

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

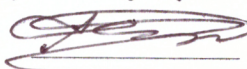
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології побудови системи поглибленого моніторингу захищеної віртуалізованої ІТ-інфраструктури підприємства»

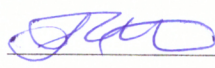
Виконав студент 2-го курсу групи КБм-23-1
спеціальності 125 «Кібербезпека та захист інформації»

 Дмитро Добровольський

Керівник, завідувач кафедри КІ та КБ, к.т.н., доцент

 Андрій Єфіменко

Рецензент, доцент кафедри КІ та КБ, к. пед. н., доцент

 Олена Головня

Житомир – 2024

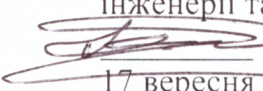
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

17 вересня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну магістра

Студент: Добровольський Дмитро Вадимович

Тема роботи: «Методи та технології побудови системи поглибленого моніторингу захищеної віртуалізованої IT-інфраструктури підприємства»

затверджена Наказом університету від 17 вересня 2024 р. № 479/с

Термін здачі студентом закінченої роботи 09 грудня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єктом дослідження є процес побудови підсистеми поглибленого моніторингу захищеної віртуалізованої IT-інфраструктури підприємства. Предметом дослідження є методи та технології побудови системи поглибленого моніторингу захищеної віртуалізованої IT-інфраструктури підприємства, що забезпечують збір, обробку та аналіз подій безпеки для виявлення потенційних загроз і вразливостей.

Обладнання та програмне забезпечення:

1. Віддалений сервер з встановленим гіпервізором Proxmox VE.
2. Операційні системи Ubuntu 22.04 LTS, Ubuntu 24.04, Debian 12.8.
3. Маршрутизатор MikroTik CHR.
4. Платформа для централізованого збору, оброблення та аналізу журналів подій (логів) з різних джерел у реальному часі Graylog.
5. Агент Graylog Sidecar.
6. Месенджери Discord і MS Teams.
7. Платформи VirusTotal, Shodan.
8. Клієнт Wireguard VPN.

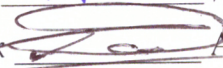
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ігор Фальковський	17.09.2024	6.10.2024
2	Ігор Фальковський	7.10.2024	3.11.2024
3	Ігор Фальковський	4.11.2024	25.11.2024

Студент  Дмитро Добровольський
Керівник  Андрій Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	20.09.2024 – 02.10.2024	
2	Написання вступної частини кваліфікаційної роботи	02.10.2024 – 05.11.2024	
3	Аналіз основних теоретичних відомостей	05.10.2024 – 15.10.2024	
4	Формування вимог та технічного завдання	15.10.2024 – 21.10.2024	
5	Вибір необхідних технологій	21.10.2024 – 25.10.2024	
6	Створення та налаштування системи поглибленого моніторингу	25.10.2024 – 01.11.2024	
7	Тестування системи на відповідність	01.11.2024 – 11.11.2024	
9	Написання висновків	22.11.2024 – 26.11.2024	
10	Оформлення кваліфікаційної роботи	26.11.2024 – 20.12.2024	
11	Захист	25.12.2024	

Студент  Дмитро Добровольський
Керівник  Андрій Єфіменко

АНОТАЦІЯ

Пояснювальна записку містить: 104 сторінки текстової частини, 66 рисунків, 5 таблиці та 27 джерел.

Метою роботи є розробка та впровадження ефективної системи поглибленого моніторингу захищеної віртуалізованої ІТ-інфраструктури підприємства. Робота націлена на створення комплексного підходу до забезпечення безпеки, що включає централізований збір, обробку та аналіз логів, а також моніторинг подій у реальному часі для виявлення та усунення потенційних загроз і вразливостей.

В даній роботі розглянуто використання сучасних технологій віртуалізації у побудові захищених віддалених інформаційних систем. У практичній частині була побудована захищена віддалена інформаційна система.

Ключові слова: ГІПЕРВІЗОР, ВІДДАЛЕНІ СИСТЕМИ, ВІРТУАЛІЗАЦІЯ, VPN, ІНСТРУМЕНТ ЦЕНТРАЛІЗОВАНОГО ЗБОРУ, АНАЛІЗУ ТА УПРАВЛІННЯ ЖУРНАЛАМИ.

ANNOTATION

The explanatory note contains: 104 pages of text, 66 figures, 5 tables and 27 sources.

The aim of the work is to develop and implement an effective system for in-depth monitoring of the enterprise's protected virtualized IT infrastructure. The work is aimed at creating a comprehensive approach to ensuring security, which includes centralized collection, processing and analysis of logs, as well as real-time event monitoring to identify and eliminate potential threats and vulnerabilities.

This paper considers the use of modern virtualization technologies in building secure remote information systems. In the practical part, a secure remote information system was built.

Keywords: HYPERVISOR, REMOTE SYSTEMS, VIRTUALIZATION, VPN, CENTRALIZED LOG COLLECTION, ANALYSIS AND MANAGEMENT TOOL.

ЗМІСТ

ВСТУП.....	11
РОЗДІЛ 1 МЕТОДИ ТА ТЕХНОЛОГІЇ ПОБУДОВИ СИСТЕМ ПОГЛИБЛЕНОГО МОНІТОРИНГУ ЗАХИЩЕНОЇ ВІРТУАЛІЗОВАНОЇ ІТ-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА	13
1.1 Інформаційна система та її компоненти в контексті ІТ-інфраструктури.....	13
1.2 Безпека та контроль ІТ-інфраструктури підприємства	18
1.3 Аналіз технологій та рішень систем віртуалізації, віддалених серверів, SIEM-систем та їх використання в ІТ-інфраструктурі	23
1.4 Особливості функціонування інформаційних систем в умовах військового стану	36
1.5 Постановка технічного завдання на розробку системи поглибленого моніторингу	39
РОЗДІЛ 2. ПРОЄКТУВАННЯ СИСТЕМИ ПОГЛИБЛЕНОГО МОНІТОРИНГУ ЗАХИЩЕНОЇ ВІРТУАЛІЗОВАНОЇ ІТ-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА	43
2.1 Методи та технології побудови системи поглибленого моніторингу .	43
2.2 Аналіз та вибір програмних рішень для побудови системи поглибленого моніторингу	53
2.3 Характеристика обраних технологій для побудови системи поглибленого моніторингу	61
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ ПОГЛИБЛЕНОГО МОНІТОРИНГУ ЗАХИЩЕНОЇ ВІРТУАЛІЗОВАНОЇ ІТ-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА НА ОСНОВІ GRAYLOG, MİKROTIK TA PROXMOX VE .	66
3.1 Реалізація базової ІТ-інфраструктури для моделювання поглибленої системи моніторингу.....	66
3.2 Реалізація системи централізованого збору, обробки та аналізу логів у віртуалізованій ІТ-інфраструктурі.....	69
3.3 Налаштування Graylog для роботи з віддаленим сервером Proxmox VE	81
3.4 Створення механізму візуалізації даних та тестування поглибленої системи моніторингу на відповідність.....	93
ВИСНОВКИ.....	97
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	100
ДОДАТКИ.....	104

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

MS – Microsoft

AD – Active Directory

VM – Virtual Machine

SIEM – Security information and event management

DHCP - Dynamic Host Configuration Protocol

OU – Organization Unit

WS – Work Station

ІС – Інформаційна система

ВСТУП

Захищена мережа на базі сучасних технологій, таких як віддалені сервери, системи віртуалізації та системи SIEM, є надзвичайно важливою для будь-якої компанії або організації, особливо в умовах військового стану. Ці технології дозволяють зберігати та обробляти конфіденційну інформацію, забезпечуючи надійний контроль доступу, аутентифікацію, авторизацію та моніторинг активностей у мережі. В умовах підвищених загроз і кібератак, які часто супроводжують військові конфлікти, побудова захищеної мережі на основі цих технологій є ключовим елементом для зменшення ризиків витоку даних та несанкціонованого доступу до критично важливої інформації.

Метою кваліфікаційної роботи є розробка та впровадження ефективної системи поглибленого моніторингу захищеної віртуалізованої ІТ-інфраструктури підприємства. Робота націлена на створення комплексного підходу до забезпечення безпеки, що включає централізований збір, обробку та аналіз логів, а також моніторинг подій у реальному часі для виявлення та усунення потенційних загроз і вразливостей.

Об'єктом дослідження є процес побудови підсистеми поглибленого моніторингу захищеної віртуалізованої ІТ-інфраструктури підприємства.

Предметом дослідження є методи та технології побудови системи поглибленого моніторингу захищеної віртуалізованої ІТ-інфраструктури підприємства, що забезпечують збір, обробку та аналіз подій безпеки для виявлення потенційних загроз і вразливостей.

Для реалізації проєкту та досягнення поставленої мети передбачимо розв'язання наступних завдань:

- Аналіз сучасних інформаційних систем, ключових технологій моніторингу та безпеки, а також формулювання технічного завдання на розробку захищеної ІТ-інфраструктури.

- Постановка цілей і задач для розробки єдиної системи поглибленого моніторингу.

- Аналіз та вибір програмних і апаратних рішень для побудови системи поглибленого моніторингу.
- Огляд і деталізація обраних технологій для впровадження у захищену IT-інфраструктуру.
- Реалізація базової IT-інфраструктури для моделювання системи поглибленого моніторингу.
- Впровадження систем централізованого збору, обробки та аналізу логів у захищеній віртуалізованій IT-інфраструктурі.
- Налаштування системи централізованого моніторингу для взаємодії з віртуалізованими серверами.
- Створення механізму візуалізації даних та проведення тестування системи поглибленого моніторингу на відповідність технічним вимогам та надійність.

Створення механізму візуалізації даних та проведення тестування системи поглибленого моніторингу на відповідність технічним вимогам та надійність. У процесі виконання кваліфікаційної роботи було розроблено проект захищеної інформаційної системи, була побудована інформаційна система і були проведені налаштування інформаційної системи. Створена мережа була протестована на відповідність вимогам щодо працездатності та захищеності в сучасних умовах.

РОЗДІЛ 1 МЕТОДИ ТА ТЕХНОЛОГІЇ ПОБУДОВИ СИСТЕМ ПОГЛИБЛЕНОГО МОНІТОРИНГУ ЗАХИЩЕНОЇ ВІРТУАЛІЗОВАНОЇ ІТ-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

1.1 Інформаційна система та її компоненти в контексті ІТ-інфраструктури

У межах цієї роботи поняття інформаційної системи розглядається в контексті ІТ-інфраструктури підприємства. Іншими словами, ІТ-інфраструктура розуміється не просто як набір апаратних і програмних компонентів, а як стратегічно організована складова інтегрованої інформаційної системи, що дає змогу підприємству ефективно функціонувати, взаємодіяти з зовнішнім середовищем і приймати обґрунтовані управлінські рішення.

ІТ-інфраструктура охоплює все різноманіття технічних елементів — від серверів, мережевого обладнання й телекомунікаційних каналів до програмного забезпечення та хмарних сервісів, — які слугують «фундаментом» для роботи інформаційної системи. Завдяки цій інфраструктурі підприємство може збирати, зберігати й обробляти великі масиви даних, а також своєчасно поширювати результуючу інформацію як усередині організації, так і назовні (наприклад, клієнтам або постачальникам).

З іншого боку, інформаційна система (ІС) втілює «логіку» та «функції» обробки даних і перетворення їх на корисну інформацію чи цифрові продукти. Підприємство може реалізовувати складні бізнес-процеси та приймати стратегічні рішення завдяки взаємодії ІТ-інфраструктури з компонентами ІС — програмними модулями, базами даних, вебсервісами, системами аналітики та іншими елементами, які впорядковують управлінську діяльність та оптимізують ланцюги поставок.

Отже, ІТ-інфраструктура й інформаційна система тісно взаємопов'язані: добре спроектована, масштабована та керована інфраструктура дозволяє інформаційним системам повноцінно функціонувати, задовольняючи потреби підприєм-

ства у динамічних і конкурентних ринкових умовах. У цій роботі докладно розглянуто обидва поняття у взаємозв'язку: як саме ІТ-інфраструктура формує технологічне підґрунтя для інформаційних систем, і які вимоги висувають ці системи до інфраструктури, щоб забезпечити необхідну продуктивність, надійність і безпеку.

Інформація про поняття інформаційна система отримана за посиланням [\[1\]](#).

Інформаційна система, інтегрований набір компонентів для збору, зберігання й обробки даних, а також для надання інформації, знань і цифрових продуктів. Підприємства та інші організації покладаються на інформаційні системи, щоб здійснювати та керувати своїми операціями, взаємодіяти зі своїми клієнтами та постачальниками та конкурувати на ринку. Інформаційні системи використовуються для управління міжорганізаційними ланцюгами поставок та електронними ринками. Наприклад, корпорації застосовують інформаційні системи для обробки фінансової документації, керування персоналом і залучення потенційних клієнтів через інтернет-рекламу. Багато великих компаній повністю побудовані навколо інформаційних систем. Серед них eBay, переважно аукціонний ринок; Amazon, електронний торговий центр, що розширюється, і постачальник послуг хмарних обчислень; Alibaba, електронний ринок між компаніями; і Google, пошукова компанія, яка отримує більшу частину свого доходу від реклами за ключовими словами під час пошуку в Інтернеті. Державні органи впроваджують інформаційні системи для ефективного надання послуг населенню. Цифрові товари, такі як електронні книги, відеопродукти та програмне забезпечення, а також онлайн-послуги, такі як ігри та соціальні мережі, постачаються разом з інформаційними системами. Люди зазвичай використовують інформаційні системи, що базуються на Інтернеті, для здійснення більшості аспектів свого особистого життя: спілкування, навчання, шопінгу, фінансових операцій та розваг.

У міру того, як протягом тисячоліть були винайдені основні нові технології для запису та обробки інформації, з'явилися нові можливості, і люди отримали повноваження. Винахід друкарського верстата Йоганном Гутенбергом у середині 15-го століття та винахід механічного калькулятора Блезом Паскалем у 17-

му столітті є лише двома прикладами. Ці винаходи призвели до глибокої революції в здатності записувати, обробляти, поширювати та отримувати інформацію та знання. Це, у свою чергу, призвело до ще глибших змін у житті людей, організації бізнесу та людському управлінні.

Першою великомасштабною механічною інформаційною системою був табулятор перепису Германа Холлеріта. Машина Холлеріта, винайдена вчасно для обробки даних перепису населення США 1890 року, стала важливим кроком у автоматизації, а також надихнула на розвиток комп'ютеризованих інформаційних систем.

Одним із перших комп'ютерів, використаних для такої обробки інформації, був UNIVAC I, встановлений у Бюро перепису населення США в 1951 році для адміністративного використання та в General Electric у 1954 році для комерційного використання. Починаючи з кінця 1970-х років, персональні комп'ютери принесли деякі переваги інформаційних систем малим підприємствам і окремим особам. На початку того ж десятиліття Інтернет почав свою експансію як глобальна мережа мереж. У 1991 році Всесвітня павутина, винайдена Тімом Бернерсом-Лі як засіб доступу до взаємопов'язаної інформації, що зберігається на глобально розсіяних комп'ютерах, з'єднаних Інтернетом, почала працювати та стала основною послугою, що надається в мережі. Глобальне проникнення Інтернету та Мережі уможливило доступ до інформації та інших ресурсів і сприяло формуванню стосунків між людьми та організаціями в безпрецедентному масштабі. Розвиток електронної комерції через Інтернет призвів до різкого зростання цифрових міжособистісних комунікацій (через електронну пошту та соціальні мережі), розповсюдження продуктів (програмне забезпечення, музика, електронні книги та фільми) та ділових операцій (купівля, продаж і реклама в Інтернеті). З розповсюдженням у всьому світі смартфонів, планшетів, ноутбуків та інших комп'ютерних мобільних пристроїв, які об'єднані бездротовими мережами зв'язку, інформаційні системи були розширені для підтримки мобільності як природного стану людини.

Оскільки інформаційні системи сприяли більш різноманітній людській діяльності, вони справляли глибокий вплив на суспільство. Ці системи прискорили ритм повсякденного життя, сприяли розвитку та підтримці нових, часто більш вигідних взаємин, трансформували структуру та склад організацій, змінили асортимент споживаних продуктів і вплинули на специфіку трудової діяльності. Інформація та знання стали життєво важливими економічними ресурсами. Проте, разом із новими можливостями, залежність від інформаційних систем принесла нові загрози. Інтенсивні галузеві інновації та наукові дослідження постійно створюють нові можливості, одночасно прагнучи стримувати загрози.

Основні складові інформаційних систем включають апаратне забезпечення, програмне забезпечення, телекомунікаційні засоби, бази даних і сховища інформації, а також людські ресурси й процедурні процеси. Апаратне забезпечення, програмне забезпечення та телекомунікації складають інформаційну технологію (ІТ), яка зараз укорінена в діяльності та управлінні організаціями. Тепер розглянемо можливі компоненти ІС окремо, більш детально.

Приклад можливих компонентів інформаційної системи.

- Комп'ютерне обладнання
- Програмне забезпечення

У сучасному світі навіть найдрібніші підприємства мають або користуються комп'ютерами. Люди можуть володіти кількома комп'ютерами у вигляді смартфонів, планшетів та інших портативних пристроїв. Великі компанії, зазвичай, використовують розподілені комп'ютерні системи, починаючи від потужних серверів з паралельною обробкою даних, розміщених у центрах обробки даних, до розподілених персональних комп'ютерів і мобільних пристроїв, що інтегруються в організаційні інформаційні системи. Датчики стають все більш поширеними в фізичному та біологічному середовищі для збору даних і, у багатьох випадках, для здійснення контролю за допомогою пристроїв, відомих як приводи. Разом з периферійним обладнанням, таким як магнітні або твердотільні накопичувачі, пристрої введення-виведення та телекомунікаційне обладнання, вони складають апаратне забезпечення інформаційних систем. Вартість апаратного забезпечення

постійно та швидко знижується, тоді як швидкість обробки та обсяг пам'яті значно зростають. Цей розвиток відбувається відповідно до закону Мура: потужність мікропроцесорів, які є серцем комп'ютерних пристроїв, подвоюється приблизно кожні 18–24 місяці. Однак розробники звертають увагу на питання використання електроенергії апаратним забезпеченням та його вплив на навколишнє середовище. Все частіше комп'ютерні послуги та послуги зберігання надаються з хмари — з спільних об'єктів, доступ до яких здійснюється через телекомунікаційні мережі.

Комп'ютерне програмне забезпечення поділяється на два великі класи: системне програмне забезпечення та прикладне програмне забезпечення. Основним системним програмним забезпеченням є операційна система. Він керує обладнанням, даними та програмними файлами та іншими системними ресурсами та надає користувачеві засоби керування комп'ютером, як правило, через графічний інтерфейс користувача (GUI). Прикладне програмне забезпечення — це програми, призначені для вирішення конкретних завдань користувачів. Додатки для смартфонів стали звичайним способом доступу людей до інформаційних систем. Інші приклади включають пакети програм загального призначення з електронними таблицями та програмами обробки текстів, а також «вертикальні» програми, які обслуговують певний сегмент галузі, наприклад, програму, яка планує, маршрутизує та відстежує доставку посилок для нічного перевізника. Більші фірми використовують ліцензовані програми, які розробляють і обслуговують спеціалізовані компанії-розробники програмного забезпечення, налаштовуючи їх відповідно до своїх конкретних потреб, а також розробляють інші програми власними силами або на сторонніх підприємствах. Компанії також можуть використовувати програми, які постачаються як програмне забезпечення як послуга (SaaS) з хмари через Інтернет. Власницьке програмне забезпечення, доступне та підтримуване його постачальниками, кидається викликом програмного забезпечення з відкритим кодом, доступного в Інтернеті для безкоштовного використання та модифікації за ліцензією, яка захищає його доступність у майбутньому.

1.2 Безпека та контроль ІТ-інфраструктури підприємства

З інтеграцією інформаційних систем у глобальну мережу Інтернет та їх широким впровадженням у функціонування та адміністрування підприємств, державних установ та повсякденного життя в усьому світі важливість інформаційної безпеки стала першочерговою проблемою.

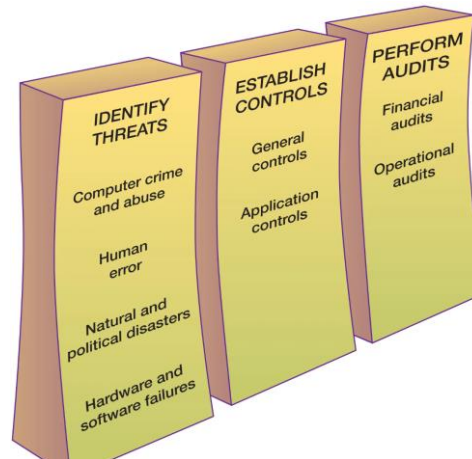


Рисунок 1.1 - Безпека інформаційних систем

У сучасному світі безпека інформаційних систем відіграє важливу роль у забезпеченні цілісності та захисту ресурсів і діяльності цих систем. Більшість організацій у розвинених країнах надійно покладаються на безпеку своїх інформаційних систем. Фактично, структура суспільства в значній мірі залежить від надійності цих систем. Різноманітні інфраструктурні мережі, такі як електропостачання, водопостачання та системи охорони здоров'я, обертаються на них. Інформаційні системи використовуються у важливих галузях, таких як лікарняні відділення і системи керування повітряним рухом. Фінансові установи не можуть допустити повного збою своїх інформаційних систем навіть на короткий період. Системи електронних фінансових трансакцій обробляють величезні суми коштів, які існують у вигляді електронних сигналів або зберігаються на дисках. Інформаційні системи піддаються різним загрозам і вимагають строгого контролю, такого як постійні заходи безпеки та регулярні аудити, щоб гарантувати їхню надійність.

Інформація про безпеку у інформаційній системі отримана за посиланням [\[2,3\]](#).

Незважаючи на те, що випадки комп'ютерних злочинів і зловживань приділяють значну увагу ЗМІ, за оцінками, помилки людини спричиняють більші втрати в роботі інформаційних систем. Стихійні лиха, як землетруси, повені та пожежі, є предметом особливого занепокоєння планування аварійного відновлення, яке є частиною корпоративного плану безперервності бізнесу. Надзвичайна схема також необхідна для покриття збоїв серверів, телекомунікаційних мереж або програмного забезпечення.

Водночас, додатковим джерелом ризику для безперебійної роботи інформаційних систем є протиправні дії з використанням комп'ютерних технологій, що можуть призвести до втрат, порівнянних або й більших за наслідки людських помилок чи стихійних лих.

Комп'ютерні злочини — протиправні дії, основним інструментом яких є комп'ютер. Метою таких кібератак є вандалізм, крадіжка особистої інформації, шпигунство на рівні держави або комерційне шпигунство, диверсія та кібервійни. Деякі з найпоширеніших методів кіберзлочинності включають фішинг та встановлення шкідливих програм, таких як віруси, черв'яки, троянські коні та логічні бомби.

Найпоширеніші методи кіберзлочинності:

- Фішинг
- Комп'ютерні віруси
- Троянській кінь

Фішинг полягає у використанні обману для отримання логінів та інших особистих даних законних користувачів за допомогою фальшивих повідомлень, які намагаються виглядати як від імовірних джерел, таких як банки або державні органи. Після успішної фішингової атаки може наступити крадіжка особистої інформації або зловмисне використання даних користувача.

Комп'ютерні віруси є широко вживаним засобом атаки. Це програмні коди, які можуть виконувати шкідливі дії та розповсюджувати свої копії через інші програми, що призводить до зараження інших комп'ютерних систем. Хробаки,

подібні до вірусів, є повноцінними програмами, що можуть швидко розповсюджуватися через мережу. Через їхню швидкість та обсяг розповсюдження вони можуть завдати значних збитків, спричиняючи переривання роботи системи, крадіжку великих обсягів даних або перевантаження систем фальшивими запитами, що може призвести до відмов у обслуговуванні.

У сучасному контексті атака троянського коня включає в себе вбудовання несанкціонованих інструкцій в авторизовану програму, щоб зловмисник міг отримати доступ до системи. Логічна бомба, зазвичай розміщена за допомогою техніки троянського коня, складається з прихованих інструкцій, які залишаються неактивними, поки не відбудеться певна подія, коли вони активуються. Наприклад, у 1985 році програміст страхової компанії у Форт-Ворті, штат Техас, вбудував логічну бомбу в систему управління персоналом компанії; коли його звільнили, і його ім'я було видалено з бази даних співробітників, вся база даних була стерта.

Після того, як система, підключена до Інтернету, зазнає вторгнення, її можна використовувати для створення ботнетів - мереж, що складаються з багатьох комп'ютерів, що керуються зловмисниками, для масових атак на інші системи з метою крадіжки інформації або завдання шкоди їхній роботі. Зросло обурення тим, що в "Інтернеті речей" підключені до мережі пристрої, такі як холодильники або телевізори, можуть бути використані для створення ботнетів. Різноманітність таких пристроїв ускладнює їхню захист від шкідливих програм.

Методи захисту інформаційної системи від кіберзагроз:

- Управління інформаційними системами
- Захист інформації
- Аудит інформаційних систем

Використання методу управління інформаційними системами для захисту інформаційної системи. Для забезпечення безпечної та ефективної роботи інформаційних систем, організації впроваджує набір процедур і технологічних заходів, відомих як засоби контролю. Ці засоби включають загальні та прикладні методи контролю для захисту інформаційних систем.

Загальні засоби контролю застосовуються до всієї діяльності інформаційних систем у межах організації. Найважливіші загальні засоби контролю включають заходи, що регулюють доступ до комп'ютерних систем та інформації, яка зберігається або передається через телекомунікаційні мережі. Цей контроль включає адміністративні заходи, які обмежують доступ працівників тільки до необхідних процесів, пов'язаних з їхніми обов'язками. Такі заходи контролю допомагають обмежити можливість шкоди, яку може заподіяти окремих працівник або той, хто намагається використувувати облікові дані працівника. Відмовостійкі комп'ютерні системи, розміщені в критичних середовищах, таких як лікарні чи фондові ринки, призначені для контролю та ізоляції проблем, щоб забезпечити неперервну роботу системи. Резервні системи, розташовані часто у віддалених місцях, можуть бути активовані у випадку відмови основної інформаційної системи.

Засоби керування програмою є специфічними для конкретної програми та включають такі заходи, як перевірка вхідних даних, реєстрація доступу до системи, регулярне архівування копій різних баз даних і забезпечення того, що інформація поширюється лише авторизованим користувачам.

У зв'язку з поширенням глобальних мереж, зокрема Інтернету, контроль доступу до інформаційних систем став значно складнішим. Користувачі, а також зловмисники, можуть здійснювати доступ до систем з будь-якого автономного комп'ютера в організації або з будь-якого місця через Інтернет. З міркувань безпеки кожен легітимний користувач має свій унікальний ідентифікатор та пароль, які періодично змінюються. Ще одним заходом безпеки є вимога до певної форми фізичної автентифікації, такої як об'єкт (фізичний маркер або смарт-карта) або особиста характеристика (відбиток пальця, малюнок сітківки, геометрія руки або підпис). Багато систем комбінують ці методи, наприклад, банкомати використовують комбінацію персонального ідентифікаційного номера (PIN) та ідентифікаційної картки. Заходи безпеки між внутрішніми мережами організації та Інтернетом відомі як брандмауери. Ці комбінації апаратного та програмного забезпечення постійно фільтрують вхідний та вихідний трафік даних.

Інший метод обмеження доступу до інформації - шифрування даних, яке набуло особливого значення в електронній торгівлі. Шифрування з відкритим ключем широко використовується у цій сфері. Для забезпечення конфіденційності тільки призначений отримувач має закритий ключ, необхідний для розшифрування повідомлень, зашифрованих відкритим ключем. Крім того, автентифікація обох сторін електронної транзакції можлива за допомогою цифрових сертифікатів, виданих обом сторонам довіреною третьою стороною, і використання цифрових підписів - додаткового коду, доданого до повідомлення для перевірки його походження. Тип коду захисту від несанкціонованого доступу також може бути доданий до повідомлення для виявлення пошкодження. Подібні засоби доступні для того, щоб сторони електронної транзакції не могли пізніше відмовитися від своєї участі. Деякі повідомлення вимагають додаткових атрибутів. Наприклад, платіж електронною готівкою - це тип повідомлення з шифруванням, що використовується для забезпечення анонімності покупця, і діє як фізична готівка.

Для постійного моніторингу інформаційних систем використовуються системи виявлення вторгнень. Вони виявляють аномальні події та записують інформацію, необхідну для створення звітів і встановлення джерела та характеру можливого вторгнення. Більш активні системи також намагаються запобігти вторгненню після виявлення в режимі реального часу.

Оцінка ефективності контрольних засобів інформаційних систем виконується за допомогою аудиту інформаційних систем. Головною метою аудиту є визначення того, чи забезпечують інформаційні системи захист корпоративних активів, збереження та передачу даних в цілості, а також ефективно дотримуються корпоративні цілі та забезпечується оптимальне функціонування. Це важлива складова загального фінансового аудиту, що оцінює бухгалтерські записи та фінансові звіти організації. Інформаційні системи розроблені з можливістю відстеження кожної фінансової операції, тобто існує контрольний шлях, який вказує, звідки походить кожна транзакція та як вона обробляється. Крім фінансових ау-

дитів, використовуються операційні аудити для оцінки ефективності роботи інформаційних систем та технологічні аудити для перевірки правильності вибору, налаштування та впровадження інформаційних технологій.

1.3 Аналіз технологій та рішень систем віртуалізації, віддалених серверів, SIEM-систем та їх використання в IT-інфраструктурі

Після розгляду поняття інформаційної системи, розгляду загроз для інформаційної системи, систем захисту та управління перейдемо до розгляду "Системи управління інформацією про безпеку та подій" (Security Information and Event Management), скорочено SIEM. [\[4,5\]](#).

Системи управління інформацією про безпеку та події (SIEM) – це рішення в галузі безпеки, яке допомагає організаціям виявляти та вирішувати потенційні загрози та вразливості безпеки до того, як вони можуть спричинити проблеми з бізнес-процесами.

SIEM-системи допомагають відділам безпеки підприємства виявляти незвичайність у поведінці користувачів та застосовувати штучний інтелект для автоматизації багатьох процесів, пов'язаних з виявленням загроз та реагуванням на події.

Початкові платформи SIEM почали як інструменти для управління журналами, які об'єднали в собі функції управління інформацією про безпеку (SIM) і керування подіями безпеки (SEM). Ці платформи забезпечували моніторинг та аналіз подій, пов'язаних з безпекою, у реальному часі, а також спрощували відстеження та реєстрацію даних безпеки для відповідності або аудиту. У 2005 році компанія Gartner вперше використала термін SIEM для опису поєднання технологій SIM і SEM.

Протягом багатьох років програмне забезпечення SIEM розвивалося, додавши аналітику поведінки користувачів і об'єктів (UEBA) та інші передові засоби аналітики безпеки, штучний інтелект і можливості машинного навчання для виявлення аномальної поведінки та індикаторів передових загроз. Сьогодні SIEM

став ключовим компонентом сучасних центрів операцій з безпеки (SOC) для моніторингу безпеки та управління відповідністю.

Після наведення загальної інформації про SIEM, перейдемо до розгляду актуальності та доцільності використання SIEM у теперішній час.

SIEM є невід'ємною складовою сучасної інформаційної безпеки. Він забезпечує комплексний підхід до моніторингу, аналізу та реагування на безпекові загрози та події в реальному часі. Інтеграція SIEM дозволяє організаціям ефективно виявляти та реагувати на потенційні та реальні загрози безпеки, сприяючи автоматизації процесів виявлення та реагування за допомогою штучного інтелекту.

SIEM також допомагає вирішувати вимоги щодо нормативного контролю та відповідності, забезпечуючи збереження журналів даних безпеки для аудиту та відповідності. Розвиток SIEM включає також нові функції, такі як аналітика поведінки користувачів і об'єктів (UEBA), що робить його необхідним інструментом для будь-якого центру операцій з безпеки (SOC).

Отже, SIEM залишається актуальним та необхідним інструментом для ефективного управління безпекою, виявлення та реагування на загрози в сучасному цифровому середовищі.

Розгляд основних можливостей SIEM більш детальноше.

- Збір даних
- Зберігання даних
- Політики та правила
- Консолідація та кореляція даних

Більшість сучасних систем SIEM отримують дані шляхом розгортання агентів збору на різних пристроях, включаючи кінцеві точки користувачів, сервери, мережеве обладнання, а також інші системи безпеки, такі як брандмауери та антивіруси. Крім того, вони можуть використовувати різні протоколи для пересилання системних журналів, такі як SNMP або WMI. Розширені SIEM можуть легко інтегруватися з хмарними сервісами для отримання журнальних даних про

інфраструктуру, розгорнуту в хмарі, або з програмами SaaS, а також здатні ефективно обробляти інші нестандартні джерела даних. Попередня обробка може проводитися на периферійних колекторах, де лише певні події або дані передаються до централізованого сховища.

У минулому SIEM зазвичай використовував централізоване сховище даних, розташоване в центрі обробки даних, що ускладнювало зберігання та керування великими обсягами інформації. В результаті були збережені лише обмежені обсяги журнальних даних.

З розвитком хмарних технологій, SIEM наступного покоління базуються на передових технологіях озера даних, таких як Amazon S3 або Hadoop, що забезпечують практично необмежену масштабованість сховища за доступну ціну. Це дозволяє зберігати та аналізувати 100% журнальних даних на ще більшій кількості платформ і систем.

Системи SIEM дозволяють працівникам служби безпеки встановлювати профілі, які визначають нормальну поведінку корпоративних систем.

Після цього вони можуть створити правила та встановити порогові значення для визначення того, які види аномальної активності вважаються інцидентами безпеки. Сьогодні все частіше SIEM використовує машинне навчання та автоматичне профілювання поведінки для автоматизованого виявлення аномалій і динамічного створення правил для обробки даних з метою виявлення подій безпеки, які потребують уваги та дослідження.

Основна мета систем SIEM полягає в тому, щоб об'єднати всі дані та забезпечити кореляцію журналів і подій у всіх системах організації. Наприклад, повідомлення про помилку на сервері може бути пов'язане зі заблокованим підключенням на брандмауері та спробою неправильного входу на корпоративний портал. Різні точки даних об'єднуються у значущі події безпеки, які передаються аналітикам за допомогою сповіщень або інформаційних панелей. Сучасні системи SIEM навчаються визнавати "справжні" події безпеки, які потребують уваги, з кожним роком.

Додаткова інформація про SIEM отримана з посилань [\[6,7\]](#).

Як і будь-яка інша технологія, SIEM має як переваги, так і недоліки, які важливо враховувати при оцінці його ефективності. Розглянемо деякі з цих плюсів та мінусів. Список основних переваг:

1. Централізоване керування
2. Виявлення загроз в реальному часі
3. Підвищена відповідність та аудит
4. Автоматизація процесів

SIEM дозволяє організаціям централізовано моніторити та управляти безпекою з різних джерел та систем, що забезпечує більшу ефективність та спрощує процес управління.

SIEM надає можливість виявлення та реагування на потенційні загрози в реальному часі, що дозволяє організаціям швидко реагувати на інциденти та мінімізувати можливі збитки.

SIEM допомагає відповідати вимогам щодо нормативного контролю та аудиту, забезпечуючи збереження журналів даних безпеки та генерацію звітів для аудиторських цілей

SIEM може автоматизувати деякі процеси виявлення та реагування на загрози за допомогою розумних алгоритмів та штучного інтелекту, що дозволяє зменшити навантаження на персонал та забезпечити швидку реакцію на інциденти.

Основні переваги розглянуті, також наведено основні недоліки подібних систем.

1. Складність впровадження та конфігурації
2. Великий обсяг даних
3. Високі витрати
4. Хибнопозитивні та хибнодивергентні сигнали

SIEM може бути складним у впровадженні та налаштуванні, вимагаючи значних зусиль та фахових знань для належної конфігурації та оптимізації.

SIEM збирає та аналізує великий обсяг даних, що може призвести до перевантаження систем та важкості в ефективному аналізі інформації.

Впровадження та підтримка SIEM може бути витратною ініціативою, особливо для невеликих організацій, що може обмежувати доступність цього рішення.

SIEM може генерувати велику кількість ложнопозитивних або ложнодивергентних сигналів, що може вимагати значних зусиль для відсіювання справжніх загроз від помилкових.

Отже, SIEM надає велику кількість переваг але потребує певний рівень навченості та підготовленості для впровадження та експлуатації у інформаційних системах. Також SIEM потребує великих матеріальних витрат для використання, безкоштовні рішення мають обмежений функціонал і не витримують потрібний рівень безпеки, тому використання SIEM має супроводжуватися попереднім плануванням і підготовкою.

Усе враховуючи, SIEM є важливим інструментом для сучасних організацій з метою забезпечення інформаційної безпеки. Він дозволяє централізовано моніторити та аналізувати безпекові події в реальному часі, виявляти потенційні загрози та реагувати на них швидко і ефективно.

SIEM допомагає підвищити відповідність з вимогами нормативного контролю та аудиту, автоматизувати процеси виявлення та реагування на інциденти, а також забезпечує цілісність та збереження журналів даних для аудитування.

Проте, використання SIEM може бути складним та витратним процесом, вимагаючи значних зусиль для впровадження, конфігурації та підтримки. Також важливо враховувати можливість генерації великої кількості ложнопозитивних сигналів, що може ускладнити процес виявлення справжніх загроз.

У підсумку, SIEM є потужним інструментом для забезпечення безпеки інформації, але перед його впровадженням в організації важливо ретельно оцінити переваги та недоліки, а також врахувати специфіку конкретної ситуації та потреби організації.

У сучасному цифровому світі інформаційні технології відіграють ключову роль у розвитку бізнесу, науки та суспільства в цілому. Швидке зростання обсягів даних, необхідність в оперативному доступі до інформації та підвищення вимог до продуктивності систем змушують організації шукати ефективні способи

управління своїми ІТ-ресурсами. Віртуалізація стала одним із найважливіших інструментів, що дозволяють оптимізувати використання апаратних та програмних ресурсів, підвищити гнучкість інфраструктури та знизити витрати на її підтримку.

Віртуалізація — це технологія, яка дозволяє створювати віртуальні представлення апаратних або програмних ресурсів, таких як сервери, сховища даних, мережеві пристрої чи операційні системи. Завдяки віртуалізації фізичні ресурси абстрагуються від програмного забезпечення, що працює на них, що дозволяє запускати декілька віртуальних машин або середовищ на одному фізичному обладнанні. Це забезпечує більш ефективне використання ресурсів та зменшує залежність програм від апаратної платформи.

Основним компонентом системи віртуалізації є гіпервізор — програмне забезпечення, яке створює та керує віртуальними машинами. Гіпервізор забезпечує ізоляцію між віртуальними машинами та розподіляє апаратні ресурси, такі як процесор, пам'ять та дисковий простір, між ними. Існують два основних типи гіпервізорів: типу 1 (bare-metal), які працюють безпосередньо на апаратному забезпеченні, та типу 2, які працюють поверх операційної системи.

Віртуальні машини (ВМ/VM) — це програмні симуляції фізичних комп'ютерів, які можуть запускати власні операційні системи та додатки. Кожна ВМ працює в ізольованому середовищі, що дозволяє забезпечити безпеку та стабільність системи в цілому.

Віртуалізація апаратного забезпечення дозволяє створювати повноцінні віртуальні машини, які емулюють фізичні комп'ютери. Цей тип віртуалізації використовується для консолідації серверів, коли на одному фізичному сервері працює декілька ВМ з різними операційними системами та додатками. Це забезпечує більш ефективне використання апаратних ресурсів та зменшує витрати на обладнання.

Типи віртуалізації.

- На рівні операційної системи, або контейнеризація
- Віртуалізація зберігання

- Віртуалізація мережі

Віртуалізація на рівні операційної системи, або контейнеризація, дозволяє запускати декілька ізольованих користувацьких просторів (контейнерів) в межах однієї операційної системи. Кожен контейнер має свої власні бібліотеки та залежності, але всі вони використовують спільне ядро ОС. Це забезпечує легкість та швидкість розгортання додатків, а також зменшує споживання ресурсів у порівнянні з повноцінними ВМ.

Віртуалізація зберігання об'єднує фізичні пристрої зберігання в єдиний віртуальний пул ресурсів. Це спрощує управління даними, підвищує масштабованість та дозволяє ефективніше використовувати дисковий простір. Адміністратори можуть динамічно розподіляти ресурси зберігання між додатками та серверами за потребою.

Віртуалізація мережі дозволяє створювати віртуальні мережеві ресурси, такі як комутатори, маршрутизатори та фаєрволи, поверх фізичної мережевої інфраструктури. Це забезпечує гнучкість у налаштуванні мережі, спрощує її управління та підвищує безпеку шляхом ізоляції трафіку різних додатків або користувачів.

Віртуалізація стала невід'ємною частиною сучасних інформаційних систем завдяки своїм численним перевагам. Однією з головних причин впровадження віртуалізації є оптимізація використання ресурсів. У традиційних системах сервери часто використовуються не на повну потужність, що призводить до неефективного витрачання ресурсів та коштів. Віртуалізація дозволяє консолідувати декілька серверів на одному фізичному обладнанні, підвищуючи рівень використання процесорів, пам'яті та дисків.

Основні переваги технології віртуалізації.

- Гнучкість та масштабованість
- Зниження витрат на апаратне забезпечення, енергоспоживання та охолодження
- Підвищення безпеки та надійності систем

- Спрощення управління та відновлення систем

Гнучкість та масштабованість є ще однією важливою перевагою. Організації можуть швидко розгортати нові віртуальні машини або контейнери для задоволення змінних потреб бізнесу, запуску нових додатків або тестування. Це дозволяє ІТ-відділам оперативно реагувати на вимоги ринку та внутрішніх користувачів.

Зниження витрат на апаратне забезпечення, енергоспоживання та охолодження є суттєвим фактором для бізнесу. Менша кількість фізичних серверів означає менші витрати на їхню покупку, розміщення в дата-центрах та підтримку. Крім того, спрощується управління інфраструктурою, що зменшує потребу в ІТ-персоналі.

Підвищення безпеки та надійності систем досягається через ізоляцію віртуальних машин та контейнерів. Якщо один додаток або ВМ зазнає атаки або збою, це не вплине на інші ВМ, що працюють на тому ж фізичному сервері. Також віртуалізація спрощує впровадження політик безпеки та управління доступом.

Спрощення управління та відновлення систем після збоїв є критичним для забезпечення безперервності бізнес-процесів. Віртуальні машини можна легко копіювати, створювати знімки стану (снапшоти) та переносити між серверами або навіть між дата-центрами. Це забезпечує швидке відновлення після збоїв та мінімізує час простою.

Наведені приклади застосування віртуалізації.

- У сфері хмарних обчислень
- У розробці та тестуванні програмного забезпечення
- Ізоляція критично важливих додатків
- Ізоляція критично важливих додатків

У сфері хмарних обчислень віртуалізація є основною технологією, що дозволяє провайдерам надавати інфраструктуру, платформи та програмне забезпечення як сервіс. Клієнти можуть орендувати обчислювальні ресурси за моделлю

"оплати за використання", що зменшує необхідність у власній інфраструктурі та дозволяє швидко масштабувати ресурси відповідно до потреб.

У розробці та тестуванні програмного забезпечення віртуалізація дозволяє створювати різні середовища для тестування додатків у контрольованих умовах. Розробники можуть швидко розгортати нові ВМ або контейнери з необхідними конфігураціями, що прискорює цикл розробки та підвищує якість продукту.

Ізоляція критично важливих додатків забезпечується за допомогою запуску кожного додатку в окремій віртуальній машині або контейнері. Це підвищує стабільність системи в цілому та запобігає конфліктам між додатками, які можуть виникнути через несумісність бібліотек або залежностей.

У навчанні та освіті віртуалізація дозволяє створювати віртуальні лабораторії, де студенти можуть експериментувати з різними технологіями без ризику пошкодити фізичне обладнання. Це забезпечує доступність ресурсів та гнучкість у навчальному процесі.

Отже, віртуалізація стала фундаментальною технологією, що трансформувала підхід до побудови та управління інформаційними системами. Вона надає можливість ефективніше використовувати ресурси, знижувати витрати, підвищувати гнучкість та забезпечувати високий рівень безпеки та надійності. У сучасному світі, де інформаційні технології швидко розвиваються і стають все більш складними, віртуалізація відкриває нові горизонти для інновацій та зростання бізнесу.

З огляду на постійні виклики, пов'язані зі зростанням обсягів даних, потребою в швидкій обробці інформації та забезпеченні безпеки, віртуалізація буде продовжувати відігравати ключову роль у розвитку інформаційних систем. Інтеграція з хмарними технологіями, розвиток контейнеризації та оркестрації, впровадження програмно-визначуваних мереж та сховищ даних — все це напрямки, де віртуалізація буде сприяти підвищенню ефективності та конкурентоспроможності організацій.

Сучасні інформаційні системи неможливо уявити без віддалених серверів, які стали фундаментом для багатьох технологій, таких як хмарні обчислення,

веб-хостинг та віддалений доступ до ресурсів. Розвиток інтернету та мережевих технологій призвів до того, що віддалений сервер став ключовим елементом, що забезпечує зручність, ефективність та гнучкість у роботі з інформацією та додатками. У цьому розділі розглянемо поняття віддаленого сервера та його роль у сучасних інформаційних системах.

Віддалений сервер — це комп'ютер або система комп'ютерів, які виконують серверні функції та доступні через мережу, зазвичай через інтернет. На відміну від локальних серверів, які знаходяться в тій же фізичній локації, що і користувач, віддалені сервери можуть бути розташовані у будь-якій точці світу. Користувачі можуть отримувати доступ до віддалених серверів для виконання різноманітних завдань, таких як зберігання даних, запуск додатків, обробка інформації та багато іншого.

Основні характеристики віддалених серверів:

- Доступність через мережу.
- Віддалене управління.
- Ресурсна потужність.

Доступність через мережу полягає в тому, що доступ до сервера здійснюється через мережеві протоколи (наприклад, HTTP, FTP, SSH), що дозволяє підключатися до нього з будь-якого місця з інтернет-з'єднанням.

Адміністрування сервера може здійснюватися віддалено, що спрощує його обслуговування та налаштування.

Віддалені сервери можуть мати високу обчислювальну потужність та великий обсяг пам'яті, що дозволяє виконувати складні задачі.

Використання віддалених серверів у сучасних інформаційних системах.

- Хмарні обчислення
- Веб-хостинг та онлайн-сервіси
- Віддалений доступ та віртуальні робочі місця
- Зберігання та обробка великих даних
- Резервне копіювання та відновлення даних

Хмарні обчислення стали одним із найпоширеніших способів використання віддалених серверів. Провайдери хмарних послуг надають інфраструктуру, платформи та програмне забезпечення як сервіс (IaaS, PaaS, SaaS). Це дозволяє організаціям орендувати обчислювальні ресурси та платити лише за фактичне використання, що знижує витрати на власне апаратне забезпечення та його обслуговування.

Віддалені сервери використовуються для розміщення веб-сайтів, додатків та сервісів. Власники сайтів можуть розміщувати свій контент на серверах хостинг-провайдерів, забезпечуючи доступність ресурсів для користувачів по всьому світу. Це також стосується стрімінгових сервісів, онлайн-ігор та інших інтернет-сервісів, які потребують постійної доступності та високої продуктивності.

З розвитком технологій віддаленої роботи, віддалені сервери стали основою для створення віртуальних робочих місць. Співробітники можуть підключатися до корпоративних серверів з будь-якого місця, отримуючи доступ до необхідних додатків та даних. Це підвищує гнучкість бізнесу та дозволяє залучати фахівців з різних регіонів.

У сфері Big Data віддалені сервери використовуються для зберігання та обробки величезних обсягів інформації. Організації можуть використовувати розподілені системи зберігання та обробки даних, такі як Hadoop або Spark, які працюють на кластерах віддалених серверів. Це дозволяє аналізувати дані в режимі реального часу та приймати обґрунтовані бізнес-рішення.

Віддалені сервери слугують для резервного копіювання критично важливих даних. Зберігання копій даних у віддаленому місці захищає їх від втрати через апаратні збої, природні катастрофи або інші непередбачені події. У разі необхідності дані можуть бути відновлені з резервних копій, забезпечуючи безперервність бізнес-процесів.

Переваги використання віддалених серверів.

- Глобальна доступність
- Економія ресурсів

- Масштабованість
- Безпека та надійність

Глобальна доступність дозволяє користувачам підключатися до сервера з будь-якої точки світу, що має ключове значення для міжнародних організацій та сервісів.

Економія ресурсів досягається завдяки зменшенню витрат на власну IT-інфраструктуру та її технічне обслуговування.

Масштабованість дозволяє динамічно збільшувати або зменшувати обсяги ресурсів відповідно до потреб бізнесу, забезпечуючи гнучкість і оптимальне використання коштів.

Безпека та надійність реалізуються через сучасні методи шифрування, захист від DDoS-атак і регулярне резервне копіювання, що мінімізує ризики для даних.

Ймовірні проблеми та ризики використання віддалених серверів.

- Безпека даних
- Залежність від провайдера
- Проблеми з продуктивністю
- Регуляторні та юридичні питання

Передача та зберігання конфіденційних даних на віддалених серверах вимагає особливої уваги до безпеки. Необхідно впроваджувати протоколи шифрування, контролю доступу та автентифікації, щоб запобігти несанкціонованому доступу та втраті даних.

Організації можуть стати залежними від постачальника послуг, особливо якщо використовуються пропрієтарні технології або якщо процес міграції до іншого провайдера є складним. Це може обмежувати гнучкість та збільшувати ризики, пов'язані з надійністю та фінансовою стабільністю провайдера.

Якість з'єднання з інтернетом та віддаленістю сервера можуть впливати на продуктивність додатків та сервісів. Висока затримка або низька пропускна здатність мережі можуть призвести до повільної роботи додатків, що негативно впливає на користувацький досвід.

Розміщення даних на серверах, що знаходяться в інших країнах, може підпадати під дію різних законодавств щодо захисту даних та конфіденційності. Організації повинні враховувати ці аспекти, щоб відповідати вимогам регуляторних органів та уникати юридичних проблем.

При виборі віддаленого сервера та провайдера послуг важливо враховувати:

Ймовірну локацію серверів, близькість до цільової аудиторії може зменшити затримку та покращити продуктивність.

Наявність і рівень підтримки. Наявність цілодобової технічної підтримки та швидкого реагування на проблеми.

Відповідність провайдера міжнародним стандартам безпеки інформації, таким як ISO 27001.

Слід зауважити наявність гнучкості умов договору, можливість легко змінювати обсяг послуг, відмовитися від них або мігрувати до іншого провайдера без значних штрафів.

Віддалені сервери є невід'ємною частиною сучасних інформаційних систем, надаючи безліч переваг для бізнесу та користувачів. Вони забезпечують доступність ресурсів, економічну ефективність та гнучкість, необхідні для успішного функціонування в умовах швидкозмінного технологічного середовища. Однак для максимального використання цих переваг необхідно уважно підходити до питань безпеки, вибору провайдера та відповідності регуляторним вимогам.

Враховуючи стрімкий розвиток технологій та зростання обсягів даних, роль віддалених серверів буде лише зростати. Інтеграція з іншими технологіями, такими як інтернет речей (IoT), штучний інтелект та машинне навчання, відкриває нові можливості для інновацій та покращення ефективності бізнес-процесів. Організації, що здатні ефективно використовувати віддалені сервери, матимуть значну конкурентну перевагу на ринку та зможуть швидко адаптуватися до нових викликів та можливостей.

1.4 Особливості функціонування інформаційних систем в умовах військового стану

В умовах військового стану в Україні інформаційні системи набувають особливої значущості, оскільки вони забезпечують критичну інфраструктуру держави, бізнесу та суспільства в цілому. ІТ-команди стикаються з низкою унікальних викликів та обмежень, пов'язаних з безпекою, доступністю, законодавчими нормами та технічними складнощами. Важливим аспектом є використання віддалених серверів та систем віртуалізації, які можуть стати як інструментом для подолання проблем, так і джерелом нових ризиків. У цьому розділі розглянемо особливості військового стану в Україні, обмеження, які він накладає, та способи, якими ІТ-команди можуть ефективно з ними боротися.

Військовий стан в Україні передбачає особливий правовий режим, спрямований на забезпечення національної безпеки та оборони. Він накладає певні обмеження на діяльність організацій та громадян, включаючи можливі обмеження свободи інформації, комунікацій та пересування. Для інформаційних систем це означає підвищені вимоги до безпеки, можливі обмеження в доступі до мереж, а також необхідність дотримання нових законодавчих норм.

Одним із ключових аспектів є посилення контролю за телекомунікаційними мережами та інформаційними ресурсами. Держава може вимагати від операторів зв'язку та провайдерів інтернет-послуг надання пріоритету військовим та урядовим комунікаціям, обмежувати або блокувати доступ до певних ресурсів, а також здійснювати моніторинг інформаційних потоків.

У таких умовах ІТ-команди стикаються з проблемами, пов'язаними з забезпеченням безперебійної роботи інформаційних систем, захистом даних та адаптацією до нових регуляторних вимог. Особливе значення набуває використання віддалених серверів та систем віртуалізації, які можуть допомогти зберегти функціональність систем та забезпечити віддалений доступ до них.

Проблеми, з якими стикаються ІТ-фахівці, включають:

- Обмеження в доступі до мережі:
- Підвищений ризик кібератак:

- Законодавчі обмеження:
- Людський фактор:

Можливі перебої в роботі інтернет-з'єднання, мобільних мереж або повне їх відключення в окремих регіонах. Це ускладнює віддалений доступ до серверів та хмарних сервісів.

Військовий конфлікт супроводжується активізацією кіберзагроз з боку ворожих держав або груп. Це може включати DDoS-атаки, фішинг, поширення шкідливого програмного забезпечення та інші види кібератак, спрямовані на дестабілізацію інформаційних систем.

Нові регуляторні акти можуть вимагати від компаній надання доступу до даних державним органам, обмежувати передачу даних за кордон або встановлювати інші обмеження, що впливають на роботу інформаційних систем.

Співробітники можуть бути мобілізовані, змушені евакуюватися або не мати можливості працювати з офісу. Це створює дефіцит кваліфікованого персоналу та вимагає організації віддаленої роботи.

Віддалені сервери та системи віртуалізації можуть стати ключовими інструментами для забезпечення безперервності бізнесу та захисту даних. Вони дозволяють:

Розмістити резервні копії даних та систем за межами зони військових дій, що знижує ризик фізичного знищення обладнання та втрати інформації.

Забезпечити віддалений доступ до систем та ресурсів, що дозволяє співробітникам працювати з безпечних локацій, не наражаючи себе на небезпеку.

Швидко масштабувати ресурси у відповідь на змінені потреби, використовуючи хмарні сервіси та віртуальні машини.

Однак використання віддалених серверів також може створювати додаткові ризики, особливо щодо безпеки даних та відповідності законодавству.

- Основні обмеження та шляхи їх подолання.
- Обмеження в доступі
- Підвищений ризик кібератак
- Законодавчі обмеження

- Людський фактор

Обмеження в доступі до мережі можна подолати, використовуючи альтернативні канали комунікації, такі як супутниковий інтернет або приватні мережі. Важливо забезпечити резервні канали зв'язку та використовувати VPN для захищеного доступу до систем.

Підвищений ризик кібератак вимагає посилення заходів кібербезпеки, включаючи оновлення систем безпеки, впровадження багатофакторної автентифікації, моніторинг аномальної активності та навчання співробітників правилам безпечної роботи в мережі.

Законодавчі обмеження потребують уважного стеження за змінами в законодавстві та консультацій з юридичними фахівцями, щоб забезпечити відповідність діяльності компанії новим вимогам. Можливо, доведеться переглянути політики зберігання та обробки даних, а також умови використання хмарних сервісів.

Людський фактор може бути вирішений шляхом організації віддаленої роботи. Необхідно забезпечити співробітників необхідними засобами для роботи з дому або безпечних локацій, включаючи ноутбуки, доступ до систем та засоби комунікації. Варто також розглянути можливість розподілу обов'язків між співробітниками, щоб компенсувати можливу відсутність ключових фахівців.

Практичні рекомендації для ІТ-команд в Україні.

- Резервне копіювання та зберігання даних
- Використання хмарних сервісів
- Планування безперервності бізнесу
- Комунікація та підтримка співробітників

Резервне копіювання та зберігання даних є критично важливими. Створюйте регулярні резервні копії та зберігайте їх у безпечних, географічно віддалених місцях. Використовуйте шифрування для захисту конфіденційної інформації.

Використання хмарних сервісів може забезпечити гнучкість та стійкість систем. Розгляньте можливість перенесення критично важливих систем до хмарних платформ, які мають високий рівень безпеки та доступності.

Планування безперервності бізнесу повинно включати детальні плани дій у разі різних сценаріїв, включаючи повну втрату доступу до офісу або мережі. Проведіть тренінги та симуляції для підготовки співробітників.

Комунікація та підтримка співробітників є важливими для збереження ефективності роботи команди. Забезпечте ефективні канали комунікації для координації дій та підтримуйте моральний дух співробітників, надаючи психологічну підтримку та створюючи умови для комфортної роботи в складних обставинах.

В умовах військового стану в Україні інформаційні системи та ІТ-команди стикаються з унікальними викликами, які вимагають швидкої адаптації та впровадження ефективних рішень. Використання віддалених серверів та систем віртуалізації може стати як порятунком, так і джерелом нових ризиків, тому необхідно підходити до цього питання обережно та зважено.

Забезпечення безпеки даних, безперервності бізнесу та підтримки співробітників є пріоритетними завданнями. Співпраця з державними органами, постачальниками послуг та іншими організаціями може допомогти подолати складнощі та знайти оптимальні рішення.

Успішне подолання викликів військового стану залежить від здатності ІТ-команд швидко адаптуватися, впроваджувати нові технології та підходи, а також підтримувати високий рівень професіоналізму та згуртованості. Це дозволить не лише зберегти функціональність інформаційних систем у складний період, але й закласти фундамент для їхнього подальшого розвитку та вдосконалення в майбутньому.

1.5 Постановка технічного завдання на розробку системи поглибленого моніторингу

1. Огляд проекту

Мета проекту: Розробка та впровадження системи поглибленого моніторингу захищеної віртуалізованої ІТ-інфраструктури підприємства. Проект спрямований на забезпечення високої безпеки, ефективності та масштабованості ІТ-систем, а також на оптимізацію використання ресурсів та підвищення стійкості до відмов.

2. Вимоги до системи

2.1 Функціональні вимоги

- Моніторинг продуктивності серверів та віртуальних машин.
- Виявлення та реагування на потенційні загрози безпеці.
- Надання звітів та аналітики в реальному часі.
- Інтеграція з існуючими системами управління та безпеки.
- Автоматичне резервне копіювання та відновлення даних.

2.2 Нефункціональні вимоги

- **Безпека:** Високий рівень захисту даних, шифрування передачі та зберігання інформації.
- **Доступність:** Безперебійна робота системи 24/7 з можливістю швидкого відновлення після збоїв.
- **Швидкодія:** Висока продуктивність системи моніторингу без затримок у обробці даних.
- **Масштабованість:** Легке розширення системи для підтримки зростаючої ІТ-інфраструктури та інтеграція з новими технологіями.

3. Архітектура системи

Основні компоненти:

- **Агенти моніторингу:** Встановлюються на віртуальні машини для збору даних.
- **Центральний сервер:** Обробляє та зберігає зібрані дані.
- **База даних:** Зберігає історичні дані та забезпечує їх доступність для аналізу.
- **Інтерфейс користувача:** Забезпечує візуалізацію даних та доступ до звітів.

Взаємодія компонентів:

1. Агенти збирають дані про продуктивність та безпеку.
2. Дані передаються до центрального сервера.
3. Центральний сервер обробляє та зберігає дані в базі.
4. Користувачі отримують доступ до інформації через інтерфейс.

4. План впровадження

1. Підготовчий етап:

- Аналіз поточної IT-інфраструктури.
- Визначення вимог та вибір програмного забезпечення.

2. Етап встановлення:

- Налаштування серверного обладнання та встановлення обраного ПЗ.
- Конфігурація агентів моніторингу на віртуальних машинах.

3. Етап інтеграції:

- Інтеграція системи моніторингу з існуючими системами безпеки.
- Налаштування звітів та сповіщень.

4. Етап тестування:

- Проведення функціональних та безпекових тестів.
- Оптимізація параметрів системи для досягнення найкращої продуктивності.

5. Етап навчання та передача:

- Проведення навчальних сесій для IT-спеціалістів.
- Передача документації та офіційне завершення проекту.

5. Очікувані результати

- **Підвищення ефективності IT-інфраструктури:** Оптимізоване використання ресурсів та зниження витрат.
- **Покращення безпеки:** Виявлення та запобігання загрозам, захист конфіденційної інформації.
- **Масштабованість та гнучкість:** Легке розширення системи відповідно до потреб бізнесу.

- **Фокус на основних бізнес-процесах:** Делегування управління IT-інфраструктурою професіоналам, що дозволяє зосередитися на розвитку компанії.

Висновки: у першому розділі було проведено широке коло теоретичних досліджень, необхідних для розуміння та проектування захищеної віртуалізованої IT-інфраструктури підприємства. Насамперед розглянуто поняття інформаційної системи, її складові та роль в організації. Встановлено, що IT-інфраструктура невіддільна від інформаційної системи й слугує її технологічним фундаментом, а ретельно спроектоване поєднання апаратного забезпечення, програмного забезпечення, мережевих ресурсів і хмарних сервісів формує основу для ефективного управління даними та бізнес-процесами. Далі проаналізовано основні загрози для інформаційних систем, включно з людськими помилками, стихійними лихами та протиправними діями з використанням комп'ютерних технологій. Наголошено, що об'єктивні чинники, такі як фізична відмова обладнання чи стихійні лиха, можуть завдавати суттєвих збитків, однак кіберзлочини й шкідливе ПЗ (віруси, троянські коні, фішинг) також становлять серйозну небезпеку й вимагають комплексних засобів захисту та контролю. Окрему увагу було приділено технології SIEM, яка дає змогу централізовано збирати, аналізувати й корелювати події в реальному часі з різних вузлів системи. Розглянуто переваги SIEM (централізоване керування безпекою, спрощення аудиту, виявлення загроз у реальному часі) та її недоліки (складність впровадження, високі витрати, ризик хибнопозитивних сигналів). Відзначено, що продумана інтеграція SIEM дає змогу оперативно реагувати на загрози, автоматизувати процес виявлення інцидентів і посилює захист всієї IT-інфраструктури. Крім того, описано системи віртуалізації та віддалені сервери, які стали основою сучасних інформаційних систем. Показано, що віртуалізація сприяє більш ефективному використанню ресурсів, покращує масштабованість і безпеку, а віддалені сервери розв'язують задачу глобальної доступності та дають змогу знизити витрати на власне обладнання. Водночас наголошено на актуальних ризиках (наприклад, залежність від провайдера, мережеві затримки та регуляторні питання).

РОЗДІЛ 2. ПРОЄКТУВАННЯ СИСТЕМИ ПОГЛИБЛЕНОГО МОНІТОРИНГУ ЗАХИЩЕНОЇ ВІРТУАЛІЗОВАНОЇ ІТ-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

2.1 Методи та технології побудови системи поглибленого моніторингу

2.1.1 Базові принципи проєктування організаційної структури

Кожна організаційна структура управління є основою для досягнення цілей і завдань підприємства, що ґрунтується на певних правилах та принципах. Структура визначає, як організовані функції підприємства, розподіляються обов'язки між різними підрозділами, і як здійснюється взаємодія між ними. Організаційна структура також є одним з ключових елементів системи управління, що поєднує економічні, виробничі та управлінські процеси, сприяючи сталому розвитку бізнесу.

Основою ефективної організаційної структури є розподіл завдань, спеціалізація кожного підрозділу на певних напрямках та інтеграція управління на всіх рівнях підприємства. Така структура має бути ієрархічною, де кожен рівень управління має свої завдання, сфери відповідальності та чіткі повноваження.

Принципи проєктування організаційної структури

1. Формулювання стратегічних пріоритетів
2. Оцінка внутрішніх та зовнішніх умов
3. Розробка оптимальної моделі управління
4. Встановлення операційних цілей і завдань
5. Адаптація структури до змін

Стратегічне планування – це перший крок на шляху до створення ефективної організаційної структури. Важливо чітко визначити ключові бізнес-пріоритети, які спрямовують компанію до досягнення її довгострокових цілей. Для кожної стратегії має бути створена відповідна модель управління, що відповідає цілям розвитку підприємства. Наприклад, якщо компанія планує впроваджувати інноваційні продукти або виходити на нові ринки, структура повинна бути гнучкою та адаптивною, щоб швидко відповідати на зміни в ринковому середовищі.

Необхідно оцінити внутрішні можливості підприємства, такі як наявні ресурси, компетенції співробітників та технологічна готовність, а також зовнішні фактори, що впливають на бізнес. До таких зовнішніх факторів належать економічні умови, державне регулювання, конкурентне середовище та технологічні зміни. Важливо врахувати, як впровадження віддалених серверів, може допомогти підвищити ефективність управління, знизити витрати на інфраструктуру та забезпечити масштабованість бізнесу.

Для досягнення максимального результату підприємству необхідно обрати модель управління, яка найкраще відповідає його стратегії та цілям. Це може бути як централізована, так і децентралізована модель управління. З використанням віддалених серверів, компанія може впроваджувати гібридну модель, де центральний офіс здійснює загальне стратегічне керівництво, а окремі підрозділи отримують автономію у прийнятті операційних рішень і керуванні своїми ресурсами.

Чітке визначення операційних завдань і цілей для кожного підрозділу є ключовим фактором успішного функціонування організації. Кожен відділ або підрозділ має знати свої функції та завдання в рамках загальної стратегії підприємства. Наприклад, відділ ІТ повинен відповідати за підтримку серверної інфраструктури, управління віртуальними машинами на базі систем віртуалізації, а також забезпечення безпеки даних. Також слід встановити технічні показники ефективності, щоб оцінювати роботу кожного підрозділу.

Сучасний бізнес-середовище постійно змінюється, тому організаційна структура підприємства повинна бути гнучкою і здатною швидко адаптуватися до нових умов. Структура має забезпечувати можливість впровадження нових технологій, зміни в управлінських процесах, а також коригування взаємодії між підрозділами. Наприклад, впровадження віддалених серверів, може змінити процеси розподілу обчислювальних ресурсів між різними відділами, що сприятиме їх більш ефективному використанню.

2.1.2 Розробка та проектування ІТ-інфраструктури підприємства

Перш ніж розпочати планування побудови системи поглибленого моніторингу захищеної віртуалізованої ІТ-інфраструктури підприємства, необхідно чітко визначити ресурси, з якими ми працюватимемо. Важливо провести детальний аналіз наявної інфраструктури, зрозуміти, які компоненти вже впроваджені, і визначити, що потрібно додати або оновити для забезпечення коректної та ефективної роботи в сучасних умовах.

Зважаючи на швидкий розвиток технологій та зростання вимог до масштабованості і безпеки, виникає потреба в модернізації існуючої інфраструктури. Локальне розташування серверів може створювати обмеження в гнучкості, масштабованості та стійкості до відмов. Тому для оптимізації до сучасних реалій ми плануємо використати наступний стек технологій: віртуалізація та віддалені сервери.

Впровадження технологій віртуалізації стане ключовим елементом модернізації. Віртуалізація дозволить нам оптимізувати використання апаратних ресурсів, замінивши кілька фізичних серверів на віртуальні машини, що працюють на одному або декількох фізичних хостах. Це знизить витрати на обладнання та обслуговування, оскільки менша кількість фізичних серверів означає менші витрати на електроенергію, охолодження та технічне обслуговування. Крім того, вона підвищить гнучкість та масштабованість, дозволяючи швидко розгортати нові сервери та додатки, а також динамічно перерозподіляти ресурси залежно від навантаження. Віртуалізація також забезпечить високу доступність та стійкість до відмов: віртуальні машини можна легко переміщувати між хостами без перерви в роботі, що гарантує безперебійну роботу критично важливих сервісів. А розміщення ІТ-інфраструктури підприємства віддалено допоможе адаптуватися до умов сьогодення.

Для впровадження цих технологій ми укладаємо контракт з надійним дата-центром, який відповідає всім необхідним вимогам безпеки та стандартам якості.

Перенесення серверів до дата-центру включає:

Міграцію існуючих сервісів та даних з забезпеченням безперервності бізнес-процесів під час переходу.

Налаштування віртуалізованого середовища, а саме встановлення та конфігурація гіпервізорів, створення віртуальних машин, налаштування мережових з'єднань.

Встановлення інструментів моніторингу для відстеження продуктивності, безпеки та доступності всіх компонентів інфраструктури.

Впровадження віртуалізації та перенесення серверів до віддаленого дата-центру дозволить компанії:

- Підвищити ефективність IT-інфраструктури
- Забезпечити високий рівень безпеки
- Покращити масштабованість та гнучкість
- Фокусуватися на основних бізнес-процесах

2.1.3 Вибір типу ПЗ та визначення основних кроків для виконання ТЗ

Після детального аналізу поточної ситуації на підприємстві, ми можемо переходити до конкретизації цілей та завдань проекту. Важливо зазначити, що перехід на віртуалізацію вже завершено, тому сам процес міграції на віртуалізовану інфраструктуру не буде розглядатися у цьому технічному завданні. Натомість, основна увага буде приділена функціонуванню системи в умовах вже налаштованого віртуалізованого серверного середовища.

Для ефективного моніторингу захищеної віртуалізованої IT-інфраструктури підприємства необхідно ретельно підійти до вибору програмного забезпечення (ПЗ). Вибір ПЗ повинен бути обґрунтованим та свідомим, враховуючи специфічні потреби підприємства, його бюджетні обмеження та технічні вимоги. Основні кроки цього процесу включають:

1. Визначення вимог до ПЗ:

- Функціональні вимоги: моніторинг продуктивності, безпеки, доступності системи, інтеграція з існуючими інструментами управління та безпеки.

- Нефункціональні вимоги: висока доступність, масштабованість, безпека даних, зручність використання, підтримка та документація.

2. Аналіз ринку ПЗ:

- Дослідження доступних рішень, як open source, так і комерційних.
- Оцінка популярності та репутації рішень на ринку.
- Вивчення відгуків користувачів та експертів.

3. Порівняння різних варіантів:

- Створення таблиці порівняння ключових характеристик різних ПЗ.
- Оцінка відповідності кожного варіанту вимогам підприємства.
- Аналіз вартості впровадження та експлуатації кожного рішення.

4. Проведення тестування:

- Встановлення пробних версій або демо-версій обраних ПЗ.
- Проведення пілотних проектів для оцінки функціональності та інтеграції з існуючою інфраструктурою.
- Збір зворотного зв'язку від користувачів та технічної команди.

5. Прийняття рішення:

- Вибір оптимального ПЗ на основі проведеного аналізу та тестування.
- Розробка плану впровадження обраного рішення.

З огляду на навчальні цілі проекту, основний акцент буде зроблено на open source рішеннях, які забезпечують гнучкість, масштабованість та можливість налаштування відповідно до специфічних потреб підприємства. Однак для повного порівняння будуть розглянуті також комерційні рішення, щоб оцінити їхні переваги та недоліки.

Основні типи систем, що будуть використані:

6. Системи віртуалізації:

- Призначення: Оптимізація використання апаратних ресурсів шляхом створення віртуальних машин на фізичних хостах.

7. SIEM (Security Information and Event Management) та подібні системи:

- Призначення: Збір, аналіз та кореляція логів і подій з різних джерел для виявлення загроз та забезпечення безпеки.

Необхідно визначити основні відмінності між Open Source та комерційними рішеннями. Виконане порівняння записане у вигляді таблиці.

Таблиця 2.2.1 – Порівняння систем віртуалізації

Критерій	Open Source Рішення	Комерційні Рішення
Вартість	Безкоштовні або низькі витрати	Висока вартість ліцензій та підтримки
Гнучкість	Висока, можливість налаштування під специфічні потреби	Обмежена гнучкість, залежить від виробника
Підтримка	Спільнота, документація, платна підтримка за додаткову плату	Професійна підтримка від виробника
Масштабованість	Добре підходять для середніх та великих середовищ з правильним налаштуванням	Висока масштабованість та оптимізація для великих підприємств
Функціональність	Базові та деякі розширені функції, потребують додаткових налаштувань	Повний набір функцій з інтуїтивним інтерфейсом
Безпека	Залежить від налаштувань та регулярних оновлень	Високий рівень безпеки з регулярними оновленнями та патчами
Інтеграція	Можлива, але може потребувати додаткової роботи	Легка інтеграція з іншими комерційними продуктами

Визначені основні кроки для виконання поставлено ТЗ.

1. Дослідження та аналіз вимог:

- Визначення специфічних потреб підприємства щодо моніторингу та безпеки.
- Оцінка поточних процесів та інфраструктури для виявлення зон для покращення.

2. Вибір програмного забезпечення:

- Проведення детального аналізу доступних рішень, як open source, так і комерційних.

- Порівняння варіантів за критеріями функціональності, безпеки, масштабованості та витрат.

- Вибір оптимального рішення з урахуванням навчальних цілей та практичних вимог підприємства.

3. Планування впровадження:

- Розробка детального плану впровадження обраного ПЗ, включаючи часові рамки та етапи.

- Визначення ресурсів, необхідних для впровадження, включаючи апаратне забезпечення та людські ресурси.

4. Встановлення та налаштування ПЗ:

- Інсталяція обраного програмного забезпечення на сервери та віртуальні машини.

- Налаштування параметрів безпеки, моніторингу та інтеграції з існуючими системами.

5. Інтеграція з існуючою інфраструктурою:

- Забезпечення сумісності обраного ПЗ з поточними системами управління та безпеки.

- Налаштування обміну даними між новою системою моніторингу та іншими компонентами ІТ-інфраструктури.

6. Тестування системи:

- Проведення функціональних тестів для перевірки коректності роботи системи.

- Тестування на безпеку для виявлення можливих вразливостей.

- Оптимізація налаштувань на основі результатів тестування.

7. Навчання персоналу:

- Розробка навчальних матеріалів та проведення тренінгів для ІТ-спеціалістів.

- Забезпечення підтримки користувачів у процесі освоєння нової системи.

8. Впровадження та експлуатація:

- Перенесення системи моніторингу у виробниче середовище.
- Постійний моніторинг та обслуговування системи для забезпечення її безперебійної роботи та адаптації до змінних умов бізнесу.

Для досягнення поставлених цілей та ефективного моніторингу захищеної віртуалізованої ІТ-інфраструктури підприємства, планується використання наступних типів систем:

1. Системи віртуалізації:

- Функціональність: Створення та управління віртуальними машинами, оптимізація використання апаратних ресурсів, забезпечення гнучкості та масштабованості ІТ-інфраструктури.

- Переваги: Зниження витрат на фізичне обладнання, спрощення управління ресурсами, підвищення стійкості до відмов через можливість швидкого переміщення віртуальних машин між хостами.

- Вибір рішень: Основний акцент буде зроблено на open source рішеннях, таких як Proxmox VE або KVM, але для порівняння також будуть розглянуті комерційні варіанти, наприклад, VMware vSphere або Microsoft Hyper-V.

1. SIEM (Security Information and Event Management) та подібні системи:

- Функціональність: Збір, аналіз та кореляція логів і подій з різних джерел для виявлення загроз та забезпечення безпеки ІТ-інфраструктури.

- Переваги: Раннє виявлення кіберзагроз, централізований моніторинг безпеки, покращення відповідності вимогам нормативних актів, автоматизація реагування на інциденти.

- Вибір рішень: Буде розглянуто як open source рішення, такі як ELK Stack або Graylog, так і комерційні продукти, наприклад, Splunk або AlienVault OSSIM, для порівняння їхніх функціональних можливостей та відповідності вимогам підприємства.

Вибір відповідного програмного забезпечення та розробка чіткого плану виконання технічного завдання є ключовими етапами для успішного впровадження системи поглибленого моніторингу захищеної віртуалізованої ІТ-інфраструктури підприємства. Використання open source рішень дозволить знизити витрати та забезпечити гнучкість, водночас порівняння з комерційними альтернативами допоможе оцінити їхні переваги та недоліки. Такий підхід забезпечить ефективне управління ІТ-ресурсами, підвищення рівня безпеки та підтримку масштабованості інфраструктури відповідно до потреб бізнесу.

2.1.4 Загальна структура інформаційної системи

Після визначення задач, вимог та розгляду основних аспектів організації та майбутньої інформаційної системи, переходимо до планування практичного представлення інформаційної системи. Інформаційна система буде представлена одним або кількома серверами, розташованими у надійному дата-центрі з високим рівнем безпеки та доступом через мережу Інтернет. Вибір дата-центру має базуватися на таких критеріях, як географічне розташування, наявність резервних джерел живлення, охолодження, фізичний доступ та відповідність стандартам безпеки (наприклад, ISO 27001).

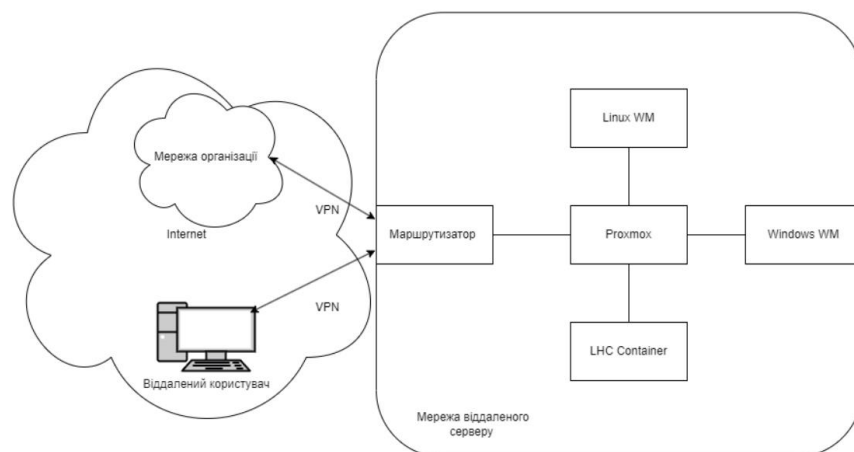


Рисунок 2.2.1 – Загальне представлення інформаційної системи

Як вирішено раніше, необхідно встановити на сервер відповідну систему віртуалізації, що забезпечить оптимальне використання апаратних ресурсів та гнучкість управління ІТ-інфраструктурою. Вибір конкретної системи віртуалізації

буде здійснено на основі проведеного аналізу функціональних можливостей, сумісності з існуючим програмним забезпеченням та бюджетних обмежень.

Після встановлення та налаштування системи віртуалізації, наступним кроком є інтеграція систем моніторингу, реагування та обробки інформації. Це передбачає встановлення програмного забезпечення для моніторингу стану серверів, віртуальних машин та мережевої інфраструктури.

Крім того, важливо забезпечити автоматизовані механізми реагування на інциденти, які дозволять швидко виявляти та нейтралізувати загрози. Це може включати налаштування сповіщень у разі виявлення аномальної активності, автоматичне блокування підозрілих IP-адрес або запуск скриптів для ізоляції заражених віртуальних машин. Всі ці заходи повинні бути документовані та регулярно оновлюватися відповідно до змін у загрозах та технологічних вимогах.

Також необхідно врахувати питання резервного копіювання та відновлення даних. Віртуалізована інфраструктура дозволяє легко створювати знімки віртуальних машин та зберігати їх у віддалених або хмарних сховищах. Це забезпечить можливість швидкого відновлення систем у разі технічних збоїв або кіберінцидентів, мінімізуючи час простою та втрати даних.

Також важливо впровадити політики безпеки, які регламентуватимуть доступ до серверів та інформаційних ресурсів. Це включає використання багатофакторної автентифікації, регулярне оновлення програмного забезпечення, проведення аудитів безпеки та навчання персоналу щодо найкращих практик кібербезпеки.

Паралельно з цим, необхідно забезпечити належну документацію всіх процесів та налаштувань системи. Це включає створення схем архітектури інфраструктури, опис конфігурацій віртуальних машин, налаштувань систем моніторингу та реагування, а також процедур резервного копіювання та відновлення даних. Документація повинна бути доступною для всіх членів ІТ-команди та регулярно оновлюватися відповідно до змін у системі.

Всі ці кроки спрямовані на створення стабільної, безпечної та ефективної інформаційної системи, яка зможе підтримувати потреби підприємства у довгостроковій перспективі, забезпечуючи високу продуктивність, надійність та гнучкість IT-інфраструктури.

2.2 Аналіз та вибір програмних рішень для побудови системи поглибленого моніторингу

2.2.1 Аналіз систем віртуалізації та їх порівняння

Створення ефективної інформаційної системи передбачає ретельний аналіз та вибір відповідних програмних рішень. Особливе значення має використання технологій віртуалізації та віддалених серверів для забезпечення гнучкості, безпеки і продуктивності системи. Одним із ключових етапів є розгляд можливостей використання віддаленого серверу для оптимізації управління ресурсами підприємства. Перейдемо до розгляду можливостей використання віддаленого серверу.

Для побудови інформаційної системи на базі віртуалізації необхідно обрати відповідну платформу, яка буде керувати віртуальними машинами та ресурсами. Розглянемо кілька популярних рішень:

- oVirt
- XenServer (Citrix Hypervisor)
- OpenNebula
- Proxmox VE

oVirt — це потужне рішення для великих організацій з великими вимогами до віртуалізації. Воно підтримує масштабовані кластери та має розширену функціональність, але для його налаштування та управління потрібні високі технічні знання. Крім того, резервне копіювання не інтегроване і потребує використання сторонніх рішень. Інформація про цю систему віртуалізації представлена на основі [\[9, 13\]](#).

XenServer (Citrix Hypervisor) пропонує базову безкоштовну версію з основними функціями та високу продуктивність, але додаткові можливості доступні лише у платній версії. Це рішення більше підходить для великих підприємств, які потребують корпоративної підтримки. Інформація про цю систему віртуалізація представлена на основі [\[10\]](#).

OpenNebula є рішенням для побудови приватних і гібридних хмарних інфраструктур. Його перевагою є підтримка різних гіпервізорів, але воно вимагає значних зусиль для налаштування і технічної підтримки. Це робить OpenNebula ідеальним для великих інфраструктур або проєктів, орієнтованих на хмарні сервіси. Інформація про цю систему віртуалізація представлена на основі [\[11, 14\]](#).

Proxmox VE (Virtual Environment) – це відкрите рішення для віртуалізації на основі KVM і LXC контейнерів. Воно дозволяє легко управляти як віртуальними машинами, так і контейнерами через зручний веб-інтерфейс. Proxmox також має вбудовані функції резервного копіювання та кластеризації, що робить його привабливим для малого та середнього бізнесу. Інформація про цю систему віртуалізація представлена на основі [\[8, 12\]](#).

Таблиця для порівняння представлених продуктів наведена у [\[Додаток В\]](#), представлення у вигляді таблиці спростить сприйняття інформації і дозволить прийняти рішення з більшою ефективністю.

Proxmox є відмінним варіантом для багатьох підприємств завдяки поєднанню простоти використання та потужних функцій. Це безкоштовне програмне забезпечення з відкритим кодом, яке легко інтегрується в існуючу інфраструктуру і забезпечує високу гнучкість для управління віртуальними машинами та контейнерами. Proxmox також має функції резервного копіювання та відновлення, що є важливим для безпеки даних. Його інтуїтивний веб-інтерфейс значно спрощує налаштування та моніторинг системи.

2.2.2 Переваги віддалених серверів в умовах військового стану

В умовах військового стану підприємства стикаються з особливими викликами, такими як ризики фізичної безпеки та нестабільність інфраструктури. Використання віддалених серверів має кілька важливих переваг:

- Безпека даних
- Гнучкість та мобільність
- Захист від втрат даних
- Швидке масштабування ресурсів

Віддалені сервери, такі як ті, що використовуються на основі Proxmox, дозволяють зберігати дані поза зоною ризику фізичних пошкоджень. Це особливо важливо в умовах військового конфлікту, коли дата-центри або офісні приміщення можуть стати мішенню атак.

Віртуалізовані сервери дозволяють швидко розгортати нові середовища, адаптувати ресурси та перенести робочі процеси в безпечніші зони. Підприємства можуть використовувати віддалені сервери для забезпечення безперервної роботи навіть при фізичній недоступності основних офісів або обладнання.

Віддалені сервери забезпечують можливість регулярного резервного копіювання даних та їх відновлення у разі пошкодження локальних систем. Це допомагає уникнути втрат критично важливої інформації в надзвичайних ситуаціях.

Використання віддалених серверів дозволяє легко збільшувати або зменшувати обчислювальні ресурси відповідно до потреб підприємства, що є важливим у нестабільних умовах.

Незважаючи на численні переваги, використання віддалених серверів має й певні недоліки, які слід враховувати:

- Проблеми з безпекою
- Залежність від Інтернет-з'єднання
- Складність налаштування і управління
- Питання щодо суверенітету даних

Використання віддалених серверів відкриває нові ризики кібербезпеки. Віддалений доступ до серверів може бути підданий атакам хакерів, зловмисникам чи внутрішнім загрозам. Особливо важливо забезпечити надійні засоби аутентифікації, шифрування даних та регулярний моніторинг мережевої безпеки.

Робота віддалених серверів повністю залежить від стабільного та швидкого Інтернет-з'єднання. У разі перебоїв в Інтернеті підприємства можуть стикатися з простоям або обмеженим доступом до ресурсів.

Для багатьох компаній, особливо тих, що не мають досвідченого ІТ-персоналу, налаштування та управління віддаленими серверами може бути складним процесом. Потрібно враховувати наявність кваліфікованих спеціалістів або можливість співпраці з аутсорсинговими ІТ-партнерами для підтримки серверної інфраструктури.

Використання віддалених серверів, які можуть фізично знаходитись в інших країнах, підпорядковує дані законодавству цих країн. Це може створювати додаткові ризики для збереження конфіденційності інформації.

2.2.3 Оцінка можливих варіантів SIEM

Після розгляду можливих варіантів систем віртуалізації для реалізації та створення інформаційної системи, перейдемо до аналізу можливих варіантів SIEM (Security Information and Event Management) чи подібних систем. SIEM-системи є невід'ємною частиною сучасної кібербезпеки, оскільки вони забезпечують централізований збір, аналіз та кореляцію даних безпеки з різних джерел.

Серед популярних SIEM-систем виділяють Graylog, Wazuh, AlienVault OSSIM та Splunk. Кожна з цих систем має свої особливості та переваги, які можуть бути корисними в різних сценаріях використання.

Graylog — це платформа для збору, індексування та аналізу логів у реальному часі. Вона забезпечує потужний пошук та візуалізацію даних, що дозволяє швидко ідентифікувати та реагувати на інциденти безпеки. Основні особливості Graylog:

- Масштабованість: Підтримує обробку великих обсягів даних.

- Модульність: Можливість розширення функціоналу за допомогою плагінів.
- Інтуїтивний інтерфейс: Зручний веб-інтерфейс для налаштування та моніторингу.

Wazuh — це відкритий агент на базі HIDS (Host Intrusion Detection System), який забезпечує моніторинг цілісності файлів, аналіз логів та виявлення руткітів. Особливості Wazuh:

- Відкрите програмне забезпечення: Безкоштовна ліцензія та активна спільнота.
- Багатоплатформність: Підтримка різних операційних систем.
- Інтеграція з ELK Stack: Можливість використання потужностей Elasticsearch та Kibana для аналізу даних.

AlienVault OSSIM (Open Source SIEM) — це комплексна платформа для управління безпекою, яка об'єднує в собі різні інструменти для виявлення загроз та управління подіями. Ключові характеристики:

- Все-в-одному: Інтеграція різних функцій безпеки в одній платформі.
- Кореляція подій: Потужний механізм для аналізу взаємозв'язків між подіями.
- Підтримка плагінів: Розширення можливостей за рахунок додаткових модулів.

Splunk — комерційна платформа для пошуку, моніторингу та аналізу машинних даних. Вона забезпечує масштабований збір та аналіз логів з різних джерел. Особливості Splunk:

- Висока продуктивність: Швидка обробка великих обсягів даних.
- Аналітика в реальному часі: Миттєве виявлення та реагування на інциденти.
- Підтримка штучного інтелекту: Використання машинного навчання для прогнозування загроз.

Порівнюючи Graylog, Wazuh, AlienVault OSSIM та Splunk, важливо детально розглянути їхні можливості, переваги та недоліки, щоб визначити найкращий варіант для наших потреб. Почнемо з Graylog:

Graylog вирізняється масштабованістю завдяки розподіленій архітектурі, має зручний веб-інтерфейс із можливістю налаштування дашбордів, підтримує плагіни та розширення, а також вирізняється активною спільнотою й невисокими вимогами до ресурсів. Водночас базові функції безпеки та обмежена підтримка стандартів можуть спричинити потребу в додаткових інструментах для виявлення загроз чи відповідності нормативам. Інформація на основі посилання [\[23\]](#).

Wazuh пропонує ширші функції безпеки, зокрема виявлення вторгнень і моніторинг цілісності файлів, а також інтегрується з ELK Stack для поглибленого аналізу даних, що допомагає дотримуватися вимог PCI DSS, HIPAA тощо. Серед недоліків — складність початкового налаштування й обмежена масштабованість, що не завжди підходить для дуже великих середовищ. Інформація на основі посилання [\[15\]](#).

AlienVault OSSIM є комплексним рішенням, яке поєднує SIEM, HIDS, NIDS і аналіз вразливостей, пропонуючи розширену аналітику для кореляції та аналізу подій, а також сприяє відповідності вимогам безпеки. Разом із цим висока складність системи, вимогливість до апаратних ресурсів і менш активна спільнота можуть ускладнити його впровадження та підтримку. Інформація на основі посилання [\[16\]](#).

Splunk славиться швидкістю пошуку й аналізу великих обсягів даних, підтримкою машинного навчання та широкими можливостями інтеграції. Він має професійну технічну підтримку, навчальні ресурси та сповіщення для мобільних пристроїв. Однак висока вартість ліцензій, обслуговування та закритість платформи можуть стати серйозною перешкодою, особливо для організацій, які прагнуть глибокої кастомізації ядра системи.

Таблиця 2.2.2 – Таблиця порівняння SIEM-систем

Критерій	Graylog	Wazuh	AlienVault OSSIM	Splunk
----------	---------	-------	------------------	--------

Ліцензія	Відкрита	Відкрита	Відкрита	Комерційна
Масштабованість	Висока	Середня	Середня	Висока
Інтерфейс користувача	Зручний	Інтуїтивний	Складний	Дружній
Функціонал	Пошук та аналіз логів	HIDS, аналіз логів	SIEM, HIDS, NIDS, аналіз вразливостей	Широкий аналіз даних
Вартість	Безкоштовно	Безкоштовно	Безкоштовно	Платно
Підтримка	Спільнота	Спільнота	Спільнота	Офіційна підтримка

Розширена таблицю порівняння SIEM-систем представлена в [Додатку Б](#).

Поглиблене порівняння SIEM та подібних систем.

- Масштабованість та продуктивність.
- Функціональні можливості.
- Вартість та ліцензування.
- Інтеграція та кастомізація.
- Підтримка та спільнота.
- Відповідність стандартам та безпека.
- Простота використання.

Graylog та Splunk забезпечують високу масштабованість, що важливо для великих підприємств або організацій з великими обсягами даних. Wazuh та AlienVault OSSIM краще підходять для середніх та малих організацій.

Splunk пропонує найширший набір функцій, включаючи машинне навчання та прогнозу аналітику. AlienVault OSSIM надає комплексне рішення з різними інструментами безпеки в одному пакеті. Graylog фокусується на збиранні та аналізі логів, тоді як Wazuh спеціалізується на виявленні вторгнень та моніторингу цілісності.

Відкриті рішення, такі як Graylog, Wazuh та AlienVault OSSIM, є безкоштовними, що знижує початкові витрати. Splunk є комерційним продуктом з високою вартістю, що може бути виправдано лише для великих організацій з відповідним бюджетом

Splunk та Graylog пропонують широкі можливості інтеграції з іншими системами та сервісами. Wazuh добре інтегрується з ELK Stack, що корисно для організацій, які вже використовують цю технологію.

Graylog та Splunk мають великі спільноти та багато доступних ресурсів. Wazuh також підтримується спільнотою, але може мати менше ресурсів порівняно з Graylog.

Wazuh та AlienVault OSSIM надають розширені можливості для відповідності нормативам безпеки, що важливо для регульованих галузей. Splunk також пропонує розширені функції безпеки, але за додаткову вартість.

Graylog та Splunk відомі своїми дружніми інтерфейсами та простотою використання. AlienVault OSSIM може бути складнішим для новачків через свою комплексність.

При виборі SIEM-системи необхідно враховувати конкретні потреби організації, її розмір, бюджет та технічні можливості. Якщо потрібна потужна, масштабована система з розширеними можливостями аналізу і бюджет не є обмеженням, Splunk може бути найкращим вибором. Для організацій, які шукають безкоштовне рішення з хорошими можливостями аналізу логів та простотою використання, Graylog є відмінним варіантом.

Wazuh підійде тим, хто потребує розширених функцій безпеки та відповідності стандартам без значних витрат. AlienVault OSSIM може бути корисним для тих, хто шукає комплексне рішення "все-в-одному", але готовий інвестувати час у його налаштування та освоєння.

2.3 Характеристика обраних технологій для побудови системи поглибленого моніторингу

2.3.1 Функціональні можливості Proxmox Virtual Environment (Proxmox VE)

Після вибору необхідного і більш підходящої нам системи віртуалізації, саме Proxmox VE, можна детально розглянути функціонал і принцип роботи що пропонує нам Proxmox VE.

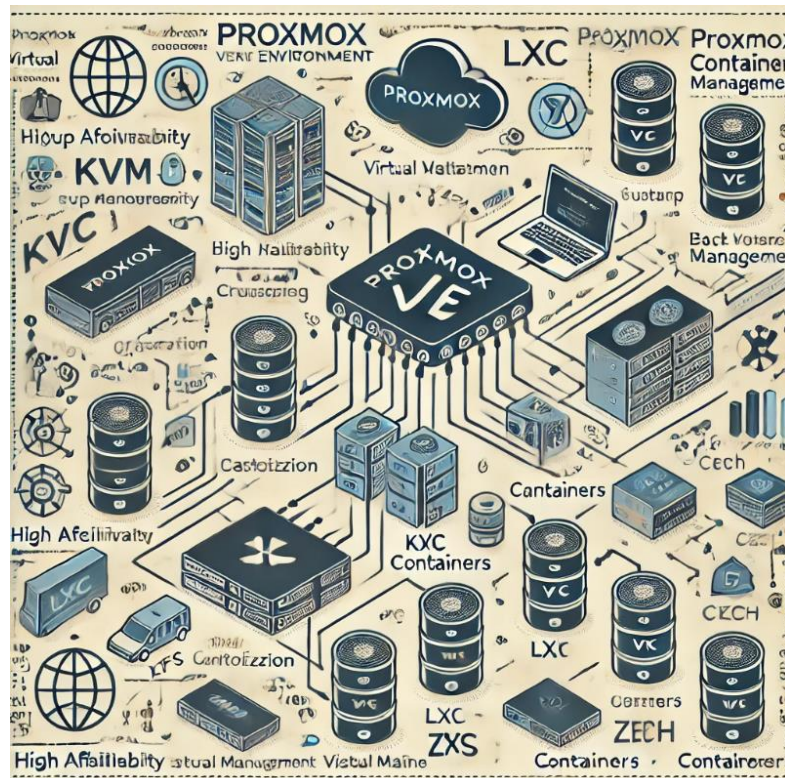


Рисунок 2.2.2 – Загальне представлення функціоналу Proxmox

Proxmox Virtual Environment (Proxmox VE) – це одна з найбільш потужних платформ для віртуалізації та управління серверами з відкритим кодом. Вона надає багато інструментів та функцій, які дозволяють створювати, адмініструвати та масштабувати віртуальні середовища. Proxmox інтегрує кілька рішень для різних типів віртуалізації і зберігання, що робить його ідеальним для малого, середнього і навіть великого бізнесу. Перейдемо до опису основних можливостей Proxmox VE.

KVM (Kernel-based Virtual Machine) є одним з найпопулярніших рішень для повної віртуалізації в Linux. Proxmox VE дозволяє створювати і керувати повноцінними віртуальними машинами (VM) із незалежними операційними системами. Основні можливості віртуалізації на базі KVM включають:

- Підтримка різних ОС: ви можете запускати різні операційні системи (Linux, Windows, BSD тощо) на одній фізичній машині.
- Легке створення VM: за допомогою зручного веб-інтерфейсу ви можете швидко створювати та налаштовувати віртуальні машини.
- Розширене управління ресурсами: налаштування кількості процесорів, пам'яті та дискового простору для кожної віртуальної машини.

На додаток до повної віртуалізації, Proxmox також підтримує контейнеризацію через LXC (Linux Containers). Контейнери використовують ядро операційної системи хоста, що робить їх легшими за віртуальні машини. Переваги контейнеризації включають:

- Ефективність ресурсів: контейнеризація дозволяє використовувати менше системних ресурсів у порівнянні з повною віртуалізацією.
- Швидке розгортання: створення контейнерів відбувається значно швидше, ніж створення VM.
- Легка ізоляція процесів: хоча контейнери використовують загальне ядро, вони повністю ізольовані від інших процесів на хості.

Proxmox VE підтримує функцію високої доступності для критичних сервісів. Це означає, що якщо один з фізичних серверів виходить з ладу, інший сервер в кластері автоматично бере на себе його роль без перерви в роботі. Основні можливості включають:

- Автоматичне перемикання: VM або контейнери переносяться на інший вузол у кластері у разі збою.
- Моніторинг стану кластеру: система постійно моніторить стан кожного вузла і приймає рішення про перемикання в разі несправностей.

Proxmox дозволяє створювати кластер з кількох серверів, об'єднуючи їх для управління як єдиною системою. Це полегшує адміністрування великої кількості віртуальних машин і контейнерів на кількох фізичних серверах.

- Масштабованість: ви можете додати нові фізичні вузли у кластер у будь-який час.
- Централізоване управління: всі вузли кластера керуються через єдиний веб-інтерфейс, що спрощує моніторинг і управління.

Proxmox підтримує кілька рішень для зберігання даних, що дозволяє гнучко керувати ресурсами сховища. Основні типи зберігання:

- ZFS: потужна файлова система з вбудованим управлінням масивами, яка підтримує миттєві знімки, клонування і самовідновлення.
- Ceph: розподілене сховище, яке забезпечує надійність і масштабованість для великих інфраструктур.
- Інші сховища: підтримка традиційних NAS, SAN, iSCSI та NFS для зберігання віртуальних машин і даних.

Proxmox дозволяє налаштовувати мережі для віртуальних машин і контейнерів з різними сценаріями використання:

- Віртуальні локальні мережі (VLAN): ізоляція трафіку для підвищеної безпеки та ефективності.
- Інтерфейси мосту (bridge): дозволяють віртуальним машинам взаємодіяти з фізичною мережею, як окремі фізичні пристрої.
- Балансування навантаження і маршрутизація: можливість розподіляти навантаження між кількома мережевими інтерфейсами.

Proxmox дозволяє легко інтегрувати віртуалізовані середовища з хмарними сервісами та провайдерами, такими як:

- Amazon Web Services (AWS): можливість створювати резервні копії або відправляти знімки на AWS.
- Google Cloud: інтеграція для збереження даних або масштабування хмарної інфраструктури.

Proxmox забезпечує гнучку систему ролей і прав доступу, що дозволяє адміністраторам налаштовувати доступ до системи для різних користувачів і груп:

- LDAP та Active Directory: інтеграція з існуючими системами автентифікації для централізованого управління доступом.
- Шифрування: підтримка шифрування для захисту конфіденційних даних.
- Багаторівнева автентифікація (2FA): підвищення безпеки через використання двофакторної аутентифікації.

Proxmox пропонує повноцінне REST API, яке дозволяє автоматизувати всі аспекти управління віртуальними машинами та контейнерами, включаючи їх створення, резервування, управління ресурсами тощо. Це корисно для великих підприємств і DevOps-процесів.

2.3.2 Обґрунтування вибору системи SIEM

Після детального аналізу та порівняння представлених SIEM-систем, обираємо Graylog для реалізації нашої інформаційної системи. Це зумовлено такими причинами:

- Відкрита ліцензія: Дозволяє використовувати систему без додаткових витрат.
- Масштабованість: Підходить для обробки великих обсягів даних, що важливо для нашої системи.
- Зручний інтерфейс: Полегшує процес налаштування та моніторингу.
- Модульність: Можливість розширення функціоналу відповідно до потреб.

Таким чином, Graylog є хорошим вибором для нашої інформаційної системи, оскільки поєднує в собі необхідний функціонал, масштабованість та зручність використання.

Висновки: у другому розділі було проведено комплексне проектування інформаційної системи управління інцидентами, включаючи визначення її цілей, задач, основних принципів побудови та аналізу технологічних рішень. Розроблена організаційна структура та IT-інфраструктура спрямовані на забезпечення

ефективного управління інцидентами, підвищення продуктивності та безпеки бізнес-процесів. Було розглянуто необхідні технології для побудови інформаційної системи, серед вибраних варіантів було проведено порівняння, на основі проведеного порівняння був здійснений вибір кращого варіанту який задовольняє необхідні для інформаційної системи вимоги.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ ПОГЛИБЛЕНОГО МО- НИТОРИНГУ ЗАХИЩЕНОЇ ВІРТУАЛІЗОВАНОЇ ІТ-ІНФРАСТРУКТУРИ ПІД- ПРИЄМСТВА НА ОСНОВІ GRAYLOG, MIKROTIK ТА PROXMOX VE

3.1 Реалізація базової ІТ-інфраструктури для моделювання поглибленої системи моніторингу

В проєкті використаний один віртуальний маршрутизатор Mikrotik. Маршрутизатор розгорнутий як віртуальна машина на сервері. Основними використаними функціями маршрутизатора MikroTik є NAT та VPN (Wireguard), протоколи типу DHCP та syslog.

Використана версія CHR, вона має увесь набір можливостей RouterOS – це маршрутизація, брандмауер, VPN, QoS, хотспоти, MPLS, BGP, OSPF, CAPsMAN та інші мережеві сервіси та легко розгортається на гіпервізорі.

Налаштуємо протокол DHCP на маршрутизаторі MikroTik.

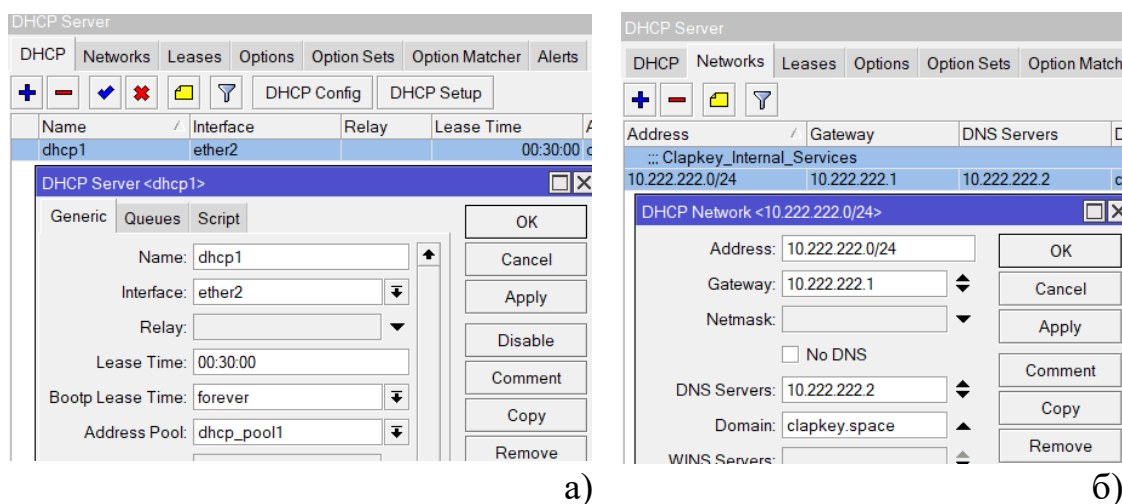


Рисунок 3.1 – Налаштування протоколу DHCP: а) DHCP Server,
б) DHCP Network

Налаштування протоколу DHCP доволі просте, тому не будемо загострювати увагу на ньому. Перейдемо до налаштування NAT, кожній сучасній мережі необхідний доступ до мережі Інтернет, тому NAT налаштувати необхідно. Налаштування NAT на маршрутизаторах MikroTik, ще простіше ніж налаштування DHCP, необхідно налаштувати вихідний інтерфейс та вказати тип NAT (masquerade).

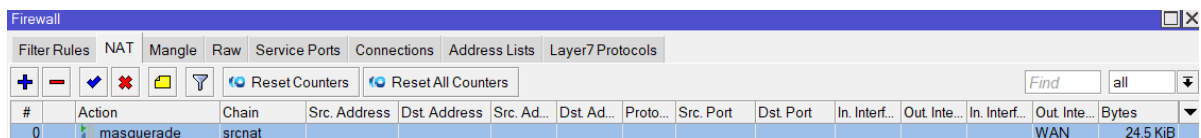
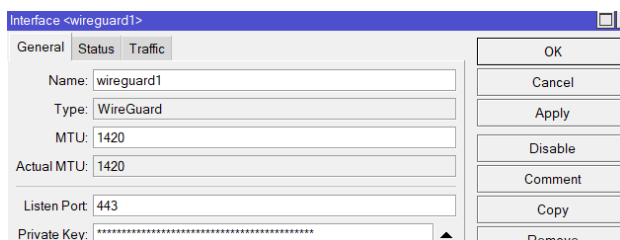
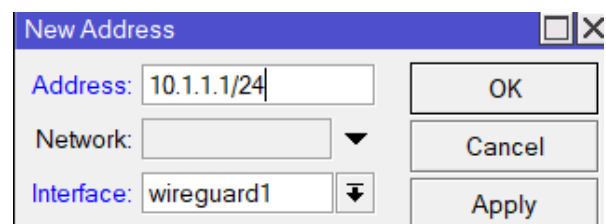


Рисунок 3.2 – Налаштування протоколу NAT

Одним з основних використаних протоколів – це протокол Wireguard. За допомогою Wireguard буде отриманий доступ у внутрішню мережу і дозволить користувачам отримувати доступ до внутрішніх ресурсів серверу. Налаштування більш цікаве, тому пройдемося детальніше. Створимо спочатку Wireguard інтерфейс і назначимо йому адресу.



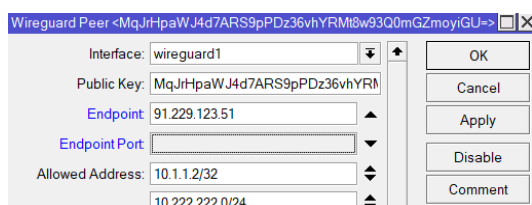
а)



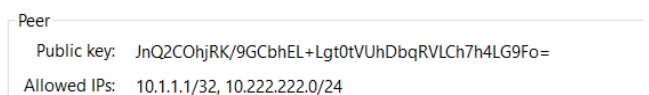
б)

Рисунок 3.3 – Створення Wireguard інтерфейсу: а) створення інтерфейсу, б) присвоєння адреси

Після цього нам необхідно створити Peer на сервері і клієнті. Peer означає будь-який пристрій, який бере участь у VPN-з'єднанні. Для цього необхідно об'єднатися відкритими ключами.



а)



б)

Рисунок 3.4 – Налаштування Peer: а) на сервері, б) на клієнті

Обмеження доступу тільки для конкретної адреси у налаштованого піра. Перевіримо налаштування, спробуємо підключитися до хостів у внутрішній мережі.

```
PS C:\Users\ABOBUS> ping 10.222.222.100

Pinging 10.222.222.100 with 32 bytes of data:
Reply from 10.222.222.100: bytes=32 time=54ms TTL=63
Reply from 10.222.222.100: bytes=32 time=55ms TTL=63
Reply from 10.222.222.100: bytes=32 time=56ms TTL=63

Ping statistics for 10.222.222.100:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 56ms, Average = 55ms
Control-C
PS C:\Users\ABOBUS>
```

а)

```
PS C:\Users\ABOBUS> ping 10.222.222.1

Pinging 10.222.222.1 with 32 bytes of data:
Reply from 10.222.222.1: bytes=32 time=111ms TTL=64
Reply from 10.222.222.1: bytes=32 time=55ms TTL=64
Reply from 10.222.222.1: bytes=32 time=55ms TTL=64

Ping statistics for 10.222.222.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 55ms, Maximum = 111ms, Average = 73ms
Control-C
```

б)

Рисунок 3.5 – Перевірка доступу до внутрішньої мережі через VPN: а) до серверу, б) до внутрішнього порту маршрутизатора

Доступ у внутрішню мережу отриманий і тепер можна взаємодіяти з ресурсами серверу віддалено. Спроба підключення до Graylog серверу через SSH.

```
PS C:\Users\ABOBUS> ssh grayserv@10.222.222.100
The authenticity of host '10.222.222.100 (10.222.222.100)' can't be established.
ED25519 key fingerprint is SHA256:cj8s96j6QdE/8y1FX8V6qjiHxiHReUwG6ocH+ojgDj8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.222.222.100' (ED25519) to the list of known hosts.
grayserv@10.222.222.100's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-126-generic x86_64)

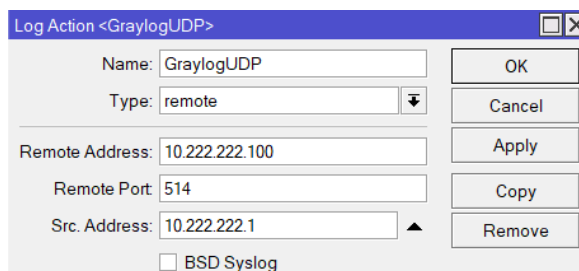
Last login: Mon Dec  9 10:43:44 2024
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

grayserv@grayserv:~$
```

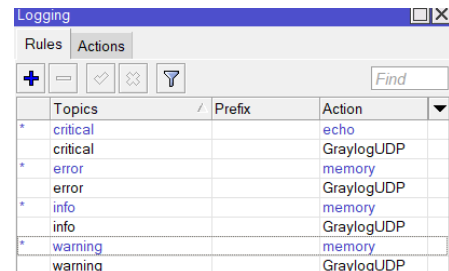
Рисунок 3.6 – Підключення через SSH

Підключення успішне, тепер можна зручно керувати сервери через CLI.

Тепер налаштуємо передачу логів на наш Graylog Server за допомогою протоколу syslog. Для цього створимо Action для передачі логів по протоколу syslog та налаштуємо що саме він буде передавати.



а)



б)

Рисунок 3.7 – Налаштування логування на MikroTik: а) налаштування action, б) вибір логів для відправлення

Після цього усі основні категорії логів повинні передаватися на Graylog Server.

3.2 Реалізація системи централізованого збору, обробки та аналізу логів у віртуалізованій IT-інфраструктурі

Розглянемо основні моменти впровадження Graylog у інформаційну систему. Graylog підтримує створення багатонодової системи, тобто є можливість створити по серверу у кожній мережі та об'єднати їх у одну систему, але ми розглядаємо лише одну мережу на основі одного фізичного серверу, тому ми використаємо розгортання в режимі standalone, тобто один Graylog сервер.

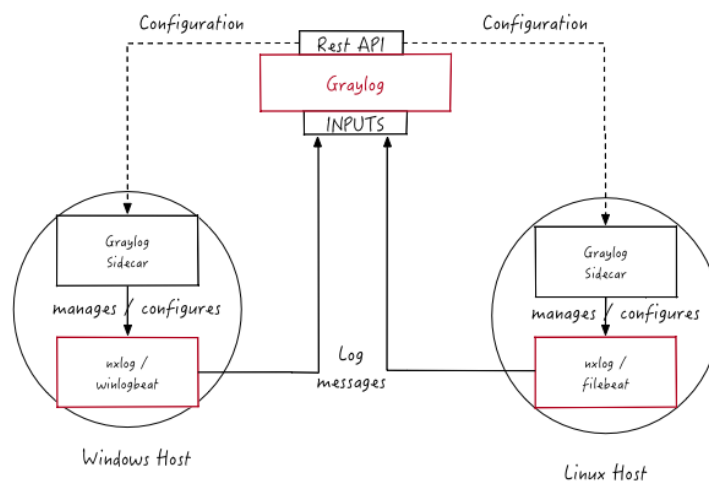


Рисунок 3.8 – Архітектура Sidecar

Розглянемо архітектуру Graylog sidecar, агентів для збирання логів, їх принцип роботи та їх спосіб їх використання у інформаційній мережі. Архітектура Sidecar базується на тому, що вузол Graylog виступає в ролі централізованого хабу зберігання конфігурацій для колекторів журналів. Демон Sidecar періодично отримує актуальні конфігурації через REST API для зазначеної цілі. Під час першого запуску або при виявленні змін у налаштуваннях Sidecar автоматично формує необхідні файли конфігурації серверів і після цього перезапускає відповідні колектори журналів. Усі параметри роботи колекторів керуються централізовано за допомогою веб-інтерфейсу Graylog.

Graylog Sidecar може працювати як служба (на Windows-хості) або як демон (на Linux-хості) на пристроях, що відповідають за генерацію повідомлень.

Відповідно до Рисунку 3.8 можна побачити, що Sidecar використовує 2 з'єднання для функціонування. З'єднання через REST API для встановлення конфігурації внутрішнього збирача логів та з'єднання через попередньо налаштований INPUT (вхід для логів, налаштований на Graylog сервері).

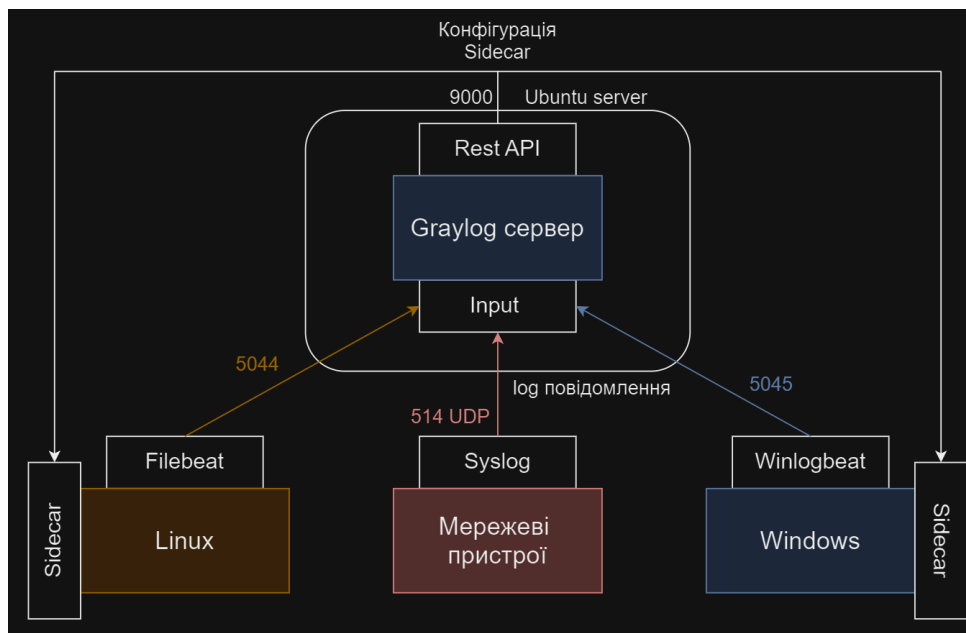


Рисунок 3.9 – Використання Graylog у системі

Використано стандартний порт 9000 для налаштування конфігурацій, а для хостів ми будемо використовувати:

- Для Linux хостів ми будемо використовувати Filebeat для збирання логів, для отримання логів на Graylog сервері ми налаштуємо окремий Input на порті 5044.
- Для Windows хостів ми будемо використовувати Winlogbeat для збирання логів, для отримання логів на Graylog сервері ми налаштуємо окремий Input на порті 5045.

Належно відмітити, Winlogbeat надає набагато ширше представлення про подію, тому для Filebeat подібно буде додатково створити екстрактори.

Екстрактор в Graylog — це інструмент, який автоматизує процес виокремлення та структурування даних із вхідних журналів. Він застосовується до вхідних повідомлень, які надходять до Graylog, і дозволяє перетворювати неструктурований текст у структуровані поля, полегшуючи подальший аналіз, пошук та візуалізацію даних.

Для мережевих пристроїв використано протокол **syslog** для збирання логів, для цього створено окремий Input для мережевих пристроїв на порті 514 UDP. Для мережевих пристроїв також необхідно буде створити екстрактори.

Закінчили з теоретичними питання, перейдемо до практичної реалізації. Для початку нам необхідно створити віртуальну машину для Graylog серверу, створимо VM на базі ОС Linux Ubuntu server.

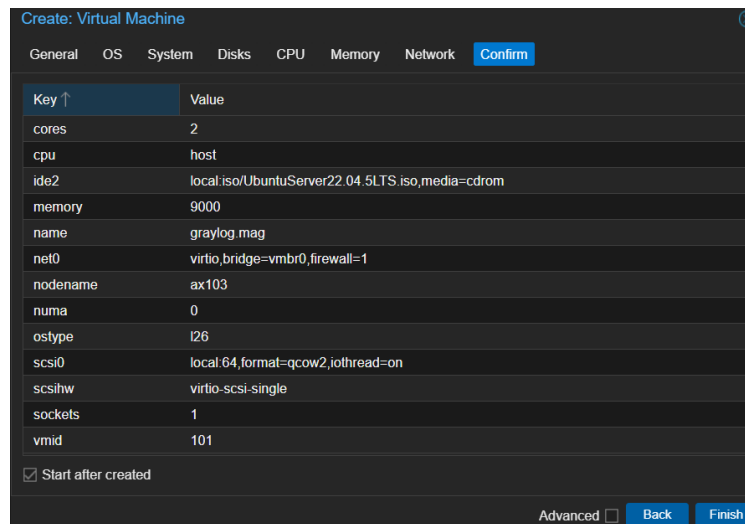


Рисунок 3.10 – Створення VM для Graylog серверу

Встановлення ОС Linux на VM створену Proxmox нічим не відрізняється від звичайного встановлення або встановлення на іншій системі віртуалізації, тому встановлення ОС ми пропустимо.

Переходимо до встановлення Graylog, для цього використаємо офіційну документацію [\[19\]](#), у роботі представлено лише основні моменти.

Розглянуто встановлення основних компонентів. Спочатку нам необхідно встановити MongoDB, слід зауважити що версія MongoDB має бути вище 5.0.7.

```
root@grayserv:/home/grayserv# systemctl status mongod.service
● mongod.service - MongoDB Database Server
   Loaded: loaded (/lib/systemd/system/mongod.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-12-10 12:01:09 UTC; 41s ago
     Docs: https://docs.mongodb.org/manual
   Main PID: 4602 (mongod)
    Memory: 68.1M
       CPU: 273ms
    CGroup: /system.slice/mongod.service
            └─4602 /usr/bin/mongod --config /etc/mongod.conf

Dec 10 12:01:09 grayserv systemd[1]: Started MongoDB Database Server.
Dec 10 12:01:09 grayserv mongod[4602]: {"t":{"$date":"2024-12-10T12:01:09.866Z"},"s":"I",  "c":"CONTROL",  "id":7484500
lines 1-12/12 (END)
```

Рисунок 3.11 – Встановлений MongoDB

Встановлення Graylog Data Node, раніше використовувався Elasticsearch (в нових версіях OpenSearch), в останніх версіях Graylog перейшов на Graylog Data Node, модифікований OpenSearch.

```
root@grayserv:/home/grayserv# sudo systemctl status graylog-datanode.service
● graylog-datanode.service - Graylog data node
   Loaded: loaded (/lib/systemd/system/graylog-datanode.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-12-10 12:13:06 UTC; 7s ago
     Docs: http://docs.graylog.org/
    Main PID: 5375 (java)
      Tasks: 52 (limit: 10333)
     Memory: 428.4M
        CPU: 7.098s
    CGroup: /system.slice/graylog-datanode.service
            └─5375 /usr/share/graylog-datanode/jvm/bin/java -Dlog4j.configurationFile=file:///etc/graylog/datanode/log
Dec 10 12:13:06 grayserv systemd[1]: Started Graylog data node.
```

Рисунок 3.12 – Встановлений Graylog Data Node

Встановлення Graylog Server, існує ще версія Graylog Enterprise, але вона потребує ліцензію, тому її ми не використовуємо.

```
Get:1 https://downloads.graylog.org/repo/debian stable/6.1 amd64 graylog-server amd64 6.1.4-2 [321 MB]
Fetched 321 MB in 9s (35.8 MB/s)
Selecting previously unselected package graylog-server.
(Reading database ... 76789 files and directories currently installed.)
Preparing to unpack .../graylog-server_6.1.4-2_amd64.deb ...
Unpacking graylog-server (6.1.4-2) ...
Setting up graylog-server (6.1.4-2) ...
#####
Graylog does NOT start automatically!

Please run the following commands if you want to start Graylog automatically on system boot:

    sudo systemctl enable graylog-server.service

    sudo systemctl start graylog-server.service

#####
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@grayserv:/home/grayserv#
```

Рисунок 3.13 – Встановили Graylog Server

Після встановлення проведено базове налаштування, згенеровано пароль та хеш, і записані у файл конфігурації. Паролі збережені.

```
password_secret =
ZzPAYKy33EkuRXVmyIhRgMUlNrDut2JCjyPoV0lp179IcLjLwTu2bC6xhA6eLePnhZ3DZkdoj
lbHTjbDZlJcp63cYybs8iXD
Enter Password: aboba
a6c79a27049109e472b246b5dfbe08aedff1e9e2259597e54032dbad4958d4ad
```

```

GNU nano 6.2 /etc/graylog/server/server.conf *
# If you are running more than one instances of Graylog server you have to select one of these
# instances as leader. The leader will perform some periodical tasks that non-leaders won't perform.
is_leader = true

# The auto-generated node ID will be stored in this file and read after restarts. It is a good idea
# to use an absolute file path here if you are starting Graylog server from init scripts or similar.
node_id_file = /etc/graylog/server/node-id

# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 64 characters.
# Generate one by using for example: pwgen -N 1 -s 96
# ATTENTION: This value must be the same on all Graylog nodes in the cluster.
# Changing this value after installation will render all user sessions and encrypted values in the database invalid
password_secret = ZzPAYKy33EkurXVmyIhRgMULNrDut2JCjyPoV0lp179IcLjLwTu2bC6xhA6eLePnhZ3DZkdojlbHTjbDZLJcp63cYybs8iXD

# The default root user is named 'admin'
#root_username = admin

# You MUST specify a hash password for the root user (which you only need to initially set up the
# system and in case you lose connectivity to your authentication backend)
# This password cannot be changed using the API or via the web interface. If you need to change it,
# modify it in this file.
# Create one by using for example: echo -n yourpassword | shasum -a 256
# and put the resulting hash value into the following line
root_password_sha2 = bc18bfee48c230318c44a4420fd7714258bac0f014fd7c9b67e2d498535aaa81

```

Рисунок 3.14 – Налаштування конфігураційного файлу

Graylog Server встановлений, але необхідно перейти у логи серверу і знайти пароль адміністратора. Така особливість з’являється коли використовується Graylog Data Node при розгортанні.

```

root@grayserv:/home/grayserv# tail -f /var/log/graylog-server/server.log
=====
It seems you are starting Graylog for the first time. To set up a fresh install, a setup interface has
been started. You must log in to it to perform the initial configuration and continue.

Initial configuration is accessible at 10.222.222.100:9000, with username 'admin' and password 'vwEUJGieSu'.
Try clicking on http://admin:vwEUJGieSu@10.222.222.100:9000
=====

```

Рисунок 3.15 – Пароль адміністратора для розгортання

При переході за адресою сервера і бачимо де потрібно ввести цей пароль.

Рисунок 3.16 – Пароль адміністратора для розгортання

Після цього необхідно налаштувати Certificate Authority на Graylog Data Node, для цього введено назву організації, встановлено терміни дії сертифікату та тип його оновлення. Назву організації яка використана – записана.

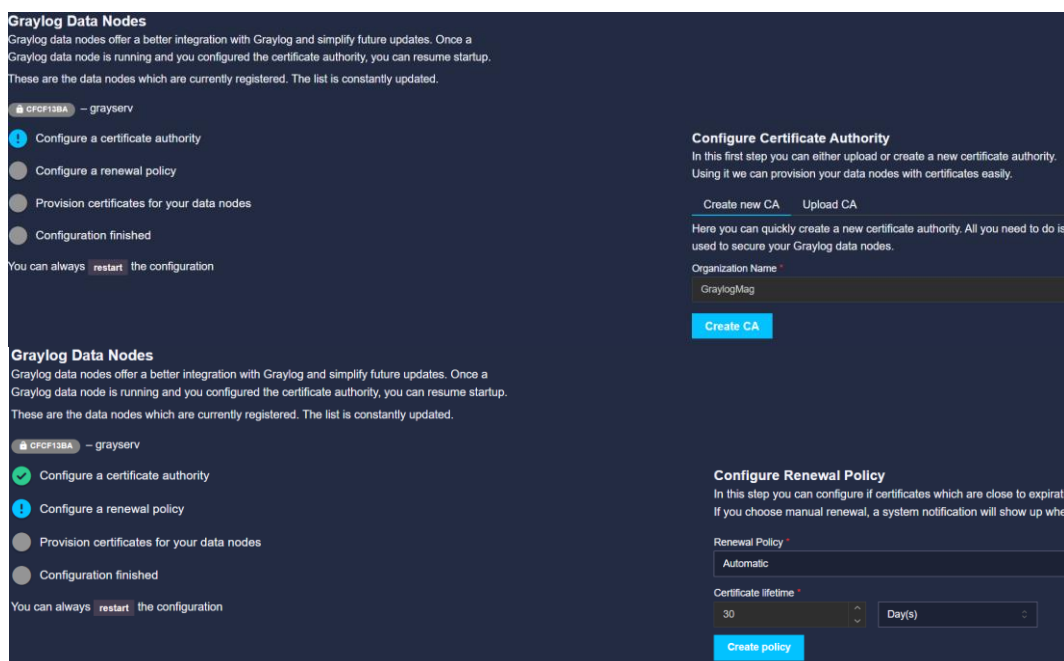


Рисунок 3.17 – Розгортання Certificate Authority на Graylog

Graylog успішно встановлений, переходимо до налаштування інфраструктури для роботи з логами. Використано для швидкого налаштування роботи з логами MikroTik мій Content Pack, автором якого є я. Content Pack в Graylog — це набір налаштувань і конфігурацій, які можна експортувати з одного середовища Graylog і імпортувати в інше. Контент-паки зазвичай використовуються для збереження й поширення налаштувань потоків, дашбордів, алертів, правил обробки даних та інших елементів. Більш детально можна дізнатися про структуру логів у Graylog по посиланню [20].

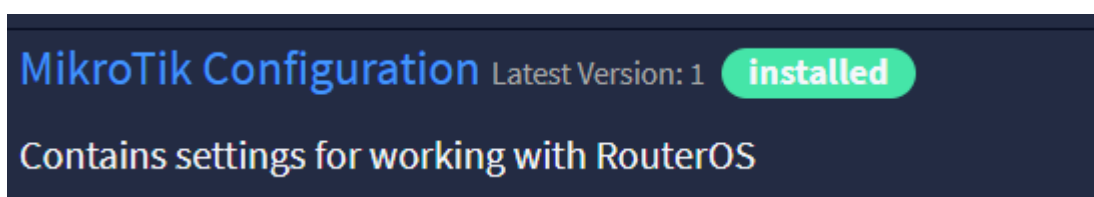


Рисунок 3.18 – Встановлення Content Pack

Використовувати Content Pack дуже зручно для перенесення конфігурацій між сервера Graylog. Після встановлення розберемо що входить у цей Content Pack і для чого використовується наявний функціонал. Мій Content Pack для MikroTik встановлює Input для прийому логів на порт 514.

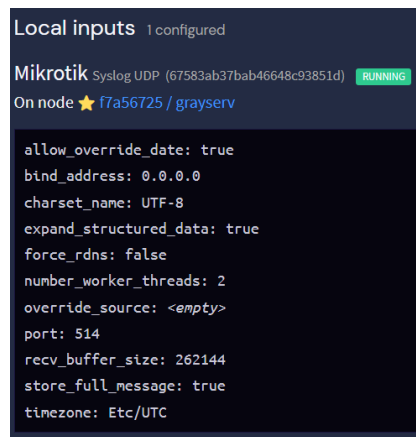


Рисунок 3.19 – Створений Input для Syslog

Саме на цей Input буде відправляти повідомлення MikroTik маршрутизатор. Налаштований окремий Stream, дане налаштування не лише допоможе у налаштуваннях Dashboards або Pipelines, а і сегментувати трафік.

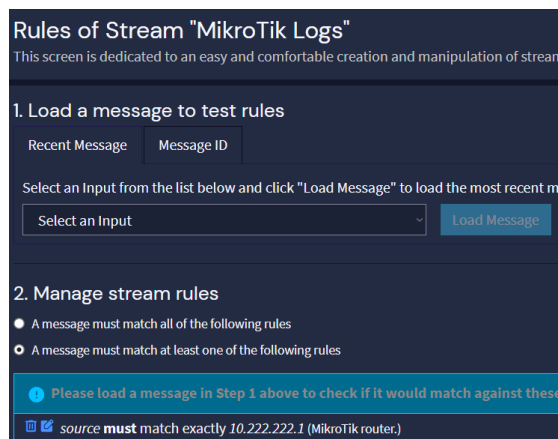


Рисунок 3.20 – Створений Input для Syslog

За замовчуванням у Graylog не має попереднє створених екстракторів для повідомлень MikroTik. Тобто виводиться лише саме повідомлення, а не розбирається на поля. За відсутності полів неможливо створювати Dashboards, тому необхідно написати патерн для повідомлень і на основі патернів створити екстрактор. Можна скористатися вже привичними регулярними виразами або використати Grok патерн.

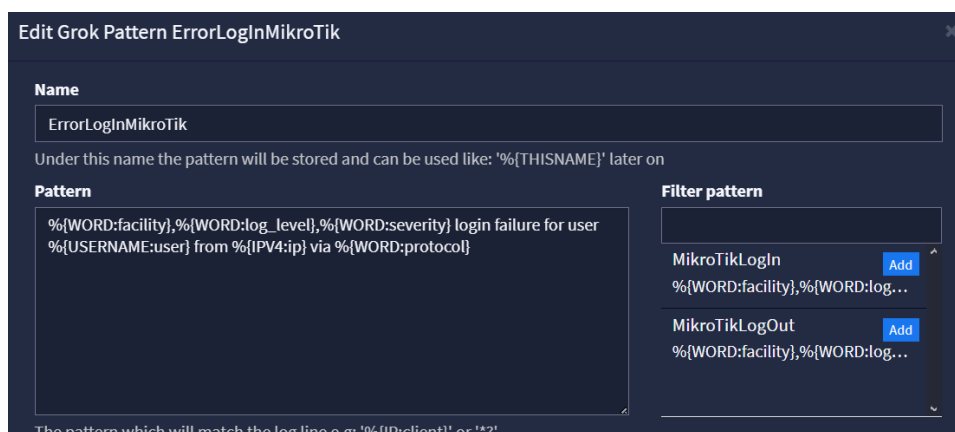


Рисунок 3.21 – Створення Grok патерну

Приклад Grok патерну для syslog повідомлення від MikroTik. Далі створено екстрактор і там використано цей патерн, у Graylog екстрактори прив'язуються до створених Input.



Рисунок 3.22 – Створений екстрактор

При створенні екстрактора використано раніше створений Grok патерн для виводу полів з повідомлення. Приведено приклад результату налаштувань.

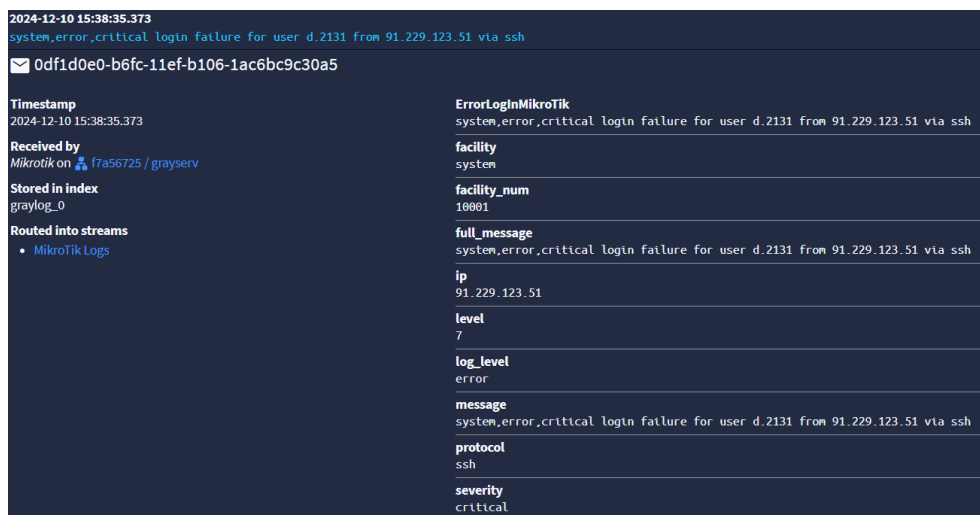


Рисунок 3.23 – Повідомлення про помилку входу

Розглянуто основні необхідні налаштування для отримання логів з мережевих пристроїв для яких нема налаштованих раніше екстракторів. Налаштовані поля можна використати в майбутньому.

Був розглянут приклад налаштувань для роботи з мережевими пристроями без попередньо налаштованих екстракторів. Переходимо до розгляду налаштувань роботи з повноцінними комп'ютерами, серверами або віртуальними машинами. Спочатку налаштовано роботу з VM на базі ОС Linux. Для цього необхідно встановити Graylog Sidecar та Filebeat, також провести їх налаштування. Для початку встановлено Graylog Sidecar, встановлено на Graylog Server. Повне розгортання можна розглянути в офіційному мануалі Graylog [21]. Також в цілому дізнатися про Graylog Sidecar можна дізнатися по [22]. Спочатку створюється API токен для сайдкарів, можна використати один токен на всі хости або сегментувати. Буде створюватися окремі токени для різних типів пристроїв.

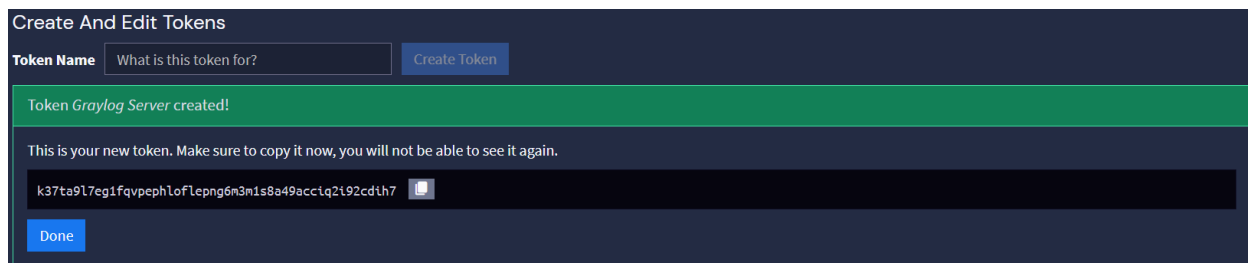


Рисунок 3.24 – Створення API токenu

Після встановлення Graylog Sidecar на Linux клієнт, у конфігураційні файлах налаштовується адреса серверу та API токен.

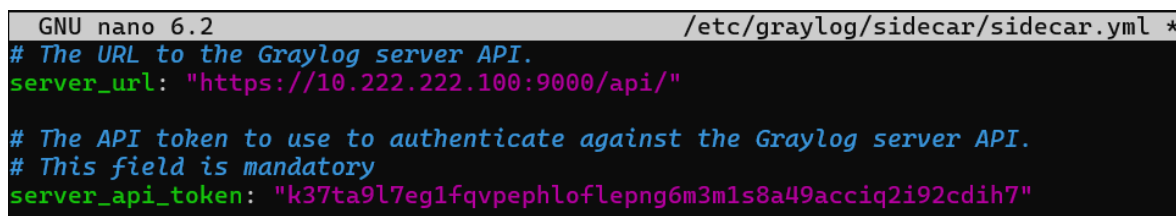


Рисунок 3.25 – Налаштування Graylog Sidecar ОС Linux

Після цього встановлюється Filebeat і на цьому налаштування на клієнті завершено. Далі необхідно на Graylog Server налаштувати конфігурацію Filebeat.

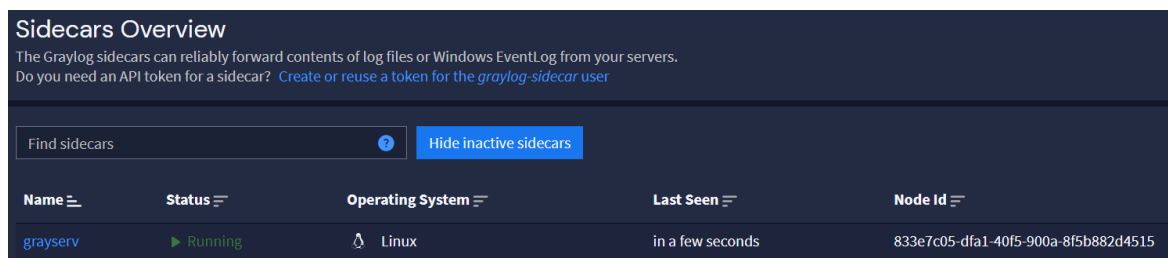


Рисунок 3.26 – Підключений Graylog Sidecar ОС Linux

Далі налаштується конфігурація Filebeat для збирання логів.

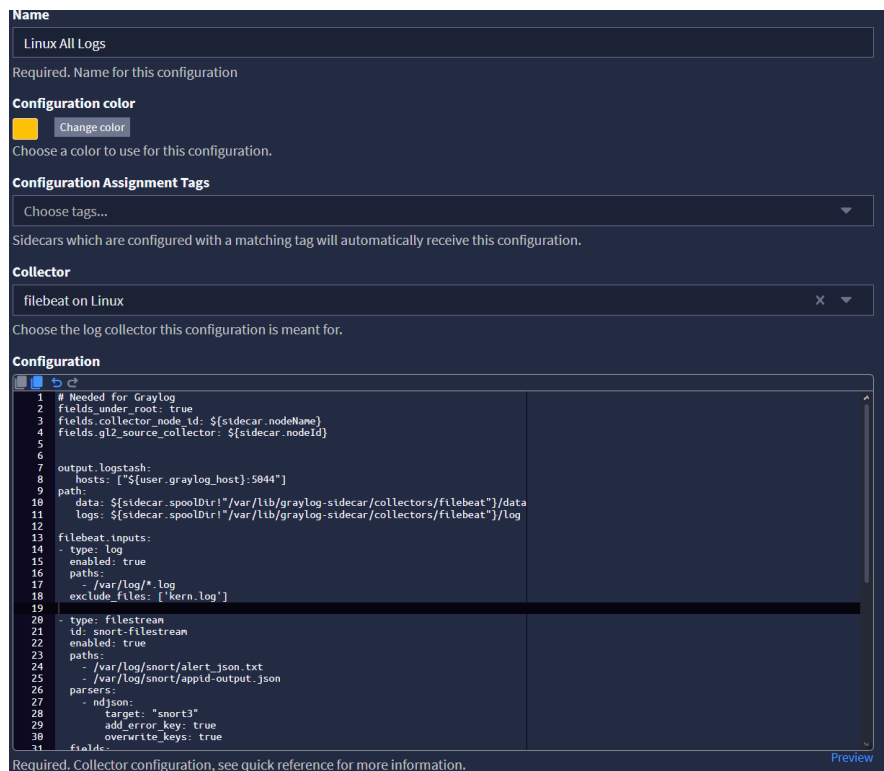


Рисунок 3.27 – Підключений Graylog Sidecar ОС Linux

Дана конфігурація збирає усі логи з папки /var/log/ і ігнорує логи ядра. Перевіримо роботу.

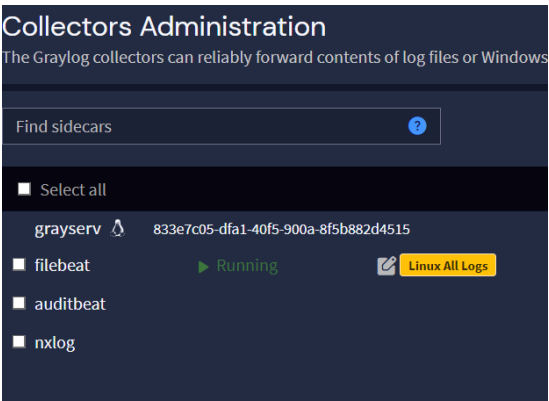


Рисунок 3.28 – Налаштована конфігурація Filebeat Graylog Sidecar ОС Linux

Переглянемо працездатність механізму збирання логів.

timestamp	source
2024-12-10 18:33:50.406	grayerv
Dec 10 16:33:46 grayerv sshd[9427]: Connection reset by authenticating user grayerv 10.1.1.2 port 58999 [preauth]	grayerv
2024-12-10 18:33:50.406	grayerv
Dec 10 16:33:45 grayerv sshd[9427]: Failed password for grayerv from 10.1.1.2 port 58999 ssh2	grayerv
2024-12-10 18:33:50.406	grayerv
Dec 10 16:33:43 grayerv sshd[9427]: pam_unix(sshd:auth): authentication failure; logname= utd=0 euid=0 tty=ssh ruser= rhost=10.1.1.2 user=grayerv	grayerv
2024-12-10 18:24:46.821	grayerv
2024-12-10 16:18:20 status installed filebeat:amd64 8.16.1	grayerv
2024-12-10 18:24:46.821	grayerv
2024-12-10 16:18:20 status half-configured filebeat:amd64 8.16.1	grayerv
2024-12-10 18:24:46.821	grayerv
2024-12-10 16:18:20 status unpacked filebeat:amd64 8.16.1	grayerv

Рисунок 3.29 – Отримані повідомлення за допомогою Filebeat

Переходимо до розгортання Graylog Sidecar на клієнті працюючому на базі ОС Windows, ознайомитися з мануалом можна за посиланням [\[22\]](#).

Встановлення на сайдкару на операційну систему Windows подібне до Linux, розберемо основні моменти.

Для завантаження sidecar необхідно перейти на сторінку [github](#) і завантажити [graylog_sidecar_installer_1.5.0-1.exe](#)

Assets 14		
CHECKSUMS-SHA256.txt	1.07 KB	Oct 26, 2023
graylog-sidecar-1.5.0-1.arm64.rpm	51.9 MB	Oct 26, 2023
graylog-sidecar-1.5.0-1.armv7.rpm	2.8 MB	Oct 26, 2023
graylog-sidecar-1.5.0-1.i386.rpm	48.5 MB	Oct 26, 2023
graylog-sidecar-1.5.0-1.x86_64.rpm	58 MB	Oct 26, 2023
graylog-sidecar-1.5.0.tar.gz	137 MB	Oct 26, 2023
graylog-sidecar.1.5.0.1.nupkg	3.84 KB	Oct 26, 2023
graylog-sidecar_1.5.0-1_amd64.deb	58.7 MB	Oct 26, 2023
graylog-sidecar_1.5.0-1_arm64.deb	52.3 MB	Oct 26, 2023
graylog-sidecar_1.5.0-1_armv7.deb	2.82 MB	Oct 26, 2023
graylog-sidecar_1.5.0-1_i386.deb	48.9 MB	Oct 26, 2023
graylog_sidecar_installer_1.5.0-1.exe	72.3 MB	Oct 26, 2023
Source code (zip)		Oct 26, 2023
Source code (tar.gz)		Oct 26, 2023

Рисунок 3.30 – Репозиторій Graylog Sidecar на GitHub

Під час встановлення введені базові параметри server_url і server_api_token.

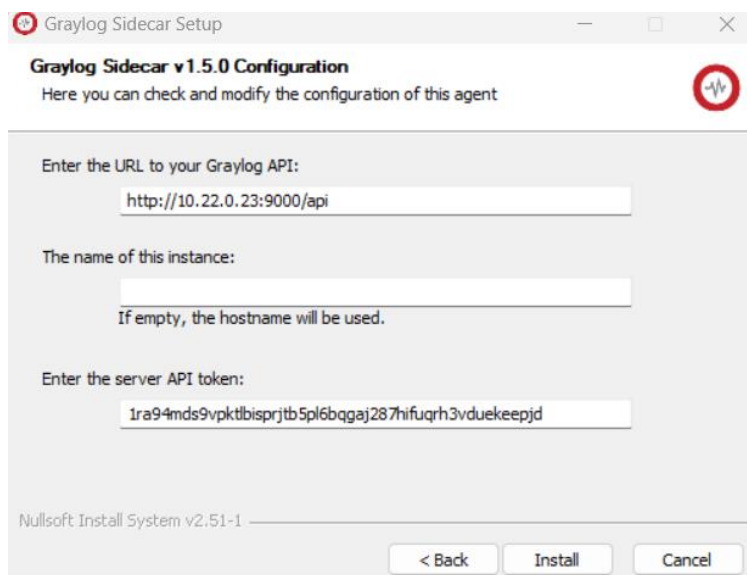


Рисунок 3.31 – Встановлення Graylog Sidecar на ОС Windows

Під час встановлення Graylog Sidecar разом з ним автоматично встановлюються агенти для збору логів, такі як Filebeat та Winlogbeat. Це дозволяє без додаткових налаштувань збирати системні логи, журнали подій Windows та інші важливі дані з хостів. Оскільки агенти вже встановлені під час налаштування сайдкару, додатково встановлювати Filebeat або Winlogbeat не потрібно.

Також налаштовано сайдкар як сервіс, для цього використано PowerShell:

```
"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service  
install
```

```
"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service  
start
```

Тепер, щоб налаштувати сайдкар або змінити його параметри, потрібно відредагувати конфігураційний файл `sidecar.yml`, який знаходиться за шляхом:

`C:\Program Files\Graylog\sidecar\sidecar.yml`

```
# The URL to the Graylog server API.  
# Default: "http://127.0.0.1:9000/api/"  
server_url: "http://10.22.0.23:9000/api"  
  
# The API token to use to authenticate against the Graylog server API.  
# Default: none  
server_api_token: "1ra94mds9vpktlbisprjtb5pl6bqgaj287hifuqrh3vduekeepjd"
```

Рисунок 3.32 – Конфігураційний файл Graylog Sidecar на ОС Windows

Переходимо до налаштування конфігурації, подібно до налаштувань системи Linux налаштування конфігурацій проводиться на сервері. Для налаштування конфігурації нам потрібен Input, допускається використання вже створений раніше або, краще, створити новий, інструкція наведена вище. Переходимо у створення конфігурації Collectors Configuration (System/Sidecars), спочатку необхідно завантажити конфігурацію за замовчуванням для winlogbeat on windows, для мінімальної роботи необхідно налаштувати, подібно до Filebeat, поля:

- Name
- output.logstash:
hosts: ["10.222.222.100:5045"]

Цих налаштувань досить для роботи колектора по збиранню логів.

3.3 Налаштування Graylog для роботи з віддаленим сервером Proxmox VE

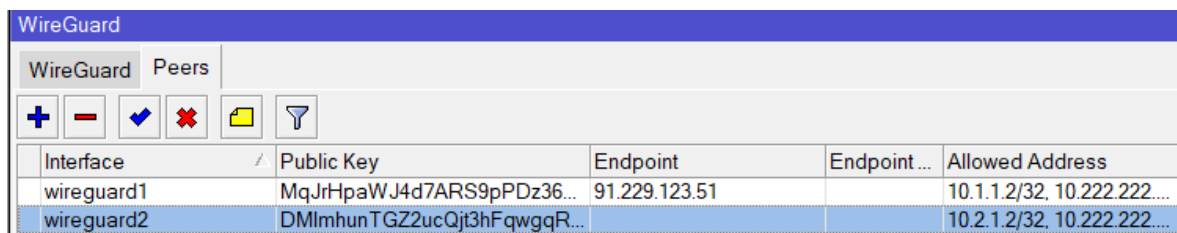
Також необхідно провести налаштування для роботи з самим сервером на якому розміщуються усі віртуальні машини. Для цього необхідно встановити Graylog Sidecar на Proxmox Server, але є декілька проблем. Перша проблема, Proxmox Server знаходиться у зовнішній мережі, а Graylog Server у внутрішній. Для налагодження зв'язку між цими хостами налагоджено VPN. VPN був використаний раніше для підключення користувачів, створено новий для підключення зовнішніх серверів.

WireGuard

WireGuardPeers

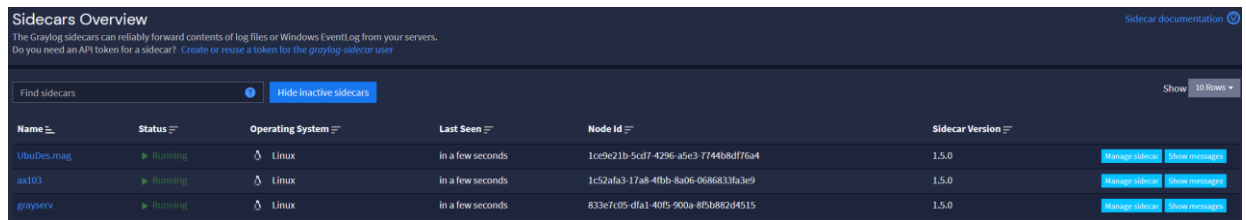
	Name	Type	MTU	Actual MTU	Listen Port	Private Key	Public Key
R	 wireguard1	WireGuard	1420	1420	443	*****	JnQ2C0hjRK/9GCbhEL+Lgt0tV...
R	 wireguard2	WireGuard	1420	1420	444	*****	qB6Zasu6WithYaHYmA85v76v...

Рисунок 3.33 – Налаштування VPN для Proxmox Server, створений інтерфейс



WireGuard				
WireGuard		Peers		
+	-	✓	✗	📁
Interface	Public Key	Endpoint	Endpoint ...	Allowed Address
wireguard1	MqJrHpaWJ4d7ARS9pPDz36...	91.229.123.51		10.1.1.2/32, 10.222.222...
wireguard2	DmImhunTGZ2ucQjt3hFqwgqR...			10.2.1.2/32, 10.222.222...

Рисунок 3.34 – Налаштування VPN для Proxmox Server, налаштований peer
 Налаштовано Proxmox Server як Wireguard Client. Після цього отримано зв'язок між хостами, перевірено працездатність у Graylog.



Sidecars Overview						
The Graylog sidecars can reliably forward contents of log files or Windows EventLog from your servers. Do you need an API token for a sidecar? Create or reuse a token for the graylog-sidecar user						
Name	Status	Operating System	Last Seen	Node ID	Sidecar Version	
ubuDes.mag	▶ Running	Linux	in a few seconds	1ce9e21b-5cd7-4296-a5e3-7744b8df76a4	1.5.0	Manage sidecar Show message
ax103	▶ Running	Linux	in a few seconds	1c52afa3-17a8-4fbb-8a06-0686833fa3e9	1.5.0	Manage sidecar Show message
graylog	▶ Running	Linux	in a few seconds	833e7c05-dfa1-40f5-900a-8f5b882d4515	1.5.0	Manage sidecar Show message

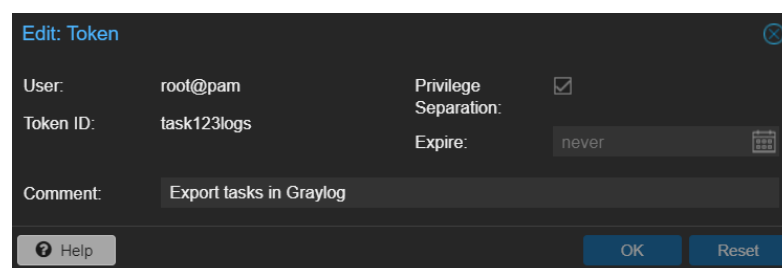
Рисунок 3.35 – Підключений Proxmox Server

Тепер логи збираються с Proxmox Server. Необхідно вирішити наступну проблему, неповні логи. Приведено приклад логу для розуміння.

Dec 12 14:47:47 ax103 pvedaemon[2875524]: <root@pam> starting task
 UPID:ax103:00310EB4:5F1F5174:675AF793:qmreboot:103:root@pam

Потрібно збирати інформацію про події з VM і ці логи успішно генеруються, створено екстрактор і отримано поля. Але проблема полягає у тому, що лог не містить інформацію про саму віртуальну машину. Необхідно знати як мінімум назву віртуальної машини з якою виконується операція. Логи даної інформації не мають але є вихід, використання REST API та Graylog Lookup Table. Graylog Lookup Table запитує у Proxmox Server інформацію про віртуальну машину за її ID.

Спочатку створено API Token на Proxmox VE та надано йому права переглядати стан VM. Створимо спочатку API Token.



Edit: Token

User: root@pam Privilege Separation: ☒

Token ID: task123logs Expire: never

Comment: Export tasks in Graylog

[Help](#) [OK](#) [Reset](#)

Рисунок 3.36 – Створений API Token

Далі надано йому необхідні права.

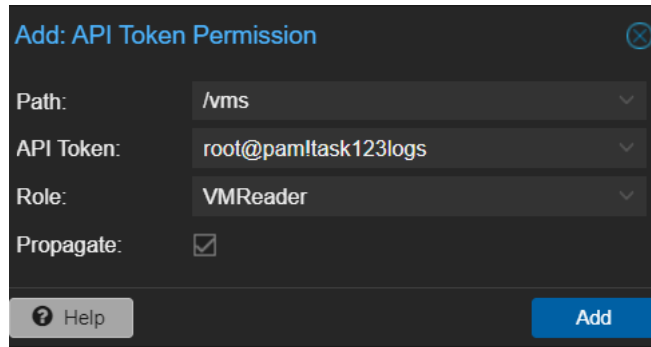


Рисунок 3.37 – Надаємо права

Розглянуто процес наддачі прав, з метою підтримання рівня безпеки необхідно надавати лише мінімальний необхідний рівень прав для кожного необхідного компоненту системи, тому він має доступ лише до віртуальних машин і може лише переглядати їх стан. Перейдемо до налаштувань на Graylog Server. Для того щоб виконати задачу необхідно використати Pipelines, Lookup Tables (Data Adapter, Caches). Налаштуємо Data Adapter, компонент який буде збирати дані за допомогою REST API.

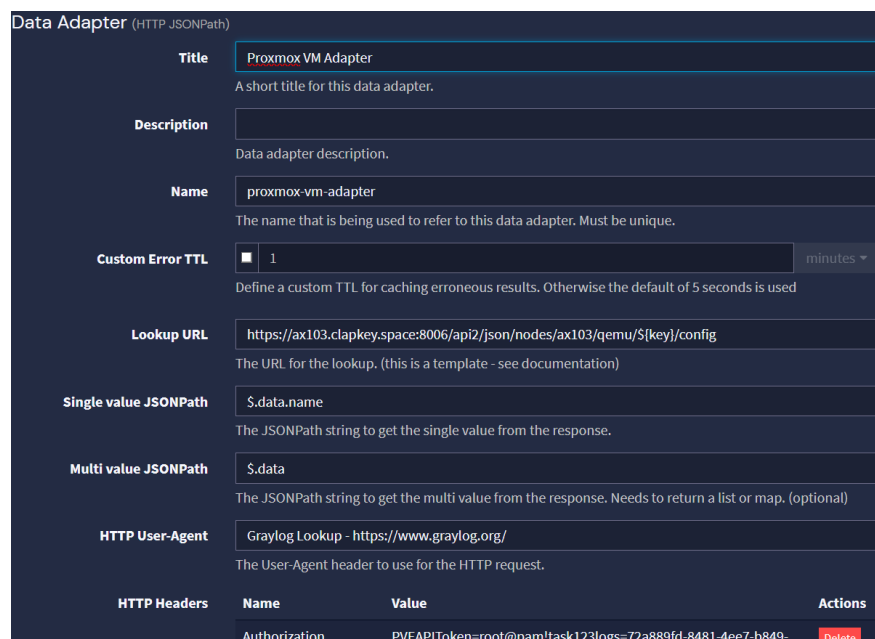


Рисунок 3.38 – Створення Data Adapter

Далі необхідно створити Caches, а після цього саму Lookup Tables, серед налаштувань нема нічого цікавого тому переходимо відразу до Pipelines. Викорис-

тано створену таблицю для модифікування логів, для додавання полів викорис-
тано Pipelines. Необхідно створити Pipeline Rule для підставлення назви віртуа-
льної машини до логу.

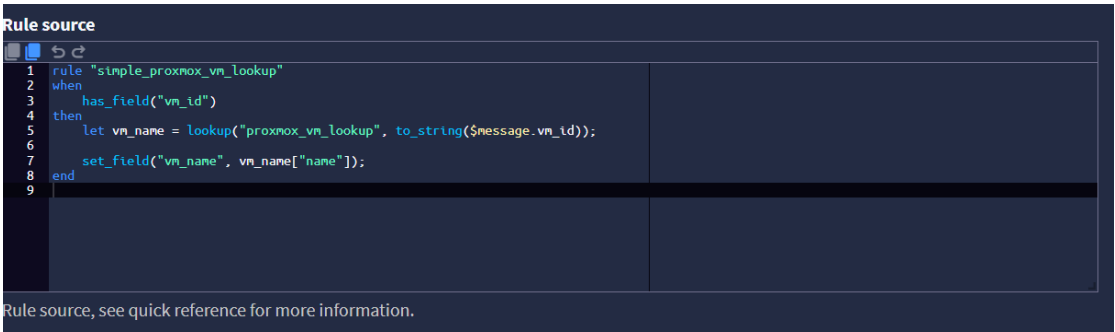


Рисунок 3.39 – Створення Pipeline Rule для підстановки

Створене правило буде додавати до логу нове поле з назвою віртуальної ма-
шини. Переглянемо отриману реалізацію.

vm_id	vm_name	task_action	pve_node	task_user	timestamp
101	graylog.mag	vncproxy	ax103	root	2024-12-12 16:25:03.598
102	AD.mag	vncproxy	ax103	root	2024-12-12 16:23:43.593
					2024-12-12 16:24:28.468
					2024-12-12 16:25:03.471
					2024-12-12 16:25:06.471
103	UbuDes.mag	qmreboot	ax103	root	2024-12-12 16:34:23.583
2024-12-12 16:34:28.511 Global Override: today					

Рисунок 3.40 – Модифіковане повідомлення

Тепер лог містить усі необхідні нам поля для подальшого використання.
Для отримання інформації о потенцій чи реальних загрозах для інформацій-
ної системи налаштовано інтеграцію з VirusTotal через API. Для цього викорис-
тано вже відомий функціонал Lookup Table та Pipeline. Для цього необхідно
отримати API key на офіційному сайті VirusTotal, переходимо особистий кабінет
і отримуємо key.

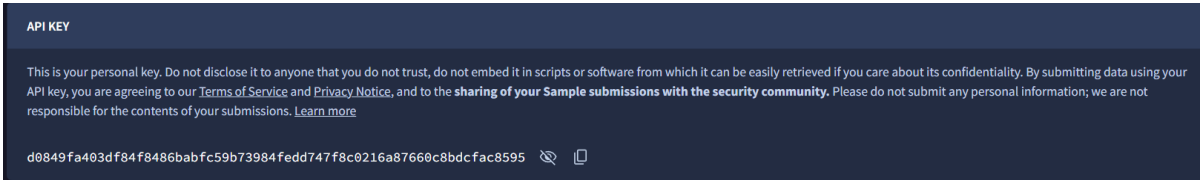


Рисунок 3.41 – API key для інтеграції VirusTotal

Цей ключ знадобиться для створення Data Adapter, слід пам'ятати що безкоштовно можна зробити лише 500 запитів по API але в навчальних цілях цього вистачить. Далі створено Data Adapter.

The screenshot shows the configuration for a Data Adapter named "VirusTotal IP Lookup". The fields are as follows:

- Title:** VirusTotal IP Lookup
- Description:** Adapter for looking up IP addresses using VirusTotal API.
- Name:** vt_ip_lookup
- Custom Error TTL:** 1 minutes
- Lookup URL:** https://www.virustotal.com/api/v3/ip_addresses/\${key}
- Single value JSONPath:** \$.data.attributes.last_analysis_stats.malicious
- Multi value JSONPath:** (empty)
- HTTP User-Agent:** Graylog Lookup - https://www.graylog.org/
- HTTP Headers:** A table with one header row (Name, Value, Actions) and one data row (x-apikey, d0849fa403df84f8486babfc59b73984fedd747f8c0216a87660c8bdcfac8595, Delete).

Рисунок 3.42 – Налаштування Data Adapter для інтеграції VirusTotal

Створення Lookup Table та переходимо до її використання. Використовувати будемо її через Pipelines, створимо нове правило для нашої інтеграції.

```
1 rule "VirusTotal IP Lookup"
2 when
3   has_field("rhost")
4 then
5   let vt_result = lookup_value("vt_ip_lookup_table", to_string($message.rhost));
6   set_field("virustotal_result", vt_result);
7 end
8
```

Рисунок 3.43 – Створення Pipeline Rule для підстановки

Створене правило буде робити запис по API і додавати нове поле virustotal_result (наприклад: virustotal_result = 11) з записом о небезпеці. Розберемо що означає цей запис, проведемо пошук традиційним методом.

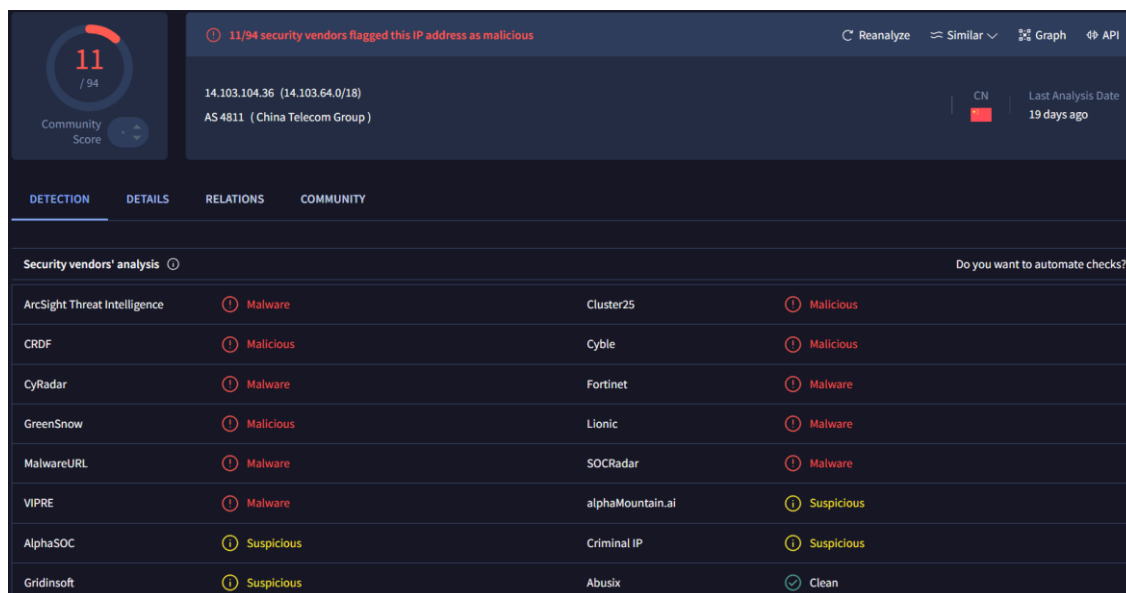


Рисунок 3.44 – Перевірка IP адреси на VirusTotal

Отримано результат перевірки у VirusTotal і використаємо цей результат у майбутньому. Наприклад створимо нове правило Pipeline яке при значенні `virustotal_result` більше 10 буде додавати нове поле з записом `PotentialThreatDetected`. Створене правило.

Rule source

```

1 rule "Mark Suspicious IPs"
2 when
3   to_long($message.virustotal_result) > 10
4 then
5   set_field("alertVT", "PotentialThreatDetected");
6 end
7

```

Рисунок 3.45 – Створення Pipeline Rule для створення мітки

Тепер логи у яких будуть зустрічатися підозрілі IP будуть помічатися записом `PotentialThreatDetected`.

Після створення механізму перевірки IP адрес можна також налаштований автоматичний збір даних о небезпечних адресах за допомогою сервісу Shodan. За допомогою цього сервісу ми зможемо отримати інформацію про IP який вважається підозрілим. Для цього використаний вже відомий інструмент Lookup Table.

✉ 2fca4bd2-75d1-4b6a-bca6-8d0b6b32efdb Not stored	
Timestamp	rhost
Stored in index	128.199.148.185
Message is not stored	shodan_asn
	AS14061
	shodan_city
	Singapore
	shodan_country
	Singapore
	shodan_fingerprint
	95:7c:20:96:7f:c3:56:59:1f:21:67:07:0a:29:b6:ec
	shodan_http_server
	nginx\1.22.0 (Ubuntu)
	shodan_ip
	128.199.148.185
	shodan_isp
	DigitalOcean, LLC
	shodan_organization
	DigitalOcean, LLC
	shodan_product
	OpenSSH
	shodan_version
	9.0p1 Ubuntu 1ubuntu7

Рисунок 3.46 – Результат роботи створеної інтеграції

Створений Pipeline модифікує повідомлення, з вже відомою небезпечною IP адресою для цього використано VirusTotal, і додає поля з інформацією про цю адресу. Далі цю інформацію можна використати для побудови дашборда.

Після налаштування усього необхідного функціоналу для отримання логів та оброблення їх належним чином, переходимо до створення механізму інформування у реальному часі. Для цього використаний вбудований функціонал Graylog Server, а саме Event Definition та Notification. Event Definition – це сама подія, а Notification – спосіб інформування. У цій роботі створено механізм інформування через Discord та MS Teams.

View "discordNotification " Notification	
Notifications alert you of any configured Event when they occur. Graylog can send Notifications directly to you or to other systems you use for that purpose.	
Details	
Title	discordNotification
Description	-
Notification Type	slack-notification-v1
Webhook URL	https://discord.com/api/webhooks/1285951378681888788/-G5rraReCrf6-AiRV9DQhUjwewj7f3jNgE1JV2bpQPETVSwv0RWux91uZ3MipiOGsmYfJR/slack
Channel	#graylog
Custom Message Template	<pre> --- [Event Definition] ----- Title: \${event_definition_title} Type: \${event_definition_type} </pre>

Рисунок 3.47 – Відправка повідомлень через Discord

Graylog Server має вже предналаштований функціонал для відправки повідомлень, тому використовується стандартний шаблон.

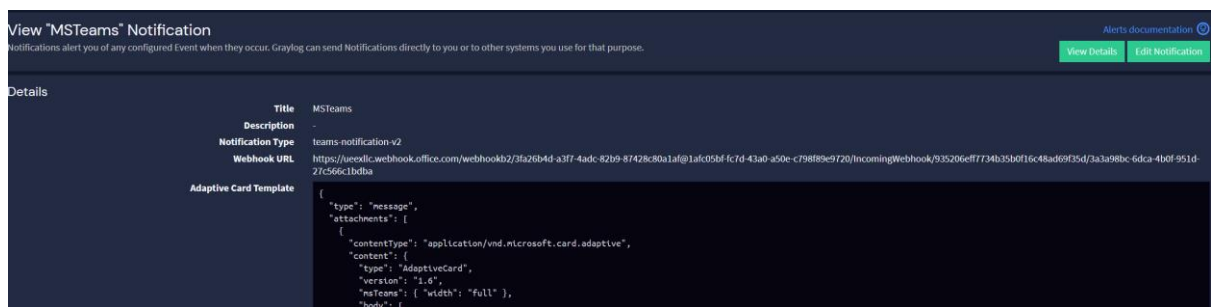


Рисунок 3.48 – Відправка повідомлень через MS Teams

Після налаштування способів передачі інформації переходимо до створення самих подій. Створено декілька основних подій для інцидентів кібербезпеки, а саме для РАМ та MikroTik. Почнемо зі створення події для MikroTik. На MikroTik використовуються ACL через те створено жорсткі правила для невдалого входу, навіть одна спроба буде визивати подію.

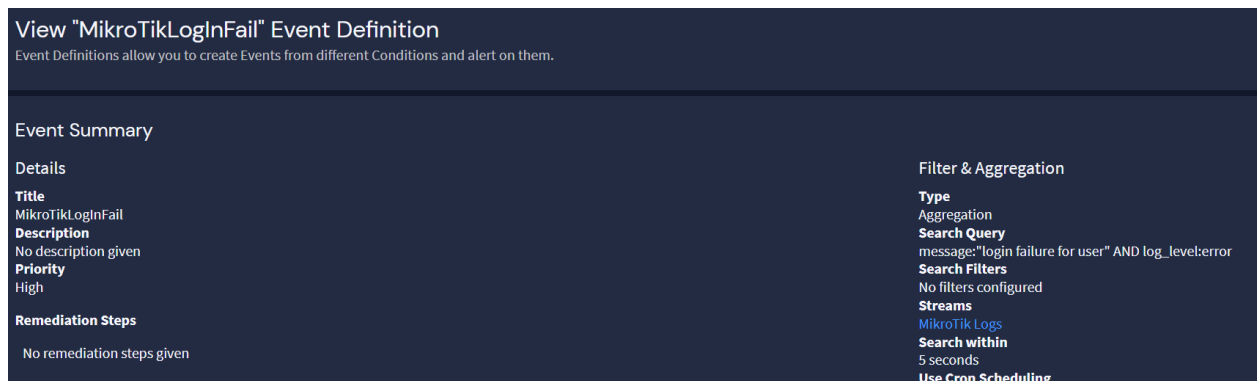
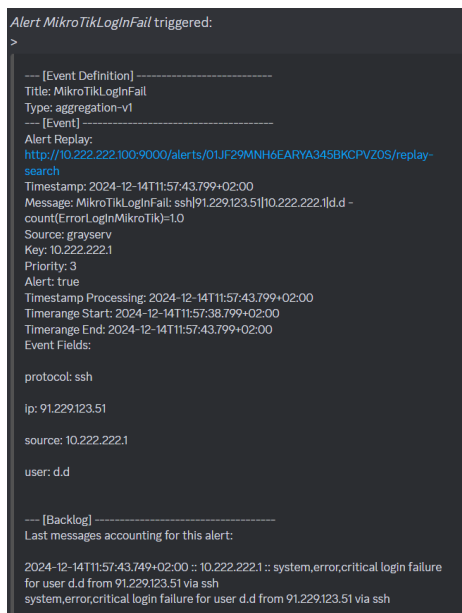
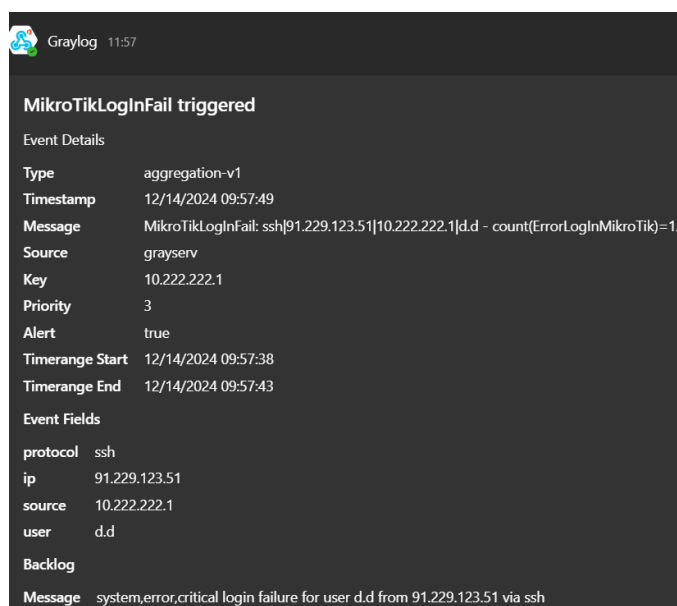


Рисунок 3.49 – Створена подія для MikroTik

Створено подію для невдалого входу до MikroTik, перевірка працездатності.



a)



б)

Рисунок 3.50 – Алерт створеної події для MikroTik: а) Discord, б) MS Teams

Переходимо до створення події для Linux PAM. Тут використовується більш м'яке правило і налаштовано для трьох невдалих входів. Також виводиться додаткові поля, які отримуються через налаштовані інтеграції.

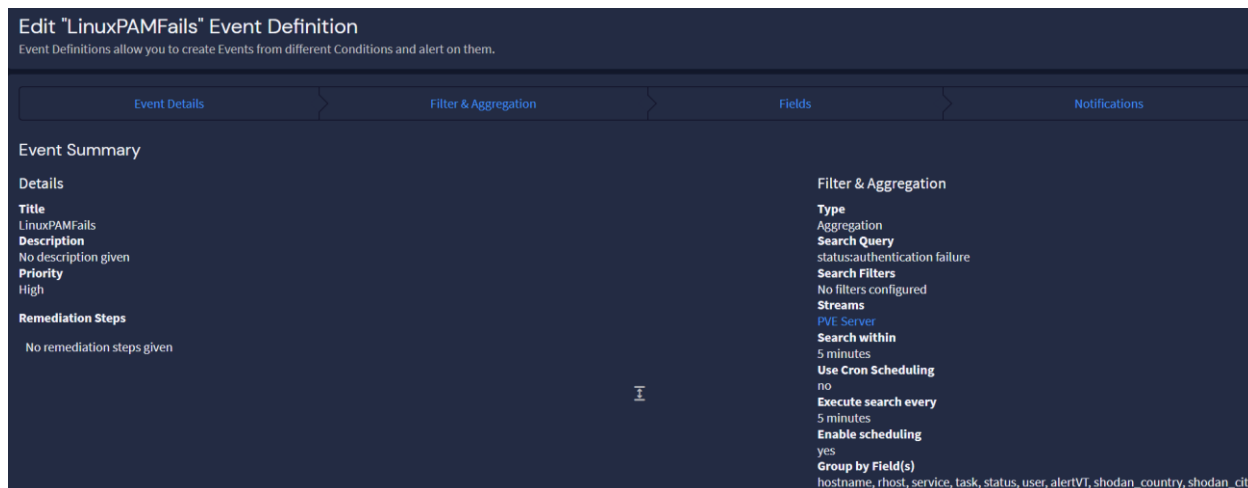


Рисунок 3.51 – Створена подія для Linux PAM

Далі перевірка працездатність створеної події подібно до MikroTik.

```
Alert LinuxPAMFails triggered:
>
--- [Event Definition] -----
Title: LinuxPAMFails
Type: aggregation-v1
--- [Event] -----
Alert Replay:
http://10.222.222.100:9000/alerts/01UF2ASEGMJQQFMG3APZY2FPYF/replay-search
Timestamp: 2024-12-14T12:17:53.961+02:00
Message: LinuxPAMFails: ax103|218.92.0.231|sshd|auth|authentication failure|root|PotentialThreatDetected|((Empty Value))((Empty Value)) - count(pamFail)=3.0
Source: grayerv
Key: 218.92.0.231
Priority: 3
Alert: true
Timestamp Processing: 2024-12-14T12:17:53.961+02:00
Timerange Start: 2024-12-14T12:12:53.961+02:00
Timerange End: 2024-12-14T12:17:53.961+02:00
Event Fields:

hostname: ax103
task: auth

shodan_country: (Empty Value)

service: sshd
alertVT: PotentialThreatDetected

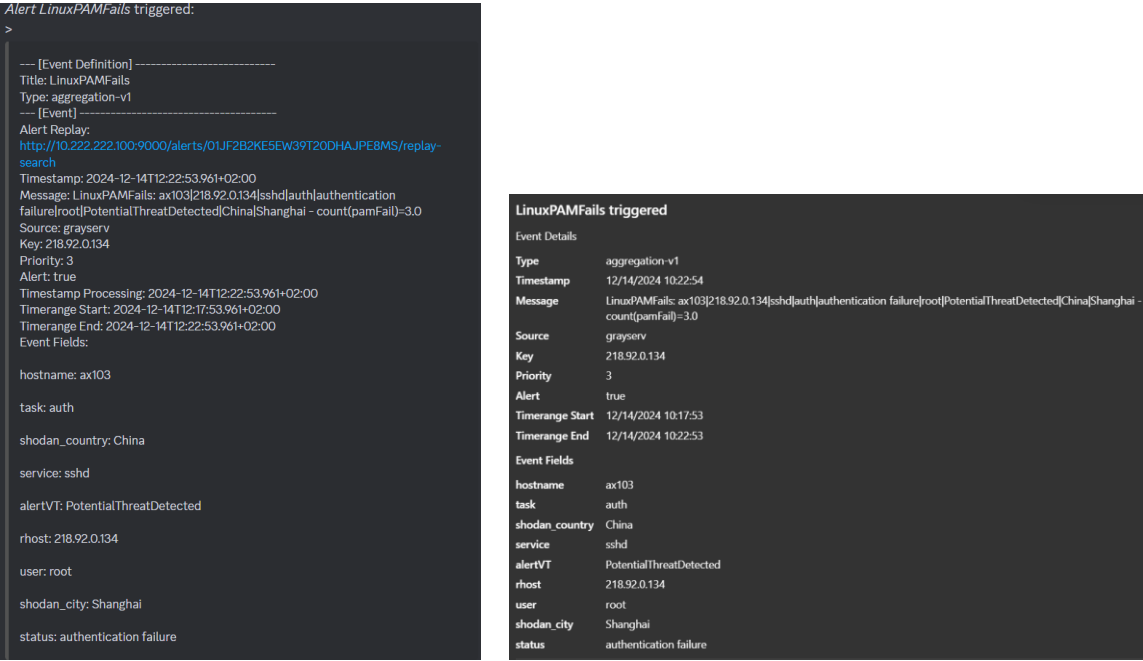
rhost: 218.92.0.231
user: root

shodan_city: (Empty Value)
status: authentication failure
```

LinuxPAMFails triggered	
Event Details	
Type	aggregation-v1
Timestamp	12/14/2024 10:17:54
Message	LinuxPAMFails: ax103 218.92.0.231 sshd auth authentication failure root PotentialThreatDetected ((Empty Value))((Empty Value)) - count(pamFail)=3.0
Source	grayerv
Key	218.92.0.231
Priority	3
Alert	true
Timerange Start	12/14/2024 10:12:53
Timerange End	12/14/2024 10:17:53
Event Fields	
hostname	ax103
task	auth
shodan_country	(Empty Value)
service	sshd
alertVT	PotentialThreatDetected
rhost	218.92.0.231
user	root
shodan_city	(Empty Value)
status	authentication failure

а) б)
Рисунок 3.52 – Створена некоректна подія для Linux PAM: а) Discord, б) MS Teams

Як можна побачити не усі поля заповнені, це трапилось бо база даних Shodan може не мати інформації про цю IP адресу, для вирішення цієї проблеми виставимо параметр: Validate that all Template values are set = Yes. Цей параметри буде підставляти поле тільки тоді коли воно заповнене.



а) б)

Рисунок 3.53 – Створена подія для Linux PAM: а) Discord, б) MS Teams

Після цього налаштування, створені подією алерти матимуть коректний вигляд. Також можна переглянути усі події у інтерфейсі Graylog Server.

Alerts	Events	Both						Show	10
Description			Key	Type	Event Definition	Timestamp			
LinuxPAMFails: ax103[218.92.0.134]sshd[auth]authentication failure[root]PotentialThreatDetected[China]Shanghai - count(pamFail)=3.0			218.92.0.134	Alert	LinuxPAMFails	2024-12-14 12:22:53			
LinuxPAMFails: ax103[218.92.0.134]sshd[auth]authentication failure[root]PotentialThreatDetected[China]Shanghai - count(pamFail)=4.0			218.92.0.134	Alert	LinuxPAMFails	2024-12-14 12:17:53			
LinuxPAMFails: ax103[218.92.0.220]sshd[auth]authentication failure[root]PotentialThreatDetected[Empty Value][Empty Value] - count(pamFail)=3.0			218.92.0.220	Alert	LinuxPAMFails	2024-12-14 12:17:53			
LinuxPAMFails: ax103[218.92.0.225]sshd[auth]authentication failure[root]PotentialThreatDetected[Empty Value][Empty Value] - count(pamFail)=3.0			218.92.0.225	Alert	LinuxPAMFails	2024-12-14 12:17:53			
LinuxPAMFails: ax103[218.92.0.231]sshd[auth]authentication failure[root]PotentialThreatDetected[Empty Value][Empty Value] - count(pamFail)=3.0			218.92.0.231	Alert	LinuxPAMFails	2024-12-14 12:17:53			
LinuxPAMFails: ax103[218.92.0.134]sshd[auth]authentication failure[root][Empty Value][Empty Value][Empty Value] - count(pamFail)=4.0			218.92.0.134	Alert	LinuxPAMFails	2024-12-14 12:07:53			
MikroTik loginFail: ssh[91.229.123.51][10.222.222.1]d.d - count(ErrorLoginMikroTik)=1.0			10.222.222.1	Alert	MikroTik loginFail	2024-12-14 11:57:43			
MikroTik loginFail: ssh[91.229.123.51][10.222.222.1]d.d - count(ErrorLoginMikroTik)=1.0			d.d	Alert	MikroTik loginFail	2024-12-14 11:56:58			

Рисунок 3.54 – Виконані події

Після налаштування усі необхідних технологій розглянемо конфігурацію нашого Proxmox серверу

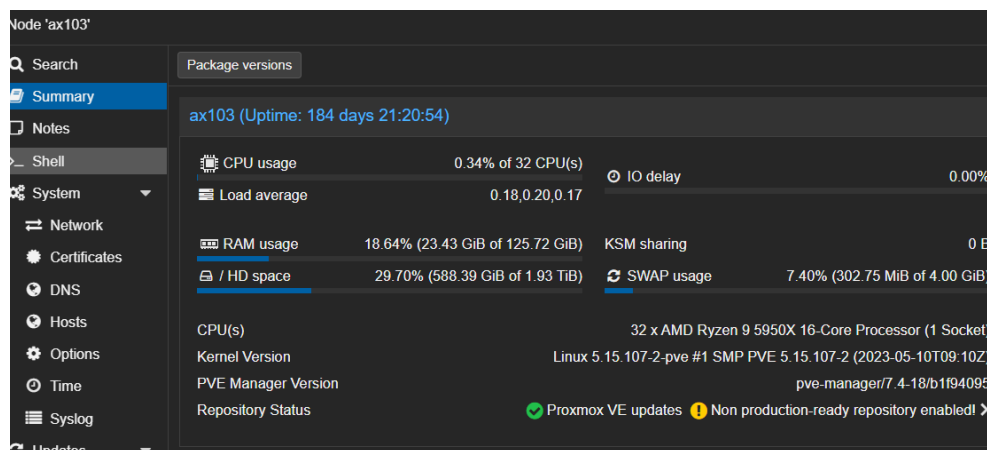


Рисунок 3.55 – Конфігурація Proxmox Server

Кластер в роботі не використовується, тобто використана лише одна Node(сервер) ax103. Він доволі потужну конфігурацію і його вистачить для усіх наявних задач. Але потребується додаткова конфігурація.

Згідно з технічним завданням нам потрібно реалізувати:

- Автоматичне резервне копіювання та відновлення даних.

Тому необхідно налаштувати автоматичний бекап, Proxmox у свій базовій конфігурації підтримує бекапи, тому задача спрощується. Proxmox підтримує створення бекапу на віддаленому бекап сервері але цього разу ми будемо зберігати бекап локально.

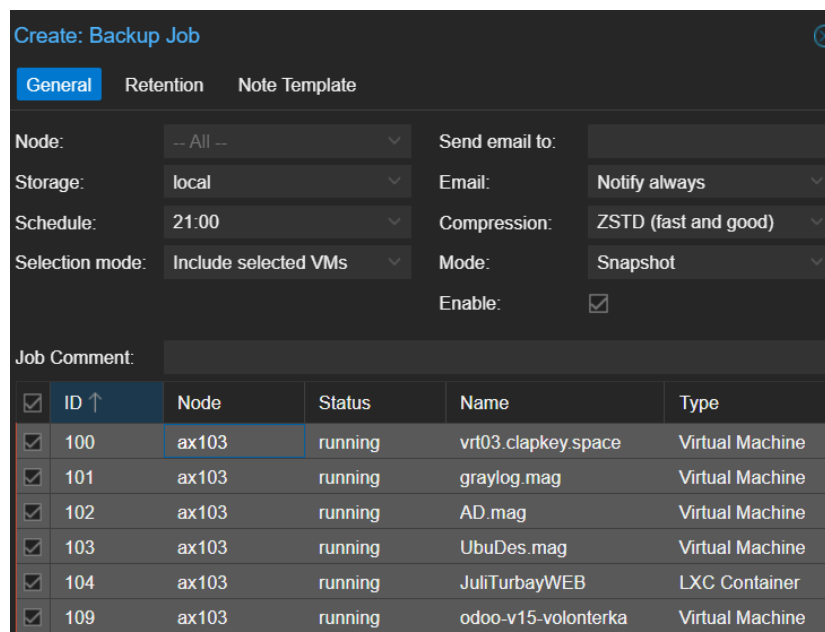


Рисунок 3.56 – Налаштування механізму створення бекапів

Налаштування створення бекапу для кожної віртуальної машини о 23.00 кожного дня. Запустимо бекап зараз щоб перевірити працездатність.

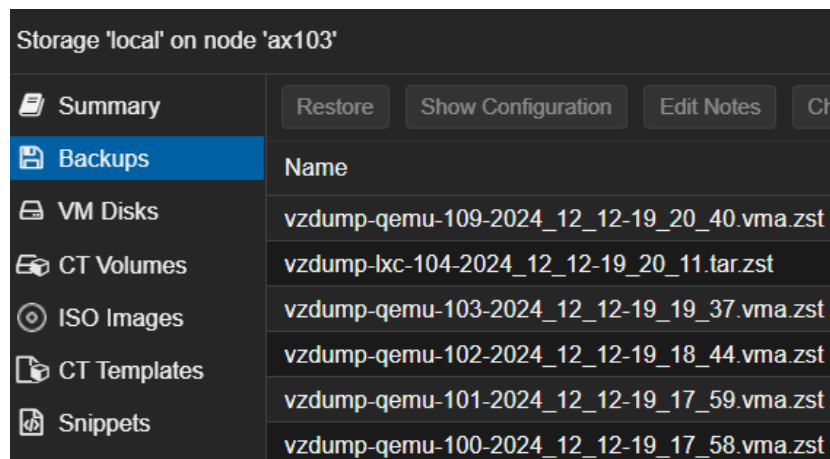


Рисунок 3.57 – Створені бекапи

Бекапи успішно створені, тепер у випадку втрати даних їх можна буде відновити.

3.4 Створення механізму візуалізації даних та тестування поглибленої системи моніторингу на відповідність.

Переходимо до розділу з тестуванням. Проводиться атака на інформаційну систему і фіксується реакція системи. Але для початку створено декілька дашбордів для кращого сприйняття інформації.

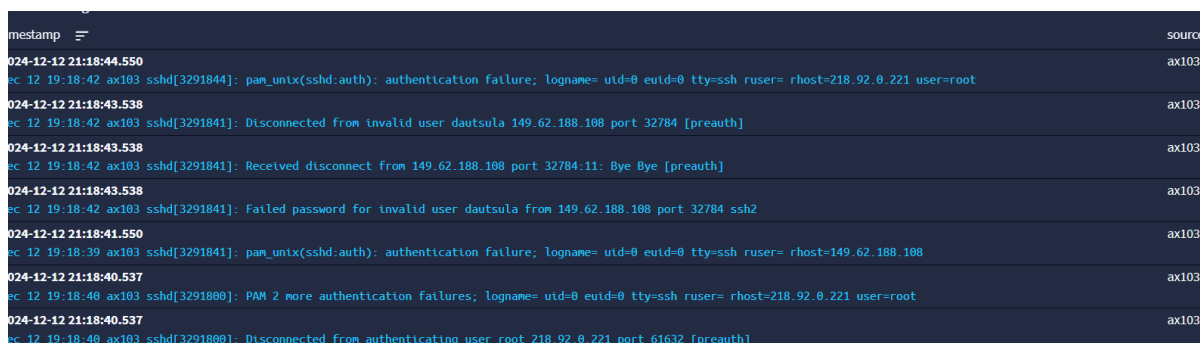


Рисунок 3.58 – Логи у стандартному вигляді

Як видно зі скріншоту [3.58], у стандартному вигляді буде складно сприймати отриману інформацію, тому необхідно покращити її візуальне сприйняття. Вирішити дану проблему можна створенням предналаштованих пошуків або дашбордів. Створено дашборд для PVE Tasks, для дій що виконуються з віртуальними машинами, та для Linux PAM.

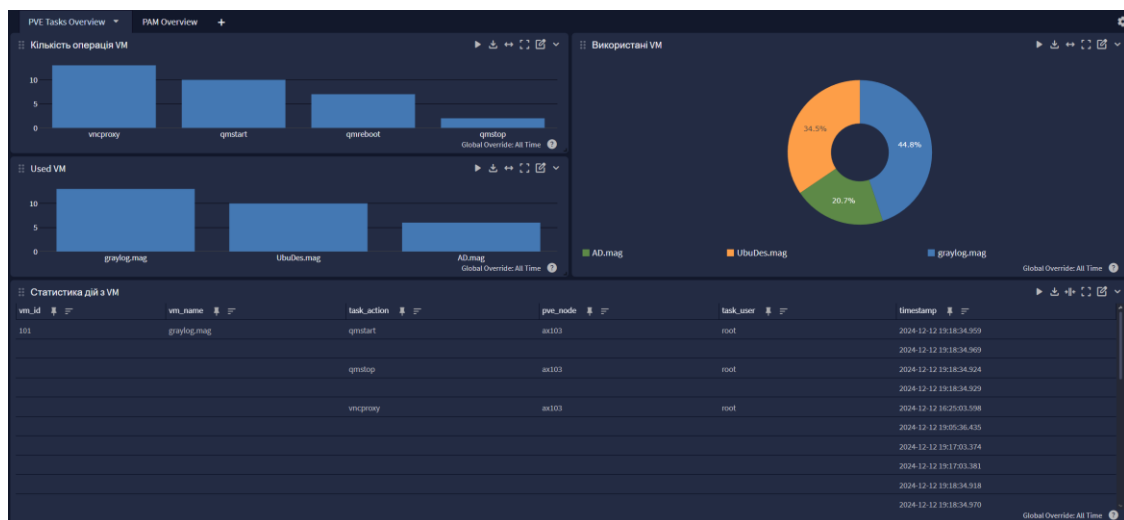


Рисунок 3.59 – Створений дашбоард PVE Tasks

На цьому дашборді виводиться статистика про операції з віртуальними машинами. На ньому відображається яка WM (назва, ID), задачу і користувач що виконав цю задачу.

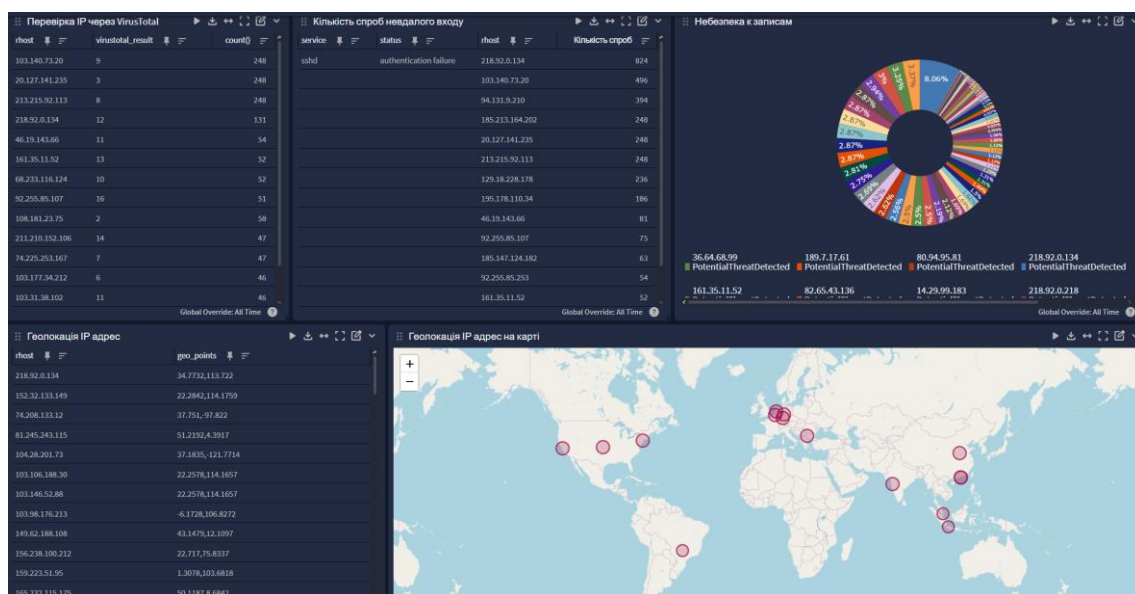


Рисунок 3.60 – Створений дашбоард Linux RAM

На цьому дашборді можна дізнатися всю необхідну інформацію, хто і звідки намагався підключитися до нашого Proxmox Server. За допомогою встановлених інтеграцій можна дізнатися чи шкідлива IP адреса з якої була спроба підключення і звідки. Пройдемося по важливим елементам.

Перевірка IP через VirusTotal		
rhost	virustotal_result	count()
103.140.73.20	9	248
20.127.141.235	3	248
213.215.92.113	8	248
218.92.0.134	12	131
46.19.143.66	11	54
161.35.11.52	13	52

Рисунок 3.61 – Елемент Перевірка IP через VirusTotal

Логічно з назви даний елемент виводить на статистику VirusTotal по IP які намагаються підключитися до серверу. Поле **virustotal_result** показує рівень небезпеки, чим більше тим гірше.

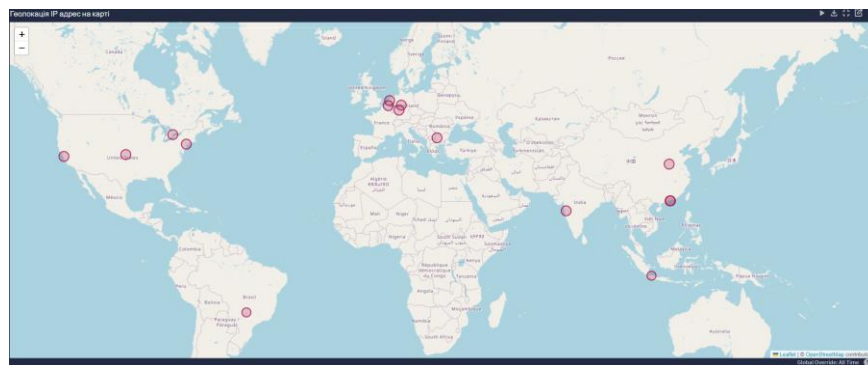


Рисунок 3.62 – Елемент геолокації

Даний елемент виводить на карті світу саме звідки, та чи і інша адреса, підключається до серверу. Останій елементу дашборда – Статистика Shodan.

Статистика Shodan									
shodan_ip	ASN	Місто	Країна	HTTP-сервер	Провайдер	latest(shodan_organization)	Продукт	Версія	
218.92.0.134	AS4134	Shanghai	China		CHINANET-BACKBONE	CHINANET jiangsu province network			
192.3.116.153	AS36352	Elk Grove Village	United States	nginx/1.18.0 (Ubuntu)	HostPapa	RackMerd LLC	OpenSSH	8.2p1 Ubuntu 4ubuntu11	
106.51.64.158	AS24309	Bengaluru	India	Apache/2.4.62 (Debian)	Atria Convergence Technologies Pvt. Ltd. Broadband Internet Service Provider INDIA	Atria Convergence Technologies Pvt. Ltd.,	OpenSSH	8.4p1 Debian 5+deb11u3	
104.248.240.197	AS14061	Frankfurt am Main	Germany		DigitalOcean, LLC	DigitalOcean, LLC	OpenSSH	9.7p1 Ubuntu 7ubuntu4	
195.178.110.65	AS48898	Lelystad	Netherlands	Apache/2.4.29 (Ubuntu)	TECHOFF SRV LIMITED	TECHOFF SRV LIMITED	OpenSSH	7.6p1 Ubuntu 4ubuntu9.7	
77.91.87.131	AS218644	Stockholm	Sweden		AEZA INTERNATIONAL LTD	Aeza International LTD	OpenSSH	8.9p1 Ubuntu 3ubuntu9.4	
94.159.103.108	AS215738	Kelsterbach	Germany		H2NEXUS LTD	H2 NEXUS Frankfurt Network	OpenSSH	9.2p1 Debian 2+deb12u3	
104.248.243.238	AS14061	Frankfurt am Main	Germany		DigitalOcean, LLC	DigitalOcean, LLC	OpenSSH	9.7p1 Ubuntu 7ubuntu4	
51.178.137.178	AS16276	Lille	France	Apache/2.4.41 (Ubuntu)	OVH SAS	OVH SAS	OpenSSH	8.2p1 Ubuntu 4ubuntu11	
77.161.36.10	AS1136	Almere Stad	Netherlands	gSOAP/2.8	KPN B.V.	KPN B.V.	OpenSSH	9.6p1 Ubuntu 3ubuntu13.5	
185.147.125.100	AS49505	Saint Petersburg	Russian Federation	Microsoft-HTTPAPI/2.0	JSC Selectel	Planeta LLC	OpenSSH	for_Windows_7.7	

Рисунок 3.63 – Елемент статистика Shodan

За допомогою створеної інтеграції з Shodan збирається статистика про небезпечні IP адреси і для покращено сприйняття інформації був створений дашборд. У цьому дашборді можна переглянути основну відому інформацію про цей IP, що може бути корисною для розслідування.

Як можна визначити за дашбордами, що на наш сервер здійснюється брутфорс-атака і що система реагує на неї в штатному режимі.

Висновки: у третьому розділі була проведена практична реалізація та тестування системи поглибленого моніторингу захищеної віртуалізованої ІТ-інфраструктури. На основі впроваджених мережевих технологій для побудови надійної платформи було розгорнуто сервер Proxmox VE та окремі віртуальні машини, що забезпечили необхідний рівень ізоляції та масштабованості. З використанням системи Graylog проведено централізований збір і обробку логів у режимі реального часу, а за допомогою Graylog Sidecar на віддалених віртуальних машинах — налаштовано їх моніторинг та транзит логів. Однією з ключових складових стала побудова механізму візуалізації та аналітики отриманих логів, що дало змогу оперативно виявляти та аналізувати потенційні загрози. Завдяки налаштованим автоматичним бекапам фізичного сервера та створених віртуальних машин вдалося підвищити рівень відмовостійкості й убезпечити системи від втрати критичних даних. Для перевірки працездатності реалізованого комплексу було проведено тестування шляхом моделювання мережевих атак: система коректно ідентифікувала підозрілу активність та зафіксувала відповідні події в логах. Таким чином, у результаті реалізації та тестування представлено комплексний підхід до моніторингу та захисту віртуалізованої ІТ-інфраструктури підприємства. Запропоновані налаштування підтвердили відповідність системи встановленим вимогам безпеки й ефективності, а результати перевірок засвідчили високий рівень надійності розробленої платформи.

ВИСНОВКИ

При виконанні кваліфікаційної роботи був проведений аналіз теми кваліфікаційної роботи, був проведений розгляд стеку технологій інформаційної мережі, визначений необхідний технологічний мінімум для побудови захищеної віртуалізованої IT-інфраструктури підприємства, підібрані відповідні технології та протоколи для реалізації інформаційної системи. Створена інформаційна система була протестована на відповідність до вимог.

У першому розділі було проведено широке коло теоретичних досліджень, необхідних для розуміння та проектування захищеної віртуалізованої IT-інфраструктури підприємства. Насамперед розглянуто поняття інформаційної системи, її складові та роль в організації. Встановлено, що IT-інфраструктура невіддільна від інформаційної системи й слугує її технологічним фундаментом, а ретельно спроектоване поєднання апаратного забезпечення, програмного забезпечення, мережевих ресурсів і хмарних сервісів формує основу для ефективного управління даними та бізнес-процесами. Далі проаналізовано основні загрози для інформаційних систем, включно з людськими помилками, стихійними лихами та протиправними діями з використанням комп'ютерних технологій. Наголошено, що об'єктивні чинники, такі як фізична відмова обладнання чи стихійні лиха, можуть завдавати суттєвих збитків, однак кіберзлочини й шкідливе ПЗ (віруси, троянські коні, фішинг) також становлять серйозну небезпеку й вимагають комплексних засобів захисту та контролю. Окрему увагу було приділено технології SIEM, яка дає змогу централізовано збирати, аналізувати й корелювати події в реальному часі з різних вузлів системи. Розглянуто переваги SIEM (централізоване керування безпекою, спрощення аудиту, виявлення загроз у реальному часі) та її недоліки (складність впровадження, високі витрати, ризик хибнопозитивних сигналів). Відзначено, що продумана інтеграція SIEM дає змогу оперативно реагувати на загрози, автоматизувати процес виявлення інцидентів і посилює захист всієї IT-інфраструктури. Крім того, описано системи віртуалізації та віддалені сервери, які стали основою сучасних інформаційних систем. Показано, що

віртуалізація сприяє більш ефективному використанню ресурсів, покращує масштабованість і безпеку, а віддалені сервери розв'язують задачу глобальної доступності та дають змогу знизити витрати на власне обладнання. Водночас наголошено на актуальних ризиках (наприклад, залежність від провайдера, мережеві затримки та регуляторні питання).

У другому розділі було проведено комплексне проєктування інформаційної системи управління інцидентами, включаючи визначення її цілей, задач, основних принципів побудови та аналізу технологічних рішень. Розроблена організаційна структура та ІТ-інфраструктура спрямовані на забезпечення ефективного управління інцидентами, підвищення продуктивності та безпеки бізнес-процесів. Було розглянуто необхідні технології для побудови інформаційної системи, серед вибраних варіантів було проведено порівняння, на основі проведеного порівняння був здійснений вибір кращого варіанту який задовольняє необхідні для інформаційної системи вимоги.

У третьому розділі була проведена практична реалізація та тестування системи поглибленого моніторингу захищеної віртуалізованої ІТ-інфраструктури. На основі впроваджених мережевих технологій для побудови надійної платформи було розгорнуто сервер Proxmox VE та окремі віртуальні машини, що забезпечили необхідний рівень ізоляції та масштабованості. З використанням системи Graylog проведено централізований збір і обробку логів у режимі реального часу, а за допомогою Graylog Sidecar на віддалених віртуальних машинах – налаштовано їх моніторинг та транзит логів. Однією з ключових складових стала побудова механізму візуалізації та аналітики отриманих логів, що дало змогу оперативно виявляти та аналізувати потенційні загрози. Завдяки налаштованим автоматичним бекапам фізичного сервера та створених віртуальних машин вдалося підвищити рівень відмовостійкості й убезпечити системи від втрати критичних даних. Для перевірки працездатності реалізованого комплексу було проведене тестування шляхом моделювання мережевих атак: система коректно ідентифікувала підозрілу активність та зафіксувала відповідні події в логах. Таким чином,

у результаті реалізації та тестування представлено комплексний підхід до моніторингу та захисту віртуалізованої ІТ-інфраструктури підприємства. Запропоновані налаштування підтвердили відповідність системи встановленим вимогам безпеки й ефективності, а результати перевірок засвідчили високий рівень надійності розробленої платформи.

На мою думку, робота має велику доцільність та практичну цінність, оскільки в ході її виконання були отримані навички створення захищених інформаційних систем. При створенні інформаційної системи були отримані корисні практичні навички, які можна використати у майбутньому для роботи уже не з навчальними системами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Information system | Definition, Examples, & Facts | Britannica [Електроний ресурс] / Britannica. - <https://www.britannica.com/topic/information-system> – 09.02.2024. – Загол. з екрану.

2. What is information systems? Definition, uses, and examples [Електроний ресурс] / Zapier. – <https://zapier.com/blog/what-is-information-systems/> – 06.06.2023. – Загол. з екрану.

3. What is information system? Why is it considered backbone of modern business? [Електроний ресурс] / Economic Times. – <https://ciso.economictimes.indiatimes.com/news/next-gen-tech/what-is-information-system-why-is-it-considered-backbone-of-modern-business/101588891> – 08.09.2023. – Загол. з екрану.

4. Що таке управління інформаційною безпекою та подіями (SIEM) і чому це важливо? [Електроний ресурс] / Eska. – <https://eska.global/blog/sho-take-up-ravlinnya-informacijnoyu-bezpekoyu-ta-podiyami-siem-i-chomu-ce-vazhlivo> – 06.06.2022. – Загол. з екрану.

5. What is SIEM? | IBM [Електроний ресурс] / IBM. – <https://www.ibm.com/topics/siem> – 14.04.2023. – Загол. з екрану.

6. What is SIEM? A Beginner's Guide - Varonis [Електроний ресурс] / Varonis. – <https://www.exabeam.com/explainers/siem/what-is-siem/> – 06.06.2022. – Загол. з екрану.

7. What Is SIEM? | Microsoft Security [Електроний ресурс] / Microsoft. – <https://www.varonis.com/blog/what-is-siem> – 29.01.2024. – Загол. з екрану.

8. Proxmox Virtual Environment (PVE) Administration Guide [Електронний ресурс] / Proxmox. – <https://pve.proxmox.com/pve-docs/pve-admin-guide.html> – 14.12.2024. – Загол. з екрану.

9. oVirt Documentation [Електронний ресурс] / oVirt. – <https://www.ovirt.org/documentation/> – 14.12.2024. – Загол. з екрану.

10. Citrix Hypervisor Documentation [Електронний ресурс] / Citrix. – <https://docs.xenserver.com/en-us/citrix-hypervisor> – 14.12.2024. – Загол. з екрану.
11. OpenNebula Documentation 6.8 [Електронний ресурс] / OpenNebula. – <https://docs.opennebula.io/6.8/> – 14.12.2024. – Загол. з екрану.
12. Proxmox Overview [Електронний ресурс] / NetApp. – <https://docs.netapp.com/us-en/netapp-solutions/proxmox/proxmox-overview.html#monitoring> – 16.12.2024. – Загол. з екрану.
13. oVirt Overview [Електронний ресурс] / SCALE 11x Supporting. – <https://www.socallinuxexpo.org/scale11x-supporting/default/files/presentations/ovirt-overview-scale-brooks.pdf> – 16.12.2024. – Загол. з екрану.
14. OpenNebula Overview [Електронний ресурс] / Csolutions.lv. – https://www.csolutions.lv/sites/default/files/opennebula_overview-rev20220624.pdf – 24.06.2022. – Загол. з екрану.
15. Wazuh Platform Overview [Електронний ресурс] / Wazuh. – <https://wazuh.com/platform/overview/> – 16.12.2024. – Загол. з екрану.
16. A Dive Into AlienVault OSSIM: Your Ultimate Free Open Source SIEM [Електронний ресурс] / Telfer Tjavf. – <https://www.linkedin.com/pulse/dive-alien-vault-ossim-your-ultimate-free-open-source-siem-telfer-tjavf/> – 16.12.2024. – Загол. з екрану.
17. What is KVM? | Red Hat [Електронний ресурс] / Red Hat. – <https://www.redhat.com/en/topics/virtualization/what-is-KVM> – 14.12.2024. – Загол. з екрану.
18. QEMU Documentation: About QEMU [Електронний ресурс] / QEMU. – <https://www.qemu.org/docs/master/about/index.html> – 14.12.2024. – Загол. з екрану.

19. Downloading and Installing Graylog on Ubuntu [Електронний ресурс] / Graylog. – https://go2docs.graylog.org/current/downloading_and_installing_graylog/ubuntu_installation.htm?tocpath=Install%20Graylog%7COperating%20System%20Packages%7C_____1 – 14.12.2024. – Загол. з екрану.

20. Getting Logs into Graylog Inputs [Електронний ресурс] / Graylog. – https://go2docs.graylog.org/current/getting_in_log_data/inputs.htm?tocpath=Get%20in%20Logs%7CGraylog%20Inputs%7C_____0 – 14.12.2024. – Загол. з екрану.

21. Installing Graylog Sidecar on Linux [Електронний ресурс] / Graylog. – https://go2docs.graylog.org/current/getting_in_log_data/install_sidecar_on_linux.htm?tocpath=Get%20in%20Logs%7CGraylog%20Sidecar%7CInstall%20Graylog%20Sidecar%7C_____1 – 14.12.2024. – Загол. з екрану.

22. Installing Graylog Sidecar on Windows [Електронний ресурс] / Graylog. – https://go2docs.graylog.org/current/getting_in_log_data/install_sidecar_on_windows.htm?tocpath=Get%20in%20Logs%7CGraylog%20Sidecar%7CInstall%20Graylog%20Sidecar%7C_____2 – 14.12.2024. – Загол. з екрану.

23. Getting Started with Graylog Sidecar [Електронний ресурс] / Graylog. – https://go2docs.graylog.org/current/getting_in_log_data/getting_started_with_graylog_sidecar.htm?tocpath=Get%20in%20Logs%7CGraylog%20Sidecar%7C_____3 – 14.12.2024. – Загол. з екрану.

24. Добровольський Д. Атаки на інформаційну систему їх наслідки та методи протидії / Дмитро Добровольський // Міжнародна науково-технічна конференція «Інформаційно-комп'ютерні технології – 2024», м. Житомир, 28 – 29 березня 2024 р. – Житомир, 2023.

25. Security Information and Event Management (SIEM) Implementation / David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask. – [S. l.] : Syngress, 2010. – 512 p.

26. The Practice of Network Security Monitoring: Understanding Incident Detection and Response / Richard Bejtlich. – [S. l.] : No Starch Press, 2013. – 376 p.
27. Virtualization Security: Protecting Virtualized Environments / Dave Shackleford. – [S. l.] : Syngress, 2012. – 336 p.

ДОДАТКИ

Таблиця А.1 – Параметри адресації модельного проєкту ІС

Хост	ІР-адреса	Маска мережі	Шлюз за замовчуванням
Mikrotik	100.222.222.1	255.255.255.0	-
graylog.mag	100.222.222.100	255.255.255.0	100.222.222.1
AD.mag	100.222.222.101	255.255.255.0	100.222.222.1
UbuDes.mag	DHCP		

Таблиця Б.1 – Розширена таблиця порівняння SIEM-систем

Критерій	Graylog	Wazuh	AlienVault OSSIM	Splunk
Ліцензія	Відкрита	Відкрита	Відкрита	Комерційна
Масштабованість	Висока	Середня	Середня	Висока
Інтерфейс користувача	Зручний	Інтуїтивний	Складний	Дружній
Функціонал	Пошук та аналіз логів	HIDS, аналіз логів	SIEM, HIDS, NIDS, аналіз вразливостей	Широкий аналіз даних
Вартість	Безкоштовно	Безкоштовно	Безкоштовно	Платно
Підтримка	Спільнота	Спільнота	Спільнота	Офіційна підтримка
Інтеграція	Плагіни	ELK Stack	Плагіни	Широка
Встановлення та налаштування	Середні	Середні	Середні	Прості
Підтримка платформ	Широка	Широка	Обмежена	Широка
Безпека та відповідність	Базова	Висока	Висока	Дуже висока
Аналітика та звітність	Середня	Середня	Висока	Дуже висока
Можливості кастомізації	Високі	Високі	Середні	Високі
Навчання та документація	Добрі	Добрі	Середні	Відмінні
Підтримка стандартів	Обмежена	Висока	Висока	Дуже висока
Потужність обробки даних	Висока	Середня	Середня	Висока

Можливості машинного навчання	Немає	Обмежені	Немає	Є
Сповіщення та алерти	Розширені	Базові	Розширені	Розширені
Підтримка мобільних пристроїв	Обмежена	Немає	Немає	Є
Обсяг спільноти	Велика	Середня	Середня	Велика
Оновлення та підтримка	Регулярні	Регулярні	Менш регулярні	Часті
Вимоги до ресурсів	Середні	Середні	Високі	Високі

Таблиця В.1 – Порівняння Систем Віртуалізації

Система віртуалізації	Тип ліцензії	Основні переваги	Недоліки	Інтерфейс	Резервне копіювання	Масштабованість
Proxmox VE	Відкрита (безкоштовна)	Простота використання, підтримка KVM та LXC, резервне копіювання, кластеризація	Обмежена комерційна підтримка, залежність від спільноти	Зручний веб-інтерфейс	Інтегроване, легке для використання	Висока, зручна для середнього бізнесу
oVirt	Відкрита (безкоштовна)	Потужне рішення на основі KVM, підтримка великих кластерів, розширена функціональність	Важкий у налаштуванні, потребує значних технічних знань	Веб-інтерфейс, але складніший у порівнянні з Proxmox	Можна налаштувати через сторонні інструменти	Висока, підходить для великих підприємств
XenServer (Citrix Hypervisor)	Відкрита (базова версія)	Безкоштовна версія з основними функціями, висока продуктивність, корпоративна підтримка	Додаткові функції доступні тільки у платній версії, складність налаштування для новачків	Веб-інтерфейс Citrix, менш інтуїтивний	Резервне копіювання через сторонні засоби	Висока, орієнтована на великі інфраструктури

OpenNebula	Відкрита (безкоштовна)	Підтримка різних гіпервізорів (KVM, VMware), побудова приватних і гібридних хмар	Складне налаштування, потребує глибоких знань для повноцінної роботи	Веб-інтерфейс, технічно складний	Інтегрується через зовнішні сервіси резервного копіювання	Дуже висока, підходить для великих хмарних і гібридних середовищ
------------	---------------------------	--	--	----------------------------------	---	--