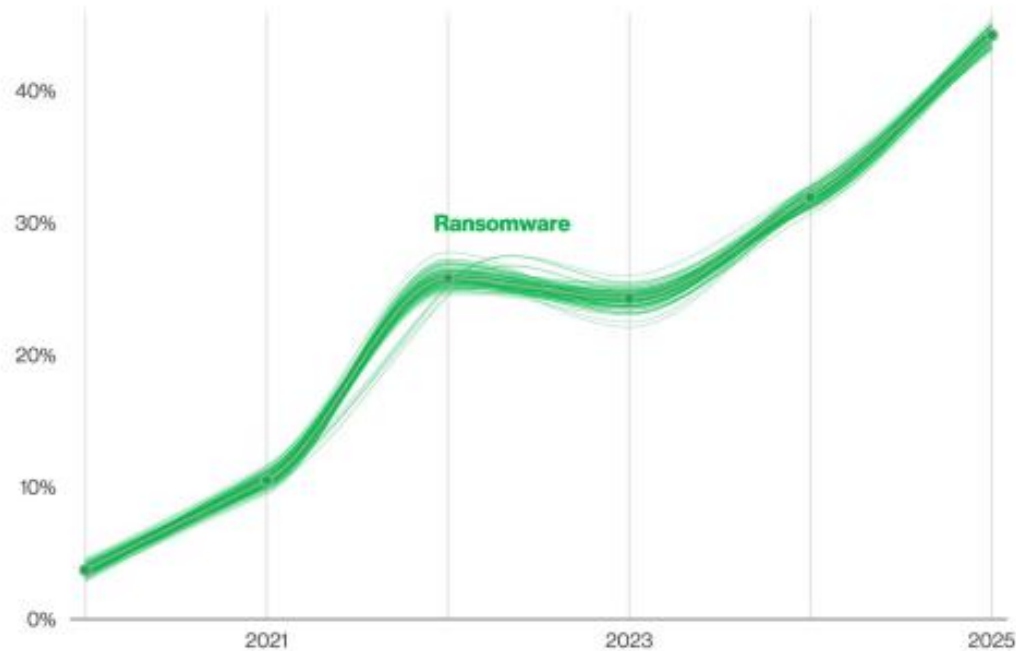


Рис. 1.7 – Дія програм-вимагачів під час порушень, з плином часу

Важливим новим викликом є зростання ролі штучного інтелекту як у діях зловмисників, так і у ненавмисних порушеннях. ENISA повідомляє, що понад 80 % фішингових листів, виявлених у 2024–2025 роках, були створені або оптимізовані за допомогою генеративних моделей [1]. Окрім цього, DBIR звертає увагу на ризики витоку даних через використання співробітниками зовнішніх GenAI-платформ: приблизно 15 % користувачів застосовували такі сервіси на робочих пристроях, і здебільшого — через особисті акаунти, що створює нові канали витоку конфіденційної інформації [2].



Рис. 1.8 – Відсотковий розподіл типів облікових записів доступу до послуг GenAI

Таким чином, аналіз сучасних загроз демонструє, що безпека корпоративних інформаційних систем перебуває під впливом взаємопов'язаних факторів: зростання кількості вразливостей, масовості соціальної інженерії, залежності від зовнішніх провайдерів, активності АРТ-груп, поширення мобільних атак, розвитку інфостілерів та застосування ШІ зловмисниками. Це потребує системного переосмислення підходів до захисту, включаючи прискорений патч-менеджмент, контроль кінцевих пристроїв, політики Zero Trust, захист ланцюгів постачання, а також формування культури інформаційної безпеки серед співробітників.

1.3 Підходи до систем виявлення та реагування на інциденти інформаційної безпеки

Сучасний кіберпростір характеризується високим рівнем складності атак, що постійно зростає. Зловмисники активно застосовують багатоступеневі техніки проникнення, комбінують соціотехнічні методи, експлуатують вразливості, використовують обхідні механізми проти традиційних засобів контролю та дедалі

частіше спрямовують атаки на хмарні середовища й ланцюги постачання. Згідно з ENISA Threat Landscape 2025 [1], кількість комплексних атак (multi-vector attacks) та інцидентів із тривалим прихованим перебуванням у системах (persistence) продовжує зростати, що суттєво ускладнює їхнє виявлення традиційними методами. Аналогічні тенденції підтверджує Verizon DBIR 2025: понад 60% досліджених інцидентів включали принаймні один етап, який неможливо виявити лише сигнатурними засобами [2].

У таких умовах пріоритет отримують системи, здатні не лише запобігати загрозам, а й ефективно виявляти їх на різних етапах життєвого циклу атаки, а також забезпечувати швидке та структуроване реагування. Відповідно до рекомендацій NIST SP 800-61 Rev.3, процес реагування повинен бути безперервним, включати збір телеметрії, кореляцію подій, аналіз інцидентів, автоматизацію рутинних дій та постійне вдосконалення процедур [3].

Ці принципи формують основу сучасних підходів до виявлення та реагування, серед яких ключову роль відіграють системи SIEM, EDR, XDR, SOAR, а також методології MITRE ATT&CK та Cyber Kill Chain. Усі зазначені компоненти формують єдину екосистему безпеки, де кожен інструмент компенсує обмеження інших, забезпечуючи багаторівневий контроль і здатність виявляти загрози на різних етапах.

Значення SIEM у сучасній архітектурі безпеки. Системи SIEM (Security Information and Event Management) стали фундаментом сучасної безпеки завдяки можливості централізовано збирати, нормалізувати та аналізувати телеметрію з усіх компонентів корпоративної інфраструктури. Вони забезпечують створення єдиного центру контролю, де журнал подій аналізується в сукупності, а не ізольовано. За класифікацією Gartner [5], SIEM є ключовою платформою рівня SOC, яка дозволяє реалізувати кореляцію подій, поведінкову аналітику UEBA та довгострокове зберігання логів для цифрової криміналістики.

Типовий цикл роботи SIEM включає збір логів, їхню нормалізацію, застосування кореляційних правил, створення інцидентів та візуалізацію у вигляді аналітичних панелей. Саме здатність корелювати події різного типу дозволяє SIEM виявляти складні атаки, які не залишають чітких сигнатур: наприклад, рух злоумисника всередині мережі (lateral movement), роботу з викраденими обліковими даними або

аномальну активність у хмарі [1].

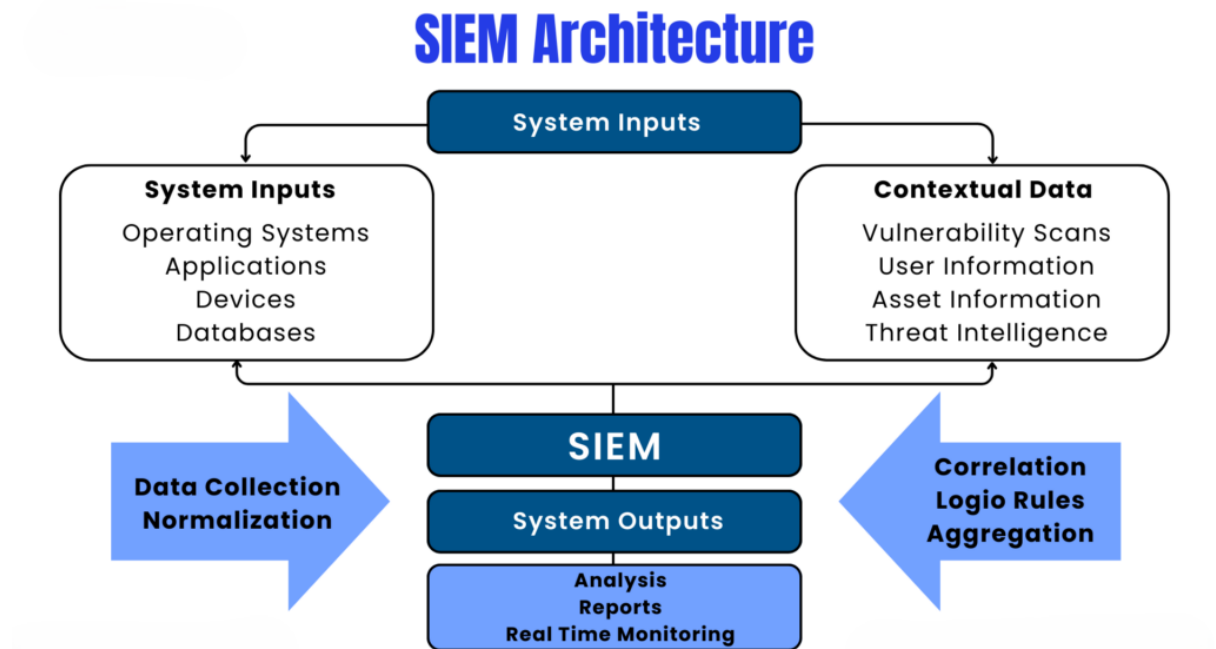


Рис. 1.9 — Архітектура системи SIEM

Водночас SIEM не забезпечує глибокого контролю активності на кінцевих точках, а також не завжди ефективно працює з подіями, які не мають чіткої кореляційної логіки. Тому до нього додаються інші підходи.

Роль EDR у виявленні поведінкових загроз. EDR (Endpoint Detection and Response) є відповіддю на те, що більшість успішних атак розпочинаються саме з компрометації кінцевої точки. За даними DBIR 2025 [2], у понад 80% інцидентів першим етапом є компрометація workstation або server endpoint через фішинг, експлуатацію вразливостей або запуск шкідливого ПЗ.

EDR-системи забезпечують глибоке відстеження активності на рівні ОС: процесів, мережових з'єднань, файлових операцій, змін у реєстрі, системних викликів тощо. Вони виявляють складні техніки MITRE ATT&CK, які неможливо фіксувати через SIEM без додаткової телеметрії: Process Injection, Credential Dumping, Abuse of Task Scheduler [4].

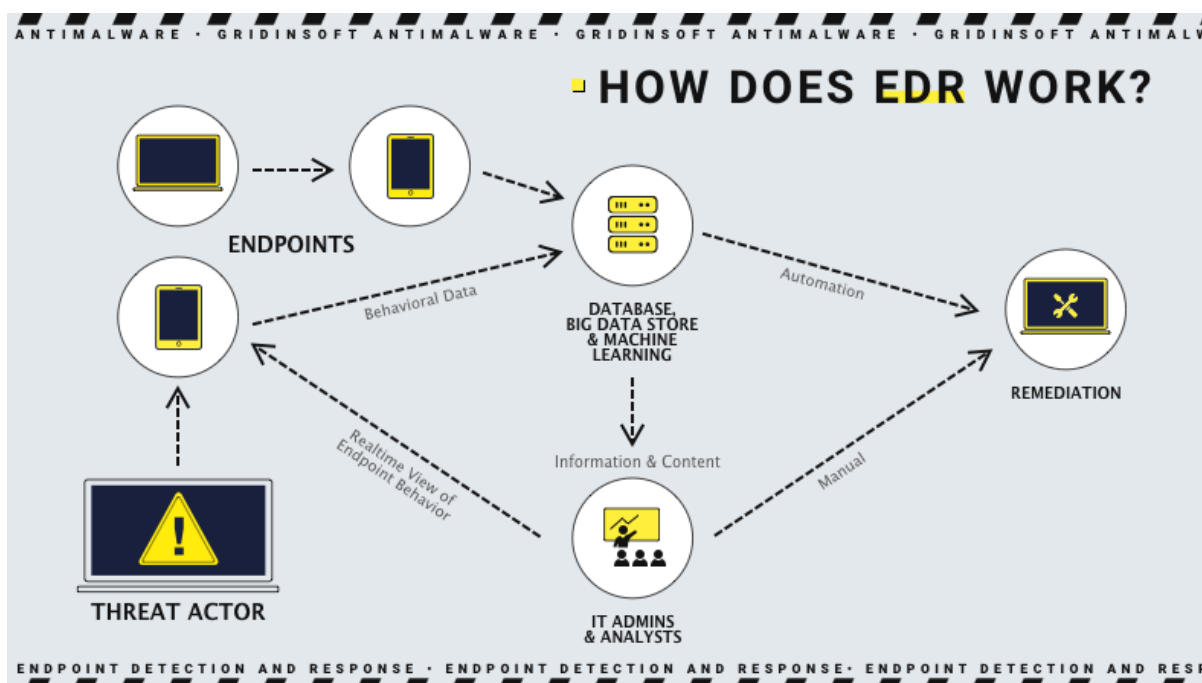


Рис. 1.10 — Структура системи EDR

EDR дозволяє не лише виявляти аномалії, а й ізолювати хост, блокувати процеси, видаляти шкідливі файли, що робить його важливим інструментом реагування.

Інтегрований підхід XDR. Поява XDR (Extended Detection and Response) стала природним кроком розвитку EDR, коли виникла потреба поєднати дані з кінцевих точок, мережевих сенсорів, хмарних логів та SIEM у єдиний контекст. Gartner визначає XDR як платформу, здатну автоматично об'єднувати розрізнені події у повноцінний ланцюг атаки [5].

Це дозволяє співставляти поведінку з різних систем — наприклад, підозрілу команду PowerShell на хості, зміну прав у AD та аномальний трафік на зовнішню IP — і пов'язувати їх у єдиний інцидент.

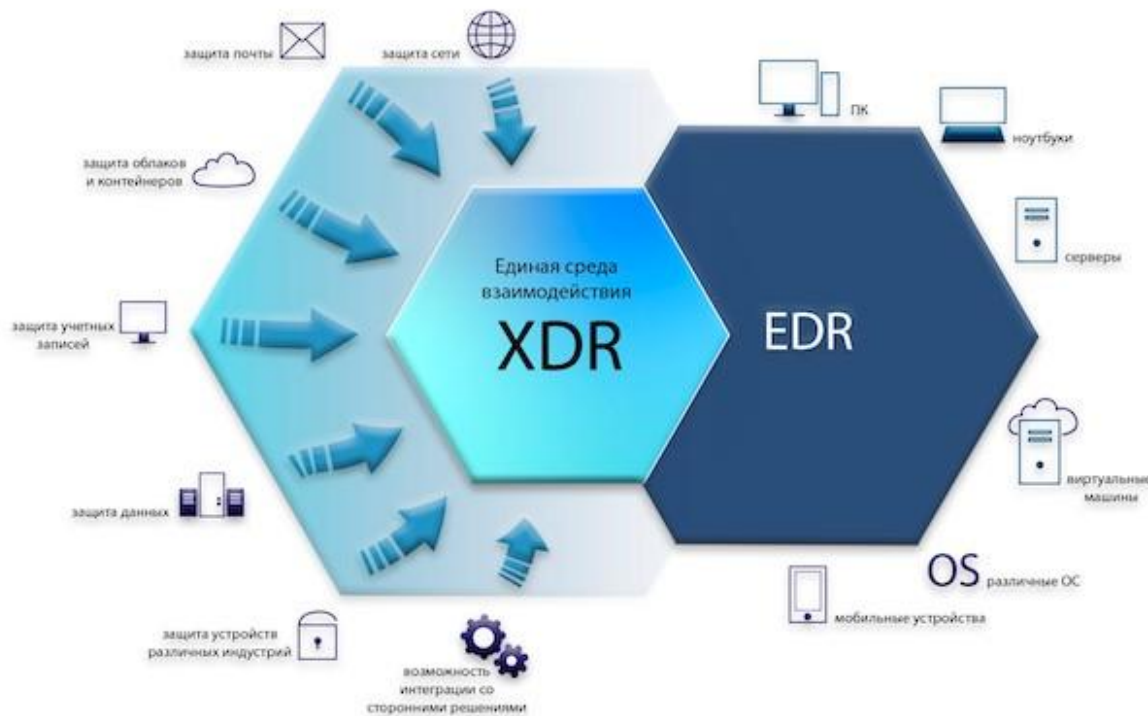


Рис. 1.11 — Концептуальна модель XDR

XDR використовує моделі машинного навчання, що значно знижує кількість хибних спрацювань у порівнянні з класичною кореляцією.

Автоматизація реагування через SOAR. Системи SOAR (Security Orchestration, Automation and Response) відповідають за автоматизацію рутинних та повторюваних дій. За NIST SP 800-61 [3], автоматизація дозволяє скоротити час реагування та зменшити залежність від людського фактору.

SOAR виконує такі завдання:

- автоматичне блокування облікових записів;
- ізоляція хостів;
- запуск скриптів розслідування;
- оновлення списків блокування;
- генерація звітів про інциденти.

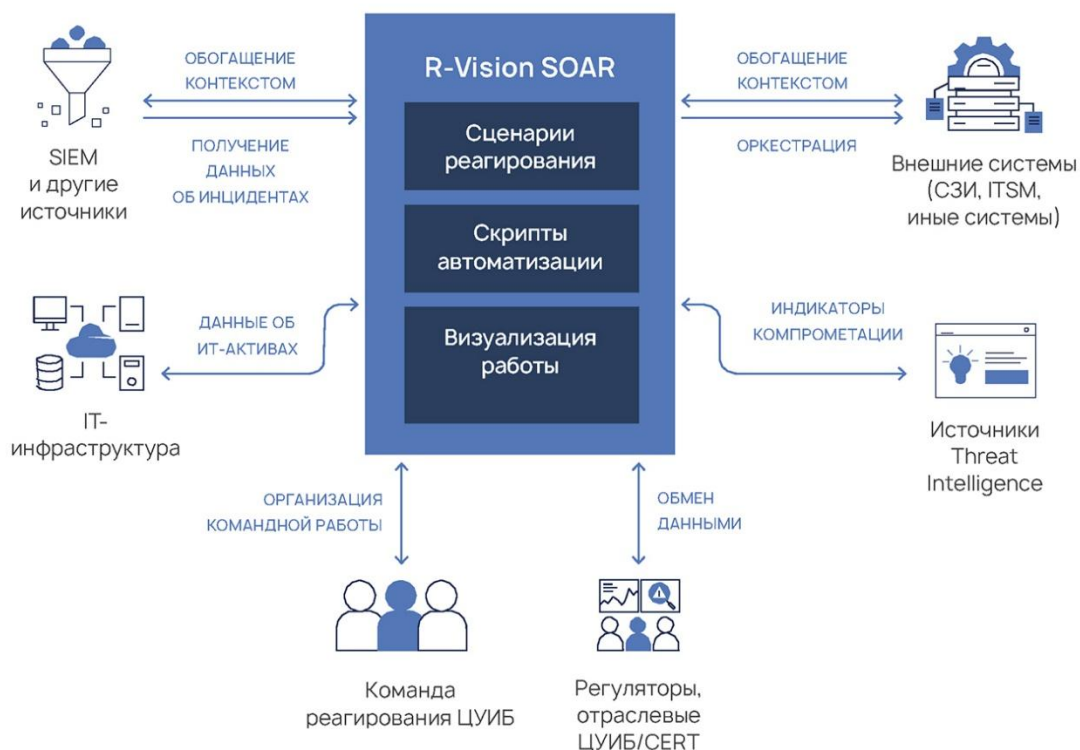


Рис. 1.12 — Автоматизоване реагування в SOAR

Методологічна основа: Cyber Kill Chain та MITRE ATT&CK. Модель Cyber Kill Chain [6] описує атаку як послідовність етапів від розвідки до досягнення цілі. Це дозволяє визначати, на яких саме фазах повинні спрацювати EDR, SIEM, XDR або SOAR.

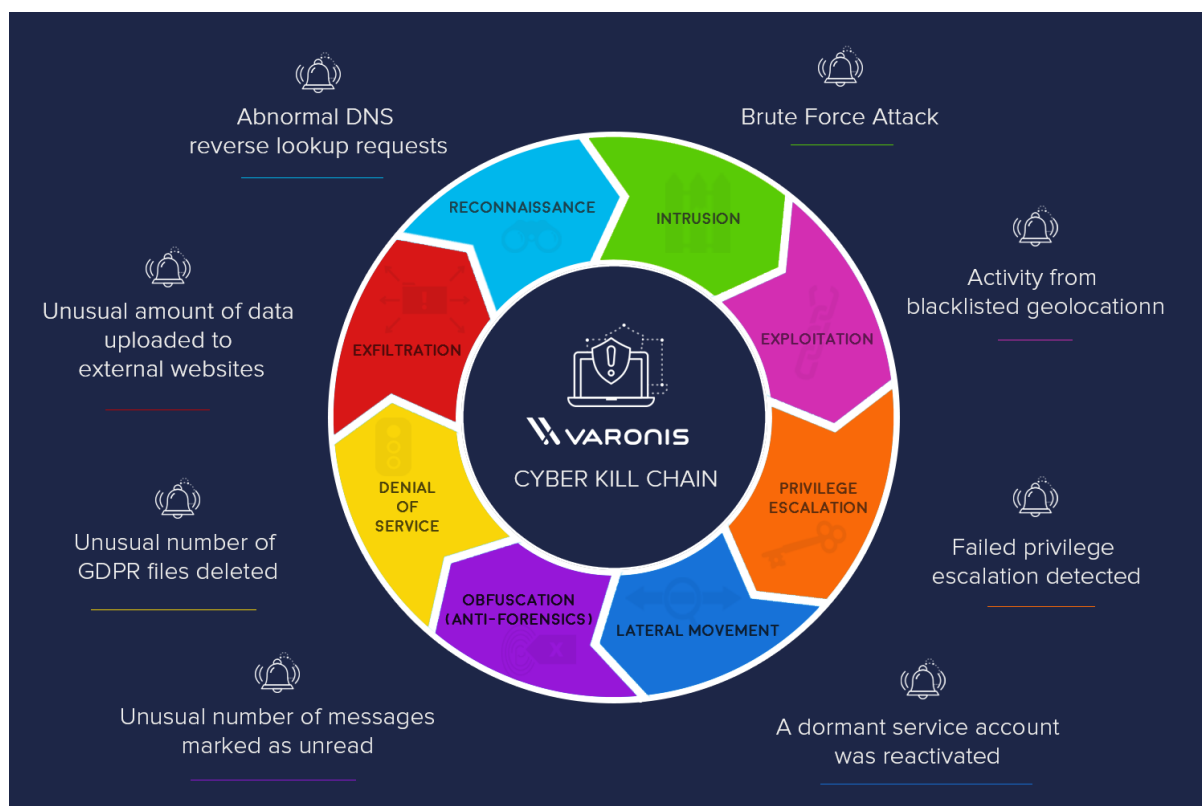


Рис. 1.13 — Модель Cyber Kill Chain

MITRE ATT&CK [4] доповнює Kill Chain детальною класифікацією технік, що використовується для розробки правил виявлення, кореляційних сценаріїв та автоматизованих дій.

Всі описані системи — SIEM, EDR, XDR, SOAR — зазвичай реалізовані у вигляді дорогих комерційних продуктів, інтеграція яких потребує значних фінансових та технічних ресурсів. Однак у багатьох організаціях, особливо середніх та бюджетних, існує необхідність у комплексному рішенні, яке:

- поєднує функціональність SIEM та EDR;
- підтримує компонент автоматизованого реагування;
- інтегрується з MITRE ATT&CK та Kill Chain;
- забезпечує гнучку кореляцію подій;
- є безкоштовним і відкритим;
- легко масштабується в хмарі або on-premise;
- має активну спільноту та велику кількість готових модулів.

Саме таким рішенням є **Wazuh**, яке органічно поєднує ключові можливості SIEM та EDR, має власні механізми поведінкових правил, підтримує автоматизацію через Active Response, інтегрується з Threat Intelligence та працює відповідно до рекомендацій міжнародних стандартів. Тому у подальшому дослідженні доцільним є фокус саме на Wazuh як на комплексній платформі для виявлення та реагування на інциденти інформаційної безпеки.

1.4 Порівняння можливостей Wazuh з іншими SIEM-рішеннями (Splunk, ELK, AlienVault)

У сучасних інформаційних системах SIEM-рішення (Security Information and Event Management) відіграють ключову роль у забезпеченні безперервного моніторингу подій, кореляції індикаторів загроз та автоматизації реагування на інциденти. На ринку представлені як комерційні системи корпоративного рівня, так і рішення з відкритим кодом, що дозволяють гнучко адаптувати платформу під конкретні потреби. У цьому підрозділі проведено порівняльний аналіз платформи Wazuh з найбільш поширеними SIEM-рішеннями — Splunk Enterprise Security, ELK Stack (Elastic Security) та AlienVault (OSSIM/USM). Аналіз зосереджений на

функціональності, архітектурі, можливостях масштабування, вартості володіння та придатності для практичного впровадження.

Підходи до архітектури та моделі обробки подій. Архітектурні особливості SIEM суттєво впливають на продуктивність системи, швидкість обробки логів та можливість її подальшого масштабування.

Wazuh реалізує модульну архітектуру, що включає агентів, центральний менеджер та інтеграцію з Elastic Stack або OpenSearch для зберігання та візуалізації даних. Агентська модель дозволяє здійснювати глибокий збір даних з хостів: аудит, контроль цілісності файлів, інвентаризацію ПЗ та моніторинг системних подій. Перевагою є можливість централізованого управління конфігураціями та правилами безпеки, а також розширюваність за рахунок написання власних модулів.

Splunk Enterprise Security є платформою з потужним механізмом індексування великих обсягів даних. Архітектура складається з форвардерів, індексерів, пошукових вузлів та окремих модулів для аналітики безпеки. Splunk відомий гнучкою системою пошуку SPL (Search Processing Language), яка дозволяє будувати складні кореляційні запити. Архітектура орієнтована на високонавантажені системи, проте вимагає значних апаратних ресурсів.

ELK Stack (Elastic Security) побудований на Elasticsearch, Logstash, Beats та Kibana. ELK є не власне SIEM-системою, а платформою для побудови SIEM-рішень. Elastic Security додає можливості кореляції, детекції загроз (включно з правилами на основі Sigma), а також machine learning у комерційній версії. Архітектура ELK є однією з найгнучкіших, але потребує високої технічної експертизи для розгортання.

AlienVault OSSIM та USM поєднує SIEM з IDS/IPS, аналізом вразливостей, управлінням активами і підтримкою плагінів. На відміну від модульних SIEM, AlienVault пропонує "все-в-одному", що спрощує впровадження, але обмежує гнучкість архітектури.

Порівняння функціональних можливостей та аналітичних інструментів. Для ефективного реагування на інциденти важливо оцінити набір функцій, які кожне з рішень пропонує "з коробки".

1. Кореляція та виявлення інцидентів. Wazuh використовує вбудовані правила на основі OSSEC, які охоплюють широкий спектр атак: brute-force, privilege escalation, зміну критичних файлів, експлуатацію вразливостей тощо. Також

платформа підтримує інтеграцію з feed-джерелами загроз (Threat Intelligence), YARA, VirusTotal. Splunk ES пропонує найпотужнішу систему кореляції завдяки SPL та можливості побудови аналітичних моделей. Elastic Security впроваджує правила на основі Sigma та має можливість ML-аналізу (платна версія). AlienVault забезпечує базову кореляцію та набір вбудованих сценаріїв виявлення інцидентів, але поступається гнучкістю.

2. Моніторинг цілісності файлів (FIM). Wazuh має вбудований FIM-модуль, який не потребує зовнішніх інструментів. У Splunk FIM відсутній у стандартній версії та реалізується за допомогою сторонніх додатків. ELK потребує Filebeat-модуля з ручною конфігурацією. AlienVault має базовий FIM.
3. Управління вразливостями. Wazuh включає нативний сканер вразливостей, який аналізує пакети, версії, порівнює їх із базами CVE. ELK такої функції не має без додаткових модулів. Splunk потребує сторонніх інтеграцій або окремих продуктів. AlienVault має вбудований сканер, але він менш точний.
4. Можливості SOAR / автоматизації реагування. Wazuh використовує Active Response для виконання автоматичних дій (блокування IP, зупинка процесів, зміна правил файрволу). Splunk ES інтегрується з Splunk SOAR — повноцінною системою автоматизації. В ELK автоматизація реалізується через Alerts & Actions, але обмежено. AlienVault має базові механізми, але без повноцінних playbooks.

Масштабування, продуктивність та вимоги до інфраструктури. При впровадженні SIEM важливо оцінювати не лише функціональність, але й здатність системи обробляти зростаючий потік подій.

Splunk має найвищу продуктивність і може працювати з сотнями тисяч EPS (Events Per Second), але потребує масштабних індексерів та розподіленої архітектури. Це робить його придатним для великих корпоративних мереж, але багатократно збільшує TCO.

ELK також добре масштабується, адже Elasticsearch оптимізований для великих обсягів даних. Однак під час масштабування виникають виклики: балансування навантаження, оптимізація індексів, розподіл шардів. Підтримка великого кластера ELK потребує кваліфікованих DevOps-фахівців.

Wazuh забезпечує достатній рівень масштабування для середніх і великих

організацій. У комбінації з розподіленим кластером Elasticsearch або OpenSearch система може працювати з високою швидкістю обробки подій. Однак завдяки ефективній агентській моделі навантаження на сервер зменшується, а вимоги до ресурсів нижчі, ніж у Splunk.

AlienVault найменш масштабований — система орієнтована на середні інфраструктури і не призначена для багатотисячних вузлів.

Вартість володіння та ліцензування. Фінансовий аспект є одним із ключових критеріїв при виборі SIEM.

- Wazuh є безкоштовною платформою з відкритим кодом. Ліцензійні витрати відсутні, що робить Wazuh надзвичайно привабливим для державних установ, освітніх закладів та компаній з обмеженим бюджетом.
- ELK безкоштовний у базовій версії, але функції SIEM, ML, Security Analytics та Alerting є частиною комерційної ліцензії Elastic X-Pack.
- Splunk — один із найдорожчих SIEM на ринку. Вартість залежить від обсягу індексованих даних на добу та може сягати значних сум у великих організаціях.
- AlienVault USM — комерційне рішення, тоді як безкоштовний OSSIM сильно обмежений у функціональності.

Таким чином, Wazuh і ELK є найбільш економічно вигідними, але Wazuh потребує менших трудових витрат на інтеграцію функцій.

Гнучкість, кастомізація та можливість адаптації

У сучасних системах кіберзахисту важливо, щоб SIEM-рішення могло адаптуватись під потреби організації.

- Wazuh надає повний доступ до правил, конфігурацій, джерел даних. Можливе створення власних модулів на Python, Bash, PowerShell. Оскільки система повністю відкрита, обмеження практично відсутні.
- Splunk підтримує широкий спектр інтеграцій і додатків, але складний у навчанні, і SPL має високий поріг входу.
- ELK є надзвичайно гнучким завдяки своїй модульності, але це одночасно є і недоліком: для кастомізації потрібні висококваліфіковані фахівці.
- AlienVault є найменш гнучким: плагіни та логіка кореляції обмежені виробником.

Нижче наведено загальну таблицю порівняння даних рішень:

Таблиця 1.1 – Порівняння можливостей Wazuh з
іншими SIEM-рішеннями

Критерій	Wazuh	Splunk Enterprise Security	ELK / Elastic Security	AlienVault (OSSIM / USM)
Тип ліцензії	Відкритий код, безкоштовно	Комерційна	Відкритий код + комерційні модулі (X-Pack)	OSSIM – безкоштовно, USM – комерційно
Модель архітектури	Агент-сервер, інтеграція з Elasticsearch / OpenSearch	Форвардери – індексери – пошукові вузли	Beats/Logstash → Elasticsearch → Kibana	«Все-в-одному»: кореляція + NIDS + вразливості
Моніторинг подій (HIDS)	Вбудований, розширений	Відсутній (через інтеграції)	Частково (Filebeat/Auditbeat)	Вбудований
Мережевий моніторинг (NIDS)	Через інтеграцію (Suricata/Snort)	Через сторонні рішення	Через інтеграції	Вбудований (Snort)
Моніторинг цілісності (FIM)	Вбудований, гнучкі правила	Через додаткові модулі	Через Filebeat (потребує налаштування)	Базовий
Управління вразливостями (Vulnerability Detection)	Вбудований автоматичний сканер	Сторонні інтеграції	Немає без сторонніх інструментів	Є (вбудований сканер)
Кореляція подій	Власний рушій правил (OSSEC-based)	Найпотужніший SPL, розширені сценарії	Кореляція на основі Sigma, ML у платній версії	Базова кореляція, обмежена
Automation / SOAR	Active Response (автоматизовані дії)	Splunk SOAR (окремий продукт)	Alerts & Actions (обмежено)	Базові реакції
Аналіз загроз, Threat Intelligence	Вбудована TI + інтеграції (VirusTotal, YARA)	Розширений TI, багато інтеграцій	Підтримка TI через інтеграції	TI з базовими можливостями
Підтримка Sigma/YARA/OSINT	Підтримка YARA, OSINT; правила схожі на Sigma	Sigma через додатки	Повна підтримка Sigma	Обмежена
Масштабування	Середнє → високе	Дуже високе (корпоративний рівень)	Високе, але важке в управлінні	Низьке → середнє
Вимоги до ресурсів	Помірні	Високі	Високі при великому кластері	Низькі/середні
Простота впровадження	Відносно проста	Складне, потребує підготовки	Складне, багато конфігурацій	Найпростіше
Простота підтримки	Середня	Складна (потрібні експерти SPL)	Складна (DevOps/SecOps компетенції)	Проста

Продовження Таблиці 1.1 – Порівняння можливостей
Wazuh з іншими SIEM-рішеннями

Критерій	Wazuh	Splunk Enterprise Security	ELK / Elastic Security	AlienVault (OSSIM / USM)
Візуалізація даних	Kibana / OpenSearch Dashboards	Потужні дашборди Splunk	Kibana	Обмежені
Рівень кастомізації	Дуже високий	Високий	Дуже високий	Низький
Придатність для SOC	Підходить для SOC малих і середніх компаній	Оптимально для великих SOC	Підходить, якщо є технічна команда	Обмежено придатний
TCO (Total Cost of Ownership)	Низький	Дуже високий	Середній (залежить від платних модулів)	Низький–середній
Оптимальний сценарій використання	Відкрите, гнучке SIEM з повноцінним HIDS	Великий корпоративний SOC, складні аналітичні задачі	Потужне SIEM для техкоманд з DevOps	Невеликі/середні організації

На основі проведеного аналізу можна сформулювати узагальнену оцінку:

1. Wazuh є оптимальним вибором для організацій, які потребують функціонального SIEM з мінімальними витратами на ліцензування та впровадження. Платформа забезпечує широкий спектр можливостей, включно з HIDS, FIM, аналізом вразливостей та Active Response, що часто відсутнє у конкурентів без додаткових модулів.
2. Splunk є найпотужнішим рішенням для корпоративного ринку, пропонуючи найкращі аналітичні інструменти, але вартість та складність впровадження роблять його недоцільним для середніх і малих організацій.
3. ELK (Elastic Security) варто обирати тим компаніям, які мають сильну команду DevOps/SecOps і готові інвестувати в налаштування системи. Це рішення забезпечує максимальну гнучкість, але вимагає значних технічних зусиль.
4. AlienVault може бути використаний як «стартове» SIEM, однак не придатний для масштабування та побудови сучасного SOC із високими вимогами.

З огляду на наведені характеристики, Wazuh являється збалансованою платформою для впровадження технологій виявлення та реагування на інциденти, особливо в тих інфраструктурах, де критично важливим є співвідношення функціональності та вартості.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА БАЗІ WAZUH

2.1 Призначення, можливості та архітектура платформи Wazuh

Wazuh — це уніфікована платформа безпеки з відкритим вихідним кодом (open-source), яка поєднує функціонал систем управління подіями безпеки (SIEM), host-based систем виявлення вторгнень (HIDS) та розширених можливостей для моніторингу кінцевих точок, контейнерів і хмарних середовищ. [11, 14]

Основна мета Wazuh — надати організаціям можливість [12, 14]:

- централізовано збирати журнали та події безпеки з різноманітних джерел (сервери, робочі станції, хмарні інстанси, контейнери і т.д.);
- здійснювати аналіз цих даних, виявляти загрози, аномалії та потенційні інциденти безпеки (неавторизовані зміни, спроби проникнення, зловмисну активність);
- контролювати цілісність системи — важливих файлів, конфігурацій, змін у системних компонентах;
- оцінювати конфігурації на відповідність корпоративним політикам або стандартам безпеки;
- виконувати автоматизовані дії реагування (Active Response) при виявленні загроз — блокування, карантин, сповіщення, інтервенції;
- вести централізований облік, зберігання та аналіз подій, у тому числі зручно переглядати їх через веб-інтерфейс, формувати звіти, проводити аудит;

Таким чином, Wazuh покликаний стати “одним центром безпеки” для інфраструктур різних масштабів — від невеликих компаній до великих підприємств із гібридними/хмарними середовищами.

Можливості Wazuh. Wazuh надає широкий набір функцій та модулів: від простого лог-моніторингу до комплексного захисту кінцевих точок, хмарних сервісів і контейнерів. [14]

Основні можливості [12-16]:

- File Integrity Monitoring (FIM): агент Wazuh відстежує зміни у файловій системі — створення, зміну, видалення файлів, зміну атрибутів, прав доступу

тощо. Це дозволяє виявляти несанкціоновані модифікації або підозрілу діяльність.

- Збір і аналіз логів / SIEM-подібні функції: Wazuh може збирати операційні, системні, прикладні логи, логін/логаут, події безпеки, події мережі тощо — нормалізувати їх, декодувати, аналізувати за правилами, корелювати події, генерувати алерти.
- Оцінка конфігурацій та політик безпеки (Configuration Assessment / SCA): Wazuh може перевіряти налаштування операційних систем, сервісів, відповідність політикам безпеки або стандартам жорсткості (hardening), наприклад через підтримку бенчмарків чи кастомних перевірок.
- Виявлення вразливостей та оцінка стану систем (Vulnerability Detection / Inventory): агенти можуть збирати інформацію про встановлене ПЗ, версії ОС, компоненти, відкриті порти — що дає змогу зіставляти з відомими вразливостями та вчасно реагувати.
- Моніторинг контейнерів, хмар і хмарних робочих навантажень: Wazuh підтримує середовища Docker, Kubernetes, хмарні провайдери — дає змогу контролювати безпеку контейнерів, змін у хмарних ресурсах, конфігурацій, доступів тощо.
- Threat Hunting, пошук загроз, кореляція подій та аналітика: за умови великого обсягу логів та подій — Wazuh дозволяє проводити глибокий аналіз, виявляти складні атаки, аномалії, проводити історичні розслідування.
- Автоматизоване реагування (Active Response): при виявленні підозрілих подій — блокування підозрілих IP, зупинка процесів, карантин файлів, запуск ремедіацій, інтеграція зі сторонніми інструментами.
- Централізоване управління агентами та масштабованість: Wazuh дає змогу керувати агентами централізовано — конфігурація, моніторинг, оновлення; підтримує розгортання як для невеликих середовищ, так і для enterprise-рівня з сотнями або тисячами агентів.

Завдяки такому набору можливостей, Wazuh може бути як простою системою моніторингу, так і основою для побудови повноцінного SOC-центру.

Архітектура Wazuh. Архітектура Wazuh є модульною і багаторівневою, що дає змогу підлаштувати платформу під різні масштаби, навантаження та потреби

безпеки[11, 12].

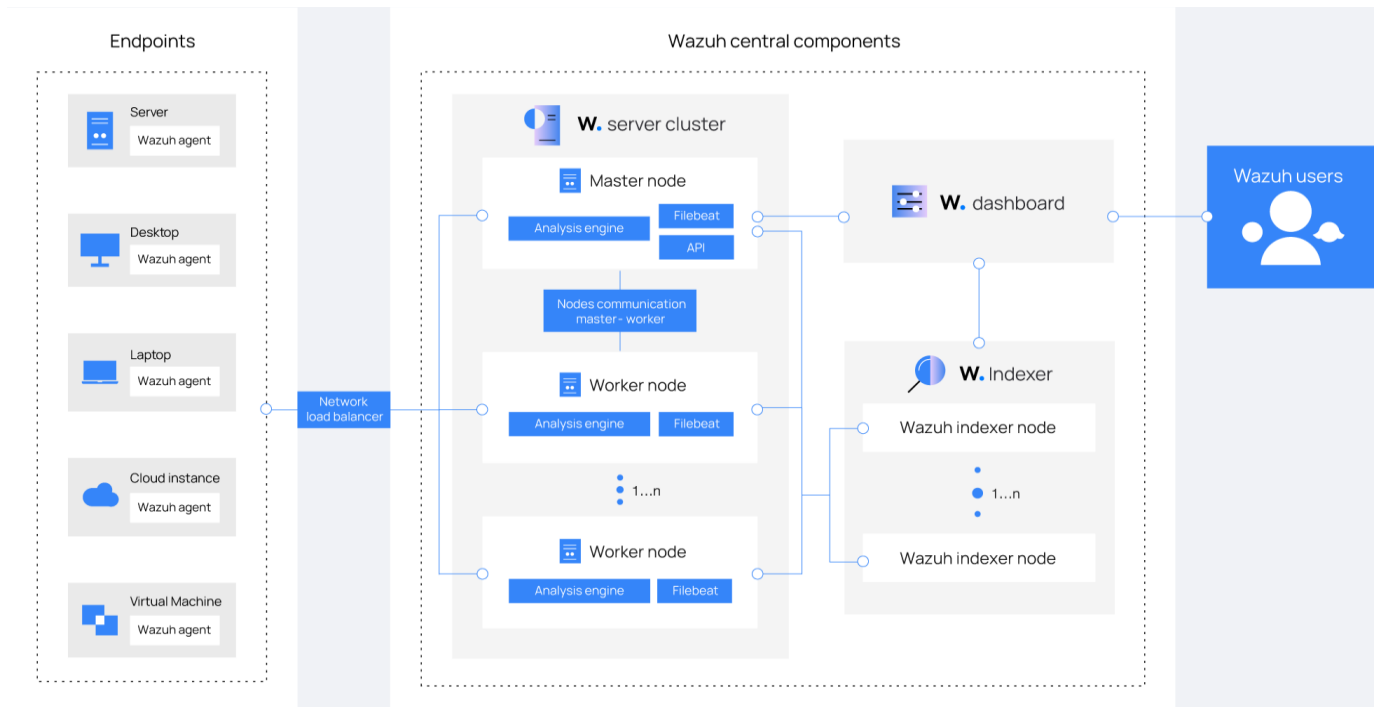


Рис. 2.1 – Архітектура Wazuh[11].

Wazuh Architecture

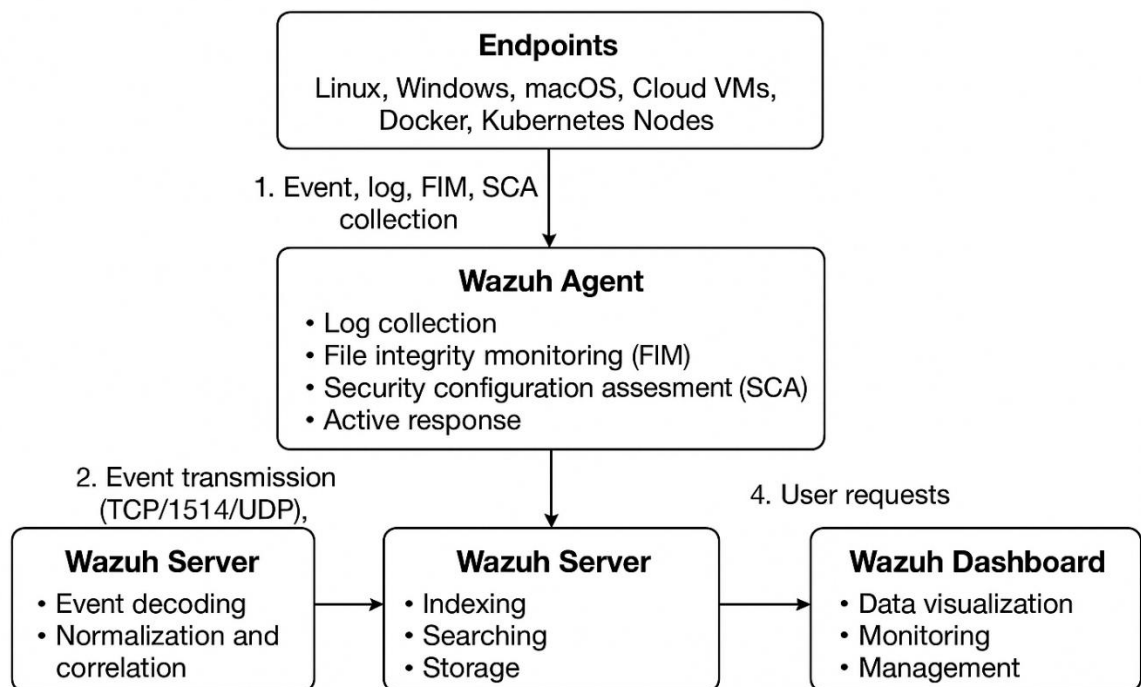


Рис. 2.2 – Архітектура Wazuh.

Головні компоненти системи [13]:

- **Wazuh Agent** — універсальний агент, який встановлюється на кінцеві хости (сервери, десктопи, VM, контейнери, хмарні інстанси). Працює на різних ОС:

Linux, Windows, macOS, Solaris, AIX тощо. Агент modular — кожен модуль відповідає за свою задачу: збір логів, FIM, SCA, інвентаризацію, перевірку конфігурацій, виявлення шкідливого ПЗ, Active Response та ін.

- Wazuh Server (менеджер) — центральний компонент, який приймає дані від агентів або агент-less джерел (наприклад, пристрої, які не підтримують агента, через syslog/SSH), аналізує їх, декодує логи, застосовує правила кореляції, виявляє загрози, генерує алерти, управляє агентами (реєстрація, конфігурація, оновлення), запускає Active Response.
- Wazuh Indexer — компонент для зберігання, індексації і пошуку нормалізованих подій, логів та алертів. Це повнотекстовий пошуковий/аналітичний движок — завдяки йому можна проводити швидкий пошук, агрегацію, аналіз історії, будувати звіти.
- Wazuh Dashboard — веб-інтерфейс для візуалізації, аналізу, моніторингу, управління конфігурацією, агентами та перегляду подій/алертів. Dashboard дає можливість створювати кастомні візуалізації, переглядати статус системи, керувати налаштуваннями, отримувати звіти.

Потік даних і взаємодія між компонентами[15]:

- Агент (або агент-less джерело) збирає дані: логи, події безпеки, зміни у файловій системі, інформацію про систему тощо, і відправляє їх на Wazuh Server. Зв'язок зазвичай здійснюється через TCP-порт 1514 (за умовчанням), з шифруванням (AES або опційно Blowfish).
- Wazuh Server отримує ці дані, декодує, нормалізує та аналізує їх за допомогою власних декодерів та правил (decoders + rules). Якщо подія відповідає певному правилу / тригеру — генерується alert / інцидент; за потреби — запускається Active Response.
- Алерти та події, які пройшли аналіз — передаються через Filebeat до Wazuh Indexer, де індексуються і зберігаються для подальшого пошуку, агрегації, історичного аналізу.
- Через Wazuh Dashboard користувачі (адміністратори, аналітики) переглядають події, статус агентів, налаштування, запускають пошук, створюють звіти, реагують на інциденти. Dashboard спілкується з сервером (для інформації про

конфігурацію/агенти) та з індексатором (для даних про події і алерти).

Варіанти розгортання та масштабованість. Wazuh дозволяє різні схеми розгортання, залежно від потреб[18]:

- All-in-one (все в одному хості) — сервер, індексатор, dashboard на одному сервері. Підходить для тестових, лабораторних або невеликих середовищ з невеликою кількістю агентів.
- Single-node production — сервер, індексатор і dashboard встановлені на різних вузлах/серверах: дає кращу продуктивність, ізолює компоненти, зменшує навантаження при зростанні кількості агентів.
- Multi-node / кластерне розгортання (cluster mode) — для середовищ enterprise: кілька серверів Wazuh Server (master + worker), кластер індексатора, окремий dashboard, load-balancer; забезпечує високу доступність (HA), горизонтальне масштабування, fault-tolerance, обробку великого потоку подій та великої кількості агентів.

Така модульна та масштабована архітектура дозволяє Wazuh бути гнучким й адаптуватися під різні за розміром та навантаженням інфраструктури.

Роль Wazuh у сучасній екосистемі безпеки. Wazuh займає проміжне місце між класичними HIDS, лог-менеджментом, SIEM — поєднуючи їх в одному рішенні. Це робить платформу привабливою для організацій, яким потрібен уніфікований інструмент для[14]:

- захисту кінцевих точок;
- моніторингу подій безпеки та мережевих логів;
- відповідності політикам і стандартам;
- автоматизації реагування;
- централізованого управління безпеки;
- підтримки heterogenous-середовищ (фізичні сервери, віртуальні машини, контейнери, хмари).

Завдяки відкритому коду, гнучкій архітектурі та широкому функціоналу Wazuh може виступати як доступна, масштабована та кастомізована альтернатива комерційним SIEM / XDR-рішенням.

2.2 Основні компоненти системи Wazuh: Manager, Agent, Indexer, Dashboard

Wazuh Manager — це центральний елемент системи, який виконує роль контролера, аналітичного ядра та координатора всіх процесів. Він відповідає за:

1. Обробку та кореляцію даних безпеки

Менеджер отримує події, журнали, результати перевірок цілісності, відповіді на правила та інші дані від Wazuh Agent або безагентних джерел. На основі вбудованих правил кореляції він визначає:

- рівень критичності події,
- категорію інциденту (наприклад, IDS/IPS, FIM, малвар, спроби ескалації привілеїв),
- відповідність стандартам (PCI DSS, CIS, GDPR тощо).

2. Виконання правил (Rules Engine)

Правила Wazuh базуються на синтаксисі OSSEC і дають змогу описувати безпекові сценарії:

- виявлення аномалій у поведінці систем,
- аналіз логів додатків,
- виявлення невідповідності конфігурацій,
- кореляцію подій у часі.

3. Реакцію на інциденти (Active Response)

Менеджер може автоматично виконувати дії:

- блокування IP через firewall,
- зупинка процесів,
- ізоляція вузлів,
- запуск скриптів реагування.

4. Керування агентами

Менеджер виконує реєстрацію агентів, розподіл конфігурацій, політик моніторингу, оновлення модулів.

5. Взаємодію з Indexer та Dashboard

Менеджер формує структуровані події та передає їх до Wazuh Indexer, забезпечуючи єдиний потік даних для подальшої аналітики та зберігання.

Завдяки цьому Wazuh Manager виступає ядром логіки системи, що забезпечує

комплексне виявлення загроз і координацію всіх компонентів.

Wazuh Agent — це легкий клієнтський компонент, що встановлюється на кінцевих вузлах: робочих станціях, серверах, контейнерах, віртуальних машинах та хмарних інстансах. Його завдання — збір телеметрії та виконання локальних перевірок безпеки.

Основні функції агента:

1. Збір логів та системних подій

Агент може збирати:

- журнали подій Windows,
- системні логи Linux та macOS,
- логи додатків, веб-серверів, служб,
- події безпеки (аудит доступу, зміни файлів, спроби авторизацій).

2. Моніторинг цілісності файлів (FIM)

Агент відстежує зміни у важливих системних файлах, конфігураціях, бібліотеках, виконуваних модулях.

Підтримується хешування (SHA1, SHA256), контроль атрибутів та виявлення модифікацій у реальному часі.

3. Виявлення атак та аномалій на рівні хоста (HIDS)

Механізми аналізу поведінки та виявлення:

- ескалації привілеїв,
- підозрілих команд,
- змін прав доступу,
- спроб експлуатації відомих вразливостей.

4. Аудит конфігурацій та відповідність стандартам (SCAP, CIS-CAT)

Агент може перевіряти конфігурації ОС на відповідність CIS Benchmarks, NIST, PCI DSS.

5. Передача даних

Усі зібрані події передаються на Wazuh Manager у зашифрованому вигляді (AES або TLS).

Таким чином, агент забезпечує «очі та вуха» системи, працюючи безпосередньо на контрольованих вузлах.

Wazuh Indexer — це високопродуктивний кластер для зберігання, пошуку та аналітики даних. Він базується на технологіях, походжених від OpenSearch (раніше — Elasticsearch), і забезпечує:

1. Індексуювання подій

Події, що надходять від Менеджера, перетворюються у структуровані документи та розміщуються у відповідних індексах.

Це дозволяє виконувати:

- повнотекстовий пошук,
- агрегації,
- аналітичні запити,
- створення складних дашбордів.

2. Горизонтальну масштабованість.

Кластер складається з master-, data- та coordinator-нод, що дає змогу масштабувати зберігання та швидкість пошуку у великих інфраструктурах.

3. Надійність та відмовостійкість

Підтримуються:

- реплікація шард,
- автоматичний перерозподіл даних у кластері,
- балансування навантаження.

4. Аналітичні можливості

Indexer забезпечує механізми:

- кореляційних запитів,
- аналітики часових рядів,
- виявлення статистичних аномалій,
- формування даних для машинного навчання.

Indexer є критичним компонентом, що забезпечує високу швидкість доступу до журналів і дає змогу виконувати глибоку аналітику подій безпеки.

Wazuh Dashboard — це веб-інтерфейс для роботи з даними, моніторингу стану системи та управління безпековими подіями. Він побудований на основі OpenSearch Dashboards і забезпечує:

1. Візуалізацію журналів та інцидентів

Дашборд надає інтерактивні графіки, таблиці, часові лінії, топологічні карти та інші візуальні елементи.

2. Моніторинг у режимі реального часу

Можна відстежувати:

- стан агентів,
- кількість і типи інцидентів,
- активність систем та служб,
- результати сканувань і перевірок.

3. Роботу з правилами та політиками

Дашборд містить інструменти для:

- редагування конфігурацій,
- перегляду спрацювань правил,
- створення власних аналітичних панелей.

4. Розмежування доступу та аудит дій

Підтримується рольова модель доступу (RBAC), що дозволяє призначати різні права для SOC-аналітиків, адміністраторів, аудиторів.

5. Інтеграцію з зовнішніми системами

Є можливість інтегрувати SIEM-системи, SOAR-платформи та інші інструменти реагування.

Dashboard формує інтуїтивно зрозумілий інтерфейс для управління всією екосистемою Wazuh.

Робота системи виглядає так:

Агент збирає телеметрію → Передає її в Manager → Manager виконує аналіз і формує події → Події зберігаються та індексуються в Indexer → Dashboard забезпечує доступ до аналітики та візуалізації.

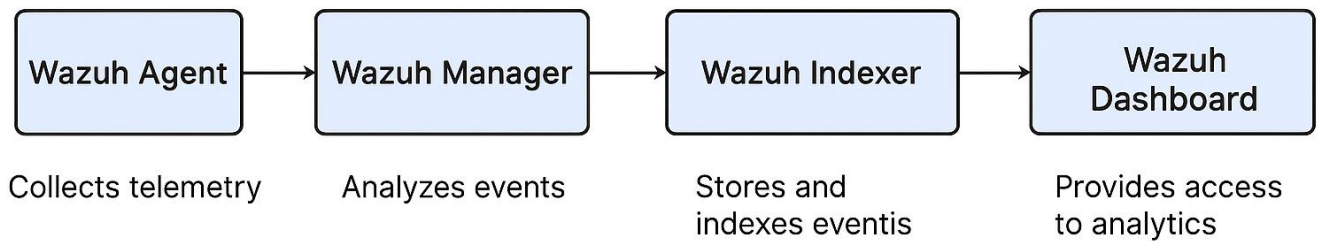


Рис. 2.3 – Робота системи.

Цей ланцюжок формує повноцінну систему моніторингу безпеки з можливістю виявлення, кореляції й реагування на загрози у реальному часі.

2.3 Механізми збору, обробки та кореляції подій безпеки в системі Wazuh

Функціонування платформи Wazuh ґрунтується на комплексній обробці широкого спектра подій безпеки, які надходять із кінцевих вузлів, мережних пристроїв, хмарних сервісів, контейнеризованих середовищ тощо. Архітектура платформи передбачає наскрізний конвеєр обробки телеметрії — від збору даних агентами до аналізу, кореляції, індексації та подальшої візуалізації — що у сукупності забезпечує можливість раннього виявлення загроз, автоматизації реагування та формування цілісної аналітичної картини подій у середовищі організації. Такий підхід визначений у офіційній архітектурі Wazuh як основа функціонування системи моніторингу безпеки [11].

Збір подій. Процес збору даних у Wazuh реалізується переважно через Wazuh Agent, який працює на кінцевих вузлах і забезпечує отримання детальної телеметрії з операційної системи та прикладних сервісів. Агент інтегрується з широким набором системних механізмів журналювання (Windows EventLog, Linux Audit, Sysmon, journald, macOS Unified Logging тощо), отримуючи події про автентифікацію, зміни конфігурацій, запуск процесів, мережеву активність, файлові операції, події ядра, стан служб, поведінкові індикатори активності та ін. [13].

Архітектура агента передбачає модульність: кожен модуль виконує певну

функцію (моніторинг цілісності файлів FIM, аудит конфігурацій SCA, виявлення rootkit-ів, збір логів, Active Response тощо). Завдяки цьому агент не просто ретранслює події — він здійснює локальну попередню фільтрацію, нормалізацію та узгодження формату даних, що знижує навантаження на центральний сервер [13].

Окрім агентів, платформа підтримує механізми безагентного збору даних (через Syslog, SSH, API-запити), що дозволяє отримувати журнали з мережевих пристроїв, систем, на які не можна встановити агент, та хмарних сервісів [12].

Таким чином, механізм збору подій в Wazuh охоплює як серверні, так і робочі станції, IoT-пристрої, мережеві компоненти, Kubernetes-кластери, Docker-контейнери, обчислювальні ресурси у хмарних середовищах, що відповідає концепції універсальної XDR/SIEM-платформи [16].

Декодування та нормалізація даних. Отримані події надходять до Wazuh Server (Manager), який виконує первинну інтелектуальну обробку. Сервер використовує механізми декодування для вилучення структурованих полів зі складних журналів, уніфікує формати подій, проводить контекстуалізацію та додає метадані про агент, систему, час, тип джерела та інші характеристики [15].

Нормалізація є критично важливою, оскільки різні ОС і застосунки генерують події у несумісних форматах. Wazuh приводить їх до єдиного внутрішнього стандарту, що дозволяє застосовувати універсальні правила аналізу та забезпечує узгодженість подій при подальшій кореляції [11].

Аналіз та застосування правил. Після нормалізації дані проходять через механізм застосування правил (Rules Engine). Wazuh Manager порівнює події зі значним набором правил, які описують:

- ознаки спроб підбору паролів;
- ескалацію привілеїв;
- зміну системних файлів;
- підозрілу мережеву активність;
- некоректну поведінку процесів;
- аномальні операції користувачів;
- події, пов'язані з malware-активністю;
- невідповідність політикам безпеки.

Правила у Wazuh згруповані у набір політик, які відповідають різним сценаріям:

відповідності нормативам, аудит конфігурацій, моніторинг активності користувачів, виявлення інцидентів. Сервер може оцінювати події у контексті, аналізуючи як окремі журнали, так і їхню історичну послідовність [15].

Кореляція подій. Кореляція подій у Wazuh здійснюється шляхом співставлення:

- часових залежностей,
- поведінкових шаблонів,
- зв'язків між подіями на одному або різних вузлах,
- змін у конфігураціях та файлах,
- логічної послідовності дій користувачів або процесів.

Кореляційний механізм дає змогу ідентифікувати інциденти, які проявляються як ланцюг подій: неуспішні спроби входу → успішний логін → зміна прав → модифікація конфігурацій → запуск підозрілих процесів.

Такі атаки важко розпізнати в межах одиничних подій, але Wazuh здатна встановити їх зв'язок, формуючи єдину структуру інциденту [15].

У кластерних розгортаннях процес кореляції розподіляється між кількома менеджерами, що забезпечує масштабованість та високу продуктивність платформи у великих середовищах [18].

Зберігання та індексація. Нормалізовані події, результати аналізу та попередження передаються до Wazuh Indexer, де вони зберігаються та індексуються. Це дає можливість виконувати:

- повнотекстовий пошук,
- агрегацію історичних даних,
- кореляційні запити,
- аналіз тенденцій,
- побудову аналітичних звітів,
- forensic-розслідування.

Індексатор працює як високопродуктивний пошуковий механізм, оптимізований для великих обсягів даних, що відповідає загальній концепції Wazuh як SIEM/XDR-рішення [12, 14].

Візуалізація та управління. Усі результати аналізу та кореляції відображаються в Wazuh Dashboard, який забезпечує:

- моніторинг стану безпеки в реальному часі;

- перегляд подій, інцидентів та детальних алертів;
- управління агентами;
- контроль політик;
- налаштування правил;
- генерацію звітів і графічних аналітичних панелей.

Dashboard виступає як центр операцій безпеки (SOC console) і забезпечує зручну взаємодію з даними та компонентами платформи [17].

Механізми Wazuh для збору, обробки та кореляції подій створюють цілісний, багаторівневий процес виявлення загроз: від локальної фільтрації й початкового аналізу на агенті до глибокої кореляції на рівні сервера, індексації та аналітики через Dashboard. Усі ці процеси органічно поєднуються в єдину архітектуру, що відповідає сучасним вимогам до відкритих SIEM/XDR-платформ, забезпечуючи гнучкість, масштабованість та повну прозорість подій безпеки у будь-якій інфраструктурі.

2.4. Інтеграція Wazuh із зовнішніми джерелами даних (Firewalls, IDS/IPS, Cloud-сервіси)

Інтеграція із зовнішніми джерелами даних є фундаментальною частиною функціональності Wazuh як сучасної SIEM/XDR-платформи. Завдяки відкритій архітектурі та розгалуженій системі декодерів і правил Wazuh здатний приймати, нормалізувати та аналізувати журнальні дані з широкого спектра пристроїв та сервісів, що охоплюють більшість сегментів корпоративної інфраструктури — мережевий рівень, серверні та хмарні середовища, системи моніторингу доступу, засоби захисту периметра та платформи виявлення вторгнень. Такий підхід дозволяє створити єдине середовище, де всі події безпеки взаємопов'язані та можуть бути комплексно проаналізовані з урахуванням контексту, походження, критичності та взаємозв'язків [11, 14].

Інтеграція з мережевим обладнанням та Firewalls. Системи мережевої безпеки, серед яких міжмережеві екрани, маршрутизатори, VPN-шлюзи та інші пристрої периметра, є одним із найважливіших джерел даних, що дозволяють виявляти спроби порушення політик безпеки на ранніх етапах. Більшість таких пристроїв підтримує

протоколи **Syslog**, **CEF**, **LEEF** або нативні формати, які можуть бути передані до Wazuh Manager через мережу. Wazuh, маючи підтримку різноманітних форматів логів, виконує автоматичну нормалізацію даних шляхом застосування набору декодерів, правил аналізу та кореляційних механізмів[12].

До типових типів даних, що надходять від мережевих пристроїв, належать:

- інформація про заблоковані або дозволені з'єднання;
- повідомлення про перевищення лімітів трафіку;
- фіксація підозрілих шаблонів звернень до внутрішніх ресурсів;
- аномалії активності користувачів VPN або адміністраторів;
- спроби сканування портів і зміну правил NAT;
- повідомлення про виконання політик доступу до різних сегментів мережі.

Після потрапляння таких подій до Wazuh Manager система застосовує механізми аналізу та визначення рівня критичності, а у випадку підтвердження загроз — може автоматично ініціювати відповідні заходи реагування (Active Response), такі як блокування IP-адреси, відключення сесії VPN або створення запису в брандмауері для тимчасового обмеження доступу [15]. Важливо, що Wazuh дозволяє комбінувати події від firewalls із подіями, отриманими від Wazuh Agent на хостах, що значно підвищує точність кореляції та дозволяє визначати шкідливу активність уже в момент її появи [13].

Інтеграція з IDS/IPS системами. Інтеграція Wazuh із системами запобігання та виявлення вторгнень (IDS/IPS), такими як **Suricata**, **Snort**, **Zeek**, є важливою складовою побудови глибокої, багаторівневої системи безпеки. IDS/IPS-рішення аналізують мережевий трафік у реальному часі та формують події, що безпосередньо вказують на спроби сканування, використання вразливостей, експлоїтацію протоколів або несанкціоновані дії з боку внутрішніх чи зовнішніх суб'єктів [12, 16].

Wazuh приймає журнали IDS/IPS кількома методами:

- через Syslog-потік;
- через агрегацію логів із файлової системи;
- через маршрутизацію подій за допомогою локального агента;
- через інтеграцію із зовнішніми брокерами журналів (наприклад, Filebeat або Fluentd).

На етапі аналізу Wazuh застосовує спеціальні декодери, оптимізовані під структуру логів Suricata та Snort. Завдяки цьому отримані події збагачуються метаданими: інформацією про протокол, тип атаки, класифікацію, CIDR-діапазон атакуючої адреси, а також можливим посиланням на CVE, якщо загроза відповідає конкретній вразливості [15].

Особливою перевагою такої інтеграції є можливість побудови кореляцій між IDS-сповіщеннями та подіями на рівні хостів. Наприклад, якщо IDS фіксує спробу проведення SQL Injection на певний веб-сервер, Wazuh може автоматично перевірити журнали цього сервера за період інциденту та виявити, чи відбулися підозрілі зміни файлів, підвищення привілеїв або виконання нетипових команд через оболонку [13, 15]. Це фактично створює повноцінний XDR-підхід, де мережевий та хостовий рівні працюють як єдина система.

Інтеграція з хмарними платформами та сервісами. З огляду на стрімку міграцію корпоративних середовищ у хмару інтеграція із сервісами AWS, Azure та Google Cloud стала одним із ключових напрямів розвитку Wazuh. Платформа включає окремі модулі для збору подій з:

- AWS: CloudTrail, GuardDuty, Config, VPC Flow Logs, ELB Logs;
- Azure: Activity Logs, AD Sign-In Logs, Security Center Alerts;
- GCP: Audit Logs, VPC Flow Logs, Cloud Armor Events.

Wazuh забезпечує централізацію цих подій у єдиному сховищі та подальшу їхню кореляцію із даними від локальних систем, мережевих пристроїв та інфраструктурних елементів [16]. Такий підхід надає можливість побудови цілісного бачення безпекової ситуації як в хмарі, так і у внутрішньому середовищі підприємства.

Наприклад, подія *AWS CloudTrail*, яка фіксує створення нового IAM-користувача, може бути автоматично поєднана з подіями входу в систему на локальних серверах через VPN, а також із подіями зміни конфігурацій на хостових агентах. Це дозволяє виявляти складні атаки, що охоплюють як хмарні, так і локальні компоненти інфраструктури [11, 18].

Крім того, Wazuh надає аналітичні панелі в Wazuh Dashboard для AWS, Azure та GCP, які дозволяють візуалізувати найважливіші метрики:

- активність користувачів у хмарному середовищі;
- підозрілі спроби доступу;
- зміни у конфігураціях;
- мережеву активність між хмарними компонентами.

Таким чином, Wazuh виконує роль універсального шлюзу між хмарним середовищем та локальною інфраструктурою підприємства, забезпечуючи централізоване управління подіями безпеки.

Інтеграція з поштовими серверами, проксі та системами контролю доступу. Окрім класичного мережевого обладнання та хмарних сервісів, Wazuh активно використовується для збору журналів зі служб, що забезпечують контроль доступу користувачів, моніторинг активності на периметрі та управління трафіком. До таких систем належать поштові сервери (Postfix, Exchange, Zimbra), веб-проксі (Squid, Blue Coat), системи автентифікації (Radius, LDAP), а також засоби контролю фізичного доступу до приміщень.

Більшість цих сервісів генерує журнали у стандартному текстовому форматі, що дозволяє Wazuh без додаткових налаштувань здійснювати їх обробку за допомогою модулів Filebeat або власних механізмів моніторингу логів (*Localfile*). У процесі інтеграції Wazuh автоматично визначає критичні події, такі як:

- багаторазові невдалі спроби входу до поштового сервера або домену;
- спроби надсилання великої кількості листів із нетипових IP-адрес (ознаки спаму чи компрометації поштової скриньки);
- підозрілі HTTP-запити, що проходять через проксі-сервери (наприклад, звернення до відомих C2-серверів);
- зміни у конфігурації облікових записів користувачів у LDAP або AD;
- несанкціоновані спроби доступу до внутрішніх ресурсів підприємства.

Усі ці події після нормалізації збагачуються інформацією про користувача, IP-адресу, пристрій, геолокацію або політику, яка була порушена. Далі Wazuh виконує кореляцію між подіями на різних рівнях — наприклад, якщо користувач спробував зайти у корпоративну пошту зі скомпрометованої IP-адреси, система автоматично перевірить інші журнали щодо цієї IP-адреси, включаючи дані firewall, VPN, IDS та агентів на хостах [12], [14].

Підтримка інтеграції через API та вебхуки. Окрім стандартної агрегації журналів, Wazuh підтримує отримання подій через REST API та вебхуки. Це дозволяє інтегрувати платформу з сучасними корпоративними сервісами, зокрема SIEM-подібними рішеннями або автоматизованими платформами SOAR.

Наприклад, сучасні SaaS-сервіси — GitHub, GitLab, Okta, CrowdStrike, Jira та інші — використовують вебхуки для передачі критичних подій безпеки у зовнішні системи. Wazuh може отримувати такі повідомлення, парсити їх за допомогою спеціалізованих декодерів та формувати події для подальшого аналізу.

Таким чином, платформа фактично перетворюється на універсальний хаб, здатний приймати структуровані JSON-повідомлення та включати їх у загальний потік подій для кореляції [15].

Побудова комплексних кореляцій у багатоджерельному середовищі. Однією з ключових причин широкої популярності Wazuh є можливість створювати кореляційні правила, які враховують події з різних зовнішніх джерел одночасно. Наприклад, у рамках єдиного інциденту Wazuh може:

1. зафіксувати, що IDS/IPS (Suricata) виявила мережеву атаку на веб-сервер;
2. отримати від firewall подію про те, що IP-адреса атакувала й інші вузли в мережі;
3. від агента на веб-сервері — подію про спробу модифікації файлів у директорії веб-додатка;
4. від хмарної платформи AWS — факт підозрілої активності в IAM (наприклад, створення ключів доступу після атаки).

У таких випадках Wazuh створює складну кореляцію, що дозволяє не лише підтвердити факт атаки, але й оцінити її масштаб і ймовірні наслідки. Це відповідає концепції XDR (Extended Detection and Response), яку офіційно підтримує платформа [16].

Інтеграція з системами контролю цілісності та керування вразливостями. Wazuh може працювати разом із зовнішніми системами контролю цілісності файлів, інструментами моніторингу конфігурацій або платформами для управління вразливостями (наприклад, OpenVAS, Nessus). Через інтеграцію журналів та API Wazuh отримує результати сканування вразливостей, які далі поєднуються з даними з

агента про фактичний стан системи:

- які пакети встановлено чи оновлено;
- які файли були змінені;
- чи є збіг хешів із відомими IOC;
- чи застосовано останні патчі.

У результаті формується повний цикл моніторингу — від виявлення вразливості до контролю фактичного її усунення [13].

Роль Wazuh Dashboard у роботі з інтегрованими даними. Отримані з різних джерел журнали та події структуруються й відображаються у Wazuh Dashboard, який забезпечує:

- дашборди для окремих інтеграцій (AWS, Suricata, Firewall тощо);
- аналіз часових шкал інцидентів;
- побудову графічних залежностей між подіями;
- перегляд детальних логів у текстовому та структурованому вигляді;
- фільтрацію подій за усіма метаданими (IP, користувач, регіон, сервіс);
- експорт даних для проведення форензики або подальшої обробки [17].

Таким чином, Dashboard виступає центральною точкою для взаємодії аналітиків із зібраними подіями, дозволяючи не лише виявляти інциденти, а й проводити постінцидентне розслідування.

Додаткові можливості інтеграції. Слід підкреслити, що Wazuh підтримує також:

- інтеграцію з Kubernetes (через модулі K8s Audit Log Collector);
- збір журналів Docker-контейнерів;
- імпорт подій із систем CI/CD (Jenkins, GitLab CI);
- моніторинг систем резервного копіювання та віртуалізації (Veeam, VMware);
- отримання IOC (Indicators of Compromise) зі зовнішніх threat intelligence-платформ.

Це робить платформу надзвичайно гнучкою та придатною для розгортання у великих гібридних середовищах, де події можуть надходити з десятків різних джерел. А завдяки кластерній архітектурі Wazuh може масштабуватися, обробляючи сотні гігабайт журналів на добу [18].

2.5. Механізми реагування на інциденти: правила, дії, автоматизація (Active Response)

Механізми реагування на інциденти у системі Wazuh є ключовим елементом її функціоналу як платформи класу SIEM/XDR. Основна мета цих механізмів полягає у забезпеченні можливості не лише виявляти потенційні загрози, а й оперативно здійснювати контрдії з метою мінімізації шкоди, локалізації інцидентів та відновлення безпечного стану інформаційної системи. Компоненти, відповідальні за реагування, тісно інтегровані з підсистемами збору подій, кореляції та аналізу, що дозволяє реалізувати повний цикл Incident Response у рамках єдиної платформи [13, 15].

У центрі механізмів реагування Wazuh лежить система правил (rules engine), яка аналізує події, що надходять від агентів або зовнішніх джерел. Кожна подія порівнюється з набором правил, які описують сигнатури загроз, аномальну поведінку, невідповідність політикам безпеки або індикатори компрометації. Якщо певне правило спрацює, воно створює alert, що містить структуровану інформацію про інцидент. На основі цього alert можуть бути виконані відповідні дії реагування, серед яких найважливішою є функціональність Active Response [13, 15].

Active Response — це механізм виконання автоматизованих або напівавтоматизованих дій на заражених чи потенційно скомпрометованих хостах. Він може бути використаний як для миттєвого блокування шкідливих процесів, IP-адрес і користувачів, так і для виконання складніших сценаріїв, включно з відновленням конфігурацій, закриттям портів або запуском сторонніх скриптів. Активні дії виконуються агентом Wazuh безпосередньо на контрольованій системі, що дозволяє реагувати максимально швидко та мінімізувати затримки, властиві централізованим моделям реагування [13].

Важливим аспектом є можливість розмежування рівня автоматизації. У Wazuh доступні три основні форми реагування:

1. Повністю автоматизоване реагування, коли Active Response виконується відразу після спрацювання правила;
2. Напівавтоматизоване реагування, що вимагає підтвердження оператора через Dashboard;
3. Ручне реагування, коли аналітик ініціює Active Response вручну,

спираючись на інформацію, отриману з панелі моніторингу або журналів [17].

Це забезпечує баланс між швидкістю реагування та контролем над критичними діями, що є важливим у високоризикових середовищах. До прикладу, блокування IP-адреси потенційного брутфорс-актора може бути повністю автоматизованим, тоді як зупинка процесів або зміна конфігурацій ОС — виконуватися лише після підтвердження фахівця з безпеки.

Механізм Active Response працює у тісній взаємодії з іншими компонентами Wazuh. Дані, зібрані модулями FIM (File Integrity Monitoring), SCA (Security Configuration Assessment), лог-модулями або IDS/IPS інтеграціями, можуть генерувати події, які запускають активні дії [11, 13]. Наприклад, якщо FIM виявляє несанкціоновану зміну системних файлів, Wazuh може автоматично відновити їх з резервної копії або обмежити доступ до системи, запобігаючи подальшому компрометуванню. Аналогічно, якщо SCA виявляє критичне порушення політики, система може виконати попереджувальні заходи або ізолювати хост.

Окрему роль відіграє взаємодія Active Response з інфраструктурою threat intelligence, що інтегрована у Wazuh Server [15]. Система здатна порівнювати IP-адреси, хеші файлів і домени, виявлені у подіях, з базами ІОС. Якщо відповідність знайдено, Active Response може застосувати захисні заходи: заблокувати з'єднання, припинити роботу процесу або видалити шкідливий файл. Це дозволяє Wazuh працювати не лише з реактивними сценаріями, але й як активний засіб попередження загроз.

Архітектура Wazuh також забезпечує можливість масштабованого реагування у кластерних середовищах, що особливо актуально для великих організацій з розподіленою інфраструктурою. Використання кластерного Wazuh Manager дозволяє рівномірно розподіляти навантаження, прискорюючи обробку подій і ініціювання активних дій реагування у середовищах з великою кількістю агентів [18]. Це забезпечує стабільність, надійність та узгодженість реакцій у реальному часі.

Таким чином, механізми реагування в Wazuh формують комплексну багаторівневу систему захисту, здатну поєднувати виявлення загроз, аналітику, кореляцію та контрдії у межах єдиного рішення. Завдяки Active Response, аналітики отримують можливість оперативно блокувати атаки, автоматизувати рутинні операції та ефективно управляти інцидентами без необхідності постійного ручного втручання.

Висока гнучкість налаштування, підтримка кастомних скриптів, інтеграція з іншими інструментами ІБ та розширюваність роблять Wazuh потужним інструментом для побудови сучасної системи реагування на кіберінциденти [13, 15, 17]

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА БАЗІ ПЛАТФОРМИ WAZUH

3.1 Розроблення архітектури системи виявлення та реагування інформаційної безпеки на базі Wazuh.

Для реалізації архітектури було обрано спосіб розгортання за допомогою Wazuh OVA Appliance[19], який представляє собою попередньо налаштований образ віртуальної машини з інтегрованими компонентами Wazuh Manager, Wazuh Indexer і Wazuh Dashboard. Такий підхід забезпечує швидке розгортання та мінімізує ризик конфігураційних помилок, що є критично важливим при побудові системи безпеки.

Віртуальна машина була імпортована у середовище VirtualBox та налаштована відповідно до рекомендованих технічних характеристик (4 ядра CPU, 8 ГБ RAM, 50 ГБ диска).

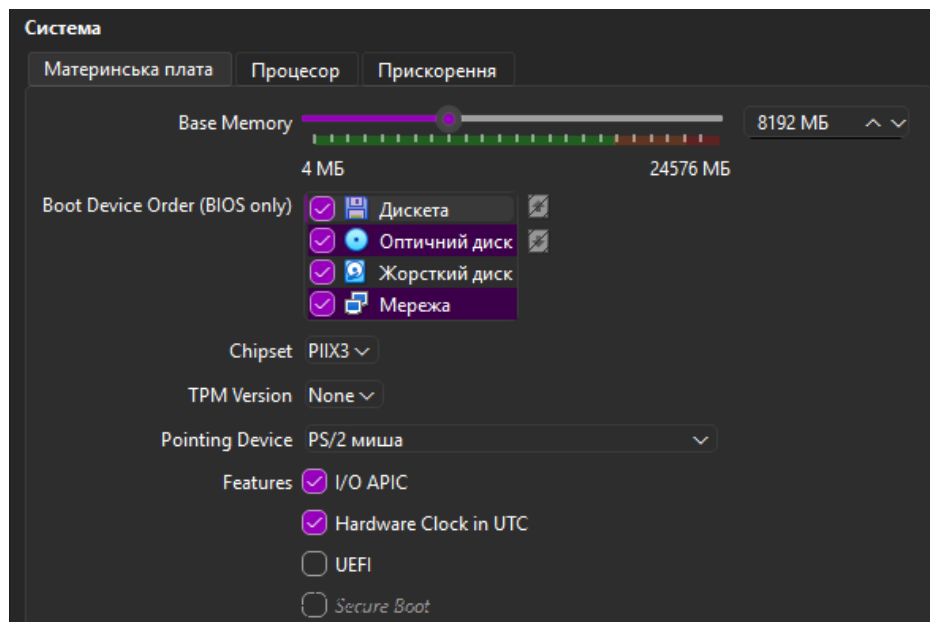


Рис. 3.1 – Налаштування ресурсів віртуальної машини (RAM).

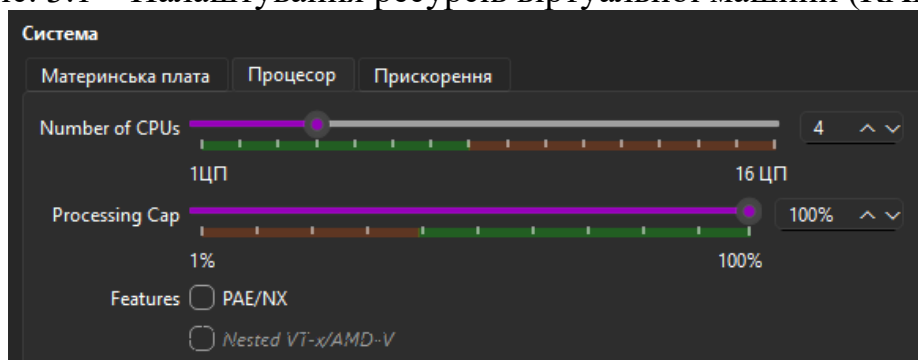


Рис. 3.2 – Налаштування ресурсів віртуальної машини (CPU).

Для забезпечення можливості підключення агентів до менеджера, мережевий інтерфейс віртуальної машини потрібно перевести в режим **Bridged Adapter**, тобто Мережевий міст; це дозволяє віртуальній машині отримати адресу в тій же мережі, що і робочі станції, що значно спрощує інтеграцію Wazuh Agent, але в мене ця функція відсутня, нажаль, скоріш за все через проблеми Windows 11 з даним типом підключення, я пробував і власноруч створити міст, але це відключає мій пристрій від доступу до інтернету, тому мною було прийняте рішення створити схему Host-only + NAT – це стабільна і правильна схема для Windows 11:

1. Адаптер 1 — Host-only → доступ з хоста, агенти, веб-інтерфейс,
2. Адаптер 2 — NAT → інтернет (оновлення, репозиторії).

Для початку створюємо **Host-only** мережу в інструментах VirtualBox(Файл → →Інструменти → Диспетчер мереж хоста → Створити).

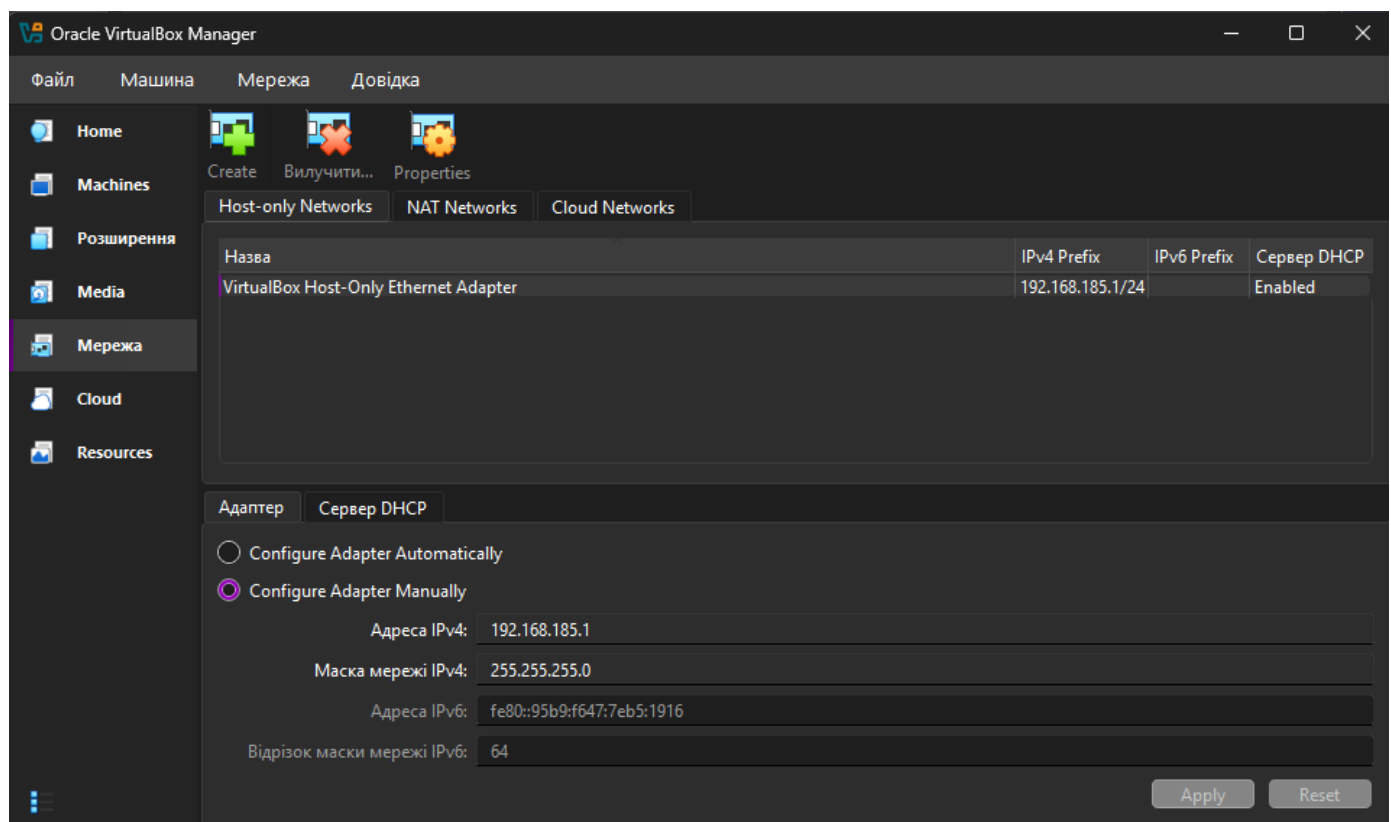


Рис. 3.3 – Диспетчер мереж хоста.

Також у вкладці Сервер DHCP, вмикаємо сервер.

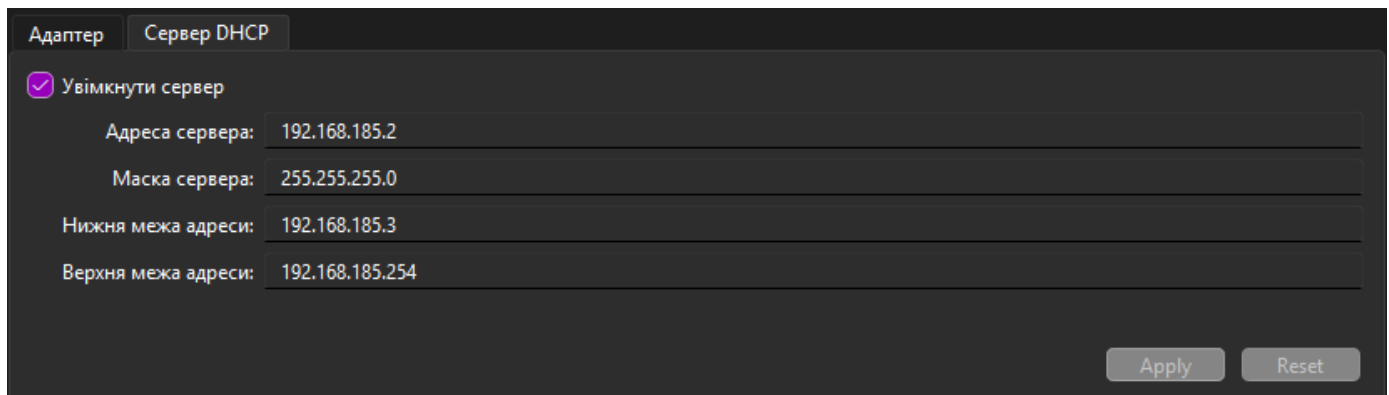


Рис. 3.4 – Вмикаємо сервер.

Далі в налаштуваннях мережі машини вмикаємо Адаптер 1 та налаштовуємо на «Лише головний адаптер», також вмикаємо Адаптер 2, налаштовуємо його на NAT.

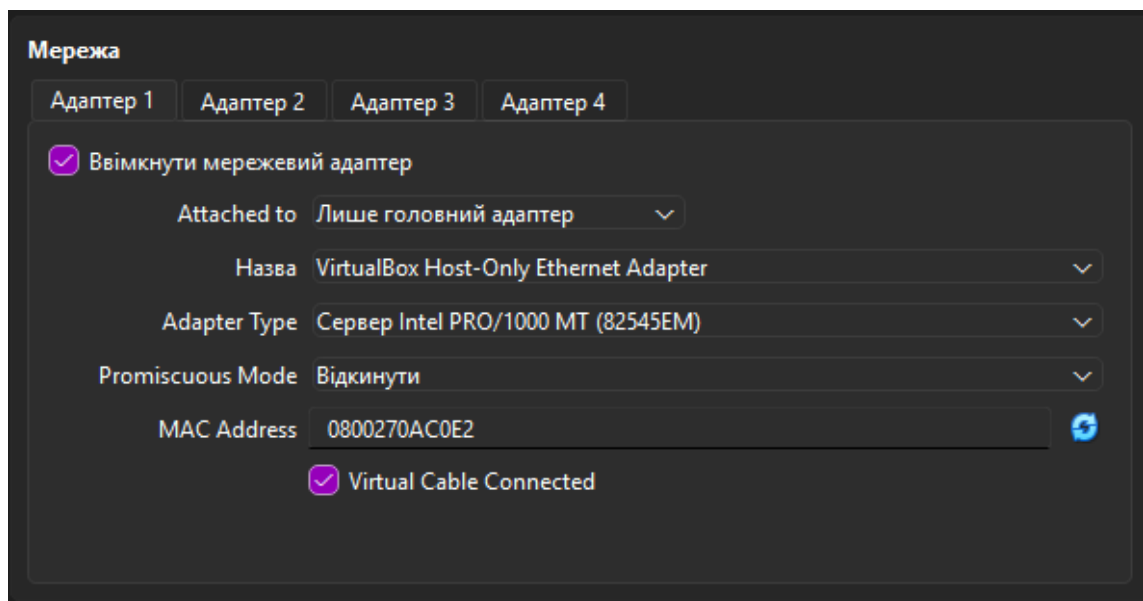


Рис. 3.5 – Налаштування Адаптер 1 (Host-only)

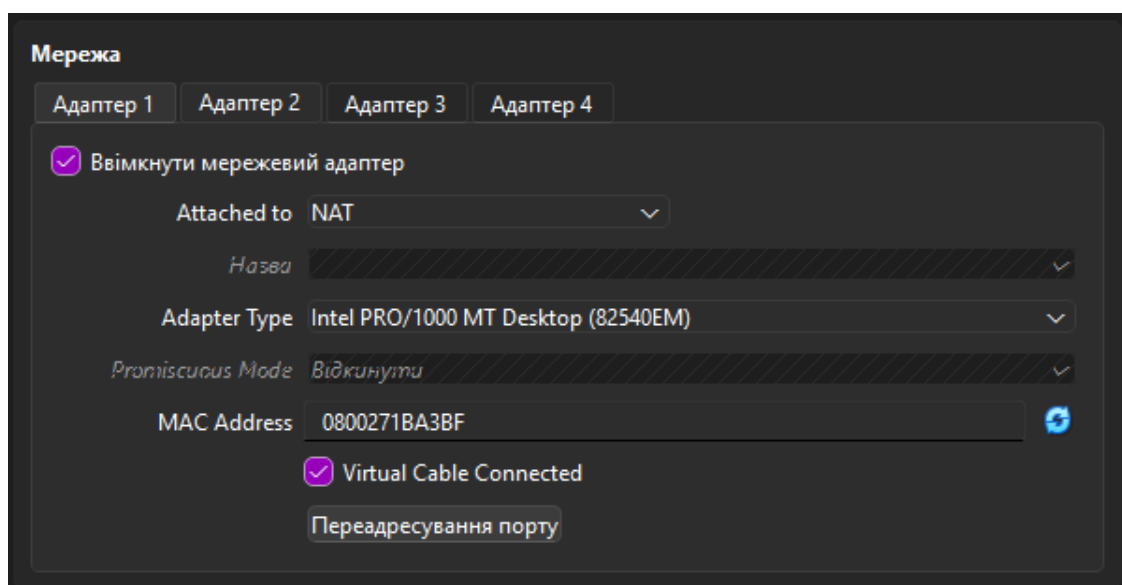


Рис. 3.6 – Налаштування Адаптер 2 (NAT)

Машина готова до запуску. Після запуску входимо в обліковий запис, якщо у вас немає свого в документації Wazuh є облікові дані «тестового» користувача:

user: wazuh-user

password: wazuh

Вхід користувача SSH root вимкнено. Користувач wazuh-user має права sudo. Щоб перейти до root-права, виконуємо наступну команду: `sudo -i`

Після входу перевіряємо IP командою: `ip a`

```
[root@wazuh-server ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:1b:a3:bf brd ff:ff:ff:ff:ff:ff
   altname enp0s8
   inet 10.0.3.15/24 metric 1024 brd 10.0.3.255 scope global dynamic eth0
       valid_lft 85940sec preferred_lft 85940sec
   inet6 fd17:625c:f037:3:a00:27ff:fe1b:a3bf/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 85943sec preferred_lft 13943sec
   inet6 fe80::a00:27ff:fe1b:a3bf/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:0a:c0:e2 brd ff:ff:ff:ff:ff:ff
   altname enp0s17
   inet 192.168.185.3/24 metric 1024 brd 192.168.185.255 scope global dynamic eth1
       valid_lft 440sec preferred_lft 440sec
   inet6 fe80::a00:27ff:fe0a:c0e2/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

Рис. 3.7 – Результати команди `ip a`

На даному знімку екрану бачимо адресу Host-only – 192.168.185.3, та NAT – 10.0.3.15.

Перевіряємо зв'язок з хостом командою: `ping 192.168.185.1`

```
[root@wazuh-server ~]# ping 192.168.185.1
PING 192.168.185.1 (192.168.185.1) 56(84) bytes of data.
64 bytes from 192.168.185.1: icmp_seq=1 ttl=128 time=0.498 ms
64 bytes from 192.168.185.1: icmp_seq=2 ttl=128 time=1.74 ms
64 bytes from 192.168.185.1: icmp_seq=3 ttl=128 time=1.28 ms
64 bytes from 192.168.185.1: icmp_seq=4 ttl=128 time=1.10 ms
^C
--- 192.168.185.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3018ms
rtt min/avg/max/mdev = 0.498/1.154/1.736/0.443 ms
```

Рис. 3.8 – Результати команди `ping 192.168.185.1`

Також варто перевірити доступ до інтернету командою: `ping 8.8.8.8`

```

[root@wazuh-server ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=21.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=255 time=21.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=22.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=255 time=22.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=255 time=21.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=255 time=21.8 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5023ms
rtt min/avg/max/mdev = 21.756/22.016/22.735/0.340 ms

```

Рис. 3.9 – Результати команди ping 8.8.8.8

Після запуску та всіх перевірок виконуємо вхід у Wazuh Dashboard за адресою https://<IP_manager> де перевірено доступність усіх компонентів та їх готовність до подальших етапів налаштування.

Так як Wazuh Dashboard це графічний інтерфейс менеджера, до нього мають доступ тільки комп'ютери з мережевим доступом до менеджера, адміністраторів безпеки, аналітиків або тих, хто моніторить події і керує системою, через Dashboard вони бачать всі підключені агенти, події, алерти, виконані реакції та статистику, тобто моніторинг і аналіз централізований.

У мене ж менеджер розгорнутий на віртуальній машині, тому мій комп'ютер, який виступає в ролі хосту, як раз має доступ до Dashboard, але цей же пристрій і виконуватиме роль агента, тобто кінцевої точки, тому варто відзначити, що Wazuh Agent не дає змоги відкривати Dashboard на кінцевих точках, а тільки відповідає за збір журналів подій, інформації про стан системи та передачу даних менеджеру. Тому в мене <IP_manager>, це IP самої машини, тобто IP хосту менеджера, як показано на Рис. 3.1.7 – 192.168.185.3.

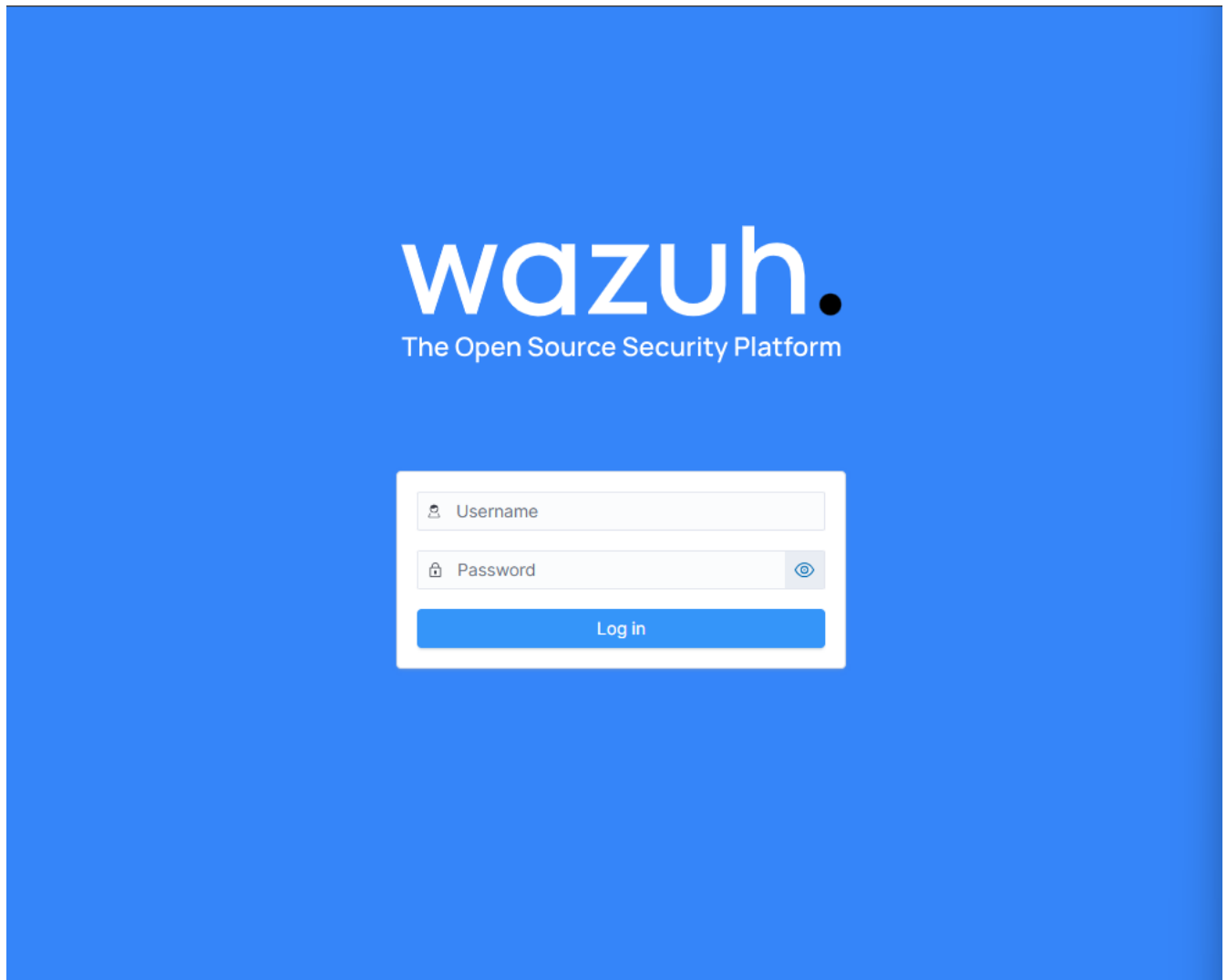


Рис. 3.10 – Сторінка авторизації Wazuh Dashboard.

У результаті виконаних кроків було сформовано повноцінну архітектуру системи виявлення та реагування на інциденти на базі Wazuh, що включає:

- центральний сервер Wazuh Manager у віртуальному середовищі;
- індексувальний кластер OpenSearch (частина OVA);
- веб-інтерфейс Dashboard для моніторингу та аналізу;
- подальше підключення агентів на кінцевих точках (описано у 3.2).

Архітектура передбачає, що Wazuh Agent на кінцевих системах передає журнали подій та іншу інформацію безпеки до менеджера, після чого вона індексується, аналізується та відображається у Dashboard. Таким чином формується взаємопов'язана система моніторингу та реагування.

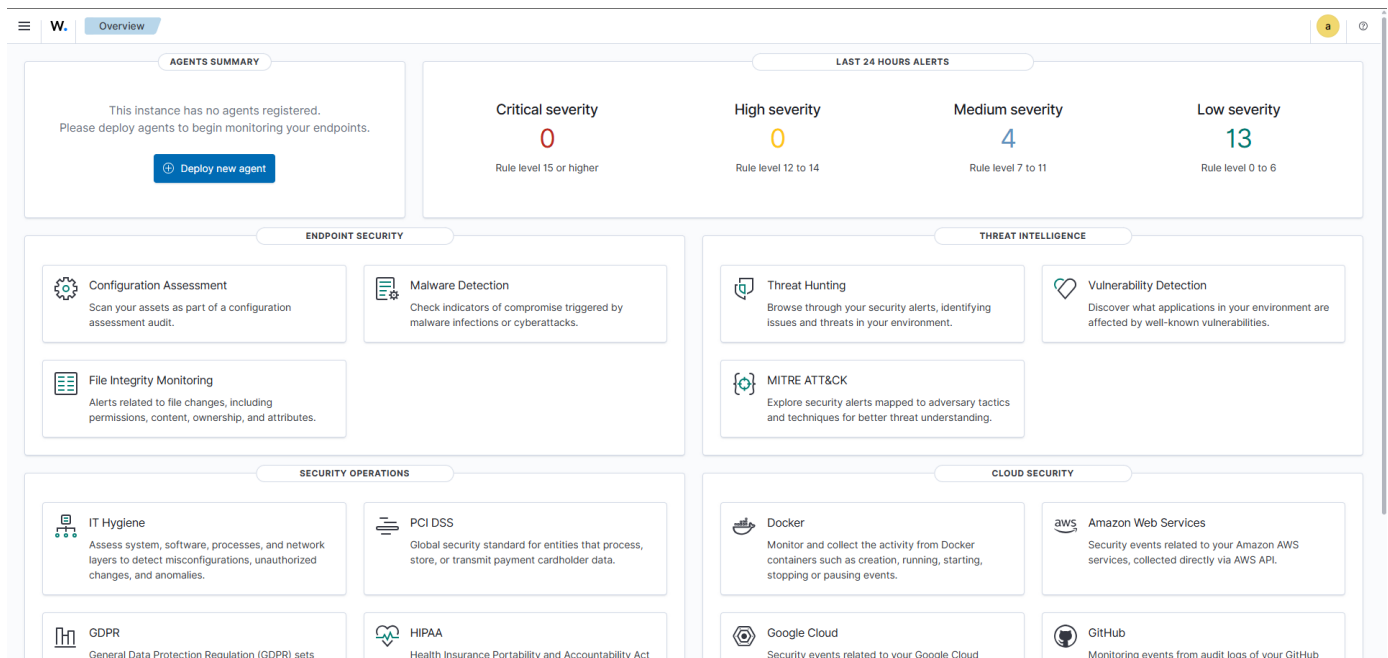


Рис. 3.11 – Головна сторінка Dashboard.

3.2 Налаштування збору логів і кореляції подій з використанням Wazuh Agent

Після розгортання архітектури системи виявлення та реагування інформаційної безпеки наступним етапом є налаштування збору логів з кінцевих точок та реалізація механізмів кореляції подій. Для цього у системі Wazuh використовується агент, який встановлюється на контрольовані вузли та забезпечує передачу інформації безпеки до центрального менеджера.

На даному етапі дослідження здійснюється налаштування механізмів збору журналів подій з кінцевих точок та їх первинної кореляції в межах системи виявлення інформаційної безпеки на базі платформи Wazuh. Основна увага приділяється роботі Wazuh Agent, який забезпечує отримання подій безпеки з операційної системи та їх подальшу передачу до централізованого менеджера для аналізу.

Вибір кінцевої точки та підготовка до встановлення агента. У рамках дипломної роботи як кінцева точка було обрано робочу станцію з операційною системою Windows, яка підлягає моніторингу. Вибір такої моделі дозволяє продемонструвати типову схему застосування Wazuh у реальному середовищі, де агент виконує роль сенсора безпеки.

Перед встановленням агента було визначено IP-адресу Wazuh Manager(192.168.185.3), яка використовується для підключення агента до

центрального сервера.

Встановлення Wazuh Agent на кінцеву систему. На підготовленій кінцевій точці було завантажено дистрибутив Wazuh Agent відповідної версії з офіційного сайту.

Після встановлення, запускаємо сам інтерфейс агента.

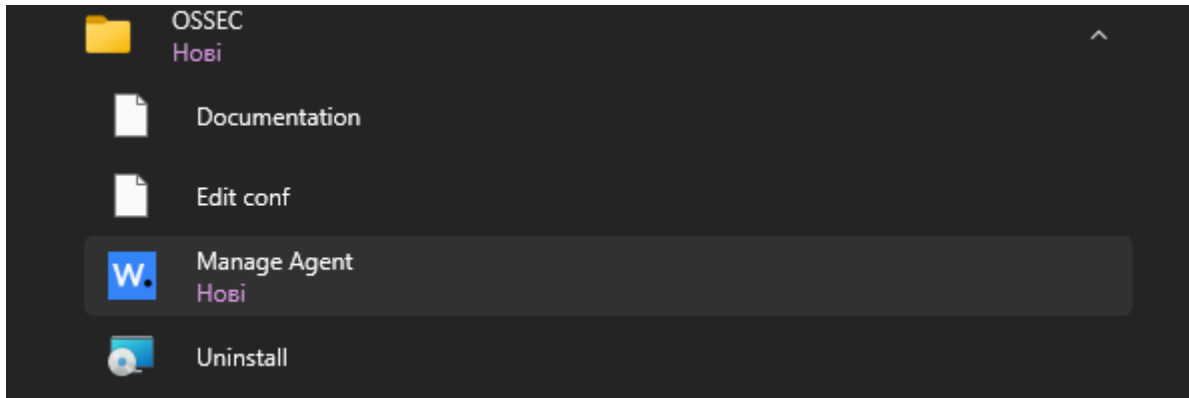


Рис. 3.12 – Знаходимо інтерфейс агента

У вікні що відкрилося вказується IP-адреса менеджера, що дозволяє агенту автоматично налаштувати мережеву взаємодію з сервером. Натискаємо кнопку “Save”.

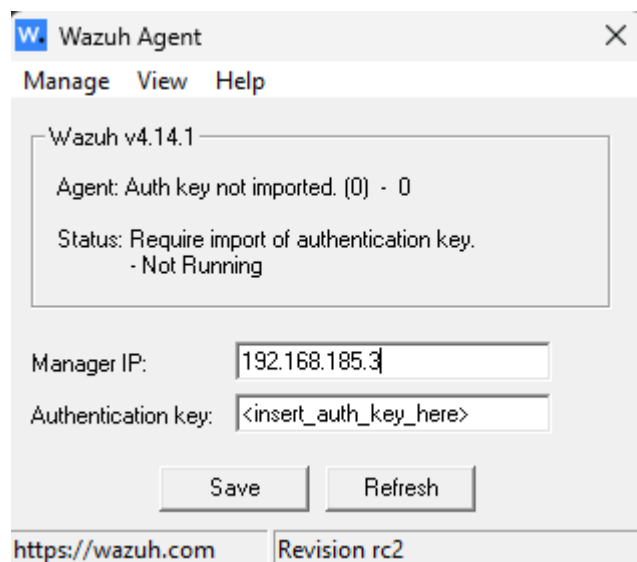


Рис. 3.13 – Вказано IP-адресу менеджера

Процес встановлення створює системну службу, яка запускається разом з операційною системою та постійно працює у фоновому режимі, забезпечуючи безперервний збір подій.

Реєстрація та підключення агента до менеджера. Після встановлення агент ініціює захищене з'єднання з Wazuh Manager та проходить процедуру реєстрації. Для підключення до менеджера, за вказаною вище IP адресою потрібно натиснути на

вкладку “Manage” → у списку вибрати функцію “Start”. У результаті агент з’являється у списку керованих вузлів у Wazuh Dashboard та отримує унікальний ідентифікатор.

Цей етап є критичним, оскільки лише зареєстровані агенти можуть передавати журнали подій та отримувати правила аналізу.

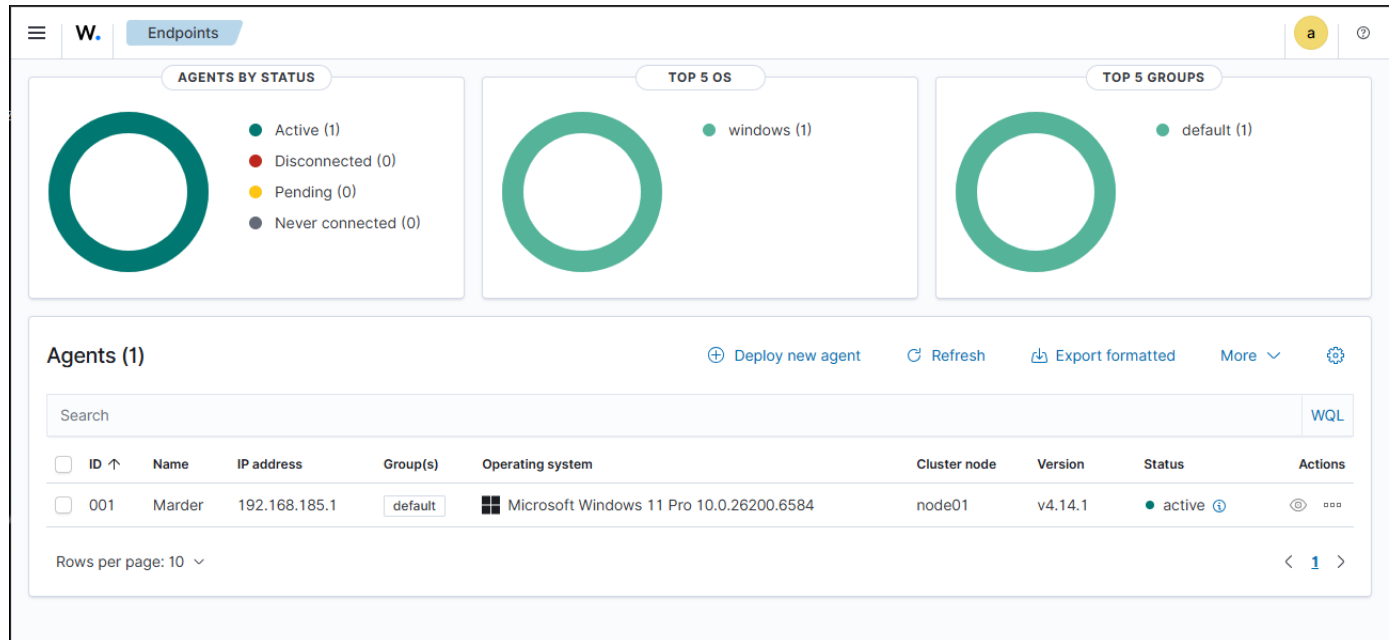


Рис. 3.14 – Відображення підключеного агента у Wazuh Dashboard (статус Active).

Налаштування збору журналів подій Wazuh Agent. Після успішного підключення Wazuh Agent до Wazuh Manager необхідно налаштувати, які саме журнали подій будуть збиратися та передаватися для аналізу. Це виконується шляхом конфігурації агенту, який здійснює локальний збір подій на кінцевій точці, через фізичне налаштування у файлі `ossec.conf`, який знаходиться за шляхом `C:\Program Files (x86)\ossec-agent\ossec.conf` але ж зазвичай адміністратори безпеки не налаштовують кожну кінцеву точку окремо, тому це можна налаштувати в Wazuh Dashboard як налаштування групи в яку поміщаються агенти, це дозволяє збирати різні логи з різних типів(груп) агентів, в залежності від конкретних вимог користувача/клієнта. Для цього переходимо в вкладку “Groups”, тут знаходиться централізоване керування конфігураціями агентів.

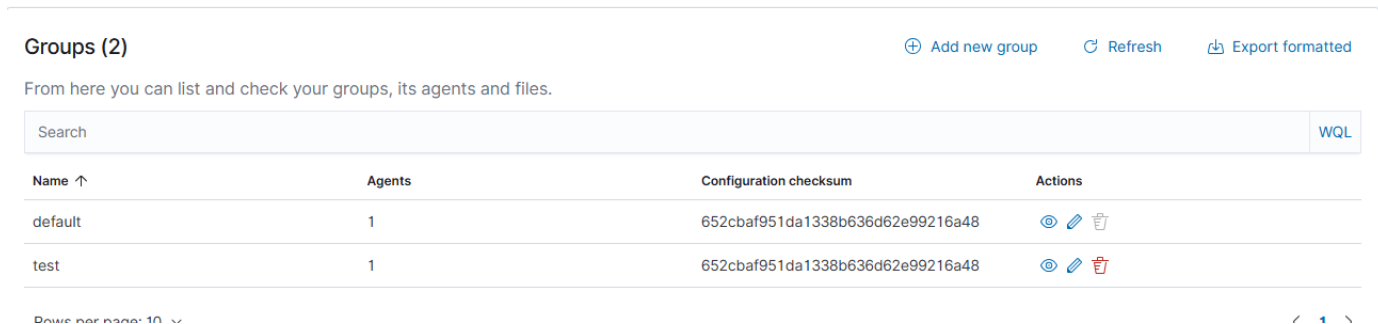


Рис. 3.15 – Groups

Далі вибираємо групу з нашими агентом, або створюємо нову та додаємо туди агент, переходимо в вкладку “Files”, та відкриваємо файл “agent.conf”.

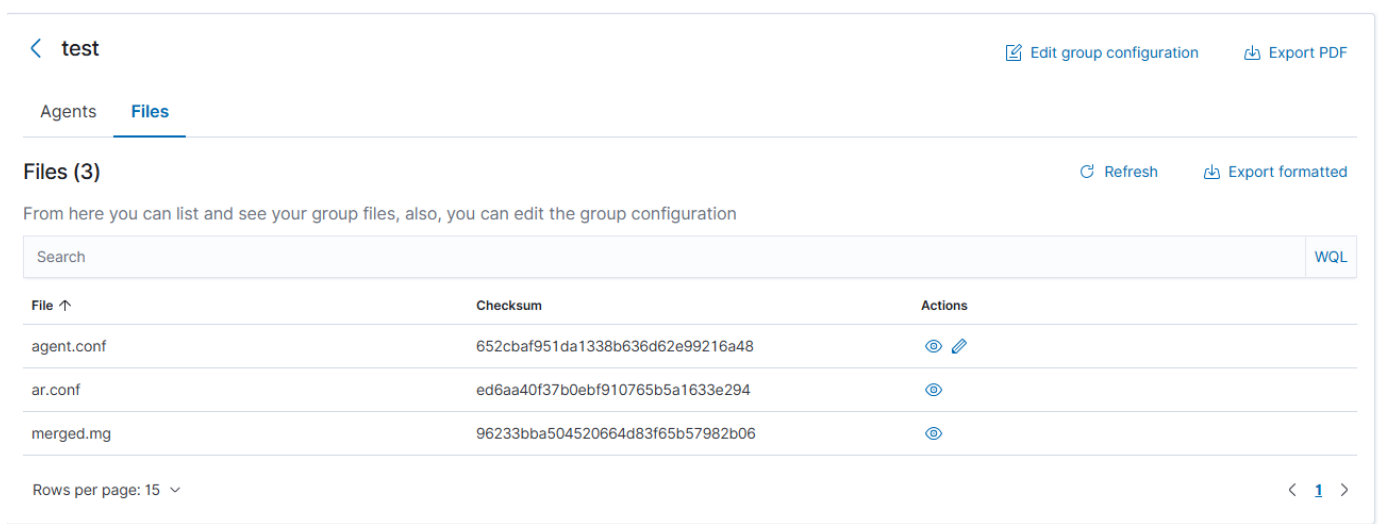


Рис. 3.16 – Перехід до конфігураційних файлів групи агентів у Wazuh Dashboard



Рис. 3.17 – Централізоване налаштування збору журналів

Даний фрагмент конфігурації визначає перелік журналів подій Windows (Security, System та Application), які Wazuh Agent повинен збирати на кінцевій точці та передавати на Wazuh Manager для подальшої кореляції та аналізу.

```

<syscheck>
  <disabled>no</disabled>
  <directories check_all="yes">C:\Windows</directories>
  <directories check_all="yes">C:\Program Files</directories>
</syscheck>

```

Даний фрагмент конфігурації активує механізм контролю цілісності файлів Wazuh Agent та визначає критичні системні каталоги, зміни в яких підлягають постійному моніторингу з метою виявлення потенційних інцидентів безпеки.

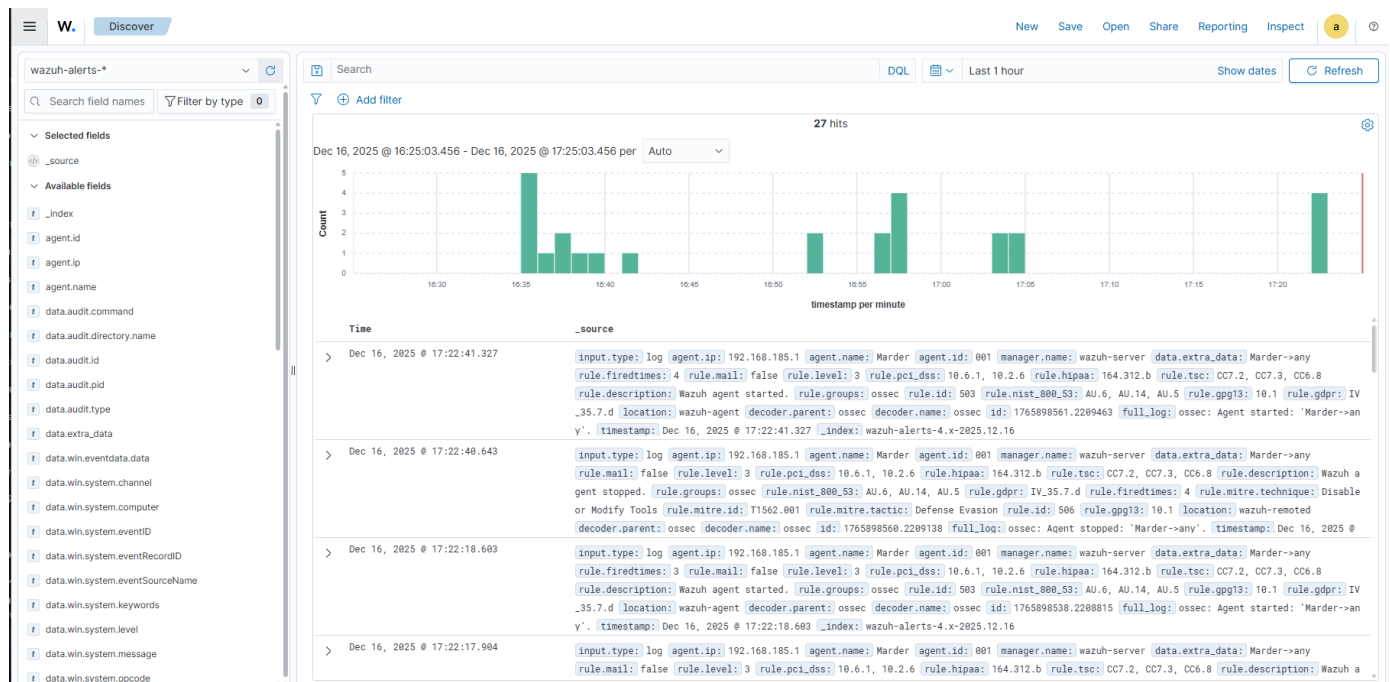


Рис. 3.18 – Результати централізованого збору логів від агента

Результати збору та первинної кореляції подій відображаються у Wazuh Dashboard, що забезпечує зручний інтерфейс для аналізу безпекових подій. Адміністратор має можливість здійснювати фільтрацію подій за агентом, часовим проміжком, типом події або іншими параметрами.

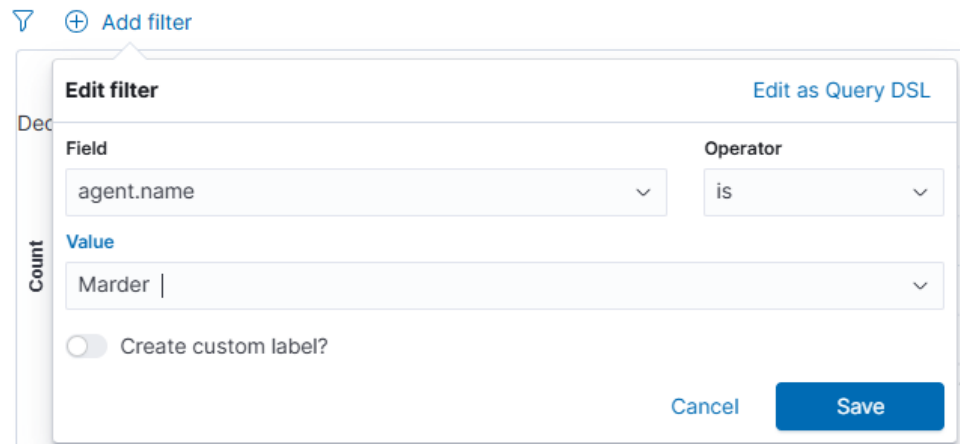


Рис. 3.19 – Додавання фільтра agent.name, для первинної кореляції

Це дозволяє оперативно оцінювати стан інформаційної безпеки кінцевих точок та формує основу для подальшої реалізації механізмів реагування на інциденти.

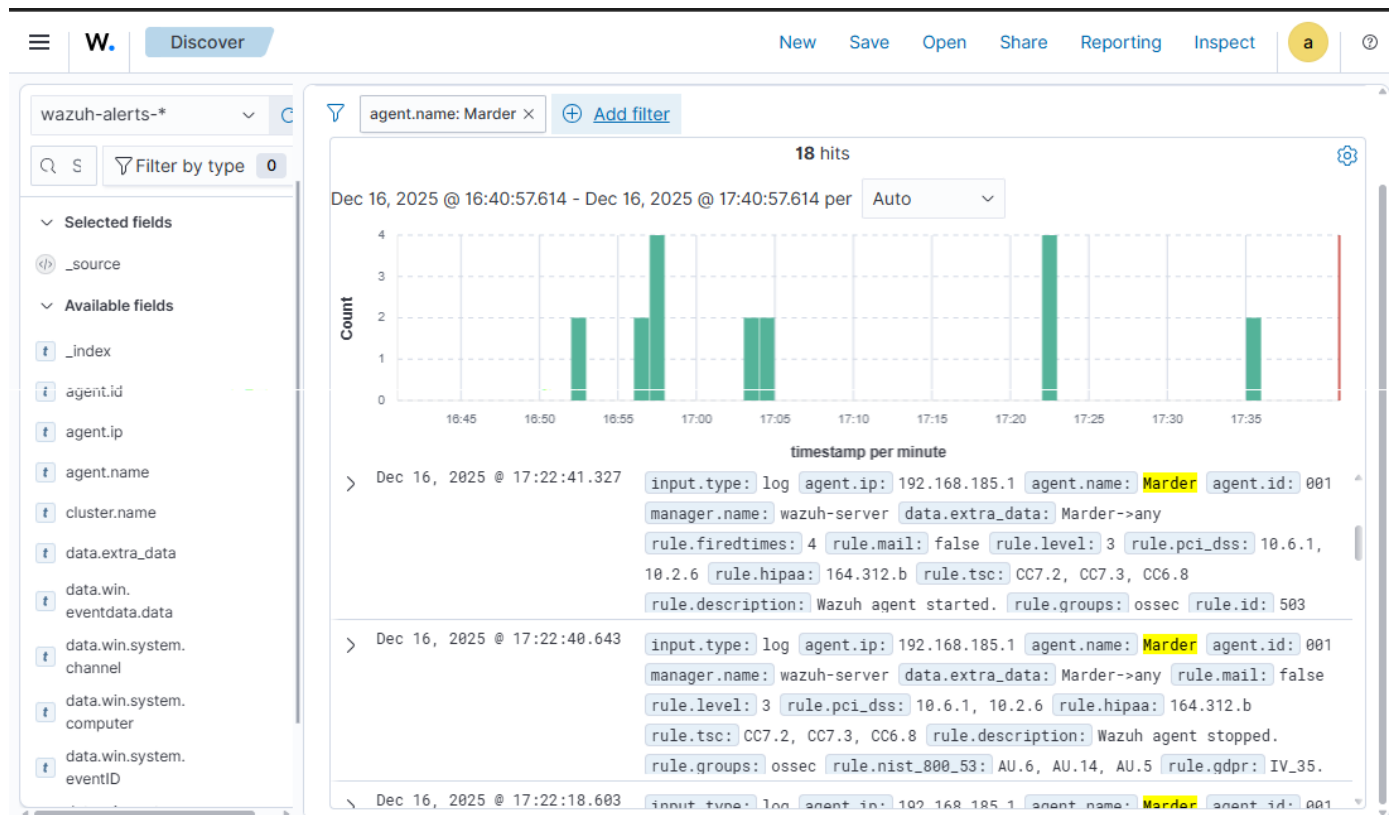


Рис. 3.20 – Відображення подій, зібраних Wazuh Agent, у Dashboard із первинною кореляцією за типом та рівнем серйозності

У результаті виконання даного етапу було налаштовано збір логів із кінцевої точки за допомогою Wazuh Agent та забезпечено їх централізовану обробку і первинну кореляцію на Wazuh Manager. Отримані результати створюють технічну основу для виявлення інцидентів інформаційної безпеки та подальшої реалізації сценаріїв реагування.

Таблиця 3.1 – Основні поля подій, зібраних Wazuh Agent та оброблених Wazuh Manager

Поле	Пояснення
timestamp	Час події
agent.ip	IP-адреса агента
agent.name	Ім'я агента (Marder)
manager.name	Ім'я менеджера, який прийняв лог
rule.id	Унікальний ідентифікатор правила, яке спрацювало
rule.level	Рівень серйозності події (0–16)
rule.groups	Категорія або група правил (ossec, syscheck тощо)
rule.description	Опис події

Дана таблиця показує тип події, рівень серйозності, ідентифікатор правила та інші ключові атрибути, які використовуються для первинної кореляції подій.

3.3 Реалізація сценаріїв реагування на інциденти безпеки (Active Response, SIEM Alerts)

На даному етапі дослідження розглядається практична реалізація механізмів реагування на інциденти інформаційної безпеки з використанням платформи Wazuh. Реагування базується на результатах кореляції подій, отриманих від агентів, та включає формування сповіщень (SIEM Alerts) і застосування автоматизованих дій реагування (Active Response).

Формування SIEM Alerts на основі корельованих подій. Після первинної кореляції подій Wazuh Manager формує SIEM Alerts для подій, які відповідають правилам безпеки з підвищеним рівнем серйозності. Алерти дозволяють оперативно виявляти потенційні інциденти та привертати увагу адміністратора до критичних подій.

У нових версіях Wazuh Dashboard (на базі OpenSearch Dashboards): немає окремого пункту “Alerts”, немає класичного SIEM Alerts як кнопки, усі алерти це записи в індексі wazuh-alerts-*

Алерт у Wazuh — це подія, яка пройшла кореляцію правилами та має рівень серйозності

Формування SIEM-алертів у Wazuh здійснюється автоматично на основі правил кореляції, а результати відображаються в інтерфейсі Wazuh Dashboard у вигляді подій безпеки в індексі `wazuh-alerts-*` (Рис. 3.18).

Аналіз інцидентів у Wazuh Dashboard. Кожен SIEM Alert містить детальну інформацію про подію, зокрема ідентифікатор агента, джерело події, опис правила, що спрацювало, та рівень ризику. Це дозволяє адміністратору виконувати первинний аналіз інциденту без необхідності звертатися до сирих журналів подій.

Використання централізованого Dashboard значно спрощує процес моніторингу та аналізу інцидентів інформаційної безпеки.



Field	Value
@timestamp	Dec 16, 2025 @ 17:58:18.167
_index	wazuh-alerts-4.x-2025.12.16
agent.id	001
agent.ip	192.168.185.1
agent.name	Marder
data.extra_data	Marder->any
decoder.name	ossec
decoder.parent	ossec
full_log	ossec: Agent stopped: 'Marder->any'.
id	1765900698.2216816
input.type	log
location	wazuh-remoted
manager.name	wazuh-server
rule.description	Wazuh agent stopped.
rule.firedtimes	5
rule.gdpr	IV_35.7.d
rule.gpg13	10.1
rule.groups	ossec
rule.hipaa	164.312.b
rule.id	506
rule.level	3
rule.mail	false
rule.mitre.id	T1562.001
rule.mitre.tactic	Defense Evasion
rule.mitre.technique	Disable or Modify Tools
rule.nist_800_53	AU.6, AU.14, AU.5
rule.pci_dss	10.6.1, 10.2.6
rule.tsc	CC7.2, CC7.3, CC6.8
timestamp	Dec 16, 2025 @ 17:58:18.167

Рис. 3.21 – Відкритий детальний перегляд одного алерту

У процесі збору журналів подій з кінцевого хоста за допомогою Wazuh Agent було зафіксовано подію зупинки служби агента (Рис. 3.21). Подія передана агентом на Wazuh Manager, де була оброблена декодером OSSEC та зіставлена з відповідним правилом кореляції.

В результаті кореляції сформовано алерт з ідентифікатором правила 506 та описом «*Wazuh agent stopped*». Алерт має рівень серйозності 3, що вказує на подію низько-середнього рівня критичності, яка потребує уваги адміністратора безпеки.

Алерт містить основні технічні параметри події, зокрема:

- ідентифікатор агента (agent.id);
- ім'я та IP-адресу хоста (agent.name, agent.ip);
- точний час виникнення події (@timestamp);
- джерело події (wazuh-remoted);
- кількість повторних спрацювань правила (rule.firedtimes).

Подія автоматично класифікована за фреймворком MITRE ATT&CK як техніка T1562.001 (Disable or Modify Tools), що відповідає спробі вимкнення або порушення роботи засобів безпеки. Додатково алерт зіставлено з контролями стандартів NIST SP 800-53, PCI DSS, GDPR та HIPAA, що забезпечує відповідність події нормативним вимогам інформаційної безпеки.

Налаштування механізмів Active Response. Після формування алерта безпеки можливе автоматизоване реагування за допомогою механізмів Active Response, що налаштовуються на сервері Wazuh. Цей механізм дозволяє виконувати заздалегідь визначені дії у відповідь на виявлені події без участі адміністратора.

До таких дій можуть належати:

- блокування IP-адреси;
- завершення підозрілого процесу;
- тимчасове блокування облікового запису;
- виконання скриптів реагування на агенті.

Налаштування Active Response здійснюється на стороні менеджера з можливістю застосування дій до окремих агентів або груп агентів.

У середовищі Wazuh налаштування механізмів Active Response здійснюється безпосередньо на рівні конфігураційних файлів менеджера та не має окремого

графічного інтерфейсу в Dashboard. Dashboard використовується виключно для моніторингу подій та відображення результатів реагування, на відміну від механізмів збору логів та моніторингу стану системи, які можуть налаштовуватися централізовано через конфігурації груп агентів, це пов'язано з тим, що рішення про виконання активної реакції приймається після кореляції подій та застосування правил безпеки, що здійснюється виключно менеджером Wazuh.

Для демонстрації механізмів реагування на інциденти було налаштовано Active Response, який активується при спрацюванні правила кореляції з рівнем загрози 5 і вище. Реакція виконується на стороні менеджера та має інформаційний характер, не впливаючи на стан кінцевої системи, що забезпечує безпечне тестування механізму реагування. Реалізовано демонстраційний сценарій Active Response з мінімальним впливом на систему з метою безпечного тестування та аналізу механізмів реагування.

Щоб відкрити конфігураційний файл у менеджері використано команду `nano /var/ossec/etc/ossec.conf`

```
GNU nano 8.3 /var/ossec/etc/ossec.conf
<!--
Wazuh - Manager - Default configuration for anzn 2023
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>15m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
    <update_check>yes</update_check>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>

  <!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->
  <logging>
    <log_format>plain</log_format>
  </logging>

  <remote>
    <connection>secure</connection>
    <port>1514</port>
    <protocol>tcp</protocol>
    <queue_size>131072</queue_size>
  </remote>

  <!-- Policy monitoring -->
  <rootcheck>
    <disabled>no</disabled>
    <check_files>yes</check_files>
    <check_trojans>yes</check_trojans>
    <check_devu>yes</check_devu>
  </rootcheck>
</ossec_config>
```

Рис. 3.22 – Відкритий файл `ossec.conf` у редакторі `nano`

Щоб прописати Active Response в файлі шукаємо відведене місця для цього, виглядає ось так:

`<active-response>`

active response here

</active-response>

і всередині пишемо:

<command>log-command</command>

<location>server</location>

<level>5</level>

```
<active-response>
  <command>log-command</command>
  <location>server</location>
  <level>5</level>
</active-response>
```

Рис. 3.23 – Фрагмент ossec.conf з доданим Active Response

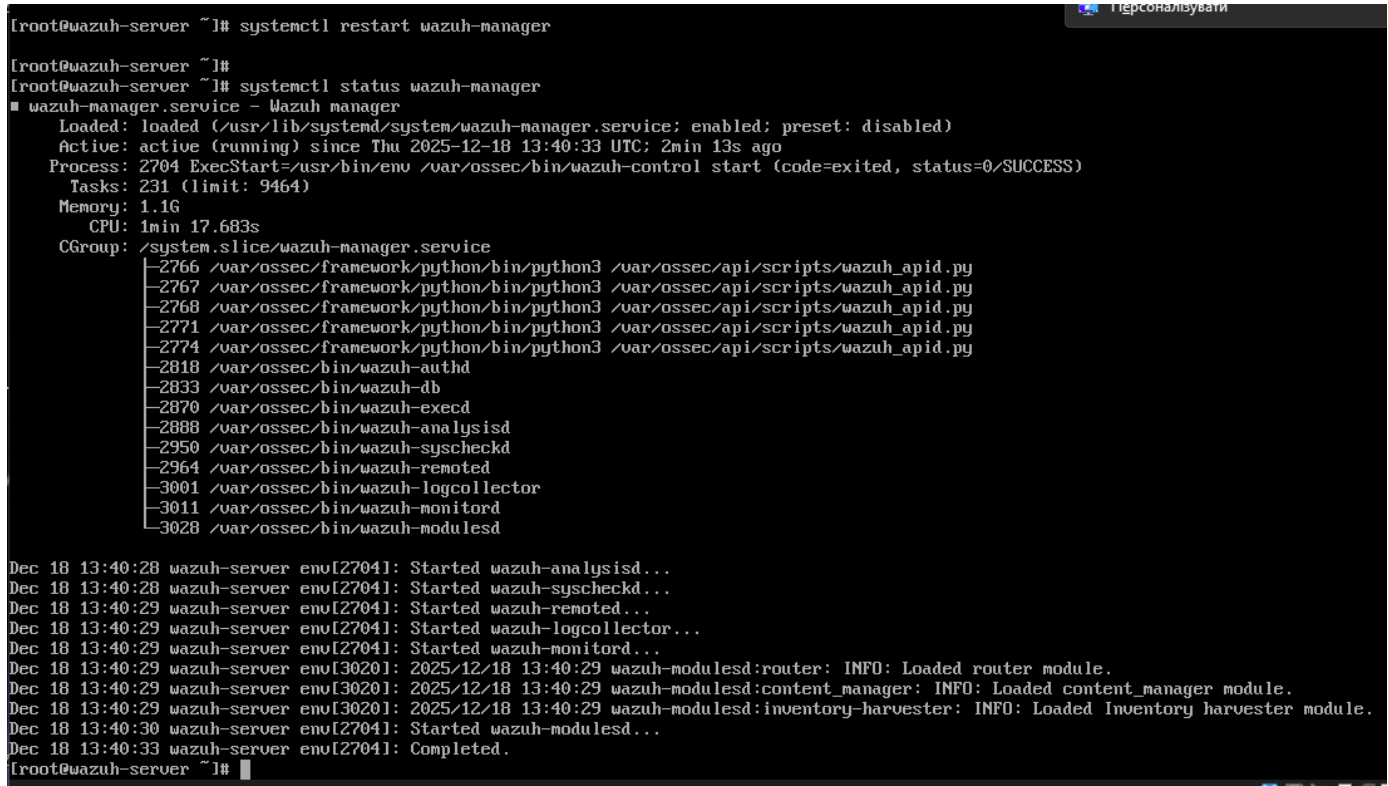
У цих рядках прописано:

<command>log-command</command> – команда, яка лише пише лог, тобто реагуванням на інцидент буде повідомлення;

<location>server</location> – параметр, що вказує на те що подія Active Response виконується на менеджері;

<level>5</level> – вказує на який саме інцидент буде виконуватись команда, у нашому випадку алерти з рівнем 5 і вище.

Щоб зміни ввійшли в силу зберігаємо файл, та перезавантажуємо менеджер(команда перезавантаження: `systemctl restart wazuh-manager`). Після цього перевіряємо стан менеджера, командою: `systemctl status wazuh-manager`.



```
[root@wazuh-server ~]# systemctl restart wazuh-manager
[root@wazuh-server ~]#
[root@wazuh-server ~]# systemctl status wazuh-manager
■ wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; preset: disabled)
   Active: active (running) since Thu 2025-12-18 13:40:33 UTC; 2min 13s ago
     Process: 2704 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
    Tasks: 231 (limit: 9464)
   Memory: 1.1G
      CPU: 1min 17.683s
   CGroup: /system.slice/wazuh-manager.service
           └─2766 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             └─2767 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
               └─2768 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                 └─2771 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                   └─2774 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                     └─2818 /var/ossec/bin/wazuh-authd
                       └─2833 /var/ossec/bin/wazuh-db
                         └─2870 /var/ossec/bin/wazuh-execd
                           └─2888 /var/ossec/bin/wazuh-analysisd
                             └─2950 /var/ossec/bin/wazuh-syscheckd
                               └─2964 /var/ossec/bin/wazuh-remoted
                                 └─3001 /var/ossec/bin/wazuh-logcollector
                                   └─3011 /var/ossec/bin/wazuh-monitor
                                     └─3028 /var/ossec/bin/wazuh-modulesd

Dec 18 13:40:28 wazuh-server env[2704]: Started wazuh-analysisd...
Dec 18 13:40:28 wazuh-server env[2704]: Started wazuh-syscheckd...
Dec 18 13:40:29 wazuh-server env[2704]: Started wazuh-remoted...
Dec 18 13:40:29 wazuh-server env[2704]: Started wazuh-logcollector...
Dec 18 13:40:29 wazuh-server env[2704]: Started wazuh-monitor...
Dec 18 13:40:29 wazuh-server env[3020]: 2025/12/18 13:40:29 wazuh-modulesd:router: INFO: Loaded router module.
Dec 18 13:40:29 wazuh-server env[3020]: 2025/12/18 13:40:29 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
Dec 18 13:40:29 wazuh-server env[3020]: 2025/12/18 13:40:29 wazuh-modulesd:inventory-harvester: INFO: Loaded Inventory harvester module.
Dec 18 13:40:30 wazuh-server env[2704]: Started wazuh-modulesd...
Dec 18 13:40:33 wazuh-server env[2704]: Completed.
[root@wazuh-server ~]#
```

Рис. 3.24 – Перезавантаження та перевірка менеджера, статус wazuh-manager — active (running)

Для генерації подій автентифікації було виконано кілька невдалих спроб входу до операційної системи Windows на кінцевій точці з установленим Wazuh Agent. Вказані події були зафіксовані в журналі безпеки та передані на менеджер Wazuh для подальшої кореляції.

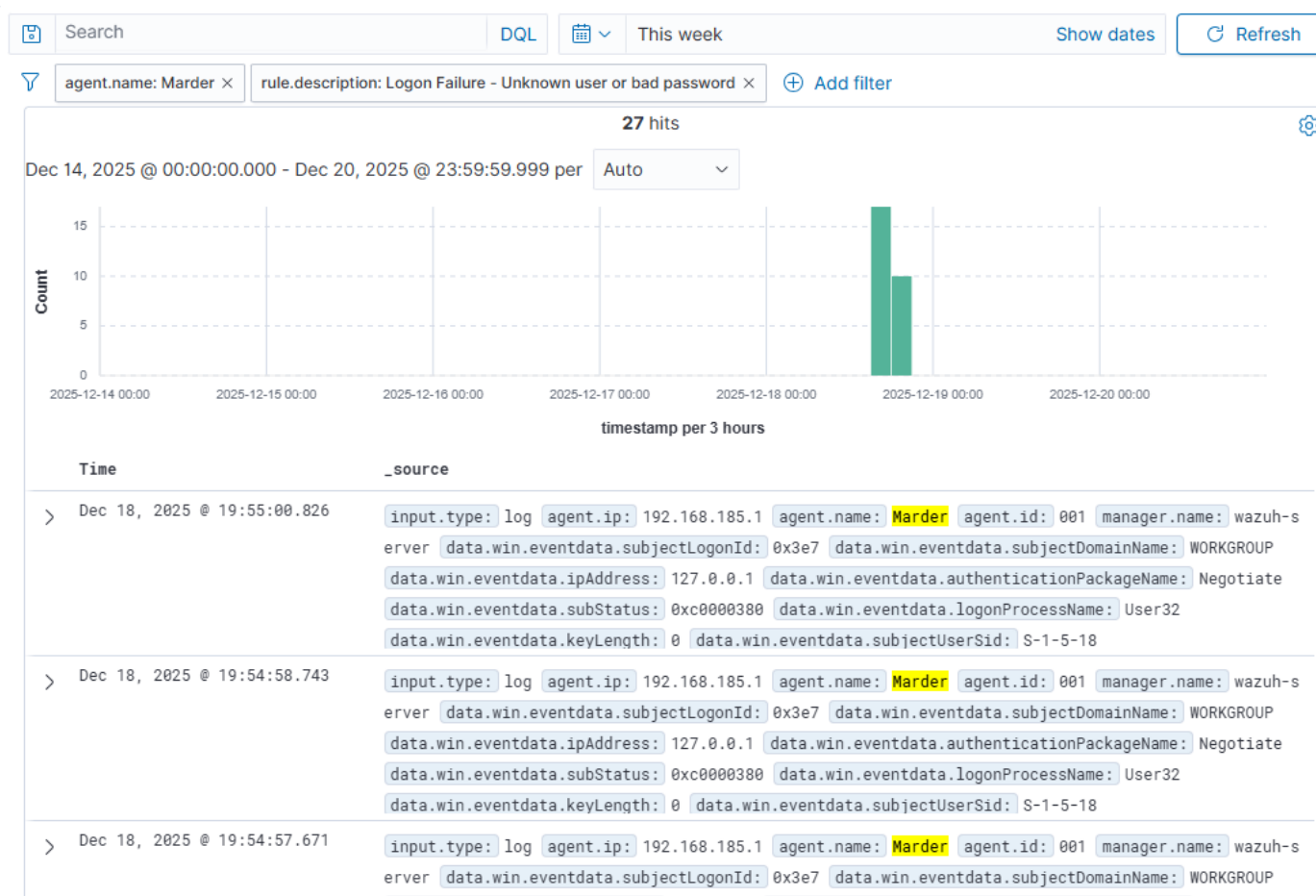


Рис. 3.25 – Журнал безпеки, з алертами некоректного входу на кінцеву точку

Саме виконання дій реагування active response на інцидент перевіряємо на менеджері командою: `cat /var/ossec/logs/active-responses.log` на менеджері час алерту вказується без врахування часового поясу, а у Wazuh Dashboard часовий кінцевої точки з агентом, враховується, тому різниця в логах виходить у моєму випадку 2 години.

```
Thu Dec 18 17:54:57 UTC 2025 ACTIVE RESPONSE TRIGGERED rule_id=62122 agent=001
Thu Dec 18 17:54:58 UTC 2025 ACTIVE RESPONSE TRIGGERED rule_id=62122 agent=001
Thu Dec 18 17:55:00 UTC 2025 ACTIVE RESPONSE TRIGGERED rule_id=62122 agent=001
```

Рис. 3.26 – Відправлені логи як спосіб реагування active response

Після реалізації сценарію реагування було зафіксовано успішне спрацювання механізму Active Response. У логах системи Wazuh Manager зафіксовані записи, як це було прописано в розробленому сценарії Active Response.

Це підтверджує, що подія, отримана від агента з ID 001, була коректно ідентифікована правилом з ID 62122, після чого система автоматично виконала відповідні дії реагування. Така реакція демонструє здатність Wazuh не лише виявляти інциденти, а й оперативно застосовувати заходи нейтралізації.

Оцінка ефективності включала:

- Швидкість реагування: подія була оброблена в межах секунди після надходження.
- Точність ідентифікації: правило коректно витягнуло IP-адресу джерела та класифікувало подію.
- Автоматизація дій: скрипт реагування був виконаний без помилок, що підтверджується записами в `active-responses.log`.

Результати підтверджують доцільність використання Wazuh як інтегрованого рішення для виявлення та реагування на інциденти інформаційної безпеки в корпоративному середовищі.

У межах даного підрозділу було реалізовано механізми реагування на інциденти інформаційної безпеки з використанням SIEM Alerts та Active Response. Застосування автоматизованих сценаріїв реагування дозволяє суттєво зменшити час виявлення та нейтралізації загроз, що підвищує загальний рівень захищеності інформаційної системи.

3.4 Розроблення рекомендацій щодо впровадження технології Wazuh у корпоративне середовище

На основі результатів, отриманих у процесі розгортання та налаштування платформи Wazuh, організації збору логів, кореляції подій і реалізації сценаріїв реагування на інциденти інформаційної безпеки, було розроблено практичні рекомендації щодо впровадження цієї технології у корпоративному середовищі.

Під час впровадження Wazuh у корпоративній інфраструктурі рекомендується на початковому етапі виконати аналіз структури мережі та визначити перелік найбільш критичних інформаційних ресурсів. Доцільно розпочинати впровадження з серверів, мережесервісів, робочих станцій адміністраторів та систем, що обробляють конфіденційну інформацію. Такий підхід дозволяє поступово масштабувати систему моніторингу без істотного впливу на продуктивність корпоративної мережі.

Для забезпечення ефективного виявлення інцидентів необхідно коректно налаштувати збір журналів подій за допомогою Wazuh Agent з урахуванням особливостей операційних систем та прикладного програмного забезпечення, що використовується в організації. Рекомендується приділяти особливу увагу журналам

автентифікації, подіям зміни системних і конфігураційних файлів, а також спробам доступу до критичних ресурсів. Варто використовувати стандартні правила кореляції Wazuh як базові та доповнювати їх власними правилами, адаптованими до специфіки корпоративних бізнес-процесів.

З метою зменшення кількості хибних спрацювань доцільно налаштовувати рівні серйозності SIEM-подій відповідно до їх потенційного впливу на інформаційну безпеку організації. Рекомендується застосовувати фільтрацію та агрегацію подій у Wazuh Dashboard, що дозволяє зосередити увагу персоналу служби безпеки на дійсно критичних інцидентах та підвищити ефективність моніторингу.

Для підвищення оперативності реагування на загрози варто впроваджувати механізми Active Response. При цьому рекомендується обмежувати автоматизовані дії реагування лише подіями з високим рівнем ризику, такими як багаторазові невдалі спроби входу, виявлення ознак шкідливої активності або порушення цілісності критичних файлів. Такий підхід дозволяє мінімізувати ризики блокування легітимних користувачів і забезпечує контрольоване використання автоматизованих сценаріїв реагування.

У процесі експлуатації системи доцільно інтегрувати SIEM-сповіщення Wazuh у загальні процеси управління інформаційною безпекою організації. Рекомендується використовувати згенеровані сповіщення для подальшого аналізу інцидентів, формування звітів та оцінки рівня захищеності інформаційних ресурсів. Використання Wazuh Dashboard варто застосовувати як інструмент візуального контролю стану безпеки та прийняття управлінських рішень.

Для забезпечення стабільної та ефективної роботи Wazuh у корпоративному середовищі необхідно регулярно оновлювати компоненти системи, переглядати правила кореляції та сценарії Active Response відповідно до актуальних загроз. Також рекомендується проводити періодичне тестування системи шляхом імітації інцидентів інформаційної безпеки, що дозволяє оцінити готовність інфраструктури до реальних атак.

Таким чином, дотримання наведених рекомендацій дозволяє впровадити технологію Wazuh у корпоративному середовищі як комплексне рішення, що поєднує централізований збір логів, кореляцію подій, формування SIEM-сповіщень та автоматизоване реагування на інциденти інформаційної безпеки.

ВИСНОВКИ

У даній дипломній роботі проведено дослідження проблеми виявлення та реагування на інциденти інформаційної безпеки в корпоративних інформаційних системах, визначено мету, завдання та актуальність використання сучасних SIEM-рішень для забезпечення належного рівня захищеності інформаційних ресурсів організації.

Виконано аналіз проблеми забезпечення інформаційної безпеки в корпоративних інформаційних системах, розглянуто сучасні загрози та основні підходи до побудови систем виявлення і реагування на інциденти інформаційної безпеки. Проведено порівняння можливостей платформи Wazuh з іншими SIEM-рішеннями, такими як Splunk, ELK та AlienVault, що дозволило обґрунтувати доцільність використання Wazuh як гнучкого та ефективного інструмента для моніторингу подій безпеки.

Досліджено призначення, архітектуру та функціональні можливості платформи Wazuh. Розглянуто основні компоненти системи, зокрема Wazuh Manager, Agent, Indexer та Dashboard, а також механізми збору, обробки та кореляції подій безпеки. Проаналізовано можливості інтеграції Wazuh із зовнішніми джерелами даних та механізми реагування на інциденти інформаційної безпеки з використанням правил і технології Active Response.

Розроблено варіант технології виявлення та реагування на інциденти інформаційної безпеки на базі платформи Wazuh. Реалізовано архітектуру системи моніторингу, виконано налаштування збору логів і кореляції подій за допомогою Wazuh Agent, а також впроваджено сценарії реагування на інциденти з використанням механізмів Active Response та SIEM-сповіщень. Проведено тестування працездатності розробленого рішення, що підтвердило ефективність виявлення подій безпеки та своєчасного реагування на загрози.

На основі результатів, отриманих у процесі виконання роботи, розроблено рекомендації щодо впровадження технології Wazuh у корпоративне середовище, які охоплюють етапи розгортання системи, налаштування збору та кореляції подій, а також використання автоматизованих механізмів реагування на інциденти інформаційної безпеки.

Таким чином, використання платформи Wazuh дозволяє побудувати ефективну систему виявлення та реагування на інциденти інформаційної безпеки в корпоративних інформаційних системах, забезпечити централізований моніторинг подій, підвищити рівень захищеності інформаційних ресурсів та зменшити час реагування на потенційні загрози.

ПЕРЕЛІК ПОСИЛАНЬ

1. ENISA. *ENISA Threat Landscape 2025*. Luxembourg: European Union Agency for Cybersecurity, 2025.

Режим доступу: <https://www.enisa.europa.eu>

2. Verizon. *2025 Data Breach Investigations Report (DBIR 2025)*. Verizon Enterprise, 2025.

Режим доступу: <https://www.verizon.com/business/resources/dbir/>

3. National Institute of Standards and Technology (NIST). *SP 800-61 Revision 3. Incident Response Recommendations and Considerations for Cybersecurity*. Gaithersburg: NIST, 2025.

Режим доступу: <https://csrc.nist.gov/publications>

4. MITRE Corporation. *MITRE ATT&CK® Framework*.

Режим доступу: <https://attack.mitre.org>

5. Gartner Research. *Market Guide for Security Information and Event Management (SIEM); Market Guide for Extended Detection and Response (XDR)*. Gartner, 2024–2025.

Режим доступу: <https://www.gartner.com>

6. Lockheed Martin. *Cyber Kill Chain® Framework*.

Режим доступу: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

7. Wazuh Documentation. — Wazuh Inc.

Режим доступу: <https://documentation.wazuh.com>

8. Splunk Enterprise Security Documentation. — Splunk Inc.

Режим доступу: <https://docs.splunk.com>

9. Elastic Security Documentation. — Elastic N.V.

Режим доступу: <https://www.elastic.co/guide/index.html>

10. AlienVault OSSIM Documentation. — AT&T Cybersecurity.

Режим доступу: <https://cybersecurity.att.com>

11. Wazuh — Getting started: Architecture. «Architecture» документація.

Режим доступу: <https://documentation.wazuh.com/current/getting-started/architecture.html>

12. Wazuh — Components. Опис компонентів: агент, сервер, індексатор, dashboard. Режим доступу:

<https://documentation.wazuh.com/current/components/index.html>

13. Wazuh — Wazuh Agent Components. Архітектура агента, модулі, функціонал, можливості FIM, SCA, Active Response тощо. Режим доступу:

<https://documentation.wazuh.com/current/components/wazuh-agent.html>

14. Wazuh — Офіційний сайт / Overview платформи. Перелік можливостей, призначення, загальний опис. Режим доступу:

<https://documentation.wazuh.com/current/index.html>

15. Wazuh — Wazuh Server Components. Детальний опис сервера: аналіз, кореляція, менеджмент агентів, threat intelligence, інтеграції. Режим доступу:

<https://documentation.wazuh.com/current/components/wazuh-server.html>

16. Wazuh — Open Source XDR / SIEM платформа. Огляд платформи, призначення, сценарії застосування (endpoint, cloud, контейнеризація). Режим доступу: <https://documentation.wazuh.com/current/index.html>

17. Wazuh — Wazuh Dashboard Components. Роль Dashboard, функції візуалізації, управління, звітів, моніторингу. Режим доступу:

<https://documentation.wazuh.com/current/components/wazuh-dashboard.html>

18. Wazuh — user manual: кластерне розгортання (cluster architecture overview). Режим доступу: <https://documentation.wazuh.com/current/installation-guide/cluster/index.html>

19. Wazuh — Wazuh Documentation. Installation alternatives. Virtual machine (VM). Режим доступу: <https://documentation.wazuh.com/current/installation-guide/installing-wazuh/vm.html>

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ(Презентація)