

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 бакалавра
на тему: «Проект SIEM-системи на базі рішення IBM
Qradar»

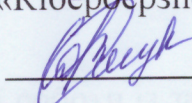
Тема роботи: Проект SIEM-системи на базі рішення IBM Qradar
затверджена Наказом університету від 2026 р. №38/о
термін здачі студентом закінченої роботи: червня 2026 р.
Вихідні дані роботи:

— підсистема моніторингу подій безпеки IBM Qradar
— методи та засоби централізованого збору, аналізу та кореляції подій безпеки з використанням платформи IBM Qradar

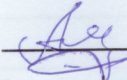
Обладнання та програмне забезпечення:

1. Інструмент віртуалізації мережі Oracle VM VirtualBox;
2. SIEM- IBM Qradar Community Edition (v. 7.3.3);
3. Windows Server 2019;
4. Windows 10;
5. Kali Linux.

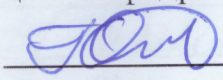
Виконала: студентка 4-го курсу групи КБ-22-3
спеціальності 125 «Кібербезпека»

 Сабріна МАЦЮК

Консультанти з випускної кваліфікаційної роботи: доценти, що їх стосуються
Керівник: Доцент кафедри КІ та КБ, к.т.н.

 Олексій ШЕЛУХА

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

 Олена ГОЛОВНЯ

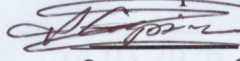
Розділ	Консультант
1	Олександр ПОКОТИЛО
2	Олександр ПОКОТИЛО
3	Олександр ПОКОТИЛО

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
2 лютого 2026 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Мацюк Сабріна Вікторівна

Тема роботи: Проект SIEM-системи на базі рішення IBM Qradar

затверджена Наказом університету від 2 лютого 2026 р. №58/с

Термін здачі студентом закінченої роботи червня 2026 р.

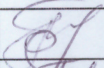
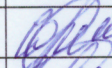
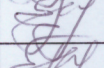
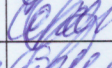
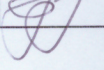
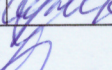
Вихідні дані роботи:

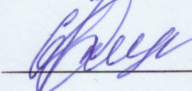
- підсистема моніторингу подій безпеки IBM Qradar
- методи та засоби централізованого збору, аналізу та кореляції подій безпеки з використанням платформи IBM Qradar

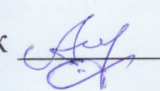
Обладнання та програмне забезпечення:

1. Інструмент віртуалізації мережі Oracle VM VirtualBox;
2. SIEM- IBM Qradar Community Edition (v.7.3.3);
3. Windows Server 2019;
4. Windows 10;
5. Kali Linux.

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

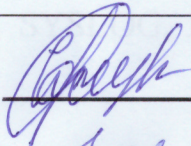
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Олександра ПОКОТИЛО	 02.02.2026	 02.02.2026
2	Олександра ПОКОТИЛО	 02.02.2026	 02.02.2026
3	Олександра ПОКОТИЛО	 02.02.2026	 02.02.2026

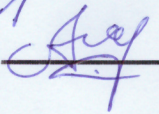
Студент  Сабріна МАЦЮК

Керівник  Олексій ШЕЛУХА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	02.02.2026	Виконано
2	Аналіз рішення IBM QRadar	15.02.2026	Виконано
3	Формування структури пояснювальної записки	28.02.2026	Виконано
4	Проектування архітектури SIEM-системи на базі IBM QRadar	14.03.2026	Виконано
5	Розгортання лабораторного сте-нду в Oracle VirtualBox	30.03.2026	Виконано
6	Налаштування мережевої інфра-структури та джерел логів	04.04.2026	Виконано
7	Налаштування Active Directory та інтеграція з IBM QRadar	15.04.2026	Виконано
8	Тестування системи	01.06.2026	Виконано
9	Написання пояснювальної запи-ски	08.06.2026	Виконано

Студент  Сабріна МАЦІЮК

Керівник  Олексій ШЕЛУХА

АНОТАЦІЯ

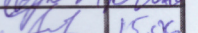
Кваліфікаційна робота бакалавра на тему «Проект SIEM–системи на базі рішення IBM QRadar» присвячена проектуванню та побудові системи моніторингу інформаційної безпеки у віртуальному корпоративному середовищі.

Метою роботи є проектування лабораторного стенду SIEM–системи на базі платформи IBM QRadar та дослідження її можливостей щодо централізованого збору, обробки й аналізу подій інформаційної безпеки.

У роботі розглянуто теоретичні основи функціонування центрів моніторингу безпеки SOC та сучасних SIEM–систем. Проведено аналіз найбільш поширених SIEM–рішень, визначено особливості їх використання та обґрунтовано вибір платформи IBM QRadar. Розроблено проект мережевої інфраструктури лабораторного стенду, виконано налаштування основних компонентів середовища та організовано централізований збір журналів подій від різних джерел. Проведено моделювання типових загроз інформаційній безпеці, зокрема мережевого сканування, підбору паролів та ARP–спуфінгу. Наведено результати тестування лабораторного стенду та виконано оцінку можливостей IBM QRadar щодо моніторингу подій безпеки.

Пояснювальна записка містить 76 сторінок, 48 рисунків та 4 таблиці. Список використаних джерел містить 30 найменувань та займає 2 сторінки.

Ключові слова: SIEM, IBM QRADAR, SOC, ІНФОРМАЦІЙНА БЕЗПЕКА, МОНІТОРИНГ ПОДІЙ, ACTIVE DIRECTORY, SYSLOG, КОРЕЛЯЦІЯ ПОДІЙ, КІБЕРБЕЗПЕКА, OPNsense.

					KKIK<.KP.B – 125 – 05 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект SIEM–системи на базі рішення IBM Qradar	Літ.	Арк.	Аркушів	
Розроб.		Мацюк С.В.		15.06.26					
Керівник		Шелуха О.О.		15.06.26			4	76	
Реценз.		Головня О.С.		15.06.26		ФІКТ, Гр. КБ–22–3			
Н. контр.		Шелуха О.О.		15.06.26					
Затверд.		Єфіменко А.А.		15.06.26					

ANNOTATION

The bachelor's qualification thesis entitled "Design of a SIEM System Based on the IBM QRadar Solution" is devoted to the design and implementation of an information security monitoring system within a virtual corporate environment.

The purpose of the thesis is to design a laboratory testbed of a SIEM system based on the IBM QRadar platform and to investigate its capabilities for centralized collection, processing, and analysis of information security events.

The thesis examines the theoretical foundations of Security Operations Centers (SOC) and modern SIEM systems. An analysis of the most widely used SIEM solutions was carried out, their features were identified, and the choice of IBM QRadar as the implementation platform was justified. A network infrastructure for the laboratory testbed was designed, the main components of the environment were configured, and centralized log collection from multiple sources was organized. Typical information security threats, including network scanning, password brute-force attacks, and ARP spoofing, were simulated. The results of laboratory testbed testing are presented, and the capabilities of IBM QRadar in monitoring and analyzing security events are evaluated.

The explanatory note contains 76 pages, 48 figures, and 4 tables. The list of references includes 30 sources and occupies 2 pages.

KEYWORDS: SIEM, IBM QRADAR, SOC, INFORMATION SECURITY, EVENT MONITORING, ACTIVE DIRECTORY, SYSLOG, EVENT CORRELATION, CYBERSECURITY, OPNsense.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				5
Змн.	Арк.	№ докум.	Підпис	Дата		

Зміст

ВСТУП	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ SIEM–СИСТЕМ ТА АНАЛІЗ СУЧАСНИХ РІШЕНЬ.....	9
1.1 Аналіз основних принципів організації SOC	9
1.2 Аналіз процесів функціонування SIEM–систем	13
1.3 Огляд сучасних SIEM–рішень	18
1.4 Обґрунтування вибору платформи IBM QRadar.....	24
1.5 Постановка технічного завдання	30
РОЗДІЛ 2 ПРОЄКТУВАННЯ SIEM–СИСТЕМИ НА БАЗІ IBM QRADAR.....	33
2.1 Вибір та обґрунтування інструментів	33
2.2 Проєктування мережевої інфраструктури	37
2.3 Моделювання загроз та проєктування системи виявлення	40
РОЗДІЛ 3 НАЛАШТУВАННЯ, РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ SIEM НА БАЗІ IBM QRADAR.....	44
3.1 Розгортання та налаштування тестового стенду.....	44
3.2 Налаштування Active Directory та IBM Qradar	56
3.3 Тестування системи та аналіз результатів.....	61
ВИСНОВКИ.....	69
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	71
ДОДАТКИ.....	73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD – Active Directory

DC – Domain Controller

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System (система доменних імен)

DSM – Device Support Module

EPS – Events Per Second (кількість подій за секунду)

IDS – Intrusion Detection System (система виявлення вторгнень)

IPS – Intrusion Prevention System (система запобігання вторгненням)

OS – Operating System

SIEM – Security Information and Event Management

SOC – Security Operations Center

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

UEBA – User and Entity Behavior Analytics

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Сьогодні інформаційні технології використовуються практично в усіх сферах діяльності людини. Разом із розвитком інформаційних систем постійно зростає і кількість кіберзагроз, які можуть призвести до втрати даних, порушення роботи сервісів або несанкціонованого доступу до ресурсів організації. У сучасних корпоративних мережах щодня генерується велика кількість журналів подій, які містять інформацію про роботу серверів, мережевого обладнання, робочих станцій та засобів захисту інформації. Аналізувати такі обсяги даних вручну складно, тому для автоматизації цього процесу використовуються SIEM-системи.

Однією з найбільш поширених платформ такого класу є IBM QRadar. Дана система дозволяє централізовано збирати події безпеки, аналізувати їх та допомагає своєчасно виявляти підозрілу активність у мережі. Саме тому дослідження можливостей побудови SIEM-системи на базі IBM QRadar є актуальним та має практичне значення для підготовки фахівців у сфері кібербезпеки.

Метою кваліфікаційної роботи є проектування та побудова лабораторного стенду системи моніторингу інформаційної безпеки на базі платформи IBM QRadar для дослідження її можливостей щодо збору, обробки та аналізу подій безпеки.

Визначена мета обумовлює наступні завдання:

- провести аналіз сучасних SIEM-систем та обґрунтувати вибір IBM QRadar;
- розробити проєкт лабораторного стенду SIEM-системи;
- виконати розгортання та налаштування компонентів стенду;
- провести моделювання загроз, тестування системи та аналіз отриманих результатів.

Об'єктом дослідження процес моніторингу подій інформаційної безпеки в корпоративних мережах.

Предметом дослідження є засоби та технології побудови SIEM-систем на базі платформи IBM QRadar для централізованого збору та аналізу подій безпеки.

У процесі виконання кваліфікаційної роботи було розроблено проєкт лабораторного стенду корпоративної мережі у віртуальному середовищі Oracle VirtualBox, до складу якого входять IBM QRadar Community Edition, Windows Server 2019 з Active Directory, робоча станція Windows 10, міжмережевий екран OPNsense та Kali Linux.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ SIEM–СИСТЕМ ТА АНАЛІЗ СУЧАСНИХ РІШЕНЬ

1.1 Аналіз основних принципів організації SOC

Security Operations Center – це централізований підрозділ організації, що відповідає за безперервний моніторинг, виявлення, аналіз та реагування на інциденти інформаційної безпеки. SOC об'єднує людей, процеси та технології в єдину структуру, що забезпечує цілодобовий захист інформаційної інфраструктури організації[7].

Головною метою функціонування центру моніторингу безпеки є своєчасне виявлення загроз інформаційній безпеці та мінімізація можливих наслідків від їх реалізації. Для досягнення цієї мети SOC виконує низку взаємопов'язаних завдань, спрямованих на забезпечення безперервного контролю за станом інформаційної інфраструктури організації.

До основних завдань SOC належать:

- моніторинг подій інформаційної безпеки в режимі реального часу;
- збір та аналіз журналів подій від різних джерел;
- виявлення ознак кібератак та несанкціонованого доступу;
- реагування на інциденти інформаційної безпеки;
- проведення аналізу причин виникнення інцидентів;
- оцінка рівня захищеності інформаційної інфраструктури;
- формування звітності щодо стану інформаційної безпеки.

Робота SOC охоплює всі етапи забезпечення інформаційної безпеки від збору подій до реагування на інциденти. Отримана інформація надходить до засобів аналізу, після чого спеціалісти приймають рішення щодо подальших дій та заходів реагування.

Організаційна структура SOC (рис. 1.1, 1.2)

Ефективність роботи центру моніторингу безпеки значною мірою залежить від його організаційної структури та кваліфікації персоналу. Для забезпечення безперервного моніторингу та швидкого реагування на загрози в більшості організацій використовується багаторівнева модель SOC[24].

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		9



Рисунок 1.1 – Структура та функції SOC

Залежно від масштабу організації кількість працівників та склад підрозділу можуть відрізнятися. У невеликих компаніях функції моніторингу можуть виконувати декілька спеціалістів, тоді як у великих організаціях центри моніторингу працюють цілодобово та складаються з окремих команд аналітиків.

Аналітики першого рівня (Tier 1) здійснюють постійний моніторинг подій безпеки та працюють безпосередньо із SIEM–системою. Вони переглядають сповіщення, визначають їх критичність та приймають рішення щодо необхідності подальшого аналізу. Основне завдання цього рівня полягає у швидкій обробці великої кількості подій та виявленні потенційних інцидентів.

У разі необхідності подія передається аналітикам другого рівня (Tier 2). Спеціалісти цього рівня виконують більш детальний аналіз інцидентів, визначають причини їх виникнення та оцінюють можливі наслідки. Крім цього, вони можуть брати участь у ліквідації наслідків атак та відновленні працездатності систем.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Аналітики третього рівня (Tier 3) займаються найбільш складними випадками та інцидентами. До їхніх обов'язків належить аналіз нових типів атак, пошук прихованих загроз, вдосконалення правил виявлення та підвищення ефективності роботи систем моніторингу.

Координацію роботи всіх спеціалістів здійснює керівник SOC (SOC Manager). Він відповідає за організацію роботи підрозділу, контроль виконання завдань, взаємодію з іншими підрозділами організації та підготовку звітності для керівництва.

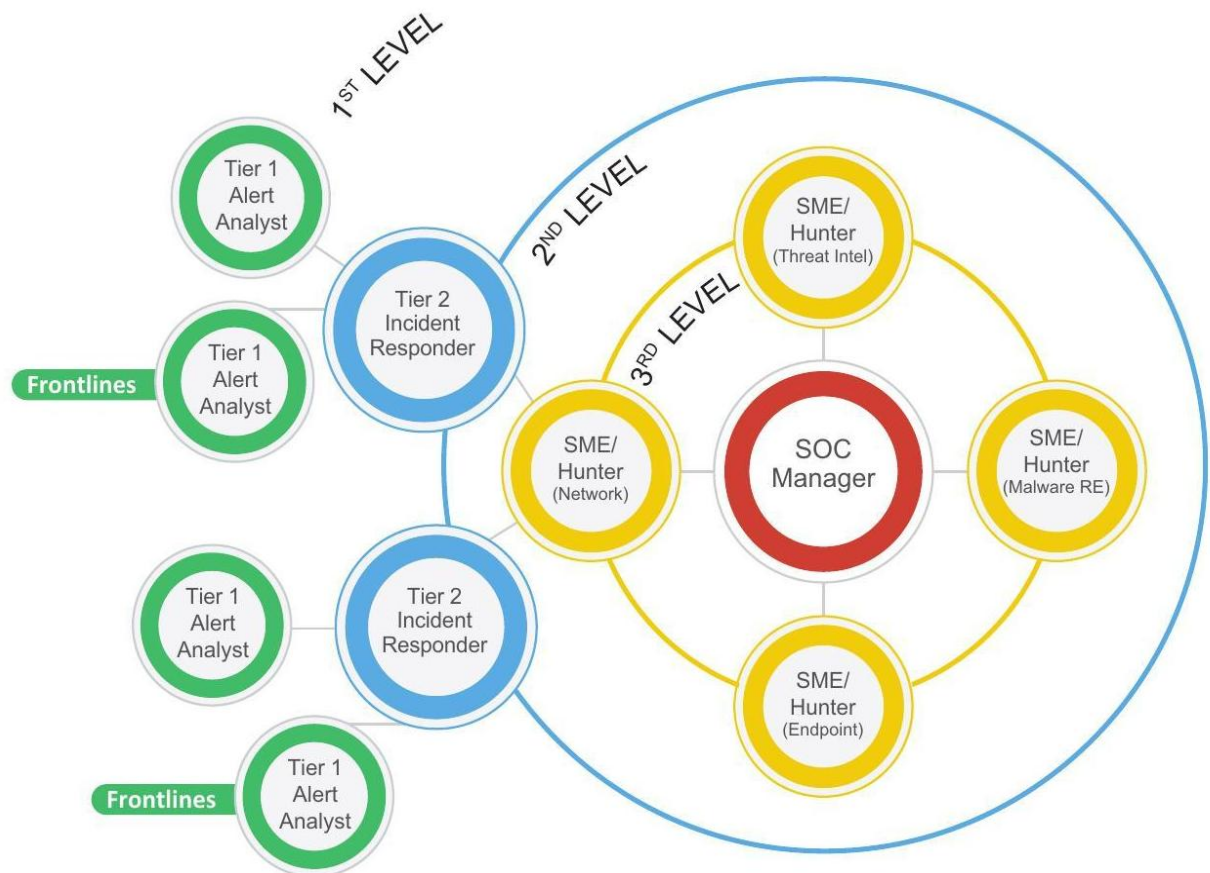


Рисунок 1.2 – Структура ролей Security Operations Center

Використання багаторівневої структури дозволяє ефективно розподілити навантаження між працівниками та забезпечити швидке реагування на інциденти інформаційної безпеки.

Основні завдання та переваги використання SOC

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Головною метою функціонування SOC є забезпечення безперервного контролю за станом інформаційної безпеки організації. Для цього здійснюється цілодобовий моніторинг усіх компонентів інформаційної інфраструктури, аналізуються журнали подій та контролюється робота засобів захисту.

До основних завдань SOC можна віднести:

- виявлення підозрілої активності;
- контроль дотримання політик безпеки;
- моніторинг роботи критичних інформаційних систем;
- реагування на інциденти безпеки;
- проведення аудиту подій;
- аналіз вразливостей та ризиків.

Однією з головних переваг використання SOC є скорочення часу виявлення інцидентів. Чим швидше буде виявлено атаку, тим меншими будуть можливі наслідки для організації. Крім того, централізований підхід до моніторингу дозволяє отримати повну картину подій, що відбуваються в інформаційній інфраструктурі.

Ще однією важливою перевагою є можливість накопичення та аналізу великих обсягів даних. Завдяки використанню сучасних засобів моніторингу можна виявляти приховані загрози та визначати закономірності в поведінці користувачів і систем.

Створення власного SOC потребує значних фінансових витрат та наявності кваліфікованого персоналу. Саме тому багато організацій використовують аутсорсингові центри моніторингу безпеки або комбінують власні та зовнішні ресурси.

SOC є одним із ключових елементів сучасної системи кіберзахисту. Його використання дозволяє забезпечити постійний контроль за станом інформаційної безпеки, своєчасно виявляти кіберзагрози та ефективно реагувати на інциденти. У сучасних умовах саме центри моніторингу безпеки стають основою побудови комплексної системи захисту інформаційних ресурсів організації[9].

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		12

1.2 Аналіз процесів функціонування SIEM-систем

З розвитком інформаційних технологій значно збільшилась кількість подій, які генеруються різними компонентами інформаційної інфраструктури. Сервери, робочі станції, мережеве обладнання, міжмережеві екрани та інші системи безпеки постійно створюють журнали подій, що містять інформацію про роботу системи та дії користувачів. У великих організаціях кількість таких подій може сягати десятків або навіть сотень тисяч на добу, що суттєво ускладнює їх ручний аналіз.

Для вирішення цієї проблеми використовуються SIEM-системи (Security Information and Event Management). Даний клас програмного забезпечення призначений для централізованого збору, зберігання, аналізу та обробки подій інформаційної безпеки, які надходять від різних джерел інформації[2].

Поява SIEM-систем стала результатом об'єднання двох окремих напрямів розвитку засобів інформаційної безпеки (рис.1.3):

- SIM (Security Information Management) – систем управління інформацією безпеки;
- SEM (Security Event Management) – систем управління подіями безпеки.

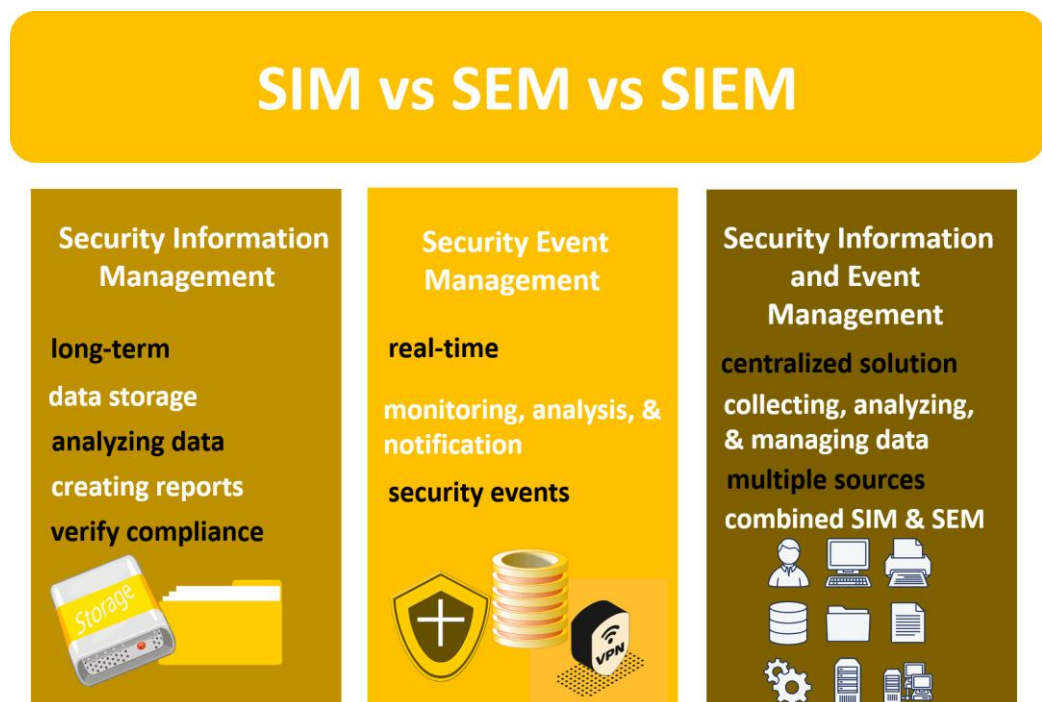


Рисунок 1.3 – Порівняння SIM, SEM та SIEM систем[26]

SIM–системи були розраховані на довгострокове зберігання журналів подій. Їх основне завдання полягало в накопиченні даних, формуванні звітів та перевірці відповідності вимогам різних регуляторів. Завдяки цьому адміністратори могли повертатись до старих подій і проводити детальний аналіз вже після того як інцидент стався. Головним недоліком таких систем була відсутність можливості реагувати на загрози в момент їх виникнення.

SEM–системи вирішували протилежне завдання вони були орієнтовані на роботу в режимі реального часу. Система збирала події з різних джерел, одразу їх аналізувала і при виявленні підозрілої активності повідомляла адміністратора. Але при цьому тривале зберігання даних та можливість глибокого ретроспективного аналізу в таких системах були відсутні.

Стало зрозуміло що обидва підходи мають свої переваги і недоліки, і жоден з них окремо не закриває всіх потреб. Саме тому виникла ідея об'єднати їх в одному рішенні. Так з'явилися сучасні SIEM–системи які поєднують в собі і довгострокове зберігання логів і моніторинг у реальному часі і кореляцію подій і автоматичне виявлення загроз[26]. По суті SIEM став інструментом який закриває одразу всі задачі пов'язані з моніторингом безпеки в одному місці

Основною метою використання SIEM–систем є отримання єдиного центру моніторингу інформаційної безпеки організації (рис. 1.4). Завдяки цьому спеціалісти можуть отримувати інформацію про стан інфраструктури з одного інтерфейсу без необхідності окремого аналізу кожного сервера або мережевого пристрою.

У загальному випадку SIEM–система отримує журнали подій від різних джерел, після чого виконує їх обробку, аналіз та зберігання. На основі отриманих даних система формує сповіщення про підозрілу активність та допомагає спеціалістам виявляти інциденти інформаційної безпеки.

До основних джерел подій для SIEM–систем належать(рис.1.4):

- серверні операційні системи;
- робочі станції користувачів;
- мережеві комутатори та маршрутизатори;
- міжмережеві екрани;

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		14

- системи виявлення вторгнень;
- антивірусні засоби;
- вебсервери та сервери баз даних;
- хмарні сервіси.

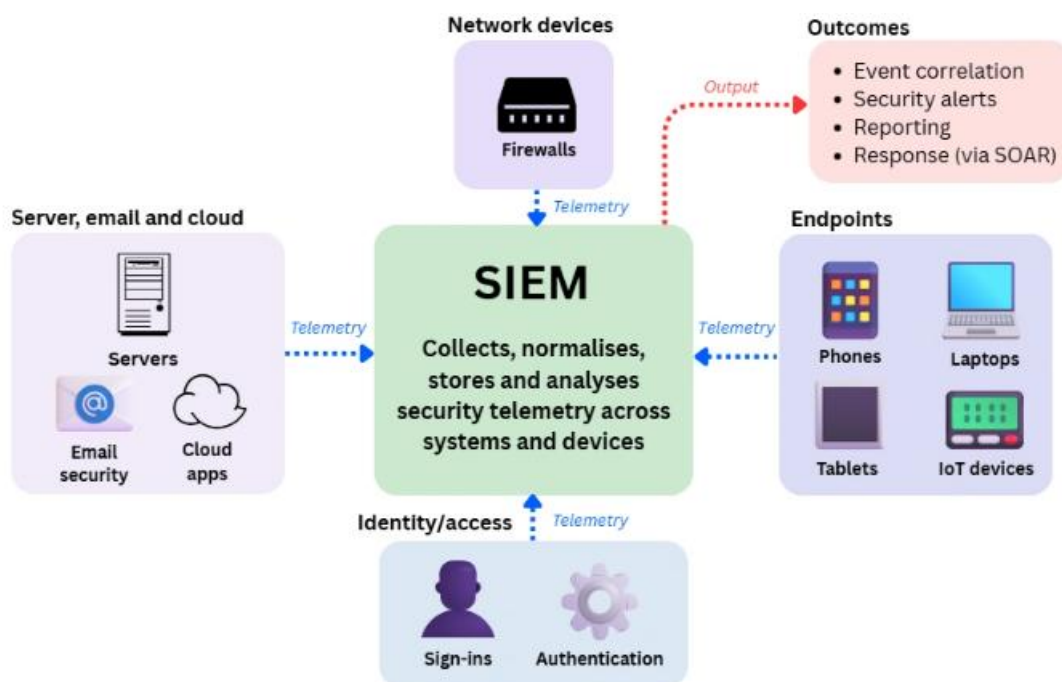


Рисунок 1.4 – Принцип роботи SIEM–системи

Централізований збір інформації дозволяє отримати повну картину подій, які відбуваються в інформаційній системі організації.

Однією з найважливіших функцій SIEM–систем є збір журналів подій. Система автоматично отримує інформацію від різних джерел та зберігає її у єдиному сховищі. Це дозволяє уникнути ситуацій, коли журнали подій розташовані на різних пристроях і потребують окремого аналізу.

Після отримання інформації виконується її нормалізація. Різні виробники програмного забезпечення використовують власні формати журналів подій, тому SIEM–система перетворює їх до єдиного стандартного вигляду. Завдяки цьому події від різних джерел можуть аналізуватися однаковою способом.

Наступною важливою функцією є кореляція подій. Кореляція дозволяє встановити взаємозв'язок між окремими подіями та об'єднати їх у єдиний ланцюг дій.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		15

Наприклад, декілька невдалих спроб входу до системи з подальшим успішним входом можуть свідчити про атаку типу brute force. Окремо кожна з цих подій може не викликати підозри, однак їх аналіз у сукупності дозволяє виявити потенційну загрозу[3].

Ще однією важливою функцією SIEM-систем є формування сповіщень та інцидентів безпеки. У разі виявлення підозрілої активності система автоматично повідомляє адміністратора або аналітика безпеки про можливу загрозу. Це дозволяє значно скоротити час реагування на інциденти.

Крім цього, SIEM-рішення забезпечують довготривале зберігання журналів подій. Це особливо важливо під час проведення розслідувань інцидентів інформаційної безпеки, коли необхідно проаналізувати події, які відбулися декілька тижнів або навіть місяців тому.

До основних функцій SIEM-систем можна віднести:

- централізований збір журналів подій;
- нормалізацію отриманих даних;
- кореляцію подій безпеки;
- виявлення підозрілої активності;
- формування інцидентів безпеки;
- моніторинг подій у режимі реального часу;
- зберігання журналів подій;
- формування звітів та аналітичних матеріалів.

Таблиця 1.1

Основні функції SIEM-систем

Функція	Опис функції	Практичне значення
Збір логів	Отримання журналів подій від серверів, робочих станцій, мережевого обладнання та засобів захисту	Забезпечує централізоване накопичення інформації про події безпеки

Продовження Таблиці 1.1

Нормалізація даних	Перетворення подій різних форматів до єдиного стандартного вигляду	Спрощує подальший аналіз інформації
Кореляція подій	Встановлення взаємозв'язків між окремими подіями з різних джерел	Дозволяє виявляти складні атаки та інциденти
Моніторинг у реальному часі	Безперервне спостереження за станом інформаційної інфраструктури	Скорочує час виявлення загроз
Виявлення інцидентів	Аналіз подій та визначення підозрілої активності	Допомагає оперативно реагувати на загрози
Формування сповіщень	Автоматичне інформування про потенційно небезпечні події	Полегшує роботу аналітиків безпеки
Зберігання журналів	Архівування подій для подальшого аналізу та аудиту	Дозволяє проводити розслідування інцидентів
Формування звітів	Створення звітів щодо стану інформаційної безпеки	Забезпечує контроль та оцінку рівня захищеності
Пошук та аналіз подій	Швидкий пошук інформації серед великого обсягу журналів	Прискорює розслідування кіберінцидентів
Підтримка аудиту	Надання інформації про події безпеки за визначений період	Допомагає виконувати вимоги стандартів та нормативних документів

Сьогодні SIEM–системи є невід'ємною складовою сучасних центрів моніторингу безпеки. Їх використання дозволяє автоматизувати процес аналізу подій, підвищити ефективність виявлення загроз та забезпечити оперативне реагування на інциденти інформаційної безпеки. Саме тому SIEM–рішення широко застосовуються як у комерційних організаціях, так і в державних установах[4].

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				17
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3 Огляд сучасних SIEM-рішень

Сьогодні ринок засобів моніторингу інформаційної безпеки представлений великою кількістю SIEM-рішень. Кожна платформа має власні особливості, архітектуру, підхід до обробки подій та механізми виявлення загроз. Незважаючи на спільну мету, різні системи можуть суттєво відрізнятися за функціональними можливостями, складністю впровадження, вимогами до інфраструктури та вартістю експлуатації.

Вибір конкретної SIEM-платформи залежить від багатьох факторів. До них належать розмір організації, кількість джерел подій, вимоги до швидкодії, наявність кваліфікованого персоналу та фінансові можливості підприємства. Саме тому перед впровадженням системи моніторингу безпеки доцільно виконати аналіз найбільш поширених рішень, які використовуються на практиці.

Однією з найвідоміших платформ є IBM QRadar. Дане рішення широко використовується як у комерційних структурах, так і в державному секторі. Система забезпечує централізований збір журналів подій, аналіз мережевого трафіку, кореляцію подій та автоматичне формування інцидентів безпеки. Однією з особливостей QRadar є можливість одночасно працювати як з логами, так і з мережевими потоками даних (Network Flows), що дозволяє отримувати більш повну інформацію про події, які відбуваються в мережі.

Платформа використовує механізм Offense Management, завдяки якому окремі події автоматично групуються в інциденти. Це дозволяє аналітикам швидше оцінювати ситуацію та концентрувати увагу на дійсно важливих загрозах. Крім того, система має значну кількість готових правил кореляції та підтримує інтеграцію з великою кількістю програмних продуктів різних виробників[10].

До основних переваг IBM QRadar можна віднести:

- потужні механізми кореляції подій;
- підтримку великої кількості джерел логів;
- можливість аналізу мережеских потоків;
- зручний механізм формування інцидентів безпеки;
- широкий набір вбудованих правил виявлення загроз.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Серед недоліків можна виділити високі вимоги до апаратних ресурсів та значну вартість комерційних ліцензій.

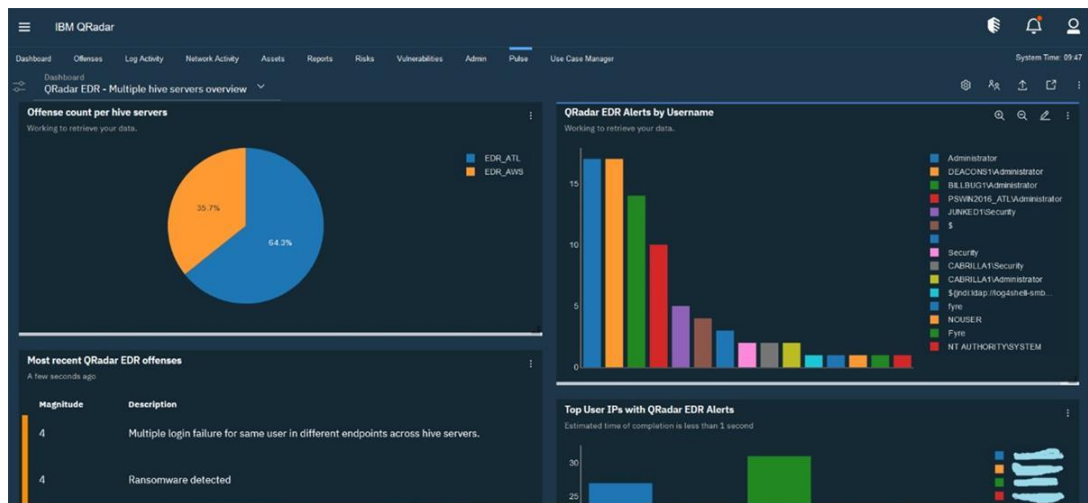


Рисунок 1.5 – Інтерфейс та основні компоненти IBM QRadar

Популярне рішення Splunk Enterprise Security. Дана система побудована на платформі Splunk та орієнтована на збір і аналіз великих обсягів даних. Однією з головних переваг Splunk вважається потужний механізм пошуку та гнучкі інструменти візуалізації інформації. Аналітики можуть створювати складні запити для пошуку подій та формувати власні інформаційні панелі[26].

Основними перевагами Splunk є:

- висока швидкість пошуку інформації;
- гнучкі можливості налаштування;
- розвинуті засоби візуалізації даних;
- підтримка великої кількості джерел подій.

Недоліки:

- висока вартість ліцензування;
- значні вимоги до серверної інфраструктури;
- складність адміністрування великих середовищ.



Рисунок 1.6 – Інформаційна панель моніторингу безпеки Splunk Enterprise Security

Microsoft Sentinel. Платформа функціонує на базі хмарної інфраструктури Microsoft Azure та забезпечує централізований моніторинг подій безпеки без необхідності розгортання власних серверів. Sentinel активно використовує можливості штучного інтелекту та машинного навчання для виявлення аномальної активності[4].

Перевагою такого підходу є швидке розгортання та простота масштабування. Організація може збільшувати обсяг оброблюваних даних без придбання додаткового обладнання. Водночас використання хмарної моделі не завжди є прийнятним для державних структур або підприємств, які мають обмеження щодо зберігання даних за межами власної інфраструктури.

До переваг Microsoft Sentinel належать:

- швидке розгортання;
- простота масштабування;
- інтеграція з сервісами Microsoft Azure;
- використання сучасних алгоритмів аналізу даних.

Недоліки:

- залежність від хмарної інфраструктури;
- постійні витрати на використання ресурсів Azure;
- можливі обмеження щодо зберігання даних у державних установах.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				20
Змн.	Арк.	№ докум.	Підпис	Дата		

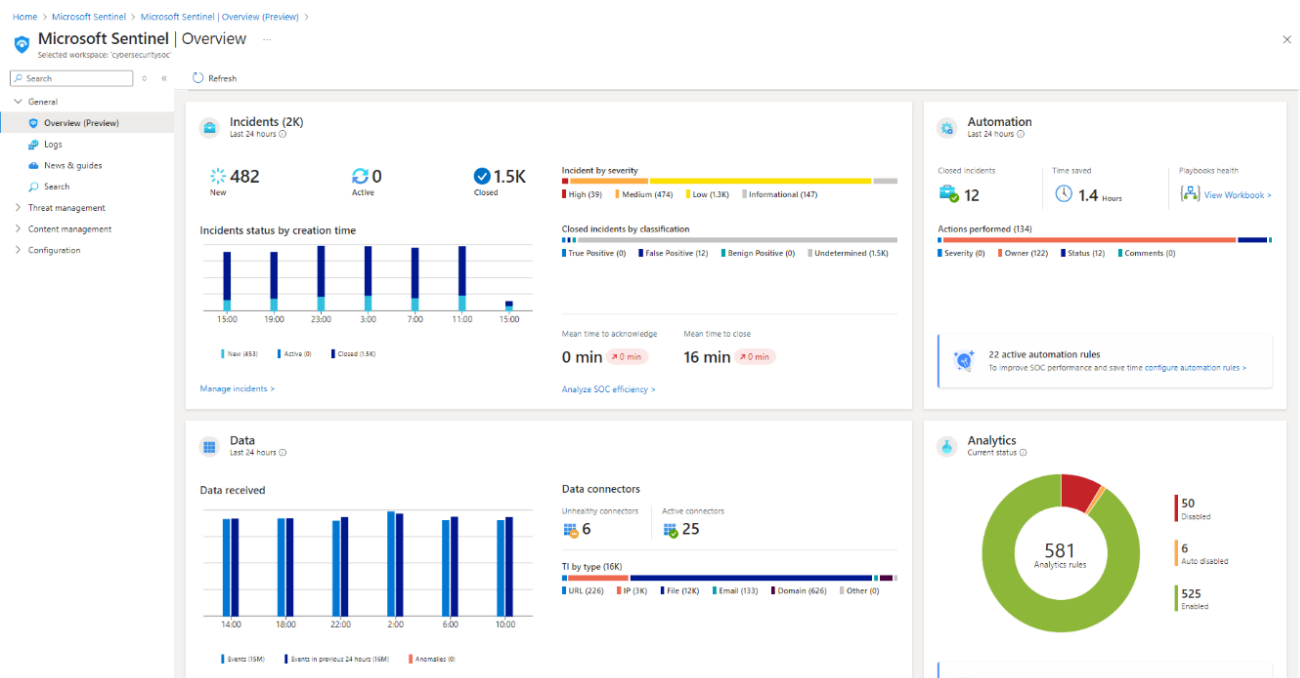


Рисунок 1.7 – Інтерфейс Microsoft Sentinel

Ще одним відомим представником класу SIEM є ArcSight ESM. Ця платформа тривалий час вважалася одним із лідерів ринку інформаційної безпеки. Система має потужні механізми кореляції подій та підтримує інтеграцію з великою кількістю джерел даних.

Основними перевагами ArcSight є:

- глибокий аналіз подій безпеки;
- висока деталізація інформації;
- широкі можливості налаштування правил кореляції.

Недоліки:

- складність впровадження;
- високі вимоги до кваліфікації персоналу;
- значні витрати на підтримку та супровід.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				21
Змн.	Арк.	№ докум.	Підпис	Дата		

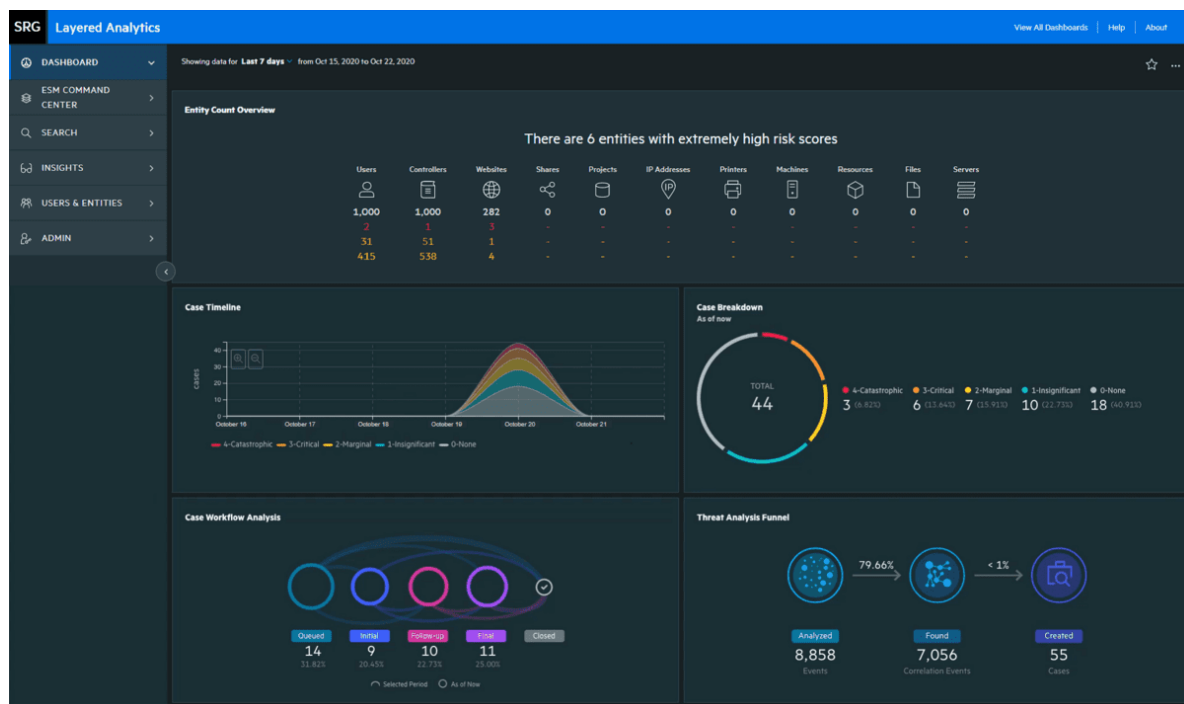


Рисунок 1.8 – Интерфейс ArcSight

Платформа Wazuh, яка останніми роками набула значної популярності серед фахівців з кібербезпеки. На відміну від більшості комерційних продуктів, Wazuh поширюється з відкритим вихідним кодом і може використовуватися без придбання дорогих ліцензій.

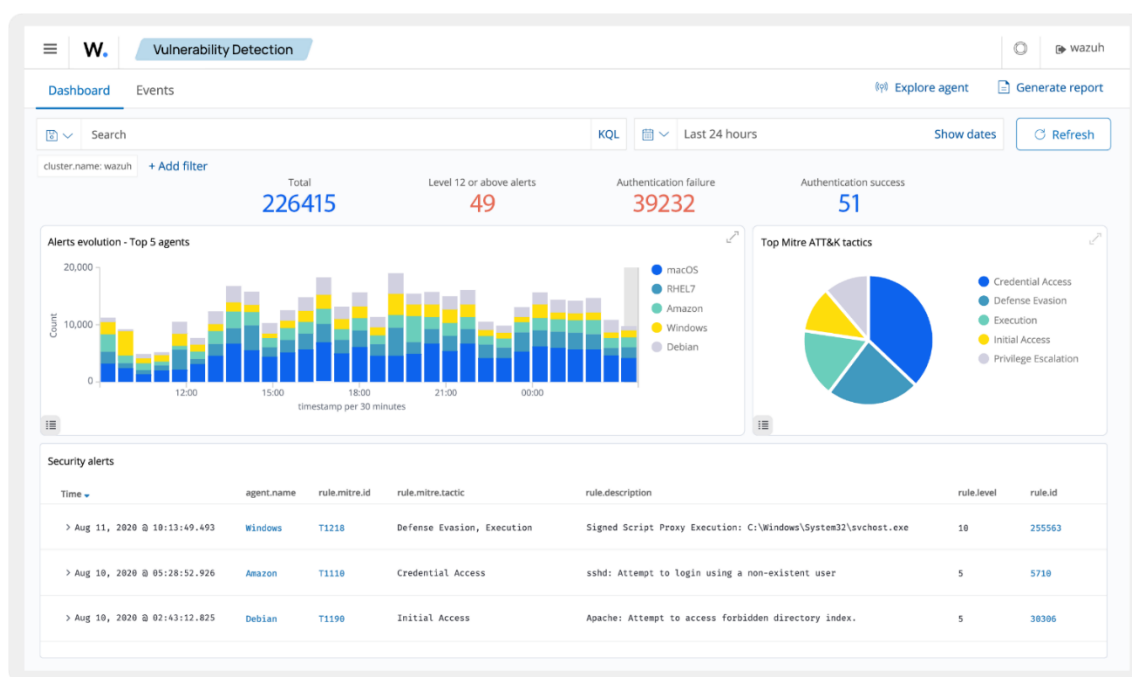


Рисунок 1.9 – Dashboard Wazuh

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Основними можливостями Wazuh є збір журналів подій, контроль цілісності файлів, виявлення шкідливого програмного забезпечення та моніторинг стану безпеки кінцевих пристроїв. Платформа добре підходить для навчальних лабораторій та невеликих організацій, однак у великих інфраструктурах може поступатися комерційним рішенням за рівнем автоматизації та масштабованості[23].

Крім зазначених продуктів, на ринку представлені також LogRhythm, RSA NetWitness, AlienVault USM та інші рішення. Проте саме IBM QRadar, Splunk, Microsoft Sentinel, ArcSight та Wazuh найчастіше згадуються під час побудови сучасних центрів моніторингу безпеки.

Для більш наочного порівняння доцільно розглянути основні характеристики зазначених платформ[10,26].

Таблиця 1.2

Порівняльний аналіз сучасних SIEM-платформ

Критерій	IBM QRadar	Splunk ES	MS Sentinel	ArcSight ESM	Wazuh
Тип ліцензії	Комерційна	Комерційна	Комерційна (SaaS)	Комерційна	Open Source
Інтеграції	450+ DSM	Marketplace	Azure-native	SmartConnectors	Агентна архітектура
Механізм кореляції	Вбудований	SPL (гнучкий)	KQL + правила	Вбудований	Вбудований
Аналіз мережевого трафіку	QFlow (нативний)	Stream4Flow	Azure Network Logs	NetFlow	Обмежено
UEBA	QRadar UBA	Додатковий модуль	Вбудована	AI Engine	Обмежено

MITRE ATT&CK	Повна під- тримка	Через дода- тки	Через до- датки	Часткова	Часткова
Хмарна підтримка	Cloud / On–Prem	Cloud / On– Prem	Azure	On–Prem	On–Prem
Складність впрова- дження	Середня	Висока	Середня	Висока	Низька
Вартість викорис- тання	Висока	Висока	Середня	Висока	Низька
Відкритий код	Ні	Ні	Ні	Ні	Так

1.4 Обґрунтування вибору платформи IBM QRadar

Після аналізу існуючих SIEM–рішень постало питання вибору конкретної платформи для реалізації лабораторного стенду. IBM QRadar є одним із найпоширеніших SIEM–рішень у світі. Його використовують банки, державні установи, телекомунікаційні компанії та великі корпорації де вимоги до безпеки є особливо жорсткими. Платформа регулярно потрапляє до лідерів магічного квадранту Gartner у категорії SIEM що є одним із найавторитетніших галузевих рейтингів[10].

Для навчального проєкту це має принципове значення. Робота з реальним промисловим продуктом дає навички які безпосередньо застосовуються на практиці. На відміну від навчальних симуляторів QRadar – це те саме рішення яке використовується у реальних SOC–центрах по всьому світу.

Підтримка різномірних джерел подій

Під час проєктування лабораторного стенду передбачалося використання декількох різних операційних систем та програмних продуктів. До складу стенду

увійшли Windows Server 2019, Windows 10, Kali Linux та міжмережевий екран OPNsense. Кожен із зазначених компонентів генерує власні журнали подій у різних форматах. Для коректного аналізу таких подій необхідний механізм їх приведення до єдиного формату. У платформі IBM QRadar ця задача реалізована за допомогою спеціальних модулів підтримки пристроїв DSM (Device Support Module).

Використання DSM дозволяє автоматично розпізнавати тип джерела подій та виконувати нормалізацію журналів без необхідності створення складних механізмів обробки вручну. IBM QRadar підтримує понад 450 DSM модулів що забезпечує сумісність з практично будь-яким обладнанням або програмним забезпеченням яке використовується в корпоративних середовищах. У результаті події від різних систем можуть аналізуватися за однаковими правилами що значно спрощує процес моніторингу та подальшого розслідування інцидентів безпеки[13].

Збір та управління журналами подій

Однією з базових функцій QRadar є централізований збір журналів подій з усіх джерел інфраструктури. Ще одним важливим фактором під час вибору платформи стала підтримка стандартних механізмів передачі журналів подій. Більшість пристроїв та програмних продуктів які використовуються в лабораторному стенді підтримують протокол Syslog. IBM QRadar дозволяє приймати такі повідомлення без встановлення додаткових серверних компонентів що значно спрощує процес інтеграції джерел подій у єдине середовище моніторингу.

Платформа підтримує широкий спектр протоколів збору даних:

- Syslog UDP та TCP,
- JDBC для підключення до баз даних,
- SNMP для мережевого обладнання,
- WMI для Windows систем
- спеціалізовані протоколи для хмарних сервісів.

Після збору всі журнали нормалізуються та зберігаються в єдиному форматі в базі даних Ariel. Це дозволяє виконувати єдині пошукові запити одночасно по всіх джерелах незалежно від їх початкового формату. Адміністратор може знайти

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		25

всі події пов'язані з конкретним IP, конкретним користувачем або конкретним типом активності за будь-який період часу. QRadar підтримує стиснення та оптимізоване зберігання журналів що дозволяє зберігати великі обсяги даних протягом тривалого часу відповідно до вимог регуляторів[12].

Аналіз подій у реальному часі

Важливим критерієм під час вибору SIEM-системи була також можливість аналізу подій у режимі реального часу. У процесі функціонування інформаційної інфраструктури щосекунди можуть генеруватися десятки або сотні подій різного типу. Для оперативного виявлення потенційних загроз необхідно забезпечити їх своєчасну обробку та відображення. У IBM QRadar для цього використовується модуль Log Activity, який дозволяє відстежувати надходження подій практично одразу після їх виникнення.

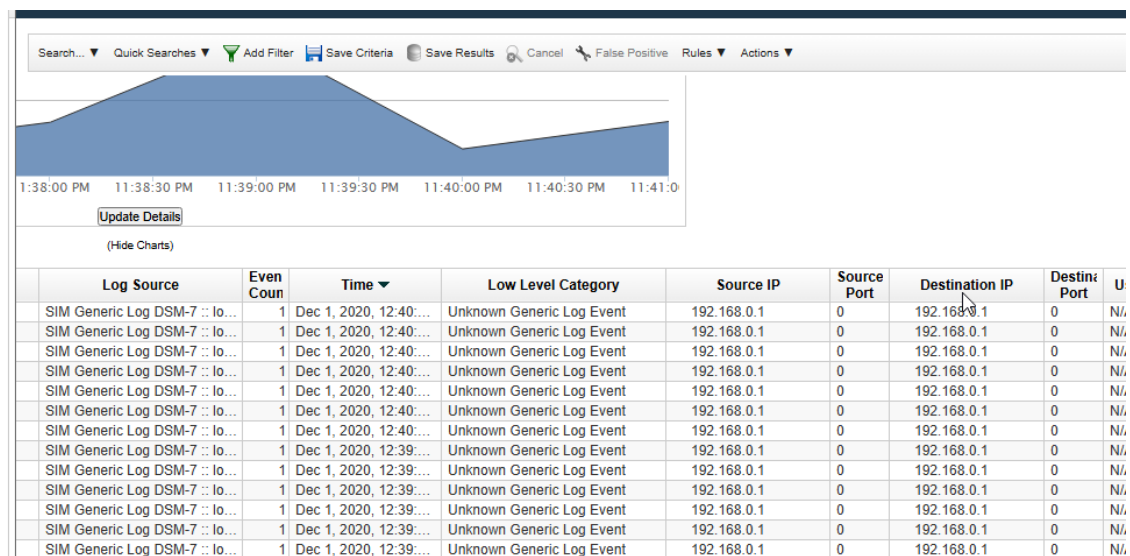


Рисунок 1.10 – Інтерфейс Log Activity

Інтерфейс Log Activity надає можливість виконувати пошук подій за різними критеріями, здійснювати їх фільтрацію та аналізувати окремі параметри. Це особливо важливо під час проведення досліджень та тестування системи моніторингу, оскільки дозволяє швидко перевіряти результати виконання різних сценаріїв імітації атак.

Кореляція подій та виявлення загроз

Кореляція подій є ключовою функцією яка відрізняє SIEM від простого агрегатора логів. Correlation Engine QRadar аналізує безперервний потік подій та шукає між ними зв'язки на основі правил. Правила кореляції поділяються на три типи:

- Прості правила спрацьовують при виявленні однієї конкретної події. Наприклад спроба входу з заблокованого облікового запису або підключення з підозрілої IP адреси.
- Складні правила аналізують послідовності або комбінації подій. Класичний приклад велика кількість невдалих спроб автентифікації з одного IP з подальшим успішним входом що є характерним патерном brute force атаки.
- Аномальні правила виявляють відхилення від нормальної поведінки. Якщо користувач який щодня входить о 9 ранку раптом починає підключатись о 3 ночі це підозріло навіть якщо сам вхід технічно успішний.

QRadar постачається з великим набором готових правил що охоплюють найпоширеніші типи атак. Адміністратор може їх адаптувати або створювати власні через графічний редактор.

Управління інцидентами через Offenses(рис.1.11)

Коли правило кореляції спрацьовує QRadar створює Offense – інцидент безпеки. Замість того щоб аналітик переглядав сотні окремих подій – система формує єдиний інцидент з усією необхідною інформацією. Кожен Offense містить:

- джерело атаки – IP адресу та геолокацію зловмисника
- цільовий хост – яка система атакується
- тип атаки та правило кореляції яке спрацювало
- рівень серйозності від 1 до 10
- часову мітку початку та тривалість інциденту
- повний перелік усіх пов'язаних подій

Offenses можна призначати конкретним аналітикам, встановлювати статуси та додавати коментарі. Це дозволяє організувати командну роботу при реагуванні на інциденти та зберігати повну історію розслідування.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Таким чином весь процес обробки подій у IBM QRadar проходить сім послідовних кроків – від отримання журналів з джерел до відображення інциденту в консолі аналітика. На першому кроці Event Collector приймає події від усіх джерел через протокол Syslog. На другому кроці DSM модулі розпізнають формат кожного джерела та нормалізують події до єдиного стандарту. На третьому кроці Event Processor класифікує та збагачує події підготовлюючи їх до аналізу. На четвертому кроці Correlation Engine застосовує правила кореляції та шукає патерни атак. На п'ятому кроці при виявленні підозрілого патерну система генерує Offense та сповіщає аналітика. Паралельно на шостому кроці всі події зберігаються в базі даних Ariel для подальшого пошуку та розслідування. На сьомому кроці аналітик отримує доступ до всієї інформації через QRadar Console веб-інтерфейс який об'єднує Dashboard, Log Activity, Offenses та Reports в одному місці.

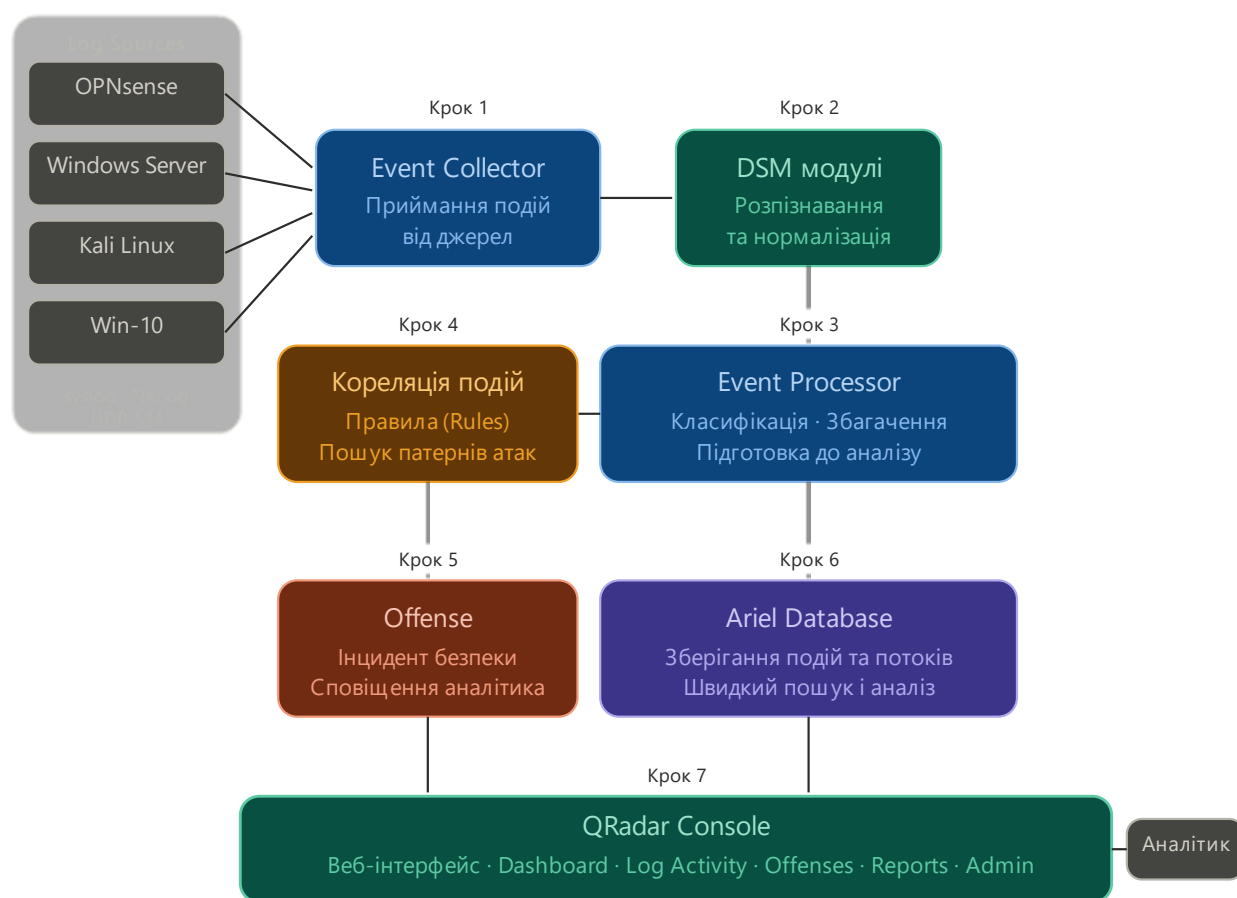


Рисунок 1.11 – Схема обробки подій в IBM Qradar

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				28
Змн.	Арк.	№ докум.	Підпис	Дата		

Dashboard та візуалізація

Використання Dashboard значно спрощує процес аналізу стану інформаційної безпеки та дозволяє отримати загальне уявлення про ситуацію в мережі без необхідності перегляду великої кількості журналів подій. Такий підхід широко застосовується в реальних центрах моніторингу безпеки та є однією з важливих складових сучасних SIEM-рішень.

Ще однією причиною вибору IBM QRadar стала можливість роботи з інцидентами безпеки через механізм Offense Management. На відміну від багатьох традиційних систем журналювання, QRadar не обмежується відображенням окремих подій. Система дозволяє групувати взаємопов'язані події та представляти їх у вигляді єдиного інциденту безпеки.

Такий підхід суттєво полегшує роботу аналітика, оскільки замість аналізу сотень окремих записів він отримує вже сформований інцидент із зазначенням його джерела, рівня критичності та пов'язаних подій. Саме тому механізм Offense є одним із ключових компонентів платформи IBM QRadar.

Для реалізації лабораторного стенду також важливе значення мала можливість використання безкоштовної версії системи. Комерційні редакції IBM QRadar потребують придбання ліцензії та відповідної серверної інфраструктури. Водночас компанія IBM надає версію Community Edition, яка призначена для навчальних та дослідницьких цілей.

IBM QRadar Community Edition містить більшість функціональних можливостей повноцінної версії продукту та дозволяє ознайомитися з основними принципами роботи системи моніторингу безпеки. Незважаючи на обмеження щодо кількості оброблюваних подій, дана редакція є достатньою для побудови лабораторного стенду та проведення досліджень у межах дипломної роботи.

Важливою перевагою Community Edition є можливість її розгортання у віртуальному середовищі. Це дозволяє використовувати платформу на звичайному персональному комп'ютері без придбання спеціалізованого серверного обладнання. Саме цей фактор став одним із визначальних під час створення лабораторного стенду на базі Oracle VirtualBox.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Отже, вибір IBM QRadar для реалізації даної роботи обумовлений можливістю централізованого збору та аналізу журналів подій, підтримкою великої кількості джерел інформації, наявністю механізмів кореляції подій та обробки інцидентів, а також доступністю версії Community Edition для використання в навчальному середовищі. Сукупність зазначених факторів дозволяє використовувати дану платформу як основу для побудови лабораторного стенду та дослідження процесів моніторингу інформаційної безпеки.

1.5 Постановка технічного завдання

Метою даної кваліфікаційної роботи є проєктування та побудова лабораторного стенду системи моніторингу інформаційної безпеки на базі платформи IBM QRadar. Розроблений стенд повинен моделювати роботу невеликої корпоративної мережі та забезпечувати можливість централізованого збору, обробки й аналізу подій безпеки, що надходять від різних джерел.

У межах роботи передбачається створення віртуального середовища, максимально наближеного до реальної корпоративної інфраструктури. Для цього планується використання декількох віртуальних машин, кожна з яких виконуватиме окрему функцію в мережі. Зокрема, передбачається використання контролера домену на базі Windows Server 2019, робочої станції Windows 10, міжмережевого екрану OPNsense, системи моніторингу IBM QRadar та тестової машини Kali Linux для моделювання дій потенційного зловмисника.

Для досягнення поставленої мети необхідно виконати такі завдання:

- розробити структуру лабораторного стенду та визначити склад його основних компонентів;
- спроектувати логічну схему корпоративної мережі та виконати її реалізацію у середовищі Oracle VirtualBox;
- налаштувати внутрішню мережу типу Internal Network для забезпечення взаємодії між усіма вузлами стенду;

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				30
Змн.	Арк.	№ докум.	Підпис	Дата		

- розгорнути та налаштувати міжмережевий екран OPNsense, який виконуватиме функції маршрутизації, фільтрації мережевого трафіку та централізованого логування подій;
- встановити та налаштувати Windows Server 2019 з роллю Active Directory Domain Services;
- створити доменне середовище та забезпечити підключення робочої станції Windows 10 до домену;
- виконати розгортання IBM QRadar Community Edition та підготувати платформу до прийому журналів подій;
- налаштувати передачу журналів подій від усіх джерел до SIEM–системи за допомогою протоколу Syslog та спеціалізованих агентів збору логів;
- перевірити коректність надходження подій до системи моніторингу та їх відображення у розділі Log Activity;
- виконати моделювання типових загроз інформаційній безпеці за допомогою інструментів Kali Linux;
- провести мережеву розвідку, імітацію підбору паролів та інші тестові дії для перевірки можливостей системи моніторингу;
- здійснити аналіз отриманих результатів та оцінити ефективність побудованого лабораторного стенду;
- визначити проблеми, які виникли під час розгортання та налаштування системи, а також розглянути можливі способи їх усунення;
- сформулювати висновки щодо доцільності використання IBM QRadar для моніторингу подій інформаційної безпеки.

Результатом виконання роботи має стати функціонуючий лабораторний стенд, який дозволяє здійснювати збір подій безпеки від різних джерел, виконувати їх централізований аналіз та досліджувати принципи функціонування сучасних SIEM–систем на прикладі платформи IBM QRadar.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до розділу 1

У першому розділі було розглянуто теоретичні основи побудови систем моніторингу інформаційної безпеки. Проведено аналіз поняття та організації Security Operations Center (SOC), визначено його основні функції та роль у забезпеченні кібербезпеки організації. Також досліджено призначення SIEM-систем, принципи їх роботи та можливості щодо централізованого збору, зберігання й аналізу журналів подій. Встановлено, що сучасні SIEM-рішення дозволяють автоматизувати процес моніторингу інформаційної безпеки та забезпечують своєчасне виявлення підозрілої активності в мережі.

Крім того, було виконано огляд найбільш поширених SIEM-платформ та проведено їх порівняльний аналіз. За результатами дослідження для реалізації лабораторного стенду обрано платформу IBM QRadar Community Edition, яка поєднує широкі можливості збору та обробки подій безпеки, підтримує велику кількість джерел логування та може використовуватися в навчальних цілях. Отримані результати стали основою для подальшого проектування лабораторного стенду та побудови підсистеми моніторингу інформаційної безпеки, що розглядається в наступному розділі.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

РОЗДІЛ 2 ПРОЄКТУВАННЯ SIEM–СИСТЕМИ НА БАЗІ IBM QRadar

2.1 Вибір та обґрунтування інструментів

Перед розробкою лабораторного стенду необхідно було визначитися з програмними засобами, які будуть використовуватися для побудови віртуальної інфраструктури та реалізації системи моніторингу інформаційної безпеки. Під час вибору враховувалися такі критерії:

- функціональні можливості програмного забезпечення;
- доступність для використання в навчальних цілях;
- сумісність між окремими компонентами;
- можливість розгортання всього середовища на одному фізичному комп'ютері;
- відповідність технологіям, що використовуються в сучасних корпоративних мережах.

Міжмережевий екран OPNsense

Для реалізації функцій маршрутизації та мережевого захисту було обрано OPNsense. Це програмний міжмережевий екран з відкритим вихідним кодом, побудований на базі операційної системи FreeBSD.

У створеному лабораторному стенді OPNsense виконує такі функції:

- маршрутизація мережевого трафіку;
- трансляція мережевих адрес (NAT);
- фільтрація пакетів за допомогою правил міжмережевого екрану;
- видача IP–адрес через DHCP–сервер;
- пересилання DNS–запитів внутрішніх вузлів.

Для роботи системи було налаштовано два мережевих інтерфейси:

- WAN – забезпечує доступ до зовнішньої мережі через NAT;
- LAN – підключений до внутрішнього сегмента мережі та має адресу 192.168.0.1.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Важливою перевагою OPNsense є підтримка віддаленої передачі журналів через протокол Syslog. Завдяки цьому події мережевої безпеки можуть надсилатися безпосередньо до IBM QRadar для подальшого аналізу.

Серверне середовище та Active Directory

Для реалізації лабораторного стенду обрано Windows Server 2019, оскільки дана версія залишається однією з найпоширеніших серверних операційних систем у корпоративних мережах. Вона забезпечує стабільну роботу служб Active Directory, має тривалий термін підтримки та не потребує значних апаратних ресурсів у порівнянні з новішими версіями Windows Server.

Active Directory забезпечує централізоване керування:

- користувачами;
- комп'ютерами;
- групами безпеки;
- мережевими ресурсами;
- політиками доступу.

Основними функціями Active Directory є:

- Автентифікація – перевірка облікових даних користувача.
- Авторизація – визначення доступних користувачу ресурсів.
- Застосування групових політик (GPO).
- Централізоване адміністрування мережі.

У межах даного стенду контролер домену виступає одним із основних джерел подій безпеки для IBM QRadar.

Робоча станція Windows 10

Для моделювання робочого місця співробітника використовується операційна система Windows 10. Дана віртуальна машина входить до домену Active Directory та виступає кінцевою точкою корпоративної мережі.

Використання робочої станції дозволяє відтворити типові дії користувачів:

- вхід до домену;
- доступ до мережевих ресурсів;

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		34

- роботу з обліковими записами;
- взаємодію із серверними службами.

Крім цього, на робочій станції можна моделювати різні сценарії порушення безпеки та аналізувати реакцію SIEM–системи на такі події.

Інструменти імітації атак Kali Linux

Для перевірки можливостей IBM QRadar щодо виявлення атак використовується Kali Linux. Це спеціалізований дистрибутив Linux, який містить велику кількість інструментів для тестування безпеки та аудиту інформаційних систем.

У роботі використовуються такі засоби:

Nmap – інструмент мережевого сканування, який дозволяє:

- визначати активні вузли;
- виявляти відкриті порти;
- отримувати інформацію про сервіси;
- визначати операційну систему віддаленого хоста.

Hydra використовується для імітації атак типу brute force на різні мережеві служби.

Основні можливості Hydra:

- підтримка великої кількості протоколів;
- багатопотоковий режим роботи;
- автоматизований перебір паролів.

Agrpsproof застосовується для проведення ARP–спуфінгу в локальній мережі.

За допомогою даного інструмента можна:

- підміняти ARP–записи вузлів;
- перенаправляти трафік через комп'ютер зловмисника;
- моделювати атаку типу «людина посередині» (Man-in-the-Middle).

Агенти збору журналів подій

Для передачі подій до IBM QRadar використовуються спеціальні агенти збору логів.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		35

На сервері Windows Server 2019 встановлено NXLog Community Edition, який забезпечує:

- збір подій Windows Event Log;
- перетворення подій у формат Syslog;
- передачу журналів до IBM QRadar.

На Kali Linux використовується syslog-ng, який виконує:

- збір системних журналів Linux;
- фільтрацію подій;
- пересилання повідомлень на SIEM-сервер.

Використання зазначених агентів забезпечує централізований збір подій від усіх вузлів лабораторного стенду та їх подальший аналіз у системі IBM QRadar.(рис.2.1)

Таким чином, обраний набір програмних засобів дозволяє створити повноцінний лабораторний стенд, максимально наближений до умов реального корпоративного середовища, а також забезпечує можливість дослідження роботи SIEM-системи IBM QRadar під час виявлення та аналізу різних типів кіберзагроз.

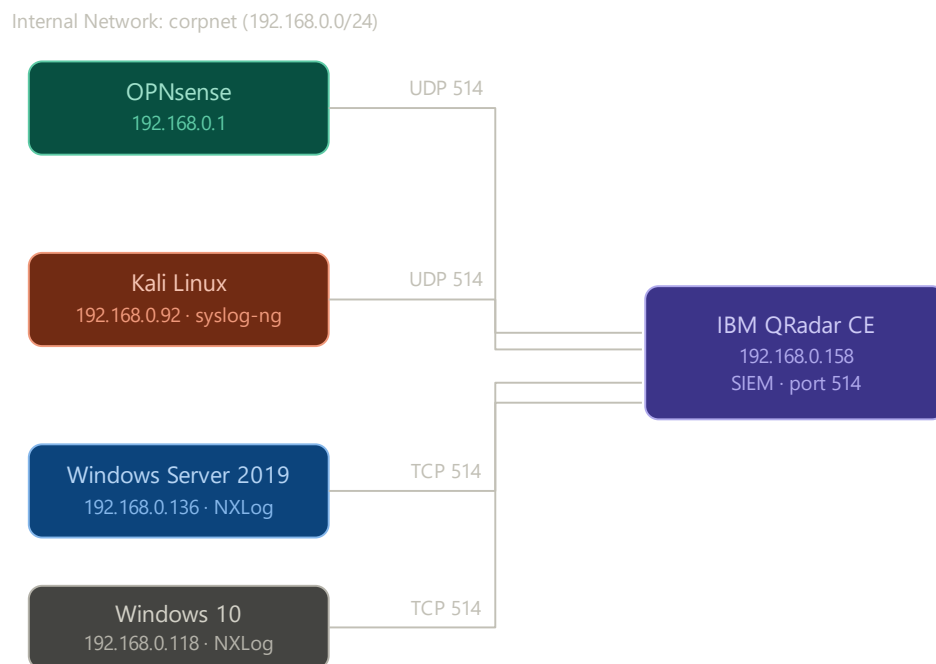


Рисунок 2.1 – Структура збору логів у лабораторному стенді SIEM-системи

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		36

В результаті було сформовано набір інструментів який дозволяє побудувати лабораторний стенд максимально наближений до реального корпоративного середовища і провести повноцінне дослідження роботи SIEM–системи IBM QRadar.

2.2 Проектування мережевої інфраструктури

У межах даної роботи розроблено лабораторний стенд, який моделює роботу невеликої корпоративної мережі. Це дозволяє відтворити процеси взаємодії між серверним обладнанням, робочими станціями та засобами захисту інформації, а також дослідити можливості платформи IBM QRadar щодо централізованого моніторингу подій безпеки.

Спроектована інфраструктура складається з п'яти віртуальних машин, кожна з яких виконує визначену функціональну роль у корпоративному середовищі. Мережева топологія побудована на основі внутрішньої мережі VirtualBox типу Internal Network з ідентифікатором «corpnet», що забезпечує ізольоване середовище для проведення досліджень без ризику впливу на зовнішню мережеву інфраструктуру(рис.2.2).

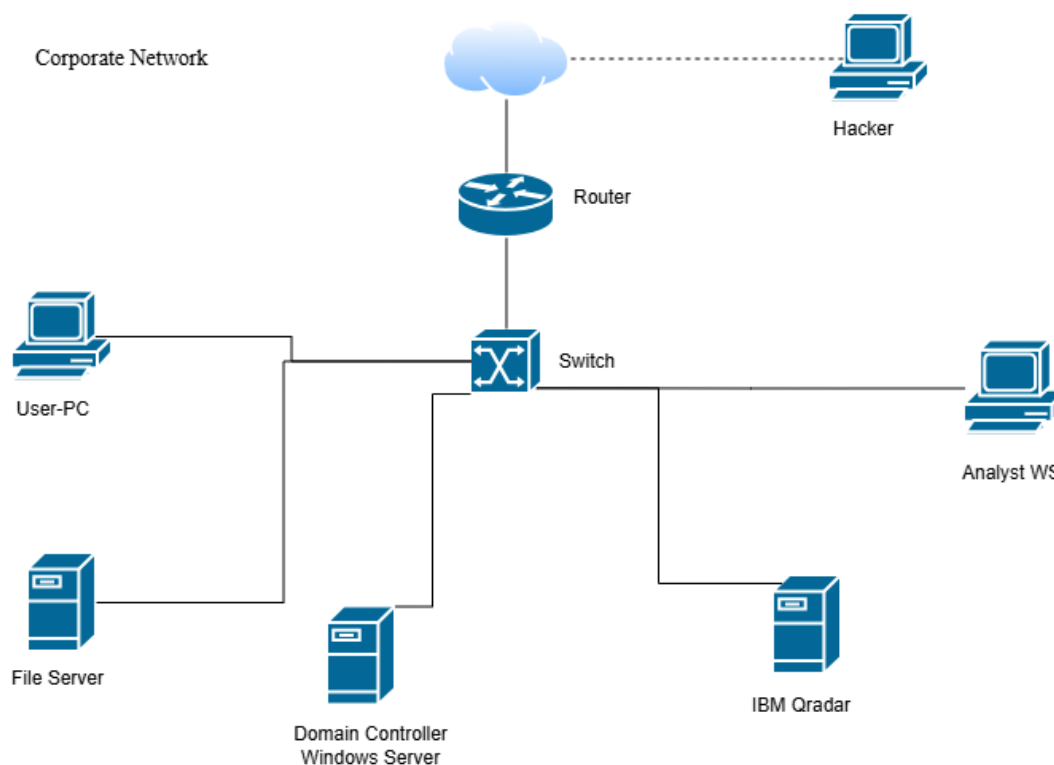


Рисунок 2.2 – корпоративна мережа

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Для забезпечення взаємодії між вузлами мережі в лабораторному стенді використовується міжмережевий екран OPNsense. Даний програмний продукт розгорнуто на окремій віртуальній машині та налаштовано як основний мережевий шлюз. OPNsense побудований на базі операційної системи FreeBSD і поєднує функції маршрутизації мережевого трафіку, міжмережевого екрану та мережевих сервісів.

У межах створеного стенду OPNsense використовує два мережеві інтерфейси. Інтерфейс WAN забезпечує підключення до зовнішньої мережі через механізм NAT, а інтерфейс LAN використовується для роботи внутрішньої корпоративної мережі та має адресу 192.168.0.1. Усі інші вузли лабораторного стенду підключені саме до внутрішнього сегмента мережі через даний шлюз.

Для лабораторного стенду було обрано підмережу 192.168.0.0/24. Використання такої адресації є достатнім для моделювання корпоративної мережі невеликого розміру та забезпечує можливість підключення необхідної кількості мережевих вузлів. Крім функцій маршрутизації, OPNsense також використовується як DHCP-сервер для автоматичної видачі IP-адрес клієнтам мережі та DNS-форвардер для обробки DNS-запитів.

Для основних компонентів інфраструктури було налаштовано статичні IP-адреси. Такий підхід спрощує адміністрування мережі та забезпечує коректну роботу системи моніторингу IBM QRadar. Оскільки SIEM-система ідентифікує джерела подій за їх мережевими адресами, використання статичної адресації дозволяє уникнути проблем із розпізнаванням джерел логів та забезпечує стабільний збір журналів подій. Мережеву адресацію всіх вузлів лабораторного стенду наведено в таблиці 2.1.

Таблиця 2.1

Адресація мережевих вузлів лабораторного стенду

Пристрій	Призначення	IP-адреса	Маска мережі	Шлюз
OPNsense (LAN)	Маршрутизатор, Firewall	192.168.0.1	255.255.255.0	—

Пристрій	Призначення	IP-адреса	Маска мережі	Шлюз
IBM QRadar CE	SIEM-сервер	192.168.0.158	255.255.255.0	192.168.0.1
Windows Server 2019	Контролер домену, джерело логів	192.168.0.136	255.255.255.0	192.168.0.1
Windows 10	Робоча станція	192.168.0.118	255.255.255.0	192.168.0.1
Kali Linux	Тестова система (атакуючий)	192.168.0.92	255.255.255.0	192.168.0.1

Також буде налаштована служба Active Directory, яка розгорнута на сервері Windows Server 2019.

Active Directory (AD) є ключовим елементом сучасної IT-інфраструктури підприємства. Це служба каталогів, розроблена корпорацією Майкрософт для доменних мереж Windows, що слугує важливим інструментом для організації та керування користувачами, їхніми атрибутами та членством у групах, обліковими записами комп'ютерів, мережевими ресурсами та багатьом іншим.

У ході виконання роботи на сервері було створено домен согр.local, до якого підключено робочу станцію Windows 10. Після входження комп'ютера до домену з'являється можливість централізованого керування обліковими записами користувачів, застосування групових політик та контролю доступу до ресурсів мережі.

Використання доменного середовища дозволяє моделювати типові сценарії роботи корпоративної мережі, зокрема:

- автентифікацію користувачів у домені;
- створення та видалення облікових записів;
- зміну паролів користувачів;
- призначення прав доступу;
- вхід користувачів на робочі станції;

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		39

- застосування групових політик безпеки.

Усі зазначені дії супроводжуються генерацією подій безпеки в журналі Windows Security. Для передачі цих подій до SIEM–системи IBM QRadar на сервері Windows Server 2019 встановлено агент NXLog Community Edition. Агент виконує збір записів із журналів Windows та передає їх до QRadar у форматі Syslog через TCP–порт 514.

Крім контролера домену, джерелами подій у лабораторному стенді виступають також міжмережевий екран OPNsense, робоча станція Windows 10 та система Kali Linux. Передача журналів подій здійснюється за допомогою протоколу Syslog на адресу сервера IBM QRadar CE. Загальна схема збору та передачі логів наведена на рисунку 2.2.

Отримані події обробляються платформою IBM QRadar, де виконується їх нормалізація, класифікація та подальший аналіз. Це дозволяє виявляти підозрілу активність у мережі, фіксувати спроби несанкціонованого доступу та формувати інциденти інформаційної безпеки на основі правил кореляції.

2.3 Моделювання загроз та проєктування системи виявлення

Після побудови лабораторного стенду необхідно визначити перелік загроз, які будуть використовуватися для перевірки роботи SIEM–системи IBM QRadar. Для цього було обрано декілька типових сценаріїв атак, які найчастіше зустрічаються в корпоративних мережах та можуть бути виявлені за допомогою аналізу журналів подій.

Для проведення тестування використовується віртуальна машина Kali Linux, з якої виконуються дії, що імітують поведінку потенційного зломисника. У свою чергу Windows Server 2019, Windows 10 та OPNsense виступають джерелами подій, які передаються до IBM QRadar для подальшого аналізу.

У межах роботи було вирішено дослідити такі сценарії(таблиця 2.2):

- мережеве сканування вузлів;
- підбір паролів до облікових записів;

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		40

- спроби несанкціонованого доступу;
- ARP–спуфінг у локальній мережі;
- зміни в облікових записах користувачів Active Directory.

Таблиця 2.2

Основні сценарії загроз лабораторного стенду

Загроза	Інструмент	Джерело подій	Очікуваний результат
Мережеве ска- нування	Nmap	OPNsense, Windows Server	Фіксація підозрілої мере- жевої активності
Підбір паролів	Hydra	Windows Security Log	Реєстрація великої кіль- кості невдалих спроб входу
Несанкціонова- ний доступ	Windows Logon Events	Windows Security Log	Виявлення спроб доступу до системи
ARP–спуфінг	Arpspoof	Kali Linux, OPNsense	Фіксація аномальної мере- жевої активності
Зміни в Active Directory	Active Direc- tory Users and Computers	Windows Server 2019	Реєстрація адміністратив- них змін

Першим сценарієм є мережева розвідка. Як правило, перед проведенням атаки зловмисник намагається отримати інформацію про структуру мережі, активні вузли та доступні сервіси. Для цього використовується утиліта Nmap, яка входить до складу Kali Linux.

За допомогою Nmap було виконано сканування вузлів лабораторного стенду з метою визначення відкритих портів та доступних мережевих служб. Подібна активність може бути зафіксована міжмережевим екраном OPNsense та відображена в журналах подій. Крім того, результати сканування дозволяють оцінити рівень доступності мережевих сервісів і визначити потенційні точки для подальших атак.

Ще одним поширеним видом загроз є підбір паролів до облікових записів користувачів. Незважаючи на використання сучасних механізмів захисту, слабкі або

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		41

типові паролі залишаються однією з найпоширеніших причин компрометації систем.

Для моделювання такого сценарію використовується інструмент Hydra. Під час тестування виконується серія спроб входу з різними комбінаціями логінів і паролів. У журналі безпеки Windows подібні дії відображаються як невдалі спроби автентифікації та супроводжуються відповідними записами Event ID 4625. У випадку успішного входу додатково фіксується подія Event ID 4624.

Окремо було розглянуто можливість виникнення атак типу Man-in-the-Middle. Для цього використовується утиліта arpspoof, яка дозволяє змінювати ARP-записи в локальній мережі та перенаправляти мережевий трафік через машину зловмисника.

Подібні атаки становлять небезпеку через можливість перехоплення переданої інформації між вузлами мережі. Навіть у спрощеному лабораторному середовищі використання такого сценарію дозволяє продемонструвати появу нетипової мережевої активності та перевірити її відображення в системі моніторингу.

Важливим джерелом подій безпеки є служба Active Directory, розгорнута на Windows Server 2019. У корпоративному середовищі саме через Active Directory здійснюється керування користувачами, групами та правами доступу. Тому будь-які зміни в домені можуть становити інтерес з точки зору інформаційної безпеки.

У межах тестування передбачається створення нових користувачів, зміна паролів, а також додавання облікових записів до груп із підвищеними привілеями. Такі дії супроводжуються генерацією подій у журналі безпеки Windows і можуть бути використані для перевірки роботи механізмів моніторингу.

На основі розглянутих сценаріїв було сформовано схему виявлення подій безпеки. Передбачається, що журнали подій від Windows Server 2019 надходитимуть до IBM QRadar через агент NXLog, події від Kali Linux передаватимуться за допомогою syslog-ng, а OPNsense використовуватиме власний механізм віддаленого логування через Syslog.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Після отримання подій IBM QRadar виконує їх обробку, класифікацію та відображення в інтерфейсі системи. Це дозволяє контролювати активність усіх вузлів лабораторного стенду та оперативно отримувати інформацію про потенційно небезпечні дії в мережі.

Таким чином, обрані сценарії дозволяють перевірити роботу системи моніторингу в умовах, максимально наближених до реальної корпоративної мережі. Отримані результати дають можливість оцінити ефективність збору журналів подій, а також дослідити особливості використання IBM QRadar для виявлення подій інформаційної безпеки.

Висновки до розділу 2

У другому розділі було виконано проектування лабораторного стенду SIEM-системи на базі IBM QRadar. Обґрунтовано вибір програмних засобів, розроблено структуру мережевої інфраструктури та визначено основні джерела подій безпеки. Для моделювання корпоративного середовища використано Windows Server 2019, Windows 10, OPNsense, Kali Linux та IBM QRadar Community Edition.

Також було сформовано модель загроз і визначено сценарії тестування, які включають мережеве сканування, підбір паролів, ARP-спуфінг та контроль змін у Active Directory. Отримані результати проектування стали основою для подальшого розгортання, налаштування та тестування SIEM-системи, що розглядається в наступному розділі роботи.

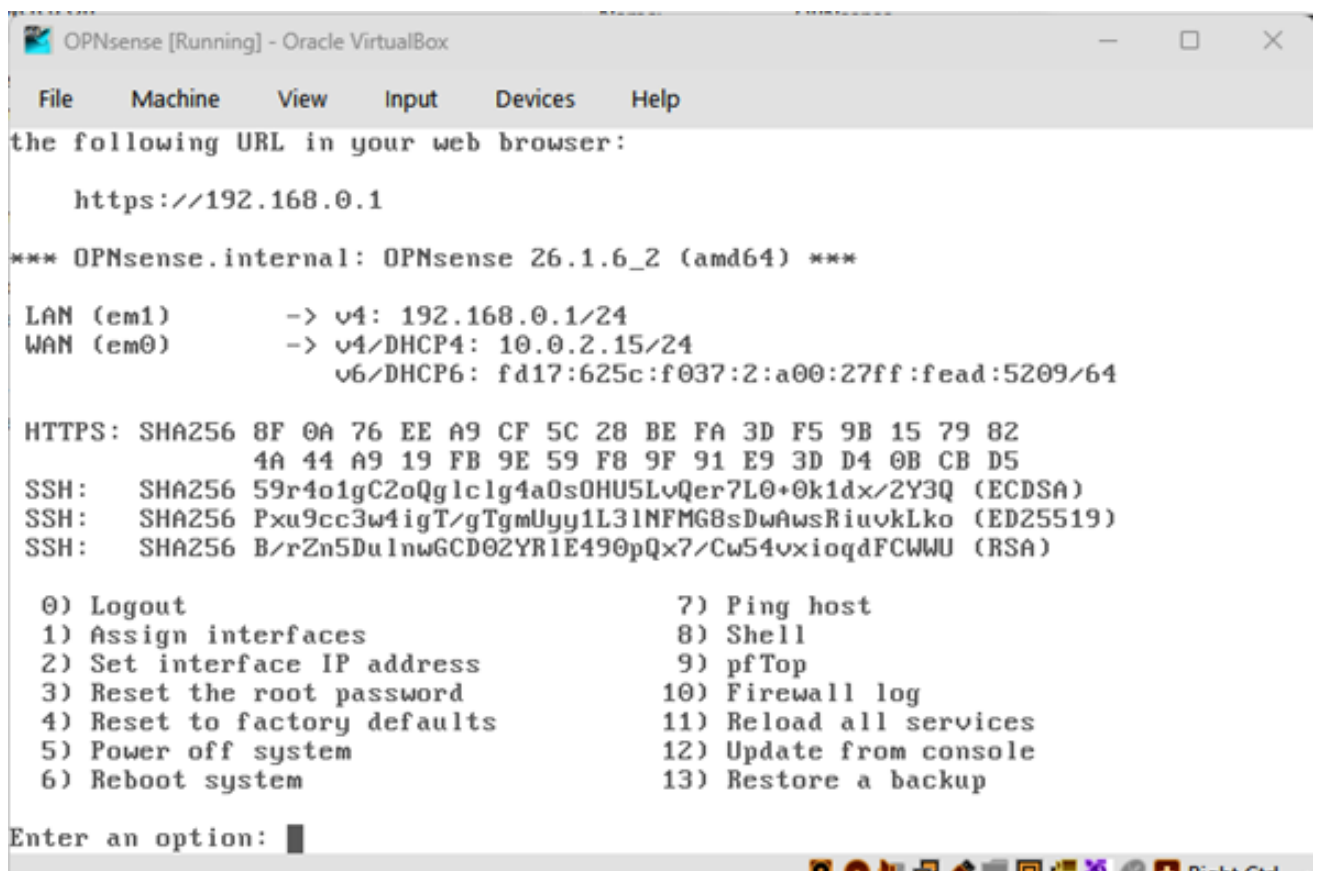
		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

РОЗДІЛ 3 НАЛАШТУВАННЯ, РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ SIEM НА БАЗІ IBM QRADAR

3.1 Розгортання та налаштування тестового стенду

Лабораторний стенд являє собою віртуальне середовище що моделює корпоративну мережу невеликої організації. До його складу входять міжмережевий екран OPNsense, сервер Windows Server 2019 з Active Directory, робоча станція Windows 10, машина атакуючого Kali Linux та SIEM–система IBM QRadar CE всі об'єднані в ізольовану мережу corpnet.

Розгортання стенду розпочалось з налаштування міжмережевого екрану OPNsense версії 26.1.6 оскільки саме він забезпечує мережеву зв'язність між усіма вузлами стенду. Налаштовано два мережеві інтерфейси LAN (em0) з адресою 192.168.0.1/24 для внутрішньої мережі та WAN (em1) підключений через NAT для виходу в інтернет. Всі інші вузли стенду використовують OPNsense як шлюз за замовчуванням(рис3.1).



```
OPNsense [Running] - Oracle VirtualBox
File Machine View Input Devices Help
the following URL in your web browser:
https://192.168.0.1
*** OPNsense.internal: OPNsense 26.1.6_2 (amd64) ***
LAN (em1)      -> v4: 192.168.0.1/24
WAN (em0)      -> v4/DHCP4: 10.0.2.15/24
                v6/DHCP6: fd17:625c:f037:2:a00:27ff:fead:5209/64
HTTPS: SHA256 8F 0A 76 EE A9 CF 5C 28 BE FA 3D F5 9B 15 79 82
          4A 44 A9 19 FB 9E 59 F8 9F 91 E9 3D D4 0B CB D5
SSH:      SHA256 59r4o1gC2oQglclg4a0s0HU5LvQer7L0+0k1dx/2Y3Q (ECDSA)
SSH:      SHA256 Pxu9cc3w4igT/gTgmUyy1L31NFMG8sDwAwsRiuvkLko (ED25519)
SSH:      SHA256 B/rZn5DulnwGCD02YR1E490pQx7/Cw54vxioqdfCWWU (RSA)

0) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system
7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup

Enter an option: █
```

Рисунок 3.1 – Консоль OPNsense з налаштованими інтерфейсами

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Далі за адресою <https://192.168.0.1> переходимо до веб-інтерфейсу OPNsense, для того щоб управляти та налаштовувати обліковий запис root(рис.3.2,3.3).

Рисунок 3.2 – Веб-інтерфейс OPNsense – сторінка автентифікації

Рисунок 3.3 – Головна сторінка після входу (Dashboard OPNsense)

Для передачі мережевих подій до QRadar в OPNsense налаштовано віддалене логування. В розділі Remote додано запис з такими параметрами: транспортний протокол UDP, адреса призначення 192.168.0.158, порт 1514, опис QRadar SIEM. Налаштовано передачу подій всіх рівнів – debug, info, notice, warn, error (рис.3.4).

Рисунок 3.4 – Детальні налаштування віддаленого логування OPNsense до QRadar

Після збереження налаштувань OPNsense розпочав автоматичну передачу мережевих подій до SIEM-системи. Передача журналів охоплює всі системні події міжмережевого екрану спроби підключення, заблокований трафік, зміни конфігурації та системні повідомлення.

Переходимо тепер до налаштувань Windows Server 2019. На даному вузлі виконано налаштування мережевого інтерфейсу та встановлення агента збору логів NXLog. Налаштовано статичну IP-адресу через властивості мережевого адаптера.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Коректність налаштування мережі перевірено командою `ipconfig` отримано підтвердження що адреса 192.168.0.136 призначена адаптеру Ethernet. Після цього перевірено з'єднання з шлюзом командою `ping 192.168.0.1` отримано чотири відповіді без втрат пакетів з мінімальним часом відгуку 1 мс(рис.3.5,3.6).

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : internal
    Link-local IPv6 Address . . . . . : fe80::bc93:7549:197f:3246%8
    IPv4 Address. . . . . : 192.168.0.136
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

C:\Users\Administrator>

```

Рисунок 3.5 – призначена адреса адаптеру Ethernet

```

C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=5ms TTL=64
Reply from 192.168.0.1: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 3ms

C:\Users\Administrator>

```

Рисунок 3.6 – Перевірка мережевого з'єднання Windows Server з шлюзом

Для передачі подій безпеки до QRadar на Windows Server встановлено агент NXLog Community Edition. Конфігураційний файл агента розташований за шляхом `C:\Program Files\nxlog\conf\nxlog.conf`(рис.3.7).

Модуль `im_msvistalog` налаштовано на збір подій з трьох журналів Windows Application, System та Security. Модуль `om_udp` передає зібрані події через UDP на адресу QRadar 192.168.0.158 порт 1514 у форматі Syslog SNARE. Маршрут Route 1 визначає напрямок потоку подій від вхідного модуля до вихідного.

```

File Edit Format View Help
</Extension>

<Input in>
  Module im_msvisialog
  Query <QueryList>\
    <Query Id="0">\
      <Select Path="Application">*</Select>\
      <Select Path="System">*</Select>\
      <Select Path="Security">*</Select>\
    </Query>\
  </QueryList>
</Input>

<Output out>
  Module om_udp
  Host 192.168.0.158
  Port 514
  Exec to_syslog_snare();
</Output>

<Route 1>
  Path in => out
</Route>

```

Рисунок 3.7 – Конфігураційний файл NXLog CE на Windows Server 2019

Після налаштування перевірено статус сервісу NXLog командою Get-Service nxlog у PowerShell отримано статус Running що підтверджує що агент запущений та активно передає події до Qradar(рис.3.8).

```

PS C:\Users\Administrator> Get-Service nxlog

Status Name      DisplayName
-----
Running nxlog      nxlog

```

Рисунок 3.8 – успішно запущений сервіс

Тепер процес налагодження Kali Linux. На даному вузлі виконано два завдання – налаштування статичної IP-адреси та конфігурацію syslog-ng для передачі системних подій до QRadar.

Спочатку Kali Linux отримала IP-адресу автоматично через DHCP від OPNsense, адреса 192.168.0.92 була призначена динамічно. Для забезпечення стабільної роботи стенду адресу зафіксовано як статичну через утиліту nmcli(рис.3.9):

sudo nmcli con mod "Wired connection 1" ipv4.addresses 192.168.0.92/24
 ipv4.gateway 192.168.0.1 ipv4.dns 192.168.0.1 ipv4.method manual

sudo nmcli con up "Wired connection 1"

```
(kali@kali)-[~]
$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:8a:35:d2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.92/24 brd 192.168.0.255 scope global dynamic noprefixroute
        eth0
        valid_lft 86059sec preferred_lft 86059sec
    inet6 fe80::31eb:ead1:88f0:9fc6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=1.30 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=1.08 ms
```

Рисунок 3.9 – Мережева конфігурація та перевірка з'єднання Kali Linux

Перевірено статус сервісу командою `systemctl status syslog-ng` отримано ста-
тус active (running) що підтверджує коректну роботу агента(рис.3.10).

```
$ sudo systemctl status syslog-ng
● syslog-ng.service - System Logger Daemon
   Loaded: loaded (/usr/lib/systemd/system/syslog-ng.service; enabled; pre>
   Active: active (running) since Tue 2026-06-09 05:52:02 EDT; 2min 36s ago
 Invocation: 67ae9e95b6044635bcc20e05760bbddc
    Docs: man:syslog-ng(8)
   Main PID: 2953 (syslog-ng)
     Tasks: 3 (limit: 2118)
    Memory: 52.9M (peak: 54.9M)
       CPU: 271ms
    CGroup: /system.slice/syslog-ng.service
            └─2953 /usr/sbin/syslog-ng -F

Jun 09 05:52:02 kali systemd[1]: Starting syslog-ng.service - System Logger >
Jun 09 05:52:02 kali (syslog-ng)[2953]: syslog-ng.service: Referenced but un>
Jun 09 05:52:02 kali syslog-ng[2953]: [2026-06-09T05:52:02.973319] systemd-j>
Jun 09 05:52:02 kali systemd[1]: Started syslog-ng.service - System Logger D>
lines 1-16/16 (END)
```

Рисунок 3.10 – Статус сервісу syslog-ng на Kali Linux

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Переходимо до налаштування робочої станції Windows 10. На даному вузлі виконано налаштування статичної IP–адреси та перевірено мережеве з'єднання(рис.3.11).

На Windows 10 налаштовано статичну IP–адресу через властивості мережевого адаптера. У вікні протоколу IPv4 встановлено адресу 192.168.0.118, маску підмережі 255.255.255.0 та основний шлюз 192.168.0.1. Як DNS сервер вказано адресу контролера домену 192.168.0.136 що є необхідним для подальшого підключення робочої станції до домену corp.local.

```
C:\Users\Student>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : internal
    Link-local IPv6 Address . . . . . : fe80::a40c:652d:4d58:66b
    IPv4 Address. . . . . : 192.168.0.118
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
```

Рисунок 3.11 – Мережева конфігурація Windows 10

Після цього перевірено з'єднання з шлюзом командою ping і отримано чотири відповіді без втрат пакетів(рис.3.12).

```
C:\Users\Student>ping 192.186.0.1

Pinging 192.186.0.1 with 32 bytes of data:
Reply from 192.186.0.1: bytes=32 time=428ms TTL=126
Reply from 192.186.0.1: bytes=32 time=423ms TTL=126
Reply from 192.186.0.1: bytes=32 time=479ms TTL=126
Reply from 192.186.0.1: bytes=32 time=435ms TTL=126

Ping statistics for 192.186.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 423ms, Maximum = 479ms, Average = 441ms
```

Рисунок 3.12 – Перевірка мережевого з'єднання Windows 10 з шлюзом

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Завершальним етапом розгортання стенду стало налаштування SIEM–системи IBM QRadar Community Edition. Систему розгорнуто як окрему віртуальну машину на базі CentOS зі статичною адресою 192.168.0.158. Після запуску віртуальної машини перевірено мережеву конфігурацію командою `ip addr show` адреса 192.168.0.158 призначена інтерфейсу `enp0s17`(рис.3.13).

```

QRadar [Running] - Oracle VirtualBox
File Machine View Input Devices Help

CentOS Linux 7 (Core)
Kernel 3.10.0-1062.4.1.el7.x86_64 on an x86_64

root login: root
Password:
root login: Wed Jun  3 18:20:18 on tty1
root@localhost ~]# ip addr show
lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
    enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:a5:00:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.158/24 brd 192.168.0.255 scope global noprefixroute dynamic enp0s17
        valid_lft 86386sec preferred_lft 86386sec
    inet6 fe80::518c:803d:85b4:e8cf/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@localhost ~]#

```

Рисунок 3.13 – Мережева конфігурація IBM QRadar

Перевірено з'єднання з шлюзом командою `ping 192.168.0.1` отримано стабільні відповіді що підтверджує коректне налаштування мережі(рис.3.14).

```

root@localhost ~]# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.935 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=3.66 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.940 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=1.41 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=0.699 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=0.952 ms

```

Рисунок 3.14 – Перевірка з'єднання QRadar з шлюзом

Додатково перевірено з'єднання між QRadar та Windows 10 командою `ping 192.168.0.118` – отримано стабільні відповіді що підтверджує мережеву зв'язність між усіма вузлами стенду(рис.3.15).

```

[root@localhost ~]# ping 192.168.0.118
PING 192.168.0.118 (192.168.0.118) 56(84) bytes of data.
64 bytes from 192.168.0.118: icmp_seq=76 ttl=128 time=0.492 ms
64 bytes from 192.168.0.118: icmp_seq=77 ttl=128 time=0.483 ms
64 bytes from 192.168.0.118: icmp_seq=78 ttl=128 time=0.884 ms
64 bytes from 192.168.0.118: icmp_seq=79 ttl=128 time=0.706 ms
64 bytes from 192.168.0.118: icmp_seq=80 ttl=128 time=1.61 ms
64 bytes from 192.168.0.118: icmp_seq=81 ttl=128 time=0.630 ms
64 bytes from 192.168.0.118: icmp_seq=82 ttl=128 time=1.23 ms
64 bytes from 192.168.0.118: icmp_seq=83 ttl=128 time=0.688 ms
64 bytes from 192.168.0.118: icmp_seq=84 ttl=128 time=0.636 ms
64 bytes from 192.168.0.118: icmp_seq=85 ttl=128 time=1.57 ms
64 bytes from 192.168.0.118: icmp_seq=86 ttl=128 time=0.918 ms
64 bytes from 192.168.0.118: icmp_seq=87 ttl=128 time=0.458 ms
64 bytes from 192.168.0.118: icmp_seq=88 ttl=128 time=0.581 ms
64 bytes from 192.168.0.118: icmp_seq=89 ttl=128 time=0.523 ms
64 bytes from 192.168.0.118: icmp_seq=90 ttl=128 time=0.361 ms
64 bytes from 192.168.0.118: icmp_seq=91 ttl=128 time=0.571 ms

```

Рисунок 3.15 – Перевірка з'єднання між QRadar та Windows 10

Веб-інтерфейс системи доступний за адресою <https://192.168.0.158> та надає доступ до всіх функцій платформи. Після цього відкриється вікно входу до консолі, де потрібно ввести відповідні облікові дані для доступу(рис.3.16).

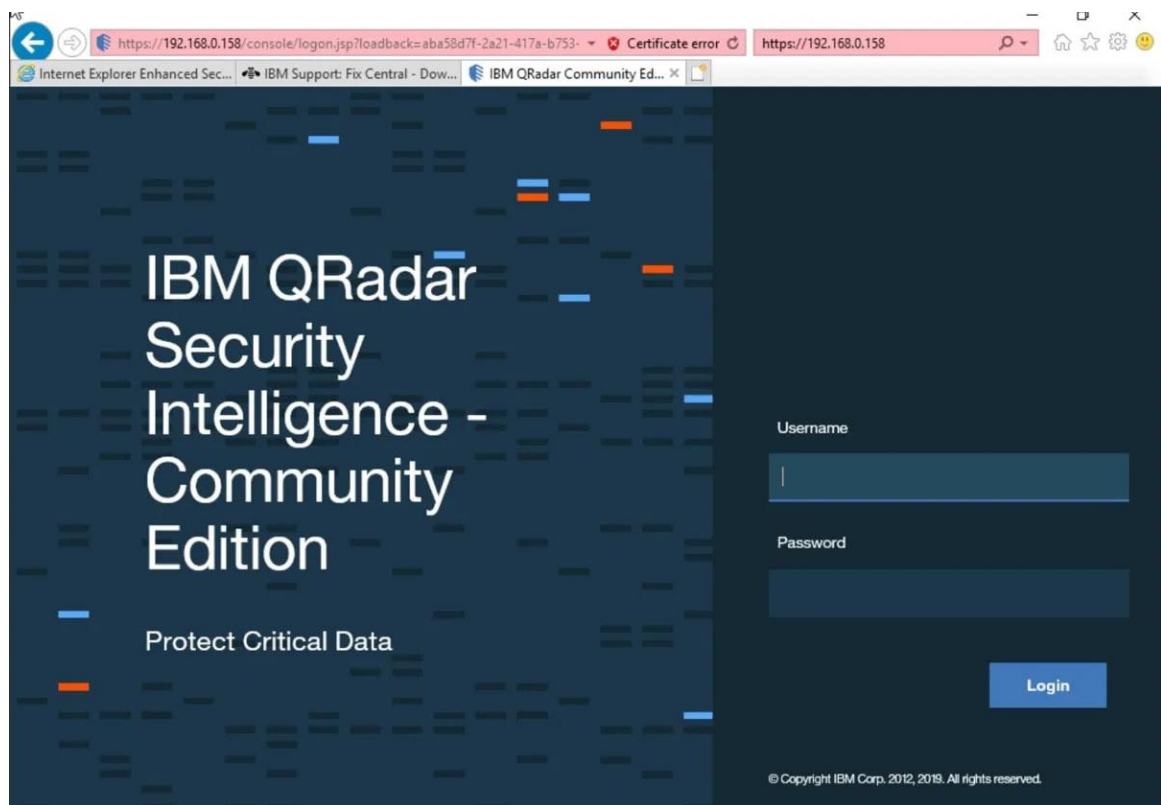


Рисунок 3.16 – Веб-інтерфейс IBM QRadar Community Edition

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				52
Змн.	Арк.	№ докум.	Підпис	Дата		

Після успішної автентифікації відкривається головна сторінка QRadar Console яка містить наступні розділи:

- Dashboard – інформаційні панелі з графіками активності, статистикою подій та сповіщеннями системи
- Offenses – розділ управління інцидентами безпеки де відображаються виявлені загрози згенеровані механізмом кореляції
- Log Activity – перегляд потоку подій у реальному часі з можливістю фільтрації та пошуку
- Network Activity – аналіз мережевого трафіку через компонент QFlow
- Reports – формування звітів про стан безпеки інфраструктури
- Admin – адміністративна панель для налаштування джерел логів, правил кореляції та параметрів системи

Після розгортання QRadar в адміністративній панелі налаштовано чотири джерела подій по одному для кожного вузла стенду(рис.3.17,3.18,3.19).

Розглянемо детально налаштування на прикладі OPNsense.

Edit a log source

Note that the connection information for this log source is shared amongst one or more other log sources

Log Source Name	OPNsense-Firewall
Log Source Description	OPNsense - Firewall
Log Source Type	Universal DSM
Protocol Configuration	Syslog
Log Source Identifier	192.168.0.1
Enabled	☒
Credibility	5
Target Event Collector	eventcollector0 :: localhost
Coalescing Events	☒
Incoming Payload Encoding	UTF-8
Store Event Payload	☒

Рисунок 3.17 – Налаштування Log Source OPNsense в Qradar

Note that the connection information for this log source is shared amongst one or more

Log Source Name: Kali-Linux

Log Source Description: Attacker

Log Source Type: Linux OS

Protocol Configuration: Syslog

Log Source Identifier: 192.168.0.92

Enabled: ☒

Credibility: 5

Target Event Collector: eventcollector0 :: localhost

Coalescing Events: ☒

Incoming Payload Encoding: UTF-8

Store Event Payload: ☒

Please select any groups you would like this log source to be a member of:

Рисунок 3.18 – Налаштування Log Source Kali Linux в Qradar

Аналогічно налаштовано джерела логів для інших вузлів стенду. Для Windows Server 2019 та Windows 10 вказано тип Microsoft Windows та відповідні ідентифікатори 192.168.0.136 та 192.168.0.118.

Name	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier	Target Destination	Credibility	Autodisc	Last Event Time	Creation Date	Modification Date	Average EPS (Last Minute)
Kali-Linux	Kali linu...	N/A	Syslog		Linux OS	True	192.168...	eventcol...	5	False	N/A	Jun 3, 2...	Jun 3, 2...	N/A
OPNSE...	OPNsen...	N/A	Syslog		Univers...	True	192.168...	eventcol...	5	False	N/A	Jun 3, 2...	Jun 3, 2...	N/A
Win-10	Window...	N/A	Syslog		Microsof...	True	192.168...	eventcol...	5	False	N/A	Jun 3, 2...	Jun 3, 2...	N/A
Window...	Window...	N/A	Syslog		Microsof...	True	192.168...	eventcol...	5	False	N/A	Jun 3, 2...	Jun 3, 2...	N/A

Рисунок 3.19 – Повний список налаштованих Log Sources в QRadar

Після налаштування Log Sources перевірено коректність передачі журналів від усіх вузлів до QRadar. На QRadar виконано перехоплення мережевого трафіку командою tcpdump(рис.3.20,3.21):

```
[root@localhost ~]# tcpdump -i any udp port 514 -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
09:47:51.162304 IP 192.168.0.1.19578 > 192.168.0.158.514: SYSLOG local0.info, l
ngth: 226
09:47:51.162379 IP 192.168.0.1.19578 > 192.168.0.158.514: SYSLOG local0.info, l
ngth: 225
09:47:51.162411 IP 192.168.0.1.19578 > 192.168.0.158.514: SYSLOG local0.info, l
ngth: 184
09:47:51.162436 IP 192.168.0.1.19578 > 192.168.0.158.514: SYSLOG local0.info, l
ngth: 183
09:47:51.162667 IP 192.168.0.1.19578 > 192.168.0.158.514: SYSLOG local0.info, l
ngth: 183
09:47:51.162715 IP 192.168.0.1.19578 > 192.168.0.158.514: SYSLOG local0.info, l
ngth: 188
09:47:51.162952 IP 192.168.0.1.19578 > 192.168.0.158.514: SYSLOG local0.info, l
ngth: 178
```

Рисунок 3.20 – Перехоплення Syslog пакетів від OPNsense до QRadar

```
0 packets dropped by kernel
[root@localhost ~]# tcpdump -i any host 192.168.0.92 -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
10:25:03.343442 IP 192.168.0.92.54732 > 192.168.0.158.514: SYSLOG kernel.info, l
ength: 82
10:25:03.343542 IP 192.168.0.158 > 192.168.0.92: ICMP 192.168.0.158 udp port 514
unreachable, length 118
10:25:03.343576 IP 192.168.0.92.54732 > 192.168.0.158.514: SYSLOG kernel.info, l
ength: 63
10:25:03.343584 IP 192.168.0.158 > 192.168.0.92: ICMP 192.168.0.158 udp port 514
unreachable, length 99
10:25:08.349342 ARP, Request who-has 192.168.0.92 tell 192.168.0.158, length 28
10:25:08.349904 ARP, Reply 192.168.0.92 is-at 08:00:27:8a:35:d2, length 46
10:25:08.634332 ARP, Request who-has 192.168.0.158 tell 192.168.0.92, length 46
10:25:08.634349 ARP, Reply 192.168.0.158 is-at 08:00:27:a5:00:87, length 28
10:25:49.616754 IP 192.168.0.92.36115 > 192.168.0.158.514: SYSLOG syslog.notice,
length: 82
10:25:49.616829 IP 192.168.0.158 > 192.168.0.92: ICMP 192.168.0.158 udp port 514
unreachable, length 118
10:25:54.621402 ARP, Request who-has 192.168.0.92 tell 192.168.0.158, length 28
10:25:54.621664 ARP, Reply 192.168.0.92 is-at 08:00:27:8a:35:d2, length 46
10:25:54.845199 ARP, Request who-has 192.168.0.158 tell 192.168.0.92, length 46
10:25:54.845250 ARP, Reply 192.168.0.158 is-at 08:00:27:a5:00:87, length 28
```

Рисунок 3.21 – Перехоплення Syslog пакетів від Kali Linux до QRadar

Після налаштування всіх вузлів та джерел логів перевірено загальний стан системи через Dashboard System Monitoring(рис.3.22).

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		55

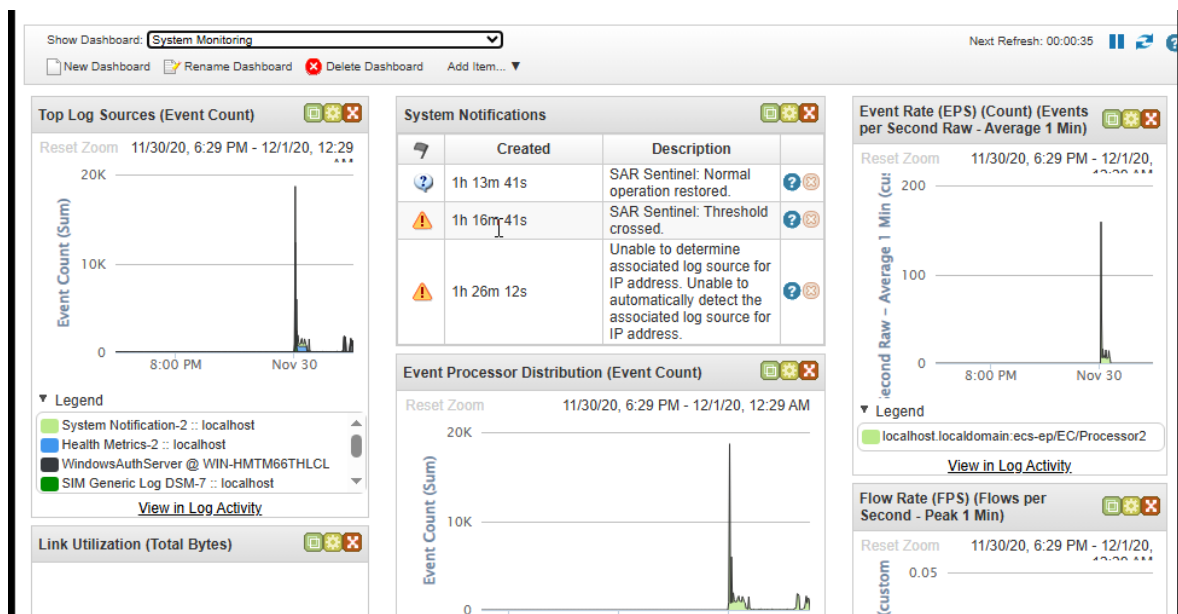


Рисунок 3.22 – Dashboard System Monitoring IBM Qradar

3.2 Налаштування Active Directory та IBM Qradar

Після розгортання мережевої інфраструктури наступним кроком стало налаштування служби Active Directory на Windows Server 2019. Active Directory є основою корпоративної мережі що забезпечує централізоване керування користувачами, комп'ютерами та ресурсами організації. Розгортання Active Directory дозволило створити повноцінне доменне середовище яке максимально наближене до реальної корпоративної інфраструктури.

Першим етапом стала інсталяція служби каталогів Active Directory Domain Services на Windows Server 2019.. Після успішного встановлення сервер підвищено до рівня контролера домену що надало йому можливість виконувати функції автентифікації та авторизації для всіх вузлів мережі(рис.3.23).

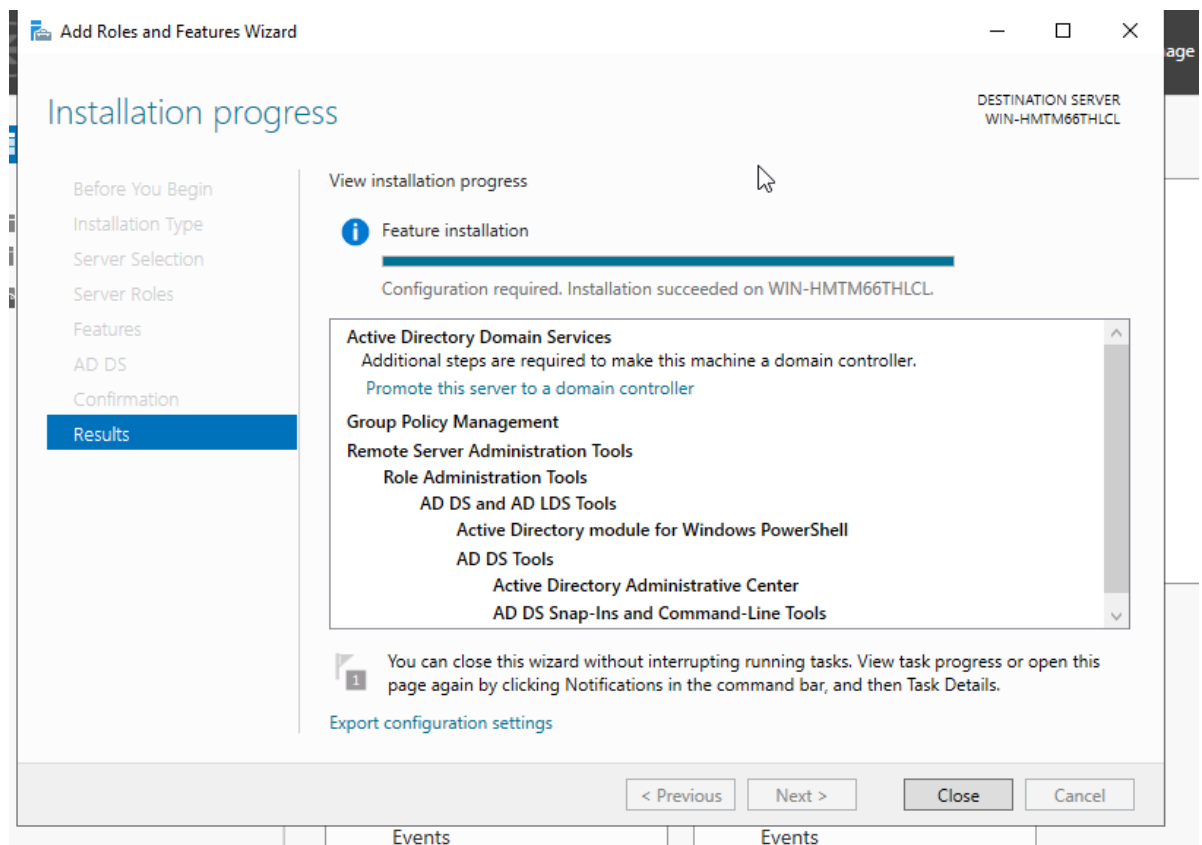


Рисунок 3.23 – Встановлення ролі AD DS на Windows Server 2019

Наступним кроком стало створення домену який є основою мережевої інфраструктури стенду. Домен corp.local слугуватиме єдиною точкою автентифікації та авторизації для всіх користувачів та пристроїв в мережі стенду(рис.3.24).

На етапі Domain Controller Options встановлено функціональний рівень Windows Server 2016 для лісу та домену. Активовано службу DNS server що забезпечить правильне функціонування мережі та дозволить пристроям знаходити необхідні ресурси та служби. Активовано Global Catalog для зберігання інформації про всі об'єкти домену.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		57

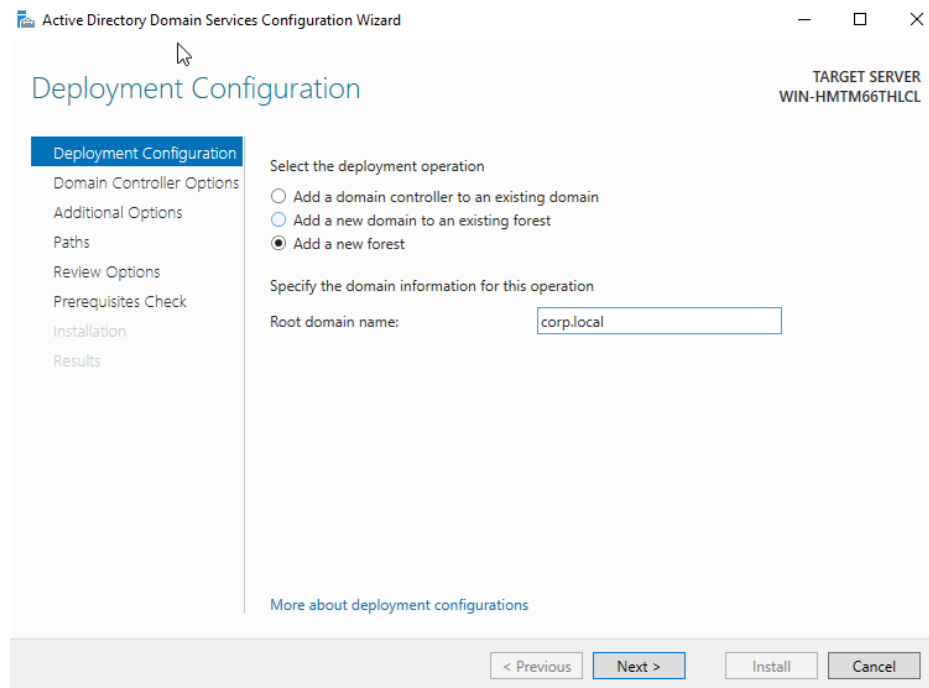


Рисунок 3.24 – Налаштування нового домену corp.local

Після завершення налаштування сервер автоматично перезавантажився. Екран входу відображає обліковий запис CORP\Administrator що підтверджує успішне розгортання домену. В консолі Active Directory Users and Computers відображається створений домен corp.local з усіма стандартними контейнерами(рис.3.25).

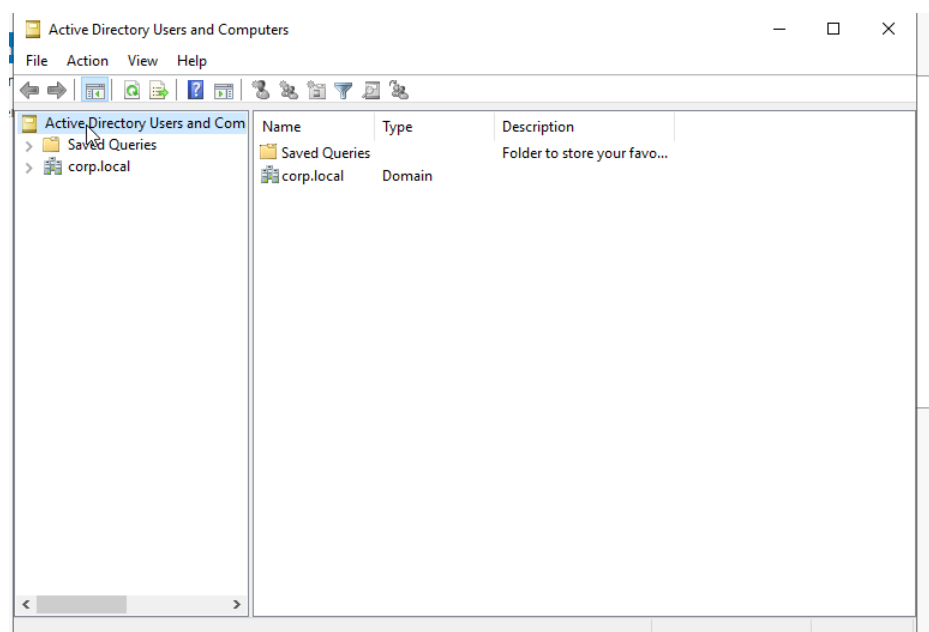


Рисунок 3.25 – Консоль Active Directory Users and Computers з доменом corp.local

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Після створення домену виконано налаштування організаційної структури та створення облікових записів користувачів. Наявність користувачів домену є необхідною умовою для моделювання реальних корпоративних сценаріїв доменного входу, доступу до мережевих ресурсів та генерації подій автентифікації які будуть фіксуватись SIEM–системою.

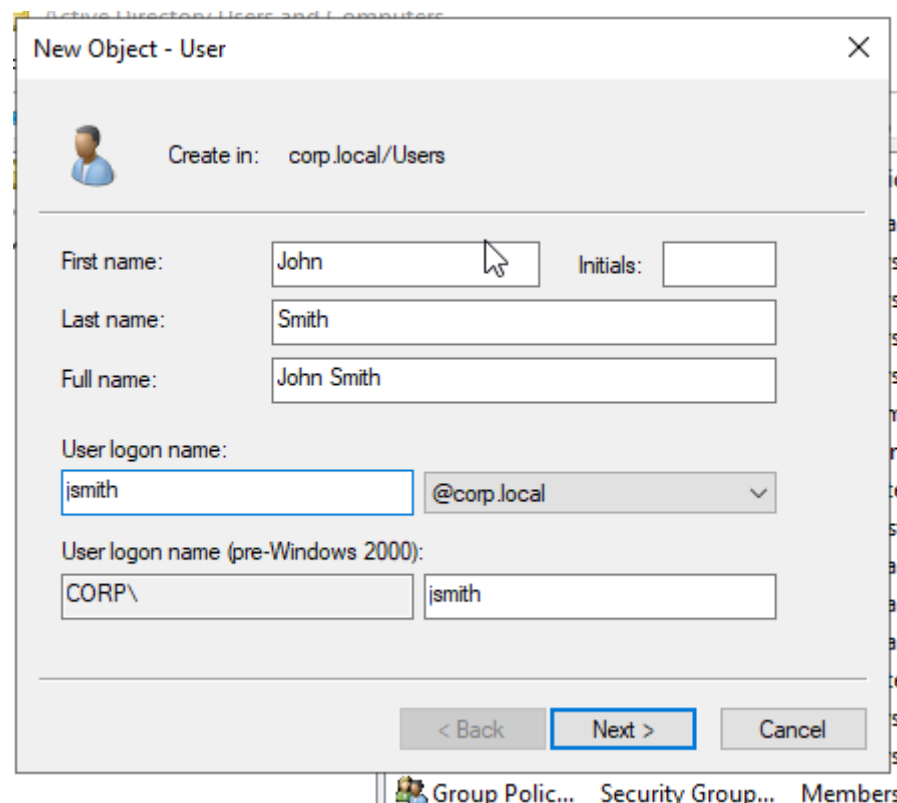


Рисунок 3.26 – Створення облікового запису John Smith в домені corp.local

Після створення користувачів список контейнеру Users містить обидва облікові записи поряд зі стандартними системними обліковими записами та групами домену(рис.3.26).

Підключення Windows 10 до домену

Завершальним етапом налаштування Active Directory стало підключення робочої станції Windows 10 до домену corp.local. Це дозволило включити робочу станцію до єдиного доменного середовища та забезпечити централізоване керування доступом до мережевих ресурсів(рис.3.27).

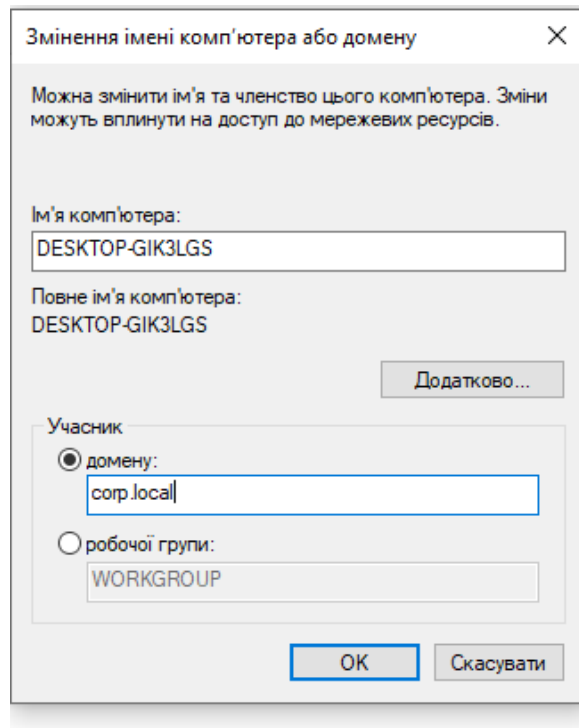


Рисунок 3.27 – Підключення Windows 10 до домену corp.local

Після перезавантаження у вікні властивостей системи відображається повне ім'я комп'ютера DESKTOP-GIK3LGS.corp.local та підтвердження членства в домені corp.local. В консолі Active Directory Users and Computers в розділі Computers відображається комп'ютер DESKTOP-GIK3LGS що підтверджує успішне підключення робочої станції до домену(рис.3.28).

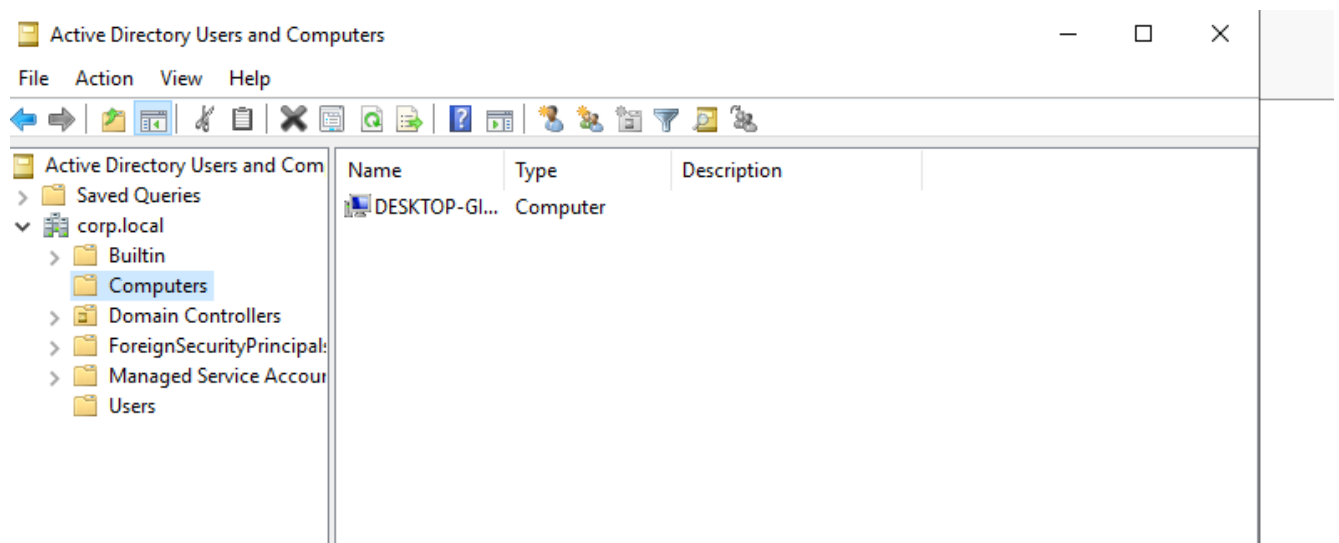


Рисунок 3.28 – Комп'ютер DESKTOP-GIK3LGS в розділі Computers домену corp.local

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		60

Таким чином налаштування Active Directory повністю завершено. Розгорнуто домен corp.local, налаштовано DNS сервер, створено облікові записи користувачів та підключено робочу станцію Windows 10 до домену. Це забезпечує повноцінне корпоративне середовище для подальшого тестування SIEM–системи IBM QRadar.

3.3 Тестування системи та аналіз результатів

В рамках тестування SIEM–системи планувалось проведення симуляції кібератак з Kali Linux на вузли корпоративної мережі стенду. Метою тестування було перевірити здатність IBM QRadar виявляти підозрілу активність та автоматично генерувати інциденти безпеки. Kali Linux є спеціалізованим дистрибутивом Linux що містить широкий арсенал інструментів для тестування на проникнення і саме тому був обраний як платформа для імітації атак. Планувалось провести наступні типи атак:

- мережева розвідка за допомогою nmap – визначення активних хостів та відкритих портів
- атака підбору паролів через Hydra – спроба отримати доступ до сервісів шляхом перебору паролів
- ARP–спуфінг за допомогою arpspoof – перехоплення мережевого трафіку між вузлами

Мережева розвідка є першим етапом будь-якої кібератаки. Зловмисник намагається отримати максимум інформації про мережу перед проведенням безпосередньої атаки. З Kali Linux виконано мережеве сканування Windows Server 2019 за допомогою утиліти nmap з визначенням версій сервісів(рис.3.29):

```
nmap -sV 192.168.0.136
```

В результаті сканування отримано детальну інформацію про цільовий хост. Визначено що хост 192.168.0.136 активний та доступний в мережі..Визначено операційну систему цільового хоста – Windows.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		61

```
(kali@kali)-[~]
$ nmap -sV 192.168.0.136
Starting Nmap 7.98 ( https://nmap.org ) at 2026-06-09 14:14 -0400
Nmap scan report for 192.168.0.136
Host is up (0.00061s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
5357/tcp  open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5985/tcp  open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:38:E4:E6 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.22 seconds

(kali@kali)-[~]
$
```

Рисунок 3.29 – Результат nmap сканування Windows Server 2019

В реальному корпоративному середовищі така активність мала б відображатись в QRadar як велика кількість мережеских з'єднань з одного джерела за короткий проміжок часу що є характерною ознакою мережевого сканування.

Атака підбору паролів або brute force є одним з найпоширеніших методів отримання несанкціонованого доступу до інформаційних систем. Для проведення атаки використано інструмент Hydra який підтримує паралельний перебір паролів для різних мережеских протоколів. Перед запуском атаки розпаковано словник паролів rockyou.txt який містить понад 14 мільйонів найпоширеніших паролів:

```
sudo gunzip /usr/share/wordlists/rockyou.txt.gz
hydra -l Administrator -P /usr/share/wordlists/rockyou.txt -t 4
rdp://192.168.0.136
```

Також виконано спробу brute force атаки через Hydra на RDP сервіс Windows Server. Однак служба RDP на Windows Server не була активована в рамках стенду тому атака не дала результату.

Паралельно з проведенням атак перевірено стан журналу безпеки на Windows Server через Event Viewer. В розділі Windows Security зафіксовано 1819 подій безпеки. Серед зафіксованих подій виявлено події з ідентифікатором 4624 що відповідає успішній автентифікації в системі та події 4672 що відповідає призначенню

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		62

спеціальних привілеїв. Наявність цих подій підтверджує що аудит безпеки на Windows Server налаштований коректно та всі події автентифікації фіксуються в журналі(рис.3.30).

Event Name	Log Source	Even Coun	Time	Low Level Category
Information	WindowsAuthServer @ WIN-...	239	Dec 1, 2020, 1:26:3...	System Status
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored
Microsoft Windows Security Event Log Message	WindowsAuthServer @ WIN-...	1	Dec 1, 2020, 1:26:4...	Stored

Рисунок 3.30 – Події безпеки в Event Viewer Windows Server

Детальний перегляд події 4624 показує повну інформацію про автентифікацію – ім'я облікового запису, домен, тип входу та часову мітку. Саме такі події передаються через NXLog до QRadar та є основою для правил кореляції пов'язаних з моніторингом автентифікації(рис.3.31).

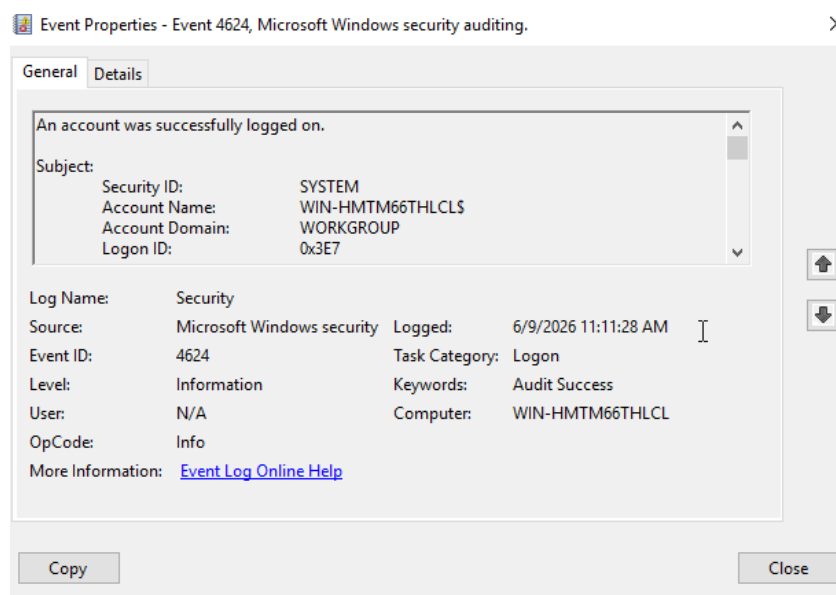


Рисунок 3.31 – Деталі події Event ID 4624 – успішна автентифікація

В процесі тестування виявлено критичну проблему яка унеможливила повноцінну симуляцію атак та їх виявлення SIEM-системою. Ключовий сервіс IBM QRadar – Event Collection Service (ecs-ec) який відповідає за збір, обробку та кореляцію подій припиняв роботу приблизно через 60 секунд після запуску з кодом завершення SIGTERM (status=143). Перевірка статусу сервісу командою systemctl status ecs-ec показала що сервіс має статус Active: failed(рис.3.32).

```
[root@localhost ~]# systemctl status ecs-ec
ecs-ec.service - Event Correlation Services Event Collector
Loaded: loaded (/usr/lib/systemd/system/ecs-ec.service; static; vendor preset: disabled)
Active: failed (Result: exit-code) since Tue 2020-12-01 00:35:10 UTC; 1min 1s ago
Process: 12562 ExecStart=/usr/bin/env ${JAVA_HOME}/bin/java $JOPTS_MS $GC_OPTS $RMI_GC_OPTS $CLASSLOADER_UNLOADING $MEM_OPTS $DUMPOPTS $REMOTE_DEBUG_OPTS -Dcom.q1labs.frameworks.jmx.port=${JMXPORT} -cp ${SERVICEPATH}/bin/* ${SERVICEMAINCLASS} ${SERVICEPATH}/ ${SERVICEPATH}/eventgnosis ecs-ec.ecs 220 noconsole (code=exited, status=143)
Process: 12335 ExecStartPre=/opt/qradar/systemd/bin/generate_environment.sh ${SERVICENAME} (code=exited, status=0/SUCCESS)
Main PID: 12562 (code=exited, status=143)

Dec 01 00:34:19 localhost.localdomain systemd[1]: Starting Event Correlation ...
Dec 01 00:34:19 localhost.localdomain systemd[1]: Started Event Correlation S...
Dec 01 00:34:19 localhost.localdomain ecs-ec[12562]: stdSplitFreeListSplitAmo...
Dec 01 00:35:10 localhost.localdomain systemd[1]: Stopping Event Correlation ...
Dec 01 00:35:10 localhost.localdomain systemd[1]: ecs-ec.service: main proces...
Dec 01 00:35:10 localhost.localdomain systemd[1]: Stopped Event Correlation S...
Dec 01 00:35:10 localhost.localdomain systemd[1]: Unit ecs-ec.service entered...
Dec 01 00:35:10 localhost.localdomain systemd[1]: ecs-ec.service failed.
Hint: Some lines were ellipsized, use -l to show in full.
```

Рисунок 3.32 – Статус сервісу ecs-ec

Причиною є вбудований механізм перевірки ліцензії IBM QRadar Community Edition. Термін дії ліцензії CE версії закінчився 31 грудня 2020 року. Після закінчення терміну дії внутрішній license checker автоматично надсилає сигнал SIGTERM процесу ecs-ec що призводить до його примусового завершення. Без працюючого ecs-ec QRadar не може обробляти вхідні події та застосовувати правила кореляції.

Методи вирішення

Для усунення проблеми було послідовно випробувано кілька методів вирішення.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Першим методом стала зміна системного часу QRadar в межах ліцензійного періоду. Виконано команду для встановлення системного часу на дату коли ліцензія була актуальною(рис.3.33):

```
[root@localhost ~]# ddate -s "2020-12-01 00:00:00"
Tue Dec  1 00:00:00 UTC 2020
[root@localhost ~]# hwclock --systohc
```

Рисунок 3.33 – Зміна системного часу QRadar в межах ліцензійного період

Метод не дав результату оскільки механізм перевірки ліцензії використовує власний незалежний таймер і не покладається на системний час операційної системи.

Другим методом стало вимкнення сервісу conman – Connection Manager який додатково блокував роботу ecs–ec. Сервіс зупинено та вимкнено(рис.3.34):

```
[root@localhost ~]# systemctl stop conman
[root@localhost ~]# systemctl disable conman
[root@localhost ~]# systemctl mask conman
Failed to execute operation: Invalid argument
[root@localhost ~]# pkill -f conman
[root@localhost ~]# ps aux | grep conman | grep -v grep
You have mail in /var/spool/mail/root
[root@localhost ~]# date -s "2020-12-01 00:00:00"
Tue Dec  1 00:00:00 UTC 2020
[root@localhost ~]# systemctl start ecs-ec
Job for ecs-ec.service failed because the control process exited with error code
. See "systemctl status ecs-ec.service" and "journalctl -xe" for details.
[root@localhost ~]# sleep 120
```

Рисунок 3.34 – Спроба вирішення проблеми зупинка conman та запуск ecs–ec

Це частково покращило ситуацію оскільки усунуло додатковий блокуючий фактор однак ecs–ec продовжував падати через внутрішню ліцензійну перевірку.

Третім методом стала модифікація файлу license.txt – змінено дату закінчення ліцензії з 12/31/20 на 12/31/30 у файлі розташованому за шляхом /opt/ibm/si/services/ecs–ec/2019.14.0.20191031163225/eventgnosis/license.txt. Метод не дав результату оскільки перевірка ліцензії реалізована через хеш–суму файлу і

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		65

зміна текстового вмісту без оновлення хешу не впливає на результат перевірки(рис.3.35).

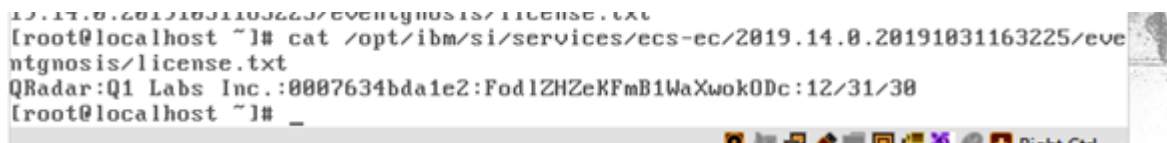


Рисунок 3.35 – Модифікація файлу license.txt

Повністю усунути проблему не вдалось. Перевірка ліцензії реалізована на рівні скомпільованого Java коду з використанням криптографічної хеш–суми що унеможлиблює її модифікацію без декомпіляції jar файлів платформи.

Як мало працювати

В штатному режимі роботи повний цикл виявлення атак мав виглядати наступним чином. Після запуску nmap сканування мережеві події від OPNsense мали надходити до QRadar через Syslog. Після запуску Hydra brute force атаки події невдалої автентифікації Event ID 4625 з Windows Server мали передаватись через NXLog до QRadar.

Сервіс ecs–ес мав приймати ці події та передавати їх до Event Processor для нормалізації через DSM модулі. Після нормалізації події мали потрапляти до Correlation Engine де застосовуються правила кореляції. При виявленні характерних патернів атак – великої кількості мережевих з'єднань від одного IP або серії невдалих спроб автентифікації – система мала автоматично генерувати інциденти безпеки Offenses. Ці Offenses мали відображатись на Dashboard та в розділі Offenses веб–інтерфейсу QRadar для подальшого аналізу адміністратором безпеки.

Аналіз результатів

Незважаючи на проблему з ecs–ес стенд демонструє коректну роботу на рівні збору та передачі логів. За результатами тестування можна зробити наступні висновки:

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		66

- Мережева інфраструктура стенду налаштована коректно , всі вузли мають мережеву зв'язність
- Агенти збору логів працюють – NXLog на Windows Server та syslog-ng на Kali Linux передають події до QRadar
- Log Sources налаштовані в QRadar – чотири джерела подій активні
- Log Activity відображає надходження подій від Windows Server
- Dashboard System Monitoring показує активність стенду з піком до 20 000 подій та Event Rate до 200 EPS
- Active Directory розгорнуто – домен corp.local функціонує, користувачі створені, Windows 10 підключено до домену
- Повноцінна кореляція подій та генерація Offenses неможлива через закінчення ліцензії CE версії

Отримані результати підтверджують що розгорнутий стенд функціонує як повноцінна платформа для збору логів. Проблема з ліцензією є обмеженням безкоштовної версії IBM QRadar Community Edition а не помилкою в налаштуванні стенду. Досвід діагностики та спроби вирішення проблеми з ліцензією є цінним практичним досвідом роботи з реальною SIEM системою в умовах нестандартних технічних обмежень. Негативний результат в частині кореляції подій є закономірним наслідком використання версії з простроченою ліцензією що також є важливим висновком даної роботи.

Висновки до розділу 3

У третьому розділі описано практичну реалізацію лабораторного стенду на базі IBM QRadar Community Edition. Розгорнуто п'ять віртуальних машин в ізольованій мережі corpnet – OPNsense, Windows Server 2019, Windows 10, Kali Linux та IBM QRadar CE. На кожному вузлі налаштовано статичну IP-адресу та перевірено мережеву зв'язність.

Налаштовано передачу журналів подій від усіх джерел до QRadar – OPNsense через вбудований Syslog, Windows Server через агент NXLog CE, Kali Linux через

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

syslog-ng. В інтерфейсі QRadar налаштовано чотири Log Sources та підтверджено надходження подій через розділ Log Activity.

Розгорнуто службу Active Directory та створено домен corp.local, облікові записи користувачів John Smith та Anna Kovalenko, робочу станцію Windows 10 підключено до домену.

В процесі тестування виявлено критичну проблему, сервіс ecs-es припиняв роботу через закінчення терміну дії ліцензії Community Edition що унеможливило повноцінну кореляцію подій та генерацію Offenses. Випробувано три методи вирішення однак повністю усунути проблему не вдалось оскільки перевірка ліцензії реалізована через хеш-суму.

Незважаючи на зазначену проблему стенд демонструє коректну роботу на рівні збору та передачі логів що підтверджує правильність налаштування всіх компонентів інфраструктури.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		68

ВИСНОВКИ

В даній кваліфікаційній роботі було спроектовано та розгорнуто підсистему SIEM для моніторингу інформаційної безпеки корпоративної мережі на базі рішення IBM QRadar .

Обґрунтування актуальності теми дало змогу оцінити важливість SIEM–систем як невід'ємної складової сучасного SOC та підтвердити доцільність їх використання для централізованого моніторингу інформаційної безпеки організації.

Після проведення аналізу сучасних SIEM–рішень – IBM QRadar, Splunk Enterprise Security, Microsoft Sentinel, ArcSight ESM та Wazuh – було обрано платформу IBM QRadar Community Edition для подальшого проектування та реалізації лабораторного стенду. Для більш наочного розуміння вибору платформи проведено порівняльний аналіз зазначених рішень за ключовими критеріями – типом ліцензії, механізмами кореляції, підтримкою джерел логів та складністю впровадження.

Для вирішення задачі проектування мережевої інфраструктури було обрано платформу віртуалізації Oracle VirtualBox та розгорнуто п'ять віртуальних машин в ізольованій мережі corpnet. До складу стенду увійшли міжмережевий екран OPNsense, сервер Windows Server 2019 з Active Directory, робоча станція Windows 10, машина атакуючого Kali Linux та SIEM–система IBM QRadar CE. Використання саме такого набору компонентів дозволило створити середовище максимально наближене до реальної корпоративної інфраструктури.

Після розгортання інфраструктури було налаштовано передачу журналів подій від усіх джерел до QRadar через протокол Syslog. На Windows Server 2019 встановлено агент NXLog CE, на Kali Linux налаштовано syslog-ng, на OPNsense активовано вбудоване віддалене логування. В інтерфейсі QRadar налаштовано чотири Log Sources та підтверджено надходження подій через розділ Log Activity. Розгорнуто домен Active Directory corp.local, створено облікові записи користувачів та підключено робочу станцію Windows 10 до домену.

В процесі тестування системи виявлено критичну технічну проблему – ключовий сервіс ecs–ес припиняв роботу через закінчення терміну дії ліцензії

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		69

Community Edition що унеможливило повноцінну кореляцію подій та генерацію інцидентів безпеки Offenses. Було послідовно випробувано кілька методів вирішення зміна системного часу, вимкнення сервісу conman та модифікація файлу license.txt. Повністю усунути проблему не вдалось оскільки перевірка ліцензії реалізована через криптографічну хеш-суму на рівні скомпільованого коду.

Незважаючи на зазначену проблему стенд демонструє коректну роботу на рівні збору та передачі логів. Dashboard System Monitoring відображає активність з піком до 20 000 подій та Event Rate до 200 EPS що підтверджує правильність налаштування всіх компонентів інфраструктури. Отриманий негативний результат в частині кореляції подій є закономірним наслідком використання версії з простроченою ліцензією та є не менш цінним практичним досвідом ніж позитивний результат.

Основною перевагою спроектованої SIEM-підсистеми є можливість централізованого збору та аналізу журналів подій від різномірних джерел в єдиному інтерфейсі. Використання підсистеми моніторингу подій безпеки на базі IBM QRadar надає змогу своєчасно виявляти та розслідувати підозрілі події в мережі та відповідно реагувати на них. Для повноцінної реалізації системи виявлення загроз рекомендується використовувати комерційну версію IBM QRadar з актуальною ліцензією або розглянути альтернативні рішення з відкритим вихідним кодом які не мають обмежень пов'язаних з терміном дії ліцензії.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				70
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Bejtlich R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. San Francisco : No Starch Press, 2013. 376 p.
2. Chuvakin A., Schmidt K., Phillips C. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Waltham : Syngress, 2013. 456 p.
3. Kim D., Solomon M. Fundamentals of Information Systems Security. 4th ed. Burlington : Jones & Bartlett Learning, 2021. 840 p.
4. Vacca J. Computer and Information Security Handbook. 4th ed. Amsterdam : Elsevier, 2023. 1168 p.
5. Easttom C. Computer Security Fundamentals. 5th ed. Hoboken : Pearson, 2022. 432 p.
6. Stallings W. Network Security Essentials: Applications and Standards. 7th ed. Pearson, 2021. 768 p.
7. NIST SP 800–61 Rev.2. Computer Security Incident Handling Guide. National Institute of Standards and Technology, 2012.
8. NIST SP 800–94. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology, 2007.
9. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, 2024.
10. IBM Security QRadar SIEM Documentation. IBM Documentation. URL: <https://www.ibm.com/docs/en/qradar-siem>
11. IBM QRadar Community Edition Guide. IBM Documentation. URL: <https://www.ibm.com/docs>
12. IBM QRadar Administration Guide. IBM Documentation. URL: <https://www.ibm.com/docs>
13. IBM QRadar DSM Configuration Guide. IBM Documentation. URL: <https://www.ibm.com/docs>
14. Microsoft Learn. Active Directory Domain Services Overview. URL: <https://learn.microsoft.com>

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				71
Змн.	Арк.	№ докум.	Підпис	Дата		

15. Microsoft Learn. Windows Security Auditing. URL: <https://learn.microsoft.com>
16. Microsoft Learn. Event ID Reference and Security Monitoring. URL: <https://learn.microsoft.com>
17. OPNsense Documentation. Official Documentation. URL: <https://docs.opnsense.org>
18. NXLog Community Edition Documentation. URL: <https://docs.nxlog.co>
19. syslog-ng Open Source Edition Administration Guide. URL: <https://www.syslog-ng.com>
20. Kali Linux Documentation. URL: <https://www.kali.org/docs>
21. Nmap Network Scanning. Official Nmap Project Guide. URL: <https://nmap.org/book>
22. Hydra Documentation. THC-Hydra Project. URL: <https://github.com/vanhauser-thc/thc-hydra>
23. MITRE ATT&CK Framework. URL: <https://attack.mitre.org>
24. SANS Institute. Security Operations Center Survey Report. URL: <https://www.sans.org>
25. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems. NIST Special Publication 800-94. Gaithersburg : NIST, 2007.
26. Lavecchia V. Caratteristiche e differenza tra SEM, SIM e SIEM in azienda. Informatica e Ingegneria Online. URL: <https://vitolavecchia.altervista.org/caratteristiche-e-differenza-tra-sem-sim-e-siem-in-azienda/>
27. Conti M., Dargahi T. Cyber Threat Intelligence. Springer, 2022. 352 p.
28. ISO/IEC 27001:2022 Information Security Management Systems – Requirements.
29. Закон України «Про основні засади забезпечення кібербезпеки України». URL: <https://zakon.rada.gov.ua>
30. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою. Вимоги.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				72
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Конфігураційний файл NXLog для передачі журналів подій Windows Server 2019 до IBM Qradar

Лістинг А.1 – Конфігураційний файл NXLog

Panic Soft

```
#NoFreeOnExit TRUE
```

```
define ROOT C:\Program Files (x86)\nxlog
```

```
define CERTDIR %ROOT%\cert
```

```
define CONFDIR %ROOT%\conf\nxlog.d
```

```
define LOGDIR %ROOT%\data
```

```
define LOGFILE %LOGDIR%\nxlog.log
```

```
LogFile %LOGFILE%
```

```
Moduledir %ROOT%\modules
```

```
CacheDir %ROOT%\data
```

```
Pidfile %ROOT%\data\nxlog.pid
```

```
SpoolDir %ROOT%\data
```

```
<Extension _syslog>
```

```
Module xm_syslog
```

```
</Extension>
```

```
<Input in>
```

```
Module im_msvistalog
```

```
Query <QueryList><Query Id="0"><Select Path="Application">*</Select><Select  
Path="System">*</Select><Select Path="Security">*</Select></Query></QueryList>
```

```
</Input>
```

```
<Output out>
```

```
Module om_udp
```

```
Host 192.168.0.158
```

```
Port 514
```

```
Exec to_syslog_snare();
```

```
</Output>
```

```
<Route 1>
```

```
Path in => out
```

```
</Route>
```

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

Мінімальні системні вимоги IBM QRadar Community Edition 7.3.3

Оперативна пам'ять: не менше 8 ГБ.

Місце на диску: не менше 250 ГБ.

Процесор: 4 віртуальні ядра (мінімально), рекомендовано 6 і більше ядер.

Мережа: один мережевий адаптер з доступом до внутрішньої мережі.

Додаткові вимоги: підтримка 64-бітної архітектури та апаратної віртуалізації Intel VT-x або AMD-V.

Мінімальні системні вимоги Windows Server 2019

Оперативна пам'ять: не менше 2 ГБ.

Місце на диску: не менше 32 ГБ.

Процесор: 64-бітний процесор із частотою не менше 1,4 ГГц.

Додаткові вимоги: підтримка ролі Active Directory Domain Services та мережеве підключення до внутрішнього сегмента мережі.

Мінімальні системні вимоги Windows 10

Оперативна пам'ять: не менше 2 ГБ.

Місце на диску: не менше 32 ГБ.

Процесор: 64-бітний процесор із тактовою частотою від 1 ГГц.

Додаткові вимоги: можливість підключення до домену Active Directory.

Мінімальні системні вимоги Kali Linux

Оперативна пам'ять: не менше 2 ГБ.

Місце на диску: не менше 20 ГБ.

Процесор: 2 віртуальні ядра.

Додаткові вимоги: мережевий доступ до всіх вузлів лабораторного стенду для проведення тестування безпеки.

Мінімальні системні вимоги OPNsense 26.1.6

Оперативна пам'ять: не менше 2 ГБ.

Місце на диску: не менше 10 ГБ.

Процесор: 1–2 віртуальні ядра.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

Додаткові вимоги: наявність двох мережевих інтерфейсів для реалізації сегментів WAN та LAN.

Мінімальні системні вимоги хостового комп'ютера

Процесор: Intel Core i5 або аналогічний AMD Ryzen з підтримкою технологій віртуалізації.

Оперативна пам'ять: не менше 16 ГБ, рекомендовано 32 ГБ.

Вільне місце на SSD: не менше 400 ГБ.

Операційна система: Windows 10 або Windows 11.

		Мацюк С.В.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Шелуха О.О				
Змн.	Арк.	№ докум.	Підпис	Дата		76