

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

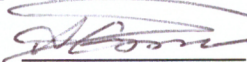
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект SIEM-підсистеми для SOC на базі
рішень IBM QRadar»

Виконав студент 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»

 Дмитро КОЦЮБА

Керівник: зав. кафедри КІ та КБ, к.т.н., доцент

 Андрій ЄФІМЕНКО

Рецензент: доцент кафедри КІ та КБ, к.т.н., доцент

 Юрій РОССІНСЬКИЙ

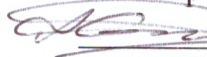
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій СФІМЕНКО

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Коцюба Дмитро Олександрович.

Тема роботи: Проект SIEM-підсистеми для SOC на базі рішень IBM QRadar.

затверджена Наказом університету від 5 березня 2024 р. № 98

Термін здачі студентом закінченої роботи 10 червня 2024 р.

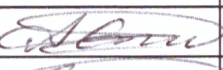
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єктом дослідження є процес проектування підсистеми збору інформації про безпеку та управління подіями для SOC з використанням рішень IBM QRadar та аналіз її функціонування. Предметом дослідження є технологія проектування підсистем моніторингу подій безпеки SOC з використанням рішень IBM QRadar.

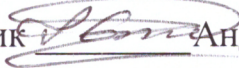
Обладнання та програмне забезпечення:

1. SIEM-рішення IBM QRadar Community Edition (v.7.3.3);
2. Windows Server 2019;
3. Windows 10 (64-bit);
4. Kali Linux 2024.1;
5. Мережевий емулятор GNS3 (v. 2.2.46).

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	05.03.2024 	05.03.2024 
2	Єфіменко А.А.	05.03.2024 	05.03.2024 
3	Єфіменко А.А.	05.03.2024 	05.03.2024 

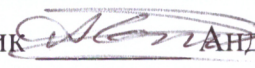
Студент  Дмитро КОЦЮБА

Керівник  Андрій ЄФІМЕНКО

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	05 березня 2024	виконано
2	Аналіз рішення IBM QRadar	14 березня 2024	виконано
3	Проектування загальної топології	19 березня 2024 – 23 березня 2024	виконано
4	Налаштування мережі	23 квітня 2024	виконано
5	Розгортання рішень IBM QRadar	26 квітня 2024	виконано
6	Налаштування засобів моніторингу	5 травня 2024	виконано
7	Тестування налаштованої мережі	10 травня 2024	виконано
8	Написання пояснювальної записки	17 травня 2024 – 9 червня 2024	виконано
9	Підготовка додаткових матеріалів	10 червня 2024	виконано
10	Отримання відгуку та рецензії на кваліфікаційну роботу	14 червня 2024	Використано
11	Захист кваліфікаційної роботи		

Студент  Дмитро КОЦЮБА

Керівник  Андрій ЄФІМЕНКО

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра представляє з себе проект підсистеми SIEM для SOC на базі рішень IBM QRadar.

Мета і завдання роботи. Метою роботи є проектування підсистеми SIEM для SOC з використанням рішень IBM QRadar.

Досягнення поставленої мети передбачає розв'язання наступних завдань:

- Вивчення основних вимог до систем управління подіями та інцидентами інформаційної безпеки (SIEM);
- Оцінка можливостей інтеграції IBM QRadar з іншими системами безпеки та інформаційними системами організації;
- Розробка архітектури підсистеми SIEM на основі IBM QRadar, включаючи визначення ключових компонентів та їх взаємодію.
- Налаштування та оптимізація IBM QRadar для забезпечення максимальної ефективності роботи.
- Проведення тестування та аналіз результатів для виявлення та усунення можливих недоліків.
- Оцінка ефективності підсистеми у виявленні та реагуванні на інциденти інформаційної безпеки.

Об'єктом дослідження є процес проектування підсистеми SIEM для SOC на базі рішень IBM QRadar.

Предметом дослідження є технологія проектування підсистеми SIEM для SOC на базі рішень IBM QRadar.

Пояснювальна записка до випускної кваліфікаційної роботи містить в собі 73 сторінки, 4 таблиці та 61 рисунок. Список використаних джерел містить 17 найменувань і займає 2 сторінки.

Ключові слова: SIEM, SOC, ІНФОРМАЦІЙНА БЕЗПЕКА, МОНІТОРИНГ БЕЗПЕКИ, РЕАГУВАННЯ НА ІНЦИДЕНТИ, ВИЯВЛЕННЯ ЗАГРОЗ, АНАЛІТИК.

KKIB.KP.B – 125 – 08 – ПЗ

Змн.	Арк.	№ докум.	Підпис	Дата	Проект SIEM-підсистеми для SOC на базі рішень IBM QRadar	Лім.	Арк.	Аркушів
Розроб.		Коцюба Д.О.		14.06				
Керівник		Сфіменко А.А.		14.06.24			4	78
Реценз.		Росінський Ю.М.		14.06.24		ФІКТ, Гр. КБ-20-1		
Н. контр.		Сфіменко А.А.		14.06.24				
Затверд.		Сфіменко А.А.		14.06.24				

ANNOTATION

The Bachelor's graduation qualification work is a project of a SIEM subsystem for SOC based on IBM QRadar solutions.

The aim and objectives of the work. The aim of the work is to design a SIEM subsystem for SOC using IBM QRadar solutions.

Achieving this aim involves solving the following tasks:

- Studying the main requirements for Security Information and Event Management (SIEM) systems;
- Assessing the possibilities of integrating IBM QRadar with other security systems and the organization's information systems;
- Developing the architecture of the SIEM subsystem based on IBM QRadar, including identifying key components and their interactions;
- Configuring and optimizing IBM QRadar to ensure maximum efficiency;
- Conducting testing and analyzing results to identify and eliminate possible deficiencies;
- Evaluating the effectiveness of the subsystem in detecting and responding to security incidents.

The object of the research is the process of designing a SIEM subsystem for SOC based on IBM QRadar solutions.

The subject of the research is the technology of designing a SIEM subsystem for SOC based on IBM QRadar solutions.

The explanatory note to the graduation qualification work contains 73 pages, 4 tables, and 61 figures. The list of references includes 17 titles and occupies 2 pages.

Keywords: SIEM, SOC, INFORMATION SECURITY, SECURITY MONITORING, INCIDENT RESPONSE, THREAT DETECTION, ANALYTICS.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПРОЕКТУВАННЯ ПІДСИСТЕМ SIEM ДЛЯ SOC	10
1.1 Security Operations Center (SOC): роль та функції	10
1.2 Основні поняття та принципи SIEM.....	16
1.3 Як працює SIEM.....	19
1.4 Переваги SIEM.....	23
1.5 Огляд SIEM-рішень.....	25
1.6 Функції та можливості IBM QRadar.....	30
РОЗДІЛ 2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ SIEM ДЛЯ SOC НА БАЗІ IBM QRADAR.....	35
2.1 Проектування мережі.....	35
2.2 Аналіз рішення QRadar та програмного забезпечення WinCollect	43
2.3 Аналіз NetFlow у контексті SIEM-рішень.....	44
РОЗДІЛ 3 НАЛАШТУВАННЯ, РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ SIEM НА БАЗІ IBM QRADAR.....	46
3.1 Налаштування мережі	46
3.2 Налаштування служби каталогів Active Directory.....	53
3.3 Налаштування серверу QRadar та встановлення програмного забезпечення WinCollect.....	55
3.4 Налаштування мережевого протоколу NetFlow	62
3.5 Проведення тестування підсистеми	64
ВИСНОВКИ.....	71
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	72
ДОДАТКИ	74

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SIEM – Security Information and Event Management

SOC – Security Operations Center

IPS – Intrusion Prevention System

UEBA – User and Entity Behavior Analytics

EDR – Endpoint Detection and Response

TIP – Threat Intelligence Platform

CISO – Chief Information Security Officer

CISSP – Certified Information Systems Security Professional

IoC – Indicator of Compromise

III – Штучний інтелект (Artificial Intelligence)

SIM – Security Information Management

SEM – Security Event Management

MTTD – Mean Time to Detect

MTTR – Mean Time to Respond

SOAR – Security Orchestration, Automation, and Response

VPN – Virtual Private Network

AD – Active Directory

DC – Domain Controller

OU – Organizational Unit

RDS – Remote Desktop Services

RDP – Remote Desktop Protocol

LDAP – Lightweight Directory Access Protocol

PoLP – Principle of Least Privilege

RBAC – Role-Based Access Control

IP – Internet Protocol

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

OSPF – Open Shortest Path First

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. У сучасному світі інформаційної безпеки, захист даних та управління інцидентами безпеки є критично важливими для організацій будь-якого масштабу. Кількість і складність кіберзагроз постійно зростають, що вимагає від організацій впровадження ефективних засобів для моніторингу, виявлення та реагування на ці загрози.

Системи управління подіями та інцидентами інформаційної безпеки (SIEM) є ключовими інструментами для забезпечення даних засобів. Вони дозволяють централізовано збирати, аналізувати та корелювати дані з різних джерел, що сприяє швидкому виявленню інцидентів безпеки та ефективному реагуванню на них.

IBM QRadar є одним із провідних рішень у сфері SIEM, відомим своєю потужністю, масштабованістю та можливістю інтеграції з іншими системами безпеки. Використання IBM QRadar дозволяє організаціям підвищити рівень захищеності своєї інформаційної інфраструктури, зменшити час на виявлення загроз та покращити процес управління інцидентами.

Метою кваліфікаційної роботи є розробка ефективної підсистеми SIEM для Security Operations Center (SOC) на базі рішень IBM QRadar, що забезпечить централізоване управління подіями та інцидентами інформаційної безпеки, підвищить рівень захищеності інформаційної інфраструктури організації, зменшить час на виявлення загроз та покращить процес реагування на інциденти.

У процесі виконання кваліфікаційної роботи було розроблено проект підсистеми SIEM для Security Operations Center (SOC) на базі рішень IBM QRadar. Проект включає в себе розробку архітектури системи, інтеграцію з іншими системами безпеки та налаштування для забезпечення максимальної ефективності виявлення та реагування на кіберзагрози.

Мета і завдання роботи. Метою роботи є проектування підсистеми SIEM для SOC з використанням рішень IBM QRadar.

Досягнення поставленої мети передбачає розв'язання наступних завдань:

– Вивчення основних вимог до систем управління подіями та інцидентами інформаційної безпеки (SIEM);

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

- Оцінка можливостей інтеграції IBM QRadar з іншими системами безпеки та інформаційними системами організації;
- Розробка архітектури підсистеми SIEM на основі IBM QRadar, включаючи визначення ключових компонентів та їх взаємодію.
- Налаштування та оптимізація IBM QRadar для забезпечення максимальної ефективності роботи.
- Проведення тестування та аналіз результатів для виявлення та усунення можливих недоліків.
- Оцінка ефективності підсистеми у виявленні та реагуванні на інциденти інформаційної безпеки.

Об’єктом дослідження є процес проектування підсистеми SIEM для SOC на базі рішень IBM QRadar.

Предметом дослідження є технологія проектування підсистеми SIEM для SOC на базі рішень IBM QRadar.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПРОЕКТУВАННЯ ПІДСИСТЕМ SIEM ДЛЯ SOC

1.1 Security Operations Center (SOC): роль та функції

Операційний центр безпеки (SOC) є централізованою функцією в організації, що об'єднує людей, процеси та технології для безперервного моніторингу та покращення стану безпеки організації, запобігаючи інцидентам кібербезпеки, виявляючи їх, аналізуючи та реагуючи на них [12].

SOC функціонує як центр або центральний командний пункт, збираючи телеметричні дані з усієї IT-інфраструктури організації, включаючи її мережі, пристрої, прилади та сховища інформації, незалежно від їх місця розташування. Поширення сучасних загроз робить особливо важливим збір контексту з різних джерел. По суті, SOC є точкою кореляції для кожної події, що реєструється в організації, яка знаходиться під моніторингом. Для кожної з цих подій SOC повинен вирішити, як ними керувати і як на них реагувати.

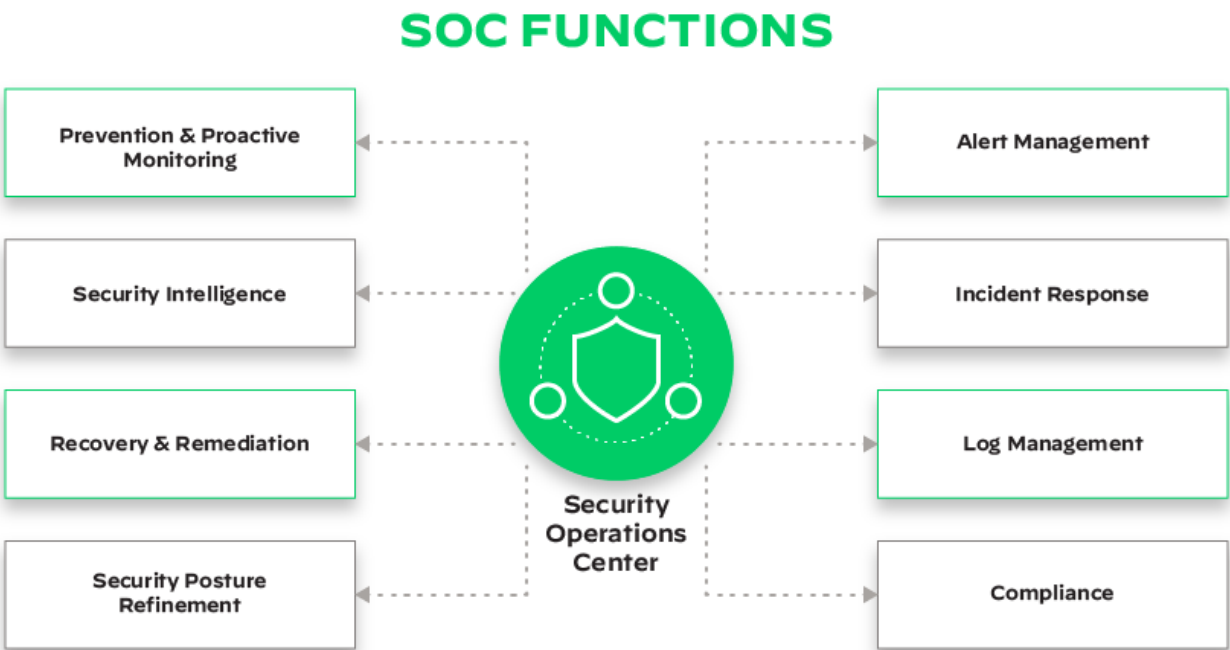


Рисунок 1.1 – Функції Security Operations Center

Функція оперативної групи з питань безпеки, а часто і оперативного центру безпеки (SOC), полягає в цілодобовому моніторингу, виявленні, розслідуванні та

реагуванні на кіберзагрози. Вони відповідають за моніторинг і захист багатьох активів, таких як інтелектуальна власність, персональні дані, бізнес-системи та цілісність бренду. Як частина загальної системи кібербезпеки організації, оперативні групи безпеки виступають центральним пунктом співпраці для скоординованих зусиль з моніторингу, оцінки та захисту від кібератак.

SOC, як правило, будуються на основі архітектури типу hub-and-spoke, причому елементи цієї моделі можуть включати різноманітні системи, такі як рішення для оцінки вразливостей, системи управління, ризиків і відповідності (GRC), сканери додатків і баз даних, системи запобігання вторгненням (IPS), аналітика поведінки користувачів і організацій (UEBA), системи виявлення і усунення вразливостей кінцевих точок (EDR), а також платформи розвідки загроз (TIP) [11].

Зазвичай SOC очолює менеджер SOC, і до її складу можуть входити фахівці з реагування на інциденти, аналітики SOC (рівні 1, 2 і 3), мисливці за загрозами та менеджер(и) з реагування на інциденти. SOC підпорядковується CISO, який, у свою чергу, підпорядковується IT-директору або безпосередньо генеральному директору.

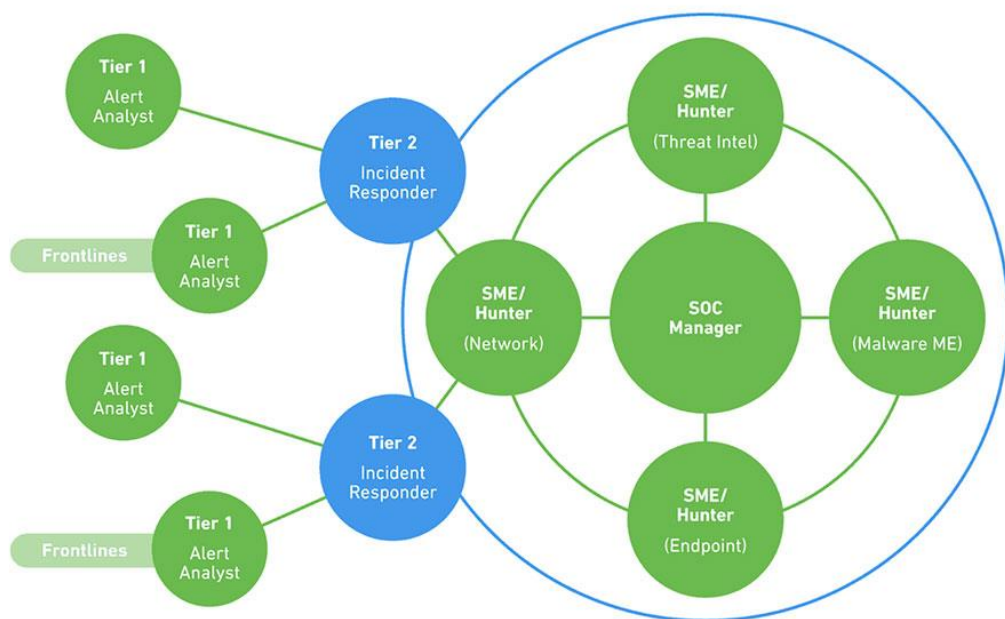


Рисунок 1.2 – Структура ролей SOC

Аналітики SOC організовані в чотири рівні. Спочатку оповіщення SIEM надходять до аналітиків рівня 1, які відстежують їх, визначають пріоритети та розслідують. Реальні загрози передаються аналітику рівня 2 з більш глибоким досвідом у сфері безпеки, який проводить подальший аналіз і приймає рішення про стратегію стримування.

Критичні порушення передаються старшому аналітику рівня 3, який керує інцидентом і відповідає за постійне активне полювання на загрози. Аналітик рівня 4 - це менеджер SOC, який відповідає за підбір персоналу, стратегію, пріоритети та безпосереднє управління персоналом SOC у разі виникнення серйозних інцидентів безпеки [9].

Аналітик рівня 1 (розслідувач з питань оповіщення):

- Кваліфікація: Навички системного адміністрування; мови веб-програмування, такі як Python, Ruby, PHP; мови сценаріїв; сертифікати безпеки, такі як CISSP або SANS SEC401.

- Обов'язки: Відстежує оповіщення SIEM, керує та налаштовує інструменти моніторингу безпеки. Визначає пріоритети та сортує оповіщення або проблеми, щоб визначити, чи має місце реальний інцидент безпеки.

Аналітик рівня 2 (реагування на інциденти):

- Кваліфікація: Подібно до аналітика рівня 1, але з більшим досвідом, включаючи реагування на інциденти. Просунута криміналістика, оцінка шкідливого програмного забезпечення, розвідка загроз. Сертифікація або навчання з етичного хакінгу є великою перевагою.

- Обов'язки: Отримує інциденти та проводить глибокий аналіз; співвідносить з розвідкою загроз для визначення суб'єкта загрози, характеру атаки, а також систем або даних, що постраждали. Визначає та реалізує стратегію стримування, виправлення та відновлення.

Аналітик рівня 3 (предметний експерт / мисливець за загрозами):

- Кваліфікація: Подібно до аналітика рівня 2, але з ще більшим досвідом, включаючи інциденти високого рівня. Досвід роботи з інструментами тестування

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

на проникнення та міжорганізаційної візуалізації даних. Досвід реінжинірингу шкідливого програмного забезпечення, досвід виявлення та розробки відповідей на нові загрози та шаблони атак.

– **Обов'язки:** Щоденно проводить оцінку вразливостей і тести на проникнення, а також аналізує оповіщення, новини галузі, аналітику загроз і дані про безпеку. Активно шукає загрози, які вже проникли в мережу, а також невідомі вразливості та прогалини в системі безпеки. У разі виникнення серйозного інциденту співпрацює з аналітиком рівня 2 для реагування та локалізації інциденту.

SOC-менеджер рівня 4:

– **Кваліфікація:** Аналогічно до аналітика рівня 3, включаючи навички управління проектами, підготовку з управління реагуванням на інциденти та сильні комунікативні навички.

– **Обов'язки:** Як командир військової частини, відповідає за найм та навчання персоналу SOC, відповідає за оборонну та наступальну стратегію. Керує ресурсами, пріоритетами та проектами, а також безпосередньо керує командою під час реагування на критично важливі для бізнесу інциденти безпеки. Контактна особа організації щодо інцидентів безпеки, дотримання вимог та інших питань, пов'язаних з безпекою.

Інженер з безпеки (підтримка та інфраструктура):

– **Кваліфікація:** Вчений ступінь в галузі інформатики, комп'ютерної інженерії або інформаційного забезпечення, як правило, в поєднанні з такими сертифікатами, як CISSP.

– **Обов'язки:** Спеціаліст з програмного або апаратного забезпечення, який фокусується на аспектах безпеки при розробці інформаційних систем. Створює рішення та інструменти, які допомагають організаціям надійно протистояти збоям в роботі або зловмисним атакам. Іноді працює в SOC, а іноді підтримує SOC у складі команд розробників або операційних команд.

Існує кілька різних способів, як організації створюють свої SOC. Деякі вирішують створити спеціальний SOC зі штатним персоналом. Цей тип SOC може

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

бути внутрішнім, з фізичним розташуванням на території організації, або віртуальним, коли співробітники координують роботу віддалено, використовуючи цифрові інструменти. Багато віртуальних SOC використовують комбінацію контрактного та штатного персоналу. Аутсорсинговий SOC, який також може називатися керованим SOC або операційним центром безпеки як послугою, управляється керованим постачальником послуг безпеки, який бере на себе відповідальність за запобігання, виявлення, розслідування та реагування на загрози. Також можливе використання комбінації внутрішнього персоналу та керованого постачальника послуг безпеки. Цей варіант називається керованим або гібридним SOC. Організації використовують цей підхід для розширення власного штату. Наприклад, якщо у них немає спеціалістів з розслідування загроз, простіше найняти третю сторону, ніж намагатися укомплектувати штат власними силами.

У той час як робота з інцидентами монополізує більшу частину ресурсів SOC, керівник служби інформаційної безпеки (CISO) відповідає за загальну картину ризиків і дотримання нормативних вимог. Для подолання розрізненості між цими функціями, ефективна стратегія вимагає адаптивної архітектури безпеки, яка дозволяє організаціям впроваджувати оптимізовані операції з безпеки. Такий підхід підвищує ефективність за рахунок інтеграції, автоматизації та оркестрування, а також зменшує кількість необхідних робочих годин, покращуючи при цьому стан управління інформаційною безпекою.

Оптимізована модель операцій з безпеки вимагає впровадження системи безпеки, яка дозволяє легко інтегрувати рішення з безпеки та аналітику загроз у повсякденні процеси. Інструменти SOC, такі як централізовані інформаційні панелі, допомагають інтегрувати дані про загрози в панель моніторингу безпеки та звіти, щоб інформувати операторів і керівництво про події та дії, що розвиваються. Пов'язуючи управління загрозами з іншими системами управління ризиками та дотриманням нормативних вимог, команди SOC можуть краще керувати загальною ситуацією з ризиками. Такі конфігурації підтримують безперервну видимість систем

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

і доменів і можуть використовувати оперативну інформацію для підвищення точності та узгодженості операцій з безпеки. Централізовані функції зменшують тягар ручного обміну даними, аудиту та звітності.

Оперативне управління загрозами має починатися з ретельної оцінки. На додаток до захисту, організація повинна оцінити процеси та політики. Де організація сильна? Які є прогалини? Яка позиція щодо ризиків? Які дані збираються і скільки з них використовується?

Хоча кожна організація відрізняється від інших, певні основні можливості та найкращі практики у сфері безпеки сьогодні потребують належної уваги. Розумний процес управління загрозами починається з плану і включає в себе виявлення (в тому числі розрахунок базової лінії для сприяння виявленню, нормалізації та кореляції аномалій), сортування (на основі ризику і цінності активів), аналіз (в тому числі контекстуалізацію) і визначення обсягу (в тому числі ітеративне розслідування). Процеси управління загрозами передають пріоритезовані та описані випадки в програми реагування на інциденти. Чітко розроблений план реагування є ключовим фактором для стримування загрози або мінімізації збитків від витоку даних.

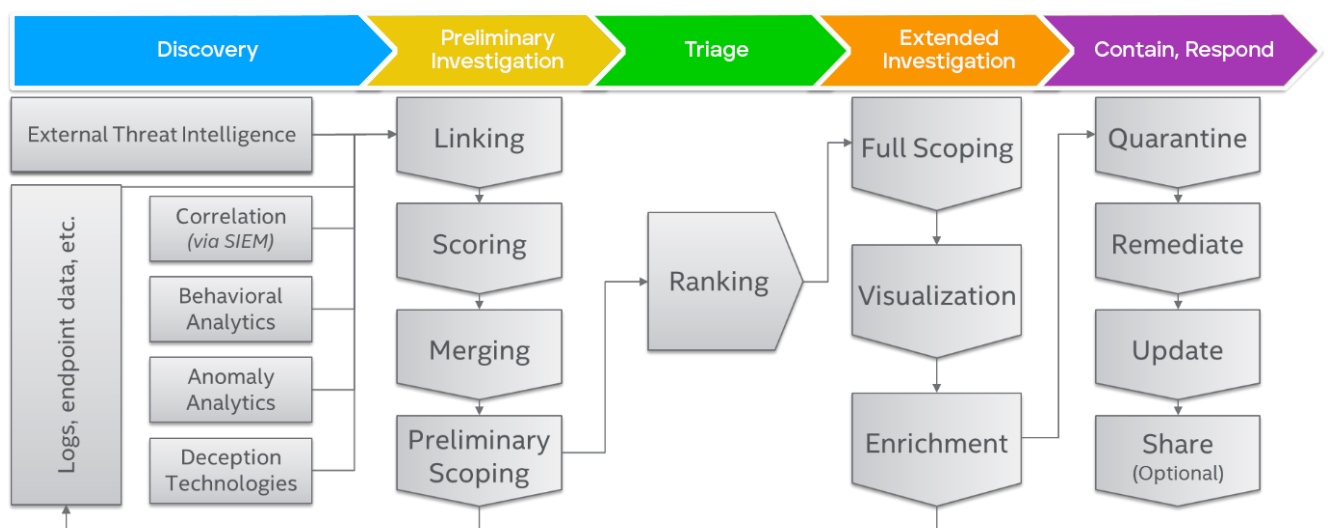


Рисунок 1.3 – Плани управління загрозами

Ефективна видимість та управління загрозами залежать від багатьох джерел даних, але відсортувати корисну та своєчасну інформацію може бути складно. Найціннішими виявляються дані про події, отримані за допомогою контрзаходів та ІТ-

активів, індикатори компрометації (IoC), зібрані як внутрішньо (через аналіз шкідливого програмного забезпечення), так і ззовні (через канали розвідки загроз), а також системні дані, доступні з датчиків (наприклад, хост, мережа, база даних тощо).

Такі джерела даних - це не просто вхідні дані для управління загрозами. Вони додають контекст і роблять інформацію цінною і придатною для дій для більш точної, достовірної і швидкої оцінки в ході ітеративних і інтерактивних зусиль з управління загрозами. Доступ до правильних даних для підтримки планів і процедур та їх ефективне використання є показником зрілості організації. «Зрілий» сценарій включає в себе робочий процес, який передає потрібну інформацію або дозволяє прямі дії в операційних консолях і в різних продуктах. Цей потік інтегрує IT-операції, команди та інструменти безпеки в реагування на інциденти, коли відбувається критична подія.

1.2 Основні поняття та принципи SIEM

Управління інформацією та подіями безпеки (SIEM) - це рішення для забезпечення безпеки, яке допомагає організаціям розпізнавати та усувати потенційні загрози та вразливості ще до того, як вони встигнуть порушити бізнес-операції. SIEM-системи допомагають командам безпеки підприємств виявляти аномалії в поведінці користувачів і використовувати штучний інтелект (ШІ) для автоматизації багатьох ручних процесів, пов'язаних з виявленням загроз і реагуванням на інциденти [15].

Перші платформи SIEM були інструментами управління журналами. Вони поєднували в собі функції управління інформацією про безпеку (SIM) та управління подіями безпеки (SEM). Ці платформи дозволяли здійснювати моніторинг та аналіз подій, пов'язаних з безпекою, в режимі реального часу. Крім того, вони полегшили відстеження та реєстрацію даних про безпеку з метою дотримання нормативних вимог або аудиту. У 2005 році компанія Gartner винайшла термін SIEM для позначення поєднання технологій SIM і SEM [15].

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		16



SIM vs SEM vs SIEM

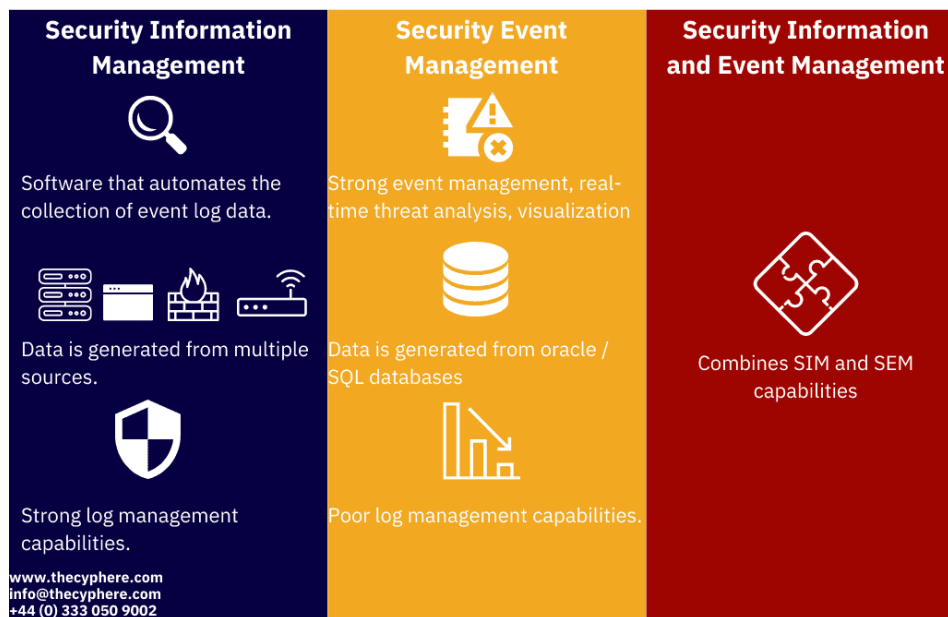


Рисунок 1.4 – Технології інформаційної безпеки та управління

З роками програмне забезпечення SIEM еволюціонувало, включивши в себе аналітику поведінки користувачів і організацій (UEBA), а також інші розширені можливості аналітики безпеки, штучного інтелекту і машинного навчання для виявлення аномальної поведінки та індикаторів сучасних загроз. Сьогодні SIEM стала основним інструментом в сучасних операційних центрах безпеки (SOC) для моніторингу безпеки та управління комплаєнсом.

На додаток до SIEM, співробітники служби безпеки можуть визначати звичайну і ненормальну активність за допомогою правил. Більш просунуті рішення, які називаються SIEM наступного покоління, пропонують машинне навчання та штучний інтелект для постійного оновлення поведінкових моделей аналітики поведінки користувачів та організацій (UEBA), щоб зменшити кількість помилкових спрацьовувань. У SIEM наступного покоління дані, зібрані системою SIEM, аналізуються відповідно до визначених правил і виявлених поведінкових патернів. Щоразу, коли виявляється аномальна активність, генерується помітна подія для аналізу.

Рішення SIEM забезпечують індивідуальний захист кібербезпеки на основі заздалегідь визначених правил, кореляції подій безпеки та машинного навчання.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Вони також зберігають дані журналів протягом тривалого часу, що полегшує пошук історичної інформації та створення звітів про дотримання нормативних вимог.

Таблиця 1.1 – Порівняння систем SIM, SEM та SIEM

Характеристика	SIM (Security Information Management)	SEM (Security Event Management)	SIEM (Security Information and Event Management)
Основне призначення	Збір, зберігання та аналіз логів	Моніторинг та обробка подій безпеки в реальному часі	Інтеграція збору логів та моніторингу подій для всебічного управління безпекою
Функціональність	Аналіз історичних даних, довготривале зберігання логів	Реальний часовий моніторинг, оповіщення про події	Поєднує функції SIM та SEM для комплексного аналізу і реагування на загрози
Виявлення загроз	Обмежено	В реальному часі	В реальному часі та ретроспективно
Аналітика та звіти	Поглиблена аналітика, історичні звіти	Оперативні звіти, реальні часові оповіщення	Поглиблена аналітика та оперативні звіти
Приклад інструментів	ArcSight Logger, Splunk	SolarWinds SEM, Sumo Logic	Splunk Enterprise Security, IBM QRadar, ArcSight

Інші інструменти також увійшли в простір SIEM, зокрема, аналіз поведінки користувачів (UBA). Також відомий як аналіз поведінки користувачів і організацій (UEBA), UBA використовується для виявлення і усунення внутрішніх і зовнішніх загроз.

Хоча UBA часто розглядається як більш просунутий інструмент безпеки, його все частіше відносять до категорії SIEM. Наприклад, магічний квадрант Gartner для SIEM включає інформацію про пропозиції UBA/UEBA.

UBA працює в двох напрямках:

- Створення базової лінії для даних будь-якого користувача або програми. Потім виділяє відхилення від цієї норми, які можуть становити загрозу.
- Моніторинг зловмисної поведінки та превентивне вирішення проблем безпеки.

Ці функції відіграють важливу роль у будь-якому рішенні SIEM, оскільки вони висвітлюють моделі поведінки в мережі організації, пропонуючи контекст, якого раніше не було. Вони також фільтрують сповіщення до того, як команда операційного центру безпеки (SOC) отримає повідомлення, допомагаючи зменшити втому від сповіщень і звільняючи час аналітиків для більш складних або термінових загроз.

1.3 Як працює SIEM

На найпростішому рівні всі рішення SIEM виконують певні функції агрегації, консолідації та сортування даних для виявлення загроз і дотримання вимог щодо відповідності даних. Хоча деякі рішення відрізняються за можливостями, більшість з них пропонують однаковий базовий набір функцій:

Управління журналами (Log management). SIEM збирає дані про події з широкого спектру джерел по всій IT-інфраструктурі організації, включаючи локальні та хмарні середовища.

Дані журналів подій від користувачів, кінцевих точок, додатків, джерел даних, хмарних робочих навантажень і мереж, а також дані з апаратного і програм-

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

ного забезпечення для забезпечення безпеки, наприклад, брандмауерів або антивірусного програмного забезпечення, збираються, співставляються і аналізуються в режимі реального часу [15].



Рисунок 1.5 – Візуалізація принципу роботи управління журналами

Деякі рішення SIEM також інтегруються зі сторонніми каналами розвідки загроз, щоб співвідносити свої внутрішні дані про безпеку з раніше розпізнаними сигнатурами і профілями загроз. Інтеграція з каналами загроз у режимі реального часу дозволяє командам блокувати або виявляти нові типи сигнатур атак.

Кореляція подій є невід'ємною частиною будь-якого рішення SIEM. Використовуючи розширену аналітику для виявлення і розуміння складних шаблонів даних, кореляція подій дає можливість швидко знаходити і зменшувати потенційні загрози для безпеки бізнесу.

Рішення SIEM значно покращують середній час виявлення (MTTD) і середній час реагування (MTTR) для команд IT-безпеки, розвантажуючи ручні робочі процеси, пов'язані з поглибленим аналізом подій безпеки.

Моніторинг інцидентів та оповіщення про безпеку. SIEM консолідує аналіз на єдиній центральній інформаційній панелі, де команди безпеки відстежують активність, сортують сповіщення, ідентифікують загрози та ініціюють реагування або усунення.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

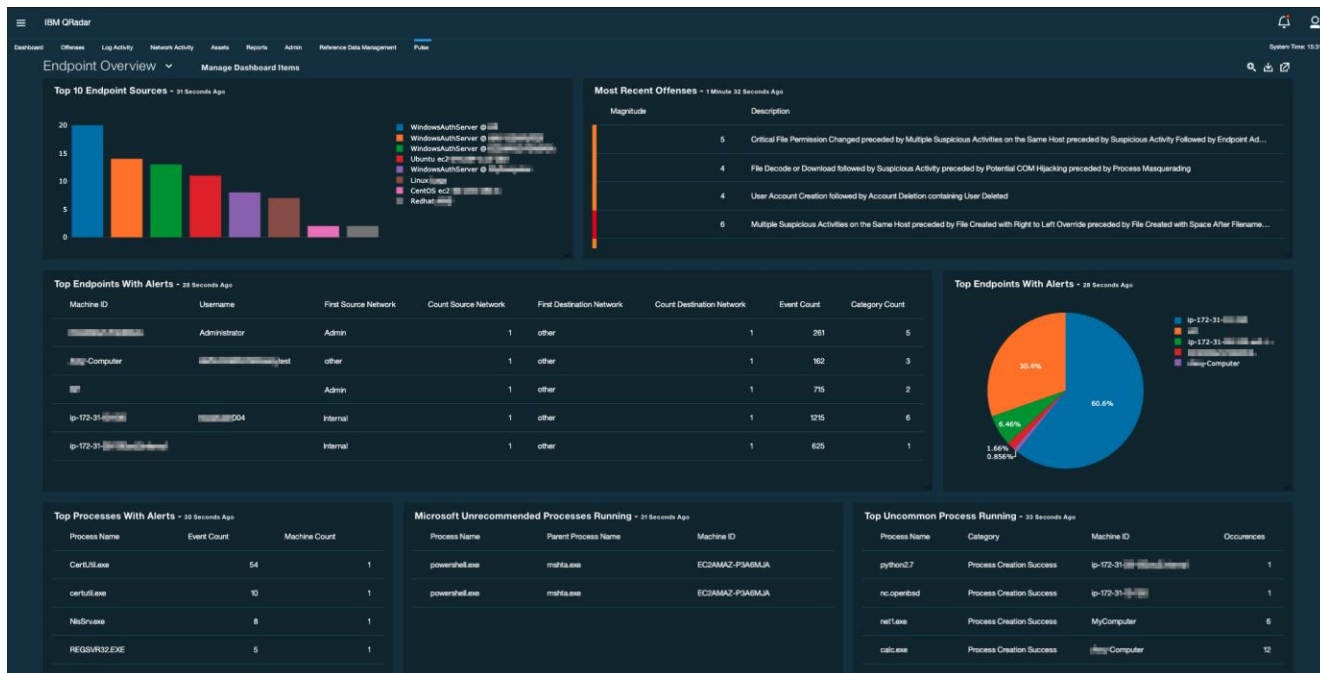


Рисунок 1.6 – Центральна інформаційна панель IBM Qradar

Більшість інформаційних панелей SIEM також включають візуалізацію даних у режимі реального часу, що допомагає аналітикам безпеки виявляти сплески або тенденції підозрілої активності. Використовуючи настроювані, заздалегідь визначені правила кореляції, адміністратори можуть негайно отримувати сповіщення та вживати відповідних заходів для зменшення загроз до того, як вони переростуть у серйозніші проблеми безпеки.

Управління дотриманням нормативних вимог та звітність. Рішення SIEM є популярним вибором для організацій, які підлягають різним формам нормативно-правового регулювання. Завдяки автоматизованому збору та аналізу даних SIEM є цінним інструментом для збору та перевірки даних про дотримання нормативних вимог у всій бізнес-інфраструктурі.

Рішення SIEM можуть генерувати звіти про відповідність вимогам PCI-DSS, GDPR, HIPAA, SOX та інших стандартів у режимі реального часу, зменшуючи навантаження на управління безпекою і виявляючи потенційні порушення на ранній стадії, щоб їх можна було усунути. Багато рішень SIEM постачаються з попередньо встановленими, готовими до використання надбудовами, які можуть генерувати автоматизовані звіти, призначені для виконання вимог нормативно-правових актів.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Атрибути, які можуть бути проаналізовані, включають користувачів, типи подій, IP-адреси, пам'ять, процеси тощо.

Продукти SIEM класифікують відхилення як, наприклад, «невдалий вхід», «зміна облікового запису» або «потенційне шкідливе програмне забезпечення». Відхилення призводить до того, що система сповіщає аналітиків з безпеки та/або діє, щоб призупинити незвичну активність. Встановлюються інструкції щодо того, що викликає сповіщення, і встановлюються процедури для роботи з підозрою на зловмисну активність.

Рішення SIEM також розпізнає шаблони та аномальну поведінку. Таким чином, якщо окрема подія не викликає тривоги, SIEM може виявити взаємозв'язок між кількома подіями, які в іншому випадку залишилися б непоміченими, що призведе до спрацьовування оповіщення.

Нарешті, рішення SIEM зберігає ці журнали в базі даних, що дозволяє проводити більш глибокі криміналістичні розслідування або доводити, що ви дотримуетесь чинних нормативних вимог.

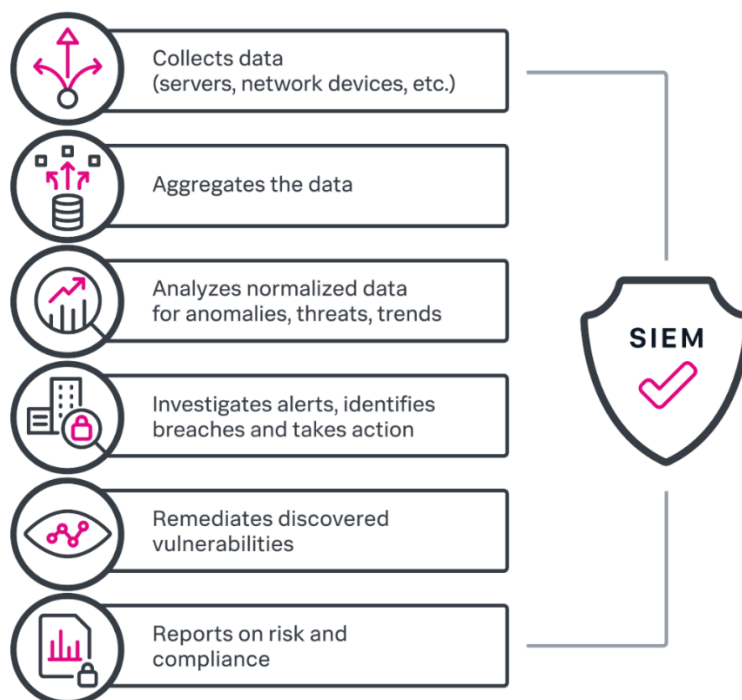


Рисунок 1.7 – Структура SIEM системи

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

1.4 Переваги SIEM

Незалежно від того, наскільки великою чи малою є організація, проактивні кроки для моніторингу та зменшення ризиків ІТ-безпеки є вкрай важливими. Рішення SIEM приносять користь підприємствам різними способами і стали важливим компонентом в оптимізації робочих процесів безпеки.

Рішення SIEM забезпечують централізований аудит відповідності та звітність по всій бізнес-інфраструктурі. Розширена автоматизація спрощує збір та аналіз системних журналів і подій безпеки, що дозволяє зменшити використання внутрішніх ресурсів, одночасно дотримуючись суворих стандартів звітності про відповідність.

Сучасні рішення SIEM нового покоління інтегруються з потужними системами оркестрування, автоматизації та реагування на загрози (SOAR), заощаджуючи час і ресурси ІТ-команд, які керують безпекою бізнесу.

Використовуючи глибоке машинне навчання, яке автоматично вчиться на поведінці мережі, ці рішення можуть обробляти складні протоколи ідентифікації загроз і реагування на інциденти за менший час, ніж фізичні команди.

Завдяки покращеній видимості ІТ-середовищ, яку вона забезпечує, SIEM може стати важливим фактором підвищення ефективності роботи між відділами.

Центральна інформаційна панель забезпечує уніфікований перегляд системних даних, оповіщень і сповіщень, що дозволяє командам ефективно спілкуватися і співпрацювати при реагуванні на загрози та інциденти безпеки.

З огляду на те, як швидко змінюється ландшафт кібербезпеки, організаціям необхідно мати можливість покладатися на рішення, здатні виявляти і реагувати як на відомі, так і на невідомі загрози безпеці [15].

Використовуючи інтегровані канали розвідки загроз і технології штучного інтелекту, рішення SIEM можуть допомогти командам безпеки ефективніше реагувати на широкий спектр кібератак, включаючи:

- **Внутрішні загрози:** Уразливості в системі безпеки або атаки, що походять від осіб, які мають санкціонований доступ до мереж і цифрових активів компанії.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

– **Фішинг:** повідомлення, які виглядають як надіслані надійним відправником, часто використовуються для крадіжки даних користувачів, облікових даних для входу в систему, фінансової інформації або іншої конфіденційної бізнес-інформації.

– **Програми-вимагачі:** Шкідливе програмне забезпечення, яке блокує дані або пристрій жертви і погрожує зберегти їх заблокованими або ще гірше, якщо жертва не заплатить викуп зловмиснику.

– **Розподілені атаки на відмову в обслуговуванні (DDoS):** Атаки, які бомбардують мережі та системи некерованим трафіком з розподіленої мережі викрадених пристроїв (ботнету), знижуючи продуктивність веб-сайтів і серверів до неможливості їх використання.

– **Витік даних:** Крадіжка даних з комп'ютера або іншого пристрою, що здійснюється вручну або автоматично за допомогою шкідливого програмного забезпечення.

Рішення SIEM ідеально підходять для проведення комп'ютерних криміналістичних розслідувань після інциденту безпеки. Рішення SIEM дозволяють організаціям ефективно збирати та аналізувати дані журналів з усіх своїх цифрових активів в одному місці.

Це дає їм можливість відтворювати минулі інциденти або аналізувати нові, щоб розслідувати підозрілу активність і впроваджувати більш ефективні процеси безпеки.

Аудит та звітність з комплаєнсу є необхідним і водночас складним завданням для багатьох організацій. Рішення SIEM значно скорочують витрати ресурсів, необхідних для управління цим процесом, забезпечуючи аудит в режимі реального часу і надання звітів про відповідність нормативним вимогам на вимогу, коли це необхідно.

Зі зростанням популярності віддаленої роботи, додатків SaaS і політик BYOD (bring your own device) організаціям потрібен рівень видимості, необхідний для зменшення мережевих ризиків за межами традиційного мережевого периметру.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Рішення SIEM відстежують всю мережеву активність всіх користувачів, пристроїв і додатків, значно підвищуючи прозорість всієї інфраструктури і виявляючи загрози незалежно від того, звідки здійснюється доступ до цифрових активів і сервісів.

1.5 Огляд SIEM-рішень

SIEM стала базовим компонентом кібербезпеки. Однак не всі рішення SIEM однакові. Приймаючи рішення про те, який SIEM обрати, важливо пам'ятати, що SIEM не є ізольованим рішенням, а має бути частиною більш широкої стратегії безпеки. Деякі з найкращих рішень SIEM перераховані нижче.

Як SIEM нового покоління, **Exabeam Fusion** - це хмарне рішення, яке використовує поведінковий підхід для виявлення, розслідування та реагування на загрози (TDIR). Об'єднуючи всі релевантні події і відсіваючи нелегітимні, Fusion SIEM підвищує продуктивність аналітиків і виявляє загрози, пропущені іншими інструментами. Це покращує показники виявлення та час реагування, а також гарантує, що всі оповіщення будуть враховані - навіть ті, що надходять від «шумних» систем, які генерують багато оповіщень.

Крім того, Fusion SIEM інтегрований з рішенням для оркестрування та автоматизації безпеки (SOAR), яке забезпечує автоматизоване реагування на інциденти. Це дозволяє автоматично (або напівавтоматично) боротися з майже будь-якою загрозою в режимі реального часу. Заздалегідь визначені робочі процеси та заздалегідь підготовлені сценарії використання (зовнішні загрози, скомпрометовані інсайдери та зловмисні інсайдери) забезпечують успішні результати SOC та автоматизацію реагування на інциденти. Fusion SIEM також забезпечує хмарне зберігання журналів, швидкий і керований пошук, а також всебічну звітність про дотримання нормативних вимог, що очікується від будь-якого сучасного SIEM [1].

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

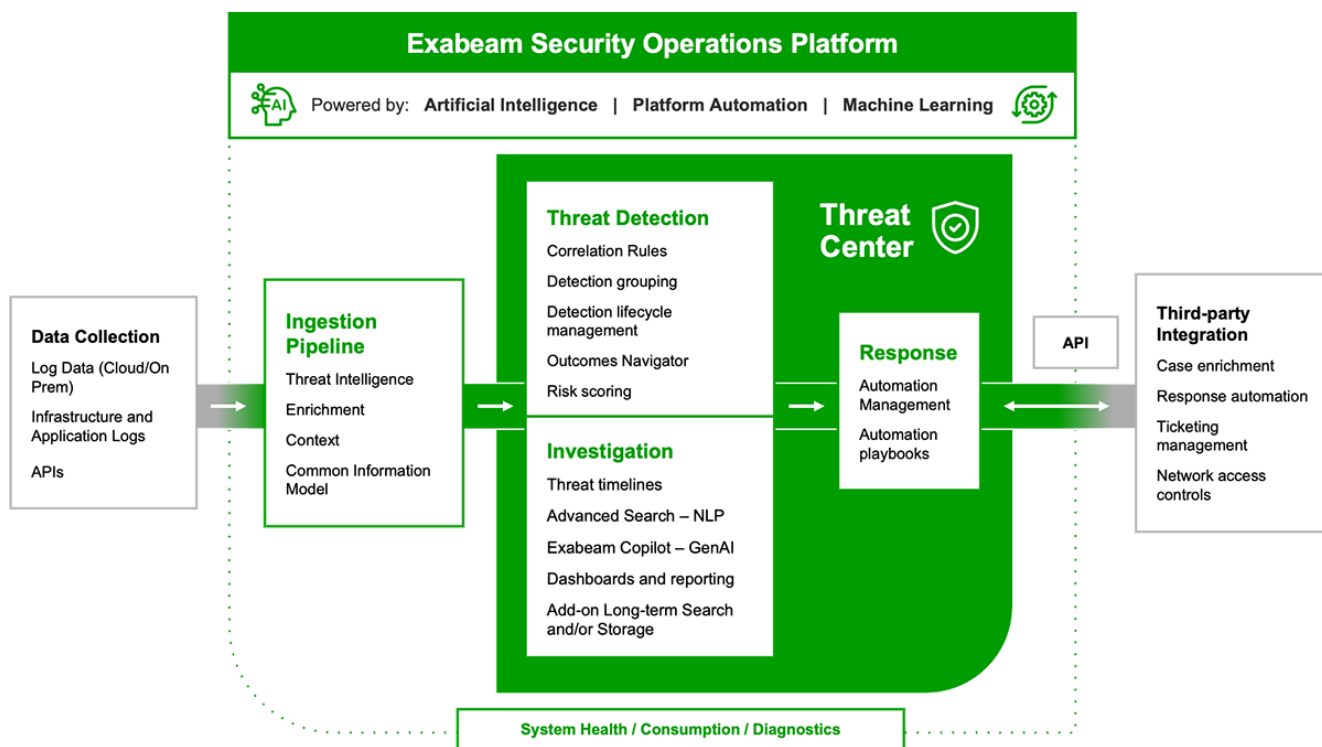


Рисунок 1.8 – Візуалізація роботи Exabeam Fusion

З Exabeam Fusion аналітики можуть запускати свої наскрізні робочі процеси TDIR з єдиної площини управління, яка виконує автоматизацію завдань, що вимагають ручної роботи, таких як сортування оповіщень з динамічним визначенням пріоритетів, детальне розслідування інцидентів та реагування на інциденти з можливістю додавання сотень інтеграцій SOAR. Щоб забезпечити краще розуміння вашої системи безпеки, Exabeam Fusion Outcomes Navigator аналізує охоплення сценаріїв використання і пропонує джерела даних, а також аналізує зміни конфігурації, щоб закрити будь-які прогалини.

Splunk має популярне рішення SIEM. Що відрізняє його від інших постачальників, так це здатність працювати як з безпекою, так і з моніторингом додатків та мережі. Це робить його популярним як серед персоналу служби безпеки, так і серед користувачів ІТ-операцій. Як і більшість найкращих SIEM-рішень, SIEM від Splunk надає інформацію в режимі реального часу, а користувацький інтерфейс є відносно зручним. Ціна базується на робочих навантаженнях, що захищаються.

Однак Splunk Enterprise Security має обмежені можливості інтегрованої поведінкової аналітики та автоматизації, що створює проблеми з виявленням сучасних загроз і методів, таких як бічний рух. Рішення вимагає значної кастомізації,

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

щоб бути ефективним для більшості організацій, і не може використовуватися «з коробки». Щоб виявити бічний рух, багато спеціальних запитів повинен виконувати спеціалізований користувач, що потенційно може призвести до великої кількості хибних спрацьовувань. Ще однією проблемою, про яку повідомляють користувачі, є відсутність інтеграції між продуктами: SIEM, SOAR, UEBA [1].

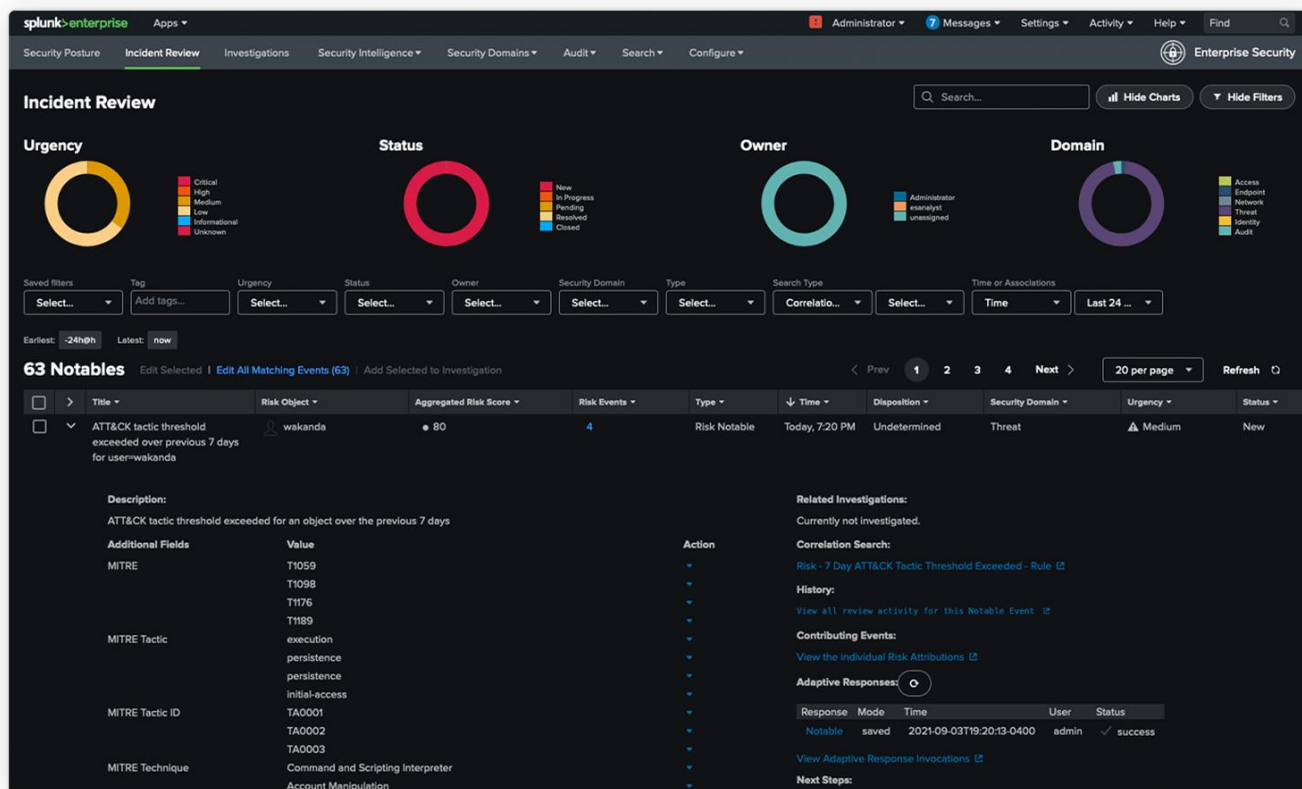


Рисунок 1.9 – Інтерфейс програмного продукту Splunk

IBM QRadar SIEM дозволяє переглядати вашу IT-інфраструктуру в режимі реального часу. Це модульна архітектура, яка полегшує виявлення та визначення пріоритетів загроз. Вона підтримує кілька протоколів реєстрації та пропонує різні варіанти конфігурації, а також аналітику високого рівня. Рішення має магазин додатків, де клієнти можуть завантажувати додатковий контент IBM і сторонніх виробників для використання з QRadar.

Однак, IBM QRadar має деякі недоліки, в тому числі відносно високу вартість (і складну модель ціноутворення), а також вимогу до функцій спільної роботи, таких як чат-інструменти і поліпшене управління активами. Крім того, QRadar має слабкі можливості UEBA, які є базовим компонентом SIEM наступного покоління.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Іншими недоліками є те, що в розподілених середовищах оновлення може бути складним і вимагати значних зусиль, оскільки підтримка продукту часто обмежена (хоча ви можете придбати оновлену підтримку). Продукт має обмежені можливості звітування, які необхідно доповнювати сторонніми скриптами [1].

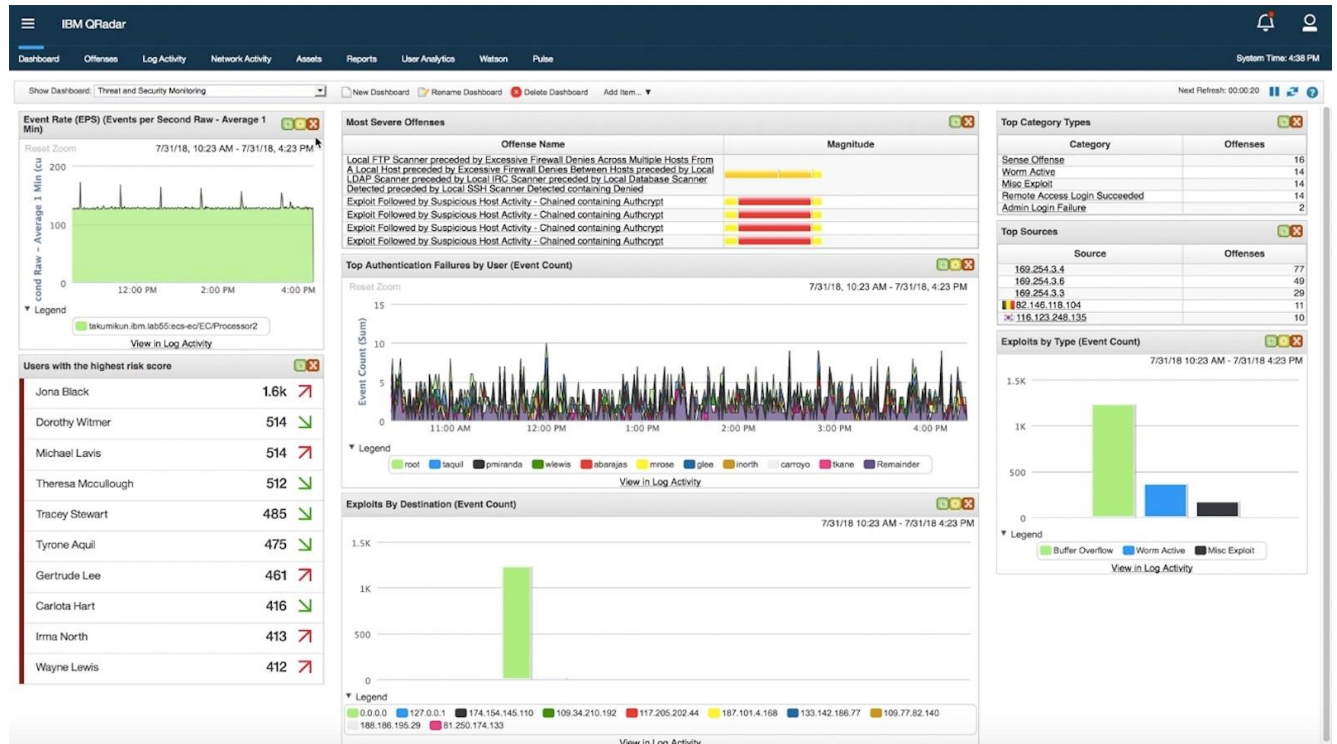


Рисунок 1.10 – Інтерфейс програмного продукту IBM QRadar

Переваги IBM QRadar:

- **Єдиний досвід аналітиків:** Інтуїтивно зрозумілий користувацький інтерфейс дозволяє аналітикам працювати швидше та ефективніше в процесі розслідування та реагування, використовуючи спільні ідеї та автоматизовані дії в різних продуктах. Використовуючи унікальні можливості штучного інтелекту корпоративного рівня, аналітики можуть автоматично контекстуалізувати загрози та визначати їх пріоритетність.
- **Хмарна доставка, швидкість і масштабування:** Продукти IBM Security QRadar Suite, що надаються як послуга на AWS, дозволяють спростити розгортання в хмарних середовищах та інтеграцію з даними журналів у публічній хмарі та SaaS.

Пакет також включає нову, хмарну функцію спостереження за безпекою та управління журналами, оптимізовану для отримання великих обсягів даних, субсекундного пошуку та швидкої аналітики.

- **Відкрита платформа та готові інтеграції:** Пакет об'єднує основні технології, необхідні в сучасних операційних центрах безпеки, побудовані на відкритій платформі і широкій партнерській екосистемі з більш ніж 900 попередньо створеними інтеграціями для гнучкості і вибору між продуктами IBM і сторонніх виробників. Він включає власні, попередньо інтегровані можливості для розвідки загроз, управління журналами, EDR, SIEM і SOAR.

LogRhythm є піонером SIEM і заробив собі добру репутацію. Рішення LogRhythm також включає в себе багато аналітичних інструментів, а також ІІІ та кореляцію логів. Хоча інтеграція з LogRhythm є відносно безпроблемною, існує більш крута крива навчання, оскільки вона не вважається такою ж зручною для користувача, як інші SIEM-системи.

Крім того, рішення LogRhythm не підтримує автоматичне виявлення всіх бічних рухів. Тому аналітикам доводиться вручну комбінувати різні часові шкали, щоб виявити перемикання акаунтів. Це проблематично, оскільки зловмисники часто використовують латеральний рух у вашій мережі для пошуку цінної інформації або активів. Механізм виявлення рішення сильно залежить від індикаторів компрометації (IOC) і має труднощі з виявленням просунутих загроз.

LogRhythm SIEM створює зручну для користувача історію інцидентів, яка консолідує дані користувача або хоста та його активність в одному вікні, допомагаючи аналітикам швидко зрозуміти та усунути інциденти безпеки. LogRhythm SIEM спрощує розслідування інцидентів та реагування на них за допомогою візуальних аналітичних панелей, які описують історію користувача або хоста, використовуючи всі доступні дані в SIEM. Це дозволяє командам безпеки зосередитися на найбільш важливих питаннях [1].

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

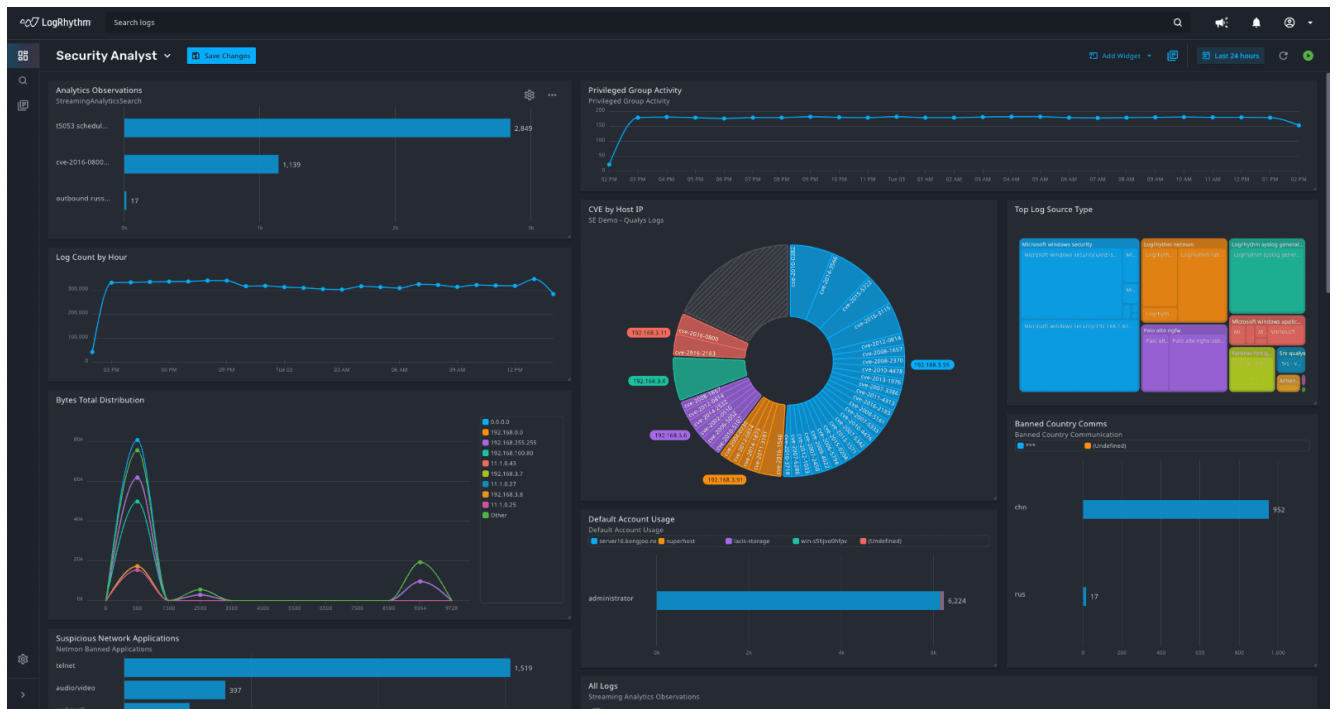


Рисунок 1.11 – Інтерфейс програмного продукту LogRhythm

1.6 Функції та можливості IBM QRadar

Сучасні кіберзлочинці під час атак систем захисту компаній використовують дедалі витонченіші методи. Щоб протидіяти загрозам, департаменти інформаційної безпеки змушені аналізувати та інтерпретувати величезну кількість подій щодня. Компанія IBM для захисту від загроз мережевої безпеки пропонує рішення IBM QRadar Security Intelligence Platform, яке надає єдину архітектуру для інтеграції інформації про безпеку та управління подіями (SIEM) і журналами, визначення аномальних ситуацій, аналізу інцидентів, реагування на них, управління налаштуваннями та усунення вразливостей.

Єдина архітектура QRadar Security Intelligence Platform дозволяє аналізувати журнали, мережеві потоки, пакети, вразливості, а також дані про користувачів і ресурси. Використання Sense Analytics надає можливість проводити аналіз кореляції для виявлення найбільш серйозних загроз, атак і вразливостей у реальному часі. Це дозволяє ІТ-відділам розставляти пріоритети та виділяти найважливіші інциденти з величезного потоку даних. Рішення автоматично реагує на інциденти і виконує нормативні вимоги завдяки можливостям збору даних, визначення їхньої кореляції

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

та складання звітності. Також передбачено прогнозний аналіз наявних ризиків, викликаних некоректним налаштуванням пристроїв і відомими вразливостями.

IBM QRadar Security Intelligence Platform включає низку різних модулів, серед яких ключовим компонентом є інструмент IBM QRadar SIEM — система збору та аналізу подій. Він консолідує інформацію з журналів подій, що надходять від пристроїв, кінцевих точок і додатків у мережі. QRadar SIEM нормалізує дані та аналізує їх кореляцію для виявлення загроз безпеці, використовуючи передовий механізм Sense Analytics для визначення нормальної поведінки, виявлення аномалій, виявлення складних загроз і усунення хибнопозитивних результатів. Цей програмний модуль дозволяє об'єднувати всі пов'язані події в один інцидент. QRadar SIEM може містити засоби аналізу загроз IBM X-Force Threat Intelligence зі списком потенційно шкідливих IP-адрес, адрес комп'ютерів зі шкідливим ПЗ, джерел спаму та інших загроз, що дає змогу впровадити випереджувальний підхід до забезпечення безпеки. Крім того, для визначення пріоритетів продукт вміє зіставляти загрози для систем з подіями і даними з мережі.

Можливість створювати докладні звіти щодо доступу до даних і дій користувачів забезпечує більш ефективне управління загрозами і відповідність стандартам. Варто також згадати, що QRadar SIEM можна використовувати в локальних і хмарних середовищах.

Крім того, варто зазначити, що найближчим часом IBM планує використовувати платформу штучного інтелекту Watson у сфері безпеки, інтегрувавши її з програмним забезпеченням QRadar і базою даних X-Force. Це дасть змогу підвищити рівень аналітики для визначення характеру загроз, а також компенсувати брак ІТ-персоналу у сфері інформаційної безпеки.

Розглянемо зазначені вище можливості IBM QRadar SIEM більш детально. Забезпечення прозорості в реальному часі дає змогу виявити неправильне використання додатків, внутрішнє шахрайство і невеликі загрози, які можна було б випустити з уваги серед мільйонів подій, що відбуваються щодня. Рішення дає змогу забезпечити збір журналів і подій із різних джерел, включно з пристроями безпеки,

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

операційними системами, застосунками, базами даних і системами керування доступом та ідентифікацією. Дані мережевих потоків надходять від комутаторів і маршрутизаторів, включно з даними рівня 7 (рівень додатків). Передбачено отримання інформації від систем управління доступом та ідентифікацією і таких служб інфраструктури, як протокол динамічного налаштування вузла (DHCP), а також від сканерів вразливості в мережі та додатках.

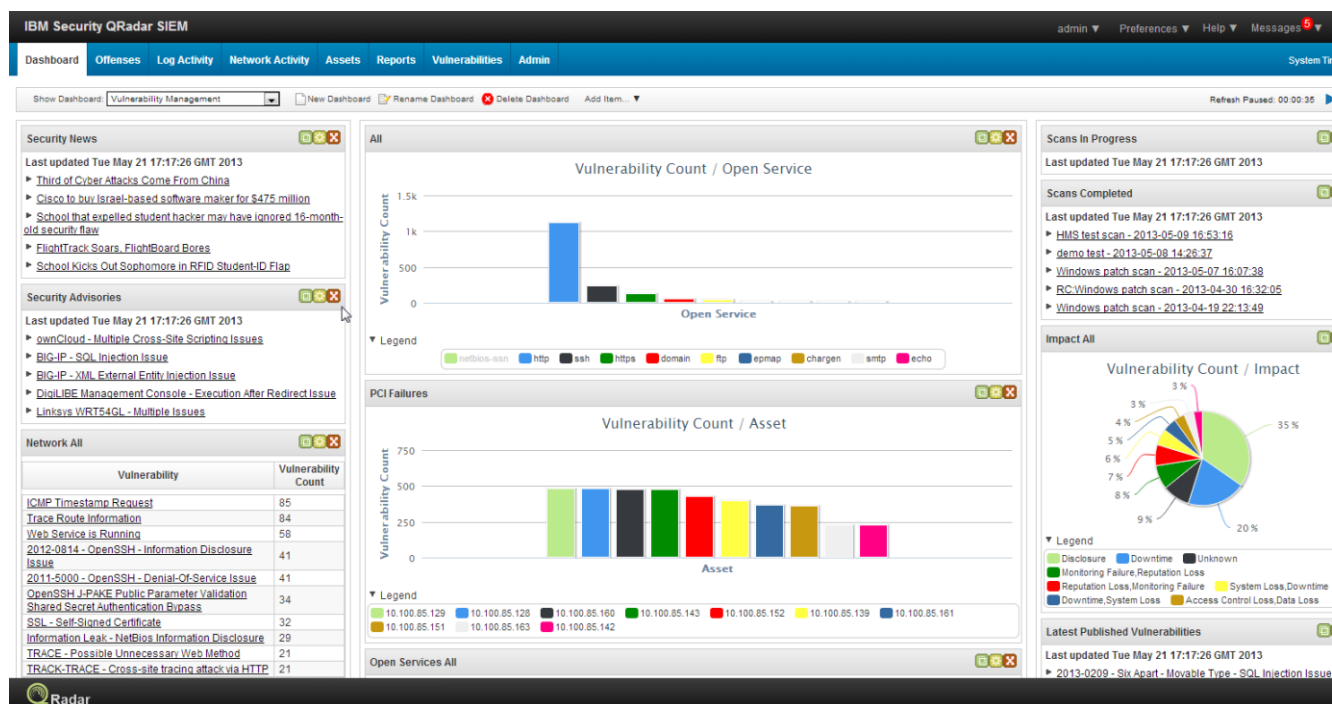


Рисунок 1.12 – Dashboard-панель IBM QRadar Siem

На Dashboard-панель IBM QRadar SIEM можна вивести всі необхідні звіти та графіки.

QRadar SIEM виконує миттєву нормалізацію подій і зіставлення з іншими даними для виявлення загроз і створення нормативних звітів. Рішення визначає пріоритети подій, виділяючи невелику кількість реальних порушень, що несуть найбільш серйозну загрозу для бізнесу. Виявлені аномалії дають можливість виявити зміни в поведінці, пов'язані з додатками, комп'ютерами, користувачами і сегментами мережі. При використанні ПЗ IBM X-Force Threat Intelligence також визначаються дії, пов'язані з підозрілими IP-адресами.

Рішення дає можливість більш ефективно управляти погрозами, відстежуючи серйозні інциденти і надаючи посилання на всі необхідні дані для проведення

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

аналізу. Це дає змогу виявити дії в неробочий час або незвичайне використання застосунків і хмарних сервісів, а також мережеву активність, що не відповідає збереженим шаблонам використання. Для поліпшення аналітики QRadar SIEM підтримує можливість пошуку в подіях і потоках даних у режимі, близькому до реального часу, а також за збереженими даними. Можливе виконання об'єднаного пошуку у великих розподілених середовищах. Для глибшого розуміння і кращого відображення застосунків, баз даних, продуктів для спільної роботи та соціальних мереж можна використовувати пристрої IBM QRadar QFlow і IBM QRadar VFlow Collector, які дають змогу проводити детальний аналіз мережевих потоків на рівні 7.

Можливість установки в хмарі SoftLayer дозволяє QRadar SIEM отримувати оперативну інформацію про безпеку в хмарних середовищах. Причому збір подій і потоків даних від додатків виконується як у хмарі, так і на локальних ресурсах.

Рішення має інтуїтивно зрозумілий модуль звітів, що не вимагає спеціальних баз даних або особливих навичок від ІТ-адміністраторів. Створення звітів про доступ до даних і активності користувачів з можливістю відстеження інформації за ім'ям та ІР-адресою гарантує дотримання політик безпеки, а також відповідність нормативним вимогам.

З інструментом QRadar SIEM інтегрується низка модулів, що підвищують його ефективність. Одним із найважливіших є QRadar Risk Manager, який зіставляє інформацію про вразливості з даними про топологію мережі та з'єднання. Рішення виявляє вразливості в мережі компанії та додатках, що працюють у ній, оцінивши ризики та мінімізувавши їх. Risk Manager відстежує конфігурацію комутаторів, маршрутизаторів, мережевих екранів і систем запобігання вторгнень (IPS), розпізнаючи умови, що становлять загрозу безпеці. Крім того, він дає змогу моделювати мережеві атаки та інші сценарії вторгнень, вносячи до конфігурації мережі зміни, які дають можливість оцінити масштаб загрози.

Ще один цікавий інструмент — модуль QRadar Log Manager. Він збирає і обробляє дані про події в режимі реального часу, які надходять від маршрутизаторів, комутаторів, брандмауерів, мереж VPN, систем виявлення і запобігання вторгнень

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

(IDS/IPS), антивірусних програм та інших джерел. QRadar Log Manager дозволяє спростити ведення необхідної звітності та контроль за дотриманням нормативно-правових вимог.

IBM QRadar SIEM є однією з найбільш ефективних аналітичних систем безпеки. Важливо зазначити, що це рішення підтримує роботу з більш ніж 200 продуктами від провідних виробників, здійснюючи збір, аналіз і кореляцію даних через широкий спектр систем, включаючи мережеві рішення, засоби безпеки, сервери, хости, операційні системи та додатки. Додатковою перевагою цього рішення є невисока вартість системи початкового рівня.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

РОЗДІЛ 2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ SIEM ДЛЯ SOC НА БАЗІ IBM QRADAR

2.1 Проектування мережі

В даній роботі розглянута модель корпоративної мережі, що може бути використана як основа для тестування та демонстрації можливостей SIEM-системи IBM QRadar. Мережа складається з наступних компонентів. Дана мережа спроектована таким чином, щоб її можна було легко розширювати за рахунок додавання нових робочих станцій, серверів та інших пристроїв. Це робить її придатною для тестування SIEM-систем в різних масштабах, від невеликих офісів до великих підприємств.

SIEM-система IBM QRadar здатна аналізувати дані з тисячі робочих станцій, що робить її ідеальним рішенням для організацій будь-якого розміру. Її модульна архітектура дозволяє гнучко розширювати систему відповідно до потреб мережі.

Мережа має просту структуру, що робить її легкою для розуміння, налаштування та розширення за рахунок додавання нових пристроїв. Модель відповідає реальним корпоративним мережам, що робить її придатною для тестування SIEM-систем в умовах, близьких до реальних.

В даній віртуальній корпоративній мережі на віртуальних машинах з Windows Server 2018 буде розгорнуто службу Active Directory (AD).

Active Directory – це служба каталогів, яка використовується для централізованого управління користувачами, комп'ютерами, групами та іншими ресурсами в мережі Windows.

У корпоративній мережі Active Directory (AD) виконує роль централізованої системи управління користувачами, комп'ютерами та ресурсами. Вона здійснює аутентифікацію та авторизацію користувачів, надаючи їм доступ до ресурсів відповідно до їхніх повноважень. AD також використовується для спрощення спільного доступу до файлів, принтерів та інших ресурсів, а також для централізованого налаштування політик безпеки та інших параметрів для всіх комп'ютерів у мережі. Це

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

економить час та ресурси адміністраторів, а також підвищує загальний рівень безпеки та продуктивності мережі.

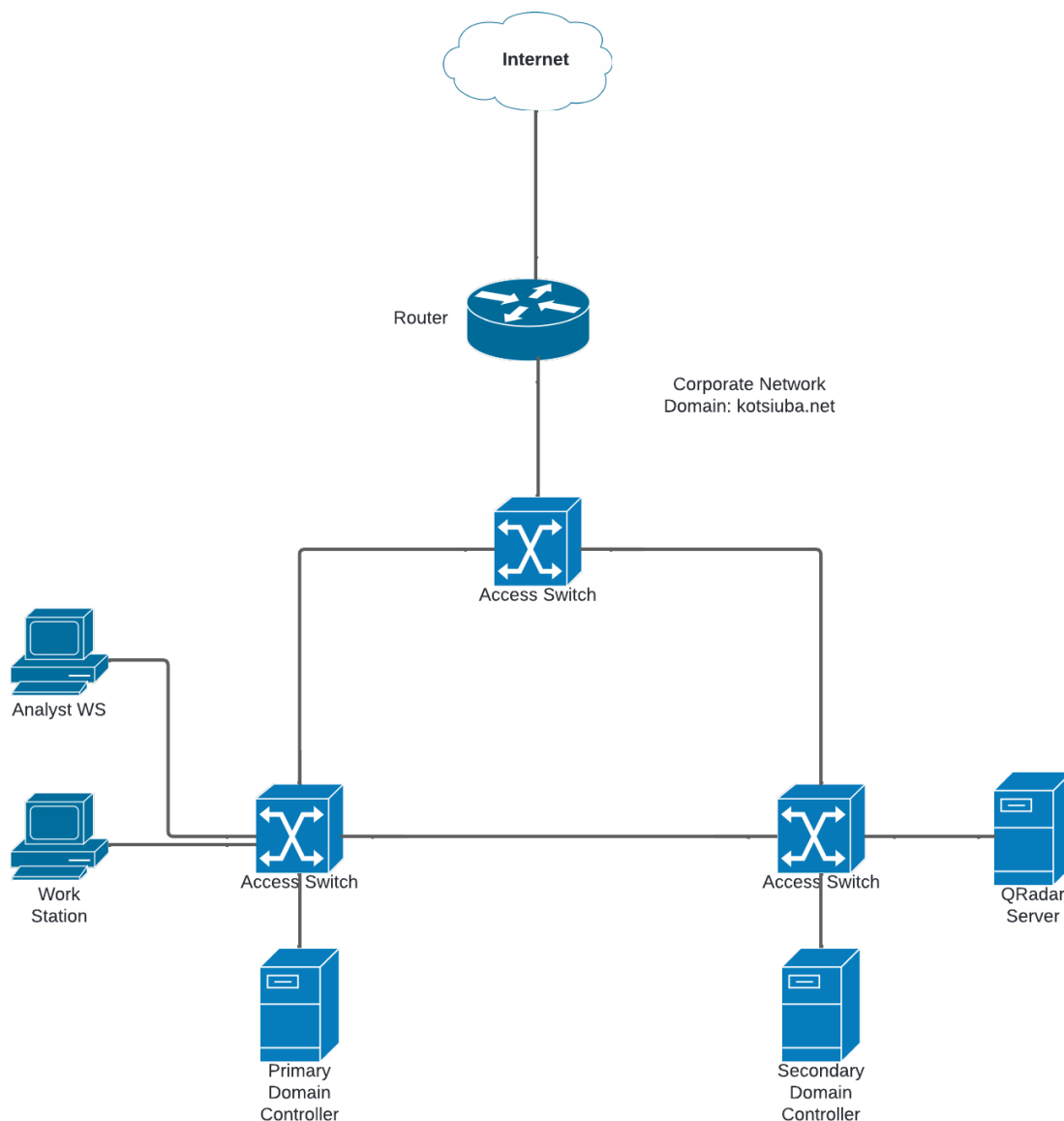


Рисунок 2.1 – Діаграма топології корпоративної мережної інфраструктури

В даній роботі буде описано розгортання віртуальної корпоративної мережі в середовищі GNS3. Мережа буде складатися з маршрутизаторів та комутаторів Cisco, а також віртуальних машин, запущених на VirtualBox.

Компоненти:

- GNS3: Емулятор мережевих пристроїв, який дозволяє створювати та тестувати віртуальні мережі;
- Маршрутизатори Cisco: Віртуальні маршрутизатори Cisco, які будуть використовуватися для з'єднання різних сегментів мережі;

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

- Комутатори Cisco: Віртуальні комутатори Cisco, які будуть використовуватися для з'єднання робочих станцій та серверів в межах одного сегмента мережі;
- VirtualBox: Програмне забезпечення віртуалізації, яке буде використовуватися для запуску віртуальних машин;
- Windows Server 2019 (64-bit): На серверах буде запущено службу каталогів Active Directory для централізованого управління користувачами, комп'ютерами, групами та іншими ресурсами в мережі. Всього буде 2 сервера – основний та дублюючий;
- Робочі станції на Windows 10 (64-bit);
- Сервер IBM QRadar: Буде збирати дані про трафік з маршрутизаторів, комутаторів та інших мережевих пристроїв. Аналізувати дані про трафік, щоб виявити підозрілу активність, яка може свідчити про кіберзагрозу. Повідомляти про підозрілу активність.
- Kali Linux 2024: Буде виступати в ролі зловмисника для проведення атак на мережу щоб перевірити її працездатність і захищеність.

Таблиця 2.1 – Параметри підключення пристроїв

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
SW-Internet	e0/0	Cloud Internet	nat0
	e0/2	Corporate-Router	g0/0
Corporate-Router	g0/0	SW-Internet	e0/2
	e2/0	Switch-Access-1	e2/0
Switch-Access-1	e2/0	Corporate-Router	e2/0
	e0/1	Switch-Access-2	e0/1
	e0/0	Switch-Access-3	e0/0
	e2/2	PDC	e0
	e2/3	SDC	e0

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Switch-Access-2	e0/1	Switch-Access-1	e0/1
	e0/2	Switch-Access-3	e0/2
	e2/0	AnalystWS	e0
	e2/1	Kali-Linux	e0
Switch-Access-3	e0/0	Switch-Access-1	e0/0
	e0/1	WS-1	e0
	e0/2	Switch-Access-2	e0/2
	e2/0	QRadar	e0
PDC	e0	Switch-Access-1	e2/2
SDC	e0		e2/3
AnalystWS	e0	Switch-Access-2	e2/0
Kali-Linux	e0		e2/1
QRadar	e0	Switch-Access-3	e2/0
WS-1	e0		e0/1

Таблиця 2.2 – Параметри IP-адресації мережі

Мережа / Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска
Підмережа kotsiuba.net	-	10.0.0.0	255.255.255.0
Маршрутизатор Corporate-Router	g0/0	DHCP	
	e2/0	10.0.0.1	255.255.255.0
Комутатор Switch-Access-1	Інтерфейс Vlan 1	10.0.0.11	255.255.255.0
	Шлюз за замовч.	10.0.0.1	-
Комутатор Switch-Access-2	Інтерфейс Vlan 1	10.0.0.12	255.255.255.0
	Шлюз за замовч.	10.0.0.1	-

Мережа / Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска
Комутатор Switch-Access-3	Інтерфейс Vlan 1	10.0.0.13	255.255.255.0
	Шлюз за замовч.	10.0.0.1	-
Сервер QRadar	Мережний адаптер	10.0.0.4	255.255.255.0
	Шлюз за замовч.	10.0.0.1	-
Primary Domain Controller	Мережний адаптер	10.0.0.2	255.255.255.0
	Шлюз за замовч.	10.0.0.1	-
Secondary Domain Controller	Мережний адаптер	10.0.0.3	255.255.255.0
	Шлюз за замовч.	10.0.0.1	-
Робоча станція AnalystWS	Мережний адаптер	DHCP	
	Шлюз за замовч.		
Робоча станція WS-1	Мережний адаптер		
	Шлюз за замовч.		
Робоча станція Kali-Linux	Мережний адаптер		
	Шлюз за замовч.		

В мережі планується розгортання двох контролерів доменів - одного основного та іншого додаткового (бекапного). Це дозволить забезпечити високу доступність та надійність служби Active Directory, забезпечуючи коректну роботу інфраструктури підприємства.

На цих контролерах доменів будуть розгорнуті всі необхідні служби, що забезпечать нормальну роботу Active Directory. Це включає служби аутентифікації, авторизації, управління груповими політиками, реплікацію даних та інші функції, які дозволяють забезпечити цілісність та безпеку домену.

Крім цього, планується налаштування групових політик (Group Policies), що дозволить нам одночасно управляти налаштуваннями безпеки, прав доступу, настройками робочого середовища та іншими параметрами для всіх комп'ютерів та

користувачів в домені kotsiuba.net. Це значно спростить адміністрування та дозволить однорідно налаштовувати і керувати всіма пристроями в мережі.

Також передбачено встановлення служб WinCollect на контролері доменів (DC) для збору даних в рамках інтеграції з системою моніторингу та аналізу подій IBM QRadar.

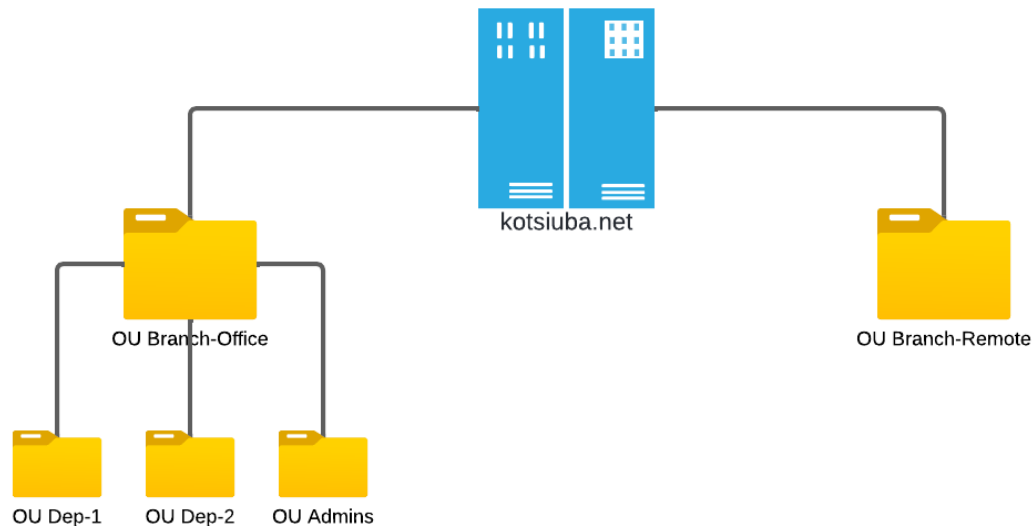


Рисунок 2.2 – Структура домену kotsiuba.net

Домен kotsiuba.net наразі включає дві організаційні одиниці (OU) під назвою Branch-Office, яка містить в собі додаткові OU: Admins та два умовних департаменти. OU Remote-Branch, яка буде використовуватися для забезпечення віддаленого доступу до мережі.

Ця структура дозволить ефективно організувати та управляти об'єктами в Active Directory відповідно до потреб організації. Відокремлення окремих груп користувачів та ресурсів у відділеннях Branch-Office та Remote-Branch сприятиме полегшенню керування правами доступу, настройкою групових політик та забезпечить безпеку мережі від внутрішніх та зовнішніх загроз.

Для забезпечення віддаленого доступу до мережі буде налаштована служба Remote Desktop Services (RDS) в Active Directory. Ця служба дозволяє користувачам віддалено підключатися до комп'ютерів та віртуальних робочих станцій через протокол Remote Desktop Protocol (RDP), отримуючи доступ до додатків та ресурсів мережі з будь-якої точки з'єднання. Налаштування RDS дозволить керувати

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

доступом, забезпечити безпеку передачі даних та забезпечити комфортні умови роботи для віддалених користувачів.

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.

AD - це як телефонна книга для IT-інфраструктури та користувачів. Він надає командам централізовані служби автентифікації та авторизації, призначені для комп'ютерів на базі Windows. AD призначена для перевірки того, чи має хтось правильні облікові дані (автентифікація), і визначає, до яких файлів або додатків він може отримати доступ на основі своєї ролі або членства в групі (авторизація).

Простіше кажучи, AD пропонує такі ключові функції та компоненти, як керування груповими політиками, доменні служби та підтримку полегшеного протоколу доступу до каталогів (LDAP).

Як основна служба каталогів у домені Windows, Active Directory Domain Services (AD DS) відповідає за зберігання та керування інформацією про користувачів, служби та пристрої, підключені до мережі в багаторівневій структурі. По суті, це основа Active Directory, оскільки вона містить централізований каталог, який дозволяє доменам і користувачам взаємодіяти.

AD DS допомагає керувати мережевими операціями, забезпечуючи структурований спосіб зберігання даних в ієрархічній організації. Це полегшує адміністраторам керування правами доступу користувачів і конфігураціями системи в різних доменах однієї мережі. AD DS також інтегрує безпеку шляхом аутентифікації функцій входу та контролю доступу до ресурсів каталогів. Це досягається за допомогою:

- **Автентифікація користувачів.** AD DS автентифікує користувачів, перш ніж вони зможуть отримати доступ до ресурсів у мережі, гарантуючи, що тільки авторизовані особи мають доступ до певних частин системи.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

- **Зберігання даних.** Зберігає дані каталогів, такі як імена користувачів, паролі та номери телефонів, які допомагають впорядкувати роботу в організації.

- **Застосування політик.** За допомогою об'єктів групової політики (GPO) адміністратори можуть застосовувати політики безпеки на декількох машинах одночасно, заощаджуючи час і зберігаючи високий рівень безпеки.

Active Directory пропонує функції безпеки, такі як списки контролю доступу (ACL), шифрування та можливості аудиту для захисту конфіденційних даних і ресурсів. Всі ці функції важливо використовувати. Але комплексний і постійний захист Active Directory передбачає багато інших кроків і стратегій.

Зловмисники прагнуть скомпрометувати облікові записи адміністраторів доменів, пов'язані з вашим AD. Це пов'язано з тим, що ці користувачі Active Directory мають високі привілеї з адміністративним контролем і повноваженнями над цілим доменом у «лісі» AD. (Ліс - це сукупність одного або декількох дерев доменів у службовому каталозі).

Одна з порад щодо захисту облікових записів адміністраторів домену - перейменувати їх зі стандартного «адміністратор» на щось більш креативне (і складніше для вгадування). Тут може допомогти впровадження надійних політик паролів і використання парольних фраз. Ще одна хороша практика - вимагати MFA для автентифікації адміністраторів доменів.

Уповноважений персонал - це єдині користувачі, які повинні мати адміністративний доступ в AD. А ті, хто має привілеї адміністратора домену, не повинні використовувати ці облікові записи для повсякденних завдань. Для цього їм слід використовувати більш типові облікові записи рівня користувача. Супутні заходи щодо обмеження доступу до Active Directory, які також можуть допомогти знизити ризик внутрішніх загроз, включають:

- Впровадження принципу найменших привілеїв (PoLP) для надання користувачам тільки тих дозволів, які необхідні їм для виконання своєї роботи - і не більше.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

- Використання контролю доступу на основі ролей (RBAC) для обмеження доступу користувачів до певних завдань або систем.
- Регулярний аудит адміністративних облікових записів.

2.2 Аналіз рішення QRadar та програмного забезпечення WinCollect

Варто зазначити систему QRadar, що є потужним засобом моніторингу та аналізу подій в мережах. QRadar відкриває широкі можливості для інтеграції з різноманітними системами, дозволяючи створювати комплексні рішення для забезпечення безпеки та ефективного моніторингу.

Одним із ключових аспектів інтеграції QRadar є використання WinCollect для збору даних з Windows-серверів та робочих станцій. WinCollect - це агент, який встановлюється на Windows-системах та забезпечує збір і передачу журнальних даних з цих систем до QRadar для подальшого аналізу та моніторингу.

Інтеграція QRadar з Active Directory є дуже важливим етапом для забезпечення безпеки та ефективності в мережі. Завдяки цій інтеграції, QRadar отримує доступ до журнальних даних та подій, пов'язаних з автентифікацією, авторизацією та управлінням доступом в AD. Це дозволяє вчасно виявляти та реагувати на потенційні загрози, спрощує аудит та відповідає вимогам безпеки.

Інтеграція QRadar з Active Directory через WinCollect створює потужний механізм для моніторингу та захисту мережі, допомагаючи виявляти аномальні активності, забезпечувати безпеку даних та знижувати ризики для організації.

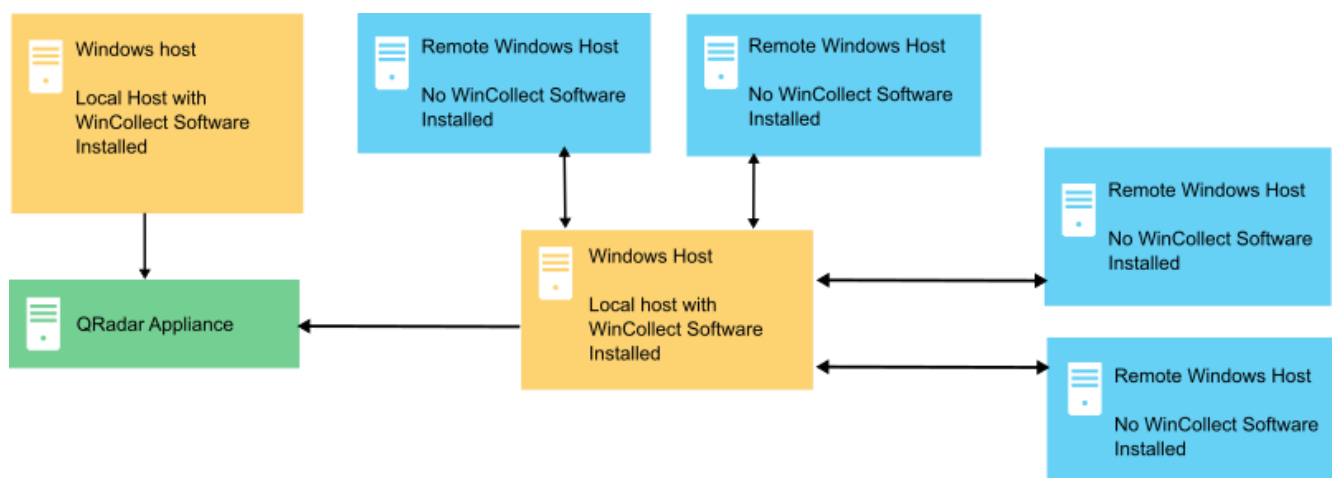


Рисунок 2.3 – Автономне розгортання WinCollect

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

2.3 Аналіз NetFlow у контексті SIEM-рішень

NetFlow - це мережевий протокол, розроблений компанією Cisco для збору інформації про IP-трафік і моніторингу мережевого потоку. Аналізуючи дані NetFlow, можна отримати картину потоку та обсягу мережевого трафіку.

NetFlow - це одностороння технологія, тому коли сервер відповідає на початковий запит клієнта, процес працює в зворотному напрямку і створює новий запис потоку. Використання рішення для моніторингу NetFlow може дозволити вам більш ефективно відстежувати і аналізувати ці записи потоку і ефективно управляти трафіком в мережі.

Інтеграція NetFlow з QRadar відкриє нові можливості для розуміння трафіку у мережі та виявлення потенційних загроз безпеці. Цей процес передбачає увімкнення та конфігурування NetFlow на маршрутизаторі Cisco, а також налаштування QRadar для прийому та аналізу цих даних.

Ця інтеграція дозволить компанії ефективно відслідковувати та реагувати на незвичайну активність у мережі, забезпечуючи високий рівень безпеки та забезпечуючи вчасні заходи протидії потенційним загрозам. Детальна аналітика трафіку з NetFlow у поєднанні з моніторингом QRadar допоможе управляти мережею ефективно та безпечно.

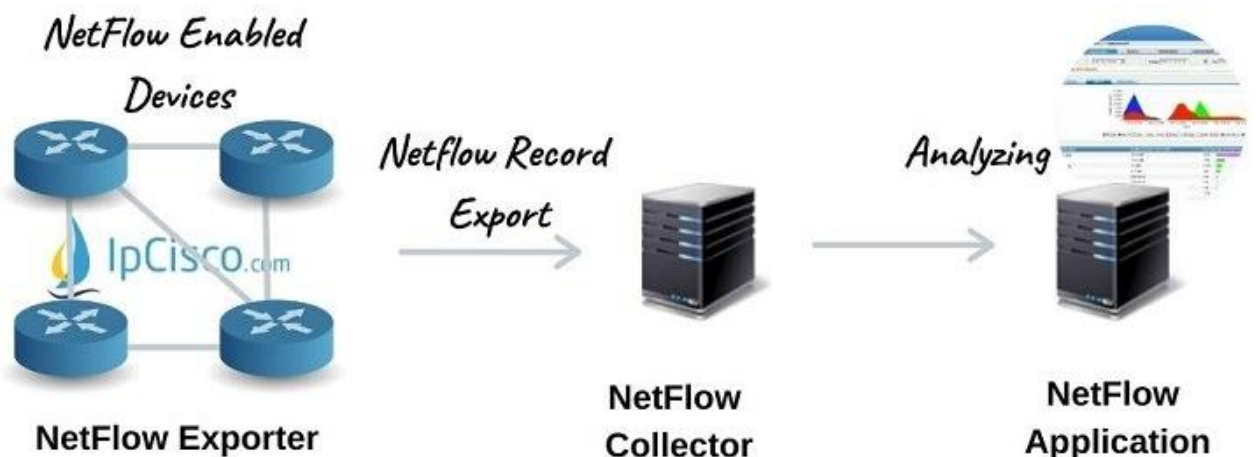


Рисунок 2.4 – Принцип роботи NetFlow

В корпоративній мережі головний маршрутизатор виступає в ролі NetFlow Exporter. Це означає, що він буде збирати та відправляти дані про мережевий

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

трафік. У свою чергу, QRadar виконує функції NetFlow Collector, отримуючи ці дані для подальшого аналізу та зберігання.

Центральна консоль QRadar використовується як NetFlow Application, забезпечуючи централізоване управління, моніторинг та аналіз зібраної інформації. Завдяки цій архітектурі можна ефективно відстежувати мережеву активність, виявляти аномалії та потенційні загрози, а також забезпечувати високий рівень безпеки мережевої інфраструктури.

Таблиця 2.3 – Версії Cisco NetFlow

Версія	Опис
v1	Вперше реалізована компанією Cisco і обмежена IPv4. Ця версія зараз застаріла.
v2	Внутрішня версія - ніколи не була публічно випущена.
v3	Внутрішня версія - ніколи не була публічно випущена.
v4	Внутрішня версія - ніколи не випускалася публічно.
v5	Це найпоширеніша версія, доступна на більшості марок маршрутизаторів.
v6	Більше не підтримується компанією Cisco.
v7	Подібна до версії 5, з вихідним маршрутизатором і доданою підтримкою комутаторів-каталізаторів Cisco. Ця версія зараз застаріла.
v8	Підтримувала різні схеми агрегації на основі маршрутизаторів. Ця версія застаріла.
v9	Ця версія заснована на шаблонах і здебільшого використовується для підтримки IPv6, MLPS і IPv4 з потоками BGP nexthop.
v10	Використовується для визначення IPFIX.

За замовчуванням більшість версій Cisco IOS після 12.0 підтримують NetFlow v9. Враховуючи це, для налаштування моніторингу трафіку в нашій мережі буде використовуватися саме ця версія NetFlow.

РОЗДІЛ 3 НАЛАШТУВАННЯ, РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПІДСИС- ТЕМИ SIEM НА БАЗІ IBM QRADAR

3.1 Налаштування мережі

Налаштування маршрутизатора передбачає кілька етапів. Почнемо з присвоєння статичної IP-адреси порту Eth2/0. Це можна зробити, увійшовши до конфігураційного режиму маршрутизатора і встановивши інтерфейс Eth2/0 в режим налаштування, а потім вказавши статичну IP-адресу разом з маскою підмережі для цього порту.

Далі, для забезпечення коректної роботи DHCP сервера, варто виключити присвоєну IP-адресу з DHCP пулу. Це можна зробити у конфігураційному режимі DHCP сервера, використовуючи відповідну команду для видалення цієї адреси з пулу DHCP.

Нарешті, для створення нового DHCP пулу з адресою 10.0.0.0 та маскою підмережі 255.255.255.0, слід також звернутися до конфігураційного режиму DHCP сервера. Там необхідно створити новий DHCP пул, вказавши необхідні параметри, такі як адреса мережі, маска підмережі, адреса шлюзу за замовчуванням, DNS сервери та інші параметри, які визначають роботу DHCP сервера на мережі.

```
Corporate-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Corporate-Router(config)#hostname Corporate-Router
Corporate-Router(config)#banner motd #Powered by Dmytro Kotsiuba#
Corporate-Router(config)#int eth2/0
Corporate-Router(config-if)#ip address 10.0.0.1 255.255.255.0
Corporate-Router(config-if)#no sh
Corporate-Router(config-if)#exit
Corporate-Router(config)#
*May 20 12:02:38.611: %LINK-3-UPDOWN: Interface Ethernet2/0, changed state to up
*May 20 12:02:39.611: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/
0, changed state to up
Corporate-Router(config)#ip dhcp excluded-address 10.0.0.1
Corporate-Router(config)#ip dhcp pool corporateNetwork
Corporate-Router(dhcp-config)#network 10.0.0.0 255.255.255.0
Corporate-Router(dhcp-config)#default-router 10.0.0.1
Corporate-Router(dhcp-config)#dns-server 8.8.8.8
Corporate-Router(dhcp-config)#exit
Corporate-Router(config)#
```

Рисунок 3.1 – Сценарій налагодження маршрутизатора Corporate-Router

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

У віртуальному середовищі GNS3, підключення до хмари (Cloud) емулює зовнішню мережу, як інтернет. Таке підключення використовує протоколи, такі як DHCP, для автоматичного отримання IP-адреси та інших мережевих параметрів.

```
Corporate-Router(config)#int gig0/0
Corporate-Router(config-if)#ip address dhcp
Corporate-Router(config-if)#no sh
Corporate-Router(config-if)#ex
*May 20 12:04:23.675: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*May 20 12:04:24.675: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Corporate-Router(config-if)#ex
Corporate-Router(config)#
```

Рисунок 3.2 – Сценарій налагодження підключення до інтернету

```
Corporate-Router(config)#ip domain-lookup
Corporate-Router(config)#ip name-server 8.8.8.8
Corporate-Router(config)#
```

Рисунок 3.3 – Сценарій налагодження автоматичного переводу доменних імен в IP-адреси та встановлення DNS сервера за замовчуванням

Налаштування протоколу маршрутизації OSPF (Open Shortest Path First) у мережі. Це дозволить оптимізувати маршрутизацію, забезпечити швидке виявлення найкращих маршрутів та автоматичне оновлення маршрутних таблиць. OSPF є динамічним протоколом маршрутизації, що розподіляє навантаження між різними шляхами та забезпечує стабільну роботу мережі. Налаштування OSPF передбачає визначення зон, призначення мережевих інтерфейсів до цих зон, встановлення маски підмережі, а також вибір основного маршрутизатора для кожної зони. В цілому, це спростить управління маршрутизацією та зробить мережу більш ефективною та надійною.

```
Corporate-Router(config)#router ospf 1
Corporate-Router(config-router)#network 10.0.0.0 0.0.0.255 area 0
Corporate-Router(config-router)#default-information originate
Corporate-Router(config-router)#ex
Corporate-Router(config)#
```

Рисунок 3.4 – Сценарій налагодження протоколу маршрутизації OSPF

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

Процес налагодження протоколу Network Address Translation (NAT) включає налаштування access-list для визначення правил перетворення IP-адрес та портів. Буде налагоджено правила NAT для ефективного управління мережевим трафіком, що дозволить забезпечити безпеку та оптимізацію мережі. Налаштовані правила NAT будуть керувати перетворенням адрес та портів для забезпечення конфіденційності та цілісності даних, а також для забезпечення доступу до ресурсів мережі зовнішнім користувачам за допомогою публічних IP-адрес. Ця настройка необхідна для забезпечення доступу до Інтернету в пристроях мережі.

```
Corporate-Router(config)#int gig0/0
Corporate-Router(config-if)#ip nat outside
Corporate-Router(config-if)#
*May 20 12:07:20.331: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
Corporate-Router(config-if)#int eth2/0
Corporate-Router(config-if)#ip nat inside
Corporate-Router(config-if)#ex
Corporate-Router(config)#$de source list 1 interface gig0/0 overload

Corporate-Router(config)#access-list 1 permit 10.0.0.0 0.0.0.255
Corporate-Router(config)#exit
Corporate-Router#
*May 20 12:08:39.971: %SYS-5-CONFIG_I: Configured from console by console
Corporate-Router#
```

Рисунок 3.5 – Процес налагодження протоколу NAT

```
C:\Users\admin>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a807:d58a:86a4:b369%5
    IPv4 Address. . . . . : 10.0.0.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

C:\Users\admin>ping google.com

Pinging google.com [172.217.16.14] with 32 bytes of data:
Reply from 172.217.16.14: bytes=32 time=30ms TTL=114
Reply from 172.217.16.14: bytes=32 time=23ms TTL=114
Reply from 172.217.16.14: bytes=32 time=28ms TTL=114
Reply from 172.217.16.14: bytes=32 time=30ms TTL=114

Ping statistics for 172.217.16.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 30ms, Average = 27ms
```

Рисунок 3.6 – Перевірка працездатності мережі шляхом виконання команди **ping google.com** на одній із робочих станцій

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

```
Corporate-Router#show ip dhcp pool

Pool corporateNetwork :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 1
  Pending event                    : none
  1 subnet is currently in the pool :
  Current index      IP address range      Leased addresses
  10.0.0.6           10.0.0.1             - 10.0.0.254      1
Corporate-Router#
```

Рисунок 3.7 – Відображення конфігураційних параметрів DHCP пулу

```
Corporate-Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 192.168.122.98:18473 10.0.0.5:18473 142.250.186.206:18473 142.250.186.206:18473
icmp 192.168.122.98:18985 10.0.0.5:18985 142.250.186.206:18985 142.250.186.206:18985
icmp 192.168.122.98:19241 10.0.0.5:19241 142.250.186.206:19241 142.250.186.206:19241
icmp 192.168.122.98:19497 10.0.0.5:19497 142.250.186.206:19497 142.250.186.206:19497
icmp 192.168.122.98:19753 10.0.0.5:19753 142.250.186.206:19753 142.250.186.206:19753
udp 192.168.122.98:23519 10.0.0.5:23519 8.8.8.8:53           8.8.8.8:53
Corporate-Router#
```

Рисунок 3.8 – Відображення таблиці перекладу адрес

```
Corporate-Router#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 6, occurred 00:01:22 ago
Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  Ethernet2/0
Hits: 12 Misses: 0
CEF Translated packets: 10, CEF Punted packets: 2
Expired translations: 6
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface GigabitEthernet0/0 refcount 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
Corporate-Router#
```

Рисунок 3.9 – Відображення статистики про роботу NAT

Процес налагодження віддаленого доступу до маршрутизатора та комутаторів на базі протоколу Secure Shell (SSHv2) включатиме створення відповідних користувачських облікових записів з відповідними правами доступу, генерацію ключів для шифрування та автентифікації, а також активацію сервісу SSH на обладнанні. Цей процес забезпечить безпечний та зашифрований доступ до мережного обладнання для адміністраторів мережі та інших уповноважених користувачів.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Також буде налагоджено протокол Network Time Protocol (NTP) з використанням реального сервера за адресою 0.ua.pool.ntp.org для синхронізації часу на маршрутизаторі та комутаторах. Ця настройка дозволить забезпечити точність часу в мережі, що є важливим аспектом для правильної роботи різноманітних мережевих процесів та служб.

```
Corporate-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Corporate-Router(config)#ip domain-name kotsiuba.net
Corporate-Router(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: Corporate-Router.kotsiuba.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Corporate-Router(config)#
*Jun  5 12:16:51.883: %SSH-5-ENABLED: SSH 2.0 has been enabled
Corporate-Router(config)#ip ssh version 2
Corporate-Router(config)#line vty 0 4
Corporate-Router(config-line)#logging synchronous
Corporate-Router(config-line)#login local
Corporate-Router(config-line)#exec-timeout 20
Corporate-Router(config-line)#transport input ssh
Corporate-Router(config-line)#exit
Corporate-Router(config)#username admin privilege 15 secret T8xsR@dK
```

Рисунок 3.10 – Сценарій налагодження віддаленого доступу

```
Corporate-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Corporate-Router(config)#ntp server 0.ua.pool.ntp.org
Translating "0.ua.pool.ntp.org"...domain server (8.8.8.8) [OK]

Corporate-Router(config)#clock timezone EET +2
Corporate-Router(config)#
*Jun  5 12:20:28.083: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:
20:28 UTC Wed Jun 5 2024 to 14:20:28 EET Wed Jun 5 2024, configured from console
by console.
Corporate-Router(config)#clock summer-time EEST recurring
Corporate-Router(config)#
*Jun  5 12:20:59.867: %SYS-6-CLOCKUPDATE: System clock has been updated from 14:20:59 EET Wed Jun 5 2024 to 15:20:5
9 EEST Wed Jun 5 2024, configured from console by console.
Corporate-Router(config)#
```

Рисунок 3.11 – Процес налагодження протоколу мережного часу

На комутаторах рівня доступу також налаштовано IP-адресацію, протокол мережного часу NTP та протокол віддаленого доступу на базі SSHv2.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

```

Switch-Access-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-Access-1(config)#hostname Switch-Access-1
Switch-Access-1(config)#username admin privilege 15 secret T8xsR@dK
Switch-Access-1(config)#int vlan 1
Switch-Access-1(config-if)#ip address 10.0.0.11 255.255.255.0
Switch-Access-1(config-if)#ntp broadcast client
Switch-Access-1(config-if)#exit
Switch-Access-1(config)#ip default-gateway 10.0.0.1
Switch-Access-1(config)#ip domain-name kotsiuba.net
Switch-Access-1(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
Switch-Access-1(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: Switch-Access-1.kotsiuba.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

Switch-Access-1(config)#
*May 22 14:14:23.471: %SSH-5-ENABLED: SSH 2.0 has been enabled
Switch-Access-1(config)#line vty 0 4
Switch-Access-1(config-line)#logging synchronous
Switch-Access-1(config-line)#login local
Switch-Access-1(config-line)#exec-timeout 20
Switch-Access-1(config-line)#transport input ssh
Switch-Access-1(config-line)#exit
Switch-Access-1(config)#ntp server 10.0.0.1
Switch-Access-1(config)#clock timezone EET +2
Switch-Access-1(config)#
*May 22 14:15:12.262: %SYS-6-CLOCKUPDATE: System clock has been updated from 14:
15:12 UTC Wed May 22 2024 to 16:15:12 EET Wed May 22 2024, configured from conso
le by console.
Switch-Access-1(config)#clock summer-time EEST recurring
Switch-Access-1(config)#
*May 22 14:15:39.367: %SYS-6-CLOCKUPDATE: System clock has been updated from 16:
15:39 EET Wed May 22 2024 to 17:15:39 EEST Wed May 22 2024, configured from cons
ole by console.

```

Рисунок 3.12 – Сценарій базового налагодження комутатора Switch-Access-1

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

```

Switch-Access-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-Access-2(config)#hostname Switch-Access-2
Switch-Access-2(config)#username admin privilege 15 secret T8xsR@dK
Switch-Access-2(config)#int vlan 1
Switch-Access-2(config-if)#ip address 10.0.0.12 255.255.255.0
Switch-Access-2(config-if)#ntp broadcast client
Switch-Access-2(config-if)#exit
Switch-Access-2(config)#ip default-gateway 10.0.0.1
Switch-Access-2(config)#ip domain-name kotsiuba.net
Switch-Access-2(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
Switch-Access-2(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: Switch-Access-2.kotsiuba.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

Switch-Access-2(config)#
*May 22 14:19:12.121: %SSH-5-ENABLED: SSH 2.0 has been enabled
Switch-Access-2(config)#line vty 0 4
Switch-Access-2(config-line)#logging synchronous
Switch-Access-2(config-line)#login local
Switch-Access-2(config-line)#exec-timeout 20
Switch-Access-2(config-line)#transport input ssh
Switch-Access-2(config-line)#exit
Switch-Access-2(config)#ntp server 10.0.0.1
Switch-Access-2(config)#clock timezone EET +2
Switch-Access-2(config)#
*May 22 14:19:58.557: %SYS-6-CLOCKUPDATE: System clock has been updated from 14:19:58 UTC Wed May 22 2024 to 16:19:58
EET Wed May 22 2024, configured from console by console.
Switch-Access-2(config)#clock summer-time EEST recurring
Switch-Access-2(config)#
*May 22 14:20:15.645: %SYS-6-CLOCKUPDATE: System clock has been updated from 16:20:15 EET Wed May 22 2024 to 17:20:15
EEST Wed May 22 2024, configured from console by console.
Switch-Access-2(config)#do write
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1690 bytes to 1052 bytes[OK]
Switch-Access-2(config)#exit
Switch-Access-2#copy tun
*May 22 14:20:23.469: %SYS-5-CONFIG_I: Configured from console by console
Switch-Access-2#copy run
Switch-Access-2#copy running-config start
Switch-Access-2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 1690 bytes to 1051 bytes[OK]
Switch-Access-2#

```

Рисунок 3.13 – Сценарій базового налагодження комутатора Switch-Access-2

```

Corporate-Router#show ntp associations

address          ref clock        st   when   poll reach  delay offset  disp
~37.53.87.250    17.253.14.125    2    25     64      1  0.000 -107974 7937.5
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Corporate-Router#show clock detail
*15:46:11.107 EEST Wed Jun 5 2024
Time source is NTP
Summer time starts 02:00:00 EET Sun Mar 10 2024
Summer time ends 02:00:00 EEST Sun Nov 3 2024

```

Рисунок 3.14 – Список серверів NTP, з якими маршрутизатор синхронізується та детальна інформація про поточний час

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

```
Switch-Access-1#show ntp associations
```

```

address      ref clock      st  when  poll reach  delay  offset  disp
~10.0.0.1    .INIT.         16   148   512    0  0.000  0.000 15937.
* sys.peer, # selected, + candidate, - outlier, x falseticker, ~ configured
Switch-Access-1#show clock detail
*12:50:28.599 EEST Wed Jun 5 2024
Time source is NTP
Summer time starts 02:00:00 EET Sun Mar 10 2024
Summer time ends 02:00:00 EEST Sun Nov 3 2024

```

Рисунок 3.15 – Список серверів NTP, з якими комутатор синхронізується та детальна інформація про поточний час

3.2 Налаштування служби каталогів Active Directory

Наступним кроком налаштування є розгортання двох контролерів домену. Це включає розгортання служби каталогів Active Directory, створення домену, організаційних одиниць (OU) та користувачів, а також створення DNS-записів.

Першим етапом є інсталяція та налаштування двох контролерів домену. Це забезпечить надійність та відмовостійкість нашої інфраструктури, оскільки в разі виходу з ладу одного з контролерів, інший зможе продовжувати виконувати функції контролю доступу.

Далі ми розгорнемо службу каталогів Active Directory, яка дозволить централізовано керувати користувачами, комп'ютерами та іншими ресурсами в мережі. Active Directory забезпечить єдину точку автентифікації та авторизації для всіх користувачів та пристроїв в нашій мережі.

Наступним кроком буде створення домену, який стане основою нашої мережевої інфраструктури. Після створення домену, ми налаштуємо організаційні одиниці (OU) для логічної структуризації наших ресурсів. Це допоможе ефективно керувати правами доступу та політиками безпеки.

Крім того, будуть створені користувачі та групи користувачів в Active Directory. Це дозволить забезпечити контрольований доступ до мережевих ресурсів та спростить управління користувацькими обліковими записами.

Завершальним етапом є створення DNS-записів, які забезпечать правильне функціонування нашої мережі. DNS-записи дозволять користувачам і пристроям в мережі швидко знаходити необхідні ресурси та служби.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

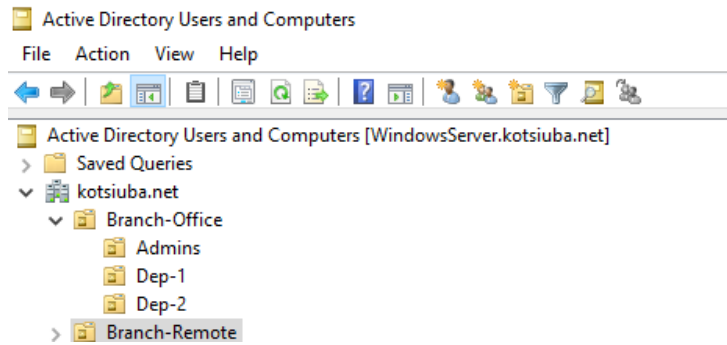


Рисунок 3.16 – Структура домену

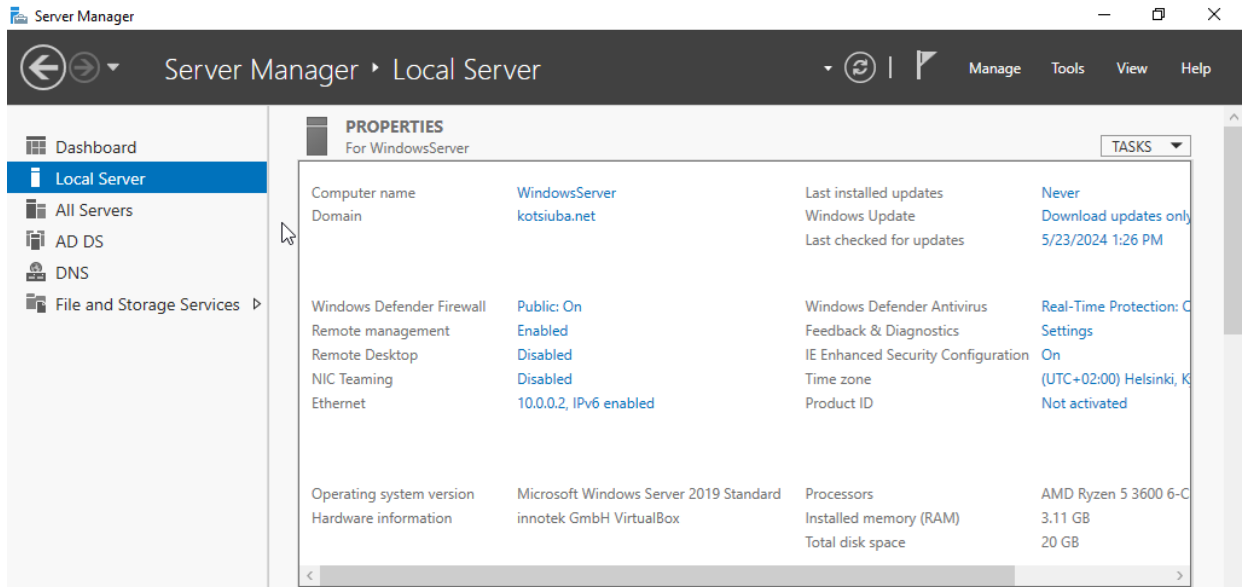


Рисунок 3.17 – Інформація про Windows Server (PDC)

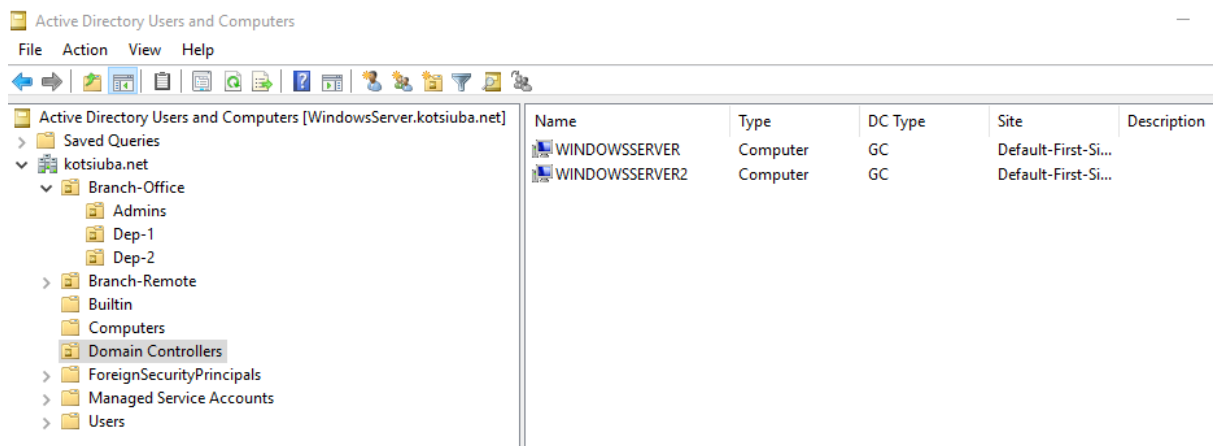


Рисунок 3.18 – Контролери домену

DNS Manager

File Action View Help

Рисунок 3.19 – DNS записи на PDC

3.3 Налаштування серверу QRadar та встановлення програмного забезпечення WinCollect

Нижче показано кроки розгортання серверу QRadar для забезпечення комплексного моніторингу та аналізу мережевих подій. Це рішення дозволить підвищити рівень безпеки мережі, виявляти потенційні загрози та ефективно реагувати на інциденти.

На сервер QRadar буде встановлено розширення WinCollect, яке є ключовим компонентом для збору журналів подій з Windows-систем. Це розширення дозволить централізовано збирати та аналізувати журнальні дані з різних джерел, включаючи контролери домену, робочі станції та інші критичні системи.

Для забезпечення максимальної ефективності та точності моніторингу програмне забезпечення WinCollect буде встановлено на Primary Domain Controller. Це дозволить отримувати доступ до важливих подій аутентифікації, авторизації та управління доступом, що є критично важливим для безпеки мережі.

```
root@localhost: /media/cdrom/post/dsmrpms
You have new mail in /var/spool/mail/root
[root@localhost ~]# sudo mount -o loop /opt/ibm/cloud/iso/QRadarCE2019_14_0_20191031163225.GA.iso /media/cdrom/
mount: /dev/loop2 is write-protected, mounting read-only
[root@localhost ~]# cd /media/cdrom/post/dsmrpms
You have new mail in /var/spool/mail/root
[root@localhost dsmrpms]#
```

Рисунок 3.20 – Процес встановлення QRadar

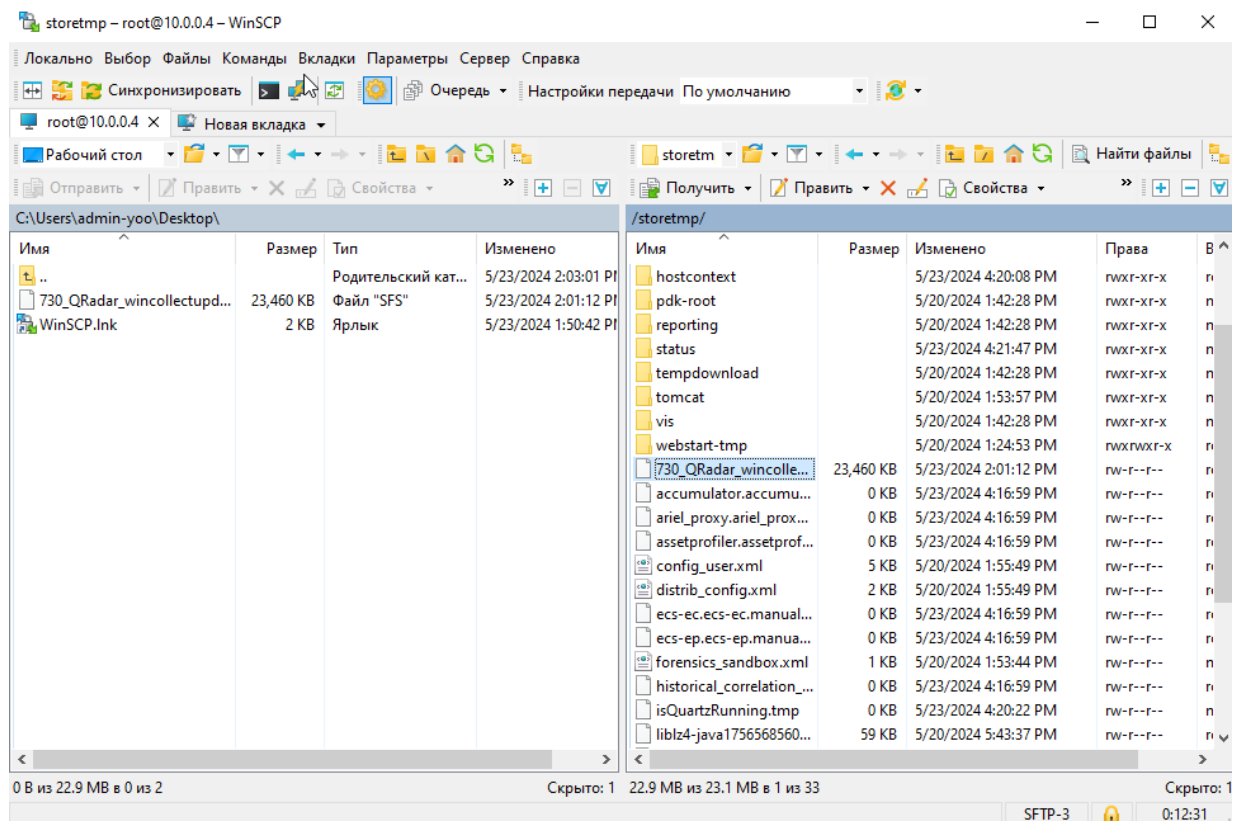


Рисунок 3.21 – Завантаження файлу на сервер QRadar для встановлення розширення WinCollect

```
root@localhost:/media/updates#  
[root@localhost dsmrps]# cd /storetmp/  
[root@localhost storetmp]# ls *.sfs  
730_QRadar_wincollectupdate-7.3.1-22.sfs  
[root@localhost storetmp]# mount -t squashfs -o loop 730_QRadar_wincollectupdate-7.3.1-22.sfs /media/updates/  
[root@localhost storetmp]# cd /media/updates/  
[root@localhost updates]# ls  
Deployment.pm      installer      onstart.d      patch.properties  repo            supplementary_scripts  
HaSystemCalls.pm  Logging.pm    Patch          Precheck          scripts        Util  
HaUtils.pm        Manifest.pm   patchInstaller.pl  pretests         store          Uutils.pm  
Info.pm           onexit.d     Patch.pm       pretests.list     superpatches.manifest.xml  
[root@localhost updates]# ./installer
```

Рисунок 3.22 – Процес встановлення WinCollect на QRadar

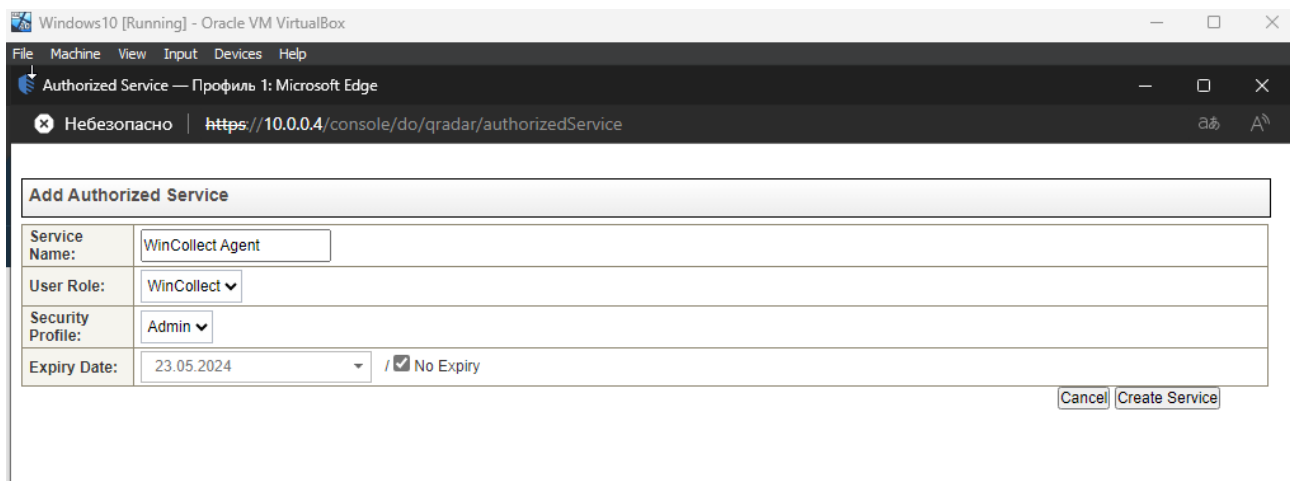


Рисунок 3.23 – Створення авторизованого сервісу для WinCollect

Після налаштування розширення WinCollect безпосередньо на самому сервері QRadar, переходимо до встановлення сервісу на основному контролері домену.

Контролер домену є центральним елементом в Active Directory, де зберігаються важливі дані про аутентифікацію, авторизацію та управління доступом. Встановлення WinCollect на контролері домену дозволяє централізовано збирати журнальні дані з різних джерел, пов'язаних з AD, що полегшує аналіз та моніторинг цих даних.

Встановлення агента WinCollect на кожній окремій робочій станції може бути більш витратним у плані ресурсів та управління. Крім того, відслідковувати та керувати багатьма інсталяціями на різних робочих станціях може бути складніше, ніж мати централізоване рішення на контролері домену.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

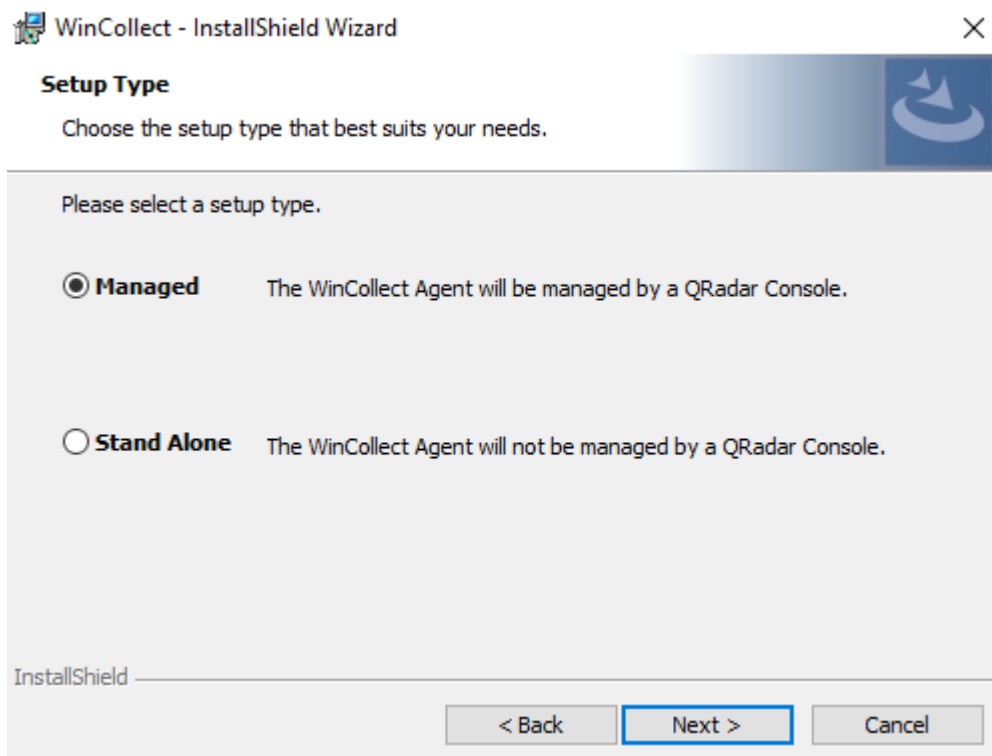


Рисунок 3.24 – Процес встановлення WinCollect на Windows Server

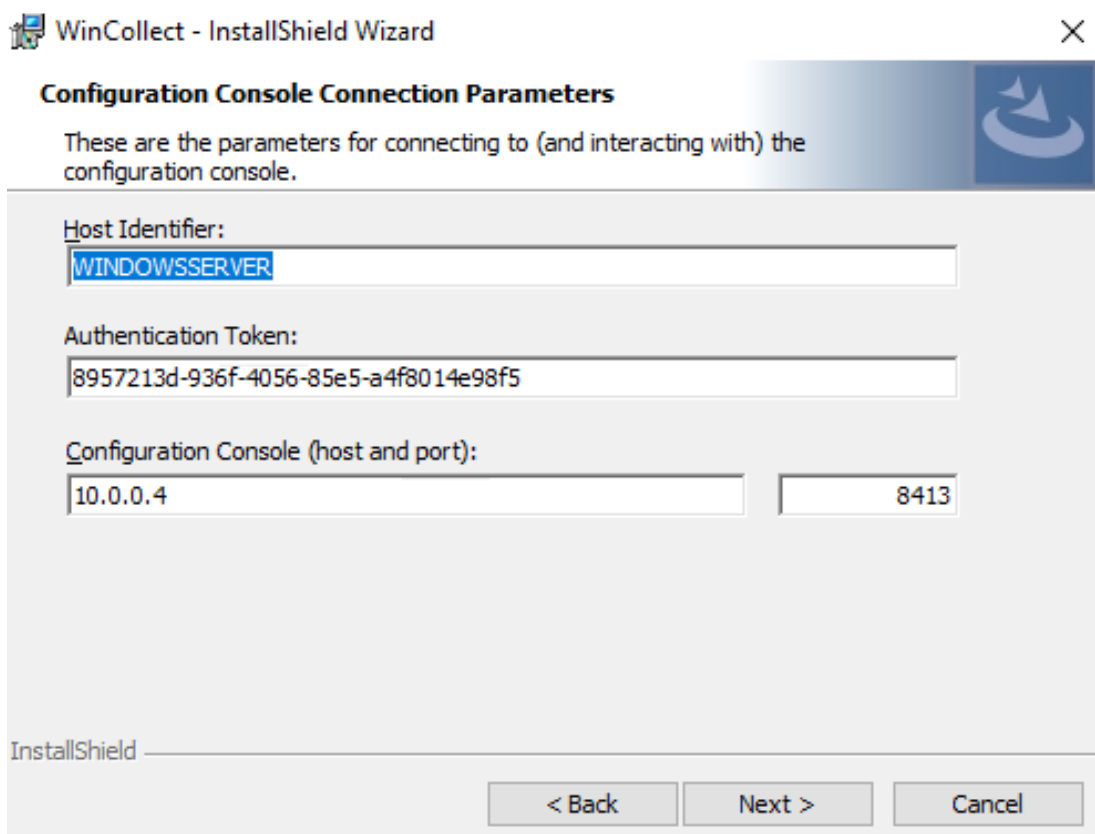


Рисунок 3.25 – Введення токена та адреси QRadar

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

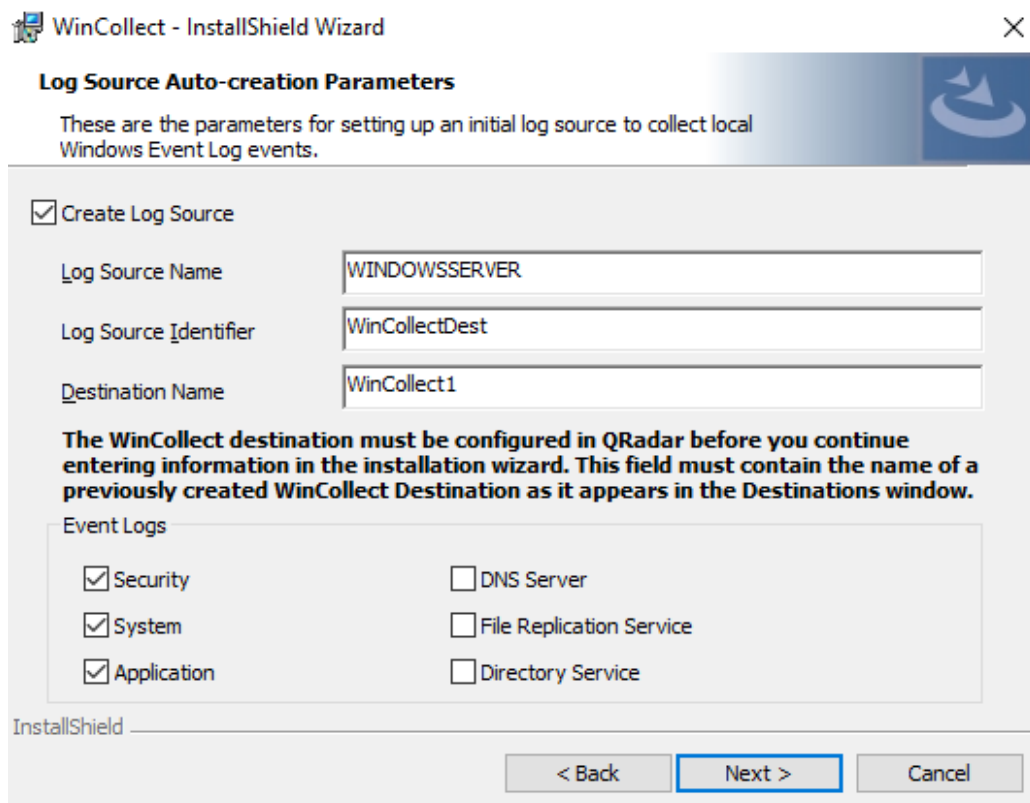


Рисунок 3.26 – Вибір типів журналів з яких буде збиратись інформація

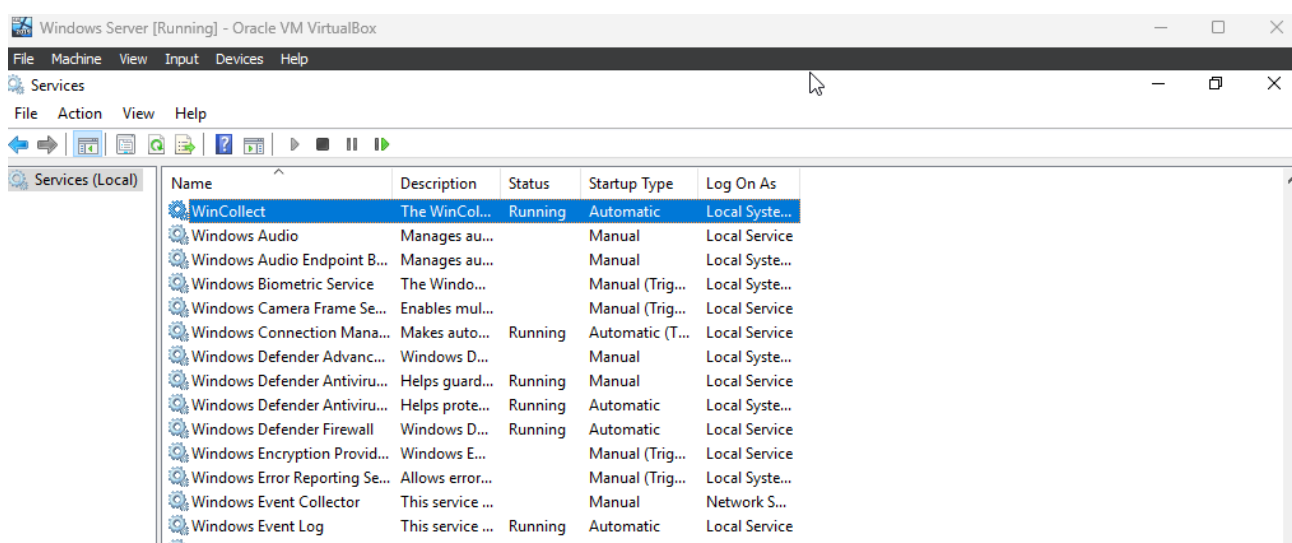


Рисунок 3.27 – Перевірка працездатності сервісу

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

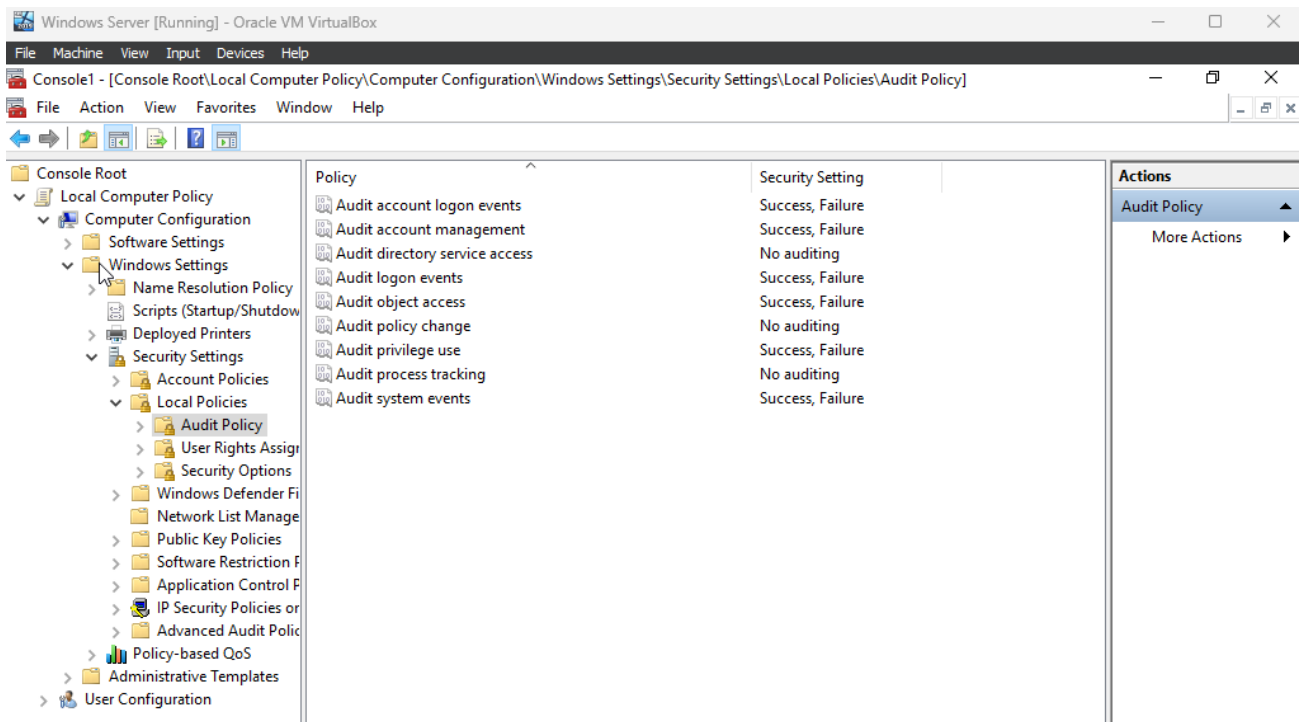


Рисунок 3.28 – Налаштування політик щодо збору інформації

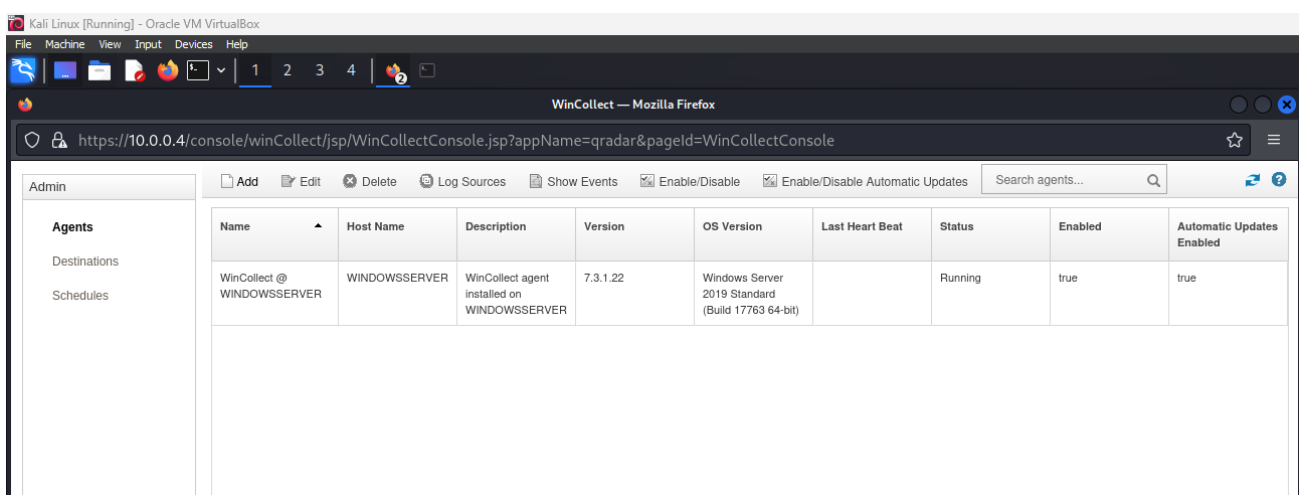


Рисунок 3.29 – Перевірка наявності Windows Server у консолі QRadar

Налаштування WinCollect успішно завершено, і тепер система QRadar активно збирає інформацію з різних джерел у мережі. Це включає дані з контролерів доменів, робочих станцій та інших важливих пристроїв, що дозволяє нам отримати повну картину стану безпеки в мережі.

Зараз настав час приступити до налаштування правил безпеки на самому QRadar. Це необхідно для того, щоб система могла визначати в яких випадках виникає потенційна загроза та вчасно попереджати про це. Шляхом створення правил

ми зможемо встановити параметри аналізу даних, визначити типи подій, які слід вважати підозрілими або загрозливими, та налаштувати механізми виявлення та реагування на інциденти.

Цей етап є критичним для забезпечення ефективного моніторингу та захисту мережі, тому ми будемо ретельно працювати над створенням правил, що відповідають вимогам безпеки та специфіки нашої організації.

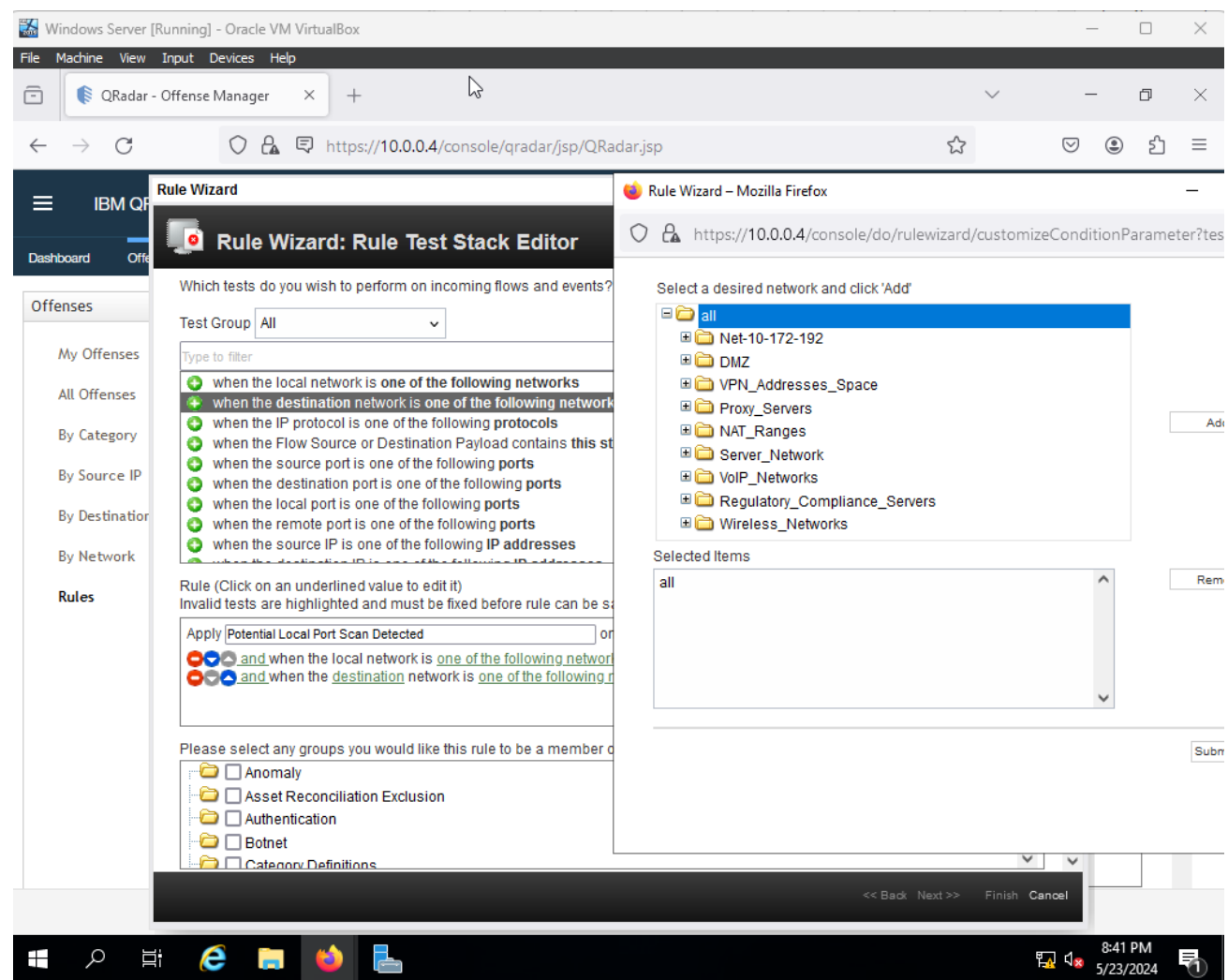


Рисунок 3.30 – Створення правила на потенційне сканування портів

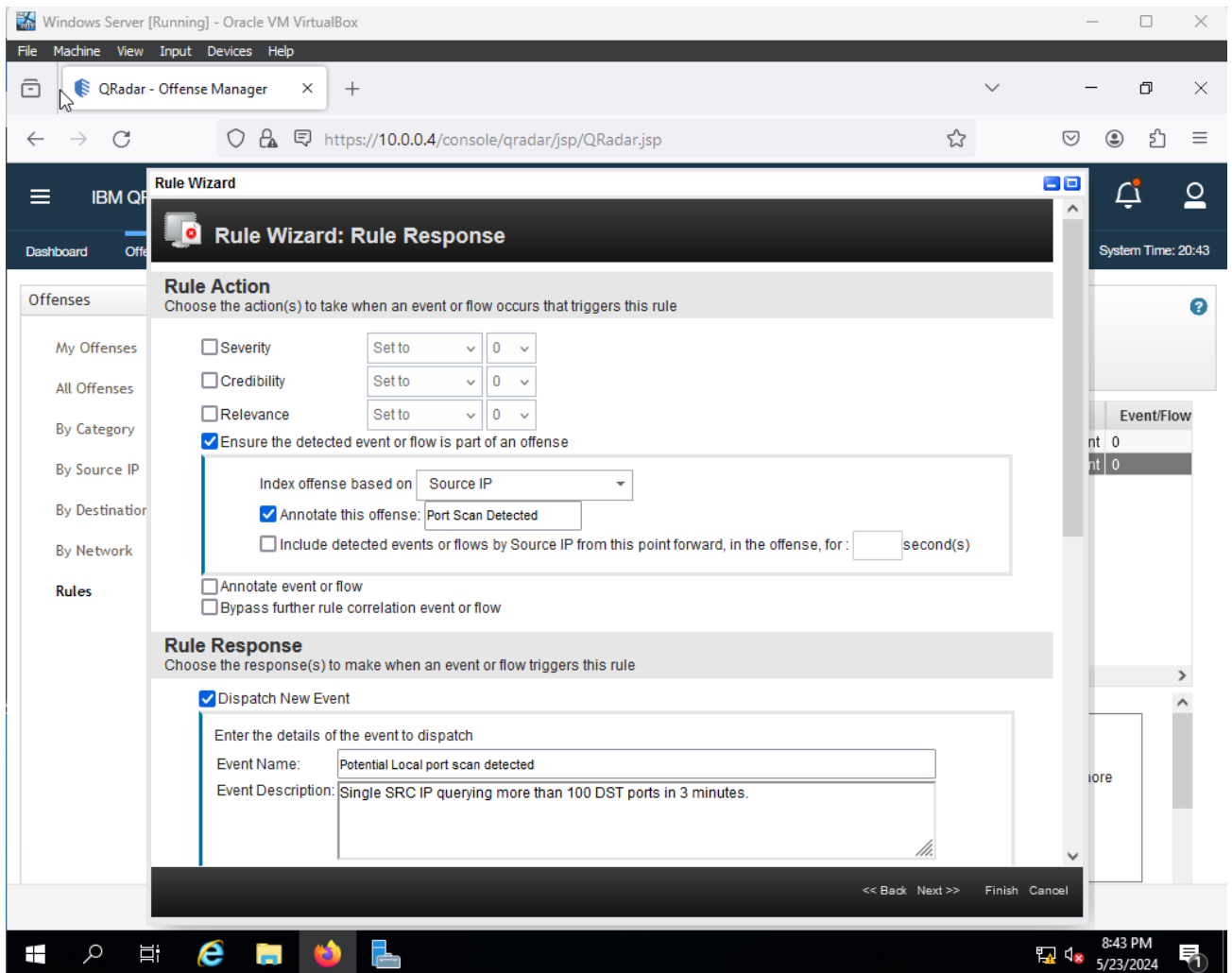


Рисунок 3.31 – Створення правила на потенційне сканування портів

3.4 Налаштування мережевого протоколу NetFlow

Наступним кроком є налаштування мережевого протоколу NetFlow на головному маршрутизаторі корпоративної мережі. Це налаштування дозволить детально моніторити трафік у мережі та забезпечити глибокий аналіз даних про мережеву активність.

Дані, зібрані за допомогою NetFlow, будуть відправлятися на сервер QRadar. Інтеграція NetFlow з QRadar дозволить централізовано аналізувати мережевий трафік, виявляти аномалії та потенційні загрози, а також здійснювати ефективний моніторинг безпеки мережі.

Цей крок є важливим для покращення видимості мережевої активності, оптимізації використання ресурсів та забезпечення своєчасного реагування на

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

інциденти безпеки. Завдяки впровадженню NetFlow та його інтеграції з QRadar, мережна інфраструктура компанії стане більш захищеною та ефективною.

```
Corporate-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Corporate-Router(config)#flow record NetFlow
Corporate-Router(config-flow-record)#match ipv4 tos
Corporate-Router(config-flow-record)#match ipv4 protocol
Corporate-Router(config-flow-record)#match ipv4 source address
Corporate-Router(config-flow-record)#match ipv4 destination address
Corporate-Router(config-flow-record)#match transport source-port
Corporate-Router(config-flow-record)#match transport destination-port
Corporate-Router(config-flow-record)#match interface input
Corporate-Router(config-flow-record)#collect interface output
Corporate-Router(config-flow-record)#collect counter bytes
Corporate-Router(config-flow-record)#collect counter packets
Corporate-Router(config-flow-record)#collect timestamp sys-uptime first
Corporate-Router(config-flow-record)#collect timestamp sys-uptime last
```

Рисунок 3.32 – Сценарій налагодження NetFlow

```
Corporate-Router(config-flow-record)#exit
Corporate-Router(config)#flow exporter QRADAR
Corporate-Router(config-flow-exporter)#desc Exported_Data_To_QRadar
Corporate-Router(config-flow-exporter)#destination 10.0.0.4
Corporate-Router(config-flow-exporter)#transport udp 2055
Corporate-Router(config-flow-exporter)#template data timeout 60
Corporate-Router(config-flow-exporter)#exit
Corporate-Router(config)#flow monitor FLOW-MONITOR
Corporate-Router(config-flow-monitor)#exporter QRADAR
Corporate-Router(config-flow-monitor)#cache timeout active 300
Corporate-Router(config-flow-monitor)#cache timeout update 60
Corporate-Router(config-flow-monitor)#statistics packet protocol
Corporate-Router(config-flow-monitor)#statistics packet size
Corporate-Router(config-flow-monitor)#record NetFlow
Corporate-Router(config-flow-monitor)#exit
```

Рисунок 3.33 – Сценарій налагодження NetFlow

```
Corporate-Router(config)#int gig0/0
Corporate-Router(config-if)#ip flow monitor FLOW-MONITOR input
Corporate-Router(config-if)#ip flow monitor FLOW-MONITOR output
Corporate-Router(config-if)#exit
Corporate-Router(config)#int e2/0
Corporate-Router(config-if)#ip flow monitor FLOW-MONITOR input
Corporate-Router(config-if)#ip flow monitor FLOW-MONITOR output
Corporate-Router(config-if)#exit
```

Рисунок 3.34 – Сценарій налагодження NetFlow

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Windows Server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Flow Source Management – Mozilla Firefox

https://10.0.0.4/console/do/surveillance/maintainFlowsources

Add Flow Source

☐ Build from existing flow source

Flow Source Details

Flow Source Name	NetFlow
Target Flow Collector	qflow0 :: localhost
Flow Source Type	Netflow v.1/v.5/v.7/v.9/IPFIX
☐ Enable Asymmetric Flows	

Netflow v.1/v.5/v.7/v.9/IPFIX Configuration

Monitoring Interface	Any
Monitoring Port	2056
Linking Protocol	UDP
☐ Enable Flow Forwarding	

Save Cancel

Рисунок 3.35 – Створення відповідного потоку даних у консолі QRadar

https://10.0.0.4/console/qradar/jsp/QRadar.jsp

IBM QRadar Security Intelligence - Community Edition

Dashboard Offenses Log Activity Network Activity Assets Reports Admin

Search... Quick Searches Add Filter Save Criteria Save Results Cancel Filter Positive Rules Actions

Quick Filter

Viewing real time flows View: Select An Option: Display: Custom

Using Search: Default-Short

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICMP Type/Code	Flow Source	Flow Interface
	5 верес. 2024 р. 1...	10.0.0.5	58170	142.250.203.194	443	udp_ip	Web.SecureWeb	2 341	3 483	8	11	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.5	45108	8.8.8.8	53	udp_ip	Misc.domain	150	0	2	0	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.4	47492	8.8.8.8	53	udp_ip	Misc.domain	72	0	1	0	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.5	46455	142.250.203.206	443	udp_ip	Web.SecureWeb	2 361	9 465	12	11	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.4	53299	8.8.8.8	53	udp_ip	Misc.domain	72	0	1	0	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	192.168.122.98	52396	142.250.196.193	443	tcp_ip	Web.SecureWeb	1 292	10 174	12	15	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	192.168.122.98	60046	46.4.92.154	443	tcp_ip	Web.SecureWeb	2 805	119 820	44	92	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	192.168.122.98	52488	77.75.149.202	80	tcp_ip	Web.Web.Misc	180	124	4	3	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	192.168.122.98	Multiple (117)	8.8.8.8	Multiple (117)	udp_ip	Misc.domain	0	N/A	0	N/A	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.4	Multiple (12)	8.8.8.8	Multiple (12)	udp_ip	Misc.domain	804	12	N/A	N/A	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.4	47695	8.8.8.8	53	udp_ip	Misc.domain	71	0	1	0	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.4	Multiple (45)	8.8.8.8	Multiple (45)	udp_ip	Misc.domain	5 310	N/A	45	N/A	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.5	58741	172.217.16.14	443	udp_ip	Web.SecureWeb	61 133	1 257 206	227	973	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.4	51081	172.217.16.40	443	udp_ip	Web.SecureWeb	6 016	10 072	9	10	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.5	60118	46.4.92.154	443	tcp_ip	Web.SecureWeb	4 881	130 077	46	99	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.4	53097	8.8.8.8	53	udp_ip	Misc.domain	72	0	1	0	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.5	59954	46.4.92.154	443	tcp_ip	Web.SecureWeb	1 758	24 693	18	24	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	192.168.122.98	39102	142.250.203.194	443	tcp_ip	Web.SecureWeb	1 782	6 332	15	19	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	192.168.122.98	60096	46.4.92.154	443	tcp_ip	Web.SecureWeb	9 614	427 396	107	302	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	192.168.122.98	58276	172.217.16.46	443	tcp_ip	Web.SecureWeb	1 372	9 397	14	16	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.4	56605	8.8.8.8	53	udp_ip	Misc.domain	72	0	1	0	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	192.168.122.98	58298	172.217.16.46	443	tcp_ip	Web.SecureWeb	1 332	7 896	13	15	N/A	localhost	localhost.gateway
	5 верес. 2024 р. 1...	10.0.0.5	79650	142.250.196.203	443	tcp_ip	Web.SecureWeb	1 123	5 544	8	10	N/A	localhost	localhost.gateway

Рисунок 3.36 – Результат роботи NetFlow

3.5 Проведення тестування підсистеми

Моніторинг всіх подій та налаштування QRadar здійснюється через Web UI Console IBM. Ця консоль є основним інтерфейсом для взаємодії з системою QRadar, надаючи доступ до всіх необхідних інструментів для аналізу, управління та налаштування.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Щоб отримати доступ до Web UI Console IBM QRadar, необхідно скористатися робочою станцією корпоративного Аналітика. Для цього потрібно відкрити веб-браузер і перейти за IP-адресою сервера QRadar, використовуючи захищений протокол HTTPS.

Якщо IP-адреса сервера QRadar — 10.0.0.4, потрібно ввести в адресний рядок браузера: `https://10.0.0.4`. Після цього відкриється вікно входу до консолі, де потрібно ввести відповідні облікові дані для доступу.

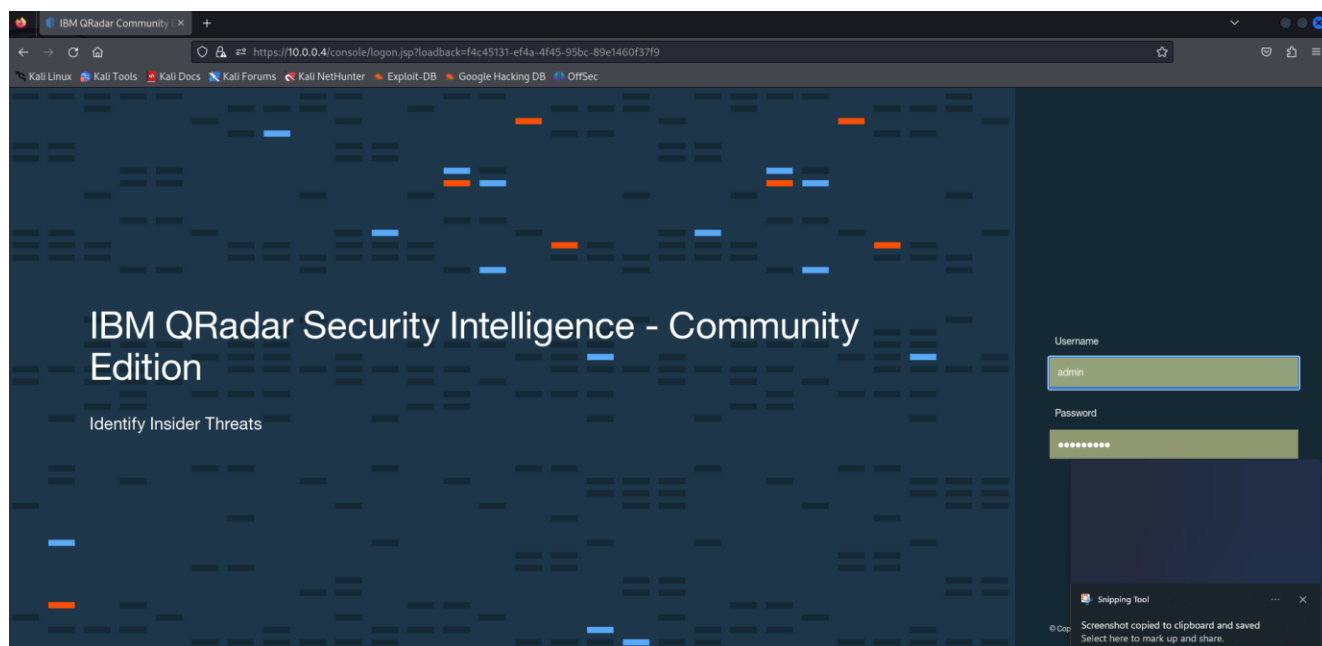


Рисунок 3.37 – Вікно входу до консолі IBM QRadar

Після введення облікових даних адміністратора ми потрапляємо на головну сторінку консолі IBM QRadar. Головна сторінка консолі є центральним вузлом для управління та моніторингу мережевих подій. Тут можна побачити **інформаційну панель (Dashboard)**. На цій панелі представлені ключові метрики та графіки, що відображають поточний стан мережі. Вона дозволяє швидко отримати огляд загальної безпеки, включаючи кількість виявлених загроз, активність користувачів та події, що потребують уваги.

Інциденти (Offenses): Розділ, де відображаються всі створені інциденти безпеки, які QRadar автоматично виявляє та класифікує. Цей розділ дозволяє аналітикам переглядати, розслідувати та реагувати на інциденти, забезпечуючи детальний

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

огляд кожного випадку, включаючи часові рамки, залучені системи та потенційні наслідки.

Активність журналів (Log Activity): Розділ, де відображаються всі зібрані журнали подій у реальному часі. Тут можна переглядати, фільтрувати та аналізувати всі події, що надходять з різних джерел у мережі. Це дозволяє швидко ідентифікувати підозрілу активність та забезпечити оперативну реакцію на інциденти.

Активність мережі (Network Activity): Розділ, де можна стежити за мережевим трафіком та аналізувати потоки даних. Тут відображаються всі дані про мережеву активність, що дозволяє виявляти аномалії в трафіку, відслідковувати взаємодію між різними вузлами мережі та забезпечувати детальний аналіз мережевих патернів.

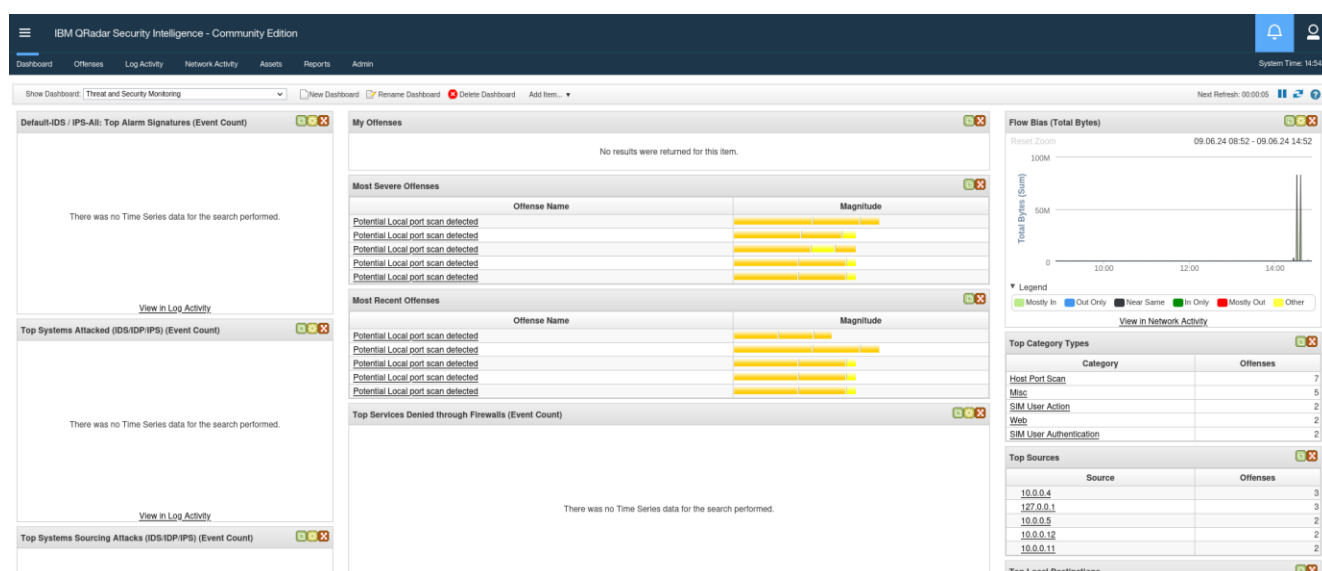


Рисунок 3.38 – Головна панель консолі IBM QRadar

Раніше було налаштовано правило для виявлення потенційного сканування портів. Давайте протестуємо це правило, щоб переконатися в його ефективності.

Сканування портів є поширеною технікою, яку зловмисники використовують для виявлення відкритих портів та служб на цільових системах. Виявлення таких спроб є важливою складовою забезпечення безпеки нашої мережі.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

Я виконаю контрольоване сканування портів з одного з внутрішніх хостів за допомогою Nmap. Нехай це буде PDC (Основний контролер домену) який має IP-адресу 10.0.0.2.

```

(kali㉿kali)-[~]
$ nmap -Pn 10.0.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 08:19 EDT
Nmap scan report for 10.0.0.2
Host is up (0.0031s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds
(kali㉿kali)-[~]
$
  
```

Рисунок 3.39 – Сканування портів з основного контролера домену

All Offenses - Offense 326 (Summary)			
Offense 326		Status	Relevance 3
Magnitude		Severity	3
Description	Potential Local port scan detected	Credibility	2
Source IP(s)	10.0.0.2 (10.0.0.2)	Offense Type	Source IP
Destination IP(s)	Local (2) Remote (35)	EventFlow count	13 events and 100 flows in 5 categories
Network(s)	Multiple (2)	Start	9 vaps, 2024 p., 15:14:58
Offense Source Summary		Duration	6m 3s
IP	10.0.0.2	Assigned to	Unassigned
Magnitude			
Location	Net:10-172-192-Net:10-0-0-0		
Vulnerabilities	0		
Username	Unknown		
MAC Address	Unknown NIC		
Host Name	Unknown		
Asset Name	10.0.0.2		
Weight	0		
Offenses	2	Events/Flows	140

Рисунок 3.40 – Повідомлення про потенційне сканування портів

QRadar журналює всі спроби аутентифікації, як безпосередньо через вікно логіну в консоль IBM QRadar, так і через протокол SSH. Це дозволяє нам своєчасно виявляти та реагувати на потенційні загрози, пов'язані з несанкціонованими спробами доступу.

IBM QRadar Security Intelligence - Community Edition						
Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Admin
Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions						
Information Message	System Notification-2 :: localhost	1	9 черв. 2024 р., 15:29:14	Information	127.0.0.1	
Information Message	System Notification-2 :: localhost	1	9 черв. 2024 р., 15:29:12	Information	127.0.0.1	
Information Message	System Notification-2 :: localhost	1	9 черв. 2024 р., 15:29:12	Information	127.0.0.1	
Information Message	System Notification-2 :: localhost	1	9 черв. 2024 р., 15:29:10	Information	127.0.0.1	
Information Message	System Notification-2 :: localhost	1	9 черв. 2024 р., 15:29:10	Information	127.0.0.1	
Login Failed Audit Log	SIM Audit-2 :: localhost	1	9 черв. 2024 р., 15:29:09	SIM User Authentication	10.0.0.2	
Login Failed Audit Log	SIM Audit-2 :: localhost	1	9 черв. 2024 р., 15:29:09	SIM User Authentication	10.0.0.2	

Рисунок 3.41 – Повідомлення про спроби логіну в консоль IBM QRadar

Offense — Mozilla Firefox							
https://10.0.0.4/console/do/sem/offensesummary							
Offense 326 (Summary)							
Top 5 Categories							
Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow		
Host Port Scan		3	23	9 черв. 2024 р., ...	9 черв. 2024 р., ...		
SIM User Authentication		1	6	9 черв. 2024 р., ...	9 черв. 2024 р., ...		
Stored		1	9	9 черв. 2024 р., ...	9 черв. 2024 р., ...		
Remote Access		1	2	9 черв. 2024 р., ...	9 черв. 2024 р., ...		
Misc		1	147	9 черв. 2024 р., ...	9 черв. 2024 р., ...		
Last 10 Events							
Event Name	Magnitude	Log Source	Category	Destination	Destination IPv6	Dst Port	
Potential Local port scan detected		Custom Rule En...	Host Port Scan	10.0.0.4	0:0:0:0:0:0:0	0	
Failed Login Attempt		SIM Audit-2 :: lo...	SIM User Authe...	10.0.0.4	0:0:0:0:0:0:0	0	
Potential Local port scan detected		Custom Rule En...	Host Port Scan	10.0.0.4	0:0:0:0:0:0:0	0	
Failed Login Attempt		SIM Audit-2 :: lo...	SIM User Authe...	10.0.0.4	0:0:0:0:0:0:0	0	
Potential Local port scan detected		Custom Rule En...	Host Port Scan	10.0.0.1	0:0:0:0:0:0:0	22	
Potential Local port scan detected		Custom Rule En...	Host Port Scan	10.0.0.1	0:0:0:0:0:0:0	53	
Potential Local port scan detected		Custom Rule En...	Host Port Scan	10.0.0.1	0:0:0:0:0:0:0	53	
Potential Local port scan detected		Custom Rule En...	Host Port Scan	10.0.0.1	0:0:0:0:0:0:0	53	
Potential Local port scan detected		Custom Rule En...	Host Port Scan	10.0.0.1	0:0:0:0:0:0:0	22	
Potential Local port scan detected		Custom Rule En...	Host Port Scan	10.0.0.2	0:0:0:0:0:0:0	0	

Рисунок 3.42 – Повідомлення про спроби підключення використовуючи SSH

Оскільки в мережі розгорнуто службу каталогів Active Directory, важливо приділити увагу збору логів з робочих станцій з операційною системою Windows.

Потрібно спочатку створити об'єкт в "Log Sources" (див. рисунок 3.42) і потім на вкладці "Log Activity" створити фільтр для відображення всіх подій, пов'язаних з Windows Server.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

Log Sources – Mozilla Firefox

https://10.0.0.4/console/do/sem/maintainSensorDevice?dispatch=edit&appName=eventviewer&pageId=SensorDeviceList&hasSearched=

Edit a log source

Log Source Name: WINDOWSSERVER

Log Source Description: WINDOWSSERVER LOGS

Log Source Type: Microsoft Windows Security Event Log

Protocol Configuration: WinCollect

Log Source Identifier: WinCollect1

Local System: ☒

Event Rate Tuning Profile: Default (Endpoint)

Polling Interval (ms): 3000

Application or Service Log Type: None

Standard Log Types

Event Log Poll Protocol: MSEVEN6

Security: ☒

Security Log Filter Type: No Filtering

System: ☒

System Log Filter Type: No Filtering

Рисунок 3.43 – Створення джерела журналу

QRadar - Log Activity

https://10.0.0.4/console/qradar/jsp/QRadar.jsp

IBM QRadar Security Intelligence - Community Edition

Dashboard Offenses Log Activity Network Activity Assets Reports Admin

System Time: 16:51

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

Quick Filter

Viewing real time events View: Select An Option: Display: Default (Normalized)

Current Filters:
Log Source is WINDOWSSERVER (Clear Filter)

	Event Name	Log Source	Event Count	Time	
	Success Audit: The Windows Filtering Platform has permitted a bind to a local port	WINDOWSSERVER	1	9 черв. 2024 р., 16:52:03	A
	Success Audit: The Windows Filtering Platform has allowed a connection	WINDOWSSERVER	1	9 черв. 2024 р., 16:52:03	A
	Success Audit: Group membership information	WINDOWSSERVER	1	9 черв. 2024 р., 16:52:03	Ir
	Success Audit: An account was logged off	WINDOWSSERVER	1	9 черв. 2024 р., 16:52:03	F-
	Success Audit: The Windows Filtering Platform has allowed a connection	WINDOWSSERVER	1	9 черв. 2024 р., 16:52:03	A
	Success Audit: An account was successfully logged on	WINDOWSSERVER	1	9 черв. 2024 р., 16:52:03	U
	Success Audit: Successful logon with administrative or special privileges	WINDOWSSERVER	1	9 черв. 2024 р., 16:52:03	A
	Failure Audit: The Windows Filtering Platform blocked a packet	WINDOWSSERVER	2	9 черв. 2024 р., 16:51:42	A
	Failure Audit: The Windows Filtering Platform blocked a packet	WINDOWSSERVER	2	9 черв. 2024 р., 16:51:42	A
	Failure Audit: The Windows Filtering Platform blocked a packet	WINDOWSSERVER	2	9 черв. 2024 р., 16:51:42	A
	Failure Audit: The Windows Filtering Platform blocked a packet	WINDOWSSERVER	2	9 черв. 2024 р., 16:51:42	A
	Failure Audit: The Windows Filtering Platform blocked a packet	WINDOWSSERVER	2	9 черв. 2024 р., 16:51:42	A
	Failure Audit: The Windows Filtering Platform blocked a packet	WINDOWSSERVER	2	9 черв. 2024 р., 16:51:42	A
	Failure Audit: The Windows Filtering Platform blocked a packet	WINDOWSSERVER	2	9 черв. 2024 р., 16:51:42	A

Рисунок 3.44 – Відображення журналів пов'язаних із Windows Server

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

QRadar успішно збирає логи з Windows Server, що включає не лише дані з самого сервера, а й інформацію з усіх робочих станцій, які підключені до Active Directory. Це дозволяє нам отримувати повну картину подій та активності в мережі, забезпечуючи відстеження та аналіз дій користувачів та системних подій у реальному часі. Збір логів з робочих станцій допомагає вчасно виявляти потенційні загрози, контролювати доступ та забезпечувати безпеку інфраструктури.

На прикладі рисунку 3.45 можна побачити, що QRadар отримав журнал аудиту з Windows Server, на якому вказано, що на одній з робочих станцій відбулась неуспішна аутентифікація.

Current Filters:				
Log Source is WINDOWSSERVER (Clear Filter)				
	Event Name	Log Source	Event Count	Time
	Success Audit: The Windows Filtering Platform has allowed a connection	WINDOWSSERVER	1	9 черв. 2024 р., 17:23:21
	Success Audit: Successful logon with administrative or special privileges	WINDOWSSERVER	1	9 черв. 2024 р., 17:23:11
	Success Audit: The Windows Filtering Platform has allowed a connection	WINDOWSSERVER	1	9 черв. 2024 р., 17:23:21
	Failure Audit: Kerberos pre-authentication failed	WINDOWSSERVER	1	9 черв. 2024 р., 17:23:21
	Failure Audit: Kerberos pre-authentication failed	WINDOWSSERVER	1	9 черв. 2024 р., 17:23:21
	Success Audit: The Windows Filtering Platform has allowed a connection	WINDOWSSERVER	1	9 черв. 2024 р., 17:23:21

Рисунок 3.45 – Журналювання подій з робочої станції мережі

ВИСНОВКИ

У даній кваліфікаційній роботі було спроектовано та розгорнуто підсистему SIEM для моніторингу інформаційної системи на базі рішень IBM QRadar.

У першому розділі було розглянуто ключові теоретичні аспекти, що стосуються проектування підсистем SIEM для Security Operations Center (SOC). Було визначено роль та функції SOC, що забезпечують централізоване управління безпекою в організації. Основні поняття та принципи роботи SIEM були детально проаналізовані, включаючи процеси збору, аналізу та кореляції подій. Окремо було розглянуто переваги використання SIEM-рішень, такі як підвищення ефективності виявлення загроз і зменшення часу реагування на інциденти. Також було проведено огляд найпопулярніших SIEM-рішень, зокрема детально розглянуто функції та можливості IBM QRadar.

У другому розділі висвітлено процес проектування підсистеми SIEM для SOC на базі IBM QRadar. Розглянуто етапи проектування мережі, необхідні для забезпечення коректного функціонування SIEM-системи. Проведено аналіз рішення QRadar, а також програмного забезпечення WinCollect, яке використовується для збору логів з різних джерел. Окрему увагу приділено аналізу протоколу NetFlow у контексті SIEM-рішень, що дозволяє забезпечити більш детальне моніторинг та аналіз мережевого трафіку.

У третьому розділі розглянуто практичні аспекти налаштування, реалізації та тестування підсистеми SIEM на базі IBM QRadar. Описано процес налаштування мережі та служби каталогів Active Directory, що є важливими елементами для інтеграції SIEM-системи в існуючу інфраструктуру. Детально описано налаштування серверу QRadar та встановлення програмного забезпечення WinCollect. Окремо розглянуто налаштування мережевого протоколу NetFlow, що забезпечує ефективний збір і аналіз мережевого трафіку. Проведено тестування підсистеми, результати якого підтвердили її ефективність та відповідність заданим вимогам.

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Best SIEM Solutions: Top 10 SIEM systems and How to Choose. *Exabeam*.
URL: <https://www.exabeam.com/explainers/siem-tools/siem-solutions/>
2. *Cisco: Software, Network, and Cybersecurity Solutions - Cisco*.
URL: <https://www.cisco.com/c/dam/en/us/td/docs/routers/asr920/configuration/guide/netmgmt/fnf-xe-3e-asr920-book.html>
3. Configuring netflow. *Cisco*.
URL: https://www.cisco.com/c/en/us/td/docs/iosxr/cisco8000/netflow/70x/configuration/guide/b-netflow-config-guide-cisco8k-r70x/b-netflow-cisco-8k-r70x_chapter_01.html
4. Exabeam security operations platform. *Exabeam*. URL: <https://www.exabeam.com/product/fusion/>
5. How to setup active directory on windows server 2022. *Active Directory Tools, Report, Monitor & Manage AD*. URL: <https://infrastos.com/how-to-setup-active-directory-on-windows-server-2022/>
6. IBM Security QRadar SIEM. *IBM - United States*.
URL: <https://www.ibm.com/products/qradar-siem>
7. Installation and configuration for data collection. *Documentation Library*.
URL: <https://docs.delinea.com/online-help/cloud-suite/siem-integrations/qradar/configuration-for-data-collection.htm>
8. Msbj. Top 10 SIEM tools for strengthening cybersecurity defenses. *Medium*.
URL: <https://medium.com/@msbj/top-10-siem-tools-for-strengthening-cybersecurity-defenses-6b288d8e894c>
9. Security operations center roles and responsibilities. *Exabeam*.
URL: <https://www.exabeam.com/security-operations-center/security-operations-center-roles-and-responsibilities/>
10. SIEM: security information & event management explained | splunk. *Splunk*.
URL: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

11. What is a security operations center (SOC)? | fortinet. *Fortinet*. URL: <https://www.fortinet.com/it/resources/cyberglossary/what-is-soc>
12. What is a security operations center (SOC)? | Microsoft Security. *Your request has been blocked. This could be due to several reasons.* URL: <https://www.microsoft.com/en-us/security/business/security-101/what-is-a-security-operations-center-soc>
13. What is a security operations center (SOC)? *Palo Alto Networks*. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-soc>
14. What is security operations center (SOC)? - threatdown by malwarebytes. *ThreatDown by Malwarebytes*. URL: <https://www.threatdown.com/glossary/what-is-soc-security-operations-center/>
15. What is SIEM? | IBM. *IBM - United States*. URL: <https://www.ibm.com/topics/siem>
16. What is splunk? Key benefits and features of splunk. *Fortinet*. URL: <https://www.fortinet.com/resources/cyberglossary/what-is-splunk>
17. IBM QRadar DSM Configuration Guide March 2024. *IBM*. URL: https://www.ibm.com/docs/en/SS42VS_DSM/pdf/b_dsm_guide.pdf

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

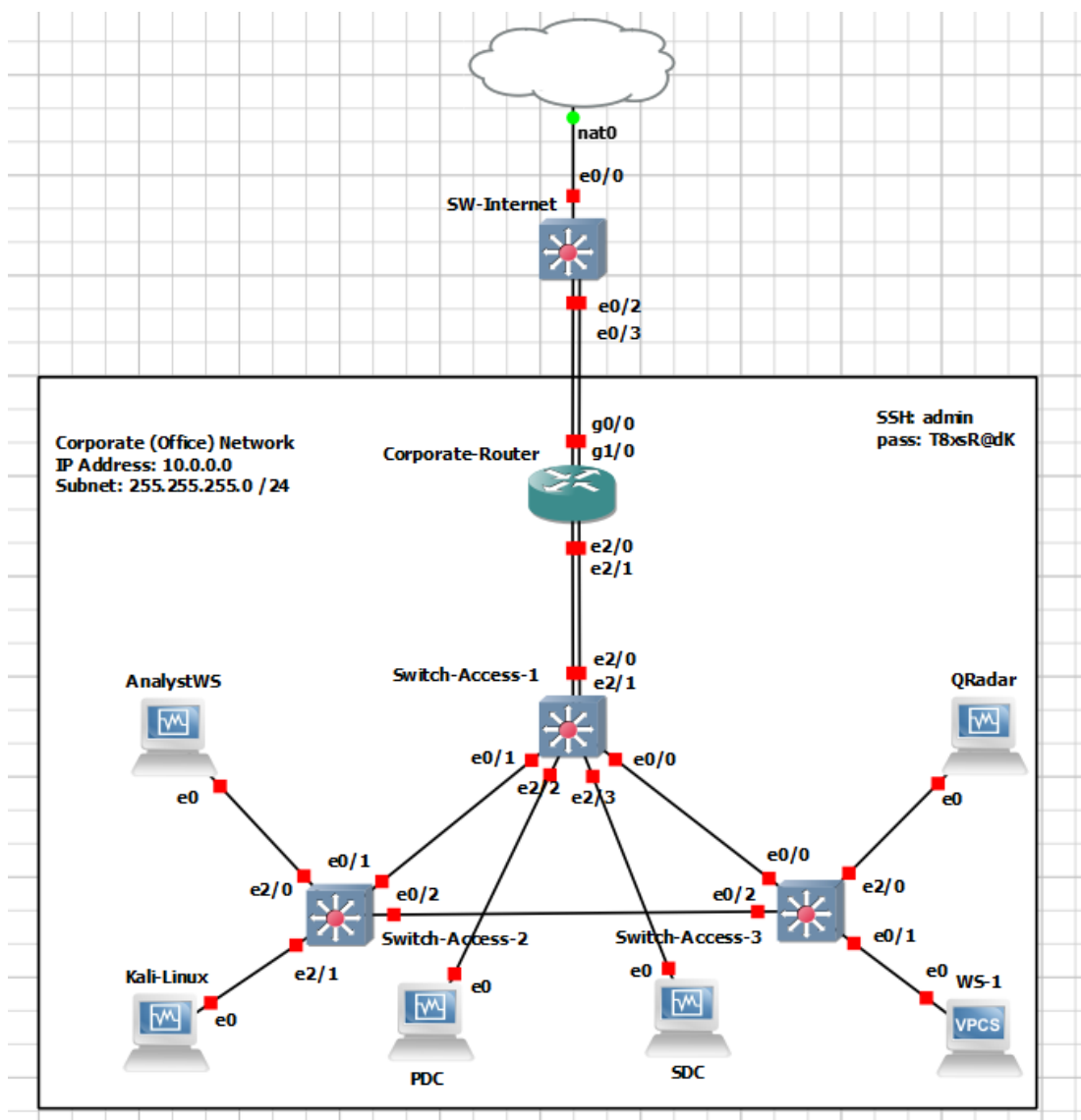


Рисунок А.1 – Топологічна схема корпоративної мережі

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ Арк. 75
		Єфіменко А.А.			
Змн.	Арк.	№ докум.	Підпис	Дата	

Файл поточної конфігурації маршрутизатора Corporate-Router:

```

Current configuration : 3005 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime
msec
service timestamps log datetime
msec
no service password-encryption
!
hostname Corporate-Router
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
clock timezone EET 2
clock summer-time EEST recurring
!
flow exporter QRADAR
description
Exported_Data_To_QRadar
destination 10.0.0.4
transport udp 2055
template data timeout 60
!
!
flow record NetFlow
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
collect interface output
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
flow monitor FLOW-MONITOR
record NetFlow
exporter QRADAR
cache timeout active 300
cache timeout update 60
statistics packet protocol
statistics packet size
!
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
ip dhcp excluded-address 10.0.0.1
ip dhcp excluded-address 10.0.0.2
ip dhcp excluded-address 10.0.0.3
ip dhcp excluded-address 10.0.0.4
ip dhcp excluded-address 10.0.0.11
ip dhcp excluded-address 10.0.0.12
ip dhcp excluded-address 10.0.0.13
!
ip dhcp pool corporateNetwork

```

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

```

network 10.0.0.0 255.255.255.0
default-router 10.0.0.1
dns-server 8.8.8.8
!
ip domain name kotsiuba.net
ip name-server 8.8.8.8
no ipv6 cef
!
multilink bundle-name
authenticated
!
username admin privilege 15 secret
5 $1$T/3V$nP/C2BpjzqNGAUPlnP2Jx/
archive
log config
hidekeys
!
ip tcp synwait-time 5
ip ssh version 2
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
ip address dhcp
ip flow monitor FLOW-MONITOR input
ip flow monitor FLOW-MONITOR
output
ip nat outside
ip virtual-reassembly
duplex full
speed 1000
media-type gbic
negotiation auto
!
interface GigabitEthernet1/0
no ip address
shutdown
negotiation auto
!
interface Ethernet2/0
ip address 10.0.0.1 255.255.255.0
ip flow monitor FLOW-MONITOR input
ip flow monitor FLOW-MONITOR
output
ip nat inside
ip virtual-reassembly
duplex half
!
interface Ethernet2/1
no ip address
shutdown
duplex half
!
interface Ethernet2/2
no ip address
shutdown
duplex half
!
interface Ethernet2/3
no ip address
shutdown
duplex half
!
ip forward-protocol nd
no ip http server

```

		Коцюба Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Єфіменко А.А.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip http secure-server
!
ip nat inside source list 1
interface GigabitEthernet0/0
overload
!
access-list 1 permit 10.0.0.0
0.0.0.255
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
banner motd ^CPowered by Dmytro
Kotsiuba^C
!

```

```

line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 20 0
logging synchronous
login local
transport input ssh
!
end

```