

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології захищеної IT-
інфраструктури корпоративної мережі на базі ОС
Windows та Active Directory»

Виконав студент 2-го курсу групи КІм-23-1
спеціальності 123 «Комп'ютерна інженерія»



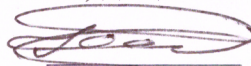
Н.Ю. Берковський

Керівник доцент кафедри комп'ютерної інженерії та
кібербезпеки, к.пед.н, доцент



О.С. Головня

Рецензент завідувач кафедри комп'ютерної
інженерії та кібербезпеки, к.т.н, доцент



А.А. Єфіменко

Житомир – 2024

Державний університет «Житомирська політехніка»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

Спеціальність 123 «Комп'ютерна інженерія»

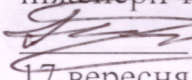
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

17 вересня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Берковський Нікіта Юрійович

Тема роботи: **«Методи та технології захищеної IT-інфраструктури
корпоративної мережі на базі ОС Windows та Active Directory»**

затверджена Наказом університету від 17 вересня 2024 р. № 478/с

Термін здачі студентом закінченої роботи 27 грудня 2024 р.

Вихідні дані роботи: проєкт підсистеми корпоративної мережі,
побудованої на основі Active Directory з інтеграцією Wazuh.

Обладнання та програмне забезпечення:

1. Мережний симулятор GNS3
2. Гіпервізор Virtualbox
3. SIEM Wazuh
4. Операційна система Windows Server 2019
5. Операційна система Windows 10

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	І.Г. Фальковський	17.09.2024	17.09.2024
2	І.Г. Фальковський	10.10.2024	10.10.2024
3	І.Г. Фальковський	12.11.2024	12.11.2024

Студент Бірю Н.Ю. Берковський
 Керівник О.С. Головня О.С. Головня

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	19.09.2024 – 23.09.2024	Виконано
2	Ознайомлення з задачею	29.09.2024 – 30.09.2024	Виконано
3	Вивчення тематики завдань	01.10.2024 – 07.10.2024	Виконано
4	Вивчення предметної області для виконання завдань	11.10.2024 – 14.10.2024	Виконано
5	Порівняння відомих рішень SIEM	15.10.2024 – 21.10.2024	Виконано
6	Розробка топології корпоративної мережі та схеми адресації	23.10.2024 – 28.10.2024	Виконано
7	Розробка підсистеми захисту та стратегії моніторингу безпеки з використанням Wazuh	29.10.2024 – 04.11.2024	Виконано
8	Вибір технічної бази	05.11.2024 – 11.11.2024	Виконано
9	Налаштування пристроїв мережі	12.11.2024 – 18.11.2024	Виконано
10	Інтеграція та налаштування роботи Wazuh	20.11.2024 – 25.11.2024	Виконано
11	Тестування функціонування мережі	26.11.2024 – 02.12.2024	Виконано
12	Написання пояснювальної записки	03.12.2024 – 13.12.2024	Виконано
13	Захист	27.12.2024	Виконано

Студент Бірю Н.Ю. Берковський
 Керівник О.С. Головня О.С. Головня

АНОТАЦІЯ

Завданням кваліфікаційної роботи було дослідження та впровадження методів і технологій для створення захищеної IT-інфраструктури корпоративної мережі на базі ОС Windows та Active Directory.

Пояснювальна записка до кваліфікаційної роботи на тему «Методи та технології захищеної IT-інфраструктури корпоративної мережі на базі ОС Windows та Active Directory» складається зі вступу, трьох розділів, висновку, списку використаної літератури. Текстова частина викладена на 60 сторінках друкованого тексту. Пояснювальна записка має список використаних джерел, який містить 18 найменування й займає 2 сторінки. В роботі наведено 54 рисунки та 3 таблиці. Загальний обсяг роботи – 67 сторінок.

В першому розділі було наведено теоретичні відомості та розглянуто основні функції, види та призначення Active Directory. Розглянуто методи та технології захисту в Active Directory. Розглянуто переваги захищеної IT-інфраструктури корпоративної мережі.

У другому розділі було проведено аналіз наявних топологій та наведено, розроблено загальну топологію мережі та схему. Також проаналізовано та обрано мережне обладнання та наведено його характеристики. Розроблено схему IP-адресації майбутньої мережі з врахуванням кількості всіх пристроїв та застосуванням динамічної адресації.

У третьому розділі було проведено налагодження пристроїв для функціонування корпоративної мережі і перевірено зв'язок між ними. Окрім цього, було реалізовано збір та перегляд логів за допомогою інструменту Wazuh.

Висновки містять результати розробки проєкту технології захищеної IT-інфраструктури корпоративної мережі на базі ОС Windows та Active Directory.

КЛЮЧОВІ СЛОВА: WINDOWS SERVER, ACTIVE DIRECTORY, SIEM WAZUH, КОРПОРАТИВНА МЕРЕЖА.

ANNOTATION

The qualification work focused on researching and implementing methods and technologies for creating a secure IT infrastructure for a corporate network based on Windows OS and Active Directory.

The explanatory note for the qualification work titled "Methods and Technologies of a Secure IT Infrastructure for a Corporate Network Based on Windows OS and Active Directory" consists of an introduction, three chapters, a conclusion, and a list of references. The textual part spans 60 pages of printed text. The explanatory note includes a reference list comprising 18 sources, covering 2 pages. The work features 54 figures and 3 tables, with a total volume of 67 pages.

The first chapter presents theoretical information and examines the main functions, types, and purposes of Active Directory. It explores the methods and technologies for protection in Active Directory and discusses the benefits of a secure IT infrastructure for a corporate network.

The second chapter provides an analysis of existing topologies and outlines the general network topology and its schematic representation. It also analyzes and selects network equipment, presenting its characteristics. Furthermore, an IP addressing scheme for the future network was developed, taking into account the number of devices and the application of dynamic addressing.

The third chapter focuses on configuring the devices for the corporate network's operation and verifying connectivity between them. Additionally, the collection and review of logs were implemented using the Wazuh tool.

The conclusion summarizes the results of the project development for a secure IT infrastructure for a corporate network based on Windows OS and Active Directory.

KEYWORDS: WINDOWS SERVER, ACTIVE DIRECTORY, SIEM WAZUH, CORPORATE NETWORK

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ НА БАЗІ ACTIVE DIRECTORY	9
1.1 Функції та призначення Active Directory	9
1.2 Основні та додаткові принципи інформаційної безпеки	12
1.3 Моделі автентифікації та управління доступом у Windows Server	14
1.4 Використання SIEM для забезпечення інформаційної безпеки в AD	16
1.5 Огляд популярних рішень SIEM	18
Висновки до першого розділу.....	25
РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ АДМІНІСТРУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ	27
2.1 Розробка топології комп'ютерної мережі та її схеми адресації	27
2.2 Розробка підсистеми захисту на базі Active Directory	31
2.3 Розробка стратегії моніторингу безпеки з використанням Wazuh	34
2.4 Вимоги до підсистеми, вибір обладнання корпоративної мережі	35
Висновки до другого розділу	39
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПІДСИСТЕМИ АДМІНІСТРУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ	41
3.1 Налагодження обладнання корпоративної мережі	41
3.2 Створення Active Directory в Windows Server.....	43
3.3 Інтеграція та налаштування системи моніторингу Wazuh	50
3.4 Аналіз логів та інцидентів безпеки за допомогою Wazuh	54
Висновки до третього розділу.....	64
ВИСНОВКИ.....	65
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	66

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD – Active Directory
AAD – Azure Active Directory
AD CS – Active Directory Certificate Services
AD DS – Active Directory Domain Services
AD FS – Active Directory Federation Service
AD LDS – Active Directory Lightweight Directory Services
AD RMS – Active Directory Right Management Services
SIEM – Security information and event management (SIEM)
API – Application Programming Interface
BGP – Border Gateway Protocol
DHCP – Dynamic Host Configuration Protocol
EIGRP – Enhanced Interior Gateway Routing Protocol
iOS – мобільна операційна система
IP – Internet Protocol
IPSec – IP Security
IPv4 – Internet Protocol version 4
ISR – Integrated Service Router
NAT – Network Address Translation
OSPF – Open Shortest Path First
PBR – Policy-Based Routing
PFR – Performance Routing
PHS – Personal Handy-phone System
PTA – Pass-through Authentication
RIP – Routing Information Protocol
VLAN – Virtual Local Area Network
VPN – Virtual Private Network
IT – інформаційні технології
VLAN – Virtual Local Area Network

ВСТУП

Актуальність теми. Тема захищеної IT-інфраструктури корпоративних мереж є надзвичайно актуальною у сучасному світі, оскільки інформаційна безпека стала ключовим аспектом діяльності будь-якої організації. Кількість кіберзагроз, таких як атаки шкідливих програм, фішинг, несанкціонований доступ до даних, продовжує зростати, що підкреслює важливість впровадження надійних засобів захисту інформаційних систем.

Особливо це стосується компаній, які використовують ОС Windows та Active Directory, адже ці платформи є одними з найпоширеніших у корпоративному середовищі. Active Directory забезпечує централізоване управління користувачами та ресурсами, однак через свою широкомасштабність та критичність для роботи організації є ціллю для багатьох атак.

Використання Active Directory дозволяє інтегрувати різноманітні системи та додатки в мережі, спрощуючи їх керування та забезпечуючи взаємодію, а також забезпечує високий рівень безпеки мережі завдяки вбудованим механізмам захисту від несанкціонованого доступу та зловмисників.

Метою дослідження є застосування методів та технологій для побудови та налаштування захищеної IT-інфраструктури корпоративної мережі на базі ОС Windows та Active Directory.

Об'єктом дослідження є процес побудови та налаштування захищеної IT-інфраструктури корпоративної мережі на базі ОС Windows та Active Directory.

Предметом дослідження є методи та технології реалізації захищеної IT-інфраструктури корпоративної мережі на базі ОС Windows та Active Directory.

Під час виконання кваліфікаційної роботи було створено модель захищеної IT-інфраструктури корпоративної мережі на базі операційної системи Windows з використанням Active Directory. У межах проєкту налаштовано служби Active Directory, розгорнуто схему IP-адресації з динамічною адресацією, а також реалізовано збір та перегляд логів за допомогою інструменту Wazuh.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ НА БАЗІ ACTIVE DIRECTORY

1.1 Функції та призначення Active Directory

Active Directory (AD) – це набір служб, розроблених для операційної системи Microsoft Server. Спочатку створений для спрощення доступу до каталогів користувачів, з часом AD отримав розширений функціонал, зокрема інтеграцію із сервісами авторизації у Windows Server 2008. Головною його метою є забезпечення виконання групової політики, що дозволяє застосовувати однакові налаштування для всіх підконтрольних комп'ютерів через System Center Configuration Manager.[2]

Простими словами, Active Directory – це роль сервера, яка дозволяє централізовано керувати доступами і дозволами в локальній мережі. AD слугує інструментом адміністрування користувачів та ресурсів мережі, спрощуючи роботу системних адміністраторів у великих організаціях. У каталогах зберігається інформація про користувачів, групи, пристрої та інші об'єкти. Наприклад, атрибути користувача можуть включати логін, пароль, адресу, телефон тощо. AD також слугує точкою автентифікації, забезпечуючи доступ до ресурсів на основі збережених даних.[8]

Основні типи Microsoft Active Directory поділяються на кілька категорій.

- Active Directory (AD) – власна служба каталогів Microsoft, яка працює на Windows Server. Вона дозволяє адміністраторам керувати доступом до мережевих ресурсів. Дані організовані у вигляді об'єктів, таких як користувачі, групи, програми чи пристрої.
- Azure Active Directory (Azure AD) – хмарна служба бізнес-ідентифікації, що входить до Microsoft Azure. Вона підтримує єдиний вхід, багатофакторну автентифікацію та умовний доступ для захисту від кіберзагроз. Azure AD побудований з нуля для створення хмарної інфраструктури і працює з REST API для передачі даних.

- Гібридний Azure Active Directory (Hybrid AAD) – поєднує локальний контролер домену та Azure AD. Містить три методи автентифікації: синхронізацію паролів (PHS), наскрізну автентифікацію та федерацію (PTA). Ця модель зручна для синхронізації локальних даних із хмарою.
- Служби домену Azure Active Directory (Azure AD DS) – надають функції, такі як LDAP, групові політики та автентифікація Kerberos/NTLM. Це рішення дозволяє використовувати керовані домени без необхідності обслуговування контролерів.

Active Directory створений для централізованого управління користувачами, пристроями та іншими ресурсами в мережі, забезпечуючи їхню автентифікацію і авторизацію.

Active Directory виконує дві основні функції: автентифікацію користувачів для доступу до ресурсів у межах домену і керування дозволами, надаючи адміністраторам можливість регулювати доступ до ресурсів. Використання Active Directory усуває необхідність введення облікових даних для кожної програми і ручного налаштування доступу до ресурсів.

Windows-мережі без Active Directory можна уявити як систему, де користувачам доводиться щоразу вводити облікові дані для доступу до кожної програми, а IT-команда змушена вручну налаштовувати дозволи та доступ до ресурсів.[1]

На сьогоднішній день існує кілька популярних служб Active Directory, кожна з яких виконує свої унікальні функції.

- Доменна служба Active Directory (AD DS) – організовує дані про об'єкти в ієрархічній структурі, доступній адміністраторам і користувачам. Наприклад, інформація про користувачів може включати їхні імена, посади, електронну пошту тощо.
- Служби об'єднання Active Directory (AD FS) – забезпечують єдиний вхід, що дозволяє користувачам надавати облікові дані лише один раз для доступу до кількох ресурсів. Служби керування правами Active

Directory (AD RMS) – керують доступом до інформації в мережі, забезпечуючи безпеку даних за допомогою політик доступу.

- Служби сертифікації Active Directory (AD CS) – дозволяють створювати і керувати інфраструктурою відкритих ключів (PKI), що використовується для шифрування і дешифрування даних.
- Полегшені служби каталогів Active Directory (AD LDS) – забезпечують підтримку програм, що працюють із каталогами, без залежності від доменних служб.

Active Directory є оптимальним вибором для роботи в середовищі на основі Windows і Microsoft, забезпечуючи ефективне централізоване управління мережею. Використання консолі Active Directory значно спрощує виконання адміністративних завдань, дозволяючи зберігати мережеві дані у впорядкованій структурі та створювати ієрархію, що відповідає організаційній структурі компанії. Система підтримує роботу з кількома доменами, кожен із яких може мати власні політики безпеки та адміністративні права.

Крім того, Active Directory забезпечує інтелектуальне керування авторизаціями, яке гарантує доступ до ресурсів і файлів виключно для тих користувачів, які мають відповідні дозволи. Такий підхід підвищує безпеку мережі та знижує ризик несанкціонованого доступу.

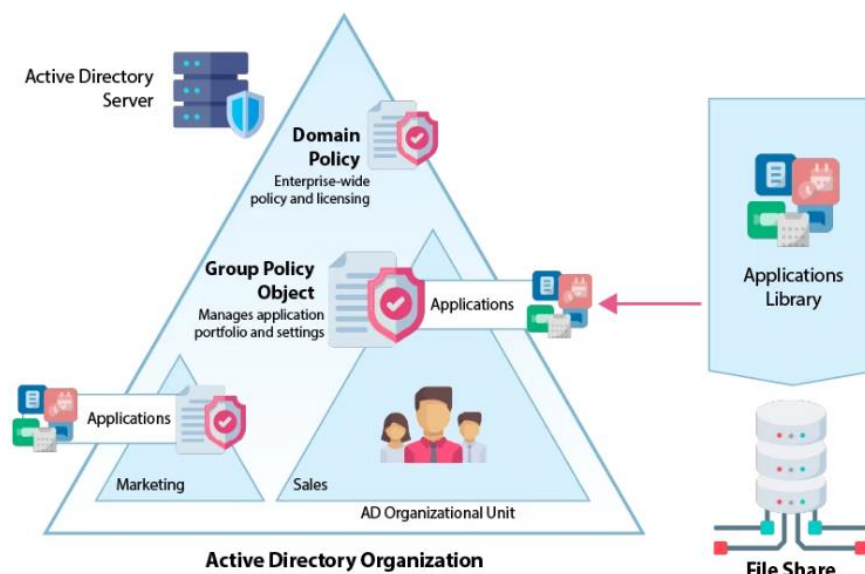


Рисунок 1.1 – Організація Active Directory

1.2 Основні та додаткові принципи інформаційної безпеки

Основні та додаткові принципи інформаційної безпеки складають основу для створення надійної системи захисту інформаційних ресурсів. Ці принципи діють як рамки, що дозволяють забезпечити конфіденційність, цілісність, доступність даних, а також гарантувати відповідальність користувачів і забезпечити безперервне відстеження потенційних загроз.[9]

Основні принципи інформаційної безпеки традиційно включають три ключові компоненти.

- **Конфіденційність** полягає в тому, щоб захистити дані від несанкціонованого доступу та гарантувати, що лише уповноважені користувачі або системи можуть отримувати доступ до певної інформації. Для забезпечення конфіденційності використовуються різні методи, зокрема шифрування, контроль доступу та автентифікація. У корпоративному середовищі, наприклад, часто застосовуються політики доступу на основі ролей (RBAC) або списки контролю доступу (ACLs), які дозволяють організаціям налаштовувати права користувачів у залежності від їхніх завдань і повноважень. Конфіденційність також передбачає захист даних під час їх передачі через мережу (використання VPN, SSL/TLS) та шифрування файлів на рівні сховища.
- **Цілісність** гарантує, що дані залишаються точними і незмінними після їхнього створення, передачі або зберігання. Цілісність важлива як для внутрішніх систем, так і для зовнішніх процесів обміну даними між різними організаціями. Порушення цілісності даних можуть відбуватися як у результаті навмисних атак (впровадження шкідливих змін), так і через випадкові помилки під час обробки інформації. Щоб запобігти таким інцидентам, використовуються хеш-функції, цифрові підписи та контрольні суми, які дозволяють виявляти зміни у файлах

або повідомленнях. Резервне копіювання також є важливим механізмом для відновлення оригінальних даних у випадку втрат або пошкоджень.

- **Доступність** гарантує, що дані, системи та сервіси будуть доступними для уповноважених користувачів у будь-який необхідний час. Цей принцип важливий як для критичних систем, так і для повсякденних операцій організацій, оскільки збій або відмова в обслуговуванні може призвести до серйозних фінансових і репутаційних втрат. Доступність забезпечується шляхом впровадження резервних систем, дублювання серверів, відмовостійких механізмів (failover), а також засобів захисту від атак на відмову в обслуговуванні (DDoS). Безперервний моніторинг і автоматичні системи відновлення можуть значно знизити ризики, пов'язані з перебоями у роботі систем.

Окрім трьох основних принципів, існує кілька **додаткових**, які також відіграють важливу роль у забезпеченні повної інформаційної безпеки. Ці принципи є наступними.

- **Автентифікація** є процесом підтвердження особи користувача або системи перед тим, як надати доступ до ресурсів. Це перший і один із найважливіших етапів захисту системи. Автентифікація може бути однофакторною (наприклад, пароль), але часто використовується багатофакторна автентифікація (MFA), яка поєднує кілька елементів, наприклад, пароль і одноразовий код, або біометричні дані, такі як відбитки пальців. Автентифікація захищає систему від несанкціонованого доступу, особливо якщо облікові записи стають ціллю атак.
- **Авторизація** йде після автентифікації і визначає, що користувач може робити у системі. Після того, як система підтвердила особу користувача, авторизація визначає, до яких саме ресурсів і операцій цей користувач має доступ. Це важливий елемент контролю доступу, який запобігає надмірному доступу до чутливих даних. Наприклад, навіть

після успішного входу до системи співробітник може мати доступ лише до певних документів, у той час як інші файли залишаються для нього закритими.

- **Неспростовність (nonrepudiation)** – це здатність системи гарантувати, що користувач не зможе заперечувати свої дії після того, як вони були виконані. Це забезпечується за допомогою цифрових підписів, які прив'язують певну дію до конкретного користувача, а також журналів аудиту, що фіксують всі дії у системі. Неспростовність важлива для створення надійного ланцюга подій, який може бути використаний як доказ у випадку виникнення інцидентів або порушень. Цей принцип є особливо важливим у системах електронної комерції та фінансових транзакціях, де кожен крок повинен бути зафіксований і підтверджений.
- **Моніторинг подій** є критичним для забезпечення безпеки в реальному часі. Системи моніторингу, такі як SIEM (Security Information and Event Management), дозволяють виявляти підозрілі дії, аномалії або спроби вторгнення. Це дозволяє адміністраторам систем реагувати на загрози оперативно, до того як вони завдадуть шкоди. Моніторинг включає в себе збирання та аналіз журналів подій, оцінку активностей користувачів, а також застосування автоматичних механізмів для блокування підозрілих дій. Це забезпечує безперервний нагляд за станом систем і дає можливість швидкого реагування у разі виявлення проблем.

1.3 Моделі автентифікації та управління доступом у Windows Server

У Windows Server для автентифікації та управління доступом використовуються кілька моделей і технологій, що забезпечують захист корпоративних мереж і ресурсів. Основною платформою для реалізації цих моделей є **Active Directory (AD)**, яка забезпечує централізоване управління обліковими записами користувачів, політиками безпеки та правами доступу.

Через AD адміністратори можуть створювати облікові записи користувачів, керувати їх ролями, налаштовувати групові політики та визначати права доступу до ресурсів.[3]

Ключовою технологією автентифікації в Windows Server є протокол **Kerberos**, який використовується за замовчуванням для автентифікації у доменах Windows. Kerberos є надійною системою автентифікації, яка заснована на криптографічних квитках і дозволяє безпечно передавати облікові дані користувачів без їх прямої передачі через мережу. Це мінімізує можливість перехоплення або підробки автентифікаційної інформації. У процесі автентифікації Kerberos видає користувачам "квитки", які вони використовують для доступу до різних ресурсів мережі, зокрема файлів, серверів або програм.

NTLM (NT LAN Manager) — це старіша модель автентифікації, яка все ще підтримується для сумісності зі старими версіями Windows. NTLM використовує хешування паролів і не настільки безпечна, як Kerberos. Однак вона досі може застосовуватись у деяких середовищах, де не працює Kerberos, наприклад, у робочих групах, для автентифікації поза доменом або для автентифікації застарілих сервісів. Водночас, не рекомендовано використовувати автентифікацію через NTLM у нових системах через низку вразливостей цього протоколу.

Інша модель автентифікації в Windows Server — це **сертифікатна автентифікація**, яка використовує інфраструктуру відкритих ключів (PKI). У цьому випадку користувачі отримують цифрові сертифікати, які підтверджують їхню особу. Це забезпечує ще вищий рівень безпеки, оскільки сертифікати важко підробити, а їх використання мінімізує необхідність зберігання та введення паролів.

Управління доступом у Windows Server здійснюється через кілька механізмів. **Role-Based Access Control (RBAC)** — це модель, в якій доступ до ресурсів надається на основі ролей користувачів у системі. Ролі визначають, які ресурси доступні кожному користувачу залежно від його функціональних

обов'язків. Це дозволяє централізовано управляти доступом, знижуючи ризики помилок і забезпечуючи контроль.

Групові політики (Group Policy) є ще одним інструментом управління доступом, який дозволяє адміністраторам централізовано керувати конфігураціями комп'ютерів і користувачів у домені. За допомогою групових політик можна встановлювати правила щодо паролів, блокувати небажані програми, налаштовувати мережеві політики, а також визначати безпекові налаштування для всієї організації. Групові політики ефективно забезпечують дотримання стандартів безпеки та мінімізують вплив людського фактора.

Для захисту конфіденційної інформації Windows Server також використовує **Dynamic Access Control (DAC)**, що дозволяє адміністраторам застосовувати більш складні правила доступу на основі атрибутів користувачів та ресурсів. Це забезпечує більш гнучке управління доступом, особливо у великих організаціях, де потрібно застосовувати складні політики доступу.

Ці моделі автентифікації та управління доступом у Windows Server працюють разом для забезпечення надійної та безпечної роботи корпоративних мереж, допомагаючи організаціям контролювати доступ до критичних ресурсів і мінімізувати загрози.

1.4 Використання SIEM для забезпечення інформаційної безпеки в AD

Керування захистом інформації та подіями SIEM є потужним інструментом для забезпечення інформаційної безпеки, що допомагає організаціям запобігати кіберзагрозам і реагувати на них до того, як вони можуть завдати шкоди бізнесу. SIEM об'єднує функції управління інформаційною безпекою та подіями в єдине рішення, що забезпечує централізоване збирання, аналіз і кореляцію даних у масштабах всієї організації. Зокрема, ця технологія збирає журнали подій з різних джерел, таких як сервери, пристрої, програми й кінцеві точки, а також виконує аналіз у реальному часі для виявлення підозрілих активностей. Завдяки використанню механізмів штучного інтелекту та

алгоритмів машинного навчання сучасні SIEM-рішення стали ще ефективнішими у виявленні та блокуванні загроз.[10]

Принцип роботи SIEM полягає у зборі та об'єднанні логів і даних з різних джерел в організації. Ці дані аналізуються на основі заздалегідь визначених правил і сценаріїв для виявлення аномалій, які можуть свідчити про спроби несанкціонованого доступу, злом або інші кібератаки. Наприклад, технологія дозволяє корелювати події, що відбуваються на різних рівнях, як-от спроби підбору пароля на сервері, а потім аномальне видалення файлів на кінцевій точці. Завдяки цьому фахівці з безпеки можуть швидко реагувати на інциденти, а організація отримує прозору картину стану кіберзахисту.

Використання SIEM для захисту Active Directory (AD) є особливо важливим, адже AD слугує критичною частиною інфраструктури організації. Active Directory відповідає за автентифікацію користувачів, управління доступом до ресурсів і забезпечення належного функціонування групових політик. SIEM-системи інтегруються з AD, збираючи журнали подій із контролерів домену, щоб ідентифікувати будь-які підозрілі зміни. Це можуть бути дії, пов'язані зі створенням привілейованих облікових записів, зміною політик безпеки або багаторазовими невдалими спробами входу.

Завдяки функціям керування журналами SIEM здатна обробляти величезні обсяги даних, автоматизуючи пошук можливих загроз та полегшуючи аудит. Кореляція подій дозволяє не лише виявляти, а й визначати закономірності між, на перший погляд, незначними інцидентами, що дає змогу вчасно розпізнати серйозну атаку. Крім того, SIEM генерує оповіщення, які допомагають фахівцям швидше реагувати, а в окремих випадках інструменти можуть автоматично блокувати підозрілі дії, мінімізуючи ризики для організації.

Серед ключових переваг використання SIEM можна виділити централізоване управління всіма подіями в корпоративній мережі, моніторинг у реальному часі, вдосконалений аналіз загроз і створення звітів, які допомагають організаціям відповідати міжнародним нормативним стандартам. Також

важливим є те, що SIEM забезпечує прозоре відстеження дій користувачів, програм і пристроїв, підвищуючи загальну видимість у мережі.

Для впровадження SIEM необхідно чітко визначити вимоги, провести тестовий запуск рішення, зібрати достатню кількість даних і розробити план реагування на інциденти. Постійна оптимізація роботи SIEM є ключовою для досягнення високої ефективності. Загалом, SIEM стає основним інструментом кіберзахисту, який не тільки захищає інфраструктуру Active Directory, але й сприяє створенню цілісної системи захисту інформації в організації.

1.5 Огляд популярних рішень SIEM

Системи SIEM є основними інструментами для забезпечення кібербезпеки в сучасних організаціях. Wazuh та його аналоги, такі як Elastic SIEM, Splunk та AlienVault OSSIM, мають різний функціонал і особливості, що відповідають потребам малих, середніх і великих бізнесів.

Elastic SIEM (рис. 1.2) є частиною потужного інструменту Elastic Stack і пропонує розширені можливості для лог-менеджменту та аналізу даних. Його головна перевага — це інтеграція з іншими компонентами Elastic Stack, такими як Logstash для обробки даних і Elasticsearch для їхнього зберігання та пошуку.

Завдяки цьому Elastic SIEM забезпечує комплексний підхід до виявлення та реагування на кіберзагрози.[15]

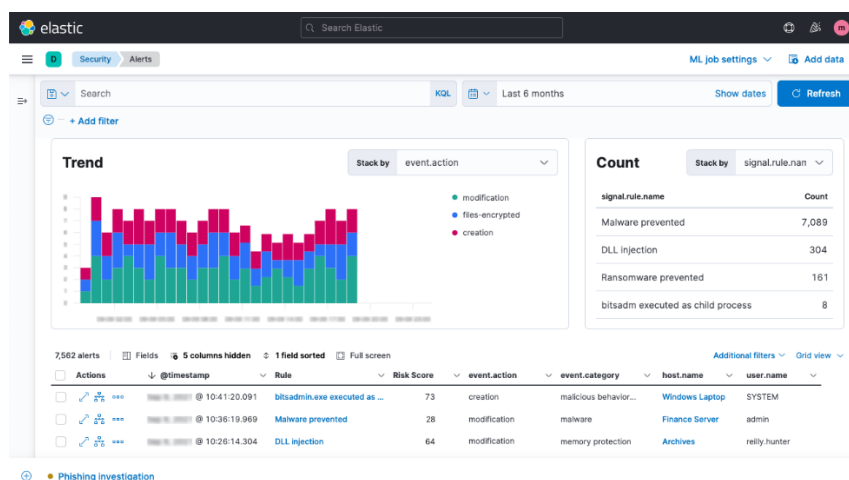


Рисунок 1.2 – Інтерфейс Elastic Security для моніторингу подій безпеки.

Ця платформа дозволяє створювати кастомізовані дашборди, які надають візуалізацію даних у режимі реального часу. Також вона пропонує функцію автоматизованого аналізу загроз, використовуючи механізми машинного навчання для виявлення аномалій. Elastic SIEM підтримує інтеграцію з популярними платформами, такими як AWS, Azure та Google Cloud, що робить його гнучким для використання в різних середовищах. Попри потужний функціонал, Elastic SIEM має складний процес розгортання, що вимагає висококваліфікованих фахівців. Крім того, ця система є ресурсоемною, що може стати проблемою для компаній із обмеженими технічними ресурсами. Однак для великих організацій, які вже використовують Elastic Stack, це ідеальний вибір.

Splunk — це комерційна SIEM-система (рис. 1.3), яка пропонує широкий спектр можливостей для аналізу великих даних і управління подіями безпеки. Її ключовою перевагою є інтуїтивний інтерфейс і потужний набір інструментів для моніторингу, аналізу та автоматизації процесів реагування на загрози. Splunk забезпечує високу точність і гнучкість завдяки інтеграції з понад 1000 сторонніх систем.[14]

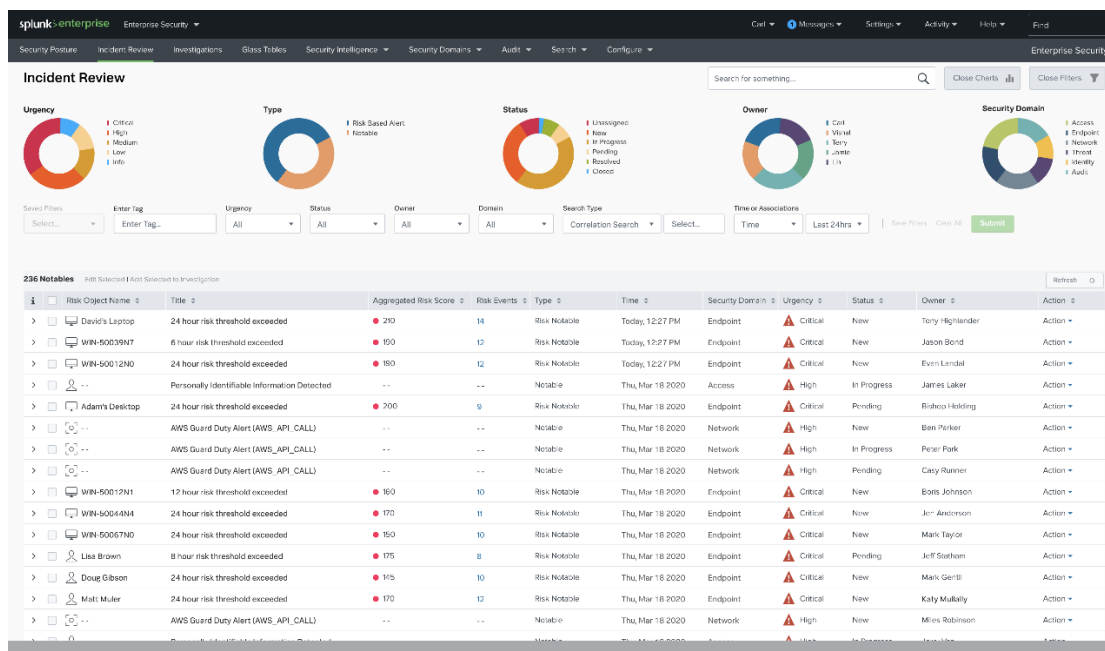
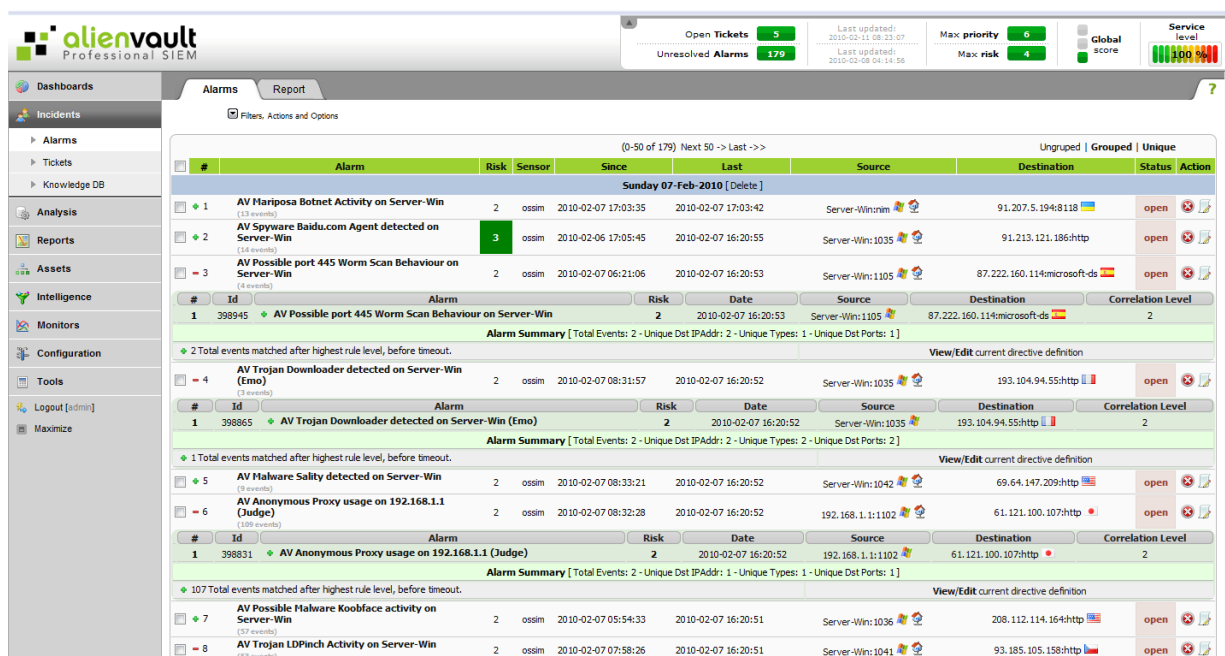


Рисунок 1.3 – Інтерфейс Splunk Enterprise Security для перегляду та управління інцидентами безпеки

Система дозволяє проводити пошук за даними в реальному часі, що допомагає швидко ідентифікувати загрози. Вона також пропонує функції машинного навчання, які дозволяють виявляти складні аномалії, що не вписуються у стандартні шаблони. Завдяки інтерактивним дашбордам користувачі можуть отримати глибокий огляд усіх подій у мережі.

Основним недоліком Splunk є його висока вартість, яка залежить від обсягу даних, що обробляються. Для малих організацій це може стати бар'єром, але для великих підприємств, які потребують максимального захисту, це рішення часто вважається виправданим.

AlienVault OSSIM — це рішення з відкритим кодом, орієнтоване на малі та середні підприємства. Воно поєднує функції SIEM із додатковими можливостями, такими як аналіз поведінкових даних, моніторинг мережі та управління інцидентами. Особливістю AlienVault (рис. 1.4) є інтеграція із сервісом Open Threat Exchange (OTX), який забезпечує доступ до спільних даних про загрози. Система має простий у використанні інтерфейс і може бути швидко розгорнута навіть без значного технічного досвіду.[16]



The screenshot displays the AlienVault OSSIM Professional SIEM interface. The top navigation bar includes the AlienVault logo, a sidebar menu with options like Dashboards, Incidents, Alarms, Tickets, Knowledge DB, Analysis, Reports, Assets, Intelligence, Monitors, Configuration, Tools, and Logout. The main content area is titled 'Alarms' and shows a list of security alerts. The alerts are organized into a table with columns for Alarm ID, Risk, Sensor, Since, Last, Source, Destination, Status, and Action. The table lists several alerts, including 'AV Mariposa Botnet Activity on Server-Win', 'AV Spyware Baidu.com Agent detected on Server-Win', 'AV Possible port 445 Worm Scan Behaviour on Server-Win', 'AV Trojan Downloader detected on Server-Win (Emo)', 'AV Malware Salty detected on Server-Win', 'AV Anonymous Proxy usage on 192.168.1.1 (Judge)', 'AV Possible Malware Kooface activity on Server-Win', and 'AV Trojan LDPinch Activity on Server-Win'. Each alert entry includes a risk level (e.g., 2 or 3), a sensor name (e.g., ossim), and a status (e.g., open). The interface also features a 'Filters, Actions and Options' section and a 'Global score' indicator.

#	Alarm	Risk	Sensor	Since	Last	Source	Destination	Status	Action
1	AV Mariposa Botnet Activity on Server-Win (13 events)	2	ossim	2010-02-07 17:03:35	2010-02-07 17:03:42	Server-Win:101	91.207.5.194:8118	open	
2	AV Spyware Baidu.com Agent detected on Server-Win (13 events)	3	ossim	2010-02-06 17:05:45	2010-02-07 16:20:55	Server-Win:1035	91.213.121.186:http	open	
3	AV Possible port 445 Worm Scan Behaviour on Server-Win (13 events)	2	ossim	2010-02-07 06:21:06	2010-02-07 16:20:53	Server-Win:1105	87.222.160.114:microsoft-ds	open	
4	AV Trojan Downloader detected on Server-Win (Emo) (2 events)	2	ossim	2010-02-07 08:31:57	2010-02-07 16:20:52	Server-Win:1035	193.104.94.55:http	open	
5	AV Malware Salty detected on Server-Win (9 events)	2	ossim	2010-02-07 08:33:21	2010-02-07 16:20:52	Server-Win:1042	69.64.147.209:http	open	
6	AV Anonymous Proxy usage on 192.168.1.1 (Judge) (105 events)	2	ossim	2010-02-07 08:32:28	2010-02-07 16:20:52	192.168.1.1:1102	61.121.100.107:http	open	
7	AV Possible Malware Kooface activity on Server-Win (57 events)	2	ossim	2010-02-07 05:54:33	2010-02-07 16:20:51	Server-Win:1036	208.112.114.164:http	open	
8	AV Trojan LDPinch Activity on Server-Win (33 events)	2	ossim	2010-02-07 07:58:26	2010-02-07 16:20:51	Server-Win:1041	93.185.105.158:http	open	

Рисунок 1.4 – Інтерфейс AlienVault OSSIM для перегляду та управління

Вона забезпечує базовий функціонал для моніторингу мережі, що включає аналіз вразливостей і виявлення загроз. AlienVault OSSIM також має вбудовані функції звітності, які допомагають відповідати регуляторним вимогам. Проте AlienVault OSSIM має обмежену масштабованість і не підходить для великих організацій із високими вимогами до продуктивності. Попри це, він залишається популярним вибором серед малих бізнесів завдяки своїй доступності.

Wazuh — це безкоштовне та відкрито доступне рішення для моніторингу безпеки та управління інцидентами (рис. 1.5). Його основна перевага — це інтеграція з Elastic Stack, яка дозволяє використовувати потужні інструменти для зберігання та аналізу даних. Завдяки цьому Wazuh може забезпечити виявлення загроз у реальному часі, керування відповідністю нормативним вимогам, таким як PCI DSS та GDPR, і моніторинг кінцевих точок.[11]

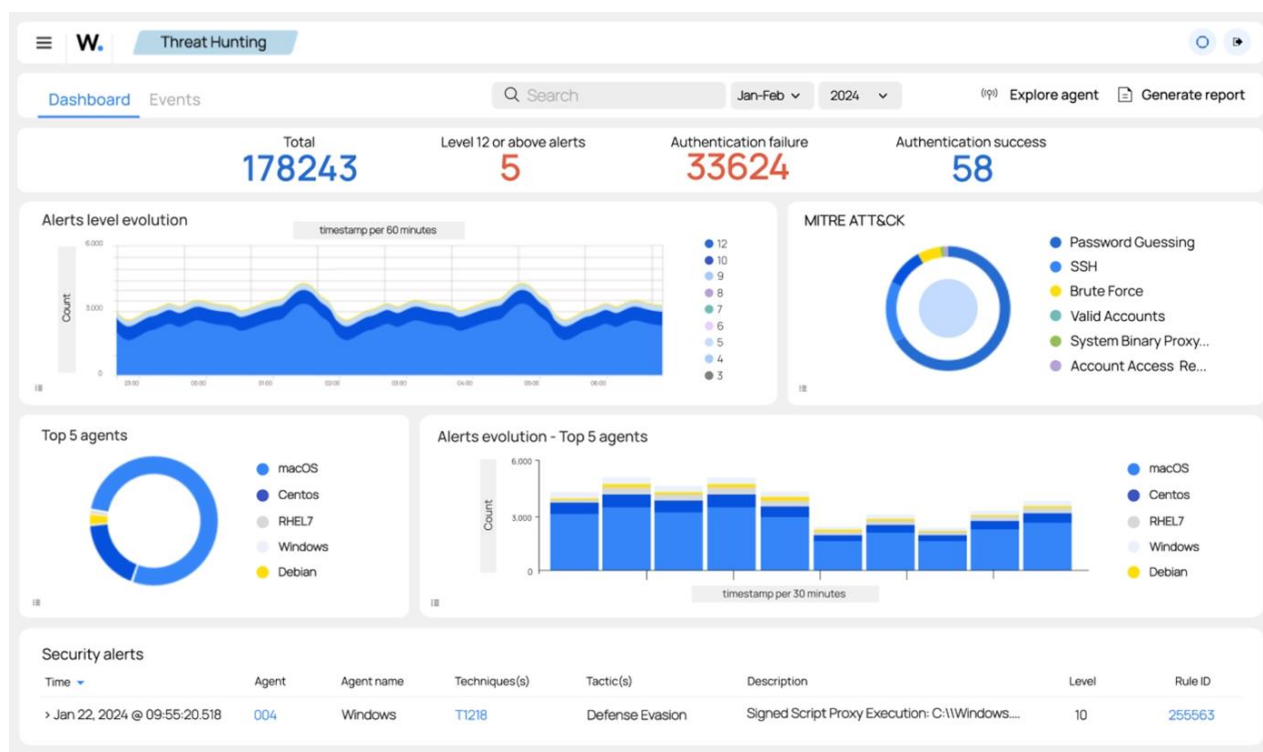


Рисунок 1.5 – Інтерфейс Wazuh для моніторингу загроз та аналізу безпеки в реальному часі

Wazuh є потужним рішенням для моніторингу безпеки інформаційних систем, яке дозволяє аналізувати події, виявляти загрози, реагувати на інциденти та забезпечувати відповідність нормативним вимогам. Система складається з агентів, що встановлюються на кінцевих пристроях, та трьох основних компонентів: сервера Wazuh, індексатора Wazuh і інформаційної панелі Wazuh. Така архітектура забезпечує централізоване управління даними безпеки з можливістю масштабування.[12]

Центральним компонентом системи (рис. 1.6) є сервер Wazuh, який відповідає за збір та обробку даних від агентів. Сервер використовує декодери для розпізнавання типу подій, які надходять, і правила для визначення підозрілих шаблонів. Основна функція сервера — аналіз загроз і створення відповідних сповіщень. Крім того, сервер дозволяє централізовано управляти агентами: змінювати їх налаштування, оновлювати та відстежувати стан.

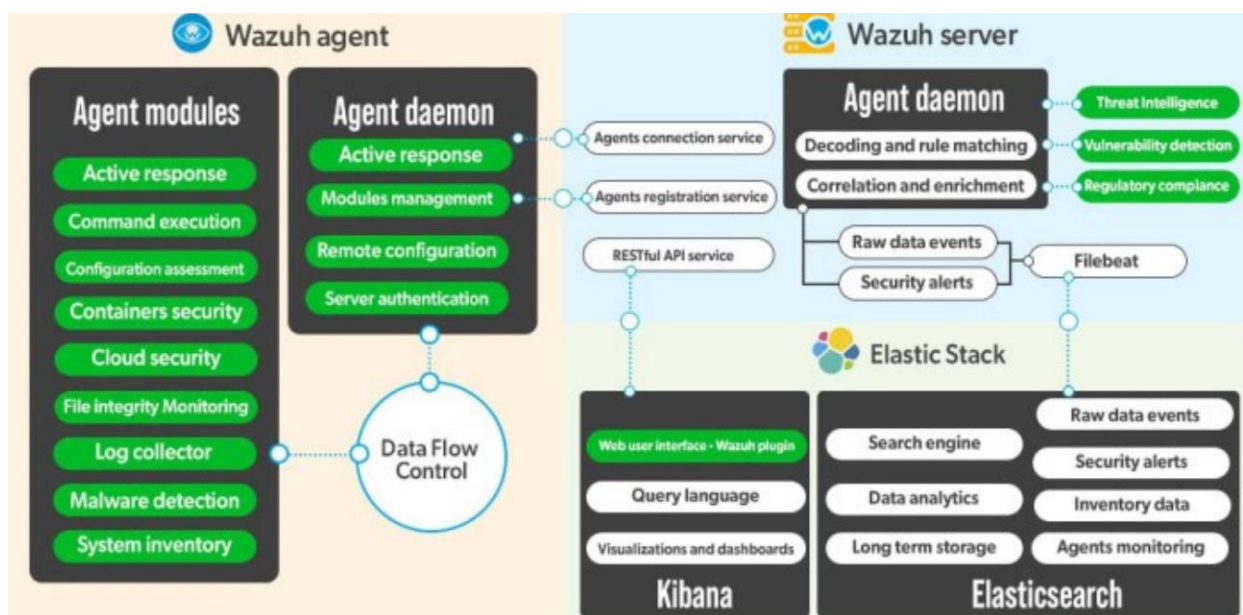


Рисунок 1.6 – Wazuh Server та агенти у структурі Wazuh

Wazuh підтримує кластеризацію серверів для забезпечення високої доступності та масштабованості. У кластерній конфігурації декілька серверів Wazuh працюють разом, забезпечуючи розподілення навантаження між вузлами та зменшуючи вплив збоїв одного з них. Головний сервер відповідає за

централізоване керування, тоді як клієнтські сервери приймають дані від агентів і передають їх у загальну інфраструктуру обробки подій. Така архітектура дозволяє системі ефективно обробляти великі обсяги даних і підтримувати стабільну роботу навіть у разі збільшення кількості кінцевих точок. Балансування навантаження між серверами забезпечує рівномірний розподіл запитів від агентів, що знижує ризик перевантаження окремих вузлів. Кластеризація (рис. 1.7) також спрощує процес управління та масштабування системи, роблячи її більш гнучкою для великих інфраструктур.

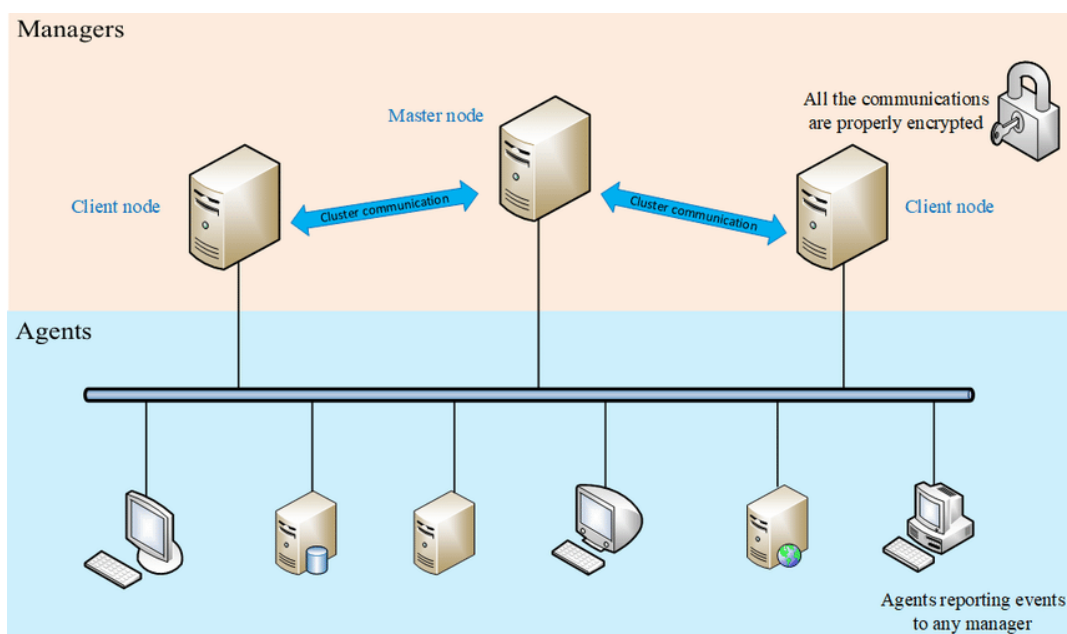


Рисунок 1.7 – Кластеризація менеджерів Wazuh

Обробка та зберігання даних відбувається за допомогою індексатора Wazuh, який індексує всі події безпеки у вигляді документів JSON. Це забезпечує можливість швидкого пошуку і запитів через інформаційну панель. Індексатор може бути налаштований як одновузловий або багатовузловий кластер для забезпечення високої доступності та масштабованості. Зберігання даних організовано за шаблонами індексів, наприклад:

- wazuh-alerts для сповіщень про загрози;
- wazuh-archives для загальних подій;
- wazuh-monitoring для моніторингу стану агентів.

Для візуалізації даних безпеки використовується інформаційна панель Wazuh, яка надає зручний доступ до аналітичної інформації. Панель дозволяє відстежувати події безпеки, виявлені вразливості, забезпечувати відповідність нормативним стандартам та моніторити стан хмарної інфраструктури. Завдяки інтеграції з RESTful API панель забезпечує просте налаштування й моніторинг усіх компонентів.

Система Wazuh має широкий спектр можливостей. Зокрема, вона дозволяє здійснювати моніторинг цілісності файлів, що включає відстеження змін у критичних файлах і каталогах у реальному часі. Для цього використовуються криптографічні хеші, які дозволяють порівнювати поточний стан файлів із базовою лінією, а у разі змін — генерувати сповіщення.

Wazuh також забезпечує аналіз журналів, збираючи дані з різних джерел, включаючи Syslog, журнали веб-серверів, SSH і Windows, для виявлення потенційних загроз. Додатково система підтримує відповідність стандартам безпеки, таким як PCI DSS, HIPAA, GDPR, NIST 800-53 та іншим, забезпечуючи аудит і звітність.

Виявлення вторгнень у мережу здійснюється за допомогою правил Snort, які дозволяють ідентифікувати несанкціоновану активність і автоматично реагувати, наприклад, блокуючи підозрілі IP-адреси. Крім того, Wazuh може збирати дані з безагентних пристроїв, таких як маршрутизатори, брандмауери та точки доступу, через Syslog, SSH або API.

Для великих середовищ Wazuh підтримує розгортання в багатовузловому кластері, що забезпечує балансування навантаження та високу доступність. Завдяки інтеграції з іншими інструментами кібербезпеки через RESTful API, система залишається гнучкою і підходить для використання в складних інфраструктурах.

Таблиця 1.1 – Порівняння SIEM-рішень

Рішення	Тип	Основні переваги	Основні недоліки	Цільова аудиторія
Wazuh	Open-source	Безкоштовне, інтеграція з Elastic Stack	Складність налаштування	Малі та середні бізнеси
Elastic	Open-source	Потужний аналіз, інтеграція з Elastic	Ресурсоємність, складність впровадження	Великі компанії
Splunk	Комерційне	Широкий функціонал, інтерактивні дашборди	Висока вартість	Великі підприємства
AlienVault	Open-source	Простота використання, інтеграція з OTX	Обмежена масштабованість	Малі бізнеси

Висновки до першого розділу

У даному розділі було проаналізовано теоретичні основи та визначені ключові функції, типи і призначення Active Directory (AD). Розглянуто, як AD сприяє управлінню обліковими записами користувачів, а також забезпечує централізовану аутентифікацію та авторизацію в мережах.

Водночас, ефективне функціонування таких систем, як Active Directory, неможливе без дотримання основних принципів інформаційної безпеки. Ці принципи забезпечують захист даних від загроз, таких як несанкціонований доступ, крадіжка чи модифікація інформації. Додаткові принципи, такі як аутентифікація, протоколювання подій і аудит, дозволяють виявляти інциденти безпеки, підвищувати прозорість дій користувачів і підсилювати контроль над інфраструктурою. Таким чином, інтеграція принципів інформаційної безпеки з функціоналом AD створює надійне середовище для захисту даних та управління корпоративними мережами.

Результати аналізу показують, що кожне SIEM-рішення має свої переваги та недоліки, які слід враховувати під час вибору для конкретної організації. Wazuh є оптимальним вибором для малих і середніх компаній завдяки своїй безкоштовності, гнучкості та підтримці регуляторної відповідності.

Загалом, вибір SIEM-системи повинен враховувати бюджет, технічну інфраструктуру та рівень складності впровадження. Для максимального ефекту варто обирати рішення, яке найкраще відповідає конкретним бізнес-потреbam.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ АДМІНІСТРУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Розробка топології комп'ютерної мережі та її схеми адресації

Ця робота присвячена проєктуванню локальної мережі, яка охоплює мережі, в яких комп'ютери розташовані на обмеженій території (до 2000 метрів). Наприклад, локальною мережею можна вважати мережу невеликого підприємства, що знаходиться у кількох будівлях. Для створення LAN використовують сучасні й часто дорогі технології, які забезпечують високу швидкість роботи мережі та передачі даних між пристроями.

Сучасні мережі доступу розділяють за територіальною ознакою:

- Локальні мережі (LAN);
- Глобальні мережі (WAN);
- Регіональні мережі (MAN).

Однією з ключових характеристик, яка відрізняє ці мережі між собою, є їх топологія. Під топологією мається на увазі спосіб розташування вузлів мережі один щодо одного. До вузлів мережі належать такі пристрої, як комп'ютери, комутатори, маршрутизатори, концентратори та точки доступу. Топологія визначає фізичну схему з'єднань між цими вузлами. Тип обраної топології впливає на характеристики мережі, включно з її надійністю, швидкістю та масштабованістю.

Вибір топології може мати значний вплив на кілька аспектів мережі, таких як типи мережевого обладнання, технологічні можливості цього обладнання, резервування пропускної здатності для можливого розширення мережі та засоби управління мережею.

Існує три основних топології мережі:

- шина (bus), при якій всі пристрої підключені до однієї загальної лінії зв'язку, а дані передаються одразу всім пристроям мережі;

- зірка (star), при якій всі периферійні пристрої підключені до одного центрального вузла, кожен через окрему лінію зв'язку;
- кільце (ring), при якій кожен вузол підключений до двох інших, утворюючи замкнене кільце, і дані передаються послідовно від одного вузла до іншого.

На практиці часто використовуються комбіновані варіанти цих базових топологій, однак більшість мереж базуються саме на зазначених трьох схемах.

У цьому проекті обрано топологію «зірка», тому детальніше розглянемо її особливості.[4]

Топологія «зірка» (рис 2.1) передбачає наявність центрального вузла, до якого підключені всі інші пристрої мережі. Уся передача даних в мережі здійснюється через цей центральний вузол, що робить його ключовим елементом інфраструктури. На центральний вузол покладається основне навантаження, оскільки саме він обробляє всі запити на обмін інформацією між підключеними пристроями. Це виключає можливість його використання для інших завдань, окрім забезпечення безперебійної роботи мережі. Через це центральний вузол має бути не тільки найпотужнішим у системі, але й оснащеним високопродуктивним обладнанням, здатним витримувати значні обсяги трафіку. Завдяки централізованій структурі виключаються конфлікти в мережі, що підвищує її стабільність і ефективність. У разі несправності периферійного пристрою мережа залишається функціональною, що є значною перевагою цієї топології. Однак відмова центрального вузла призводить до повної зупинки роботи мережі, тому необхідно забезпечити його резервування для мінімізації ризиків.

Що стосується стійкості топології «зірка» до відмов, то вихід з ладу периферійного пристрою не впливає на роботу всієї мережі. Натомість відмова центрального вузла призводить до повної непрацездатності мережі, тому для нього потрібно передбачити додаткові заходи для підвищення надійності. У разі

обриву кабелю або короткого замикання зв'язок втрачається лише з одним пристроєм, тоді як інші продовжують нормально функціонувати.[6]

На відміну від топології «шина», в «зірці» кожна лінія зв'язку з'єднує лише два вузли – центральний та периферійний. Для їх підключення часто використовують дві окремі лінії зв'язку, кожна з яких працює тільки в одному напрямку, що дозволяє використовувати простіше мережеве обладнання. Завдяки цьому «зірка» не потребує зовнішніх термінаторів, а проблема загасання сигналів вирішується ефективніше, оскільки кожен вузол отримує сигнал однакового рівня. Серед недоліків топології «зірка» варто відзначити обмеження кількості пристроїв, які можуть бути підключені до центрального вузла, що робить її менш масштабованою у великих мережах.

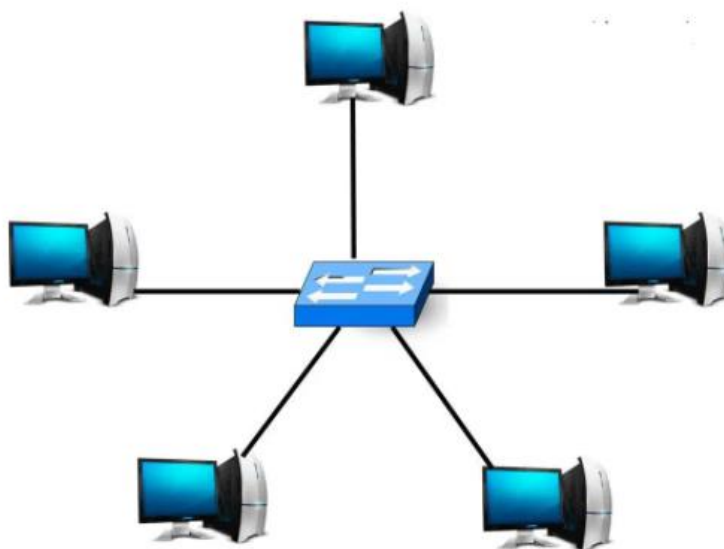


Рисунок 2.1 – Топологія «Зірка»

Переваги:

- Легко підключати додаткові пристрої.
- Продуктивність не залежить від швидкодії окремих елементів, тому залишається на стабільному високому рівні.
- Просто знайти несправність.

Недоліки:

- Несправність центрального приладу припиняє діяльність всіх користувачів.
- Кількість підключень обумовлено числом портів серверного пристрою.
- На сітку витрачається багато кабелю.
- Дороге обладнання.

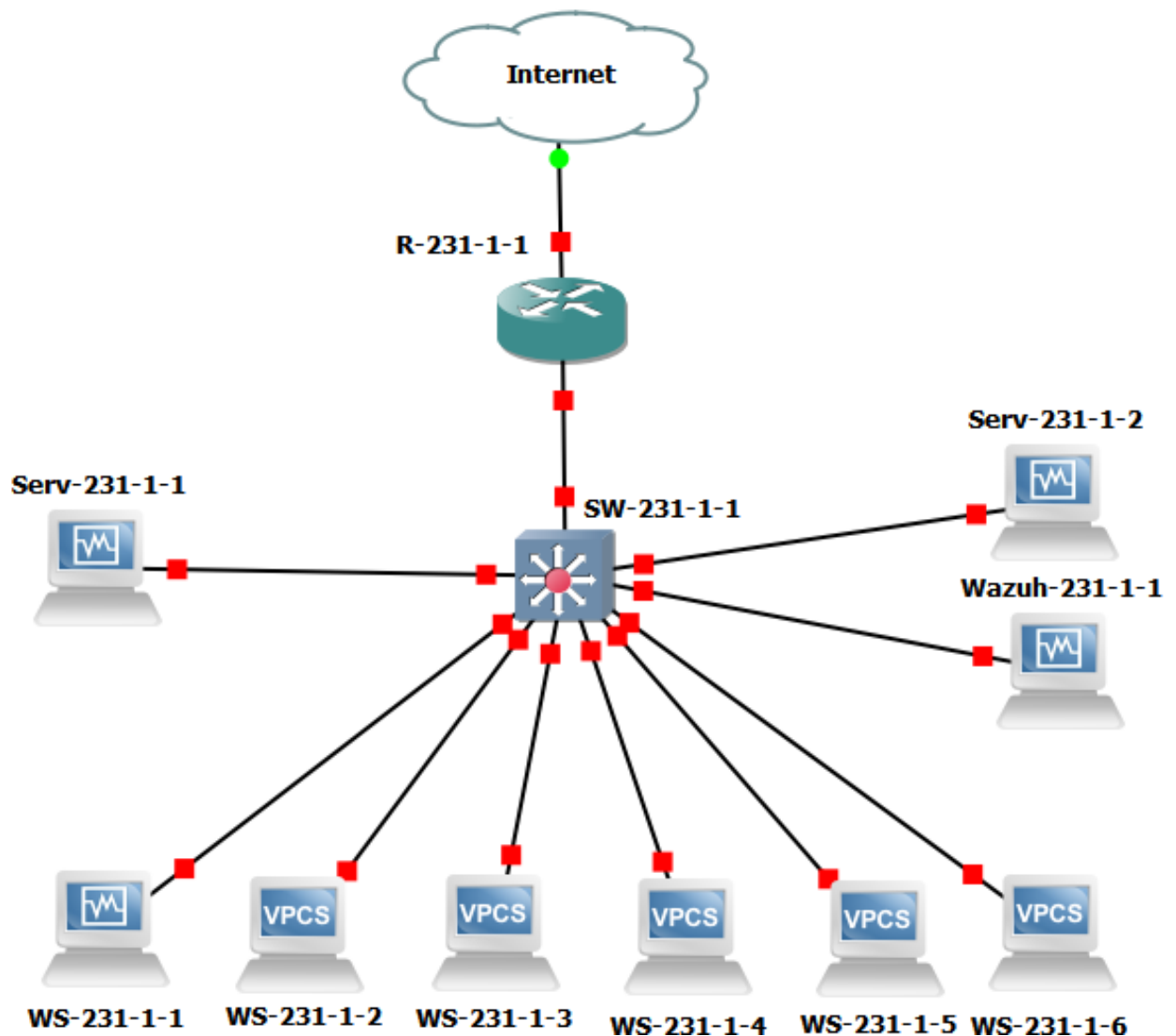


Рисунок 2.2 – Побудована мережа

Розрахунок IP адрес для мережі:

Таблиця 2.1 – Адресація локальної корпоративної мережі

Призначення	IP-адреса
Адреса мережі	192.231.1.0

Маска мережі	255.255.255.0 /24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.231.1.1
Максимальна адреса	192.231.1.254
Широкомовна адреса	192.231.1.255
Шлюз по замовчуванню	192.231.1.1
Адреса комутатора	192.231.1.2
Діапазон адрес майбутніх ПК	192.231.1.5 - 192.231.1.10
Діапазон вільних адрес	192.231.1.10 - 192.231.1.254

Таблиця 2.2 – Адресація пристроїв

Мережа/пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP - адреса	Маска	Префікс
Мережа А	—	192.231.1.0	255.255.255.0	/24
Маршрутизатор R-231-1-1	Інтерфейс Fast/Ethernet 0/1	192.231.1.1	255.255.255.0	/24
Комутатор SW-231-1-1	Інтерфейс Vlan 1	192.231.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.231.1.1	—	—
Сервер Serv-231-1-1	Інтерфейс Vlan 1	192.231.1.3	255.255.255.0	/24
	Шлюз за замовчуванням	192.231.1.1	—	—
Сервер Serv-231-1-2	Інтерфейс Vlan 1	192.231.1.4	255.255.255.0	/24
	Шлюз за замовчуванням	192.231.1.1	—	—
Сервер Wazuh-231-1-1	Інтерфейс Vlan 1	192.231.1.11	255.255.255.0	/24
	Шлюз за замовчуванням	192.231.1.1	—	—
Робоча станція WS-231-1-1 - WS-231-1-6	Мережевий інтерфейс	DHCP		/24
	Шлюз за замовчуванням	192.231.1.1		—

2.2 Розробка підсистеми захисту на базі Active Directory

Розробка захищеної IT-інфраструктури корпоративної мережі на базі Active Directory (AD) є центральним елементом управління та безпеки в сучасній корпоративній IT-інфраструктурі. Ця служба каталогів дозволяє централізовано

керувати користувачами, комп'ютерами, мережевими ресурсами та політиками безпеки. Основою її роботи є структура доменів (рис 2.3), яка забезпечує логічну організацію об'єктів та дозволяє гнучко управляти доступом до ресурсів.

Контролери домену (Domain Controllers) відіграють ключову роль у роботі AD, забезпечуючи автентифікацію користувачів та їхній доступ до ресурсів мережі. Процес автентифікації базується на протоколі Kerberos, який забезпечує високий рівень захисту, знижуючи ризики перехоплення або підробки облікових даних. Для додаткового захисту застосовується шифрування трафіку між клієнтами і серверами, що дозволяє уникнути загроз, пов'язаних із перехопленням даних.

Розробка захищеної IT-інфраструктури корпоративної мережі вимагає чіткої структуризації ієрархії доменів та організаційних одиниць (OU). Організаційні одиниці дозволяють групувати об'єкти, наприклад, користувачів чи пристрої, за підрозділами компанії або їх функціональними обов'язками. Така ієрархія сприяє впровадженню централізованих політик доступу і безпеки для конкретних груп.[7]

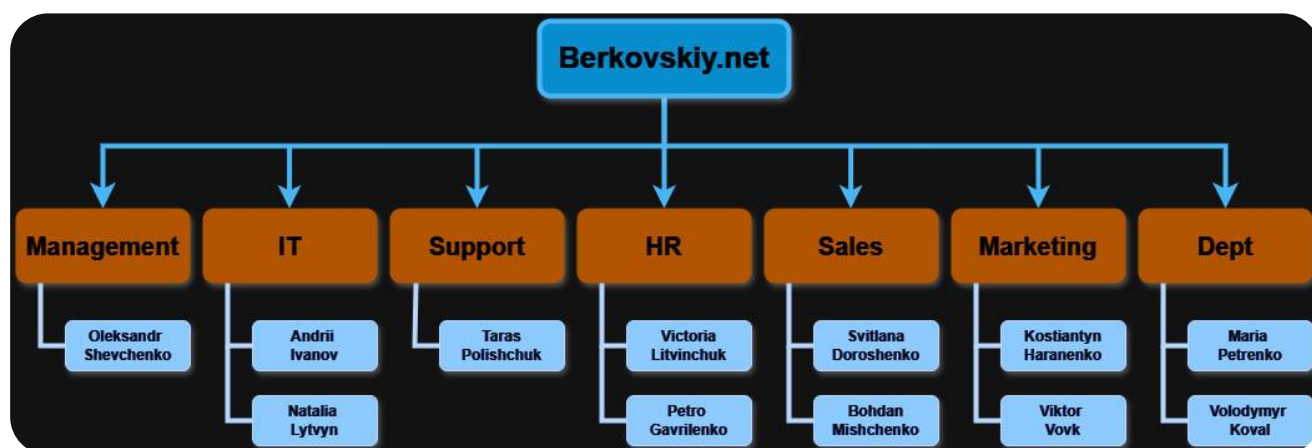


Рисунок 2.3 – Приклад моделі організації інфраструктури на базі Active Directory

Зокрема, адміністратори можуть використовувати групові політики (Group Policy Objects, GPO), які дозволяють встановлювати вимоги до паролів, обмежувати використання зовнішніх пристроїв або блокувати запуск небажаних

програм. Наприклад, у середовищі з високими вимогами до безпеки можна встановити політику багатофакторної автентифікації (MFA) для підвищення захисту облікових записів користувачів. Групові політики, які застосовуються до конкретних ОУ, забезпечують гнучке управління, даючи змогу адаптуватися до змін у структурі організації. Успішна реалізація підсистеми захисту на базі AD включає впровадження механізмів аудиту, які допомагають відстежувати зміни в конфігурації системи, дії користувачів та спроби несанкціонованого доступу. Функція Advanced Threat Analytics (ATA), доступна в деяких версіях Windows Server, дозволяє виявляти аномалії в поведінці користувачів і попереджати потенційні загрози. Наприклад, якщо користувач намагається підвищити свої привілеї або отримати доступ до конфіденційних ресурсів, ATA сповіщає адміністратора про підозрілу активність. Крім того, адміністратори можуть налаштувати детальний аудит доступу до файлів, що дозволяє відстежувати, хто і коли відкривав, змінював чи видаляв файли в корпоративній мережі. Ця функція критично важлива для відповідності міжнародним стандартам безпеки, таким як ISO/IEC 27001 чи GDPR.

Ще одним важливим елементом захисту є впровадження резервного копіювання (backup) бази даних Active Directory, що дозволяє забезпечити відновлення після критичних збоїв або атак. Наприклад, у разі атаки з використанням програм-вимагачів (ransomware), резервна копія дозволяє швидко повернути систему до працездатного стану без втрати важливої інформації. Резервне копіювання рекомендується проводити регулярно, використовуючи інструменти, такі як Windows Server Backup або спеціалізовані системи, що забезпечують можливість створення інкрементальних копій. Крім того, важливим аспектом захисту є налаштування реплікації між контролерами домену, що забезпечує синхронізацію даних між різними серверами та підвищує доступність сервісу навіть у разі виходу одного з контролерів із ладу.

2.3 Розробка стратегії моніторингу безпеки з використанням Wazuh

Розробка стратегії моніторингу безпеки з використанням Wazuh

Ефективний моніторинг безпеки є критично важливим компонентом захисту корпоративної IT-інфраструктури. Використання системи Wazuh дозволяє створити комплексну стратегію моніторингу, яка забезпечує збір, аналіз і кореляцію даних про події в мережі. Wazuh, як SIEM-платформа (Security Information and Event Management), інтегрується з Active Directory, серверами, робочими станціями та мережевими пристроями, що дозволяє централізувати обробку логів і виявлення загроз.

Основна ідея впровадження Wazuh полягає у побудові системи раннього виявлення аномалій і атак, що дає змогу адміністраторам реагувати на інциденти до того, як вони завдадуть шкоди. Процес розробки стратегії моніторингу починається з визначення ключових точок контролю в інфраструктурі. Це включає сервери, контролери домену Active Directory, робочі станції, мережеве обладнання та сервіси. На цих пристроях встановлюються агенти Wazuh, які відповідають за збір інформації, наприклад, журналів доступу, змін у системних файлах або налаштуваннях, а також підозрілої мережевої активності. Агенти передають ці дані на центральний сервер Wazuh, де вони аналізуються за допомогою правил і сигнатур. Наприклад, система може виявити підозрілу спробу входу в обліковий запис адміністратора домену або спробу експлуатації вразливостей у програмному забезпеченні.[13]

Основним етапом стратегії моніторингу є налаштування алертів для виявлення критичних подій. У Wazuh це здійснюється за допомогою вбудованих правил або створення кастомних політик, адаптованих до специфіки мережі. Наприклад, для контролера домену можна налаштувати відстеження великої кількості невдалих спроб входу, що може свідчити про атаку типу brute force.

Крім того, система підтримує інтеграцію з іншими SIEM-рішеннями, такими як Elastic Stack, що дозволяє візуалізувати дані через Kibana. Завдяки

цьому адміністратор отримує повний огляд поточного стану мережі, зокрема інформацію про аномальні події або зміни конфігурації.

Важливим аспектом стратегії є впровадження автоматизованих механізмів реагування на інциденти. Wazuh дозволяє виконувати автоматичні дії, наприклад, блокування підозрілих IP-адрес за допомогою файрволів або сповіщення адміністратора через електронну пошту. Це значно прискорює реагування на загрози та мінімізує людський фактор. Додатково, Wazuh забезпечує дотримання нормативних вимог і стандартів безпеки, таких як ISO 27001, PCI DSS або GDPR, шляхом регулярного аналізу конфігурацій і надання звітів про відповідність.

2.4 Вимоги до підсистеми, вибір обладнання корпоративної мережі

Вимоги до захищеної IT-інфраструктури корпоративної мережі на базі Active Directory можуть бути різноманітними, оскільки вони залежать від потреб та специфіки кожної організації. Проте, існує кілька загальних вимог, які можна врахувати при розробці такої підсистеми.

Перша вимога до підсистеми – це забезпечення повного й ефективного управління об'єктами Active Directory. Це включає можливість створення, редагування та видалення об'єктів, таких як користувачі, групи, комп'ютери й інші ресурси Active Directory. Крім того, необхідно підтримувати налаштування прав доступу, політик безпеки й інших параметрів для ефективного управління цими об'єктами.

Друга важлива функція підсистеми – автоматизація рутинних завдань, яка є ключовим аспектом її функціональності. Це означає, що підсистема має підтримувати створення та виконання автоматизованих процесів для різноманітних завдань, таких як додавання нових користувачів, налаштування політик безпеки чи надання прав доступу. Така автоматизація значно полегшує адміністрування мережі, підвищує його швидкість, зменшує ризик людських помилок і забезпечує узгодженість виконання завдань.

Ще однією необхідною функцією є моніторинг і звітність. Підсистема повинна мати інструменти для відстеження та аналізу стану мережі, автоматизованих процесів і виконаних завдань. Це дозволить адміністраторам контролювати продуктивність системи, виявляти помилки та відповідати вимогам безпеки й стандартам організації. Звіти, які генерує підсистема, мають бути інформативними, зрозумілими та підтримувати функції фільтрування й сортування, що дозволить адміністраторам швидко отримувати повну й точну інформацію про стан мережі.

Безпека є окремою і дуже важливою вимогою. Підсистема повинна забезпечувати надійний захист даних, автентифікацію користувачів і авторизацію доступу до функцій та об'єктів Active Directory. Вона повинна підтримувати шифрування даних, контроль доступу, аудит дій користувачів та інші механізми, які запобігають несанкціонованому доступу чи зловживанням.

Ще одним важливим аспектом є зручність використання та налаштування підсистеми. Інтерфейс повинен бути інтуїтивно зрозумілим, зручним і дозволяти налаштовувати параметри відповідно до потреб користувачів. Простота впровадження й використання підсистеми допоможе знизити витрати часу та ресурсів на її освоєння.

Крім того, підсистема має забезпечувати якісну технічну підтримку й доступну документацію. Розробник повинен надавати регулярні оновлення, виправлення помилок і консультації. Документація повинна включати детальні посібники користувача, документацію API та інші інформаційні матеріали, які допоможуть адміністраторам використовувати підсистему максимально ефективно.

Таким чином, основні вимоги до підсистеми для адміністрування захищеної IT-інфраструктури на базі Active Directory включають ефективне управління об'єктами, автоматизацію рутинних завдань, засоби моніторингу й звітності, забезпечення високого рівня безпеки, зручність використання та підтримку.

Однак також важливо враховувати потреби конкретної організації. Вимоги можуть варіюватися залежно від масштабів мережі, її структури, вимог безпеки, розподіленості користувачів, необхідності автоматизації та інших факторів. Аналіз потреб організації дозволяє обрати рішення, яке оптимально відповідатиме вимогам і забезпечить ефективне управління корпоративною мережею на базі Active Directory.

Для організації підсистеми корпоративної мережі використовуватиметься обладнання, зокрема маршрутизатор Cisco ISR4331/K9 (рис. 2.4). Цей пристрій оснащений багатоядерним процесором і програмним забезпеченням Cisco IOS XE. Завдяки своїй здатності масштабуватися і підтримувати інтеграцію нових сервісів він забезпечує високоякісне обслуговування локальної мережі, що охоплює організації та їх філії (рис. 2.4). Пристрій має механізми прискореного шифрування, сервіси для обробки мультимедійного трафіку та підтримує різні способи підключення, включаючи T1/E1, T3/E3 і порти Gigabit Ethernet.

Маршрутизатор Cisco ISR4331/K9 ідеально підходить для обслуговування філій, забезпечуючи обробку аудіо- й відеоданих, високий рівень мережевої безпеки та доступ до мережі для мобільних користувачів. Завдяки модульній конструкції цей пристрій можна адаптувати до специфічних потреб мережі, додаючи нові модулі в спеціальні слоти.

Маршрутизатори серій Cisco ISR4300 і Cisco ISR4400 підтримують роботу з протоколами NAT, IPSec VPN, RIP v1/v2, EIGRP, OSPF, BGP, PBR, PFR, а також IPv4 і IPv6 адресацією. Пристрої серії Cisco ISR4000 забезпечують користувачам високоякісні послуги, мають масштабовану архітектуру, захищають інвестиції та мінімізують витрати на встановлення.[17]



Рисунок 2.4 – Cisco ISR4331/K9

Основним критерієм при виборі моделей комутаторів є кількість портів, а також швидкість передачі цих портів (рис. 2.5). У нашій мережі використовуються комутатори на 24 порти. Оптимальним рішенням є комутатор фірми Cisco, а саме модель Cisco Systems WS-C2960-24TT-L.



Рисунок 2.5 – Cisco Systems WS-C2960-24TT-L

Cisco Systems WS-C2960-24TT-L — це керований комутатор з 24 портами Fast Ethernet і 2 комбінованими Gigabit SFP портами. Комутатори серії Cisco Catalyst 2960, 2960-C і 2960-S підтримують передачу голосу, відео та даних із високими стандартами безпеки доступу, а також забезпечують масштабоване управління відповідно до вимог бізнесу.[18]

Особливості комутатора Cisco Catalyst 2960 , 2960 -L і 2960- S є наступними.

- Універсальність: підтримка передачі даних, бездротового зв'язку і голосового трафіку.

- Інтелектуальне управління: можливість призначення пріоритетів голосовому трафіку або даним для досягнення найвищої ефективності передачі інформації в організації.
- Підвищена безпека: забезпечення захисту важливої інформації, виявлення несанкціонованого доступу користувачів і забезпечення безпечної роботи.
- Надійність: використання стандартних методів та модулів FlexStack для підвищення надійності та швидкого виявлення помилок.
- Зручність налаштування: використання набору функцій Cisco Catalyst Kit Smart Operations і Cisco Network Assistant для спрощення процесу налаштування, оновлення та усунення помилок.

В ролі сервера буде комп'ютер з встановленою операційною системою Windows Server. Windows Server - це операційна система, розроблена компанією Microsoft, спеціально призначена для використання на серверах. Вона надає набір функцій та інструментів, які дозволяють організаціям будувати, управляти та розширювати комп'ютерні мережі та інфраструктуру. Windows Server має декілька версій, таких як Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 та інші. Кожна версія пропонує різні можливості та функціональність, що відповідають потребам різних типів організацій.[5]

Висновки до другого розділу

У підсумку, розробка підсистеми захисту на базі Active Directory є важливим етапом у створенні сучасної IT-інфраструктури, яка відповідає вимогам інформаційної безпеки. Завдяки централізованому управлінню доступом, впровадженню політик безпеки, налаштуванню аудиту та резервного копіювання, AD забезпечує надійний захист інформаційних ресурсів, зменшуючи ризики, пов'язані з кіберзагрозами.

Також проаналізовано та обрано мережне обладнання та наведено його характеристики. Було розроблено схему IP-адресації майбутньої мережі з врахуванням кількості всіх пристроїв та застосуванням динамічної адресації. Підсистема захисту, створена на базі Active Directory, дозволяє централізовано управляти доступом, виконувати автентифікацію користувачів через протокол Kerberos, відслідковувати їхні дії за допомогою аудиту та застосовувати групові політики (GPO) для підвищення рівня безпеки. Використання механізмів резервного копіювання та реплікації даних значно підвищує стійкість інфраструктури до збоїв.

Система моніторингу безпеки Wazuh забезпечує комплексний збір та аналіз даних про події в мережі, виявлення загроз і автоматизацію реагування на інциденти. Завдяки інтеграції з Active Directory, серверами та мережевим обладнанням, Wazuh сприяє підвищенню рівня безпеки та відповідності мережі сучасним стандартам.

Використання сучасного мережевого обладнання Cisco та серверів Windows Server гарантує високу продуктивність, масштабованість та стабільність мережі. Таким чином, комплексний підхід до проєктування та захисту локальної мережі дозволяє забезпечити її ефективну, надійну та безпечну роботу.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПІДСИСТЕМИ АДМІНІСТРУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Налаштування обладнання корпоративної мережі

Налаштування корпоративної мережі починається з налаштування основних мережевих пристроїв: маршрутизаторів та комутаторів. У цьому розділі розглянемо налаштування для маршрутизатора та комутатора на прикладі пристроїв R-231-1-1 (маршрутизатор) і SW-231-1-1 (комутатор). Правильна конфігурація цих пристроїв є ключовою для забезпечення надійної та безпечної роботи корпоративної мережі.

Маршрутизатор виконує функцію передачі даних між різними мережами, а також з'єднання з глобальною мережею Інтернет. Налаштування маршрутизатора починається з призначення IP-адреси інтерфейсу, що дозволяє пристрою мати унікальну адресу в локальній мережі для обміну даними. Активування інтерфейсу є наступним кроком, оскільки без цього фізичний порт залишається неактивним. Для забезпечення маршрутизації поза межами локальної мережі додається маршрут за замовчуванням, який спрямовує весь невизначений трафік до зовнішнього шлюзу, наприклад, провайдера Інтернету.

Надійність мережі підвищується завдяки налаштуванню аутентифікації адміністратора маршрутизатора (рис 3.1). Це включає створення облікового запису з привілеями адміністратора та встановлення безпечного пароля. Для віддаленого керування маршрутизатором використовується протокол SSH, який забезпечує зашифрований доступ до пристрою. Завершальним етапом є збереження конфігурації, щоб вона залишалася актуальною після перезавантаження пристрою.

```

R-231-1-1(config-if)#ip address 192.231.1.1 255.255.255.0
R-231-1-1(config-if)#no shut
R-231-1-1(config-if)#do write
Building configuration...
R-231-1-1(config-if)#ip route 0.0.0.0 0.0.0.0 68.231.1.1
R-231-1-1(config)#username admin privilege 15 secret green9
R-231-1-1(config)#enable secret burn19
R-231-1-1(config)#line vty 0 4
R-231-1-1(config-line)#login local
R-231-1-1(config-line)#transport input ssh
R-231-1-1(config-line)#ex
% Ambiguous command: "ex"
R-231-1-1(config-line)#exit
R-231-1-1(config)#line console 0
R-231-1-1(config-line)#password burn19
R-231-1-1(config-line)#line aux 0
R-231-1-1(config-line)#exit
R-231-1-1(config)#do write

```

Рисунок 3.1 – Налаштування маршрутизатора R-231-1-1

Комутатор відповідає за передачу даних між пристроями всередині локальної мережі. Його налаштування включає призначення IP-адреси на віртуальний інтерфейс VLAN1, що дозволяє адміністраторам здійснювати керування пристроєм (рис 3.2). Для забезпечення доступу до інших мереж, таких як Інтернет, встановлюється шлюз за замовчуванням. Як і у випадку з маршрутизатором, для доступу до комутатора налаштовується обліковий запис адміністратора та SSH-з'єднання, що забезпечує захищене керування пристроєм через мережу. Завершальним кроком також є збереження конфігурації.

```

SW-231-1-1(config)#int vlan 1
SW-231-1-1(config-if)#ip address 192.231.1.2 255.255.255.0
SW-231-1-1(config-if)#ip default-gateway 192.231.1.1
SW-231-1-1(config)#no shut
SW-231-1-1(config)#username admin privilege 15 secret green9
SW-231-1-1(config)#enable secret black9
SW-231-1-1(config)#line vty 0 4
SW-231-1-1(config-line)#login local
SW-231-1-1(config-line)#transport input ssh
SW-231-1-1(config-line)#line console 0
SW-231-1-1(config-line)#password black9
SW-231-1-1(config-line)#logging synch
SW-231-1-1(config-line)#logging synch
SW-231-1-1(config-line)#line aux 0
SW-231-1-1(config-line)#exit
SW-231-1-1(config)#do write

```

Рисунок 3.2 – Налаштування комутатора SW-231-1-1

3.2 Створення Active Directory в Windows Server

Почнемо з додавання ролей служб та Active Directory і налаштування IP-адресації серверів (рис.3.3). Налаштування серверів та сервера Wazuh, початкові налаштування першого та другого сервера не відрізняються, зміни будуть далі.

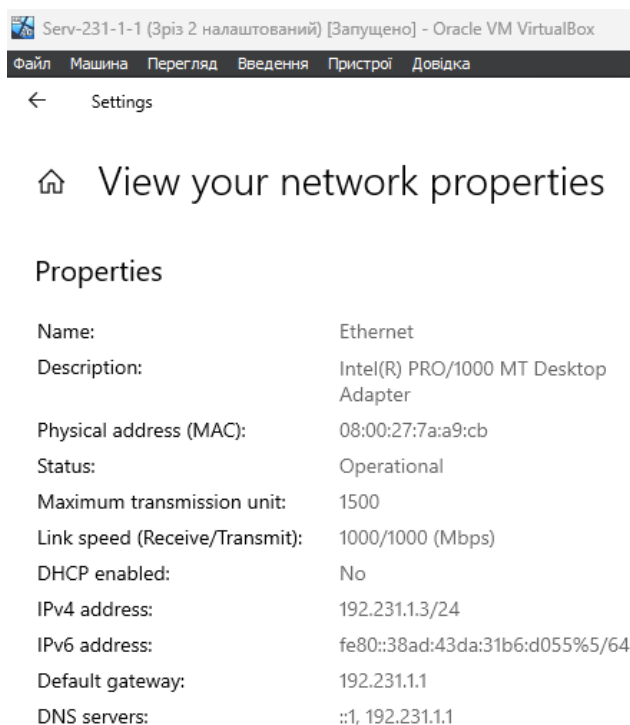


Рисунок 3.3 – Налаштування IP-адресації на Serv-231-1-1

Properties	
Name:	Ethernet
Description:	Intel(R) PRO/1000 MT Desktop Adapter
Physical address (MAC):	08:00:27:88:a1:d7
Status:	Operational
Maximum transmission unit:	1500
Link speed (Receive/Transmit):	1000/1000 (Mbps)
DHCP enabled:	No
IPv4 address:	192.231.1.4/24
IPv6 address:	fe80::14fc:8224:bea9:2403%14/64
Default gateway:	192.231.1.1
DNS servers:	::1, 192.231.1.3, 127.0.0.1

Рисунок 3.4 – Налаштування IP-адресації на Serv-231-1-2

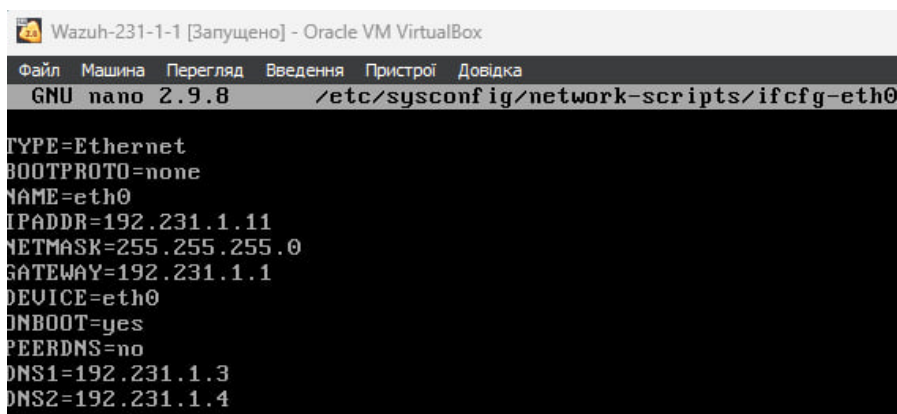


Рисунок 3.5 – Налаштування IP-адресації на Wazuh-231-1-2

Далі створюємо домен в Active Directory. Відкриваємо диспетчер серверів, натискаємо піктограму прапорця вгорі праворуч, а потім натискаємо (Зробити цей сервер контролером домену).

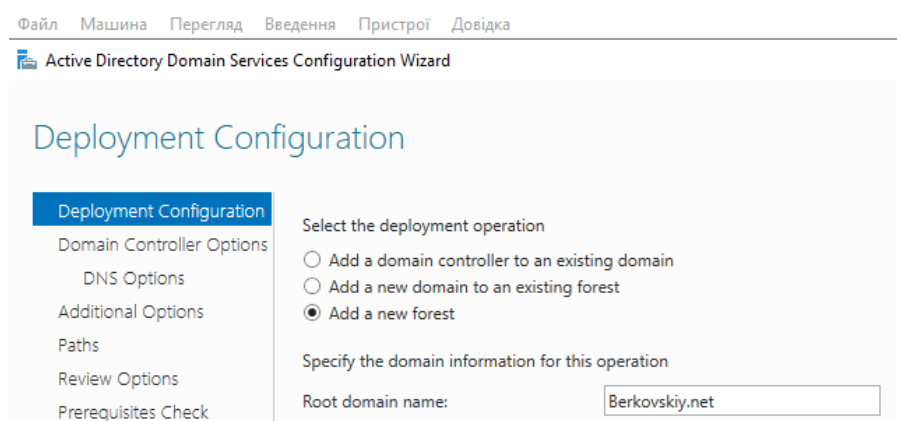


Рисунок 3.6 – Створюємо домен

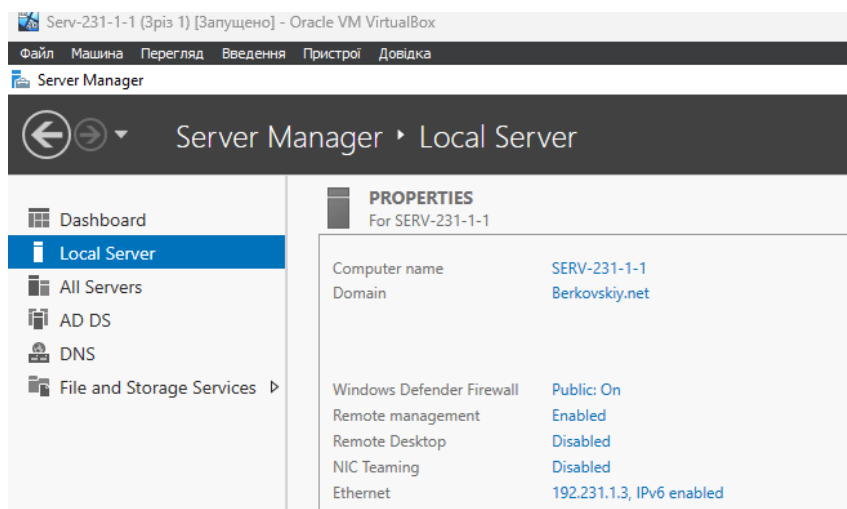


Рисунок 3.7 – Перевірка встановлення

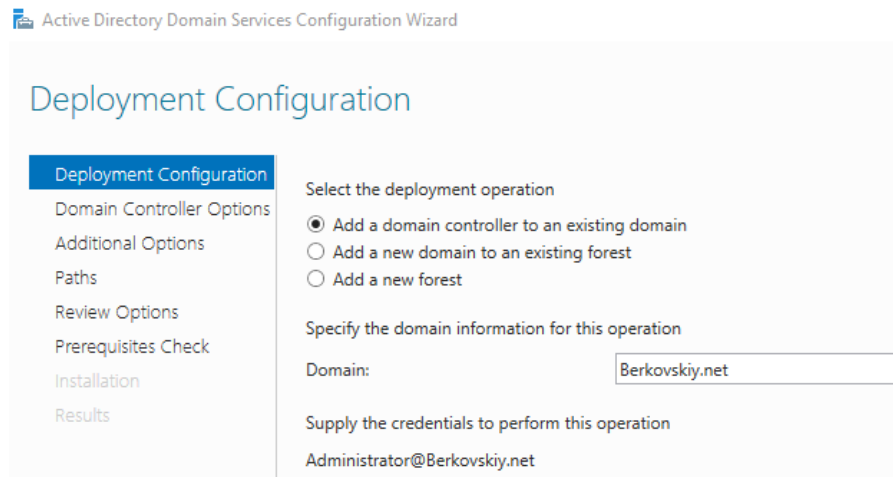


Рисунок 3.8 – Приєднання до домену Berkovskiy.net

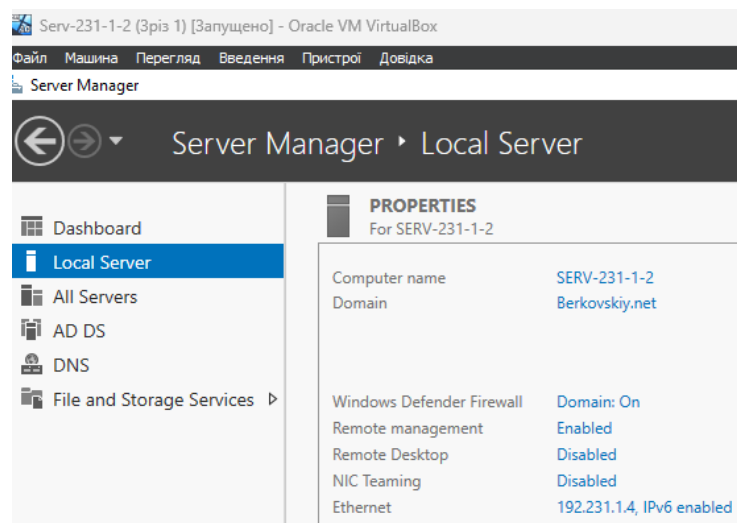


Рисунок 3.9 – Перевірка встановлення

Далі виконуємо реєстрацію об'єктів користувача. Натискаємо правою кнопкою миші (Користувачі) у створеному домені Active Directory.

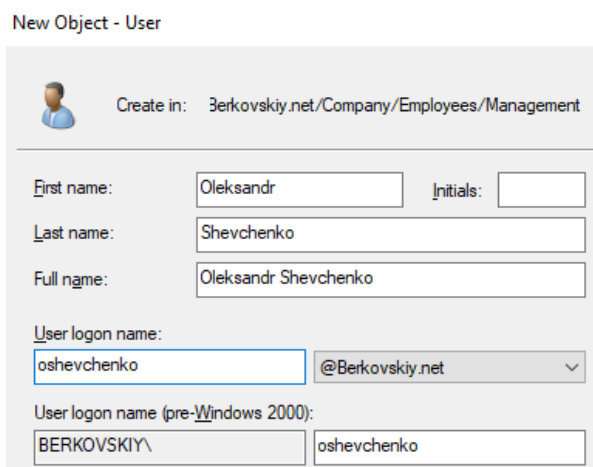


Рисунок 3.10 – Створення нового користувача і встановлення пароля

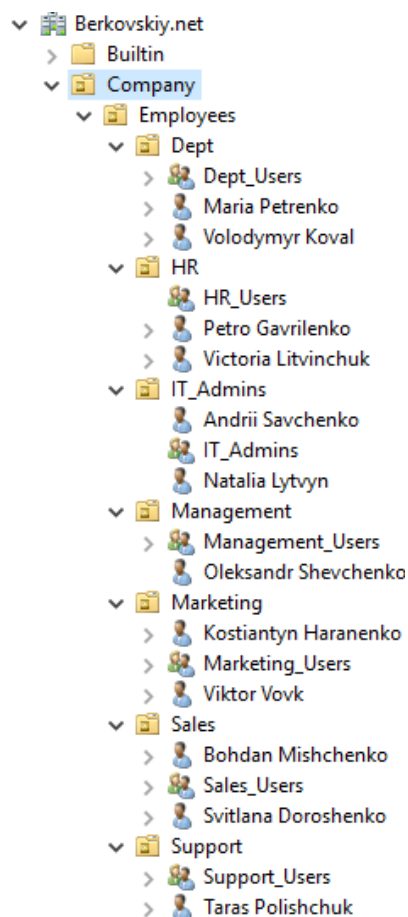


Рисунок 3.11 – Створення локальних груп і додавання в них користувачів

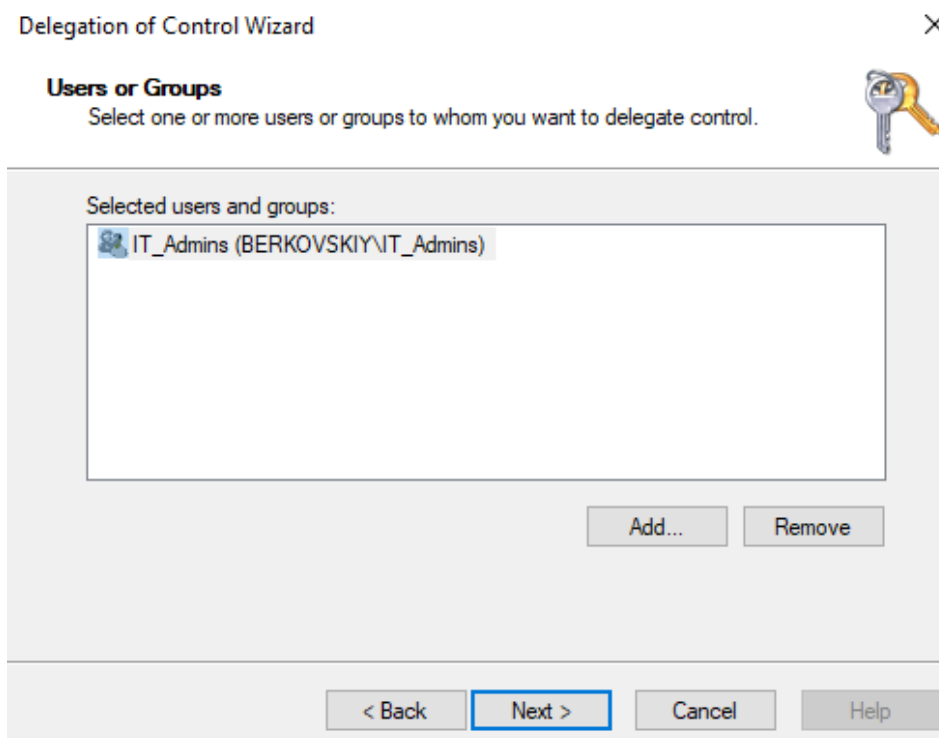


Рисунок 3.12 – Додавання групи для делегації контролю

Далі виконуємо налаштування реплікації між двома контролерами домену в Active Directory.

Далі робимо налаштування протоколу динамічного конфігурування вузлів DHCP для домену Active Directory

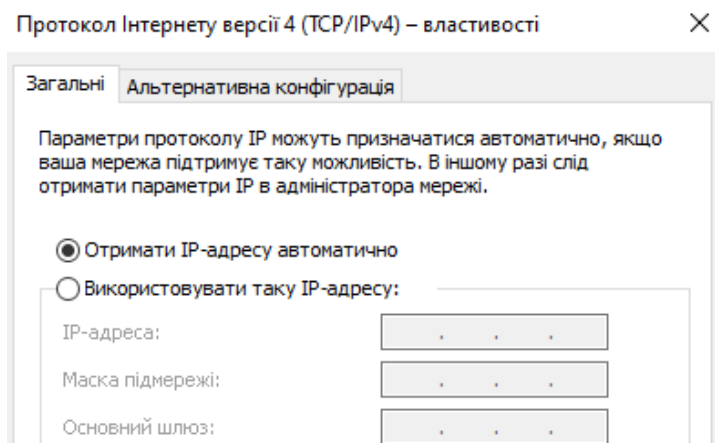


Рисунок 3.13 – Отримання IP-адреси автоматично, аналогічно на WS_231_1_2 - WS_231_1_6

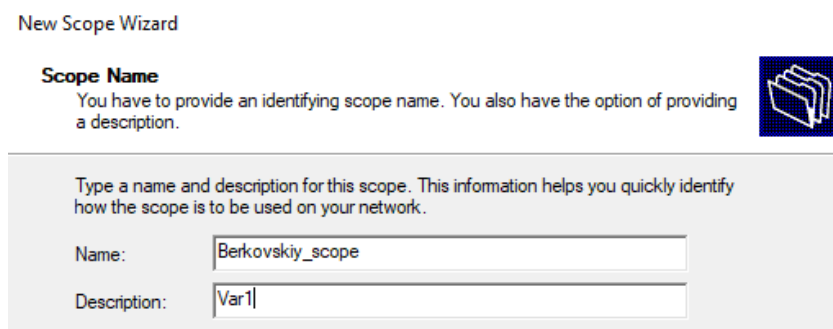


Рисунок 3.14 – Створення області

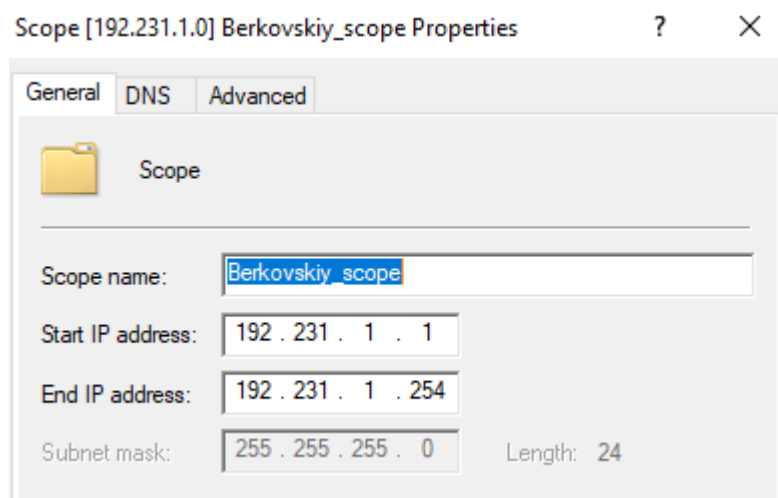


Рисунок 3.15 – Діапазон адрес

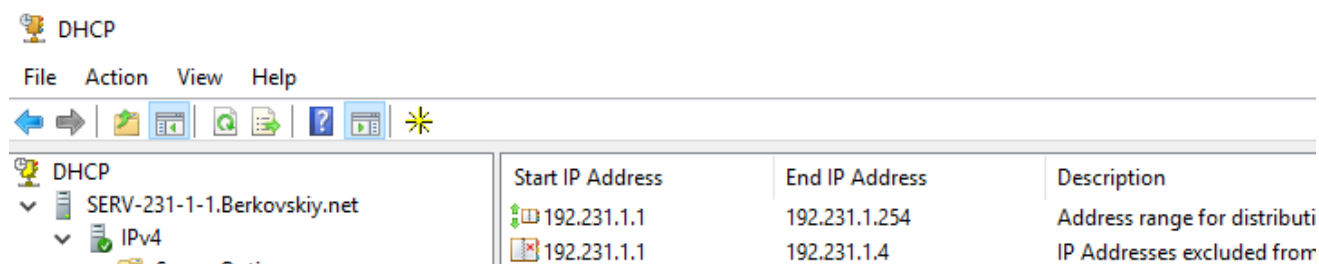


Рисунок 3.16 – Виключені адреси

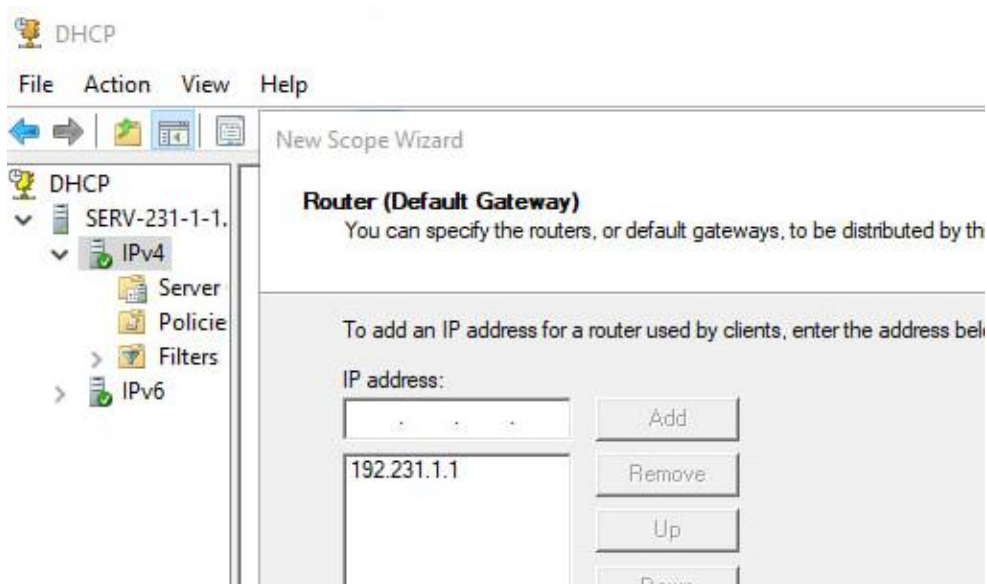


Рисунок 3.17 – Конфігурація роздачі шлюзу

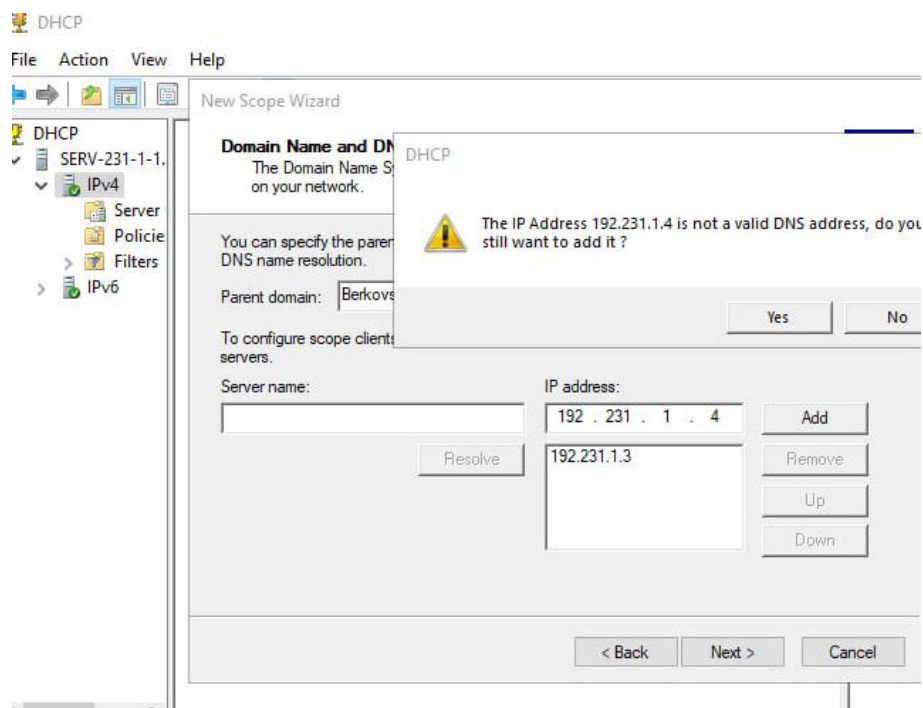


Рисунок 3.18 – Автоматична генерація батьківського домену та DNS-серверу

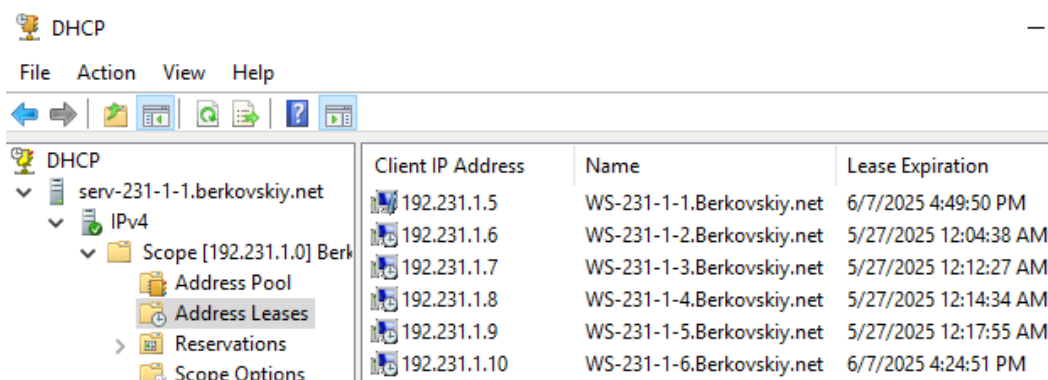


Рисунок 3.19 – Створена область та відображення орендованих IP-адрес

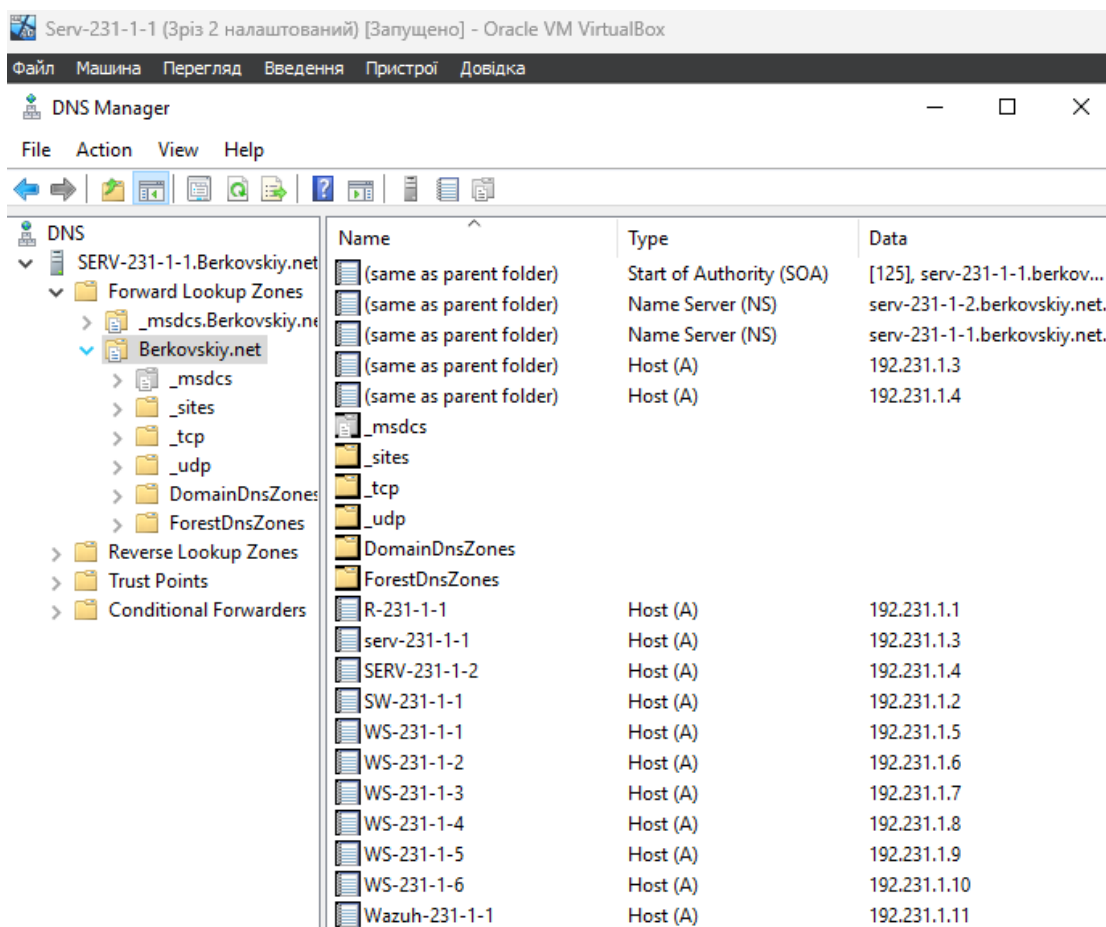


Рисунок 3.20 – Додані DNS-запити типу А

У процесі налаштування корпоративної мережі було додано ролі служб, налаштовано IP-адресацію серверів, включаючи сервер Wazuh, та створено домен в Active Directory. Виконано реєстрацію об'єктів користувачів, створено локальні групи, додано користувачів до груп і делеговано контроль доступу. Реалізовано реплікацію між контролерами домену для забезпечення їх узгодженої роботи. Налаштовано протокол DHCP для автоматичної видачі IP-

адрес із врахуванням виключених адрес і конфігурації шлюзу. Завершено створення DNS-запитів типу A, що забезпечило стабільну роботу мережі з централізованим управлінням.

3.3 Інтеграція та налаштування системи моніторингу Wazuh

Після успішного налаштування Wazuh-сервера та запуску його на базі OVA-образу доступ до веб-інтерфейсу здійснюється через браузер, ввівши IP-адресу Wazuh-сервера. У цьому випадку була використана IP-адреса 192.231.1.11, яка була попередньо вказана під час налаштування сервера. У браузері вводиться адреса: <https://192.231.1.11>, після чого відкривається сторінка входу до Wazuh Dashboard. На сторінці авторизації (рис. 3.21) користувач вводить створені раніше облікові дані адміністратора. У нашому випадку це логін admin і попередньо заданий пароль.

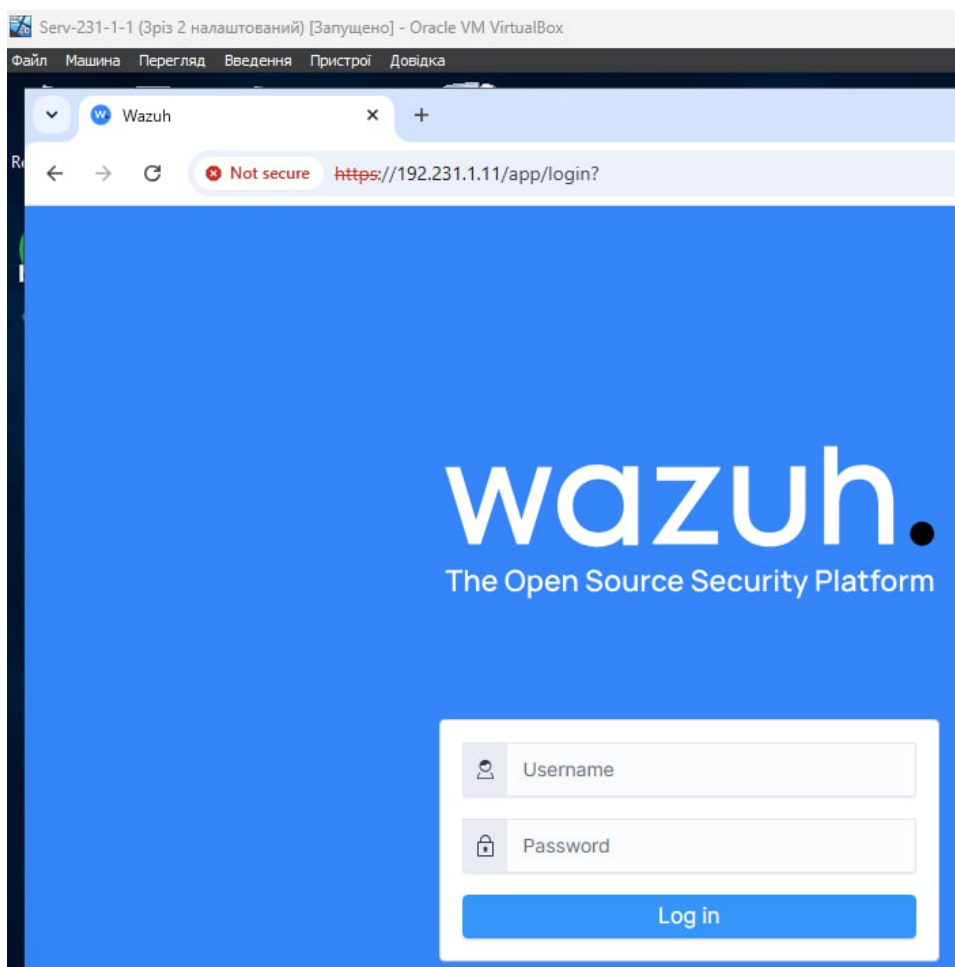


Рисунок 3.21 – Вхід до веб-інтерфейсу Wazuh за IP-адресою 192.231.1.11

Після натискання кнопки Log in система завантажує основний інтерфейс Wazuh Dashboard.

Головна сторінка інтерфейсу (рис. 3.22) відображає загальну інформацію про статус системи, кількість підключених агентів, активні загрози та інші дані. На цьому етапі підключені агенти відсутні, оскільки їх додавання ще не було виконано. Це підтверджує коректну роботу веб-інтерфейсу та готовність до подальшого налаштування системи.

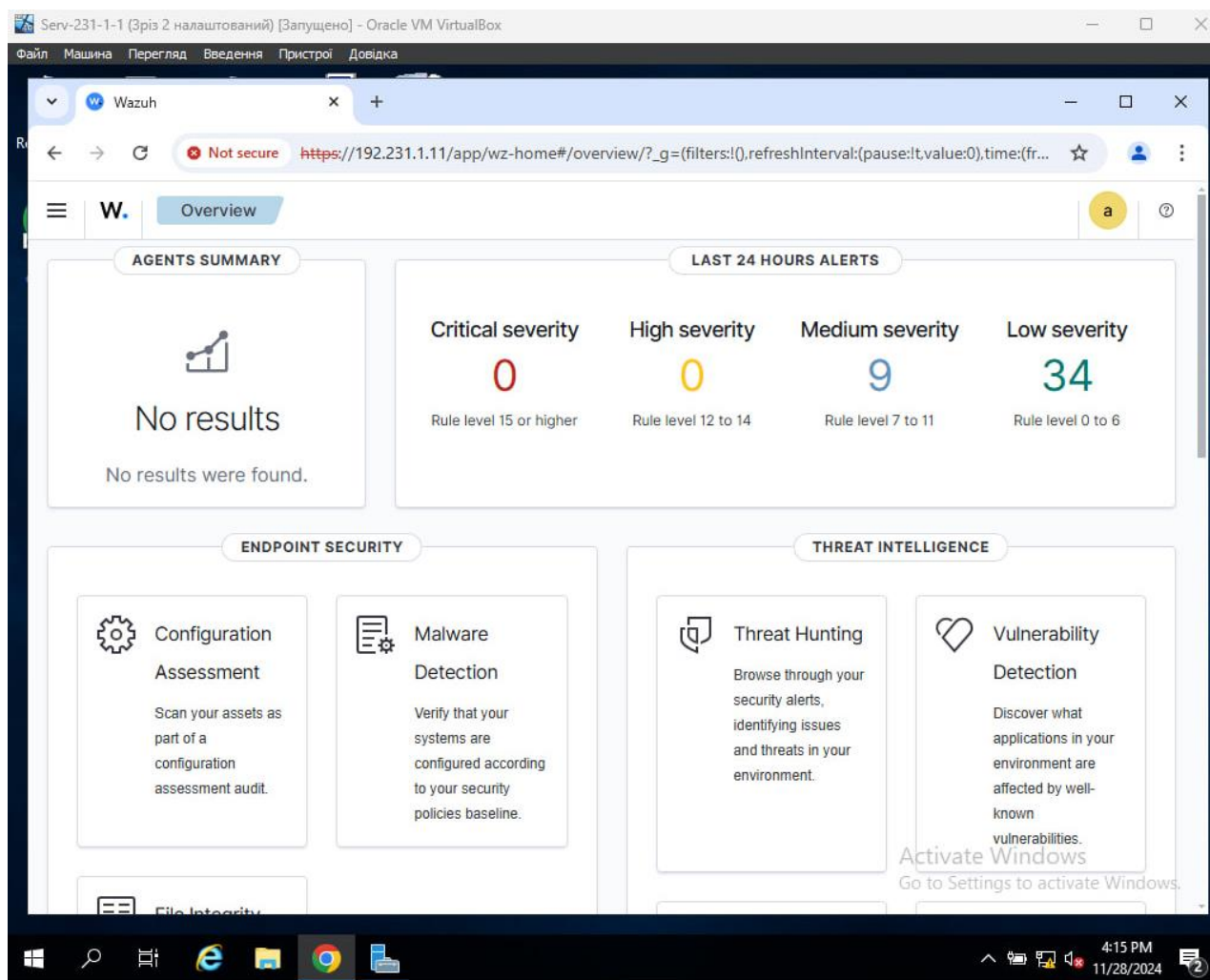


Рисунок 3.22 – Інтерфейс Wazuh статус агентів та оповіщення

Для моніторингу станцій та серверів необхідно встановити агенти Wazuh на кожен із вузлів мережі. Інсталяційні файли агентів були завантажені з офіційного сайту Wazuh (<https://documentation.wazuh.com>) відповідно до типу

операційної системи. Для пристроїв на базі Windows було завантажено інсталяційний пакет wazuh-agent.msi, далі виконується інсталяція файлу.

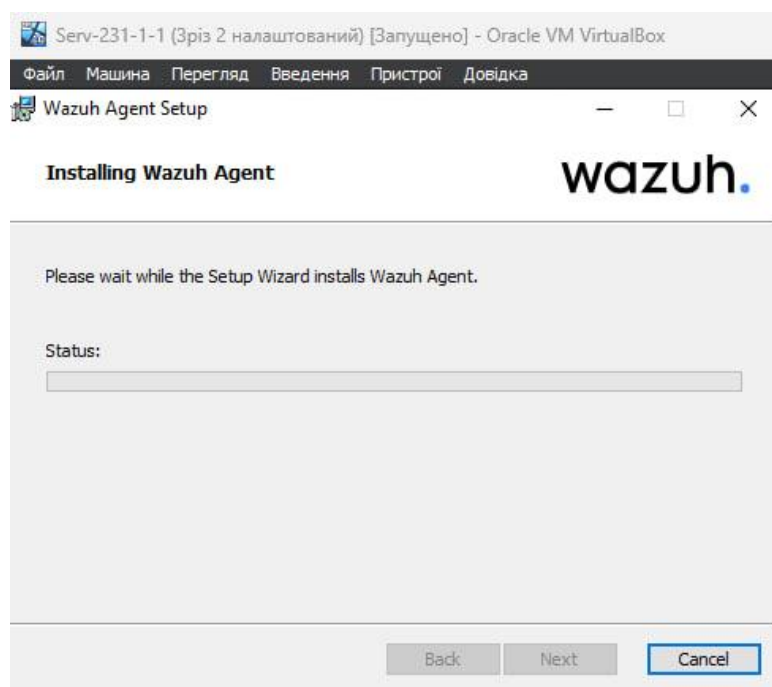


Рисунок 3.23 – Процес встановлення агента Wazuh

Після встановлення агента (рис. 3.24) на станціях необхідно додати їх до Wazuh Dashboard. Це робиться через веб-інтерфейс, де в меню налаштувань вибирається розділ для керування агентами. У цьому розділі додається новий агент, у якого вказується назва вузла та IP-адреса.

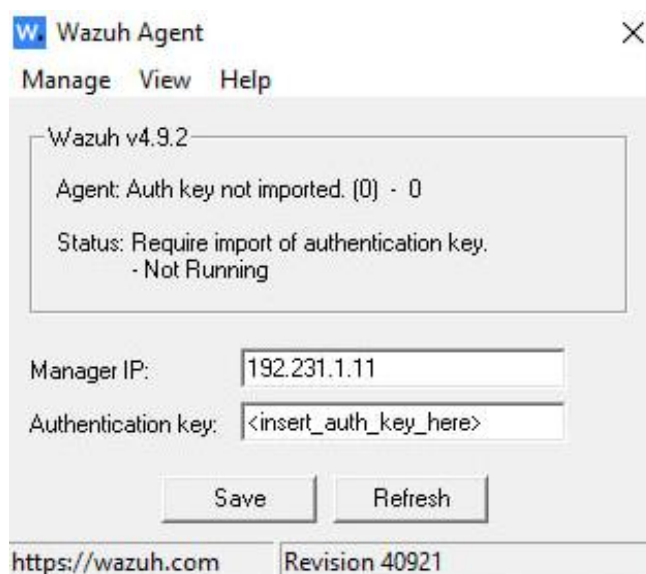


Рисунок 3.24 – Додавання нового агента Wazuh

Система автоматично виконує перевірку підключення агента до сервера. Якщо налаштування виконані правильно, на Wazuh Dashboard з'являється інформація про підключений вузол.

Після додавання агентів (рис. 3.25) проводиться тестування їх роботи. У веб-інтерфейсі перевіряється отримання журналів подій із підключених станцій. У разі успішної інтеграції агента на Dashboard можна побачити дані про активність станцій, виявлені загрози чи інші інциденти безпеки.

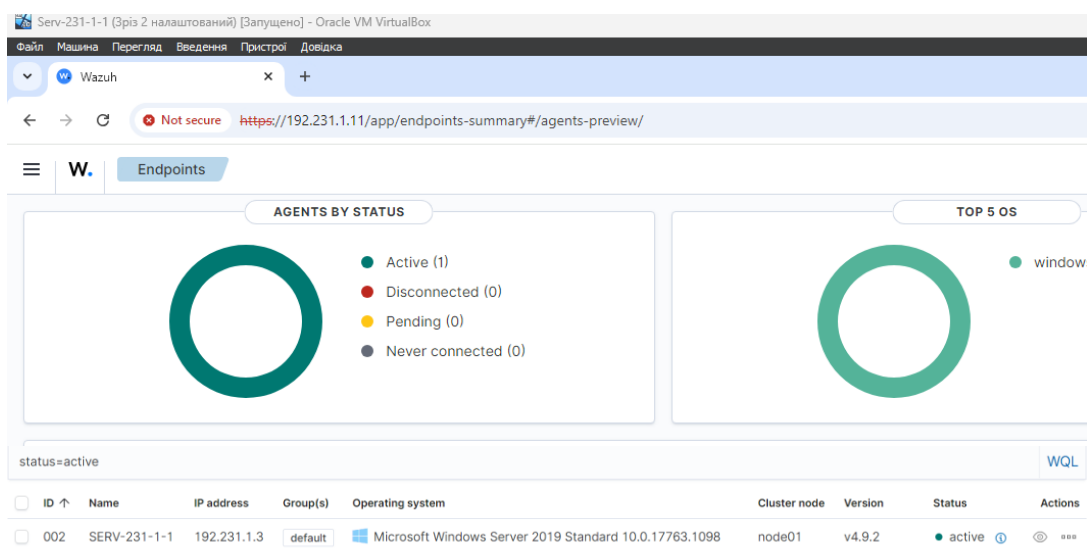


Рисунок 3.25 – Перевірка підключення агента до сервера та тестування його роботи на Wazuh Dashboard

На рисунку (3.26) можна побачити активний статус агента та створений ключ авторизації, що підтверджує коректність налаштування агента.

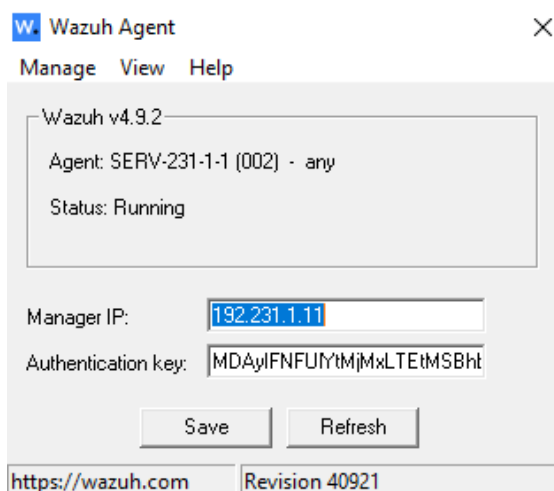


Рисунок 3.26 – Перегляд змін агента Wazuh

Після встановлення IP-адреси або FQDN (повного доменного імені) сервера Wazuh, агент Wazuh автоматично запитує ключ клієнта та імпортує його для авторизації. Цей процес забезпечує швидку й безпечну реєстрацію агента на сервері.

Ключ авторизації Wazuh, також відомий як ключ агента або реєстраційний токен, створюється на сервері Wazuh для кожного нового агента під час його реєстрації. Він забезпечує унікальну прив'язку агента до сервера і використовується для автентифікації та встановлення захищеного з'єднання. Ключ містить зашифровані дані, що гарантують конфіденційність та цілісність інформації. Формується він за допомогою криптографічних алгоритмів і зазвичай представлений у форматі Base64 як довгий рядок символів. Цей ключ необхідний для авторизації агента при підключенні до сервера і є важливим елементом безпечної взаємодії в системі Wazuh.

3.4 Аналіз логів та інцидентів безпеки за допомогою Wazuh

Розглянемо інтерфейс Wazuh Dashboard (рис. 3.27), що використовується для моніторингу та аналізу подій безпеки. Особлива увага приділяється вкладці (Threat Hunting) та розділу (Events), де відображаються всі зібрані логи, які надходять від агентів, встановлених на клієнтських машинах чи серверах. Цей розділ є ключовим для виявлення потенційних загроз, аналізу активності користувачів і систем, а також забезпечення ефективного управління безпекою інфраструктури. На панелі (Overview), можна обрати розділ (Threat Intelligence). Після його вибору продовжуємо ознайомлення з інтерфейсом.

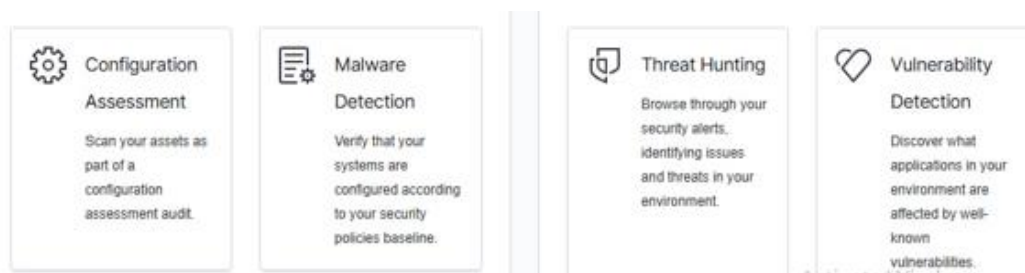


Рисунок 3.27 – Вибір розділу Threat Intelligence у списку.

На даному етапі у розділі Threat Intelligence Wazuh Dashboard відображається низка візуалізацій, які дозволяють проаналізувати отримані дані щодо інцидентів безпеки.

На рисунку 3.28 представлено статистику зафіксованих подій, де перша колонка показує загальну кількість подій (Total), друга — кількість критичних алертів рівня 12 і вище (Level 12 or above alerts), третя — кількість невдалих спроб авторизації (3 Failed Authentications), Остання колонка відображає кількість успішних авторизацій, що також пов'язана із загальною статистикою подій.

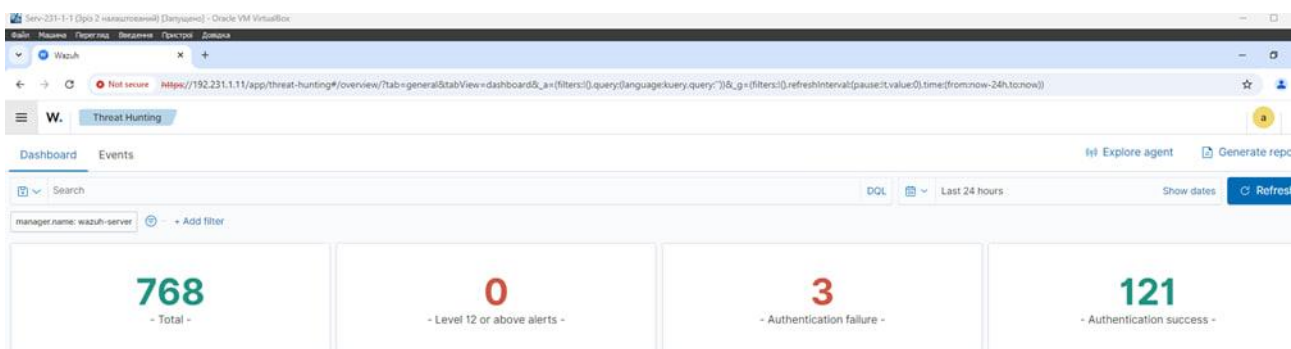


Рисунок 3.28 – Статистика зафіксованих подій

Після огляду статистичних даних на сторінці, далі представлено графіки, зокрема (Top 10 Alert LML Evolution), який демонструє динаміку найбільш критичних або часто виникаючих алертів, що дозволяє визначити події безпеки з найбільшим впливом на інфраструктуру.

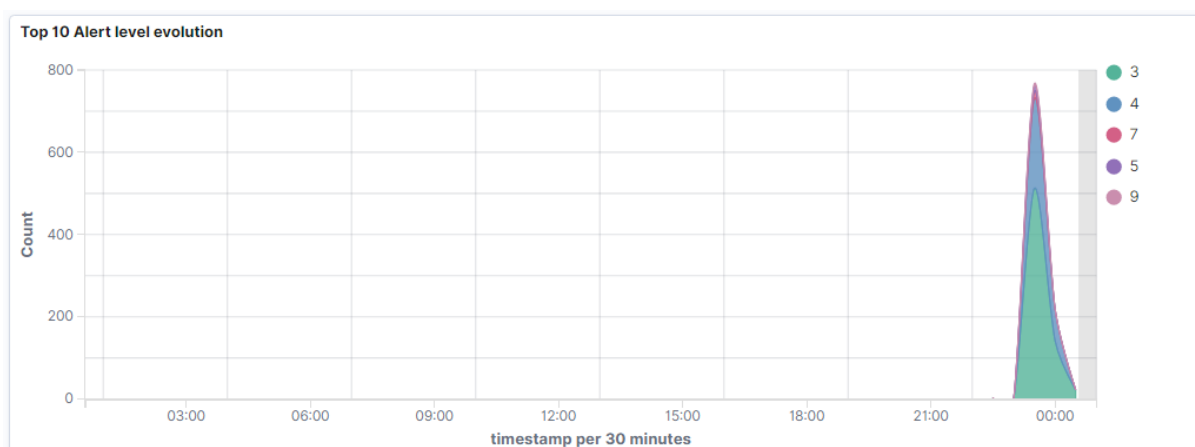


Рисунок 3.29 – Динаміка топ 10 тривога за рівнем впливу

Далі на сторінці представлено графік (Top 5 Agents), який показує активних агентів, серед яких Windows Server 2019 (SERV-231-1) та сервер Wazuh, забезпечуючи швидкий огляд активності системи.

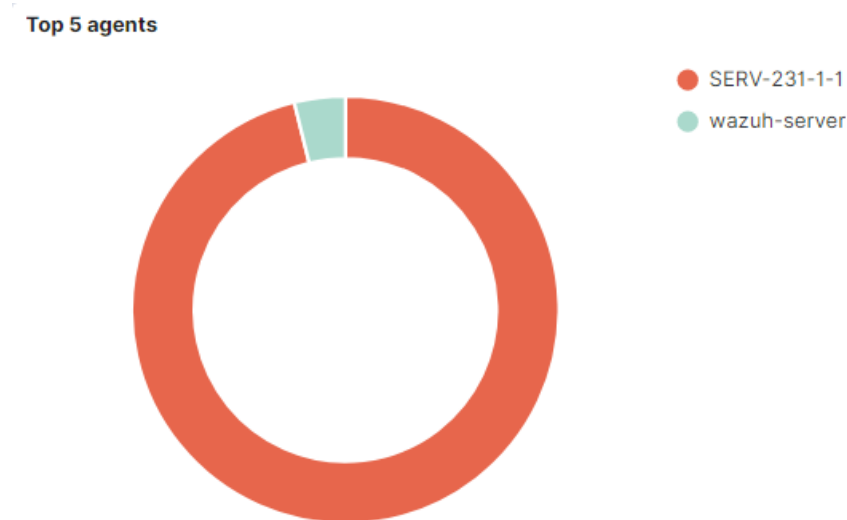


Рисунок 3.30 – Графік активних агентів

Далі на сторінці представлено графік категорій подій, який демонструє детальний розподіл подій за типами, зокрема активні облікові записи, використання команд sudo, зміни в політиках домену, доступ до облікових записів і спроби вимкнення або модифікації критичних елементів безпеки.

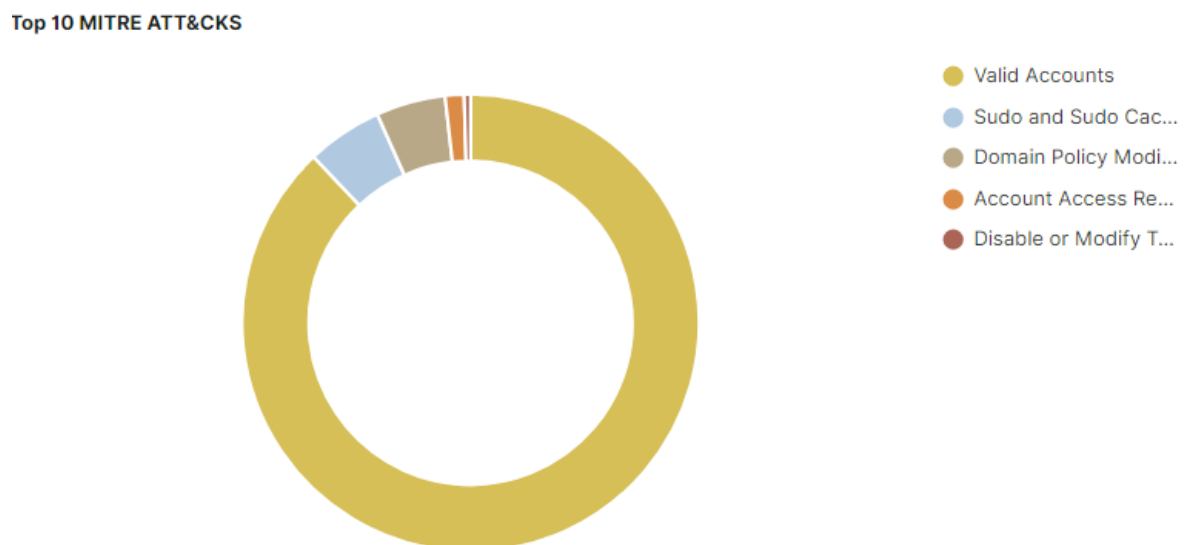


Рисунок 3.31 – Графік розподілу категорій подій

Переходимо до вкладки (Events), вона є критично важливою для моніторингу та аналізу подій безпеки, оскільки саме тут зібрані логи, які надходять від агентів, встановлених на клієнтських машинах і серверах.

Цей розділ (рис. 3.32) дозволяє перевіряти коректність збору логів та виявляти можливі загрози, адже події, які фіксуються агентами, можуть включати логи авторизації, аудити доступу до файлів і директорій, а також інформацію про аномальну активність.

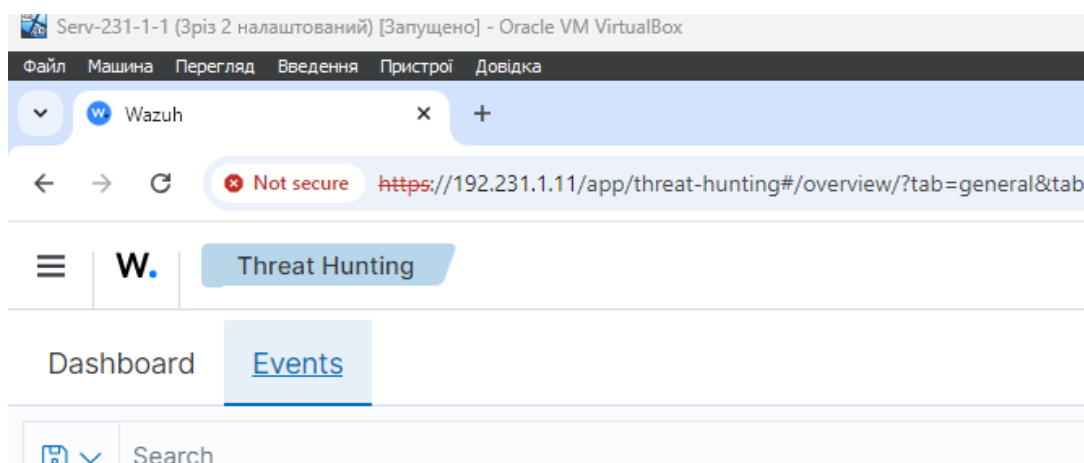


Рисунок 3.32 – Перехід до вкладки Events через розділ Threat Hunting

Спробуємо використати фільтрацію у вкладці (Events), щоб швидко знайти потрібну інформацію серед великої кількості логів. Цей інструмент (рис. 3.33) дозволяє зосередитися на подіях, які мають ключове значення для аналізу безпеки чи моніторингу інфраструктури. Наприклад, можна застосувати фільтр за ключовим словом (Authentication failure), щоб виявити всі невдалі спроби авторизації.

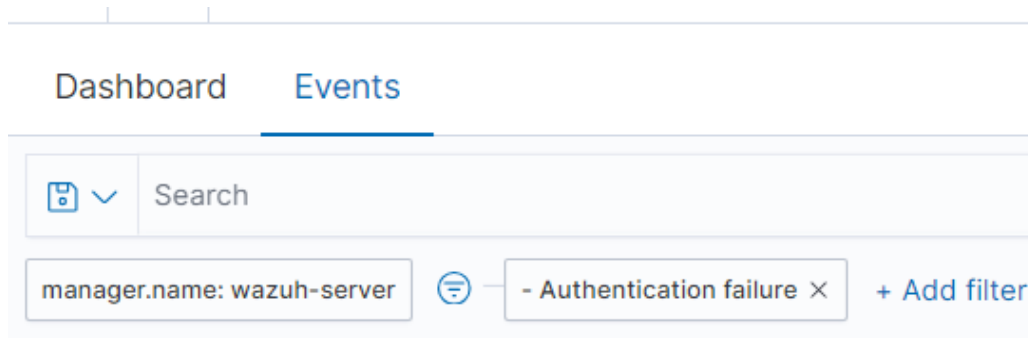


Рисунок 3.33 – Перехід до вкладки Events через розділ Threat Hunting

Після застосування фільтрації за ключовим словом (Authentication failure) у вкладці (Events), система видала три події. У таблиці відображаються важливі параметри, що дозволяють детально проаналізувати кожну з них. Перш за все, поле timestamp (мітка часу) фіксує точний момент виникнення події — у цьому випадку це було 14 грудня 2024 року о 23:54:50.929. Така деталізація дозволяє чітко визначити, коли сталася підозріла активність.

Поле (agent.name) ідентифікує пристрій, з якого був переданий лог. У даній події це агент із назвою SERV-231-1-1, що вказує на сервер або клієнтську машину, де було зафіксовано проблему. Опис події наведено в колонці (rule.description), яка вказує на те, що сталася невдала спроба авторизації з повідомленням: (Logon Failure - Unknown user or bad password). Це означає, що введений логін або пароль були некоректними, що може свідчити про помилку користувача або спробу несанкціонованого доступу.

Додаткову інформацію надає поле (rule.level), що відображає рівень важливості події. Для цієї події рівень дорівнює 5, що класифікується як низький або середній рівень серйозності. Поле (rule.id) дозволяє ідентифікувати унікальний ідентифікатор правила, яке було спрацьовано, — у цьому випадку це 60122. Завдяки цьому ID можна знайти деталі про правило у відповідній базі даних системи Wazuh, щоб зрозуміти, які умови викликали цю подію.

3 hits			
Dec 14, 2024 @ 00:03:47.261 - Dec 15, 2024 @ 00:03:47.261			
Export Formated 541 columns hidden Density 1 fields sorted Full screen			
	timestamp	agent.name	rule.description
	Dec 14, 2024 @ 23:54:50.929	SERV-231-1-1	Logon Failure - Unknown user or bad password
	Dec 14, 2024 @ 23:54:46.543	SERV-231-1-1	Logon Failure - Unknown user or bad password
	Dec 14, 2024 @ 23:54:41.468	SERV-231-1-1	Logon Failure - Unknown user or bad password

Рисунок 3.34 – Результат фільтрації подій у Wazuh Dashboard із ключовим словом (Authentication failure)

rule.level	rule.id
5	60122
5	60122
5	60122

Рисунок 3.35 – Результат фільтрації подій із відображенням рівня важливості та ідентифікатора правила у Wazuh Dashboard

У цій таблиці передбачена можливість перегляду розширеної версії логів. Для цього достатньо натиснути на ярлик із лупою з підказкою (Inspect document details). Ця функція дозволяє отримати детальний огляд події, включаючи всі пов'язані дані, що можуть бути корисними для глибокого аналізу логів.

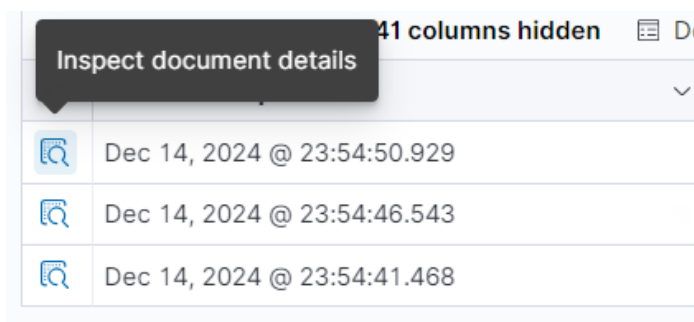


Рисунок 3.36 – Перехід до розширеної версії логів у Wazuh Dashboard

Далі представлено серію рисунків (рис. 3.37-3.40), які демонструють деталізовані дані логів у Wazuh Dashboard. Вони дозволяють візуалізувати ключову інформацію про події, пов'язані з безпекою, зокрема ідентифікатор агента, ім'я робочої станції, IP-адресу та інші важливі параметри, що допомагають у моніторингу та аналізі.

Document Details		View surrounding documents	View single document
Table	JSON		
t _index	wazuh-alerts-4.x-2024.12.15		
t agent.id	002		
t agent.ip	192.231.1.3		
t agent.name	SERV-231-1-1		

Рисунок 3.37 – Перехід до розширеної версії логів у Wazuh Dashboard

Важлива інформація з логів:

- Домен: BERKOVSKIY
- Цільовий користувач: Administrator
- Ім'я сервера: SERV-231-1-1
- Повне ім'я комп'ютера: SERV-231-1-1.Berkovskiy.net
- IP-адреса агента: 192.231.1.3
- Ідентифікатор агента: 002
- Ідентифікатор події: 4625 (невдала спроба входу)
- Причина помилки: Невірний пароль (status: 0xc000006d, subStatus: 0xc000006a)
- Ім'я робочої станції: SERV-231-1-1
- Опис правила: Logon Failure - Unknown user or bad password
- Канал: Security
- Тип входу: 2 (інтерактивний логін).

t	data.win.eventdata.status	0xc000006d
t	data.win.eventdata.subStatus	0xc000006a
t	data.win.eventdata.subjectDomain Name	BERKOVSKIY
t	data.win.eventdata.subjectLogonId	0x3e7
t	data.win.eventdata.subjectUserName	SERV-231-1-1\$
t	data.win.eventdata.subjectUserSid	S-1-5-18
t	data.win.eventdata.targetDomain Name	BERKOVSKIY
t	data.win.eventdata.targetUserName	Administrator
t	data.win.eventdata.targetUserSid	S-1-0-0
t	data.win.eventdata.workstationName	SERV-231-1-1
t	data.win.system.channel	Security
t	data.win.system.computer	SERV-231-1-1.Berkovskiy.net
t	data.win.system.eventID	4625

Рисунок 3.38 – Деталі невдалої спроби входу в систему Windows (подія 4625)

t	data.win.system.version	0
t	decoder.name	windows_eventchannel
t	id	1734249290.2994679
t	input.type	log
t	location	EventChannel
t	manager.name	wazuh-server
t	rule.description	Logon Failure - Unknown user or bad password
#	rule.firedtimes	3
t	rule.gdpr	IV_35.7.d, IV_32.2
t	rule.gpg13	7.1
t	rule.groups	windows, windows_security, authentication_failed
t	rule.hipaa	164.312.b
t	rule.id	60122
#	rule.level	5
🔗	rule.mail	false

Рисунок 3.39 – Деталі невдалої спроби входу в систему Windows (подія 4625)

Якщо натиснути на (View single document), відкриється розгорнута версія документа, яка надає повну інформацію про конкретний лог. У цьому режимі можна побачити всі деталі події у структурованому вигляді, включаючи додаткові атрибути, які не відображаються в стандартній таблиці. Це дає можливість детальніше вивчити лог, а також скопіювати його для подальшого аналізу або експорту. Така функція є корисною для глибшого розуміння події та для використання цієї інформації у звітах чи зовнішніх інструментах.

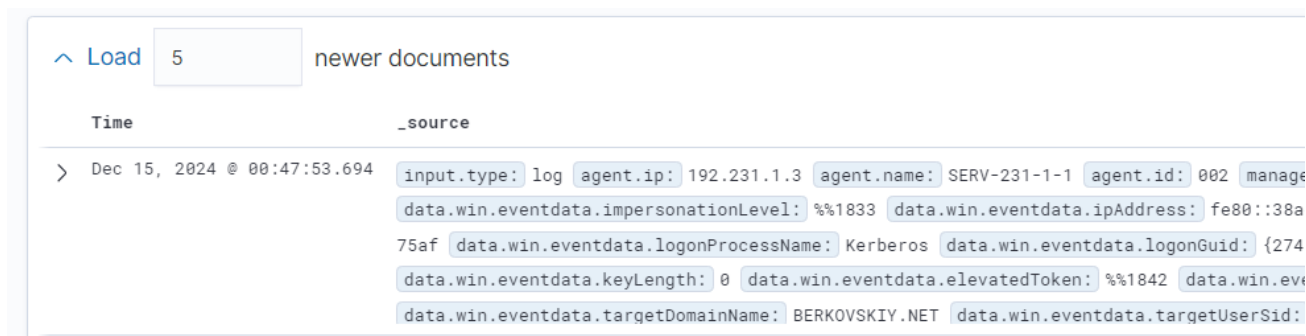


Рисунок 3.40 – Розгорнуті деталі події в Wazuh через опцію (View single document)

Перейдемо до розділу (Discover) через інтерфейс (Wazuh Dashboard) та застосуємо фільтр alerts, що дозволило знайти події відповідного рівня критичності (від 7 до 11). За допомогою цього інструмента (рис. 3.41) можна аналізувати отримані логи, а також визначати активність загроз у певний часовий проміжок. Це дає змогу швидко виявити потенційні проблеми та провести детальніший аналіз подій безпеки.

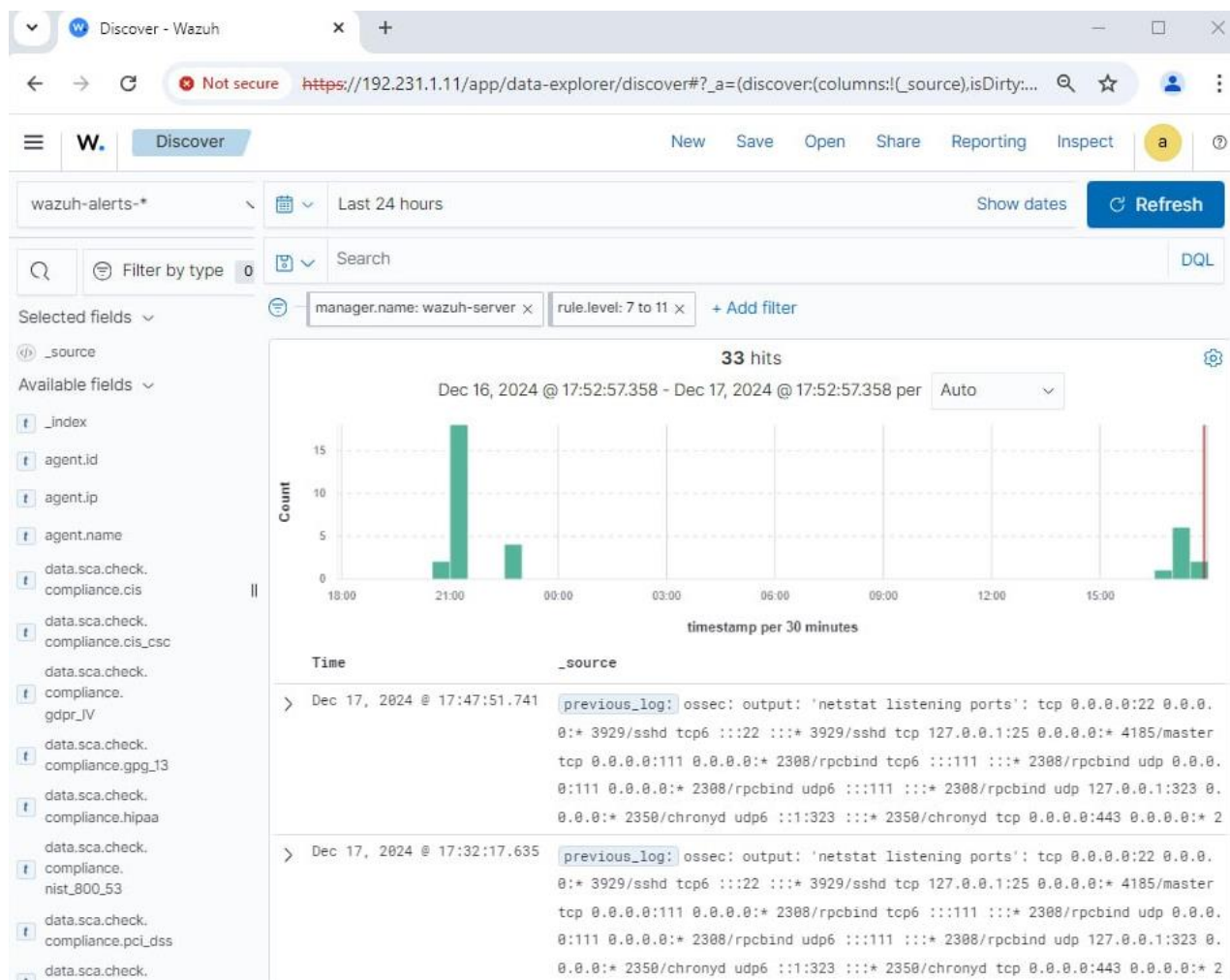


Рисунок 3.41 – інтерфейс Wazuh Dashboard у вкладці Discover

Розглянемо першу подію зі списку (рис. 3.42). Час події зафіксовано на 17:32:17 18 грудня 2024 року. Логи зібрані з (wazuh-server), про що свідчить поле (manager.name). Тип введення позначений як (log), а місце події визначено як (netstat listening ports), що вказує на перевірку відкритих портів сервера. У полі (full_log) відображається результат команди (netstat), де показано активні TCP та

UDP-з'єднання на сервері, включно з портами (3864/sshd, 2380/rpcbind) та іншими службами. Також наведено (previous_log), що дозволяє порівняти поточний стан портів із попереднім виводом для відстеження змін. Цей аналіз дозволяє оцінити роботу сервера, перевірити активні з'єднання та виявити потенційні загрози або незвичну активність у мережі.

index	wazuh-alerts-4.x-2024.12.18
agent.id	000
agent.name	wazuh-server
decoder.name	ossec
full_log	> ossec: output: 'netstat listening ports': tcp 0.0.0.0:22 0.0.0.0:* 3864/sshd tcp6 :::22 :::* 3864/sshd tcp 127.0.0.1:25 0.0.0.0:* 4160/master tcp 0.0.0.0:111 0.0.0.0:* 2381/rpcbind tcp6 :::111 :::* 2381/rpcbind udp 0.0.0.0:111 0.0.0.0:* 2381/rpcbind
id	1734486471.1915017
input.type	log
location	netstat listening ports
manager.name	wazuh-server
previous_log	> ossec: output: 'netstat listening ports': tcp 0.0.0.0:22 0.0.0.0:* 3929/sshd tcp6 :::22 :::* 3929/sshd tcp 127.0.0.1:25 0.0.0.0:* 4185/master tcp 0.0.0.0:111 0.0.0.0:* 2308/rpcbind
rule.description	Listened ports status (netstat) changed (new port op
rule.firedtimes	1
rule.gdpr	IV_35.7.d
rule.gpg13	10.1
rule.groups	ossec
rule.hipaa	164.312.b
rule.id	533
rule.level	7
rule.mail	false
rule.nist_800_53	AU.14, AU.6
rule.pci_dss	10.2.7, 10.6.1
rule.tsc	CC6.8, CC7.2, CC7.3
timestamp	Dec 17, 2024 @ 17:47:51.741

Рисунок 3.42 – Деталі першої події у Wazuh Discover

Таким чином, за допомогою інструменту Wazuh Discover вдалося зібрати та проаналізувати події відповідного рівня. Використовуючи застосовані фільтри, можна переглядати детальну інформацію про кожну подію, зокрема час, джерело, агент та інші важливі параметри. Це дозволяє ефективно моніторити стан системи, оперативно виявляти потенційні загрози та приймати відповідні рішення для забезпечення безпеки інфраструктури.

Висновки до третього розділу

В даному розділі було описано процес створення бази даних каталогу за допомогою Active Directory у Windows Server та перевірено її працездатність. Було проведено налагодження пристроїв для функціонування корпоративної мережі і перевірено зв'язок між ними.

Окрім цього, було реалізовано збір та перегляд логів за допомогою інструменту Wazuh. Було застосовано фільтри для аналізу подій різного рівня, розглянуто конкретні логи, їхні деталі та час виникнення. Це дозволило оцінити працездатність системи моніторингу, виявити важливі події та перевірити коректність передачі даних від агентів до сервера.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було реалізовано налаштування Active Directory на базі Windows Server для створення захищеної IT-інфраструктури корпоративної мережі, що відповідає темі роботи «Методи та технології захищеної IT-інфраструктури корпоративної мережі на базі ОС Windows та Active Directory».

У першому розділі досліджено ключові функції, типи та призначення Active Directory (AD), яка забезпечує централізоване управління обліковими записами користувачів, аутентифікацію та авторизацію в мережах. Крім того, було проведено огляд SIEM-рішень, серед яких виділено Wazuh як ефективний інструмент для моніторингу подій та виявлення загроз.

У другому розділі виконано детальний аналіз мережевих топологій, розроблено загальну схему корпоративної мережі та підібрано відповідне обладнання. Було також створено схему IP-адресації з урахуванням кількості пристроїв і використанням динамічної адресації. Для забезпечення безпеки реалізовано механізми резервного копіювання, реплікації даних та впроваджено групові політики (GPO), що дозволяють централізовано управляти доступом.

У третьому розділі було описано процес створення бази даних каталогу за допомогою Active Directory у Windows Server та перевірено її працездатність. Проведено налагодження пристроїв для функціонування корпоративної мережі та перевірено зв'язок між ними, що підтвердило стабільність і ефективність роботи інфраструктури. Було налаштовано систему моніторингу Wazuh для збору та аналізу логів. Це дозволило ефективно відслідковувати події в корпоративній мережі, своєчасно виявляти потенційні загрози та контролювати стан систем.

Виконання кваліфікаційної роботи дало змогу здобути поглиблені теоретичні знання та практичні навички в проєктуванні, налаштуванні та захисті корпоративної мережі на базі Active Directory.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Маду Д. Інструменти керування Active Directory: що це таке та все, що вам потрібно про це знати [Електронний ресурс] / Дженніфер Маду // businessyield.com. – 2023. – Режим доступу до ресурсу: <https://businessyield.com/uk/management/active-directory-management-tools/>.
2. Що ж таке Active Directory? [Електронний ресурс] / Job. Career.. – 2012. – Режим доступу до ресурсу: <https://qagroup.com.ua/publications/what-is-active-directory/>.
3. Групове керування користувачами Active Directory [Електронний ресурс] // ADmanagerPlus. – 2013. – Режим доступу до ресурсу: https://www.manageengine.com/products/ad-manager/uk-ua/active_directory_bulk_user_management.html.
4. Топологія комп'ютерів [Електронний ресурс] // Copyright Comp-Net.at.ua. – 2009. – Режим доступу до ресурсу: https://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6.
5. Поради по установці, налаштуванні і роботі з Microsoft Windows. [Електронний ресурс] // telusuri.info . – 2023. – Режим доступу до ресурсу: <https://www.telusuri.info/articles/windows/chto-takoe-powershell.html>.
6. Романець А. В. Види топологій [Електронний ресурс] / Андрій Володимирович Романець // ТОВ «Всеосвіта». – 2017. – Режим доступу до ресурсу: <https://vseosvita.ua/lesson/vydy-topolohii-341873.html>.
7. How to Setup Active Directory Domain With VirtualBox [Електронний ресурс] // www.kindsonthegenius.com. – 2020. – Режим доступу до ресурсу: <https://www.kindsonthegenius.com/how-to-setup-active-directory-domain-with-virtualbox-and-join-computers-part-1/>.
8. Архітектура Active Directory [Електронний ресурс] // studfile.net. – 2015. – Режим доступу до ресурсу: <https://studfile.net/preview/4603396/page:2/>.
9. Що таке інформаційна безпека (InfoSec)? | Захисний комплекс Microsoft. Your request has been blocked. This could be due to several reasons.

– Режим доступу до ресурсу: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-information-security-infosec>.

10. Що таке SIEM? | Захисний комплекс Microsoft. [Електронний ресурс] // [www.microsoft.com](https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem). – 2024. – Режим доступу до ресурсу: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem>

11. Wazuh - платформа безпеки з можливостями XDR та SIEM | ESKA. ESKA. – Режим доступу до ресурсу: <https://eska.global/products/wazuh>.

12. Wazuh - CoreWin. CoreWin. – Режим доступу до ресурсу: <https://corewin.ua/en/security/wazuh/>

13. Blocking SSH brute-force attack with Active Response - Use cases. Wazuh documentation. – Режим доступу до ресурсу: <https://documentation.wazuh.com/current/user-manual/capabilities/active-response/ar-use-cases/blocking-ssh-brute-force.html>About>

14. Splunk | What is Splunk?. Splunk. – Режим доступу до ресурсу: https://www.splunk.com/en_us/about-splunk.html

15. Get started with Elastic Observability | Elastic Observability [8.17] | Elastic. Elastic – The Search AI Company | Elastic. – Режим доступу до ресурсу: <https://www.elastic.co/guide/en/observability/current/observability-get-started.html>.

16. N-iX - Building Security Management Platform for AlienVault, part of AT&T. Software Development Company - N-iX. – Режим доступу до ресурсу: <https://www.n-ix.com/clients/alienvault/>.

17. Cisco 4331 Integrated Services Router. Cisco. – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/routers/4331-integrated-services-router-isr/model.html>.

18. Cisco Catalyst 2960 Series Switches. Cisco. – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html?dtid=osscdc000283>.