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 засоби Graylog для підвищення рівня безпеки Microsoft Active Directory»

Виконав: студент 2-го курсу групи КБм-24-1
спеціальності 125 «Кіберберзпека та захист інформації»
_____ Євгеній ШИТОВ
Керівник: старший викладач кафедри КІ та КБ
_____ Ігор ФАЛЬКОВСЬКИЙ
Рецензент: доцент кафедри КІ та КБ, к.пед.н.
_____ Олена ГОЛОВНЯ

Житомир – 2025

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

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
_____ Андрій ЄФІМЕНКО
6 жовтня 2025 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу магістра

Студент: Шитов Євгеній Артемович

Тема роботи: «Методи та засоби Graylog для підвищення рівня безпеки Microsoft Active Directory»

затверджена Наказом університету від 6 жовтня 2025 р. № 566/с

Термін здачі студентом закінченої роботи 22 грудня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
Об'єктом дослідження є процес забезпечення інформаційної безпеки та моніторингу подій у середовищі контролерів домену Microsoft Active Directory. Предметом дослідження є методи та засоби централізованого збору, аналізу та кореляції подій безпеки з використанням платформи Graylog для виявлення кіберзагроз та автоматизованого реагування на інциденти.

Обладнання та програмне забезпечення:

1. Персональний комп'ютер з встановленим гіпервізором VMware Workstation.
2. Серверна операційна система Ubuntu 22.04 LTS (для розгортання SIEM).

3. Серверна операційна система Windows Server 2022 Standard (контролер домену).
4. Платформа для управління логами Graylog 6.0.
5. Система індексації та пошуку OpenSearch 2.12, СКБД MongoDB 6.0.
6. Агент транспортування логів Winlogbeat.
7. Месенджер Discord (для отримання сповіщень про інциденти).
8. Тестові утиліти для симуляції атак (файл EICAR).

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Завідувач кафедри КІ та КБ, к.т.н., доцент Андрій ЄФІМЕНКО	6.10.25	06.10.25

Студент _____ Шитов Євгеній

Керівник _____ Ігор Фальковський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання, аналіз літературних джерел та нормативної бази за темою дослідження.	17.09.2025 – 25.09.2025	Виконано
2	Написання Розділу 1. Аналіз існуючих рішень (Graylog, Splunk, ELK) та загроз безпеці Active Directory.	26.09.2025 – 10.10.2025	Виконано
3	Проектування архітектури тестового стенду та вибір програмного забезпечення (початок Розділу 2).	11.10.2025 – 20.10.2025	Виконано
4	Розгортання віртуального середовища, встановлення та налаштування сервера Graylog, MongoDB, OpenSearch.	21.10.2025 – 05.11.2025	Виконано
5	Налаштування політик аудиту Active Directory та конфігурація агента Winlogbeat для збору логів.	06.11.2025 – 15.11.2025	Виконано
6	Проведення експериментальних досліджень: моделювання атак (Brute Force, EICAR) та їх детектування.	16.11.2025 – 25.11.2025	Виконано
7	Написання Розділу 3. Аналіз результатів, створення дашбордів візуалізації та налаштування сповіщень.	26.11.2025 – 05.12.2025	Виконано
8	Оформлення вступу, висновків, списку літератури та додатків. Перевірка роботи на нормоконтроль.	06.12.2025 – 10.12.2025	Виконано
9	Попередній захист роботи на кафедрі, перевірка на плагіат, отримання відгуку керівника.	11.12.2025 – 14.12.2025	Виконано
10	Подання закінченої роботи на кафедру.	17.12.2025	Виконано

Студент _____ Шитов Євгеній

Керівник _____ Ігор Фальковський

АНОТАЦІЯ

Випускна кваліфікаційна робота магістра складається з пояснювальної записки, яка містить вступ, три розділи, висновки, список використаної літератури та додатки. Текстова частина викладена на 73 сторінках друкованого тексту. Пояснювальна записка має 5 сторінок додатків. Список використаних джерел містить 28 найменувань і займає 3 сторінки. В роботі наведено 62 рисунки. Загальний обсяг роботи – 78 сторінок.

У вступі обґрунтовано актуальність теми дослідження, яка зумовлена необхідністю захисту критичної інфраструктури Active Directory від сучасних кіберзагроз, зазначено мету та завдання роботи, визначено об'єкт та предмет дослідження.

Розділ 1 «Аналіз системи реєстрації подій Graylog та її аналогів» присвячено теоретичному аналізу проблем безпеки контролерів домену та огляду інструментів централізованого моніторингу. Проведено порівняльний аналіз функціональних можливостей систем Graylog, Splunk та ELK Stack, визначено основні типи загроз та сформульовано вимоги до системи захисту.

Розділ 2 «Проектування та розгортання системи моніторингу безпеки» описує технічну реалізацію проекту. Детально розглянуто процес розгортання лабораторного стенду на базі віртуальних машин, інсталяцію та налаштування компонентів SIEM-системи, конфігурацію політик аудиту Active Directory та налаштування агента Winlogbeat для транспортування логів.

Розділ 3 «Експериментальне дослідження ефективності системи» містить результати практичної перевірки розробленого рішення. Реалізовано сценарії типових кібератак (Brute Force, несанкціоноване створення користувачів, ескалація привілеїв, вірусна активність) та продемонстровано їх успішне детектування. Описано створення аналітичних дашбордів та налаштування автоматичного сповіщення в Discord. Проведено оцінку ефективності системи шляхом порівняння часу реакції на інциденти.

У висновках підведено підсумки проведеного дослідження, які підтверджують, що впровадження запропонованої системи дозволяє забезпечити моніторинг інцидентів у реальному часі. Список використаної літератури містить джерела, використані під час написання роботи.

Ключові слова: кібербезпека, Active Directory, SIEM, Graylog, Winlogbeat, моніторинг подій, аналіз логів, детектування атак, Brute Force, автоматичне сповіщення.

ANNOTATION

The Master’s qualification thesis consists of an explanatory note, which contains an introduction, three chapters, conclusions, a list of references, and appendices. The text part is presented on 73 pages of printed text. The explanatory note has 5 pages of appendices. The list of references contains 28 items and occupies 3 pages. The paper presents 62 figures. The total volume of the work is 78 pages.The introduction substantiates the relevance of the research topic, which is driven by the necessity to protect critical Active Directory infrastructure from modern cyber threats. It specifies the goal and tasks of the work, and defines the object and subject of the research.

Section 1, "Analysis of the Graylog Event Logging System and its Analogues," is devoted to the theoretical analysis of domain controller security problems and an overview of centralized monitoring tools. A comparative analysis of the functional capabilities of Graylog, Splunk, and ELK Stack systems was conducted, the main types of threats were defined, and requirements for the security system were formulated.

Section 2, "Design and Deployment of the Security Monitoring System," describes the technical implementation of the project. It examines in detail the process of deploying a laboratory stand based on virtual machines, the installation and configuration of SIEM system components, the configuration of Active Directory audit policies, and the setup of the Winlogbeat agent for log transport.

Section 3, "Experimental Research of System Effectiveness," contains the results of the practical verification of the developed solution. Scenarios of typical cyberattacks (Brute Force, unauthorized user creation, privilege escalation, virus activity) were implemented, and their successful detection was demonstrated. The creation of analytical dashboards and the configuration of automatic notification in Discord are described. An evaluation of the system's effectiveness was conducted by comparing incident response times. The conclusions summarize the conducted research, confirming that the implementation of the proposed system allows for real-time. The list of references contains sources used during the writing of the thesis.

Keywords: cybersecurity, Active Directory, SIEM, Graylog, Winlogbeat, event monitoring, log analysis, attack detection, Brute Force, automatic notification.

ЗМІСТ

ВСТУП..... 9

РОЗДІЛ 1. Аналіз системи реєстрації подій Graylog та її аналогів...... 10

1.1. Вступ до проблематики реєстрації подій та кібербезпеки Active Directory
..... 10

1.1.1. Визначення поняття системи реєстрації подій та її компонентів..... 10

1.1.2. Огляд систем збору та аналізу логів: Graylog, Splunk, ELK Stack... 12

1.1.3. Застосування систем логування для підвищення безпеки доменних контролерів...... 14

1.2. Аналіз основних серсісів реєстрації подій 17

1.2.1. Порівняння популярних платформ: Graylog, Splunk, та ELK Stack 17

1.2.2. Основні типи загроз які можуть виявити сервіси реєстрації подій. 22

1.3. Вимоги до систем реєстрації подій для захисту доменних контролерів Active Directory..... 23

1.3.1 Рекомендації щодо вибору та впровадження системи реєстрації подій для захисту доменних контролерів Active Directory...... 25

ВИСНОВКИ 27

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА РОЗГОРТАННЯ СИСТЕМИ МОНІТОРИНГУ БЕЗПЕКИ 28

2.1. Архітектура тестового стенду та обґрунтування вибору засобів..... 28

2.2. Інсталяція та конфігурація сервера збору логів (Graylog)..... 31

2.2.1. Налаштування базових компонентів (MongoDB, OpenSearch)...... 31

2.2.2. Розгортання Graylog Server. 37

2.2.3 Налаштування об'єкта захисту (Active Directory)..... 41

2.2.4 Встановлення та конфігурація агента транспортування подій Winlogbeat..... 45

ВИСНОВКИ 48

РОЗДІЛ 3. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ 49

3.1Методика проведення експерименту та сценарії загроз 49

3.2 Виявлення та аналіз інцидентів інформаційної безпеки 53

3.2.1. Аналіз спроб несанкціонованого доступу та реакції системи захисту 53

3.2.2. Контроль цілісності облікових записів та груп 55

3.2.3. Моніторинг змін у складі привілейованих груп та виявлення ескалації привілеїв 57

3.2.4. Виявлення шкідливого програмного забезпечення та інтеграція з антивірусним захистом 58

3.2.5. Реалізація системи автоматичного реагування та оповіщення (Alerting) 61

3.3 Візуалізація даних та побудова комплексної аналітичної панелі (Dashboard) 64

3.4 Оцінка ефективності впровадженої системи 67

ВИСНОВКИ 69

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 70

ДОДАТКИ 74

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Основні умовні позначення та їх розшифрування:

БД – база даних

ОС – операційна система

ПЗ – програмне забезпечення

СКБД – система керування базами даних

AD – Active Directory (служба каталогів)

AD DS – Active Directory Domain Services (доменні служби Active Directory)

API – Application Programming Interface (прикладний програмний інтерфейс)

CPU – Central Processing Unit (центральний процесор)

DC – Domain Controller (контролер домену)

DDoS – Distributed Denial of Service (розподілена атака на відмову в обслуговуванні)

DNS – Domain Name System (система доменних імен)

DoS – Denial of Service (атака на відмову в обслуговуванні)

GPO – Group Policy Object (об'єкт групової політики)

JSON – JavaScript Object Notation (текстовий формат обміну даними)

JVM – Java Virtual Machine (віртуальна машина Java)

MTTD – Mean Time to Detect (середній час виявлення інциденту)

NAT – Network Address Translation (трансляція мережевих адрес)

RAM – Random Access Memory (оперативна пам'ять)

SIEM – Security Information and Event Management (система управління інформацією та подіями безпеки)

SOC – Security Operations Center (операційний центр безпеки)

TTD – Time to Detect (час виявлення)

TTR – Time to Respond (час реагування)

ВСТУП

Сучасні інформаційні технології потребують високого рівня безпеки для захисту критичних систем, таких як доменні контролери Active Directory (AD). Одним із ключових методів забезпечення безпеки є централізоване логування подій, що дозволяє виявляти загрози та здійснювати аналіз інцидентів безпеки в режимі реального часу.

Доменні контролери Active Directory відіграють важливу роль в управлінні обліковими записами користувачів, ресурсами мережі та політиками доступу. Вразливості в AD можуть призвести до масштабних кібератак, включаючи несанкціонований доступ, крадіжку облікових даних та компрометацію інфраструктури підприємства. Тому впровадження систем збору та аналізу логів є необхідним для оперативного реагування на інциденти безпеки.[1]

Серед сучасних рішень для побудови систем моніторингу широко застосовуються Graylog, Splunk та ELK Stack. Ці платформи дозволяють ефективно обробляти великі обсяги логів та використовуються як інструменти оперативного реагування на інциденти. Застосування платформ централізованого логування дозволяє організаціям зменшити кількість інцидентів безпеки та підвищити контроль над подіями в мережі.

Метою даної роботи є аналіз системи реєстрації подій Graylog та її аналогів, а також їх застосування для захисту доменних контролерів Active Directory. Дослідження включає порівняльний аналіз функціональних можливостей популярних платформ для збору та обробки логів, оцінку їх ефективності в забезпеченні безпеки AD та визначення оптимальних методів їх впровадження

Об’єкт дослідження – процес реєстрації подій у доменних контролерах Active Directory.

Предмет дослідження – методи та засоби аналізу логів для забезпечення безпеки AD за допомогою централізованих систем реєстрації подій.[2]

РОЗДІЛ 1. Аналіз системи реєстрації подій Graylog та її аналогів.

1.1. Вступ до проблематики реєстрації подій та кібербезпеки Active Directory

1.1.1. Визначення поняття системи реєстрації подій та її компонентів

Контролери домену AD є фундаментальним елементом корпоративної інфраструктури. Будь-які зміни або атаки на них можуть вплинути на доступність сервісів та безпеку всієї мережі. Захист таких систем вимагає впровадження механізмів моніторингу, аналізу логів та своєчасного реагування на потенційні загрози.

Централізоване логування є одним із ключових механізмів підвищення безпеки доменних контролерів. Воно надає можливість агрегувати події з різних джерел, аналізувати їх та оперативно реагувати на підозрілу активність. Платформи на кшталт Graylog, Splunk чи ELK Stack реалізують повний цикл обробки логів, включаючи отримання, нормалізацію, зберігання та аналітику. [3]

Цей розділ присвячено аналізу основних рішень для централізованого збору логів, їх особливостей та методів застосування у контексті захисту доменних контролерів Active Directory.

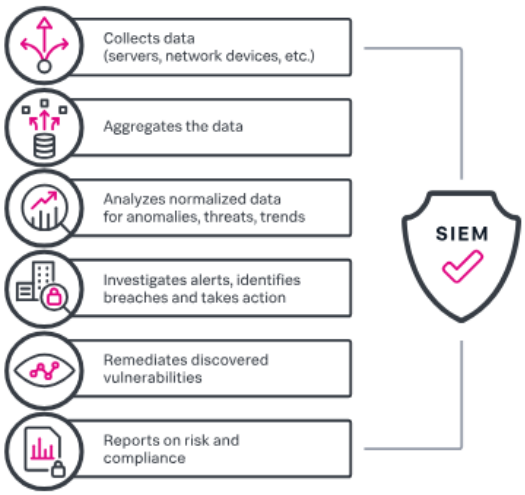


Рисунок 1.1 — Складові SIEM

Централізована система реєстрації подій становить собою комплекс взаємопов'язаних компонентів, що забезпечують повний цикл обробки даних. Першою ланкою є агент збору логів, який відповідає за отримання подій із різноманітних джерел, таких як сервери, мережеві пристрої, додатки та бази даних, і функціонує у вигляді встановленого програмного забезпечення або через протоколи Syslog, Winlogbeat чи Filebeat. Зібрана інформація передається до модуля прийому та нормалізації даних, який отримує логи у різних форматах та конвертує їх у стандартизований вигляд (наприклад, JSON, GELF, CSV), здійснюючи при цьому фільтрацію, структурування та доповнення логів метаданими.

Для збереження обробленої інформації використовується система зберігання логів, яка відповідає за довготривале утримання даних для подальшого аналізу, використовуючи реляційні або нереляційні бази даних (Elasticsearch, MongoDB, PostgreSQL) та забезпечуючи доступність і резервне копіювання. Обробка накопиченого масиву інформації покладається на аналітичний модуль, який аналізує дані за заданими критеріями за допомогою пошукових запитів, машинного навчання та кореляції подій для виявлення загроз (на прикладі Splunk, Graylog або ELK Stack).[4]

Візуалізація зібраних даних здійснюється через інтерактивні панелі моніторингу, де оператор може спостерігати за подіями в режимі реального часу. За допомогою Kibana або Grafana дані подаються у зручному графічному форматі, що значно полегшує аналіз та контроль стану системи. У разі виявлення аномалій або загроз спрацьовує система оповіщення та реагування, яка автоматично надсилає повідомлення адміністраторам через E-mail, Telegram, Slack або інші канали. Завершальним елементом є інтеграція з SIEM-системами (IBM QRadar, Microsoft Sentinel), що дозволяє виконувати глибоку кореляцію логів із різних джерел для виявлення складних атак.[5][6]

1.1.2. Огляд систем збору та аналізу логів: Graylog, Splunk, ELK Stack.

Системи збору та аналізу логів, такі як Graylog, Splunk та ELK Stack, є потужними інструментами для централізованого моніторингу, аналізу та візуалізації подій, що відбуваються в IT-системах. Вони дозволяють ефективно обробляти великі обсяги даних, отриманих із різноманітних джерел, таких як сервери, мережеві пристрої, додатки та бази даних, допомагаючи адміністраторам і аналітикам безпеки виявляти аномалії, усувати несправності та реагувати на потенційні загрози.

- Graylog [7]

Graylog – це потужна система для збору, індексації та аналізу логів, яка дозволяє організаціям моніторити, шукати та візуалізувати дані про події з різних джерел у реальному часі. Основною перевагою Graylog є його простота в налаштуванні та гнучкість у інтеграціях з різними джерелами логів. Він використовує ElasticSearch для зберігання даних і MongoDB для метаданих, що забезпечує високу швидкість пошуку та ефективне зберігання. Graylog підтримує збір даних через різні протоколи, такі як Syslog, GELF (Graylog Extended Log Format), а також інші стандарти, що дозволяє інтегрувати систему з різноманітними інфраструктурами. Зібрані логи можна аналізувати за допомогою потужних запитів, створювати оповіщення про аномальні події та отримувати детальні звіти для подальшого розслідування. Інтерфейс користувача Graylog дозволяє створювати візуалізації та дашборди, що полегшують моніторинг і дають змогу оперативно реагувати на інциденти безпеки. Однією з важливих особливостей є можливість налаштування політик ретенції даних, що дозволяє оптимізувати зберігання великих обсягів логів та знижує навантаження на систему.[8]

- Splunk [9]

Splunk є однією з найбільш відомих і широко використовуваних платформ для збору, аналізу та візуалізації машинних даних, включаючи логи, метрики, конфігураційні дані та інші системні події. Він забезпечує гнучкість при роботі з великими обсягами даних, завдяки своїй здатності обробляти та індексувати величезну

кількість записів за короткий проміжок часу. Splunk може працювати з даними в реальному часі та з історичними даними, що дозволяє організаціям здійснювати глибокий аналіз логів і реагувати на події в реальному часі. Особливість Splunk полягає в його потужному механізмі пошуку, який дає змогу оперативно виявляти аномалії, проводити кореляцію подій і отримувати корисні інсайти. Крім того, Splunk має дуже розвинуту екосистему додатків, які можуть бути використані для інтеграції з різними сервісами та пристроями, а також для додаткових функцій, таких як моніторинг продуктивності, аудиту безпеки та розслідування інцидентів. Платформа підтримує створення кастомізованих дашбордів і звітів, що допомагає представити дані в доступному та зрозумілому вигляді для користувачів різного рівня. Водночас варто зазначити, що Splunk може бути досить дорогим рішенням для малих і середніх підприємств через модель ліцензування, яка залежить від обсягу зібраних даних.

- ELK Stack [10]

ELK Stack (ElasticSearch, Logstash, Kibana) – це популярне рішення для збору, зберігання та аналізу логів, яке складається [11] з трьох основних компонентів:

- ElasticSearch [12]

ElasticSearch – потужний пошуковий движок, який забезпечує швидке індексування та пошук по великих обсягах даних.

- Logstash

Logstash – інструмент для збору, обробки та транспортування логів з різних джерел. Logstash дозволяє обробляти дані, фільтрувати їх, трансформувати в потрібний формат та надсилати до ElasticSearch.

- Kibana

Kibana – інтерфейс для візуалізації та аналізу даних, що зберігаються в ElasticSearch. Kibana дозволяє створювати графіки, діаграми, дашборди та візуалізувати дані логів у зрозумілій формі, що полегшує моніторинг і прийняття рішень.

ELK Stack є відкритим рішенням, що робить його дуже привабливим для організацій, які шукають безкоштовні або недорогі інструменти для збору та аналізу логів. Однак, незважаючи на його відкритість, для великих підприємств може знадобитися додаткове налаштування та оптимізація продуктивності, щоб впоратися з великими обсягами даних. Завдяки своїй гнучкості та розширюваності, ELK Stack часто використовується для побудови складних систем моніторингу та аналізу даних у реальному часі. У Kibana користувачі можуть створювати інтуїтивно зрозумілі візуалізації і дашборди, що дозволяють відстежувати важливі метрики та події, наприклад, статус серверів, активність користувачів і багато іншого.[13]

1.1.3. Застосування систем логування для підвищення безпеки доменних контролерів.

Системи логування відіграють важливу роль у підвищенні безпеки доменних контролерів (DC) в середовищі Active Directory. Правильна конфігурація та використання інструментів для збору та аналізу логів допомагають виявляти аномальну активність, запобігати несанкціонованому доступу та знижувати ймовірність успішних кібератак. Оскільки доменні контролери є критичними елементами в інфраструктурі Active Directory, їх безпека повинна бути пріоритетом для адміністратора. Системи логування можуть використовуватися для моніторингу дій користувачів і адміністраторів, аналізу змін у конфігураціях і доступах, а також для реагування на підозрілі події в реальному часі.

Журнал подій безпеки (Security Log) є важливим джерелом для відстеження активності в доменних контролерах. Завдяки цьому журналу адміністратори можуть отримати детальну інформацію про спроби входу в систему, включаючи успішні та невдалі спроби аутентифікації користувачів. Події, такі як неуспішні спроби входу (наприклад, ID події 529 для неправильних паролів), спроби ескалації привілеїв або зміни в політиках безпеки, можуть сигналізувати про підготовку до

атаки. Своєчасне виявлення таких спроб дозволяє вжити відповідних заходів, наприклад, тимчасово заблокувати підозрілі облікові записи або змінити налаштування доступу.

Журнал подій безпеки також містить записи про критичні дії адміністраторів системи, наприклад, створення нових облікових записів, зміна прав доступу та делегування прав, що є важливим для моніторингу можливих зловживань. Для підвищення безпеки доменних контролерів необхідно налаштувати аудиторські політики, які б записували всі зміни прав доступу та додавання нових облікових записів, оскільки ці дії можуть вказувати на потенційне порушення політики безпеки.

Збір і централізований аналіз логів з усіх доменних контролерів забезпечує більш ефективний моніторинг. За допомогою таких інструментів, як Graylog, Splunk чи ELK Stack, адміністратори можуть отримати єдиний погляд на всю інфраструктуру і виявляти аномалії або інциденти, що можуть бути не помічені при локальному перегляді логів. Ці інструменти дозволяють налаштовувати алерти на основі певних подій, наприклад, на підозрілі спроби доступу або зміни в критичних налаштуваннях контролера домену. Для забезпечення високого рівня безпеки в доменних контролерах важливо налаштувати інтеграцію з системами збору логів таким чином, щоб дані з усіх серверів передавалися в реальному часі і були доступні для аналізу, що дає можливість оперативно реагувати на інциденти.

Моніторинг доступу до Active Directory і змін об'єктів AD є ще одним важливим аспектом безпеки доменних контролерів. Для цього потрібно налаштувати аудит доступу до об'єктів каталогу через політику Group Policy. Журнал подій Active Directory фіксує всі важливі події, такі як додавання або видалення користувачів, зміну прав доступу, делегування прав на певні об'єкти в AD. Це дозволяє виявляти несанкціоновані зміни, наприклад, коли зловмисник намагається додати користувача до адміністративної групи або змінити пароль адміністратора. Звітність і аналіз таких подій допомагають вчасно виявити потенційні загрози та відновити без-

пеку домену. Крім того, регулярний перегляд таких подій допомагає адміністраторам бути в курсі змін, що відбуваються в середовищі, та вчасно коригувати політики безпеки, щоб запобігти можливим атакам.

Однією з основних технологій аутентифікації в Windows Server є Kerberos, який широко використовується в середовищі Active Directory. Керівники доменних контролерів повинні уважно слідкувати за подіями, пов'язаними з аутентифікацією Kerberos, що можна зробити через журнал подій Security. Системи збору логів можуть відслідковувати такі важливі події, як успішні та невдалі спроби аутентифікації, видання квитків Kerberos (події з ID 4768), а також події, пов'язані з пошкодженими або простроченими квитками. Це дозволяє оперативно реагувати на підозрілі спроби несанкціонованого доступу або зловживання обліковими записами.

Для підвищення безпеки доменних контролерів важливо здійснювати моніторинг адміністративних дій, таких як зміна політик безпеки, додавання нових адміністраторів або зміна конфігурацій. Це можна досягти за допомогою налаштування політики Audit Directory Service Access в Active Directory, яка дозволяє записувати всі дії адміністратора, пов'язані з управлінням об'єктами AD. Оскільки зміни, здійснені адміністраторами, можуть мати серйозні наслідки для безпеки, важливо мати механізми моніторингу цих дій і бути готовим до оперативної реакції.[14]

Для забезпечення безпеки та відповідності стандартам, зокрема в умовах комплаєнсу та аудиту, важливо впровадити систему централізованого зберігання та архівації логів. Це дозволить забезпечити цілісність даних, полегшити процеси розслідування інцидентів та аудитів, а також зберігати записи подій на випадок перевірок або юридичних запитів. Архівація логів з доменних контролерів також допомагає зберігати історичну інформацію для подальшого аналізу і надання звітів. Системи логування є важливим елементом безпеки доменних контролерів, оскільки дозволяють організувати ефективний моніторинг, аудит і реагування на події в середовищі Active Directory.[15] Використання централізованих систем збору та аналізу

логів, таких як Graylog, Splunk або ELK Stack, дозволяє забезпечити високий рівень безпеки шляхом своєчасного виявлення аномальних або підозрілих дій.

Забезпечення належного моніторингу адміністраторів, контролю доступу, а також правильна архівація та збереження логів є запорукою надійної роботи та безпеки доменних контролерів в корпоративних мережах.[16]

1.2. Аналіз основних серсісів реєстрації подій

1.2.1. Порівняння популярних платформ: Graylog, Splunk, та ELK Stack

Основні сервіси реєстрації подій, такі як Graylog, Splunk, та ELK Stack, є популярними платформами для збору, аналізу та зберігання логів, кожна з яких має свої унікальні переваги, можливості та використання в різних сценаріях. Оскільки для вас основним інструментом буде Graylog, порівняємо його з іншими двома платформами для кращого розуміння їх сильних сторін та обмежень.

1. Graylog

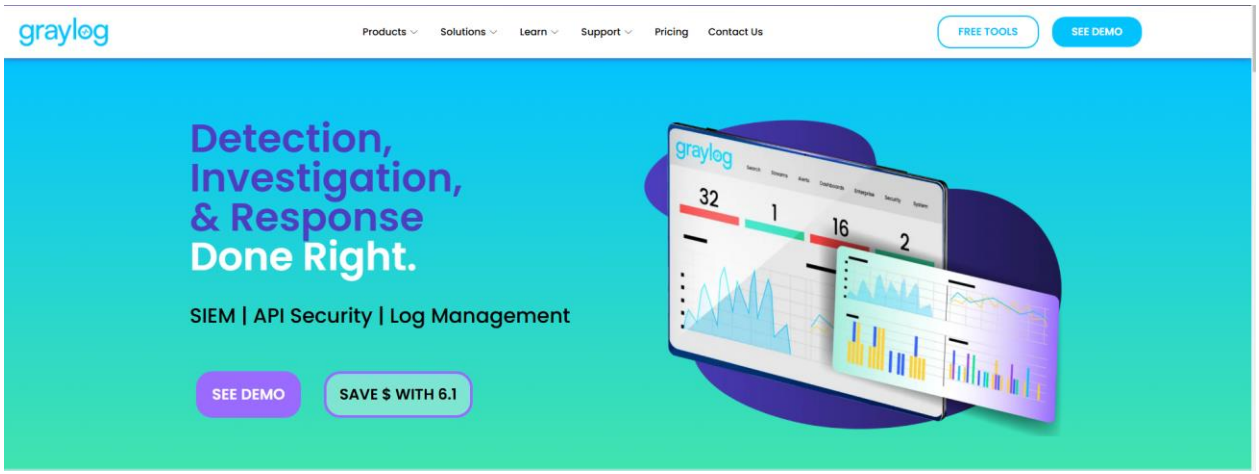


Рисунок 1.2 — Сервіс реєстрації подій Graylog

Graylog — це відкритий сервіс для централізованого збору та аналізу логів, який спеціалізується на обробці значних масивів даних і оснащений зручним інтерфейсом для моніторингу та візуалізації подій. Однією з ключових характеристик системи є висока гнучкість та масштабованість, що дозволяє налаштовувати збір та обробку інформації з різнорідних джерел, забезпечуючи можливість адаптації під

зростаючі обсяги даних в організації. Взаємодія з платформою здійснюється через інтуїтивно зрозумілий веб-інтерфейс, який надає інструменти для створення функціональних панелей моніторингу, а також фільтрації та глибокого аналізу даних.

Архітектура Graylog відзначається модульністю, підтримуючи різноманітні плагіни та інтеграції зі сторонніми інструментами, при цьому для ефективної обробки та надійного зберігання даних використовується пошуковий рушій Elasticsearch. Як Open Source рішення, продукт пропонує безкоштовну версію з базовим функціоналом, а також комерційні варіанти з розширеними можливостями масштабування та технічної підтримки. Важливою перевагою платформи є гнучкий механізм пошуку та аналітики, який дозволяє оперативно виявляти критичні події, генерувати детальні звіти та ефективно діагностувати інциденти інформаційної безпеки.

2. Splunk

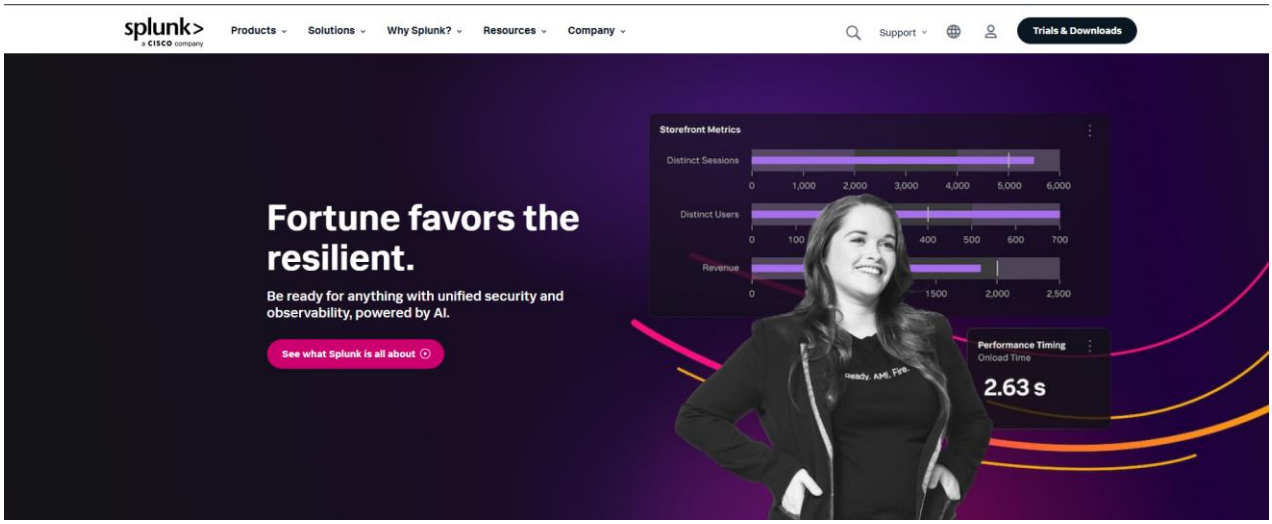


Рисунок 1.3 — Сервіс реєстрації подій Splunk

Splunk позиціонується як провідне комерційне рішення для моніторингу та аналізу логів, здатне здійснювати високошвидкісну обробку значних масивів даних у режимі реального часу. Однією з ключових переваг платформи є надзвичайно потужний механізм пошуку та аналітики, який дозволяє проводити детальний розбір подій безпосередньо під час їх надходження. Архітектура системи розроблена з

урахуванням вимог до масштабованості, що дозволяє ефективно опрацьовувати мільйони подій на секунду, а взаємодія з користувачем забезпечується через інтуїтивно зрозумілий інтерфейс, призначений для створення інформативних панелей моніторингу та швидкої оцінки стану інфраструктури.

Система підтримує широкі можливості інтеграції з різноманітними інструментами, включаючи мережеві пристрої, сервіси безпеки та зовнішні бази даних. Окремої уваги заслуговує відповідність вимогам безпеки та комплаєнсу: Splunk оснащений інструментарієм для підтримки таких стандартів, як PCI DSS та GDPR. Варто зазначити, що як комерційний продукт, платформа передбачає платну модель використання, що може бути фінансово обтяжливим для малих організацій, проте вартість ліцензії компенсується потужним функціоналом та можливостями рівня корпоративних систем.

3. ELK Stack (Elasticsearch, Logstash, Kibana)

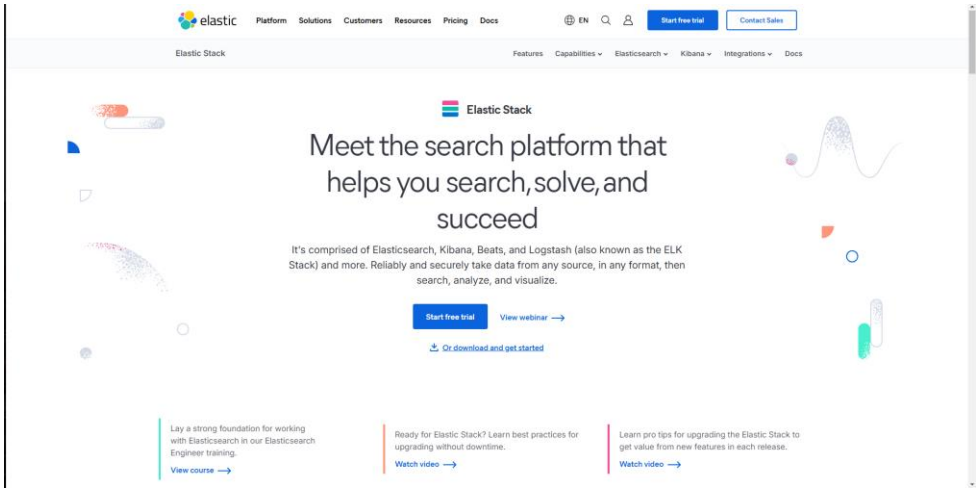


Рисунок 1.4 — Сервіс реєстрації подій ELK Stack

ELK Stack визначається як інтегрований набір інструментів, що включає Elasticsearch, Logstash та Kibana, і забезпечує наскрізний процес збору, зберігання та аналізу лог-файлів. Зберігання та пошук логів реалізовані за допомогою Elasticsearch, який входить до складу стандартних компонентів системи. За попере-

дню обробку та нормалізацію відповідає компонент Logstash, який підтримує розширені механізми трансформації даних з різнорідних джерел перед їх збереженням.

Візуалізація результатів аналізу реалізується через інтерфейс Kibana, що надає широкі можливості для створення динамічних панелей моніторингу та графічного представлення метрик. Важливою перевагою стеку є його відкрита архітектура (Open Source), що забезпечує гнучкість розгортання та можливість адаптації під специфічні потреби інфраструктури без ліцензійних витрат. Попри високу ефективність у роботі з Big Data, варто враховувати, що архітектура ELK може вимагати значних апаратних ресурсів для забезпечення стабільної продуктивності на великих масштабах.

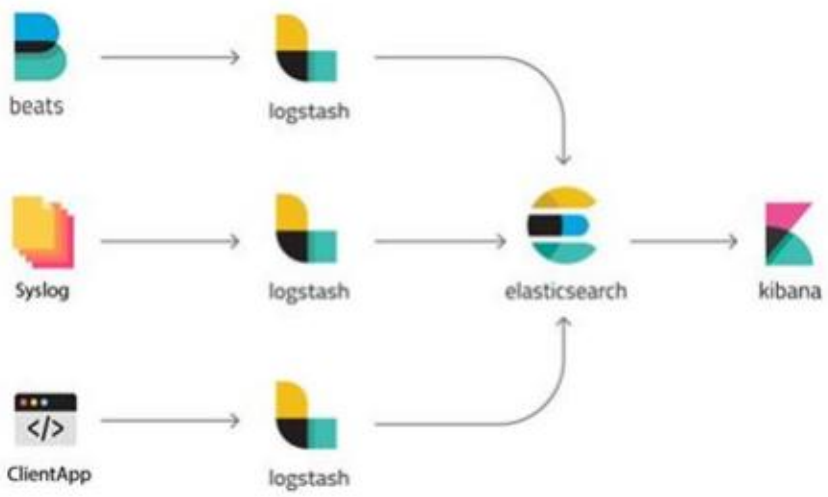


Рисунок 1.5 — Схема взаємодії компонентів Elastic Stack

Порівняння:

- **Ціна**: Graylog і ELK Stack мають відкриті версії з безкоштовним доступом, тоді як Splunk є платним рішенням, яке може бути дорогим, але пропонує велику кількість функцій за ці гроші.

- **Масштабованість**: Splunk і ELK Stack забезпечують велику масштабованість для обробки великих обсягів даних, але ELK Stack потребує більше налаштувань і ресурсів. Graylog також є масштабованим, але в порівнянні з Splunk менш ресурсозатратний.
- **Інтерфейс користувача**: Splunk має найрозвиненіший інтерфейс серед трьох платформ, з більш розвинутими можливостями для створення панелей моніторингу і звітів. Graylog і ELK Stack теж мають потужні інтерфейси, але вони можуть бути менш інтуїтивно зрозумілими для новачків.
- **Інтеграції та підтримка**: Splunk має найкращу інтеграцію з іншими корпоративними системами та сервісами. ELK Stack і Graylog також підтримують інтеграцію з іншими інструментами, але можуть вимагати більше налаштувань.
- **Використання в реальному часі**: Всі три системи підтримують моніторинг в реальному часі, однак Splunk має найкращу продуктивність для аналізу в реальному часі завдяки своїй архітектурі.

Табл. 1. Порівняльна таблиця популярних платформ

Характеристика	**Graylog**	**Splunk**	**ELK Stack**
Ліцензія	Відкритий код	Комерційний	Відкритий код
Масштабованість	Висока	Дуже висока	Висока
Підтримка форматів логів	Syslog, GELF, JSON	Syslog, JSON	JSON, Syslog
Інструменти візуалізації	Вбудовані	Вбудовані	Kibana
Вартість	Безкоштовно	Висока	Безкоштовно

Оскільки для вас основним буде Graylog, це рішення має гарний баланс між відкритістю, гнучкістю та функціональністю для збору і аналізу логів, що робить його відмінним вибором для середніх і великих організацій.

1.2.2. Основні типи загроз які можуть виявити сервіси реєстрації подій.

Системи реєстрації подій, зокрема журнали безпеки, виступають ключовим інструментом для виявлення спроб несанкціонованого доступу, фіксуючи всі процедури автентифікації незалежно від їх успішності. Аналіз цих даних дозволяє ідентифікувати атаки типу Brute Force, спроби входу з підозрілих IP-адрес, а також нелегітимні зміни в облікових записах, такі як ескалація прав доступу або несанкціонована зміна паролів. Паралельно здійснюється моніторинг мережевої активності для виявлення DoS та DDoS-атак, індикаторами яких виступають аномальні обсяги трафіку, підключення до неавторизованих портів та збої в роботі мережевих пристроїв або сертифікатів.[17]

Окрім мережевих загроз, аналіз подій дозволяє діагностувати спроби виведення системи з ладу через експлуатацію вразливостей програмного забезпечення або перевантаження апаратних ресурсів, таких як центральний процесор та оперативна пам'ять. Системи логування також ефективні у виявленні шкідливого програмного забезпечення шляхом відстеження неавторизованих змін у системних файлах, появи невідомих процесів або спроб втручання в роботу самих журналів подій.

Важливим аспектом є захист від витоків інформації та внутрішніх загроз. Централізований моніторинг дозволяє фіксувати підозрілі зміни в налаштуваннях доступу до баз даних, несанкціоноване копіювання великих масивів інформації, а також активність користувачів у неробочий час. Це допомагає ідентифікувати зловживання повноваженнями з боку співробітників та аномальну поведінку персоналу. Крім того, аналіз журналів дозволяє виявляти спроби експлуатації вразливостей програмного забезпечення та контролювати процес встановлення критичних оновлень. Нарешті, системи реєстрації подій здатні детестувати спроби маніпуляції самими логами, такі як їх видалення, модифікація або генерація фальшивих повідомлень, що використовується зловмисниками для приховування слідів атаки.[18]

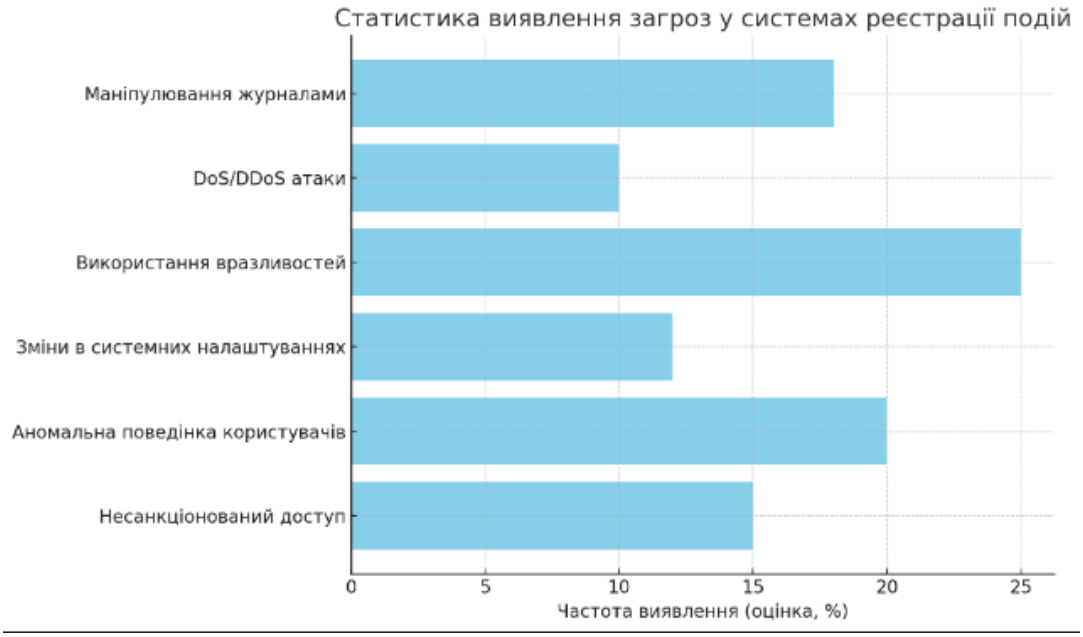


Рис 1.6 — Графік найпопулярніших загроз виявлених сервісами реєстрації подій.

1.3. Вимоги до систем реєстрації подій для захисту доменних контролерів Active Directory

Функціональні вимоги

- Збір та централізація логів: Система повинна забезпечувати збір логів безпеки з усіх доменних контролерів Active Directory в єдиному централізованому сховищі для спрощення аналізу та моніторингу.
- Фільтрація та нормалізація: Система повинна мати можливість фільтрувати та нормалізувати логи для спрощення їх аналізу та ідентифікації важливих подій.
- Аналіз в реальному часі: Система повинна забезпечувати можливість аналізу логів в реальному часі для своєчасного виявлення загроз та інцидентів безпеки.
- Візуалізація та звітування: Система повинна надавати інструменти для візуалізації даних та створення звітів для спрощення аналізу та моніторингу.

- Сигналізація та оповіщення: Система повинна мати можливість налаштування сигналізації та оповіщення про виявлені загрози або аномалії.
- Інтеграція з іншими системами безпеки: Система повинна інтегруватися з іншими системами безпеки, такими як SIEM, для комплексної обробки та аналізу даних.
- Масштабованість та продуктивність: Система повинна бути масштабованою для обробки великих обсягів даних та забезпечувати високу продуктивність.
- Безпека та захист даних: Система повинна забезпечувати безпеку та захист даних, включаючи захист від несанкціонованого доступу та змін.

Вимоги до безпеки

- Захист від несанкціонованого доступу: Доступ до системи реєстрації подій повинен бути обмежений та захищений.
- Захист від змін та видалення логів: Логи повинні бути захищені від несанкціонованих змін та видалення.
- Шифрування даних: Дані, що зберігаються в системі, повинні бути зашифровані для забезпечення конфіденційності.
- Аудит та контроль: Система повинна забезпечувати аудит та контроль дій користувачів для виявлення зловживань.

Вимоги до інфраструктури

- Відмовостійкість: Система повинна бути відмовостійкою та забезпечувати безперервну роботу.
- Резервне копіювання та відновлення: Система повинна забезпечувати резервне копіювання та відновлення даних.

- Моніторинг та обслуговування: Система повинна забезпечувати моніторинг та обслуговування для забезпечення її ефективної роботи.

1.3.1 Рекомендації щодо вибору та впровадження системи реєстрації подій для захисту доменних контролерів Active Directory.

Перш за все, перед вибором системи реєстрації подій необхідно чітко визначити потреби вашої організації та конкретні вимоги до такої системи. Важливо врахувати обсяг даних, який потрібно обробляти, кількість доменних контролерів, рівень безпеки, який необхідно забезпечити, а також бюджет, який ви готові виділити на впровадження та підтримку системи.

Після визначення потреб необхідно провести ретельний аналіз функціональності різних систем та порівняти їх з вимогами вашої організації. Зверніть увагу на такі параметри, як можливість збору та централізації логів з усіх доменних контролерів, наявність інструментів для фільтрації та нормалізації даних, можливість аналізу в реальному часі, візуалізація та звітування, сигналізація та оповіщення про інциденти безпеки, інтеграція з іншими системами безпеки, масштабованість та продуктивність, а також безпека та захист даних.

Важливим кроком є оцінка вартості впровадження та підтримки системи. Потрібно врахувати не тільки вартість ліцензій на програмне забезпечення, але й витрати на обладнання, навчання персоналу, а також подальшу підтримку та оновлення системи.

Перед прийняттям остаточного рішення рекомендується провести тестування та пілотування обраної системи. Це дозволить вам переконатися в тому, що система відповідає вашим вимогам та ефективно працює у вашій інфраструктурі.

Після вибору системи необхідно розробити детальний план її впровадження. План повинен включати етапи впровадження, терміни виконання, відповідальних осіб, а також ресурси, необхідні для успішного завершення проекту.

Важливим етапом є правильне налаштування системи для забезпечення збору та аналізу необхідних даних. Зверніть увагу на налаштування параметрів безпеки, фільтрів, правил обробки даних, а також інтеграцію з іншими системами безпеки.

Після впровадження системи необхідно провести навчання персоналу для її ефективного використання. Персонал повинен бути ознайомлений з функціональністю системи, правилами роботи з нею, а також процедурами реагування на інциденти безпеки.

Після успішного впровадження системи необхідно здійснювати постійний моніторинг та обслуговування для забезпечення її ефективної роботи. Потрібно регулярно аналізувати логи, налаштовати сигналізацію для отримання своєчасних повідомлень про важливі події, а також регулярно оновлювати систему для забезпечення її безпеки та ефективності.

ВИСНОВКИ

У першому розділі магістерської роботи проведено комплексне теоретичне дослідження проблематики захисту контролерів домену Active Directory засобами централізованого логування подій. Встановлено, що Active Directory є критичним компонентом IT-інфраструктури, компрометація якого несе значні ризики для організації, що зумовлює необхідність переходу від локального аудиту до використання спеціалізованих систем моніторингу. Детальний аналіз архітектури сучасних систем реєстрації подій дозволив виділити їх ключові модулі, такі як агенти збору, механізми нормалізації, сховища даних та аналітичні інструменти, які у сукупності забезпечують повний цикл обробки інцидентів безпеки від моменту їх виникнення до реагування .

В ході порівняльного аналізу провідних платформ ринку — Graylog, Splunk та ELK Stack — було визначено їхні переваги та недоліки в контексті використання на підприємствах різного масштабу. На основі критеріїв вартості, функціональності та складності впровадження було обґрунтовано вибір системи Graylog як основного інструменту для подальшої практичної реалізації, оскільки вона забезпечує оптимальний баланс між гнучкістю налаштувань, масштабованістю та доступністю у форматі Open Source. Також було систематизовано основні вектори кіберзагроз, включаючи несанкціонований доступ, мережеві атаки типу DoS/DDoS, внутрішні загрози та діяльність шкідливого програмного забезпечення, які можуть бути ефективно виявлені шляхом глибокого аналізу журналів подій .

Завершальним етапом розділу стало формування чітких функціональних вимог та вимог до безпеки проектованої системи моніторингу, а також розробка методичних рекомендацій щодо її впровадження, які включають етапи пілотування, налаштування фільтрації даних та навчання персоналу. Отримані результати теоретичного аналізу створюють необхідне науково-технічне підґрунтя для переходу до практичної частини роботи, присвяченої проектуванню та розгортанню лабораторного стенду захисту Active Directory на базі Graylog .

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА РОЗГОРТАННЯ СИСТЕМИ МОНІТОРИНГУ БЕЗПЕКИ

2.1. Архітектура тестового стенду та обґрунтування вибору засобів

Для реалізації практичної частини магістерської роботи було розгорнуто віртуальний лабораторний стенд на базі гіпервізора VMware Workstation. Вибір віртуалізації дозволив змоделювати мережеву взаємодію між сервером безпеки та корпоративною інфраструктурою в межах одного фізичного хоста.

Склад стенду:

1. Сервер моніторингу (SIEM):
    - ОС: Ubuntu 22.04 LTS.
    - Ресурси: 4 ГБ RAM, 2 vCPU.
    - ПЗ: Graylog 6.0, OpenSearch 2.12, MongoDB 6.0.
    - IP-адреса: 192.168.52.129.
2. Об’єкт захисту (Domain Controller):
    - ОС: Windows Server 2022 Standard.
    - Ресурси: 2 ГБ RAM, 2 vCPU.
    - Роль: Active Directory Domain Services (AD DS).
    - IP-адреса: 192.168.52.128.

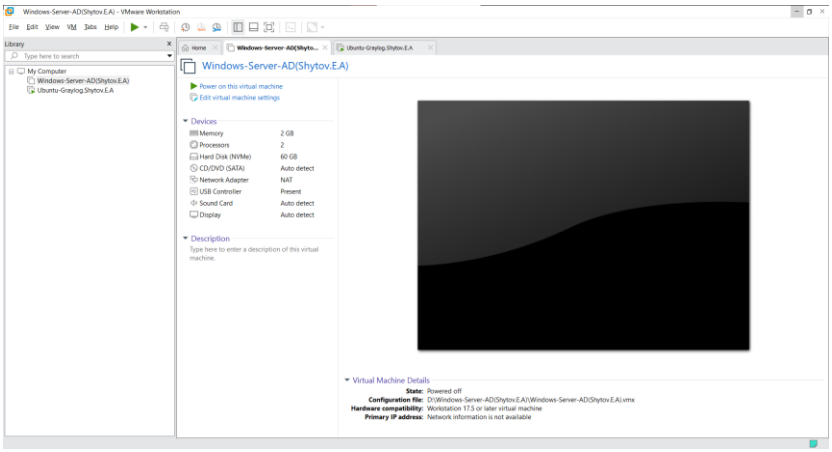


Рисунок 2.1 — Тестовий стенд

Мережева взаємодія налаштована в режимі NAT, що дозволило віртуальним машинам мати доступ до Інтернету для завантаження пакетів та одночасно перебувати в одній підмережі для обміну логами.

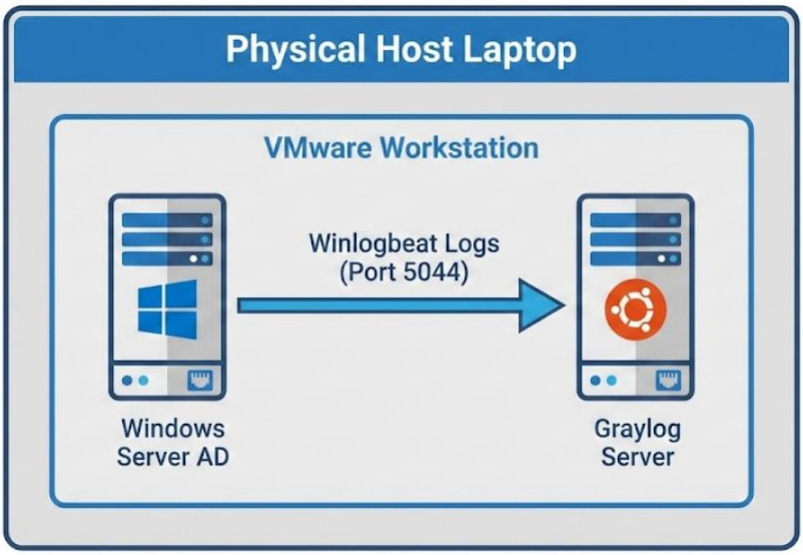


Рисунок 2.2 — Схема тестового стенду

Під час проектування архітектури тестового стенду було враховано апаратні обмеження фізичного хоста (ноутбука), який має загальний обсяг оперативної пам'яті 16 ГБ. Для одночасної роботи хостової операційної системи, віртуальної машини з Windows Server (Active Directory) та віртуальної машини з сервером моніторингу (Ubuntu), для останньої було виділено ліміт у 4 ГБ RAM.[19]

Програмні компоненти системи моніторингу — Graylog Server та пошуковий рушій OpenSearch — працюють на базі віртуальної машини Java (JVM). Стандартна конфігурація цих сервісів передбачає резервування 1 ГБ оперативної пам'яті під Heap (динамічну пам'ять) для кожного процесу. Сумарно це складає 2 ГБ, що разом із потребами операційної системи Ubuntu та СУБД MongoDB створювало критичне навантаження на віртуальну машину та призводило до збоїв типу Out of Memory (OOM).

Для забезпечення стабільності роботи системи було проведено оптимізацію параметрів JVM. У конфігураційних файлах opensearch та graylog-server параметри розподілу пам'яті було змінено наступним чином:

- Початковий розмір кучі (-Xms) зменшено з 1g до 512m.
- Максимальний розмір кучі (-Xmx) зменшено з 1g до 512m.

Дане налаштування дозволило вивільнити 1 ГБ оперативної пам'яті для потреб операційної системи, що забезпечило безперебійну роботу всіх компонентів SIEM-системи в умовах обмежених ресурсів.

Вибір операційної системи для сервера моніторингу (Ubuntu 22.04 LTS) У якості базової платформи для розгортання компонентів SIEM-системи (Graylog, OpenSearch, MongoDB) було обрано дистрибутив Ubuntu 22.04 LTS (Jammy Jellyfish). Цей вибір зумовлений наступними факторами:

Стабільність та підтримка (LTS): Версії Long Term Support гарантують отримання оновлень безпеки та виправлень помилок протягом 5 років, що є критично важливим для серверів безпеки.

Сумісність: Ubuntu 22.04 має офіційну підтримку з боку розробників Graylog та OpenSearch, що забезпечує коректну роботу всіх залежностей (зокрема, бібліотек OpenJDK та системних служб systemd).[20]

Ефективність використання ресурсів: У порівнянні з Windows-аналогами або графічними дистрибутивами, серверна версія Linux дозволяє гнучко керувати системними ресурсами (RAM, CPU), що є вирішальним фактором при розгортанні складного стеку ПЗ на обмежених апаратних потужностях.

Для розгортання служби каталогів Active Directory було обрано Windows Server 2022 Standard. Вибір цієї версії зумовлений тим, що вона є актуальною серверною платформою Microsoft з покращеними механізмами безпеки (Secured-core server), підтримкою TLS 1.3 за замовчуванням та оптимізованою продуктивністю, що є критично важливим для побудови сучасної захищеної інфраструктури. Вибір цієї версії ґрунтується на наступному:

Репрезентативність: Windows Server 2022 наразі є однією з найбільш поширених серверних ОС у корпоративному секторі, що робить результати дослідження актуальними для реальних умов експлуатації.

Функціональність аудиту: Дана версія ОС підтримує розширені політики аудиту (Advanced Audit Policy Configuration), які дозволяють детально налаштовувати генерацію подій безпеки, необхідних для детектування складних атак.

Повна підтримка Active Directory: ОС забезпечує функціонування контролера домену на функціональному рівні лісу, який підтримує всі сучасні механізми аутентифікації (Kerberos, NTLM) та управління груповими політиками (GPO), що є об’єктом захисту в даній роботі.

2.2. Інсталяція та конфігурація сервера збору логів (Graylog)

2.2.1. Налаштування базових компонентів (MongoDB, OpenSearch).

Сімейство програмних продуктів Graylog використовує документо-орієнтовану систему керування базами даних MongoDB для зберігання критично важливої інформації, зокрема конфігураційних даних, метаданих, профілів користувачів, налаштувань потоків та правил оповіщення. Для забезпечення повної сумісності з обраною версією Graylog 6.0 у рамках дослідження було використано стабільну версію MongoDB 6.0.

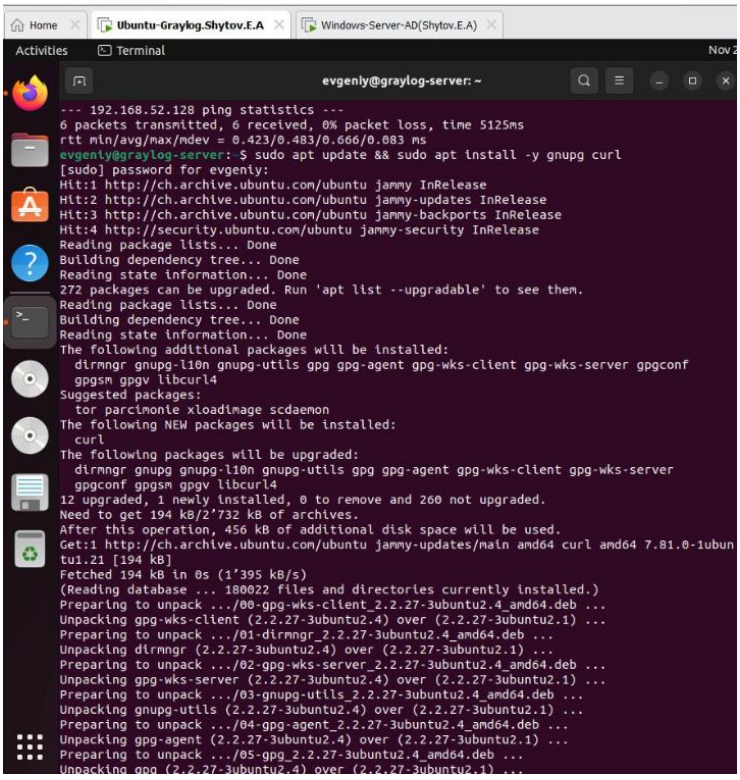


Рисунок 2.3 — Встановлення допоміжних програм

Процес розгортання СКБД на сервері під управлінням ОС Ubuntu 22.04 LTS розпочався з попередньої підготовки операційної системи, що включала оновлення локального індексу пакетів та інсталяцію необхідних утиліт gnupg і curl для роботи із захищеними з'єднаннями. З метою забезпечення цілісності та автентичності завантажуваних компонентів було імпортовано офіційний GPG-ключ MongoDB, що дозволяє менеджеру пакетів верифікувати цифрові підписи файлів та запобігає встановленню скомпрометованого програмного забезпечення.

```
evgeniy@graylog-server:~$ curl -fsSL https://pgp.mongodb.com/server-6.0.asc
 | sudo gpg -o /usr/share/keyrings/mongodb-server-6.0.gpg --dearmor
```

Рисунок 2.4 — Додавання ключа безпеки MongoDB

Оскільки стандартні репозиторії операційної системи часто містять застарілі версії програмного забезпечення, до списку джерел пакетів було додано офіційний репозиторій MongoDB 6.0.

```
evgeniy@graylog-server:~$ echo "deb [ arch=amd64,arm64 signed-by=/usr/share
/keyrings/mongodb-server-6.0.gpg ] https://repo.mongodb.org/apt/ubuntu jamm
y/mongodb-org/6.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-or
g-6.0.list
deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-server-6.0.gpg
 ] https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/6.0 multiverse
evgeniy@graylog-server:~$
```

Рисунок 2.5 — Додавання джерела завантаження (Репозиторію)

Безпосередня інсталяція виконувалася шляхом розгортання мета-пакету mongodb-org, який включає всі необхідні компоненти: демон бази даних, демон маршрутизації та інструменти адміністрування.

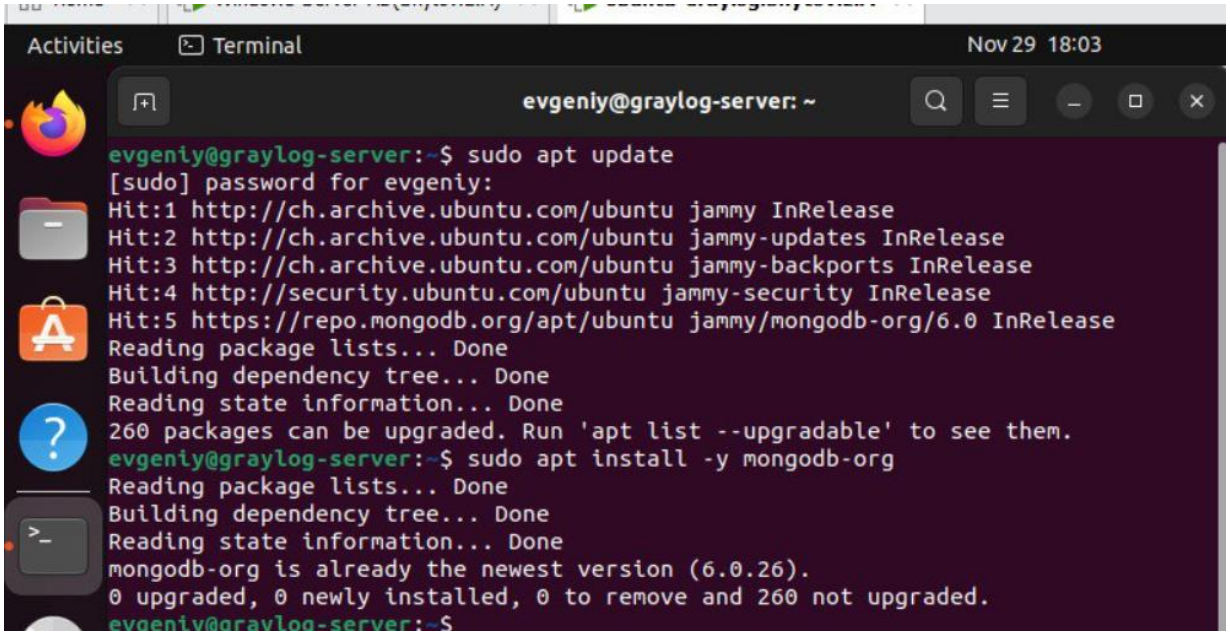


Рисунок 2.6 — Встановлення MongoDB

Для забезпечення безперервної роботи системи моніторингу службу MongoDB було додано до автозавантаження засобами systemd, що гарантує її автоматичний старт після перезавантаження сервера.[21]

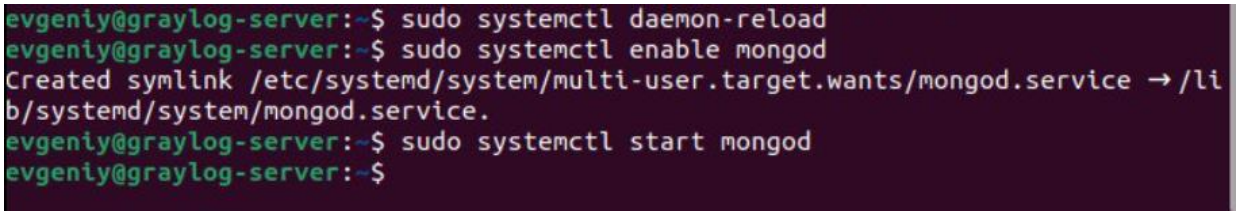


Рисунок 2.7 — Забезпечення безперервної роботи системи моніторингу

Фінальним етапом налаштування стала верифікація працездатності служби, яка підтвердила статус active (running), що свідчить про успішне розгортання бази даних та її готовність до взаємодії з іншими компонентами SIEM-системи.



Рисунок 2.8 — Перевірка успішного встановлення та запуску MongoDB

Наступним критичним етапом розгортання SIEM-системи стала інсталяція компонента OpenSearch, який виконує функцію індексації, зберігання та забезпечення швидкого повнотекстового пошуку по масивах лог-файлів. Для забезпечення сумісності з Graylog 6.0 було обрано версію OpenSearch 2.12. Враховуючи особливості роботи з GPG-ключами репозиторіїв у поточній версії ОС, було прийнято рішення про використання методу прямого розгортання через бінарний пакет. Інсталяційний файл формату .deb було завантажено з офіційного ресурсу розробника та встановлено за допомогою пакетного менеджера dpkg.

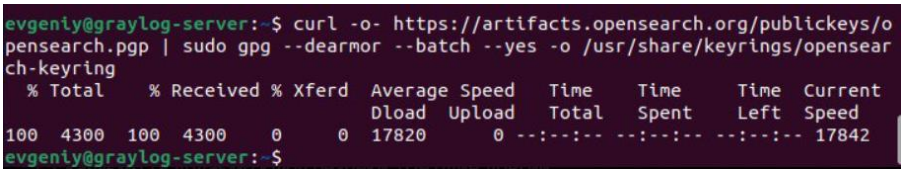


Рисунок 2.9 — Завантаження та додавання ключа безпеки



Рисунок 2.10 — Додавання репозиторію

Перед першим запуском служби було виконано обов’язкове налаштування параметрів ядра операційної системи Linux. Оскільки OpenSearch інтенсивно використовує механізм відображення пам’яті (memory mapping) для роботи з індексами Lucene, стандартне обмеження операційної системи є недостатнім. Параметр vm.max_map_count було збільшено до значення 262144 шляхом внесення змін у конфігураційний файл /etc/sysctl.conf, що забезпечило стабільність роботи процесу індексації.

Важливим аспектом налаштування стала оптимізація споживання системних ресурсів, зумовлена апаратними обмеженнями лабораторного стенду. У конфігураційному файлі jvm.options параметри виділення динамічної пам’яті для віртуальної

машини Java (Heap Size) — -Xms (початковий розмір) та -Xmx (максимальний розмір) — було зменшено зі стандартного 1 ГБ до 512 МБ. Це дозволило запобігти вичерпанню оперативної пам’яті сервера та аварійному завершенню роботи служб.

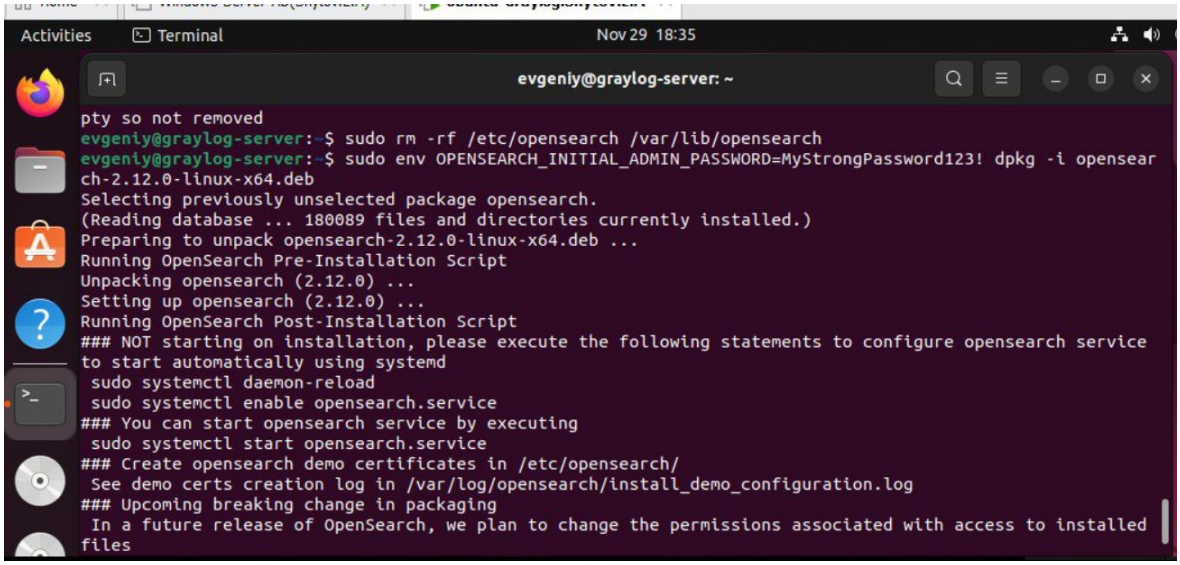


Рисунок 2.11 — Успішне встановлення програмного забезпечення

Конфігурація мережевої взаємодії та кластеризації здійснювалася у файлі /etc/opensearch/opensearch.yml. Було задано ідентифікатори кластера та вузла, а мережевий інтерфейс налаштовано на прослуховування всіх доступних IP-адрес (0.0.0.0) для забезпечення зв’язку з іншими компонентами.

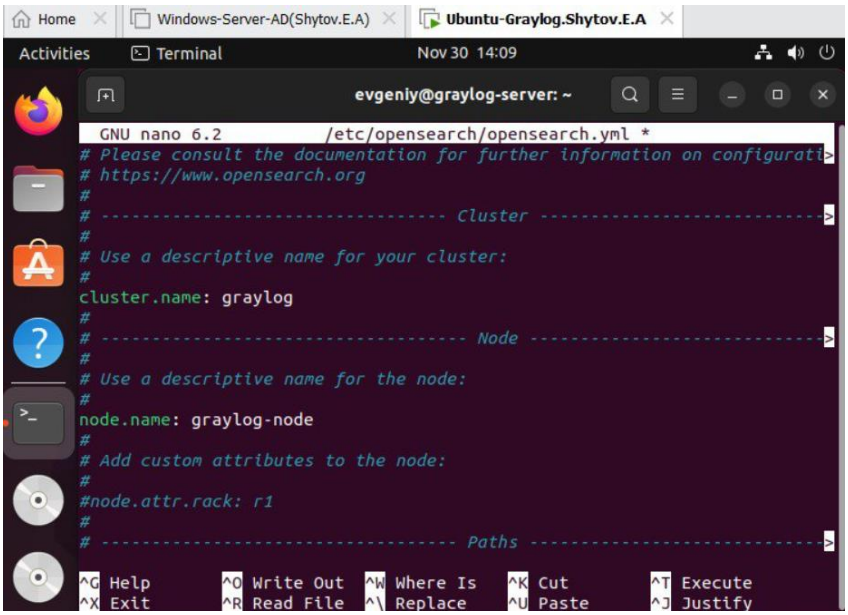


Рисунок 2.12 — Налаштування конфігураційних файлів

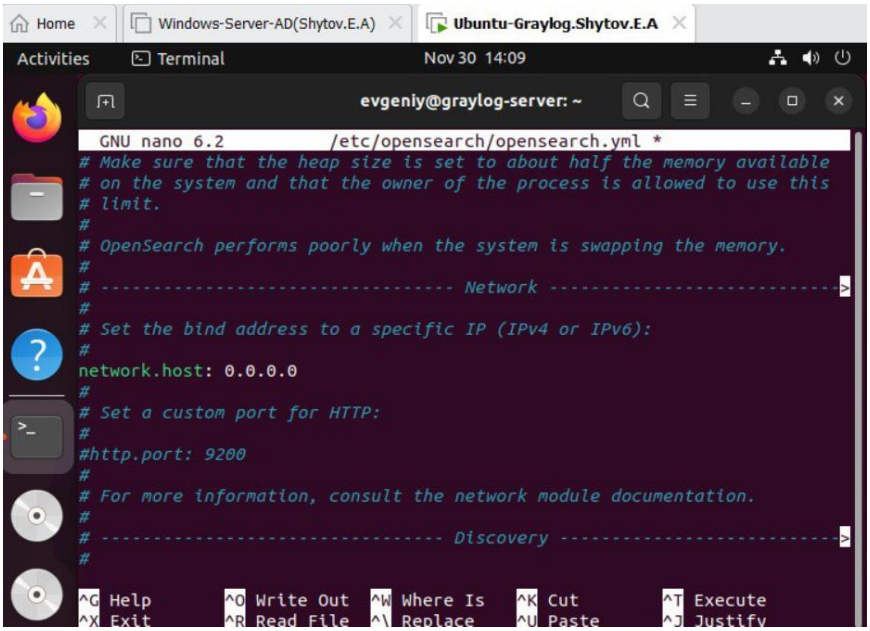


Рисунок 2.13 — Налаштування конфігураційних файлів

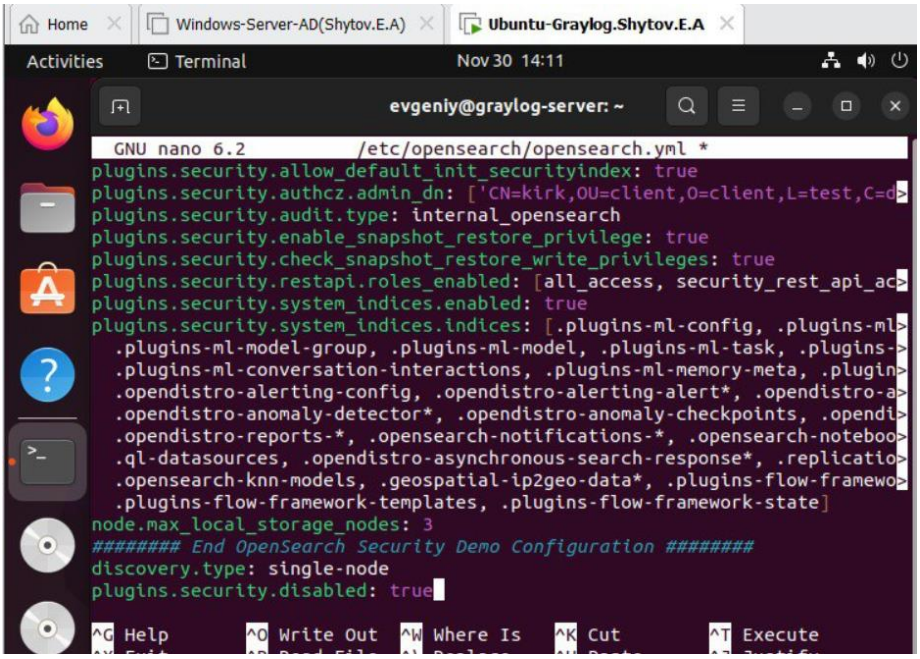


Рисунок 2.14 — Налаштування конфігураційних файлів

З метою спрощення інтеграції з Graylog у межах ізольованого тестового середовища вбудований плагін безпеки OpenSearch Security було деактивовано. Після застосування налаштувань службу було успішно запущено та додано до автозавантаження.[22]

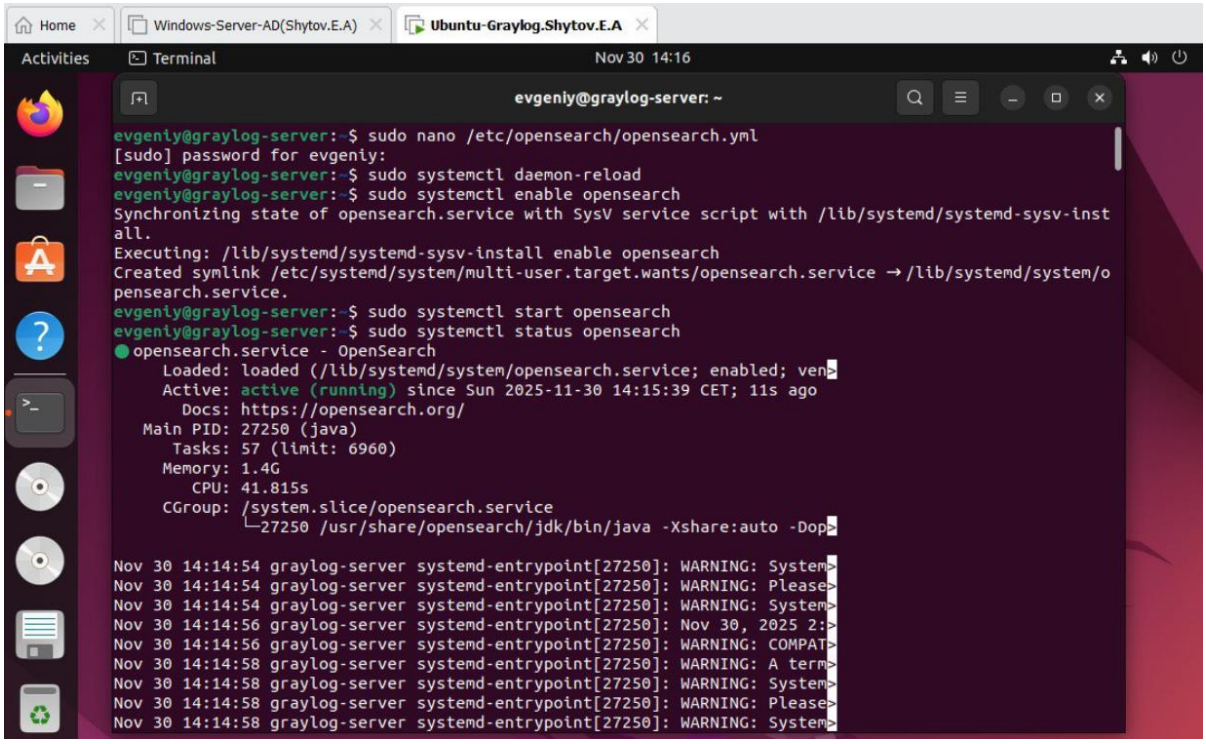


Рисунок 2.15 — Запуск та перевірка працездатності служби

2.2.2. Розгортання Graylog Server.

Завершальним етапом підготовки серверної частини SIEM-системи стала інсталяція ядра платформи — Graylog Server. Процес розгортання розпочався з інтеграції офіційного репозиторію Graylog у систему керування пакетами Ubuntu, що дозволило отримати актуальну версію 6.0. Безпосередня інсталяція виконувалася за допомогою команди apt install graylog-server, яка автоматично розгорнула необхідні бінарні файли, бібліотеки та створила системні служби.

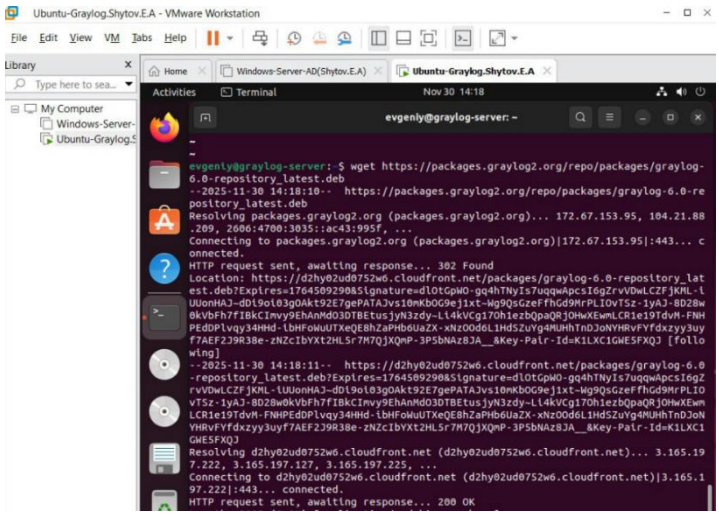


Рисунок 2.16 — Завантаження Graylog-server

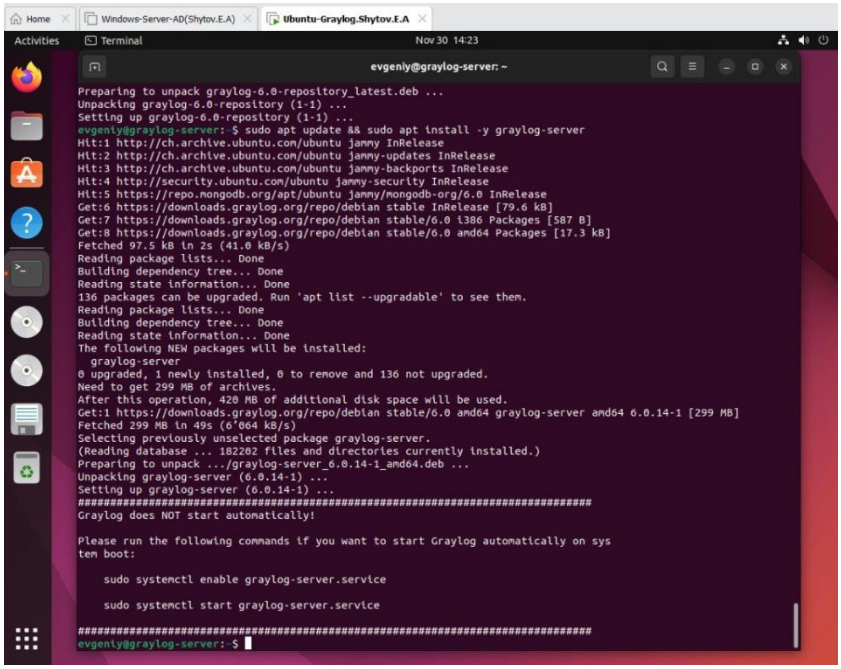


Рисунок 2.17 — Встановлення Graylog-server

Критично важливим етапом налаштування було забезпечення безпеки облікових записів та сесій користувачів. Архітектура Graylog не дозволяє запуск сервера без попередньої генерації двох секретних параметрів у конфігураційному файлі server.conf:

password_secret: Цей параметр використовується для "соління" (salting) та шифрування сесій користувачів. Для генерації криптографічно стійкого рядка символів з високим рівнем ентропії було використано утиліту pwgen з параметрами -N 1 -s 96, що створила випадкову послідовність довжиною 96 символів. Це унеможливлює атаки типу "session hijacking" через передбачення ключів шифрування.

root_password_sha2: Graylog не зберігає пароль адміністратора у відкритому вигляді. Замість цього система вимагає SHA-256 хеш пароля. Генерація хешу виконувалася за допомогою команди echo -n "password" | sha256sum. Такий підхід гарантує, що навіть у випадку компрометації конфігураційного файлу, зловмисник не отримає прямий доступ до пароля адміністратора.

```
evgeniy@graylog-server:~$ sudo apt install -y pwgen
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  pwgen
0 upgraded, 1 newly installed, 0 to remove and 136 not upgraded.
Need to get 17.4 kB of archives.
After this operation, 53.2 kB of additional disk space will be used.
Get:1 http://ch.archive.ubuntu.com/ubuntu jammy/universe amd64 pwgen amd64 2.08-2build
1 [17.4 kB]
Fetched 17.4 kB in 0s (216 kB/s)
Selecting previously unselected package pwgen.
(Reading database ... 182539 files and directories currently installed.)
Preparing to unpack .../pwgen_2.08-2build1_amd64.deb ...
Unpacking pwgen (2.08-2build1) ...
Setting up pwgen (2.08-2build1) ...
Processing triggers for man-db (2.10.2-1) ...
evgeniy@graylog-server:~$
```

Рисунок 2.18 — Встановлення генератора секретних ключів

```
evgeniy@graylog-server:~$ pwgen -N 1 -s 96
nP0EaM85mTjKUMwOSeHGbi61kOvKYl0KWDGJMvIouVFhx10nR1roaHiMQpJ7ybvijey3dJbZQtFsLCjJGUu3eu
43Vxkrquds
evgeniy@graylog-server:~$
```

Рисунок 2.19 — Генерація хеш-ключа

Наступним кроком стала конфігурація мережевого інтерфейсу для доступу до веб-панелі керування. За замовчуванням Graylog прослуховує лише локальний інтерфейс (127.0.0.1), що унеможливлює доступ до нього ззовні віртуальної машини. Для забезпечення можливості керування системою з хостового комп'ютера параметр http_bind_address у файлі /etc/graylog/server/server.conf було змінено на 0.0.0.0:9000. Це дозволило серверу приймати з'єднання на всіх доступних мережевих інтерфейсах.

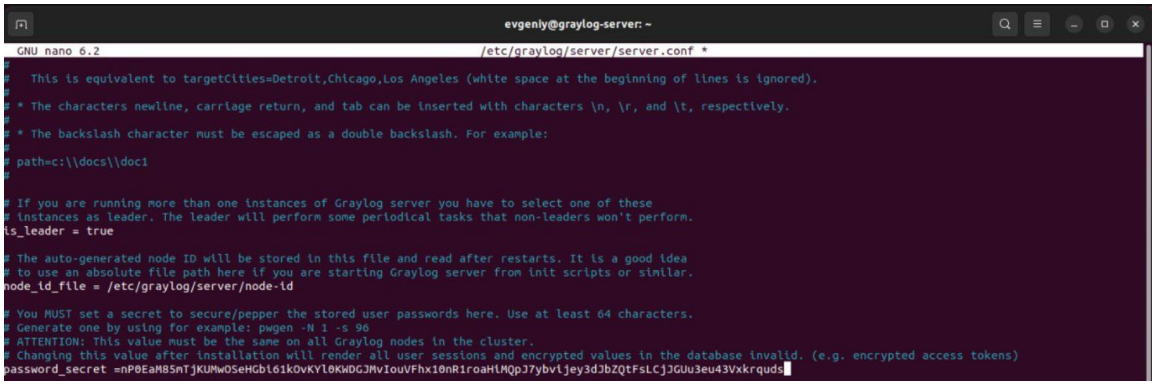


Рисунок 2.20 — Редагування конфігураційних файлів

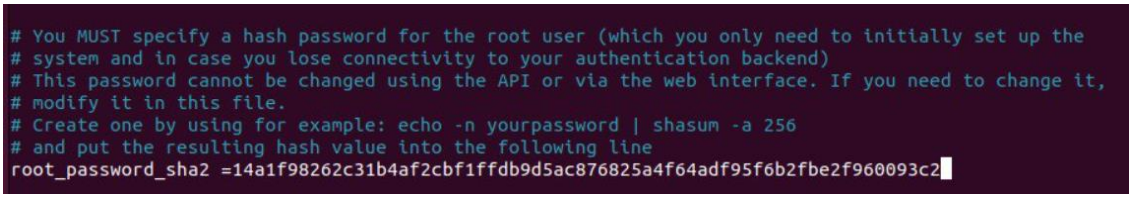


Рисунок 2.21 — Редагування конфігураційних файлів

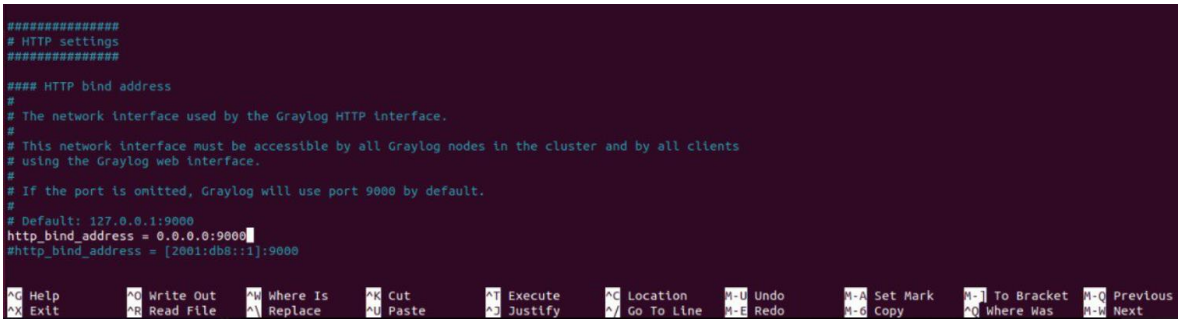


Рисунок 2.22 — Редагування конфігураційних файлів

Додатково, аналогічно до налаштувань OpenSearch, було проведено оптимізацію споживання оперативної пам'яті. У файлі параметрів запуску /etc/default/graylog-server ліміт пам'яті для Java (Heap Size) було обмежено до 512 МБ (-Xms512m -Xmx512m), що забезпечило стабільну роботу всіх компонентів системи в умовах обмежених ресурсів лабораторного стенду. Після завершення конфігурації службу було успішно запущено та перевірено доступність веб-інтерфейсу.

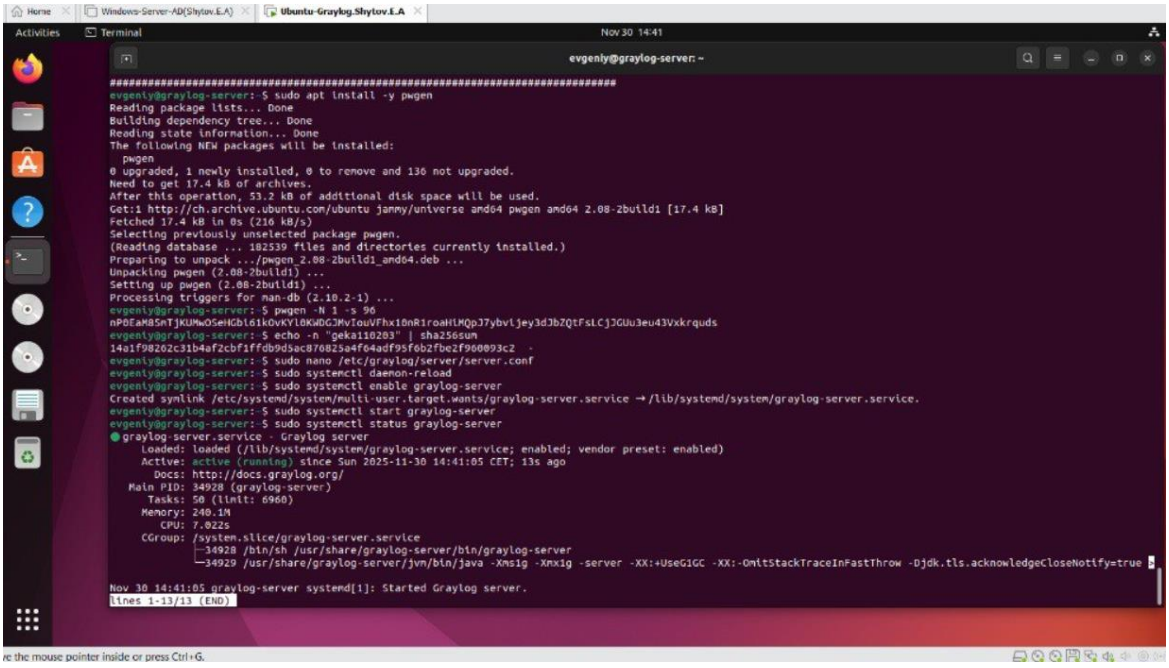


Рисунок 2.23 — Перевірка працездатності graylog-server

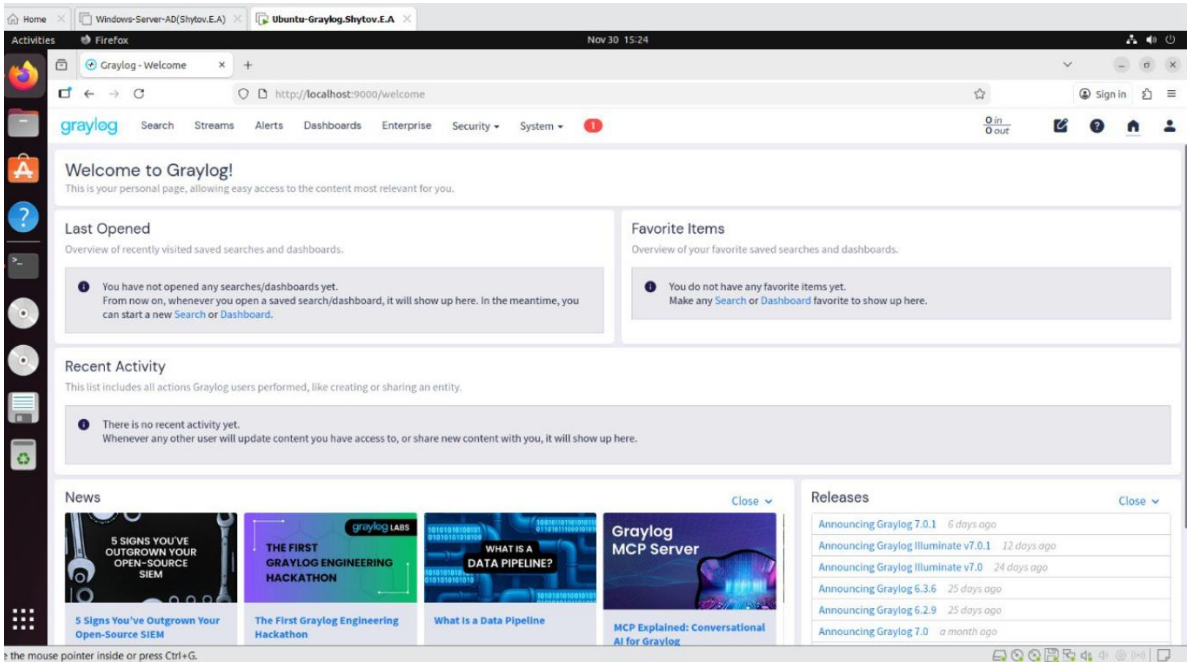


Рисунок 2.24 — Перевірка доступу до веб-інтерфейсу graylog-server

2.2.3 Налаштування об'єкта захисту (Active Directory)

Ключовим етапом побудови захищеного периметра корпоративної мережі стало розгортання служби каталогів Active Directory (AD). Вона виступає централізованою базою даних для керування обліковими записами, групами безпеки та політиками доступу. Для реалізації цього завдання віртуальну машину під управлінням Windows Server 2022 було налаштовано як єдиний контролер домену (Domain Controller, DC) у новому лісі.

Процес конфігурації розпочався зі встановлення ролі Active Directory Domain Services (AD DS) через диспетчер серверів. На етапі підвищення ролі сервера до рівня контролера домену було обрано опцію розгортання нового лісу з кореневим доменним ім’ям diploma.local. Використання доменної зони .local було обрано для ізоляції внутрішнього простору імен від зовнішніх мереж. Оскільки функціонування Active Directory неможливе без служби доменних імен, роль DNS-сервера була встановлена автоматично, що забезпечило коректну реєстрацію SRV-записів, необхідних для роботи механізмів аутентифікації Kerberos.

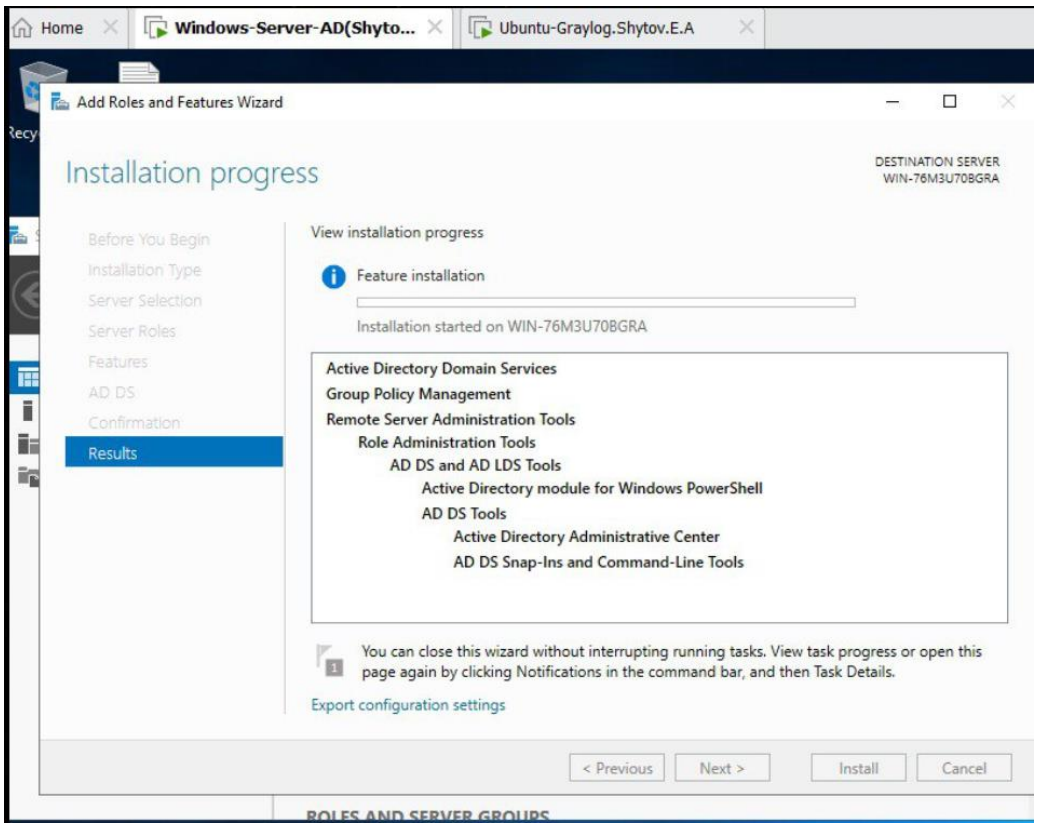


Рисунок 2.25 — Інсталяція та налаштування WindowsAD

Під час етапу перевірки попередніх вимог (Prerequisites Check) було виявлено невідповідність політикам безпеки: пароль локального облікового запису адміністратора не відповідав вимогам складності, які застосовуються за замовчуванням до адміністраторів домену. Оскільки локальний адміністратор після підвищення ролі набуває повноважень глобального адміністратора домену (Enterprise Admin), система заблокувала процес інсталяції. Для вирішення цієї проблеми без переривання процесу налаштування було використано командний інтерфейс. За допомогою утиліти net user пароль адміністратора було змінено на криптографічно стійкий, що дозволило успішно пройти перевірку безпеки та завершити інсталяцію.

Після автоматичного перезавантаження сервера, яке тривало значний час через ініціалізацію бази даних AD, вхід у систему виконувався вже в контексті створеного домену (DIPLOMA\Administrator). Це підтвердило успішне розгортання контролера домену та готовність інфраструктури до подальшого налаштування політик аудиту.

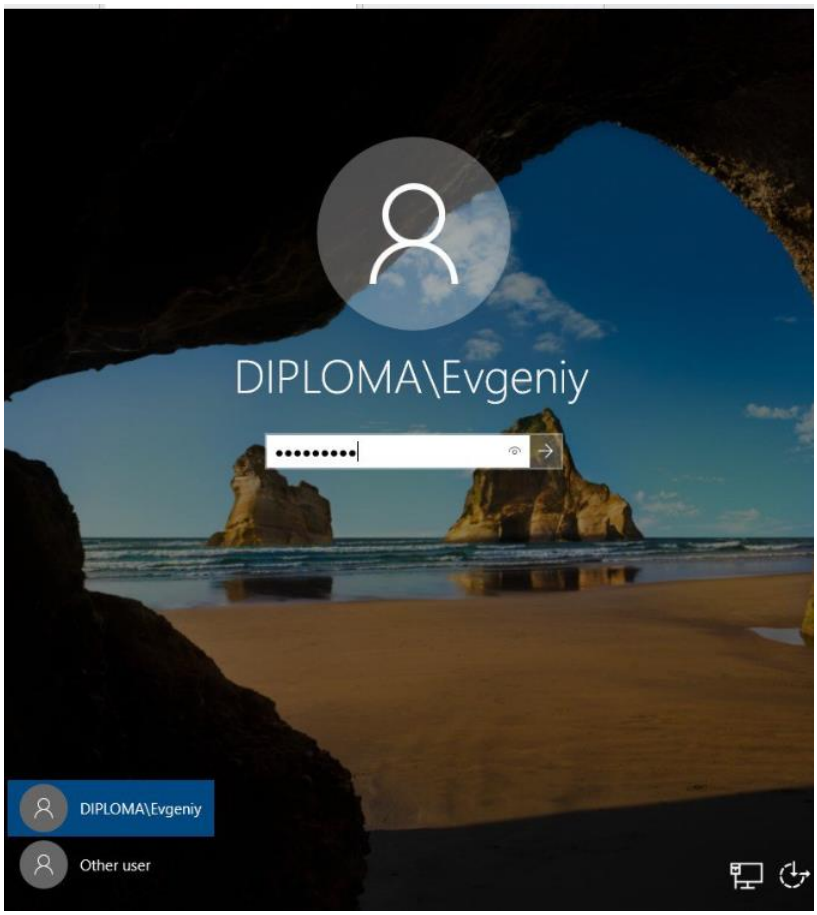


Рисунок 2.26 — Успішне створення домену

Після розгортання контролера домену було виконано налаштування політик безпеки для забезпечення можливості детектування атак типу Brute Force. У середовищі Active Directory за замовчуванням політика блокування облікових записів часто відключена або налаштована нестрого, що робить систему вразливою до повного перебору паролів.

Для виправлення цього недоліку та генерації подій безпеки було сконфігуровано групову політику Account Lockout Policy (Політика блокування облікових записів) у межах політики домену за замовчуванням (Default Domain Policy).

Налаштування виконувалося за наступним алгоритмом:

У редакторі групових політик (Group Policy Management Editor) було здійснено перехід за шляхом: Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Account Lockout Policy.

Ключовий параметр «Account lockout threshold» (Поріг блокування) було встановлено на значення 3 невдалі спроби входу.

Параметри «Account lockout duration» (Тривалість блокування) та «Reset account lockout counter after» (Час скидання лічильника) були автоматично встановлені системою на рекомендоване значення 30 хвилин.

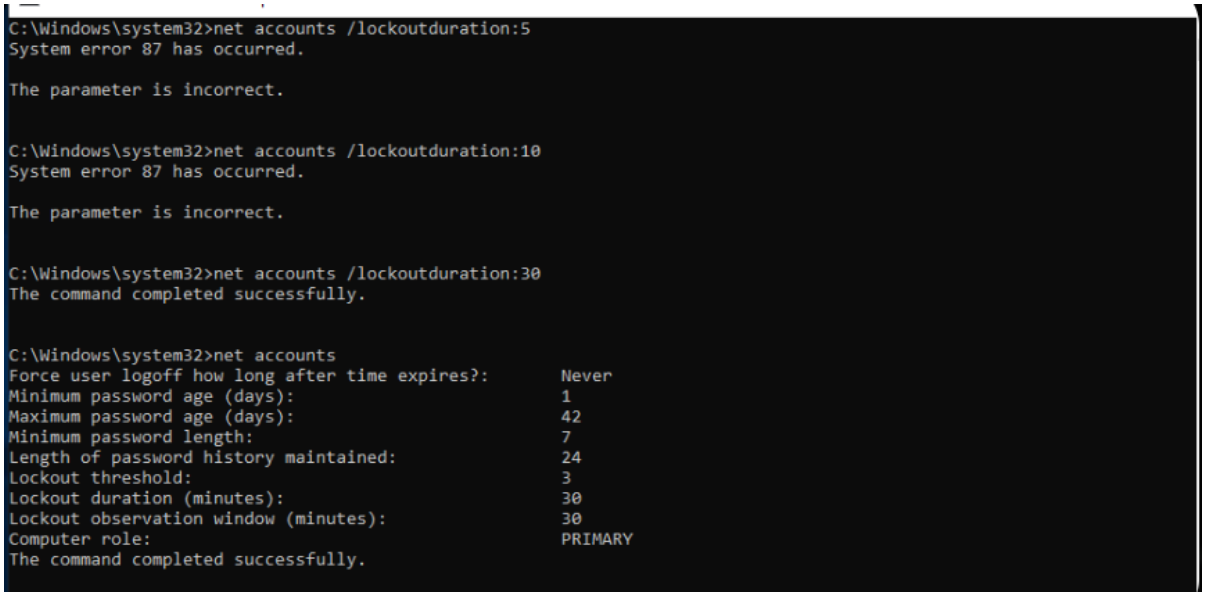


Рисунок 2.27 — Успішне створення домену

Варто зазначити, що через обмежені апаратні ресурси віртуальної машини (2 ГБ RAM) графічний інтерфейс редактора політик працював із затримками. Тому для гарантованого застосування налаштувань було використано альтернативний метод конфігурації через командний рядок з правами адміністратора. За допомогою команди net accounts /lockoutthreshold:3 політика була застосована безпосередньо до бази даних безпеки (SAM) контролера домену.

Обґрунтування налаштування: Встановлення порогу блокування є критично важливою умовою для функціонування розробленої системи моніторингу. Тільки за наявності цього обмеження операційна система Windows генерує подію безпеки з ідентифікатором Event ID 4740 («A user account was locked out»). Без цього налаштування Graylog фіксував би лише численні події помилок входу (4625), але не зміг би ідентифікувати факт успішного відбиття атаки системою захисту.

2.2.4 Встановлення та конфігурація агента транспортування подій Winlogbeat

Для забезпечення надійної та захищеної передачі журналів подій з Windows Server до системи Graylog було обрано легковаговий агент Winlogbeat. На відміну від застарілих методів (наприклад, NXLog), Winlogbeat забезпечує буферизацію даних у разі втрати зв'язку та підтримує шифрування.

Враховуючи обмеження безпеки серверної ОС (посилена конфігурація Internet Explorer), завантаження та встановлення агента виконувалося засобами командної оболонки PowerShell. За допомогою командлету Invoke-WebRequest архів з програмним забезпеченням було завантажено безпосередньо з офіційного репозиторію Elastic, після чого розпаковано у системну директорію C:\Program Files.[23]



Рисунок 2.28 — Встановлення агента



Рисунок 2.29 — Розпакування архіву

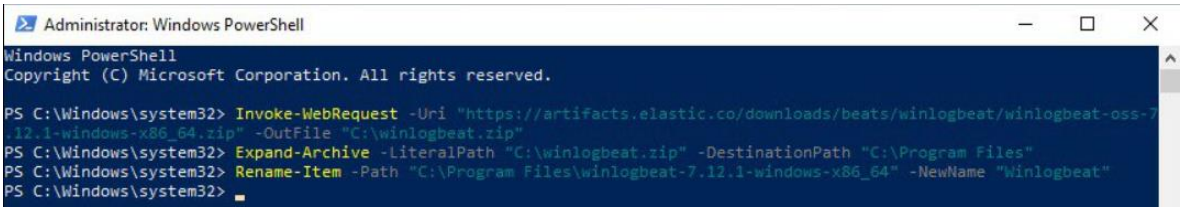


Рисунок 2.30 — Перейменування папки (для зручності)

Ключовим етапом стала конфігурація файлу winlogbeat.yml. У ньому було визначено перелік журналів для моніторингу: стандартні Security, System, Application, а також додатковий спеціалізований канал Microsoft-Windows-Windows Defender/Operational. Останній було додано для реалізації моніторингу антивірусного захисту та виявлення шкідливого ПЗ.



Рисунок 2.31 — Перейменування папки (для зручності)

У секції виводу даних (output.logstash) було прописано IP-адресу сервера Graylog (192.168.52.129) та порт 5044. В процесі налаштування було вирішено проблему прав доступу при збереженні конфігураційного файлу у захищену системну директорію шляхом запуску текстового редактора з підвищеними привілеями через PowerShell. Після перевірки синтаксису конфігурації агент було встановлено як системну службу та запущено в автоматичному режимі.

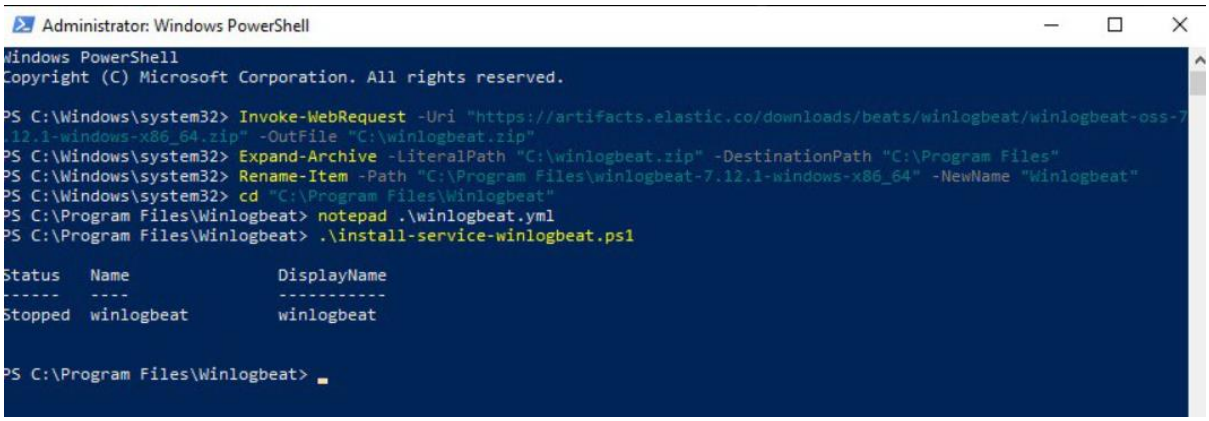


Рисунок 2.32 — Налаштування служби за допомогою Powershell

Для того щоб сервер Graylog міг приймати дані від агента Winlogbeat, було налаштовано точку входу (Input). Процедура виконувалася через веб-інтерфейс у розділі «System / Inputs».

Параметри створеного Input:

- Тип входу: Beats (оскільки Winlogbeat використовує протокол Beats/Lumberjack).

- Node: Обрано вузол Graylog-server.
- Bind address: Вказано адресу 0.0.0.0, що дозволяє приймати з'єднання на всіх мережевих інтерфейсах сервера, а не тільки локально.
- Port: Встановлено стандартний порт 5044.

Після запуску Input перейшов у статус RUNNING, а в метриках «Network IO» було зафіксовано вхідний потік даних, що підтвердило успішне встановлення з'єднання між контролером домену та SIEM-системою.

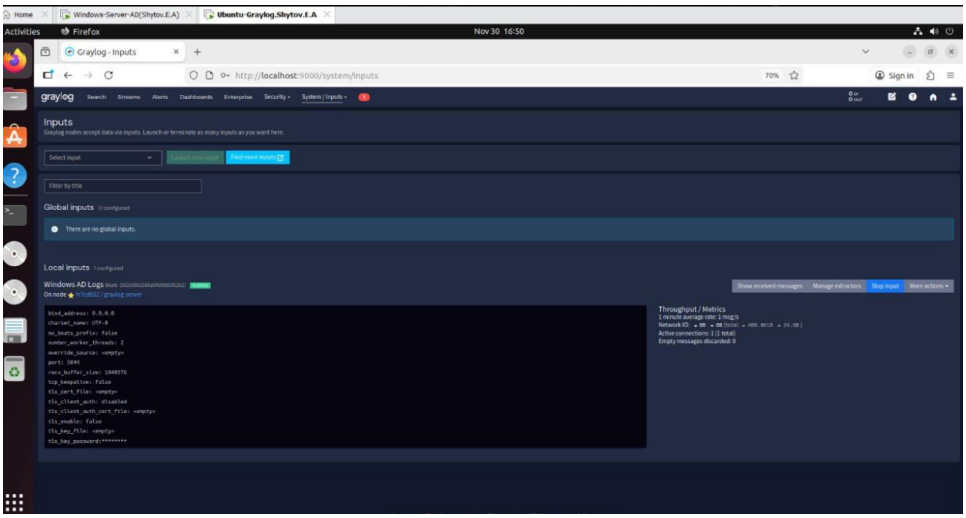


Рисунок 2.33 — Зафіксований вхідний потік даних

ВИСНОВКИ

У другому розділі магістерської роботи реалізовано практичну частину дослідження, яка полягала у проектуванні та розгортанні комплексного стенду для моніторингу безпеки інфраструктури Active Directory. На базі гіпервізора VMware Workstation було створено ізольоване віртуальне середовище, що включає контролер домену на базі Windows Server 2022 та сервер моніторингу під управлінням Ubuntu 22.04 LTS. Така архітектура дозволила змоделювати реальні умови функціонування корпоративної мережі та забезпечити контрольоване проведення експериментів.

В ході роботи було виконано розгортання та детальне налаштування компонентів SIEM-системи Graylog, включаючи базу даних MongoDB для зберігання метаданих та пошуковий рушій OpenSearch для індексації логів. Особливу увагу було приділено оптимізації параметрів віртуальної машини Java (JVM) для забезпечення стабільної роботи серверних додатків в умовах обмежених апаратних ресурсів. На стороні об'єкта захисту — контролера домену — було налаштовано політики аудиту та блокування облікових записів, що є необхідною умовою для генерації релевантних подій безпеки.

Для організації надійного транспортування логів було обрано та сконфігуровано агент Winlogbeat, який забезпечує передачу даних із журналів Windows Event Log (Security, System, Application) та спеціалізованого каналу Windows Defender безпосередньо до сервера Graylog. Успішне налаштування вхідного потоку (Input) та підтвердження отримання даних свідчать про повну працездатність розгорнутої системи моніторингу. Створений лабораторний стенд є готовою платформою для проведення наступного етапу досліджень — моделювання кібератак та оцінки ефективності їх виявлення засобами централізованого аналізу подій.

РОЗДІЛ 3. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ

3.1Методика проведення експерименту та сценарії загроз

Для верифікації ефективності розгорнутої системи моніторингу та оцінки її здатності виявляти інциденти інформаційної безпеки в режимі реального часу було розроблено комплексну методику експериментального дослідження. Дана методика базується на моделюванні ланцюжка типових дій зловмисника (Cyber Kill Chain), спрямованих на компрометацію контролера домену Active Directory, та охоплює різні вектори загроз: від спроб проникнення до закріплення в системі та знищення доказів.

Перший етап експерименту передбачав реалізацію сценарію атаки на підбір пароля (Brute Force Attack). Метою цього сценарію була імітація спроби зловмисника отримати несанкціонований доступ до облікового запису адміністратора шляхом багаторазового введення невірних облікових даних. Очікуваною реакцією системи захисту у цьому випадку є фіксація масових помилок аутентифікації з ідентифікатором Event ID 4625, а також, як наслідок спрацювання налаштованих політик безпеки, реєстрація критичної події блокування облікового запису Event ID 4740.[24]

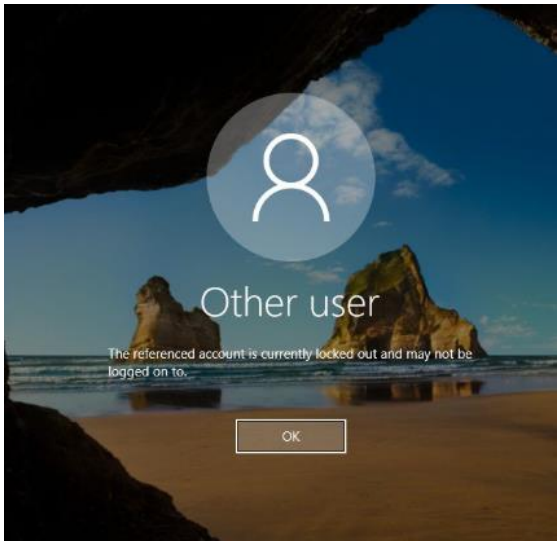


Рисунок 3.1 — Блокування акаунту за допомогою невдалого введення паролю

Наступним кроком було моделювання створення «бекдору» (Persistence) для забезпечення постійного доступу до скомпрометованої системи. Сценарій полягав у виявленні факту створення нелегітимного облікового запису користувача в обхід встановлених процедур. Система моніторингу повинна була зареєструвати подію Event ID 4720, зафіксувавши при цьому не тільки ім'я нового користувача, але й ім'я облікового запису, від імені якого виконувалася дія.

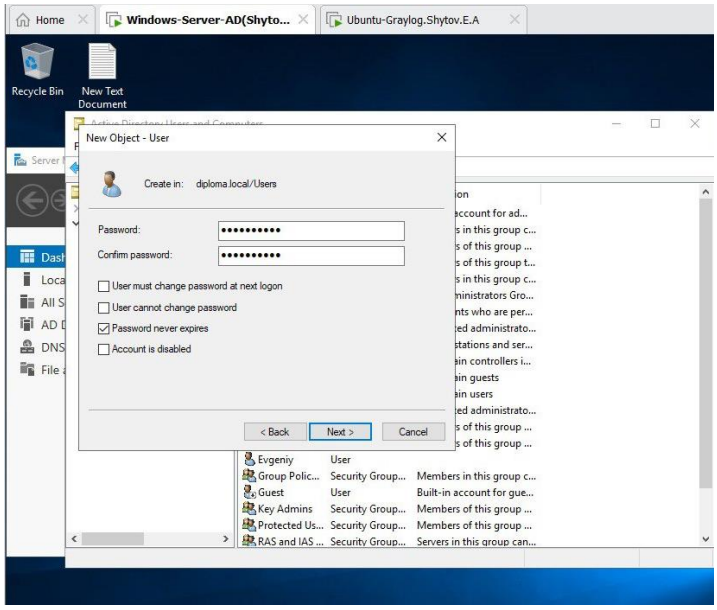


Рисунок 3.2 — Створення нелегітимного облікового запису користувача

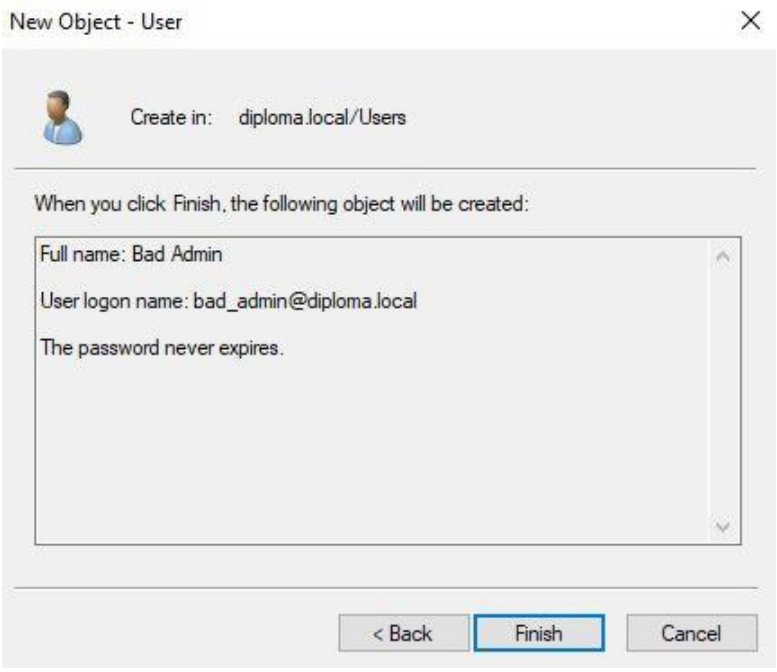


Рисунок 3.3 — Створення нелегітимного облікового запису користувача

Для перевірки контролю за привілейованими доступами було реалізовано сценарій ескалації привілеїв (Privilege Escalation). Оскільки для повного контролю над доменом зловмиснику необхідно підвищити права створеного користувача до рівня адміністратора, метою цього етапу була фіксація змін у складі привілейованих груп безпеки, зокрема групи «Administrators».

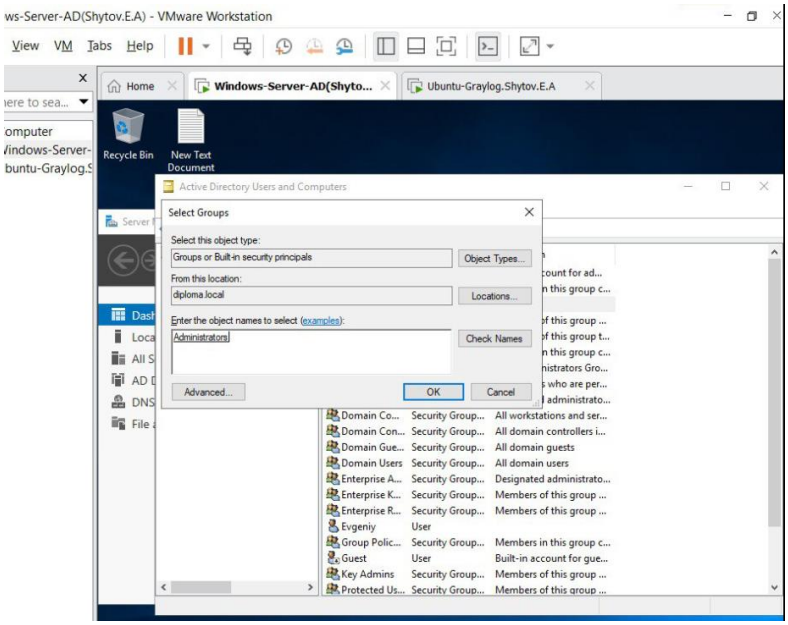


Рисунок 3.4 — Додавання нелегітимного користувача до групи адміністраторів

Індикатором такої активності слугували події з ідентифікаторами Event ID 4732 або 4728, що свідчать про додавання учасника до глобальної групи безпеки.

Завершальний етап моделювання атаки був спрямований на приховування слідів злочину (Covering Tracks). Цей сценарій передбачав видалення тимчасових облікових записів та спробу очищення журналів подій для ускладнення розслідування інциденту.

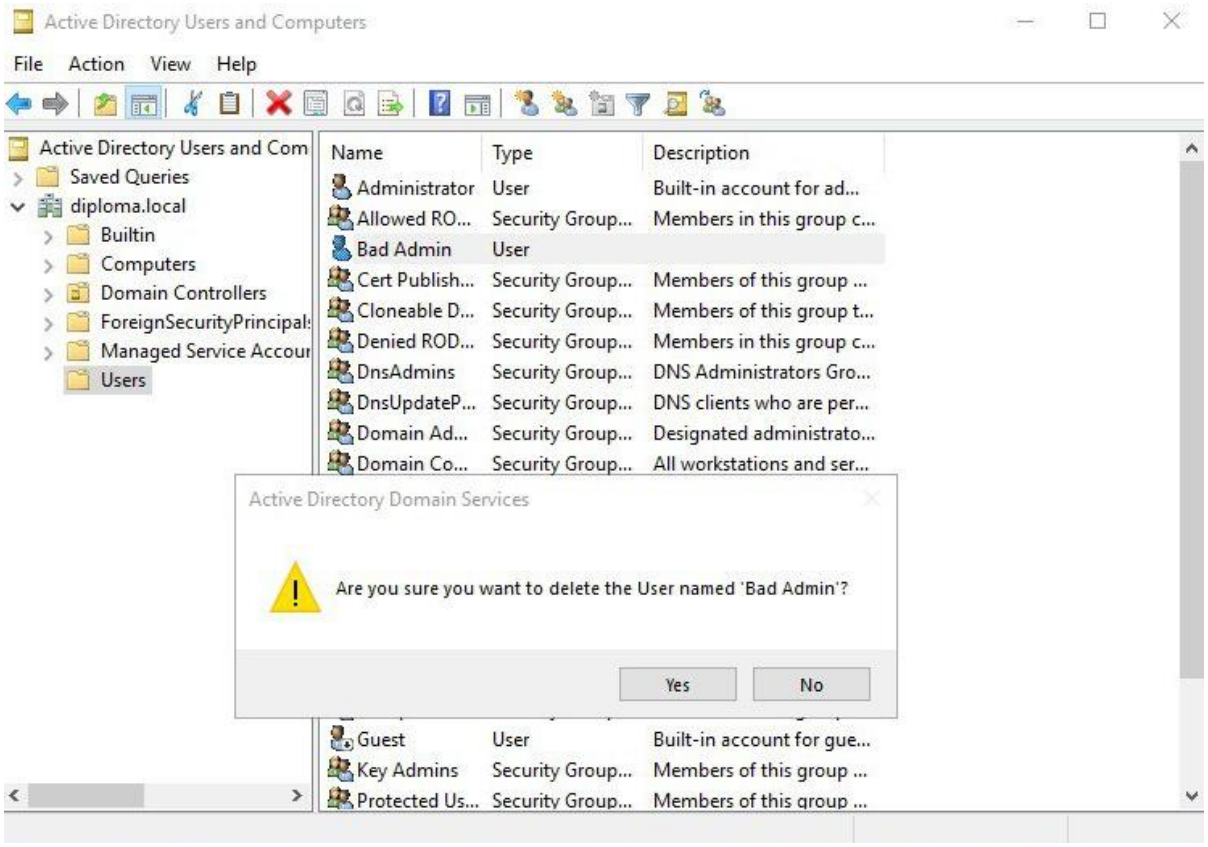


Рисунок 3.5 — Видалення(замітання слідів)існування нелегітимного користувача

Система SIEM повинна була виявити факти видалення об'єктів Active Directory (Event ID 4726) та критичну подію очищення журналу аудиту (Event ID 1102).

Додатково, для перевірки інтеграційних можливостей системи, було протестовано сценарій виявлення шкідливого програмного забезпечення (Malware Detection). За допомогою безпечного тестового файлу EICAR було перевірено коректність надходження та індексації логів від джерела Windows Defender, зокрема реєстрацію події виявлення загрози з ідентифікатором Event ID 1116. Реалізація зазначеної послідовності сценаріїв дозволила комплексно оцінити роботу налаштованих правил кореляції, засобів візуалізації та системи автоматичного оповіщення.

3.2 Виявлення та аналіз інцидентів інформаційної безпеки

3.2.1. Аналіз спроб несанкціонованого доступу та реакції системи захисту

Першим етапом експериментального дослідження стала імітація атаки типу «Brute Force» (повний перебір паролів), яка є одним з найпоширеніших методів отримання несанкціонованого доступу до корпоративних мереж. Метою даного етапу було перевірити здатність системи Graylog детектувати численні помилки аутентифікації та зафіксувати автоматичну реакцію засобів захисту Windows Server, а саме блокування облікового запису. Для реалізації сценарію на стороні контролера домену було ініційовано спробу входу в систему під попередньо створеним тестовим обліковим записом test_lock. Було виконано серію з 10 спроб введення завідомо невірних паролів з коротким інтервалом часу, що імітує роботу автоматизованого скрипта-брутфорсера. У результаті операційна система Windows, відповідно до налаштованих політик аудиту, зафіксувала помилки аутентифікації та згенерувала відповідні події безпеки.

Система моніторингу в режимі реального часу отримала та проіндексувала потік даних від агента Winlogbeat. За допомогою пошукового запиту winlog.event_id:4625 у консолі Graylog було миттєво виявлено серію повідомлень «An account failed to log on». На деталізованому перегляді події (рис. 3.1) чітко ідентифікуються ключові параметри інциденту: ім’я об’єкта атаки (TargetUserName: test_lock), ім’я робочої станції, з якої здійснювалися спроби входу (WorkstationName), IP-адреса джерела атаки (IpAddress) та причина відмови в доступі.

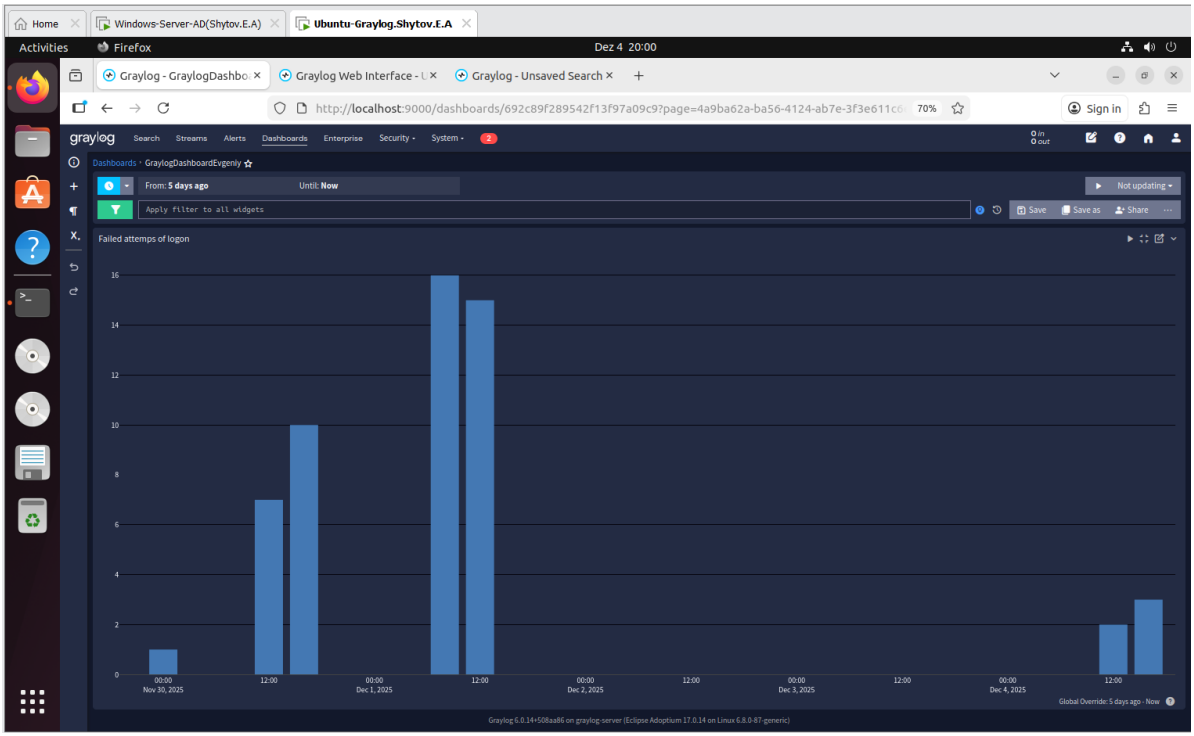


Рисунок 3.6 — Графік невдалих спроб входу

Важливим результатом експерименту стала перевірка спрацювання політики безпеки. Оскільки в налаштуваннях групової політики (Account Lockout Policy) було встановлено поріг у 3 невдалі спроби, після четвертого введення невірного пароля система захисту Active Directory автоматично заблокувала обліковий запис test_lock. Цей факт був зафіксований системою Graylog як критична подія з ідентифікатором Event ID 4740 («A user account was locked out»). Для оперативного оповіщення адміністратора про цей інцидент на головному дашборді було налаштовано спеціальний віджет-індикатор Він налаштований таким чином, що при появі хоча б однієї події блокування його фон змінює колір на червоний, сигналізуючи про необхідність негайної реакції.

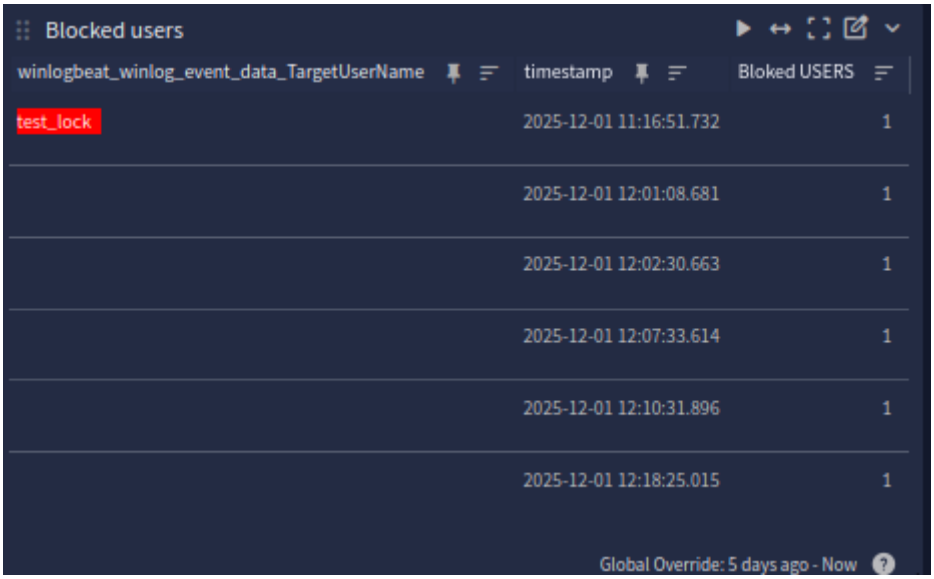


Рисунок 3.7 — Індикація блокування облікового запису (Event ID 4740) на панелі моніторингу

Таким чином, експеримент підтвердив, що розгорнута система дозволяє не лише ретроспективно аналізувати спроби злому, але й візуалізувати успішне відбиття атаки засобами штатного захисту операційної системи.

3.2.2. Контроль цілісності облікових записів та груп

Наступним етапом експериментального дослідження стала перевірка механізмів контролю життєвого циклу облікових записів, що є критично важливим для виявлення спроб зловмисників закріпитися в системі (Persistence) або створити приховані канали доступу («бекдори»). Для моделювання даного сценарію загроз на контролері домену було ініційовано процес створення нового користувача з іменем bad_admin в обхід стандартних процедур погодження. Ця дія мала на меті імітувати поведінку зловмисника, який, отримавши первинний доступ, створює додатковий обліковий запис для забезпечення постійної присутності в інфраструктурі.

Система моніторингу Graylog успішно зафіксувала цю активність у реальному часі, зареєструвавши подію з ідентифікатором Event ID 4720 («A user account was created»). Аналіз перехопленого лог-файлу дозволив отримати повну атрибуцію інциденту, включаючи час створення, ім’я новоствореного об’єкта

(TargetUserName: bad_admin) та, що найважливіше, ідентифікатор облікового запису, під яким виконувалася ця операція (SubjectUserName: Administrator). Така деталізація дозволяє однозначно встановити джерело компрометації або факт зловживання повноваженнями легітимним адміністратором.

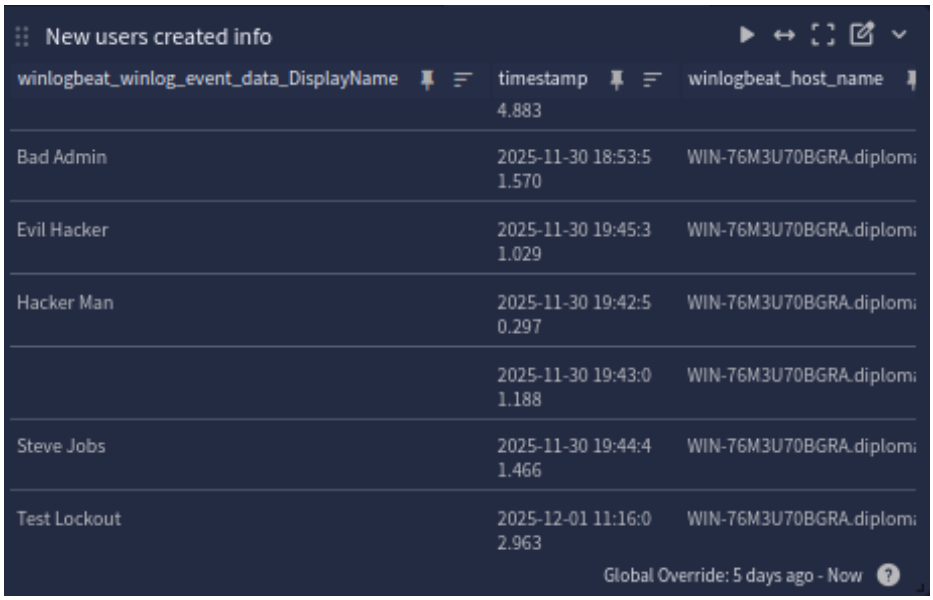


Рисунок 3.8 — Фіксація події несанкціонованого створення облікового запису (Event ID 4720)

Для перевірки здатності системи виявляти спроби приховування слідів кіберзлочину (Defense Evasion) було реалізовано сценарій видалення компрометованого облікового запису. Після виконання необхідних маніпуляцій тестовий користувач bad_admin був видалений з Active Directory. Система SIEM миттєво ідентифікувала цю дію, згенерувавши запис про подію Event ID 4726 («A user account was deleted»). Налаштовані на дашборді віджети табличного типу дозволили візуалізувати цей процес у хронологічному порядку, зіставивши факт створення та подальшого видалення користувача, що є характерною ознакою нелегітимної активності в корпоративній мережі.

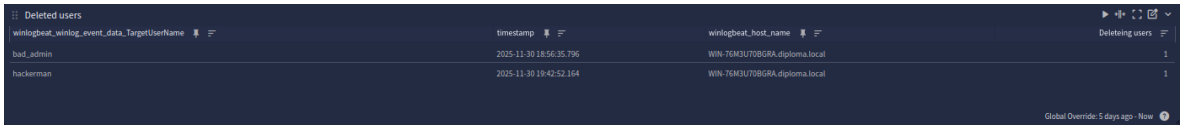


Рисунок 3.9 — Реєстрація факту видалення облікового запису (Event ID 4726)

Отримані результати підтверджують, що впроваджена система забезпечує повний аудит життєвого циклу об’єктів Active Directory, унеможливлюючи непомітне створення або знищення облікових записів без залишення цифрових слідів у централізованому сховищі логів.

3.2.3. Моніторинг змін у складі привілейованих груп та виявлення ескалації привілеїв

Однією з найбільш небезпечних стадій розвитку кібератаки є ескалація привілеїв (Privilege Escalation), коли зловмисник намагається отримати адміністративний доступ до системи для повного контролю над інфраструктурою. Для моделювання цього сценарію на контролері домену було виконано додавання попередньо створеного облікового запису bad_admin до вбудованої групи безпеки «Administrators», яка надає необмежені права управління сервером та доменом. Ця дія імітувала успішну спробу зловмисника закріпитися в системі з найвищим рівнем доступу.

Система моніторингу Graylog зафіксувала цю зміну в режимі реального часу, зареєструвавши подію з ідентифікатором Event ID 4732 («A member was added to a security-enabled local group») або Event ID 4728 (для глобальних груп).

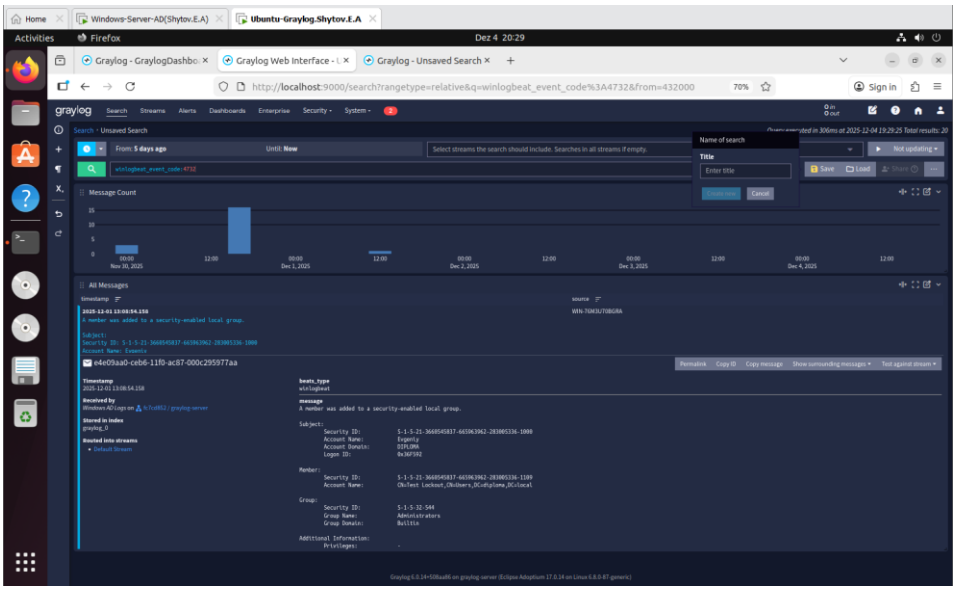


Рисунок 3.10 — Реєстрація події несанкціонованого надання адміністративних прав (Event ID 4732)

Аналіз перехопленого повідомлення дозволив чітко ідентифікувати деталі інциденту: поле TargetUserName вказувало на змінену групу («Administrators»), поле MemberName містило ідентифікатор доданого користувача (bad_admin), а поле SubjectUserName вказувало на обліковий запис, під яким виконувалася операція. Така деталізація дозволяє службі безпеки миттєво визначити легітимність дій та виявити потенційно скомпрометовані облікові записи адміністраторів.

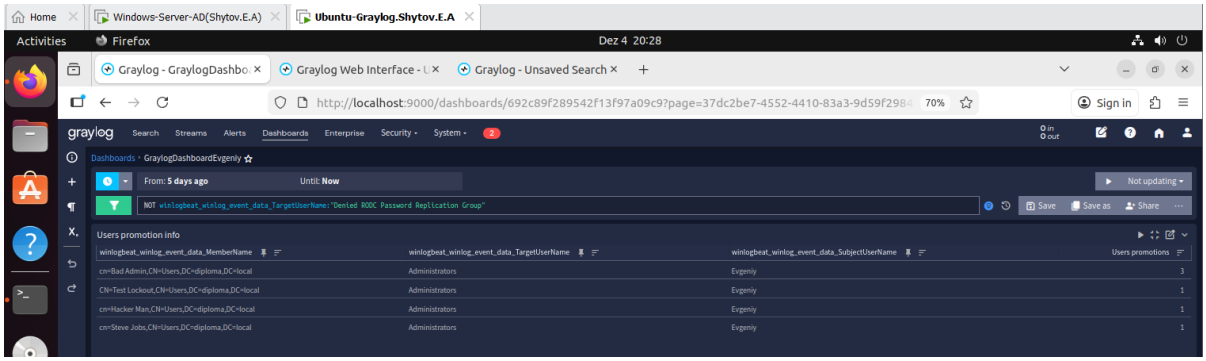


Рисунок 3.11 — Таблиця реєстрації подій несанкціонованого надання адміністративних прав (Event ID 4732)

Виявлення подібних подій є критично важливим для забезпечення інформаційної безпеки, оскільки отримання зловмисником прав адміністратора домену фактично означає повну компрометацію мережі. Маючи такі привілеї, атакуючий отримує можливість доступу до будь-яких конфіденційних даних, може змінювати налаштування безпеки, встановлювати шкідливе програмне забезпечення, очищати журнали подій для приховування своєї присутності та навіть знищити всю інфраструктуру Active Directory. Саме тому налаштована в рамках роботи система автоматичного оповіщення реагує на такі події з найвищим пріоритетом, що дозволяє адміністраторам заблокувати скомпрометований обліковий запис до того, як буде завдано непоправної шкоди.

3.2.4. Виявлення шкідливого програмного забезпечення та інтеграція з антивірусним захистом

Окремим напрямком експериментального дослідження стала перевірка можливостей системи щодо централізованого збору інформації про вірусні загрози.

Оскільки сучасні кібератаки часто супроводжуються впровадженням шкідливого програмного забезпечення (Malware) на сервери інфраструктури, критично важливим є забезпечення єдиної консолі моніторингу, яка об'єднує події безпеки Active Directory та алерти антивірусного захисту. Для реалізації цього завдання було попередньо налаштовано агент Winlogbeat на збір подій зі спеціалізованого журналу Microsoft-Windows-Windows Defender/Operational.

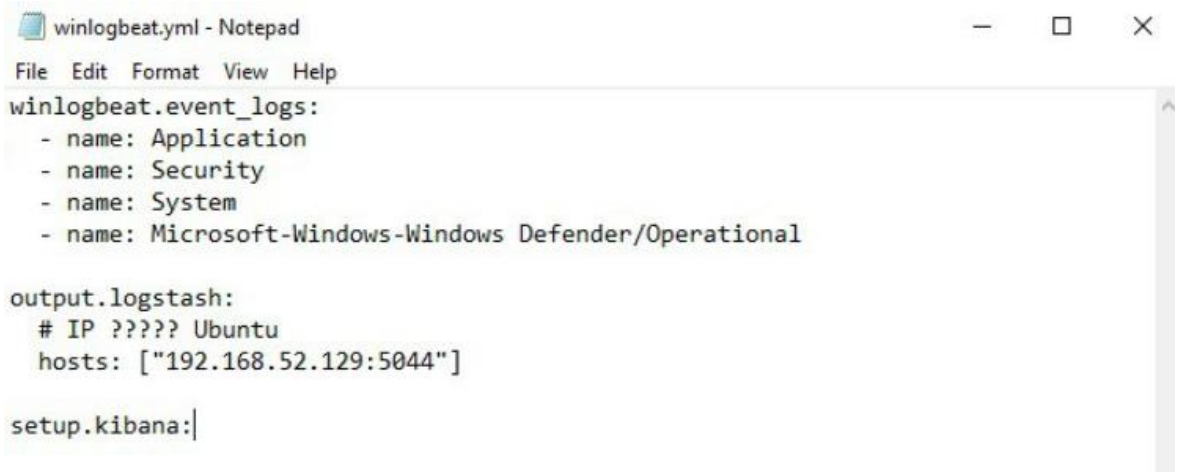


Рисунок 3.12 — Зміна конфігураційних файлів агента Winlogbeat

Для безпечного моделювання інциденту зараження системи без ризику для лабораторного стенду було використано стандартний тестовий файл EICAR (European Institute for Computer Antivirus Research). Цей файл містить специфічний рядок ASCII-символів, який усі антивірусні продукти розпізнають як вірус, що дозволяє перевірити реакцію системи захисту. В ході експерименту на робочому столі контролера домену було створено текстовий файл, що містив сигнатуру EICAR.[25]



Рисунок 3.13 — Створення тестового файлу EICAR

Вбудований засіб захисту Windows Defender миттєво ідентифікував загрозу, класифікував її як «Virus:DOS/EICAR_Test_File» та виконав автоматичну дію з ізоляції файлу (карантин/видалення).



Рисунок 3.14 — Ідентифікація загрози у Windows Defender

Система Graylog успішно отримала та обробила повідомлення про інцидент, зареєструвавши подію з ідентифікатором Event ID 1116 («The antimalware platform detected malware or other potentially unwanted software»). Аналіз лог-файлу в інтерфейсі SIEM-системи дозволив отримати вичерпну інформацію про інцидент: назву виявленої загрози (ThreatName), повний шлях до інфікованого файлу (Path), ступінь небезпеки (Severity) та вжиті заходи.

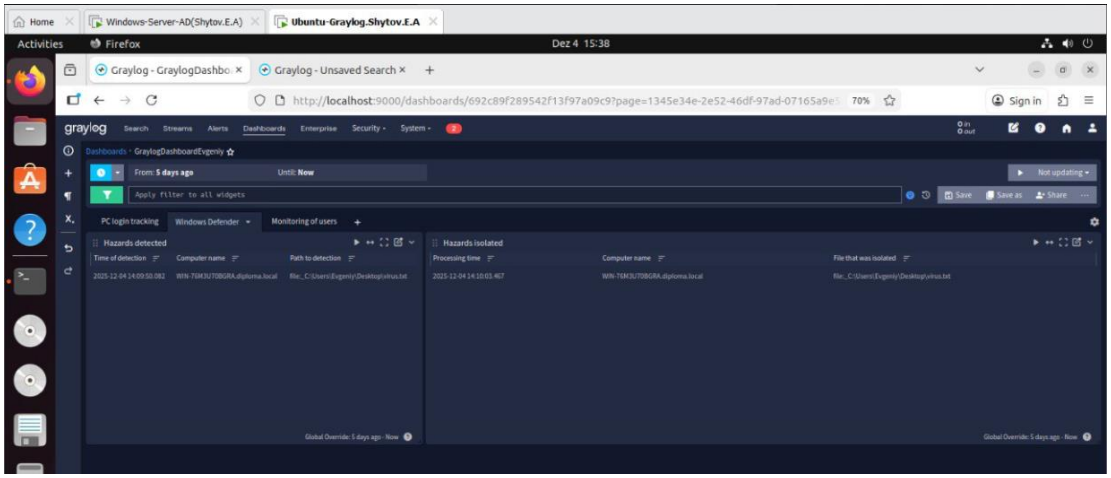


Рисунок 3.15 — Вивід актуального логу у таблицю Graylog

Інформація про виявлені загрози була виведена на головний дашборд безпеки у вигляді окремого індикатора та деталізованої таблиці. Це підтверджує, що розроблена система здатна виконувати функції комплексного центру моніторингу безпеки (SOC), надаючи адміністратору повну картину стану захищеності інфраструктури не лише на рівні облікових записів, а й на рівні файлової системи та захисту від шкідливого коду.[26]

3.2.5. Реалізація системи автоматичного реагування та оповіщення (Alerting)

Невід'ємною складовою будь-якої сучасної SIEM-системи є підсистема автоматичного реагування на інциденти. Покладання виключно на візуальний моніторинг дашбордів є неефективним через вплив людського фактора та неможливість забезпечення цілодобового спостереження за екраном оператора. З метою мінімізації часу реакції на критичні події (Time to Respond, TTR) у розгорнутій системі було реалізовано механізм миттєвих оповіщень.

Як канал доставки повідомлень було обрано платформу корпоративного месенджера Discord. Інтеграція між сервером Graylog та месенджером була реалізована з використанням технології Webhook. На стороні Discord було згенеровано спеціалізовану URL-адресу (endpoint), яка дозволяє зовнішнім системам відправляти дані за допомогою HTTP POST-запитів у форматі JSON. Цей підхід забезпечує надійну доставку повідомлень без необхідності встановлення додаткового клієнтського програмного забезпечення на сервер моніторингу.[27]

Логіка виявлення інцидентів у Graylog базується на створенні правил кореляції (Event Definitions). Для тестування системи оповіщення було створено правило для реагування на критичну подію блокування облікового запису. У налаштуваннях правила визначено умову: поява у вхідному потоці хоча б одного повідомлення з полем event_id, що дорівнює 4740. До цього правила було прив'язано профіль сповіщення (Notification) типу «Discord / Slack».

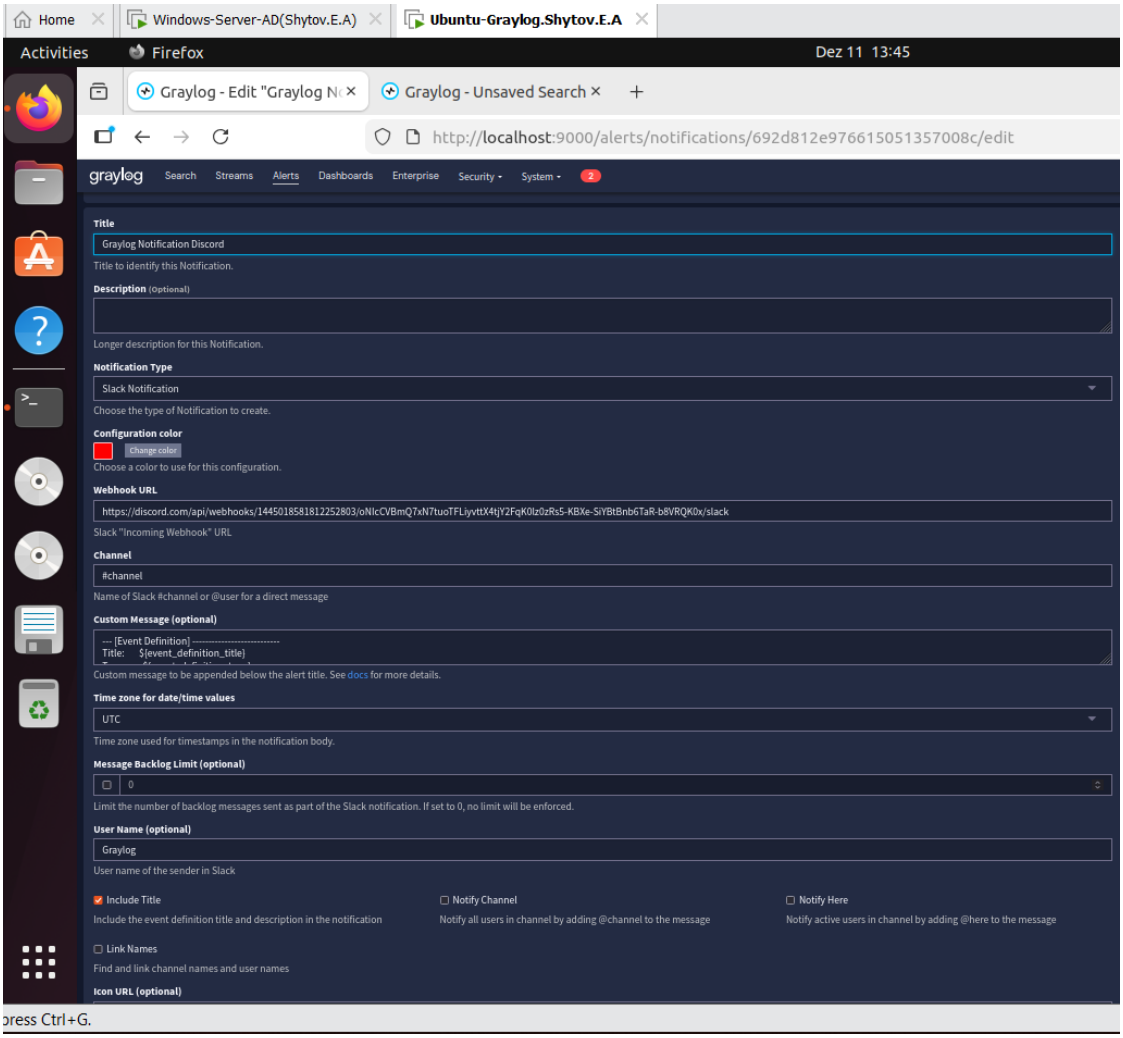


Рисунок 3.16 — Створення сповіщення типу «Discord / Slack».

Було розроблено кастомізований шаблон повідомлення, який автоматично підставляє у текст динамічні поля з логу: ім'я заблокованого користувача, час інциденту та джерело події.

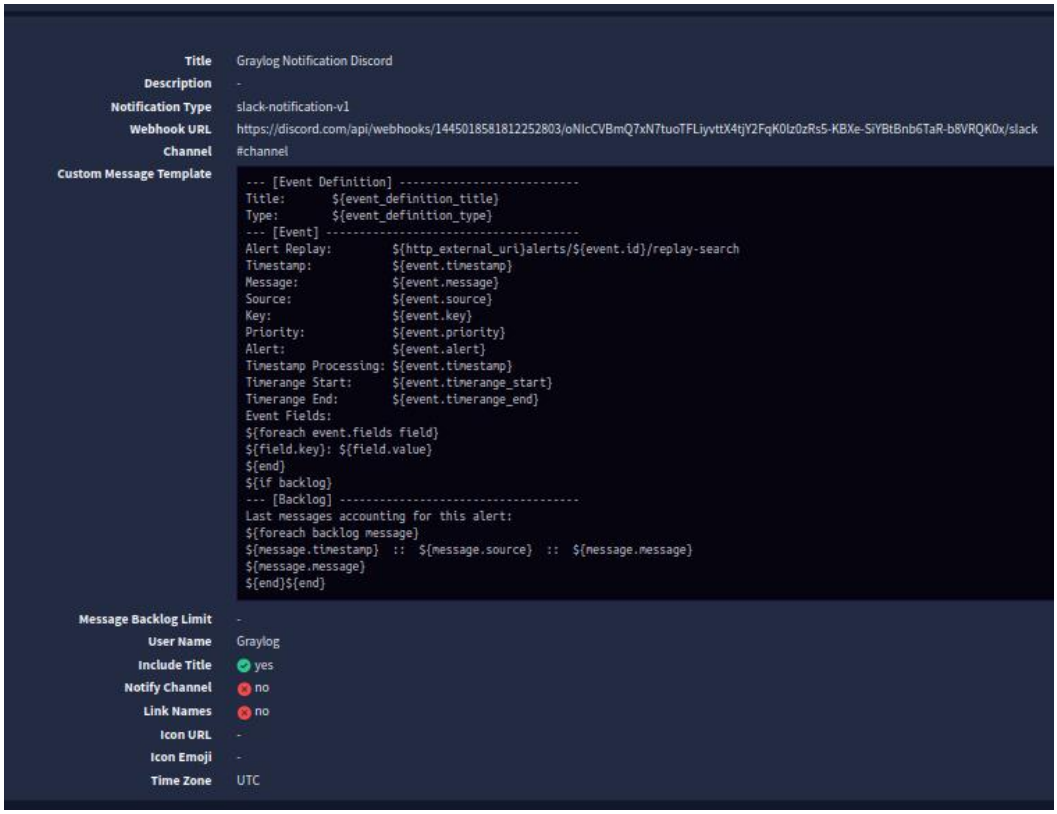


Рисунок 3.17 — Кастомізований шаблон повідомлення

Експериментальна перевірка підтвердила працездатність механізму: безпосередньо після фіксації блокування тестового облікового запису (описаного у пункті 3.2.1) у відповідний канал Discord надійшло структуроване повідомлення про інцидент.

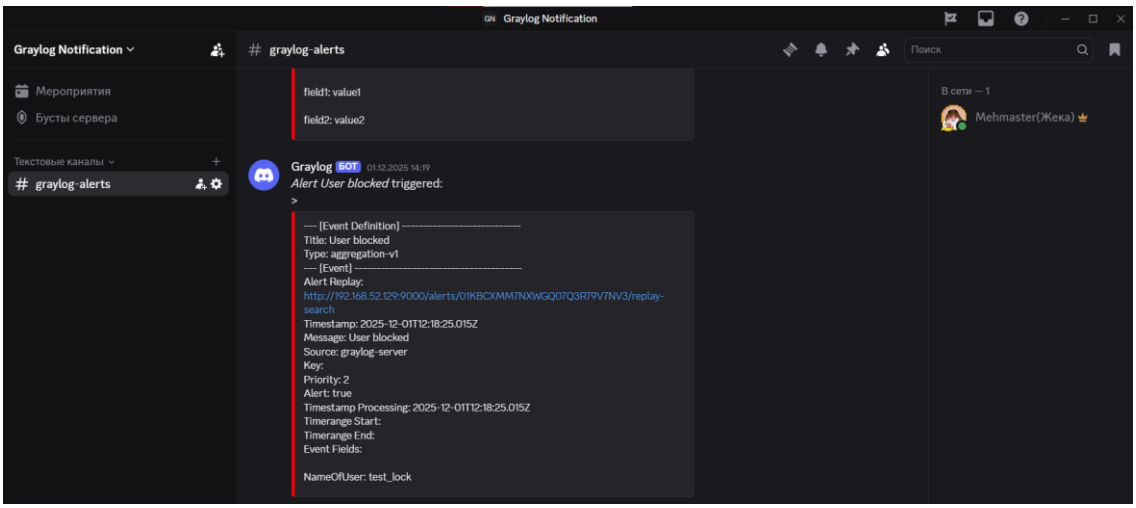


Рисунок 3.18 — Приклад автоматичного сповіщення про інцидент безпеки у месенджері Discord(User Blocked)

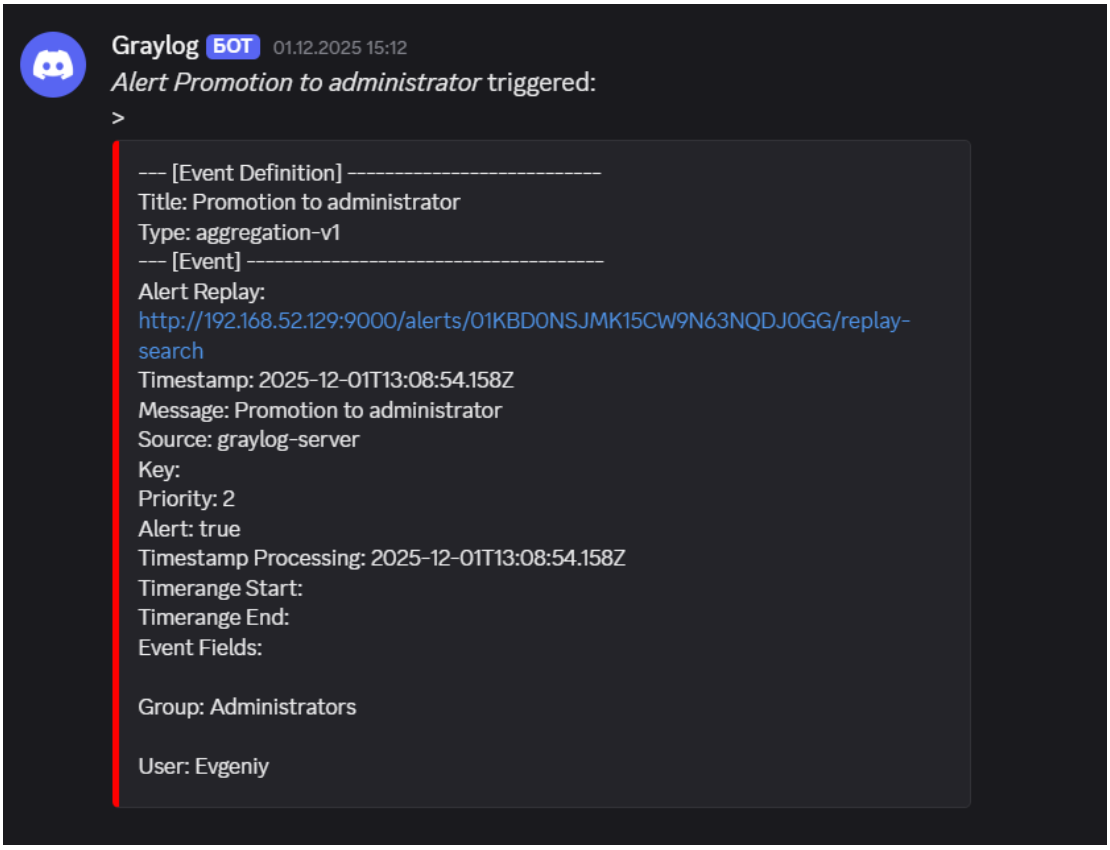


Рисунок 3.19 — Приклад автоматичного сповіщення про інцидент безпеки у месенджері Discord(Promotion to administrator)

Це дозволяє адміністратору безпеки миттєво дізнатися про атаку, навіть не знаходячись за робочим місцем, що значно підвищує загальний рівень захищеності інформаційної системи.

3.3 Візуалізація даних та побудова комплексної аналітичної панелі (Dashboard)

Для забезпечення цілісного бачення стану інформаційної безпеки та реалізації концепції «Single Pane of Glass» (управління через єдине вікно), всі налаштовані метрики та потоки подій були агреговані на централізованій інформаційній панелі (Dashboard).

З метою уникнення перенасичення інформацією та спрощення роботи оператора, архітектура дашборда була структурована за тематичними вкладками, кожна з яких відповідає за окремий вектор моніторингу.

1. Вкладка «PC login tracking» (Моніторинг аутентифікації) Дана секція призначена для загального огляду активності входів у систему. Ключовим елементом візуалізації є кругова діаграма (Pie Chart), що демонструє співвідношення успішних (Event ID 4624) та невдалих (Event ID 4625) спроб входу. Така візуалізація дозволяє миттєво оцінити загальний "фон" безпеки: різке зростання сектору невдалих входів свідчить про початок атаки. Поруч розміщено гістограму розподілу помилок аутентифікації у часі, що дозволяє виявити пікові навантаження, характерні для роботи автоматизованих брутфорс-скриптів.

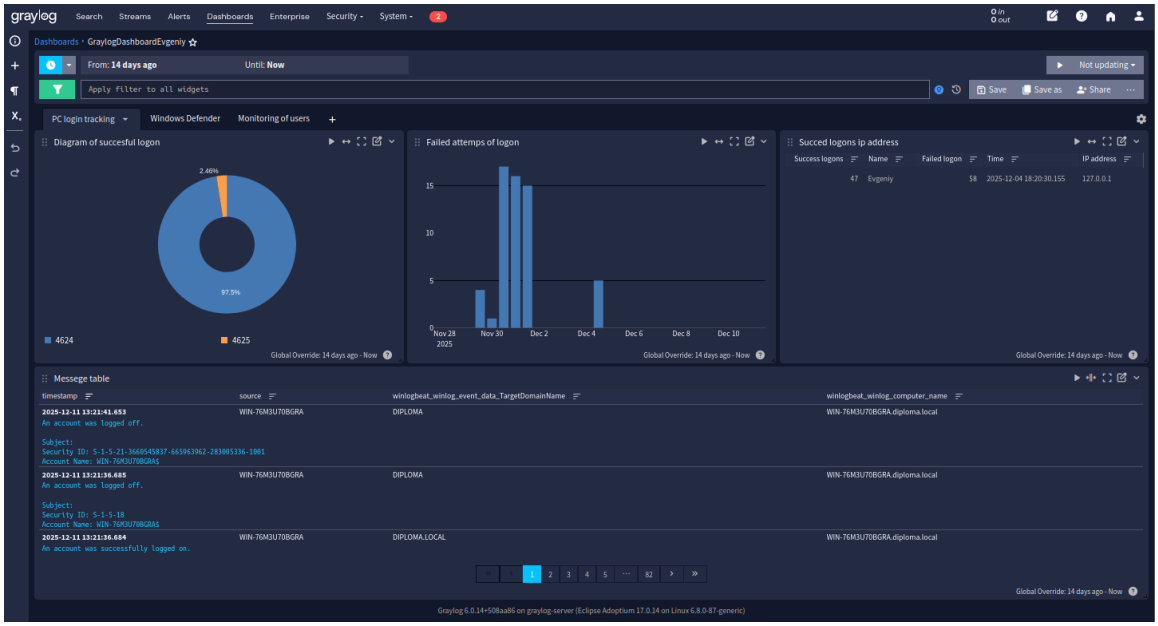


Рисунок 3.20 — Візуалізація статистики аутентифікації та спроб несанкціонованого доступу

2. Вкладка «Monitoring of users» (Контроль облікових записів) Ця вкладка фокусується на аудиті життєвого циклу користувачів та привілейованих груп. Реалізовано табличні віджети, які в режимі реального часу відображають:

New users created info: Деталізований список новостворених користувачів із зазначенням часу та ініціатора дії.

Users promotion info: Критично важливий віджет для відстеження ескалації привілеїв (додавання користувачів до груп адміністраторів).

Blocked users: Індикатор тривоги, що підсвічує імена заблокованих системою користувачів (наприклад, test_lock), що є прямим свідченням відбитої атаки.

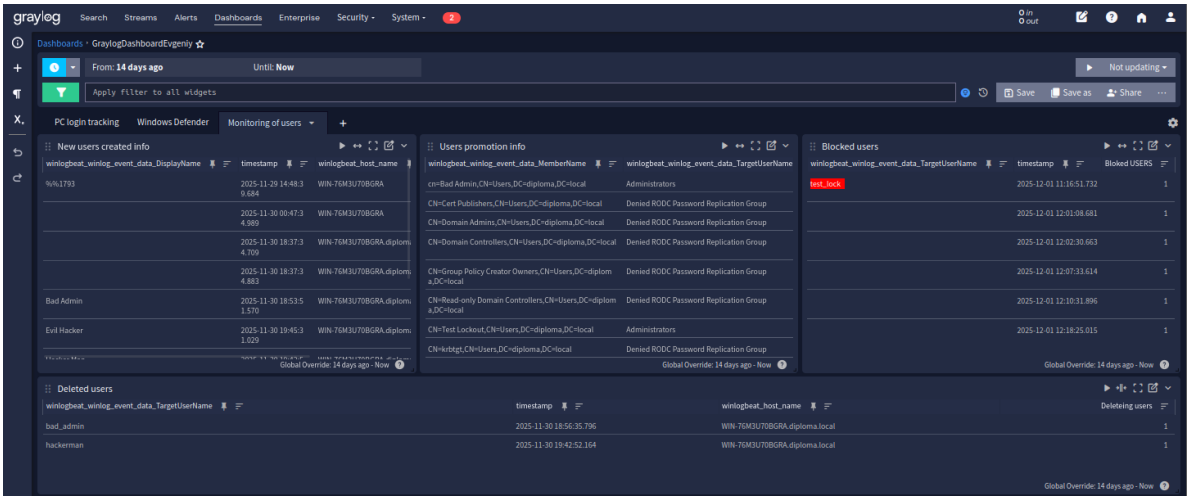


Рисунок 3.21 — Панель контролю змін облікових записів та блокувань

3. Вкладка «Windows Defender» (Антивірусний захист) Окрема секція присвячена подіям, отриманим від підсистеми захисту від шкідливого ПЗ. Тут агрегуються дані про виявлені загрози (Hazards detected) та статус їх знешкодження (Hazards isolated). Таблиці містять інформацію про тип загрози, інфікований об'єкт (файл) та хост, на якому відбувся інцидент. Це дозволяє адміністратору швидко ідентифікувати джерело зараження в мережі.

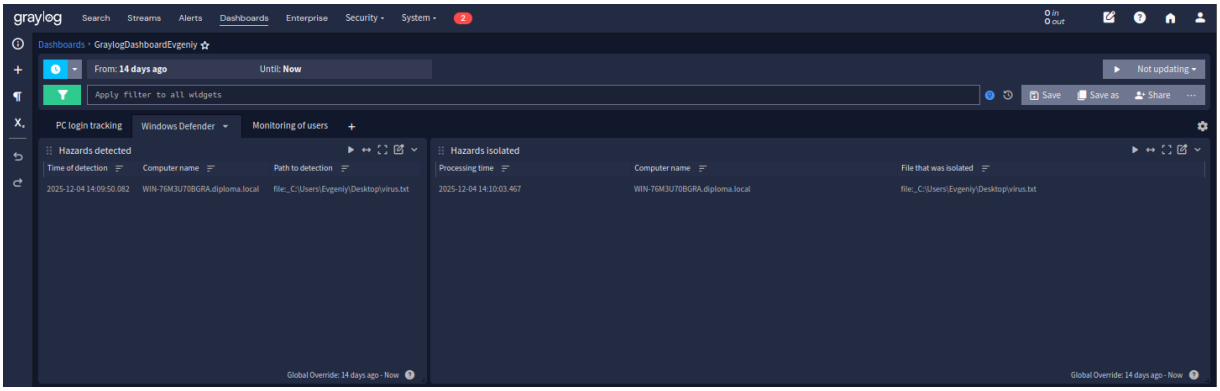


Рисунок 3.22 — Візуалізація подій антивірусного захисту

Створена аналітична панель дозволяє скоротити час виявлення інцидентів (Time to Detect) з десятків хвилин (при ручному аналізі журналів) до кількох секунд, надаючи адміністратору готову аналітичну картину в зрозумілому графічному форматі.

3.4 Оцінка ефективності впровадженої системи

Для комплексної оцінки ефективності розробленої системи моніторингу було проведено порівняльний аналіз двох підходів до забезпечення інформаційної безпеки: використання штатних засобів операційної системи Windows та використання впровадженого комплексу Graylog. Порівняння проводилося на основі реальних сценаріїв атак, реалізованих у ході експериментального дослідження, з фокусом на швидкості виявлення загроз та зручності роботи адміністратора.

Перший сценарій передбачав виявлення атаки підбору пароля. При використанні традиційного підходу адміністратор змушений самостійно відкривати оснастку Event Viewer, застосовувати фільтри для пошуку подій з ідентифікатором 4625 та вручну аналізувати велику кількість записів для виявлення аномалій. Цей процес є трудомістким і займає від 10 до 15 хвилин, причому лише за умови, що адміністратор вирішив перевірити журнали саме в момент атаки. Натомість система Graylog виконує цю роботу автоматично, будуючи графіки невдалих входів у реальному часі, а при блокуванні облікового запису миттєво надсилає сповіщення у Discord, скорочуючи час реакції до кількох секунд.

Другий сценарій стосувався виявлення шкідливого програмного забезпечення. У ручному режимі події антивірусу записуються в окремий журнал, який перевіряється адміністраторами нерегулярно або під час планового аудиту, що може призвести до значної затримки у виявленні інциденту, іноді до 24 годин. Впроваджена система Graylog дозволяє виводити інформацію про виявлені загрози на головний дашборд миттєво, що дає змогу адміністратору побачити інцидент одразу після його виникнення.[28] Для забезпечення достовірності отриманих результатів кожен сценарій атаки було відтворено тричі. Узагальнені результати порівняльного аналізу ефективності наведені в таблиці 3.1.

Таблиця 3.1 Аналіз покращення продуктивності

Показник	***Ручний моніторинг (Event Viewer)***	***Система Graylog***	***Результат впро-ваджження***	***Кількість повторів***
Швидкість ви-явлення атаки	Від 15 хв до 24 годин	Менше 10 се-кунд	Миттєве ре-агування	3
Режим роботи	Реактивний (аналіз мину-лого)	Проактивний (реальний час)	Попере-дження інци-дентів	-
Ризик пропу-стити загрозу	Високий (люд-ський фактор, втома)	Низький (авто-матизація)	Виключення помилок опе-ратора	-
Зручність сприйняття	Тисячі рядків тексту	Графіки та діаграми	Швидке прий-няття рішень	-

Впровадження системи Graylog дозволило здійснити перехід від періодичного ручного перегляду журналів до автоматизованого моніторингу в режимі реального часу. Час виявлення критичних інцидентів скоротився з десятків хвилин до кількох секунд, а інтеграція з месенджером Discord гарантує, що адміністратор дізнається про атаку миттєво, навіть не перебуваючи за робочим місцем, що значно підвищує загальний рівень захищеності інформаційної системи.

ВИСНОВКИ

У третьому розділі магістерської роботи проведено комплексне експериментальне дослідження ефективності розробленої системи моніторингу шляхом моделювання реальних сценаріїв кібератак відповідно до методики Cyber Kill Chain.

Практична верифікація підтвердила здатність комплексу на базі Graylog успішно детектувати широкий спектр загроз, включаючи атаки типу Brute Force, спроби закріплення в системі через створення нелегітимних облікових записів, ескалацію привілеїв до рівня адміністратора, а також активність шкідливого програмного забезпечення. Налаштовані правила кореляції забезпечили точну фіксацію критичних подій безпеки та їх детальну візуалізацію на створеній комплексній інформаційній панелі, що дозволило реалізувати концепцію управління через єдине вікно. Важливим результатом роботи стала успішна реалізація підсистеми автоматичного оповіщення через інтеграцію з платформою Discord, яка гарантує миттєве інформування адміністраторів про критичні інциденти незалежно від їхнього місцеперебування. Проведений порівняльний аналіз ефективності, що базувався на серії тестових прогонів, продемонстрував кардинальну перевагу впровадженого рішення над традиційними методами ручного аудиту журналів Windows: час виявлення загроз скоротився з десятків хвилин або годин до кількох секунд.

Варто зазначити певні обмеження проведеного експерименту: дослідження виконувалося на віртуальному лабораторному стенді з обмеженою кількістю хостів та відсутністю реального «шумового» трафіку користувачів. Також використовувався лише один контролер домену, що не повною мірою відображає складність реплікації у розподілених корпоративних мережах. Напрямками подальших досліджень є тестування системи під високим навантаженням (High Load) та налаштування кластеризації Graylog для забезпечення відмовостійкості у мультидоменному середовищі.Таким чином, експериментальне дослідження довело, що розгорнута система дозволяє здійснити перехід від реактивної моделі безпеки до проактивної, забезпечуючи надійний захист та контроль цілісності інфраструктури Active Directory у режимі реального часу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 12.12.2025).
2. Гнатюк С. О., Корченко О. Г. Кібербезпека: підручник. Київ : НАУ, 2020. 320 с.
3. Діагностика та журнали. AlexHost. URL: https://alexhost.com/uk/faq/diagnostyka-ta-zhurnaly/ (дата звернення: 30.01.2025).
4. Логування: поняття, вимоги, рівні. QATestLab. URL: https://training.qatestlab.com/blog/technical-articles/logging-in-concepts-requirements-levels/ (дата звернення: 30.01.2025).
5. The Importance of Logging and Traffic Monitoring for Information Security. SANS Institute. URL: https://www.sans.org/white-papers/1379/ (дата звернення: 30.01.2025).
6. SIEM: Security Information & Event Management Explained. Splunk. URL: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html (дата звернення: 30.01.2025).
7. Graylog Documentation. The Centralized Log Management Solution. URL: https://go2docs.graylog.org/6-0/home.htm (дата звернення: 20.11.2024).
8. What is graylog? Graylog Docs. URL: https://go2docs.graylog.org/5-0/what_is_graylog/what_is_graylog.htm (дата звернення: 30.01.2025).

9. What Is Splunk & What Does It Do? Splunk. URL: https://www.splunk.com/en_us/blog/learn/what-splunk-does.html (дата звернення: 30.01.2025).

10. Elastic Stack (ELK) Overview. Elastic. URL: https://www.elastic.co/elastic-stack (дата звернення: 10.11.2024).

11. What is ELK Stack? AWS. URL: https://aws.amazon.com/what-is/elk-stack/ (дата звернення: 30.01.2025).

12. What is ElasticSearch? Elastic. URL: https://www.elastic.co/elasticsearch (дата звернення: 30.01.2024).

13. Splunk vs ELK stack vs Graylog vs Loki. Reddit Thread. URL: https://www.reddit.com/r/homelab/comments/wnsmf8/splunk_vs_elk_stack_vs_graylog_vs_loki/ (дата звернення: 30.01.2025).

14. Audit Policy Recommendations. Microsoft Learn. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations (дата звернення: 30.01.2025).

15. How To Configure Group Policies to Set Security for System Services. Microsoft Learn. URL: https://learn.microsoft.com/en-us/troubleshoot/windows-server/group-policy/configure-group-policies-set-security (дата звернення: 30.01.2025).

16. Основні загрози для Active Directory. Oberig IT. URL: https://oberig-it.com/ru/stati/osteregajtes-vot-nekotorye-osnovnye-ugrozy-active-directory-skryvayushhiesya-v-vashej-seti/ (дата звернення 31.01.2025).

17. Common Active Directory Attacks and Detection Techniques. Medium. URL: https://medium.com/@araman99/common-active-directory-attacks-and-detection-techniques-193411836d93 (дата звернення 31.01.2025).

18. Загрози інформаційної безпеки. Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B8_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8 (дата звернення: 31.01.2025).

19. VMware Workstation Pro Documentation. VMware by Broadcom. URL: https://docs.vmware.com/en/VMware-Workstation-Pro/index.html (дата звернення: 15.11.2024).

20. Ubuntu Server Documentation. Canonical Ltd. URL: https://ubuntu.com/server/docs (дата звернення: 20.11.2024)

21. MongoDB Manual. The database for modern applications. URL: https://www.mongodb.com/docs/manual/ (дата звернення: 25.11.2024).

22. OpenSearch Documentation. Scalable, flexible, and extensible open-source software suite. URL: https://opensearch.org/docs/latest/ (дата звернення: 25.11.2024).

23. Winlogbeat Overview. Lightweight Shipper for Windows Event Logs. Elastic. URL: https://www.elastic.co/guide/en/beats/winlogbeat/current/winlogbeat-overview.html (дата звернення: 28.11.2024).

24. The Cyber Kill Chain. Lockheed Martin. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата звернення: 01.12.2024).

25. EICAR Test File. European Institute for Computer Antivirus Research. URL: https://www.eicar.org/download-anti-malware-testfile/ (дата звернення: 04.12.2024).

26. Windows Defender Antivirus events. Microsoft Learn. URL: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus (дата звернення: 04.12.2024).

27. Discord Webhook API Documentation. Discord Developer Portal. URL: https://discord.com/developers/docs/resources/webhook (дата звернення: 05.12.2024).

28. Security Awareness and Log Management for Security Analysts. Graylog Blog. URL: https://graylog.org/post/security-awareness-and-log-management-for-security-analysts/ (дата звернення: 30.01.2025).

ДОДАТКИ

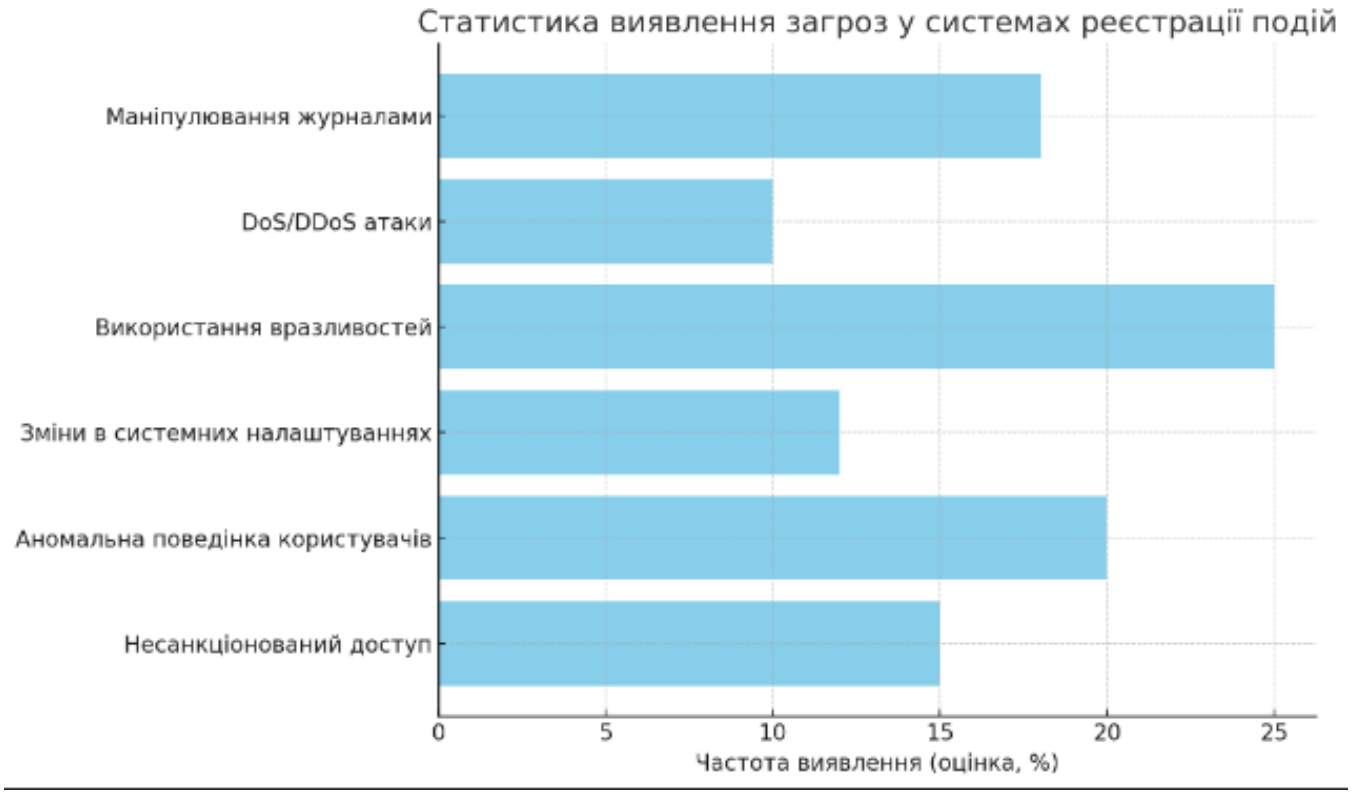
Додаток А

Таблиця порівняння програмного забезпечення від різних виробників

Характеристика	**Graylog**	**Splunk**	**ELK Stack**
Ліцензія	Відкритий код	Комерційний	Відкритий код
Масштабованість	Висока	Дуже висока	Висока
Підтримка форматів логів	Syslog, GELF, JSON	Syslog, JSON	JSON, Syslog
Інструменти візуалізації	Вбудовані	Вбудовані	Kibana
Вартість	Безкоштовно	Висока	Безкоштовно

Додаток Б

Графік виявлення загроз у системах реєстрації подій



Додаток В

Таблиця порівняння результативності різних типів моніторингу

Показник	***Ручний моніторинг (Event Viewer)***	***Система Graylog***	***Результат впро-ваджження***	***Кількість повторів***
Швидкість ви-явлення атаки	Від 15 хв до 24 годин	Менше 10 се-кунд	Миттєве ре-агування	3
Режим роботи	Реактивний (аналіз мину-лого)	Проактивний (реальний час)	Попере-дження інци-дентів	-
Ризик пропу-стити загрозу	Високий (люд-ський фактор, втома)	Низький (авто-матизація)	Виключення помилок опе-ратора	-
Зручність сприйняття	Тисячі рядків тексту	Графіки та діаграми	Швидке прий-няття рішень	-

Додаток Г

Схема взаємодії компонентів Elastic Stack

