МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МОДУЛЬ ПІДТРИМКИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ШЛЯХОМ ІНТЕГРАЦІЇ SIEM ТА SOAR-РІШЕНЬ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Артур САВИЦЬКИЙ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Артур САВИЦЬКИЙ
Ім’я, ПРІЗВИЩЕ

Керівник: Ірина ЛОЗОВА
к.т.н. Ім’я, ПРІЗВИЩЕ

Рецензент: Сергій ГАХОВ
к.в.н. Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Савицькому Артуру Олександровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Модуль підтримки реагування на кіберінциденти шляхом інтеграції SIEM та SOAR-рішень”,
керівник кваліфікаційної роботи Лозова Ірина, к.т.н.,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “12” травня 2026р.

3. Вихідні дані до кваліфікаційної роботи: *інциденти інформаційної безпеки в корпоративних мережах, процеси реагування на кіберінциденти в Security Operations Center (SOC), SIEM-системи, SOAR-платформи, IBM QRadar, міжнародні стандарти та рекомендації з управління інформаційною безпекою, наукова і технічна література у сфері кібербезпеки.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати сучасні підходи до реагування на кіберінциденти та особливості функціонування Security Operations Center (SOC).
4.2. Дослідити можливості інтеграції SIEM та SOAR-рішень для автоматизації процесів реагування на кіберінциденти.
4.3. Розробити модуль підтримки реагування на кіберінциденти на основі IBM QRadar та оцінити ефективність його використання шляхом моделювання типових сценаріїв реагування.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Аналіз сучасних підходів до реагування на кіберінциденти.	08.04.2026	
4.	Розробка модуля підтримки реагування на кіберінциденти.	15.04.2026	
5.	Експериментальне дослідження ефективності рішення.	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ЕК.	12.06.2026	

Здобувач вищої освіти _____ Артур САВИЦЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ірина ЛОЗОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувачем Савицький А.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Модуль підтримки реагування на кіберінциденти шляхом інтеграції SIEM та SOAR-рішень"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач САВИЦЬКИЙ Артур у кваліфікаційній роботі проаналізував сучасні підходи до реагування на кіберінциденти та особливості функціонування центрів моніторингу безпеки (SOC), дослідив можливості інтеграції SIEM- та SOAR-рішень для автоматизації процесів реагування, розробив модуль підтримки реагування на кіберінциденти на основі IBM QRadar та виконав оцінювання його ефективності.

САВИЦЬКИЙ Артур продемонстрував здатність до самостійного аналізу технічної літератури, володіння сучасними технологіями кібербезпеки, навички проєктування архітектури систем автоматизованого реагування та використання засобів моніторингу інформаційної безпеки. Результати дослідження мають практичне значення для підвищення ефективності роботи SOC шляхом скорочення часу первинної обробки інцидентів та зменшення навантаження на аналітиків.

Все це дозволяє оцінити кваліфікаційну роботу здобувача САВИЦЬКОГО Артура на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Ірина ЛОЗОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Савицький А.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри управління кібербезпекою та захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти САВИЦЬКОГО Артура
на тему “ Модуль підтримки реагування на кіберінциденти шляхом інтеграції SIEM та SOAR-рішень ”

Актуальність. У сучасних умовах кількість кіберінцидентів та складність кіберзагроз постійно зростають, що створює необхідність підвищення ефективності роботи центрів моніторингу безпеки (SOC). Значна частина процесів аналізу та реагування на інциденти досі виконується вручну, що збільшує час обробки подій та навантаження на аналітиків. Одним із перспективних напрямів розвитку кібербезпеки є автоматизація процесів реагування шляхом інтеграції SIEM- та SOAR-рішень. Тому дослідження можливостей побудови модуля підтримки реагування на кіберінциденти є актуальним науково-практичним завданням.

Позитивні сторони.

1. У роботі проведено аналіз сучасних підходів до реагування на кіберінциденти та функціонування Security Operations Center.
2. Досліджено можливості використання IBM QRadar, SOAR-рішень та систем управління вразливостями для автоматизації процесів реагування.
3. Розроблено архітектуру модуля підтримки реагування на кіберінциденти та алгоритм його функціонування.
4. Проведено експериментальне дослідження ефективності запропонованого підходу та виконано порівняння з традиційними процесами реагування.

Недоліки.

Доцільно було б розширити перелік досліджуваних сценаріїв реагування та розглянути можливість інтеграції додаткових джерел threat intelligence для підвищення точності автоматизованого аналізу інцидентів.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач САВИЦЬКИЙ Артур заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Сергій ГАХОВ
к.в.н. *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена розробці модуля підтримки реагування на кіберінциденти шляхом інтеграції SIEM та SOAR-рішень. Робота складається зі вступу, трьох розділів, що містять 17 рисунків, 6 таблиць, висновків та списку використаних джерел із 36 найменувань. Загальний обсяг роботи становить 66 сторінок.

Мета роботи. Розробка модуля підтримки реагування на кіберінциденти шляхом інтеграції SIEM та SOAR-рішень.

Об'єкт дослідження. Процеси реагування на кіберінциденти в центрах моніторингу безпеки (Security Operations Center, SOC).

Предмет дослідження. Методи та засоби автоматизації процесів реагування на кіберінциденти на основі інтеграції SIEM та SOAR-рішень.

Методи дослідження. Для досягнення поставленої мети використано методи аналізу та синтезу, порівняння, системного аналізу, моделювання, узагальнення, а також методи дослідження процесів управління інформаційною безпекою.

Як результат у роботі проаналізовано сучасні підходи до реагування на кіберінциденти та особливості функціонування центрів моніторингу безпеки; досліджено можливості використання SIEM-, SOAR-рішень і засобів управління вразливостями для автоматизації процесів реагування; розроблено модуль підтримки реагування на кіберінциденти на основі IBM QRadar та проведено оцінювання ефективності запропонованого рішення.

Галузь застосування. Результати роботи охоплюють центри моніторингу безпеки (SOC), підрозділи інформаційної безпеки підприємств, організацій та установ, що використовують системи моніторингу подій безпеки та потребують автоматизації процесів реагування на кіберінциденти.

Ключові слова: КІБЕРІНЦИДЕНТ, INCIDENT RESPONSE, SOC, SIEM, SOAR, IBM QRADAR, NESSUS VULNERABILITY MANAGEMENT, АВТОМАТИЗАЦІЯ РЕАГУВАННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

The qualification work is devoted to the development of a cyber incident response support module through the integration of SIEM and SOAR solutions. The thesis consists of an introduction, three chapters containing 17 figures, 6 tables, conclusions, and a list of references including 36 sources. The total volume of the thesis is 66 pages.

The purpose of the study is to develop a module to support cyber incident response by integrating SIEM and SOAR solutions.

The object of the study is cyber incident response processes within Security Operations Centers (SOC).

The subject of the study is methods and tools for automating cyber incident response processes through the integration of SIEM and SOAR solutions.

Research methods. To achieve the stated objective, methods of analysis and synthesis, comparison, system analysis, modeling, generalization, and methods used in information security management research were applied.

As a result, the work analyzes modern approaches to cyber incident response and the operation of Security Operations Centers; investigates the possibilities of using SIEM, SOAR and vulnerability management solutions for incident response automation; develops a cyber incident response support module based on IBM QRadar and evaluates the effectiveness of the proposed solution.

Field of application. The results of the study can be applied in Security Operations Centers (SOC), information security departments of enterprises, organizations and institutions that use security monitoring systems and require automation of cyber incident response processes.

Keywords: CYBER INCIDENT, INCIDENT RESPONSE, SOC, SIEM, SOAR, IBM QRADAR, NESSUS VULNERABILITY MANAGEMENT, RESPONSE AUTOMATION, INFORMATION SECURITY.

ЗМІСТ

ВСТУП

У сучасних умовах цифрової трансформації економіки та державного управління спостерігається стрімке зростання кількості та складності кіберзагроз. Організації різних секторів дедалі частіше стають об’єктами цілеспрямованих атак, що призводить до витоку конфіденційної інформації, фінансових втрат та порушення безперервності бізнес-процесів. Відповідно до вимог законодавства України, зокрема Закону України «Про основні засади забезпечення кібербезпеки України», важливим завданням є забезпечення ефективного виявлення та реагування на кіберінциденти.

Одним із ключових інструментів забезпечення кіберзахисту є центри моніторингу безпеки (SOC), які використовують системи класу SIEM (Security Information and Event Management). Такі системи дозволяють здійснювати централізований збір, аналіз та кореляцію подій інформаційної безпеки. Водночас традиційні підходи до реагування на інциденти часто передбачають значну участь людини, що знижує оперативність реагування та підвищує ризик помилок.

Сучасним напрямом розвитку є використання SOAR-платформ (Security Orchestration, Automation and Response), які забезпечують автоматизацію процесів реагування, оркестрацію дій між різними засобами захисту та реалізацію стандартизованих сценаріїв реагування. Інтеграція SIEM та SOAR-рішень дозволяє створити єдину екосистему управління кіберінцидентами, що значно підвищує ефективність роботи SOC.

Таким чином, **актуальність теми** дипломної роботи зумовлена необхідністю підвищення рівня автоматизації процесів реагування на кіберінциденти, скорочення часу обробки інцидентів та зменшення впливу людського фактора під час роботи центрів моніторингу безпеки.

Метою роботи є розробка модуля підтримки реагування на кіберінциденти шляхом інтеграції SIEM та SOAR-рішень.

Для досягнення поставленої мети необхідно вирішити такі **завдання:**

- провести аналіз існуючих SIEM та SOAR-рішень і можливостей їх інтеграції;
- розробити архітектуру модуля підтримки реагування та реалізувати сценарії автоматизованого реагування;
- провести експериментальне дослідження ефективності запропонованого рішення.

Об’єкт дослідження - процес реагування на кіберінциденти в інформаційних системах.

Предмет дослідження - методи та засоби інтеграції SIEM та SOAR для автоматизації реагування на кіберінциденти.

Методи дослідження включають аналіз сучасних засобів моніторингу безпеки, моделювання архітектури інтегрованої системи, експериментальне оцінювання ефективності автоматизованого реагування та порівняння отриманих результатів із традиційними підходами.

Практичне значення роботи полягає у можливості використання розробленого модуля в корпоративних SOC та інформаційних системах організацій для підвищення швидкості й ефективності реагування на кіберінциденти.

Новизна роботи. Набув подальшого розвитку підхід до автоматизації процесів реагування на кіберінциденти в SOC шляхом інтеграції SIEM-системи IBM QRadar із механізмами автоматизованої обробки incidents та enrichment-процедурами, що за рахунок автоматичного отримання загроз(offenses), перевірки IP-адрес, аналізу результатів Nessus Vulnerability Management, створення білетів(ticket) і надсилання сповіщень дозволило скоротити час первинної обробки(triage) інцидентів на 40–60 % та зменшити навантаження на аналітиків SOC.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» 25 лютого 2026 року, де було представлено тези доповіді «Модуль підтримки реагування на кіберінциденти шляхом інтеграції SIEM та SOAR-рішень» [36].

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

1.1 Кіберінциденти та процеси реагування в системах інформаційної безпеки

Стрімкий розвиток інформаційних технологій та цифровізація бізнес-процесів призводять до постійного зростання кількості кіберзагроз і складності атак на інформаційні системи. Сучасні організації активно використовують хмарні сервіси, веб-застосунки, мобільні платформи та віддалений доступ до корпоративних ресурсів, що суттєво збільшує поверхню атаки[10]. У таких умовах забезпечення ефективного реагування на кіберінциденти є одним із ключових завдань системи інформаційної безпеки.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кіберінцидентом є подія або сукупність подій, що можуть призвести до порушення конфіденційності, цілісності чи доступності інформаційних ресурсів [1]. До основних видів кіберінцидентів належать:

- несанкціонований доступ до інформаційних систем;
- шкідливе програмне забезпечення;
- фішингові атаки;
- DDoS-атаки;
- витік конфіденційної інформації;
- компрометація облікових записів;
- внутрішні загрози.

Сучасні кібератаки часто мають складний багатоетапний характер та можуть залишатися непоміченими протягом тривалого часу. Це вимагає від організацій впровадження комплексних механізмів моніторингу та реагування, здатних оперативно виявляти аномалії та мінімізувати наслідки інцидентів [9].

Процес реагування на кіберінциденти є складовою системи управління інформаційною безпекою та включає сукупність організаційних і технічних

заходів, спрямованих на виявлення, аналіз, локалізацію та усунення загроз. Відповідно до ДСТУ ISO/IEC 27035:2018 [2, 9], життєвий цикл реагування на інциденти складається з таких етапів:

- підготовка до реагування;
- виявлення та реєстрація інциденту;
- оцінювання та класифікація;
- локалізація інциденту;
- усунення наслідків;
- відновлення роботи систем;
- післяінцидентний аналіз.

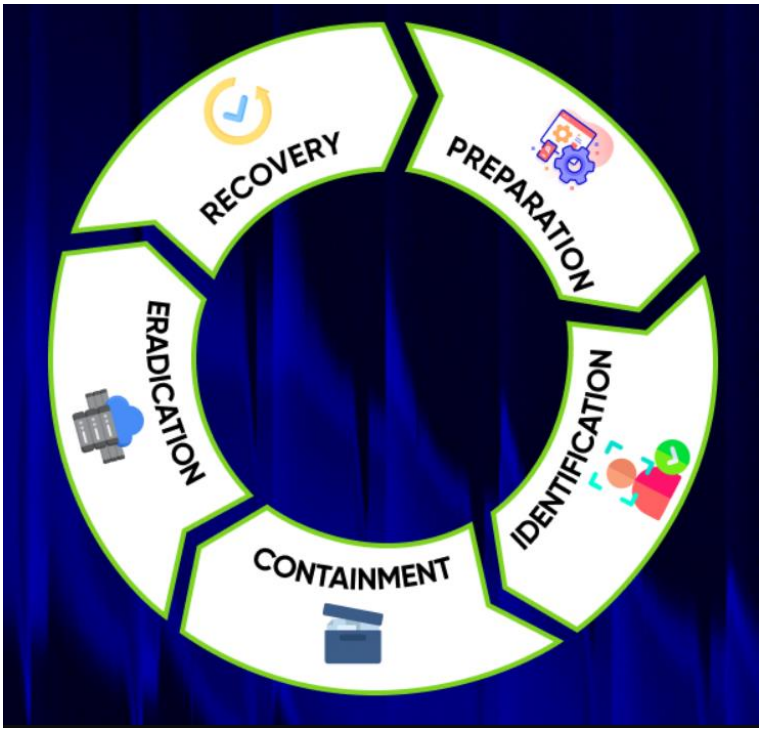

Рис.1.1. Основні етапи реагування на кіберінциденти

Ефективність реагування безпосередньо залежить від швидкості виявлення інциденту та своєчасності прийняття рішень. У сучасних інформаційних системах обсяг подій безпеки може досягати сотень тисяч записів за добу, що унеможливлює їх ручний аналіз. Саме тому важливу роль відіграють автоматизовані системи

моніторингу безпеки, здатні виконувати централізований збір та кореляцію подій [6, 7].

Крім технічних аспектів, процес реагування на кіберінциденти включає організаційні процедури, такі як визначення ролей і відповідальності персоналу, формування політик реагування та ведення документації щодо інцидентів. У більшості організацій ці функції реалізуються в межах центрів моніторингу безпеки (Security Operations Center, SOC) [8, 25].

Однією з основних проблем традиційних підходів реагування є значна залежність від людського фактора. Аналітики SOC змушені вручну аналізувати велику кількість сповіщень, перевіряти їх достовірність і приймати рішення щодо подальших дій. Це призводить до збільшення часу реагування, високого навантаження на персонал та ризику помилкової класифікації інцидентів [9].

Для підвищення ефективності реагування сучасні організації впроваджують системи автоматизації та оркестрації процесів інформаційної безпеки. Зокрема, широкого поширення набули рішення класу SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation and Response), які забезпечують автоматизований аналіз подій, централізоване управління інцидентами та реалізацію сценаріїв автоматизованого реагування [14, 16].

Використання сучасних підходів до автоматизації процесів моніторингу та реагування дозволяє скоротити час обробки інцидентів і підвищити ефективність роботи фахівців інформаційної безпеки. Саме тому інтеграція засобів аналізу подій та автоматизованого реагування є одним із ключових напрямів розвитку сучасних SOC.

1.2 Архітектура та функціональні можливості центрів моніторингу безпеки (SOC)

У сучасних умовах постійного зростання кількості кіберзагроз організації потребують не лише засобів захисту інформації, а й механізмів безперервного контролю за станом безпеки інформаційної інфраструктури. Для виконання цих завдань створюються центри моніторингу безпеки - Security Operations Center

(SOC), основною метою яких є виявлення, аналіз та реагування на кіберінциденти в режимі реального часу.

SOC являє собою комплекс організаційних, програмних і технічних засобів, а також фахівців з інформаційної безпеки, які здійснюють постійний моніторинг подій безпеки в інформаційній системі організації [8, 25]. Основне завдання SOC полягає у своєчасному виявленні загроз, мінімізації наслідків атак та забезпеченні стабільного функціонування інформаційної інфраструктури.

Архітектура SOC може відрізнятися залежно від масштабу організації, однак у більшості випадків вона включає кілька основних компонентів:

- системи збору журналів подій;
- платформи моніторингу та аналізу безпеки;
- засоби виявлення вторгнень;
- системи управління інцидентами;
- бази знань та Threat Intelligence;
- засоби автоматизації реагування.

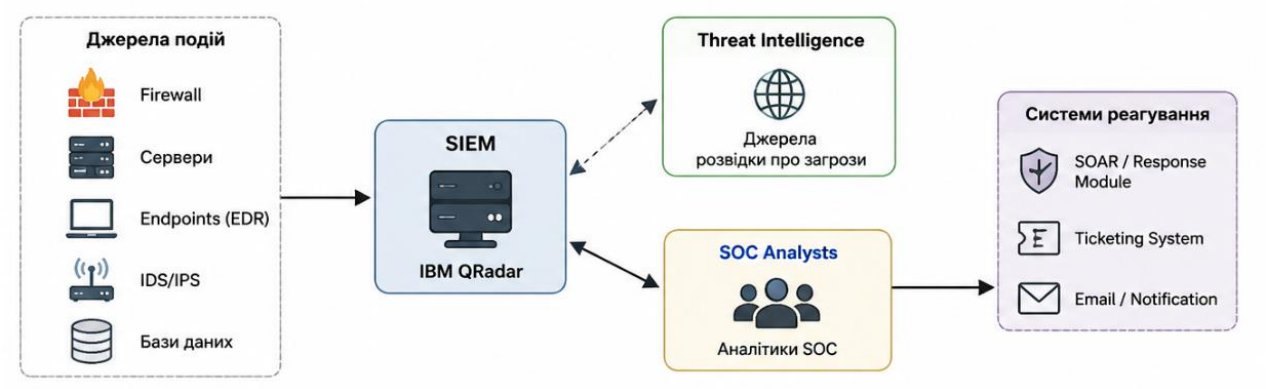

Рис.1.2. Типова архітектура центру моніторингу безпеки (SOC)

Одним із ключових компонентів SOC є SIEM-система, яка виконує централізований збір журналів подій із різних джерел: серверів, мережевого обладнання, між мережевих екранів, антивірусних рішень, систем контролю доступу та кінцевих пристроїв. Отримані дані приводяться до єдиного формату,

після чого система виконує їх аналіз і кореляцію для виявлення підозрілої активності [6, 7].

Важливою складовою роботи SOC є процес кореляції подій. Його сутність полягає у виявленні взаємозв'язків між окремими подіями безпеки, які самі по собі можуть не виглядати небезпечними. Наприклад, декілька невдалих спроб автентифікації, підключення з незвичної IP-адреси та підвищення привілеїв користувача можуть свідчити про компрометацію облікового запису.

Залежно від рівня зрілості організації виділяють декілька моделей SOC:

- внутрішній SOC, який повністю функціонує в межах організації;
- аутсорсинговий SOC, де функції моніторингу передаються зовнішньому провайдеру;
- гібридний SOC, що поєднує внутрішні та зовнішні ресурси.

Крім цього, сучасні SOC активно використовують підходи Threat Intelligence - отримання та аналіз інформації про актуальні загрози, шкідливі IP-адреси, домени, хеші файлів та тактики зловмисників. Це дозволяє оперативніше виявляти атаки та підвищувати точність аналізу подій безпеки [23, 31].

Важливу роль у функціонуванні SOC відіграють аналітики безпеки. Зазвичай структура центру моніторингу включає кілька рівнів спеціалістів:

- аналітики першої лінії (L1), які здійснюють первинний аналіз сповіщень;
- аналітики другої лінії (L2), які проводять детальне дослідження інцидентів;
- експерти третьої лінії (L3), які займаються складними атаками та цифровою криміналістикою.

Проте зі збільшенням кількості подій безпеки традиційні SOC стикаються з низкою проблем. Основними серед них є:

- велика кількість хибнопозитивних спрацювань;
- перевантаження аналітиків;
- тривалий час реагування;

- складність інтеграції різних засобів захисту;
- значна кількість ручних операцій.

Для вирішення цих проблем сучасні центри моніторингу безпеки поступово переходять до використання автоматизованих підходів реагування. Саме тому останніми роками активно впроваджуються SOAR-платформи, які дозволяють автоматизувати виконання типових дій у відповідь на інциденти, координувати взаємодію між засобами захисту та зменшувати навантаження на фахівців SOC [8, 26].

Ефективність роботи SOC значною мірою залежить від рівня автоматизації процесів аналізу та реагування на інциденти. Зі збільшенням кількості подій безпеки традиційні підходи вже не забезпечують необхідної швидкості обробки, що обумовлює активне впровадження SIEM та SOAR-рішень.

1.3 Принципи роботи та можливості SIEM і SOAR-рішень

У сучасних умовах забезпечення кібербезпеки організації використовують спеціалізовані системи моніторингу та реагування на інциденти, які дозволяють автоматизувати аналіз подій безпеки та підвищити ефективність роботи центрів моніторингу безпеки. Найбільш поширеними рішеннями в цій сфері є платформи класу SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation and Response) [7, 14].

SIEM-системи призначені для централізованого збору, обробки та аналізу журналів подій, що надходять із різних джерел інформаційної інфраструктури. До таких джерел належать сервери, маршрутизатори, міжмережеві екрани, системи виявлення вторгнень, антивірусне програмне забезпечення, кінцеві пристрої користувачів та хмарні сервіси. Основною метою SIEM є виявлення підозрілої активності та формування сповіщень про потенційні інциденти інформаційної безпеки.

Принцип роботи SIEM базується на кількох основних процесах [6, 7]:

- збір журналів подій;
- нормалізація даних;

- кореляція подій;
- аналіз активності;
- формування сповіщень та звітів.

Після надходження подій система приводить їх до єдиного формату для подальшої обробки. Це дозволяє аналізувати інформацію незалежно від типу джерела або програмного забезпечення. Одним із найважливіших механізмів SIEM є кореляція подій, яка дозволяє виявляти взаємозв'язки між різними подіями безпеки та формувати цілісне уявлення про потенційну атаку [6].

Наприклад, окремі події у вигляді декількох невдалих спроб автентифікації можуть не становити значної загрози. Проте якщо такі події супроводжуються успішним входом у систему з нетипової IP-адреси та подальшим підвищенням привілеїв, це може свідчити про компрометацію облікового запису користувача.

Сучасні SIEM-рішення також забезпечують [11, 17]:

- моніторинг подій у режимі реального часу;
- візуалізацію даних;
- централізоване зберігання журналів;
- формування звітності;
- підтримку Threat Intelligence;
- аудит подій інформаційної безпеки.

Серед найбільш поширених SIEM-платформ можна виділити Splunk Enterprise Security, IBM QRadar SIEM, ArcSight та Microsoft Sentinel. Дані рішення відрізняються архітектурою та функціональними можливостями, проте мають спільну мету - забезпечення централізованого контролю за станом інформаційної безпеки організації.

Під час практичної роботи з IBM QRadar SIEM було встановлено, що система забезпечує ефективний аналіз мережевої активності, централізований моніторинг подій безпеки та автоматичне формування offenses на основі правил кореляції. Використання механізмів Log Activity, Assets та Log Sources дозволяє аналітикам

SOC швидко визначати джерела підозрілої активності та виконувати первинний аналіз інцидентів [11, 12].

Водночас використання SIEM-систем має певні обмеження. Однією з основних проблем є велика кількість сповіщень, що потребують ручного аналізу з боку аналітиків SOC. Значна кількість хибно позитивних спрацювань створює додаткове навантаження на персонал та збільшує час реагування на реальні інциденти.

Практичний досвід роботи з offenses у QRadar показує, що навіть за наявності автоматизованих правил кореляції значна частина подій потребує додаткової ручної перевірки. Зокрема, аналізу потребують інциденти, пов’язані з аномальною мережевою активністю, підозрілими підключеннями та спробами несанкціонованого доступу. Це ускладнює оперативне реагування та підвищує актуальність автоматизації процесів аналізу й обробки інцидентів.

Для вирішення зазначених проблем використовуються SOAR-платформи, основною метою яких є автоматизація реагування на кіберінциденти та координація взаємодії між різними засобами інформаційної безпеки [14, 16, 26].

SOAR-системи дозволяють автоматизувати виконання типових дій реагування за допомогою спеціальних сценаріїв - playbooks. Такі сценарії визначають послідовність дій, які виконуються після виникнення певного типу інциденту. Наприклад, система може автоматично:

- перевірити IP-адресу через Threat Intelligence;
- виконати аналіз репутації файлу;
- заблокувати користувацький обліковий запис;
- ізолювати кінцевий пристрій;
- створити інцидент у системі ticketing;
- повідомити відповідальних фахівців.

Однією з ключових переваг SOAR є можливість інтеграції з різними компонентами інфраструктури через API. Це дозволяє створювати єдину систему управління інцидентами, у межах якої засоби моніторингу, захисту та реагування взаємодіють між собою автоматично [14, 15].

Серед найбільш поширених SOAR-рішень можна виділити Splunk SOAR, IBM Security SOAR та Cortex XSOAR. Дані платформи підтримують автоматизацію реагування, централізоване керування інцидентами та інтеграцію з великою кількістю засобів кіберзахисту.

Додатково для підвищення ефективності реагування можуть використовуватись системи управління вразливостями, зокрема Nessus Vulnerability Management. Інтеграція даних про вразливості із SIEM та SOAR дозволяє враховувати критичність активів і наявність відомих CVE під час визначення пріоритетності інцидентів [20, 21].

Інтеграція SIEM та SOAR дозволяє реалізувати повний цикл реагування на кіберінциденти - від виявлення події до автоматичного виконання заходів реагування. У такій моделі SIEM виконує функції збору та аналізу подій безпеки, а SOAR забезпечує автоматизацію подальших дій та координацію взаємодії між різними компонентами системи захисту.

Рис.1.3. Схема взаємодії SIEM та SOAR у процесі реагування на інциденти

Інтеграція SIEM та SOAR дозволяє не лише централізувати моніторинг подій безпеки, а й автоматизувати значну частину процесів реагування на інциденти. Це знижує навантаження на аналітиків SOC та забезпечує більш оперативну обробку критичних подій.

1.4 Аналіз сучасних SIEM та SOAR-платформ і проблем інтеграції

У сучасних системах кіберзахисту платформи класу SIEM та SOAR є основними компонентами центрів моніторингу безпеки. Їх використання дозволяє

організаціям централізовано контролювати події безпеки, автоматизувати процеси реагування та підвищувати ефективність роботи SOC. Водночас велика кількість доступних рішень відрізняється функціональними можливостями, підходами до інтеграції та рівнем автоматизації, що потребує проведення порівняльного аналізу [11, 12, 13].

Одним із найбільш відомих SIEM-рішень є IBM QRadar SIEM. Дана платформа забезпечує централізований збір журналів подій, аналіз мережевої активності та механізми кореляції подій безпеки. Однією з ключових особливостей QRadar є система offenses, яка дозволяє об’єднувати пов’язані події в єдиний інцидент для подальшого аналізу аналітиками SOC. Також система підтримує роботу з Log Sources та Assets, що дозволяє структурувати інформацію про джерела подій та активи організації.

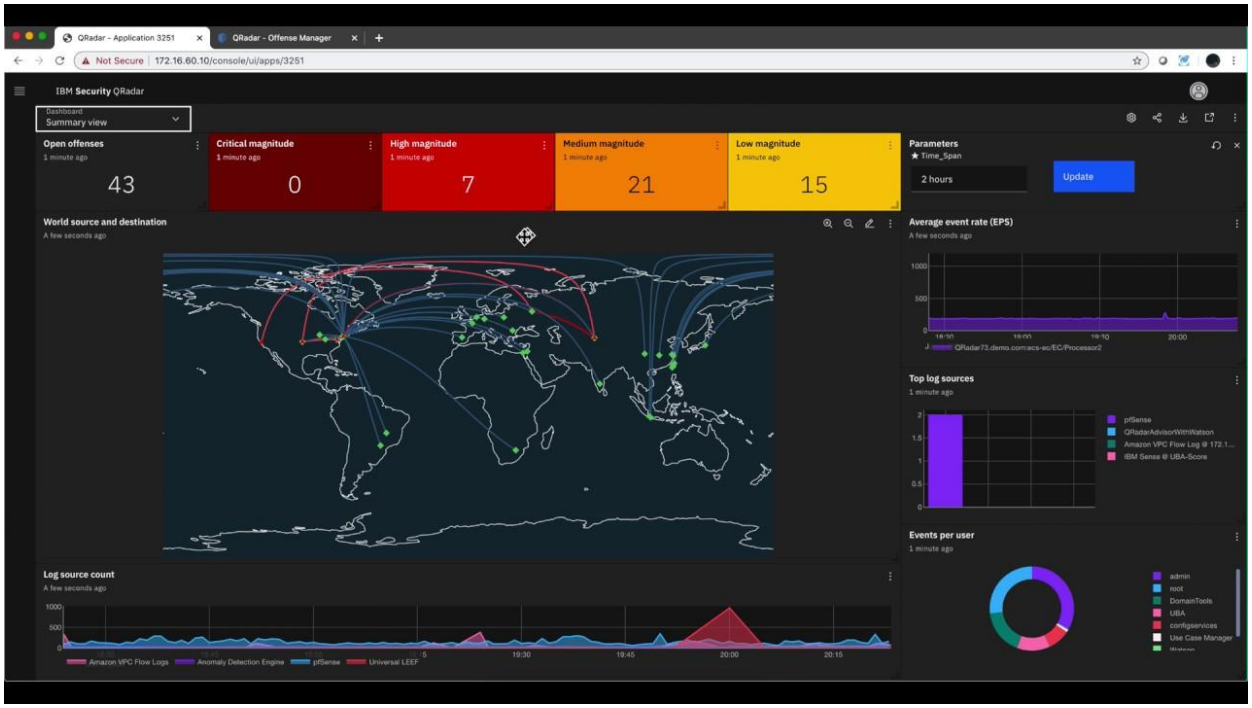

Рис.1.4. Інтерфейс розширення Pulse Dashboard у Qradar

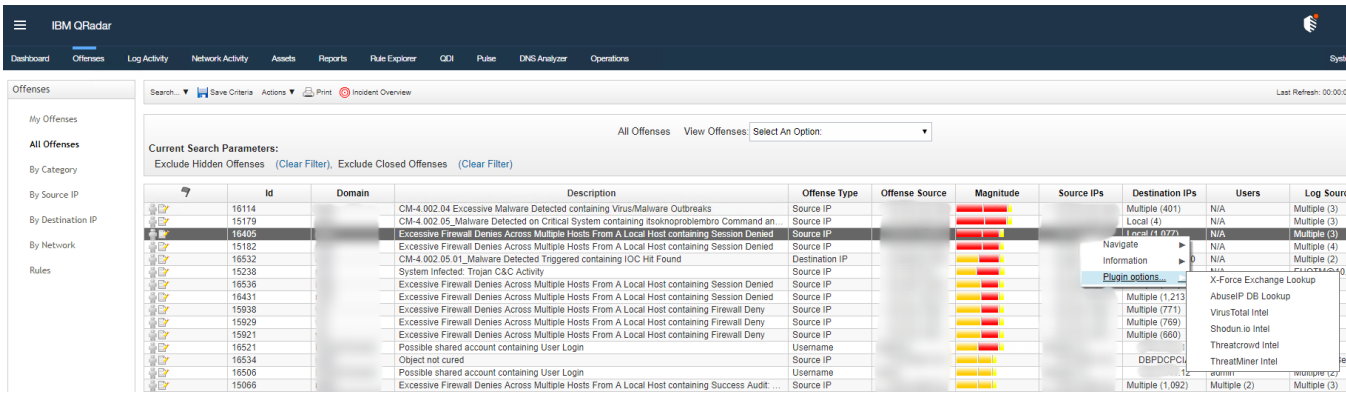

Рис.1.5. Вкладка Offense у Qradar

Практичний досвід використання QRadar показує, що система ефективно виконує централізований моніторинг подій та виявлення підозрілої активності. Водночас значна частина процесів аналізу та реагування все ще потребує ручної участі аналітиків SOC. Зокрема, додатковий час витрачається на перевірку індикаторів компрометації, аналіз мережевої активності та виконання типових дій реагування.

Ще одним поширеним SIEM-рішенням є Splunk Enterprise Security, яке відзначається широкими можливостями обробки великих обсягів даних, гнучкими механізмами пошуку та розвинутими засобами візуалізації інформації. Платформа дозволяє створювати складні правила кореляції та підтримує інтеграцію з великою кількістю зовнішніх сервісів [17, 28].

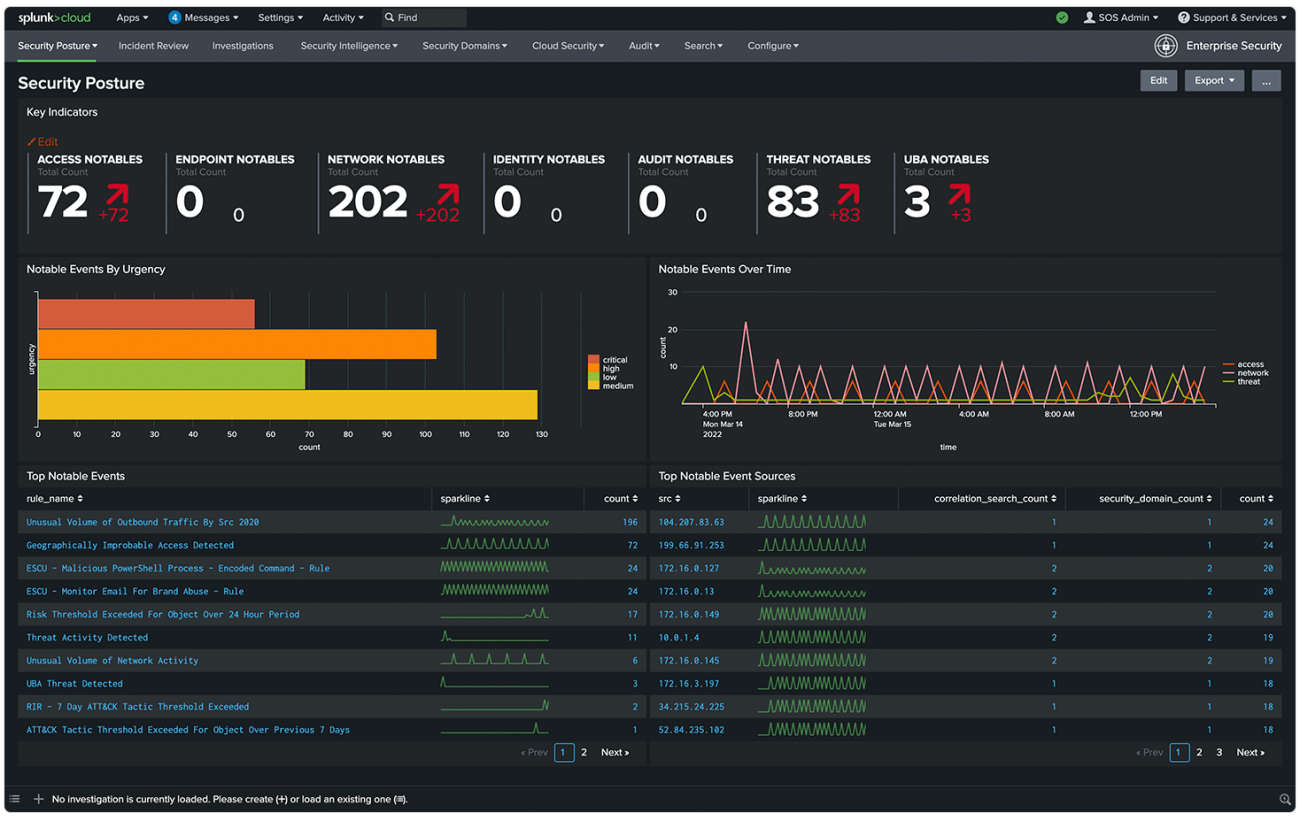

Рис.1.6. Головний інтерфейс Splunk Enterprise Security

Microsoft Sentinel є хмарним SIEM-рішенням, орієнтованим на інтеграцію з сервісами Microsoft Azure та Microsoft 365. Перевагами платформи є масштабованість, підтримка хмарної інфраструктури та можливість використання вбудованих механізмів аналітики на основі штучного інтелекту [18, 19].

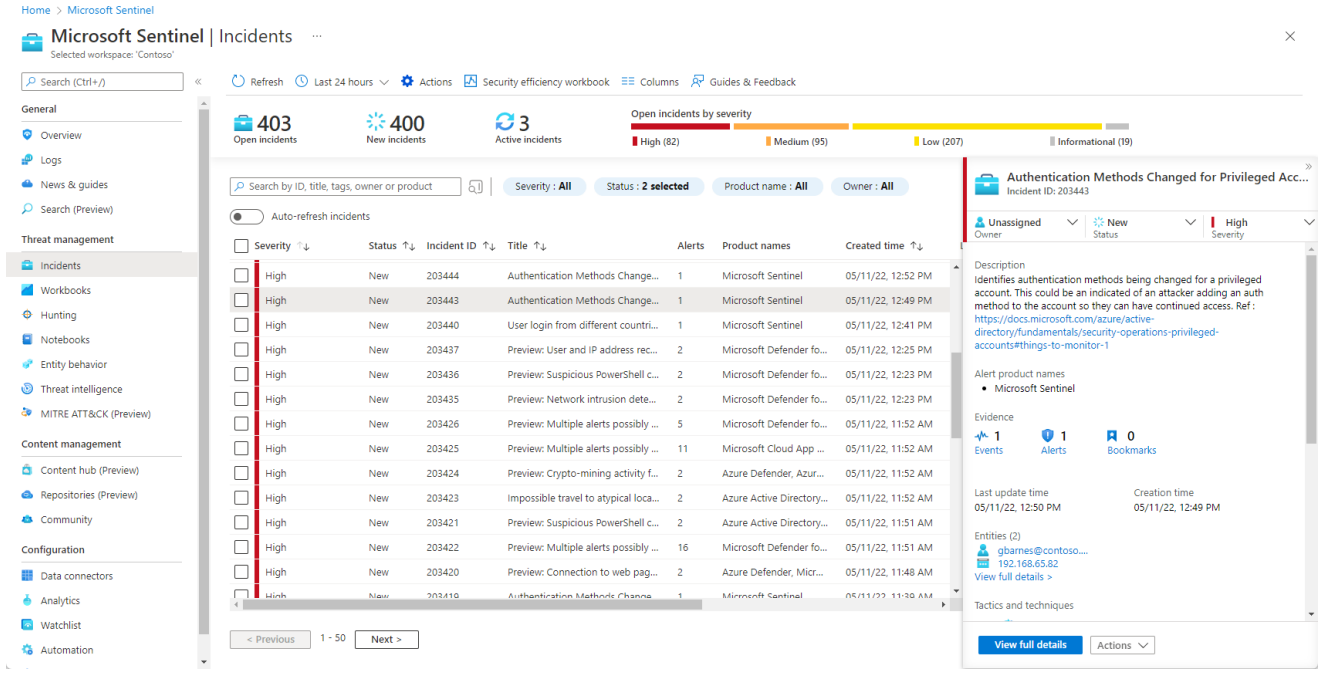

Рис.1.7. Інтерфейс Incidents у Microsoft Sentinel

Серед SOAR-платформ найбільш поширеними є IBM Security SOAR, Splunk SOAR та Cortex XSOAR. Основною функцією таких систем є автоматизація реагування на інциденти за допомогою playbooks - сценаріїв, що визначають послідовність дій під час виникнення певних типів загроз.

IBM Security SOAR забезпечує централізоване управління інцидентами та підтримує інтеграцію з продуктами IBM Security, зокрема QRadar. Це дозволяє автоматизувати передачу offenses до системи реагування та виконувати типові дії без участі аналітика [14, 30].

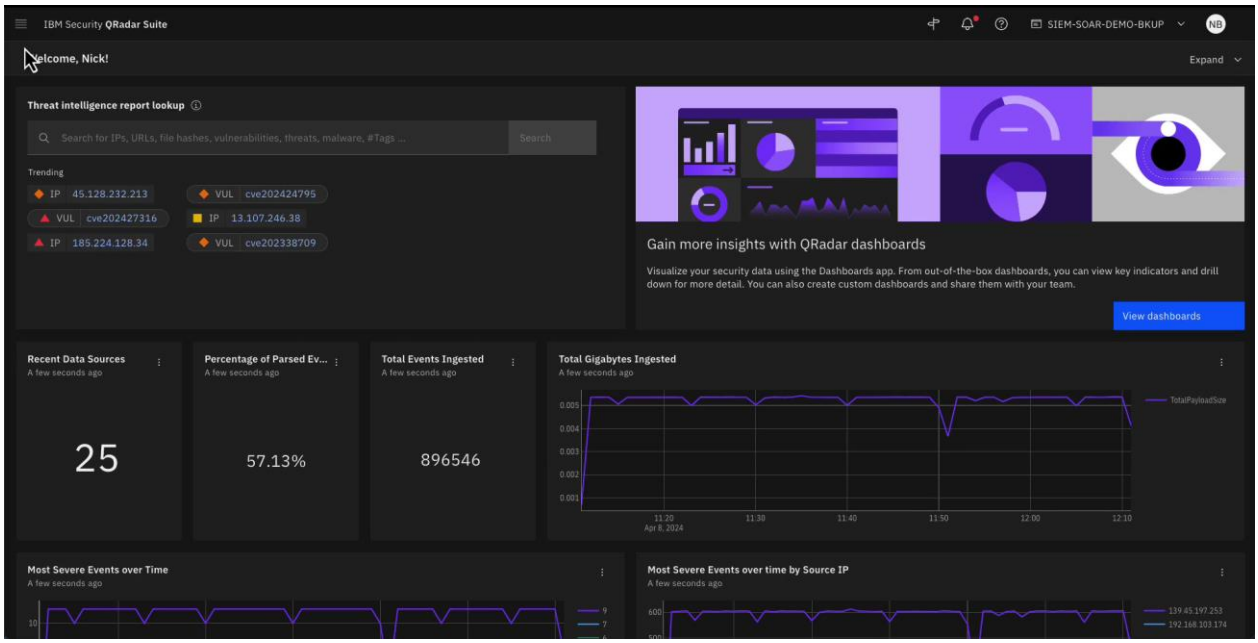

Рис.1.8. Інтерфейс IBM Security SOAR

Splunk SOAR орієнтований на автоматизацію процесів обробки інцидентів та інтеграцію з великою кількістю сторонніх сервісів. Платформа підтримує побудову складних сценаріїв реагування та централізоване управління робочим процесом(workflow) безпеки.

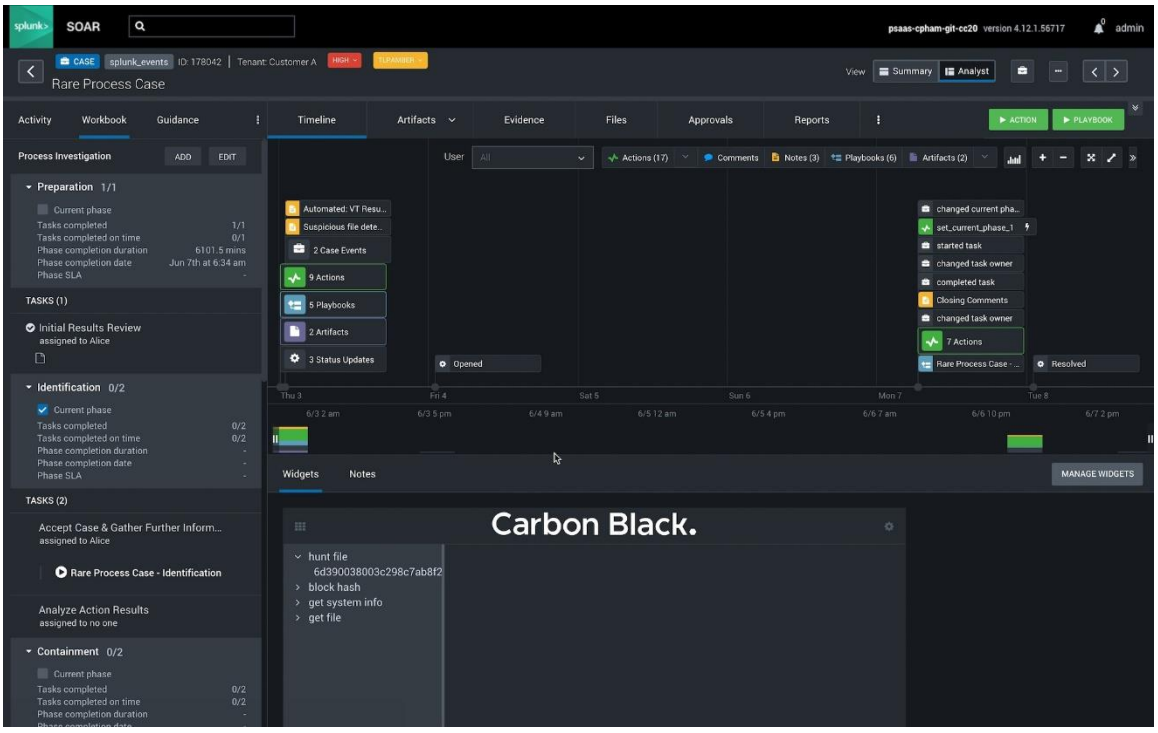

Рис.1.9. Інтерфейс Splunk SOAR

Cortex XSOAR забезпечує високий рівень автоматизації та підтримує інтеграцію із засобами захисту різних виробників. Однією з особливостей рішення є використання єдиного інтерфейсу для управління інцидентами, Threat Intelligence та сценаріями реагування [15].

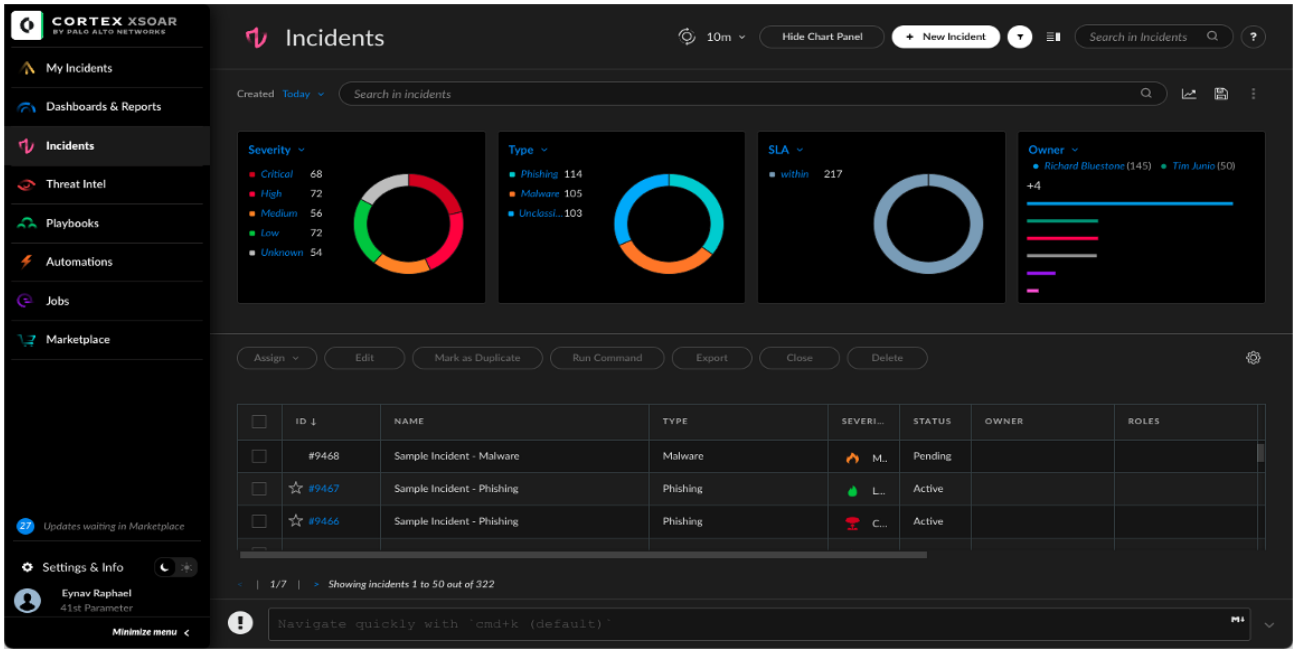

Рис.1.10. Інтерфейс Cortex XSOAR

Таблиця 1.1.

Порівняльна характеристика SIEM та SOAR-рішень

Рішення	**Тип**	**Переваги**	**Недоліки**	**Інтеграція (API)**	**Автоматизація**
IBM QRadar	SIEM	Розвинена кореляція подій, offenses, інтеграція з IBM Security	Високі вимоги до налаштування	REST API	Часткова
Splunk Enterprise Security	SIEM	Гнучкий пошук та аналітика	Висока вартість	REST API	Часткова

Продовження таблиці 1.1.

Рішення	**Тип**	**Переваги**	**Недоліки**	**Інтеграція (API)**	**Автоматизація**
Microsoft Sentinel	SIEM	Хмарна архітектура, інтеграція з Azure	Залежність від Microsoft ecosystem	API	Часткова
IBM Security SOAR	SOAR	Автоматизація incident response	Складність впровадження	Широка інтеграція	Висока
Cortex XSOAR	SOAR	Велика кількість playbooks	Складність адміністрування	API	Висока

На основі проведеного аналізу встановлено, що сучасні SIEM та SOAR-рішення забезпечують високий рівень централізованого моніторингу та автоматизації реагування, проте впровадження повноцінних SOAR-платформ часто супроводжується складністю інтеграції та значними витратами. У зв’язку з цим доцільним є використання модулів підтримки реагування, інтегрованих із SIEM-платформами.

Попри значні можливості сучасних платформ, інтеграція SIEM та SOAR-рішень супроводжується низкою проблем. Однією з основних є складність взаємодії між продуктами різних виробників. У багатьох випадках інтеграція потребує використання API, налаштування конекторів та адаптації форматів даних [12, 14, 15].

Ще однією проблемою є неоднорідність журналів подій і форматів передачі інформації. Різні системи можуть використовувати власні формати логування, що ускладнює нормалізацію та коректну кореляцію подій. Це особливо актуально у великих інфраструктурах, де використовується значна кількість різнорідних засобів захисту.

Важливою проблемою також залишається велика кількість хибно позитивних спрацювань. Навіть сучасні SIEM-платформи можуть генерувати значну кількість

подій, які не становлять реальної загрози. У результаті аналітики SOC змушені витрачати значний час на перевірку таких спрацювань.

Крім цього, автоматизація реагування потребує чіткого визначення сценаріїв обробки інцидентів. Неправильно налаштовані playbooks можуть призводити до помилкових дій, зокрема блокування легітимних користувачів або ізоляції критичних систем.

Окрему роль у процесах реагування відіграють системи управління вразливостями, наприклад Nessus Vulnerability Management [20, 21]. Використання даних про наявні вразливості дозволяє більш точно оцінювати критичність інцидентів та визначати пріоритетність реагування. Інтеграція результатів сканування вразливостей із SIEM та SOAR забезпечує додатковий контекст для прийняття рішень під час обробки інцидентів.

На основі проведеного аналізу встановлено, що сучасні SIEM-платформи забезпечують ефективний централізований моніторинг подій безпеки та підтримують механізми кореляції incidents, проте значна частина процесів реагування все ще потребує ручної участі аналітиків SOC. SOAR-рішення дозволяють автоматизувати типові workflow реагування, однак їх впровадження часто супроводжується складністю інтеграції та додатковими витратами.

У результаті аналізу було визначено доцільність розробки модуля підтримки реагування, орієнтованого на інтеграцію IBM QRadar із механізмами автоматизованої обробки incidents та використанням даних vulnerability management. Такий підхід дозволяє поєднати можливості централізованого моніторингу SIEM та автоматизації SOAR без необхідності впровадження окремої повноцінної SOAR-платформи [11, 14].

Висновки до розділу 1

У першому було проведено аналіз сучасних підходів до реагування на кіберінциденти та особливостей функціонування центрів моніторингу безпеки SOC. Розглянуто основні етапи процесу incident response, включаючи виявлення,

аналіз, локалізацію, усунення наслідків інциденту та відновлення працездатності інформаційних систем.

У межах дослідження проаналізовано принципи роботи SIEM та SOAR-рішень, їх функціональні можливості та роль у забезпеченні централізованого моніторингу й автоматизації процесів реагування на кіберінциденти. Особливу увагу приділено SIEM-платформам IBM QRadar, Splunk Enterprise Security та Microsoft Sentinel, а також SOAR-рішенням IBM Security SOAR і Cortex XSOAR.

У результаті порівняльного аналізу встановлено, що сучасні SIEM-системи забезпечують ефективний збір та кореляцію подій безпеки, однак значна частина процесів incident response все ще виконується вручну аналітиками SOC. Водночас використання механізмів автоматизації та orchestration дозволяє скоротити час обробки incidents, зменшити навантаження на персонал та підвищити узгодженість workflow реагування.

Також у першому розділі було проаналізовано можливості інтеграції SIEM-платформ із системами vulnerability management, зокрема Nessus Vulnerability Management. Визначено, що використання даних про вразливості дозволяє підвищити точність оцінювання критичності інцидентів та оптимізувати процес визначення пріоритетності реагування.

На основі проведеного аналізу обґрунтовано доцільність розробки модуля підтримки реагування на кіберінциденти, побудованого на інтеграції IBM QRadar, механізмів автоматизованої обробки incidents та даних vulnerability management. Отримані результати стали основою для розробки архітектури та практичної реалізації запропонованого рішення у наступних розділах роботи.

РОЗДІЛ 2. РОЗРОБКА МОДУЛЯ ПІДТРИМКИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

2.1 Архітектура інтеграції SIEM та SOAR

Ефективність сучасних центрів моніторингу безпеки значною мірою залежить від швидкості обробки подій безпеки та оперативності реагування на кіберінциденти. У традиційних SOC значна частина дій виконується вручну аналітиками, що призводить до збільшення часу реагування та підвищення навантаження на персонал. Для вирішення цієї проблеми доцільним є використання підходів автоматизації та оркестрації процесів реагування, реалізованих у SOAR-рішеннях [14-16, 36].

У межах даної роботи запропоновано архітектуру модуля підтримки реагування на кіберінциденти, побудовану на основі інтеграції SIEM-платформи IBM QRadar та механізмів автоматизованого реагування. Основною метою розробленого модуля є скорочення часу обробки інцидентів, автоматизація типових дій аналізу та зменшення навантаження на аналітиків SOC.

Запропонована архітектура включає такі основні компоненти [20, 21]:

- джерела подій безпеки;
- SIEM-платформу IBM QRadar;
- модуль підтримки реагування;
- систему аналізу вразливостей Nessus Vulnerability Management;
- механізм автоматизованого створення ticket;
- інтерфейс взаємодії з аналітиком SOC.

На першому етапі журнали подій надходять до QRadar із різних компонентів інформаційної інфраструктури:

- серверів;
- мережевого обладнання;
- міжмережевих екранів;
- кінцевих пристроїв;

- систем захисту інформації.

Після отримання подій QRadar виконує їх нормалізацію, аналіз та кореляцію [11, 12]. У разі виявлення підозрілої активності система автоматично формує offense, який містить інформацію про тип загрози, джерело події, задіяні активи та рівень потенційного ризику.

Наступним етапом є передача offense до модуля підтримки реагування через API-взаємодію. Для цього використовується REST API QRadar, що дозволяє отримувати інформацію про активні offenses, їх параметри та пов’язані події. Використання API забезпечує автоматизований обмін даними між SIEM та модулем реагування без необхідності ручного втручання.

Після отримання offense модуль виконує процедуру доповнення інциденту додатковими даними(enrichment) [23]. У межах роботи реалізовано такі механізми:

- перевірка IP-адрес;
- аналіз репутації мережевих індикаторів;
- перевірка активів на наявність відомих вразливостей;
- визначення критичності активу.

Для отримання інформації про вразливості використовується Nessus Vulnerability Management. Модуль аналізує результати сканування та визначає наявність критичних CVE для активу, який бере участь в інциденті. Якщо система виявляє висококритичні вразливості, рівень пріоритету incident response автоматично підвищується [20, 21].

Однією з ключових функцій модуля є автоматизована пріоритезація інцидентів. Визначення критичності виконується на основі:

- severity(серйозності) offense у QRadar;
- наявності критичних CVE;
- типу активу;
- характеру мережевої активності;
- результатів перевірки IP-адрес.

Такий підхід дозволяє зменшити кількість інцидентів, які потребують ручної перевірки, та забезпечити концентрацію уваги аналітиків на найбільш небезпечних загрозах.

Після завершення аналізу модуль автоматично ініціює подальші дії реагування. У межах запропонованої архітектури реалізовано механізм автоматичного створення ticket для подальшої обробки інциденту аналітиком SOC. Ticket містить:

- ідентифікатор offense;
- опис інциденту;
- рівень критичності;
- результати доповнення;
- рекомендації щодо реагування.

Автоматизація створення ticket дозволяє скоротити час первинного сортування(triage) та стандартизувати процес обробки інцидентів [14, 16].

Особливістю запропонованої архітектури є використання SOAR-підходу без необхідності впровадження окремої повноцінної SOAR-платформи. Функції оркестрації та автоматизації реалізуються безпосередньо в модулі підтримки реагування, який взаємодіє з QRadar та іншими компонентами інфраструктури через API.

Запропонована архітектура забезпечує:

- централізований аналіз подій безпеки;
- автоматизацію обробки інцидентів;
- інтеграцію даних про вразливості;
- скорочення часу реагування;
- зниження навантаження на аналітиків SOC.

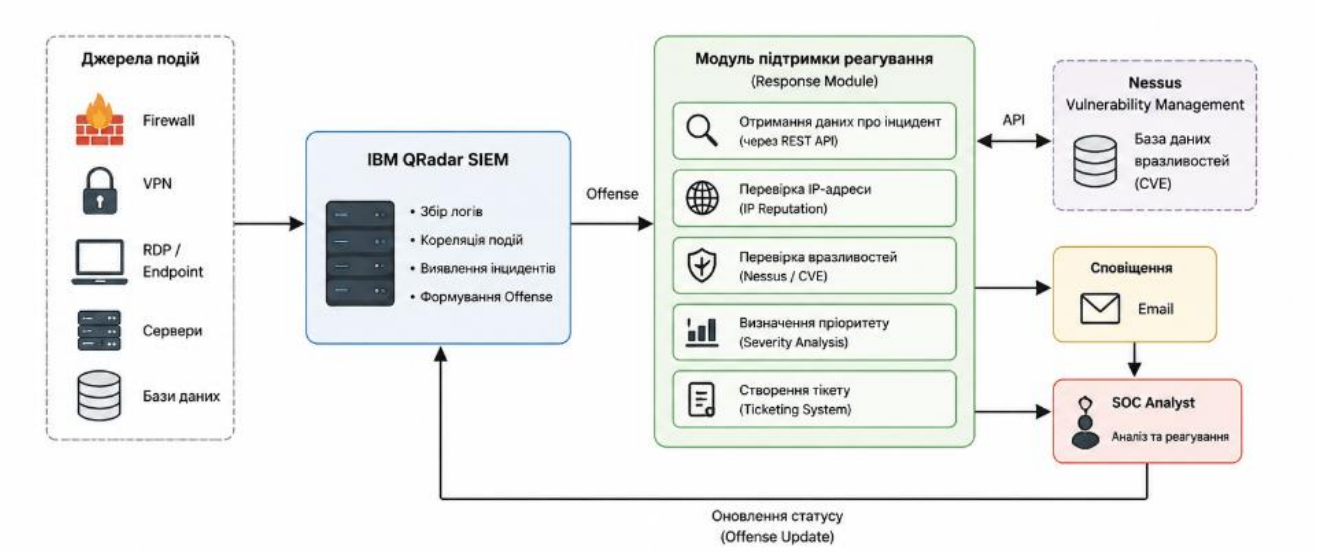

Рис. 2.1. Архітектура модуля підтримки реагування на кіберінциденти

Запропонована архітектура забезпечує централізовану обробку інцидентів, автоматизацію типових дій реагування та інтеграцію даних про вразливості в єдиний workflow SOC. Це дозволяє скоротити час triage та спростити роботу аналітиків під час обробки подій безпеки.

2.2 Модель обробки та класифікації кіберінцидентів

Одним із ключових елементів ефективного реагування на кіберінциденти є правильна організація процесу обробки подій безпеки та визначення їх пріоритетності. У сучасних SOC кількість подій, які надходять до SIEM-систем, може досягати десятків або сотень тисяч на добу, що значно ускладнює ручний аналіз усіх спрацювань. У таких умовах особливо важливим є використання механізмів автоматизованої класифікації та пріоритезації інцидентів [6, 7].

У межах даної роботи запропоновано модель обробки кіберінцидентів, побудовану на інтеграції SIEM-платформи IBM QRadar, даних про вразливості з Nessus Vulnerability Management та модуля автоматизованого реагування. Основною метою моделі є скорочення часу triage, зменшення навантаження на аналітиків SOC та автоматизація виконання типових дій реагування.

Запропонована модель складається з кількох основних етапів [11, 20]:

- отримання та аналіз offense;

- enrichment інциденту;
- визначення критичності;
- автоматизоване реагування;
- створення ticket та сповіщення аналітика.

На першому етапі QRadar виконує збір і кореляцію подій безпеки з різних джерел інфраструктури. У разі спрацювання правила кореляції система формує offense, який містить інформацію про тип підозрілої активності, джерело події, IP-адреси, задіяні активи та базовий рівень severity.

Після формування offense модуль підтримки реагування отримує дані через REST API QRadar [12]. На цьому етапі здійснюється первинний аналіз інциденту та перевірка параметрів offense, зокрема:

- категорії інциденту;
- типу мережевої активності;
- джерела події;
- рівня severity;
- активів, що беруть участь в інциденті.

Наступним етапом є enrichment інциденту - доповнення offense додатковими даними, необхідними для більш точної оцінки ризику. У межах запропонованої моделі реалізовано [23]:

- перевірку репутації IP-адрес;
- перевірку активів на наявність критичних вразливостей;
- аналіз результатів сканування Nessus;
- визначення критичності активу.

Використання даних із Nessus Vulnerability Management дозволяє враховувати наявність відомих CVE під час аналізу інциденту. Якщо актив, що бере участь у suspicious activity, містить критичні або високоризикові вразливості, модуль підвищує пріоритетність реагування [20, 21].

У межах моделі пріоритетність інцидентів визначається на основі:

- severity offense у QRadar;

- наявності критичних CVE;
- типу активу;
- рівня потенційного ризику;
- характеру підозрілої активності.

Такий підхід дозволяє більш ефективно розподіляти навантаження між аналітиками SOC та концентрувати увагу на найбільш небезпечних інцидентах.

Для спрощення обробки подій у моделі використовується умовний поділ інцидентів на три категорії [9]:

- низький пріоритет;
- середній пріоритет;
- високий пріоритет.

Інциденти низького пріоритету можуть потребувати лише моніторингу або додаткової перевірки. Події середнього рівня ризику передаються аналітикам SOC для подальшого аналізу. У разі високого пріоритету система автоматично ініціює процедури реагування та створює відповідний ticket.

Після завершення enrichment модуль виконує автоматизовані дії реагування.

У межах роботи реалізовано:

- автоматичне створення ticket;
- надсилання email-сповіщення;
- оновлення інформації в offense QRadar.

Ticket містить:

- ідентифікатор offense;
- короткий опис інциденту;
- рівень критичності;
- результати перевірки IP-адрес;
- інформацію про виявлені вразливості;
- рекомендації щодо подальших дій.

Email-повідомлення надсилається аналітикам SOC для оперативного інформування про критичні інциденти. Додатково модуль оновлює offense у

QRadar шляхом додавання нотатків(note) або результатів доповнення, що дозволяє централізовано зберігати інформацію про процес реагування.

Запропонована модель забезпечує:

- скорочення часу сортування;
- зменшення кількості ручних операцій;
- автоматизацію аналізу інцидентів;
- централізоване управління інформацією про реагування;
- підвищення ефективності роботи SOC.

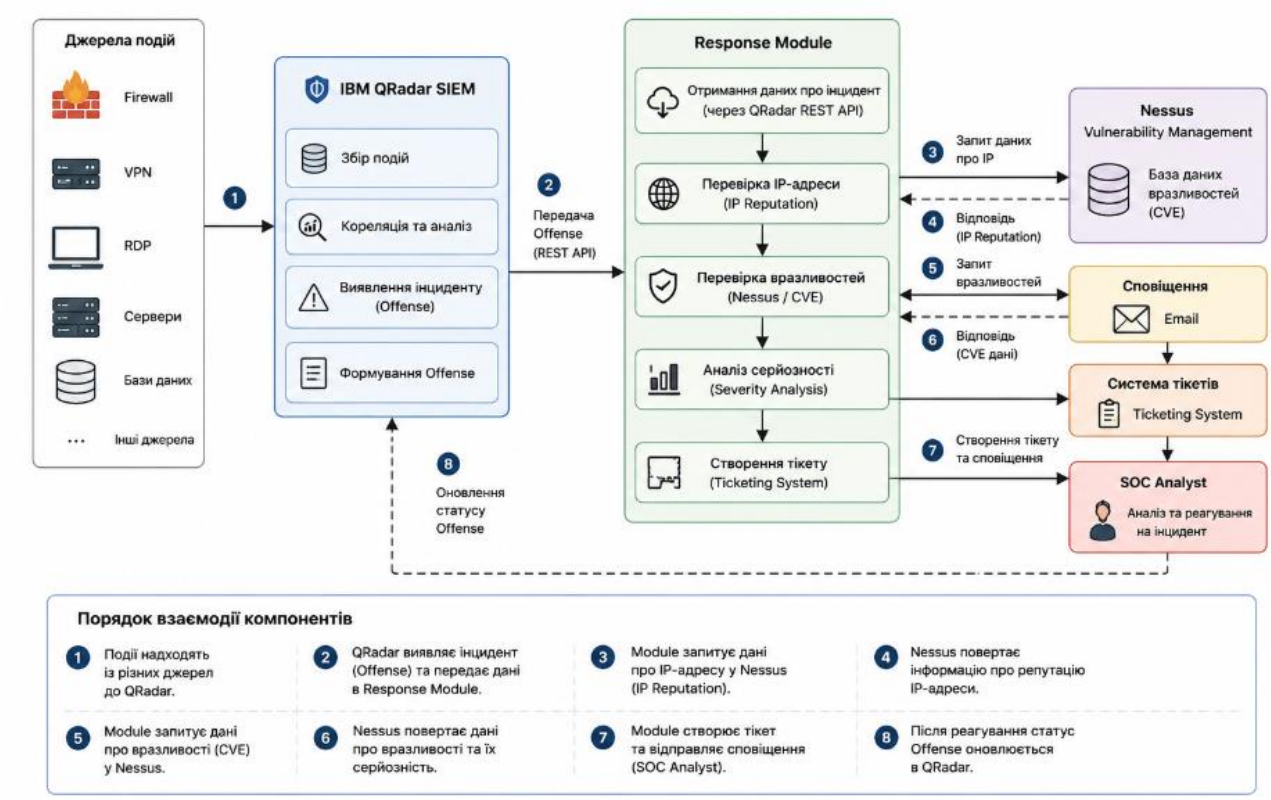

Рис. 2.2. Схема взаємодії компонентів запропонованого рішення

На відміну від традиційного підходу, де значна частина дій виконується вручну, запропонована модель дозволяє автоматизувати обробку типових інцидентів та мінімізувати вплив людського фактора.

Запропонований підхід дозволяє автоматизувати значну частину процесів первинного аналізу інцидентів та створює основу для подальшої реалізації сценаріїв автоматизованого реагування в межах SOC.

2.3 Розробка сценаріїв автоматизованого реагування

Одним із ключових елементів сучасних SOAR-підходів є використання сценаріїв автоматизованого реагування – playbooks [14-16, 36]. Їх основним призначенням є автоматизація типових дій під час обробки інцидентів інформаційної безпеки, зменшення навантаження на аналітиків SOC та скорочення часу реагування на загрози.

У межах даної роботи playbooks реалізуються в модулі підтримки реагування та використовуються для автоматичної обробки offenses, отриманих із IBM QRadar. Запропонований підхід дозволяє частково автоматизувати процес сортування та забезпечити централізоване виконання типових дій реагування.

Розроблені сценарії реагування орієнтовані на обробку інцидентів, пов’язаних із:

- підозрілою мережевою активністю;
- спробами несанкціонованого доступу;
- аномальною поведінкою користувачів;
- спрацюваннями правил кореляції SIEM;
- виявленням потенційно скомпрометованих активів.

Загальна логіка роботи playbook складається з кількох послідовних етапів:

- Отримання offense із QRadar.
- Первинний аналіз параметрів інциденту.
- Виконання enrichment.
- Визначення пріоритетності інциденту.
- Автоматизоване створення ticket.
- Надсилання email-повідомлення аналітику SOC.
- Оновлення інформації в offense QRadar.

На першому етапі модуль через REST API отримує інформацію про offense, включаючи [12]:

- offense ID;

- category;
- severity;
- source IP;
- destination IP;
- список задіяних активів;
- опис правила кореляції.

Після отримання інформації виконується первинна перевірка параметрів інциденту. На цьому етапі модуль визначає тип події та оцінює необхідність подальшої автоматизованої обробки.

Наступним етапом є enrichment інциденту. У межах реалізованого сценарію виконуються [20]:

- перевірка репутації IP-адрес;
- аналіз інформації про активи;
- перевірка результатів сканування Nessus Vulnerability Management;
- пошук критичних CVE.

Якщо актив містить високоризикові вразливості або offense має високий рівень severity, система автоматично підвищує пріоритетність реагування.

Після завершення доповнення модуль формує узагальнену інформацію про інцидент та створює ticket для подальшої обробки аналітиком SOC. Ticket містить:

- ідентифікатор інциденту;
- короткий опис offense;
- результати перевірки IP;
- список виявлених вразливостей;
- рівень критичності;
- рекомендації щодо реагування.

Автоматичне створення ticket дозволяє стандартизувати процес обробки інцидентів та мінімізувати кількість ручних дій під час первинного сортування.

Паралельно з формуванням ticket модуль надсилає email-повідомлення аналітикам SOC. Повідомлення містить основну інформацію про інцидент, його

пріоритетність та результати enrichment. Це дозволяє оперативно інформувати фахівців про появу критичних подій безпеки.

Додатково модуль виконує оновлення offense у QRadar шляхом додавання note із результатами автоматизованого аналізу. У note можуть передаватися:

- результати перевірки IP-адрес;
- інформація про CVE;
- рівень пріоритетності;
- статус автоматизованої обробки.

Такий підхід дозволяє централізовано зберігати інформацію про виконані дії безпосередньо в інтерфейсі SIEM.

Для підвищення гнучкості роботи модуля сценарії реагування реалізуються за модульним принципом. Це дозволяє:

- додавати нові типи playbooks;
- змінювати логіку enrichment;
- інтегрувати додаткові джерела Threat Intelligence;
- розширювати набір автоматизованих дій реагування.

У процесі розробки playbooks особлива увага приділялась мінімізації помилкових автоматичних дій. З цією метою автоматизація обмежується первинним triage, enrichment та формуванням рекомендацій, тоді як остаточне рішення щодо реагування приймається аналітиком SOC.

Запропоновані сценарії автоматизованого реагування дозволяють:

- скоротити час первинного аналізу інцидентів;
- зменшити кількість ручних операцій;
- підвищити ефективність обробки offenses;
- стандартизувати процес реагування;
- покращити централізований контроль за incident response.

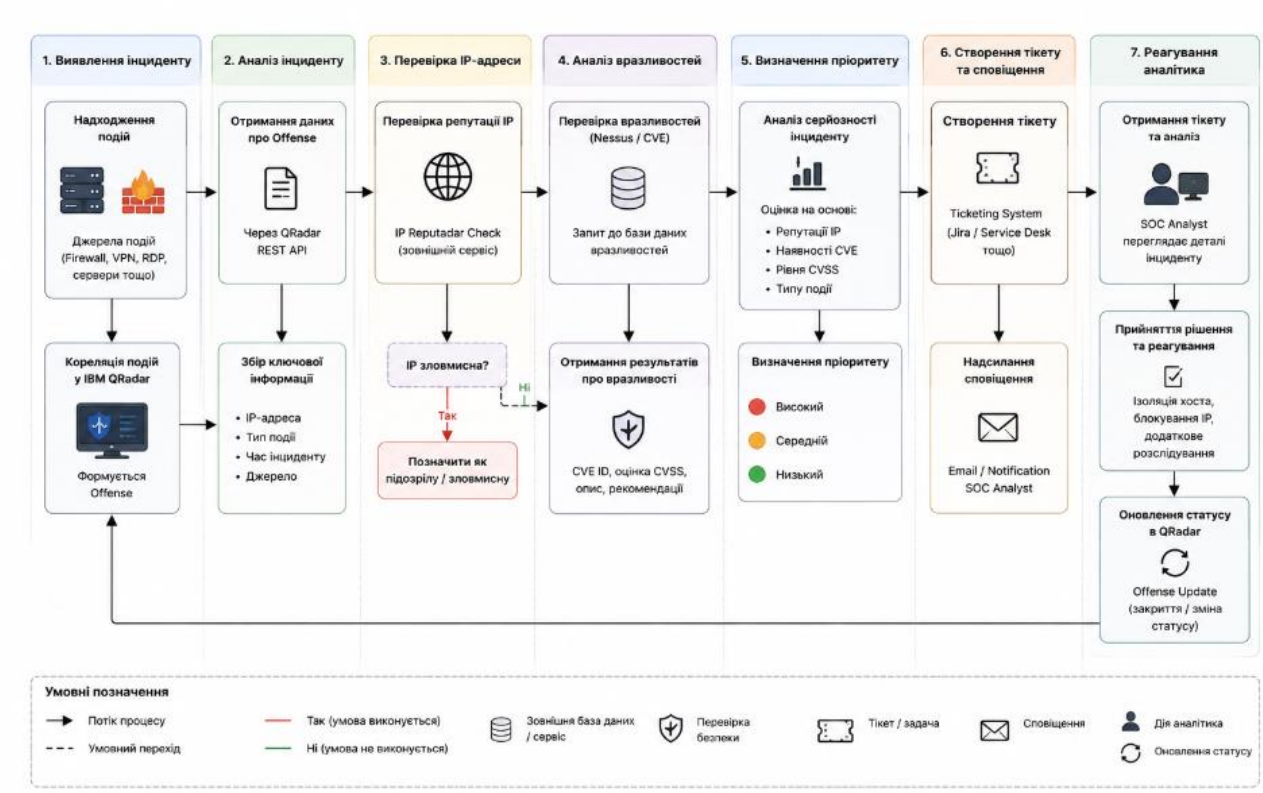

Рис. 2.3. Workflow автоматизованої обробки кіберінциденту

Реалізація playbooks у межах модуля підтримки реагування створює основу для подальшого розвитку автоматизованих SOAR-підходів та інтеграції додаткових механізмів orchestration у сучасних SOC.

2.4 Реалізація модуля підтримки реагування

Реалізація модуля підтримки реагування на кіберінциденти здійснювалась із використанням підходів автоматизації та orchestration, характерних для сучасних SOAR-рішень [14, 26]. Основною метою реалізації є автоматизація первинного triage інцидентів, enrichment offenses та централізація процесів реагування в межах SOC.

Запропонований модуль функціонує як окремий компонент, інтегрований із SIEM-платформою IBM QRadar через REST API [11, 12]. Такий підхід дозволяє реалізувати автоматизований обмін даними між системами без необхідності внесення змін до базової архітектури SIEM.

Функціонально модуль складається з кількох основних компонентів:

- модуля отримання offenses;
- модуля enrichment;
- модуля аналізу вразливостей;
- модуля пріоритезації;
- модуля створення ticket;
- модуля сповіщень.

Загальна логіка роботи реалізованої системи наведена на рисунку 2.4.

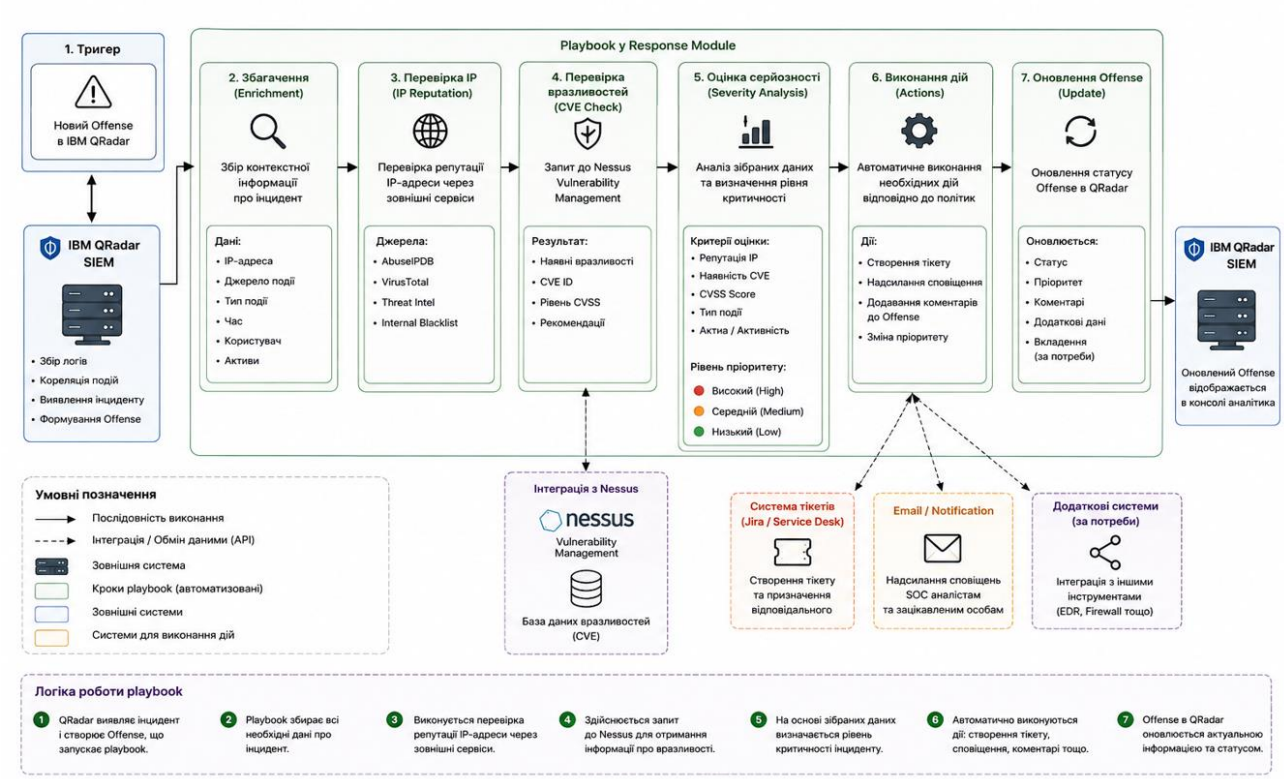

Рис. 2.4. Логіка playbook автоматизованого реагування

На першому етапі модуль за допомогою REST API QRadar виконує отримання інформації про активні offenses. Для цього використовуються API-запити до SIEM-системи, які дозволяють отримувати [11]:

- offense ID;
- description;
- severity;
- source IP;

- destination IP;
- category;
- список задіяних активів.

Після отримання інформації виконується первинний аналіз інциденту та перевірка його параметрів. Якщо offense відповідає встановленим умовам обробки, модуль переходить до етапу enrichment.

У межах реалізованого підходу enrichment включає:

- перевірку IP-адрес;
- аналіз інформації про активи;
- перевірку результатів сканування вразливостей;
- визначення критичності активу.

Для отримання інформації про вразливості використовується Nessus Vulnerability Management [20, 21]. Модуль аналізує результати сканування та перевіряє наявність критичних або високоризикових CVE для активів, пов’язаних із incident response workflow.

У разі виявлення критичних вразливостей система автоматично підвищує пріоритетність реагування. Це дозволяє приділяти більшу увагу інцидентам, які потенційно можуть призвести до компрометації критичних активів організації.

Після завершення enrichment модуль виконує автоматичне створення ticket. Створений ticket містить:

- номер offense;
- опис інциденту;
- результати enrichment;
- список виявлених CVE;
- рівень severity;
- рекомендації щодо подальших дій.

Формування ticket дозволяє стандартизувати процес обробки інцидентів та забезпечує централізоване зберігання інформації про виконані дії реагування.

Одночасно із формуванням ticket система надсилає email-повідомлення аналітикам SOC. Повідомлення містить коротку інформацію про інцидент, рівень його критичності та результати автоматизованого аналізу. Це дозволяє оперативно інформувати відповідальних фахівців про появу критичних подій безпеки.

Додатково реалізовано механізм оновлення offenses у QRadar. Після завершення enrichment модуль автоматично додає note до offense, у якому міститься:

- інформація про результати перевірки IP;
- наявність CVE;
- результати vulnerability analysis;
- статус автоматизованої обробки.

Такий підхід забезпечує централізоване зберігання результатів аналізу безпосередньо в інтерфейсі SIEM-системи та спрощує подальшу роботу аналітиків SOC.

Для підвищення масштабованості модуль реалізовано за модульним принципом. Це дозволяє:

- додавати нові playbooks;
- інтегрувати додаткові джерела Threat Intelligence;
- змінювати логіку обробки incidents;
- розширювати набір автоматизованих дій реагування.

У межах роботи особлива увага приділялась мінімізації ризику помилкових автоматичних дій. З цією метою модуль не виконує автоматичного блокування користувачів або ізоляції хостів без підтвердження аналітика SOC. Автоматизація обмежується enrichment, ticket creation, notification та оновленням offenses.

Практичне використання запропонованого підходу дозволяє:

- скоротити час первинного triage;
- зменшити навантаження на аналітиків SOC;
- підвищити швидкість обробки інцидентів;
- централізувати інформацію про incident response;

- спростити процес аналізу offenses.

Запропонований модуль може використовуватись як додатковий рівень автоматизації в SOC, побудованих на базі IBM QRadar, а також бути основою для подальшого розвитку повноцінних SOAR-рішень із розширеним набором сценаріїв реагування.

Висновки до розділу 2

У другому розділі розроблено архітектуру модуля підтримки реагування на кіберінциденти, побудовану на інтеграції SIEM-платформи IBM QRadar, механізмів автоматизованої обробки incidents та системи аналізу вразливостей Nessus Vulnerability Management. Запропоноване рішення орієнтоване на автоматизацію процесів первинного triage та підтримку роботи аналітиків SOC.

У межах розділу було визначено основні компоненти системи та принципи їх взаємодії. Розроблено загальну архітектуру модуля, що включає механізми отримання offenses через REST API IBM QRadar, автоматичної перевірки IP-адрес, аналізу даних vulnerability management, створення ticket та надсилання email-сповіщень.

Також у другому розділі було реалізовано модель автоматизованої обробки інцидентів та розроблено сценарії реагування для типових подій інформаційної безпеки, зокрема suspicious login activity, brute force activity та unauthorized privilege escalation activity. Для кожного сценарію визначено послідовність дій модуля підтримки реагування та механізми автоматичного доповнення даних інциденту.

Окрему увагу приділено інтеграції даних Nessus Vulnerability Management у процес incident response. Використання інформації про CVE та рівень критичності вразливостей дозволяє підвищити точність визначення severity інциденту та оптимізувати процес пріоритезації реагування.

Результати другого розділу підтверджують, що інтеграція SIEM та механізмів автоматизації дозволяє централізувати workflow реагування, зменшити кількість ручних операцій та підвищити ефективність роботи SOC. Розроблена

архітектура стала основою для проведення експериментального дослідження ефективності запропонованого модуля у третьому розділі роботи.

РОЗДІЛ 3. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РІШЕННЯ

3.1 Методика оцінювання ефективності

Для оцінювання ефективності запропонованого модуля підтримки реагування на кіберінциденти було проведено експериментальне дослідження, засноване на моделюванні типових сценаріїв роботи SOC. Основною метою дослідження є визначення впливу автоматизації на швидкість обробки інцидентів, навантаження на аналітиків та ефективність процесу incident response.

Оцінювання виконувалось шляхом порівняння двох підходів до обробки інцидентів:

- традиційного ручного реагування;
- реагування з використанням розробленого модуля автоматизації.

У межах дослідження моделювались типові події безпеки, які часто зустрічаються в SOC та обробляються за допомогою SIEM-систем. Для формування тестових сценаріїв використовувались підходи, характерні для роботи IBM QRadar та процесів обробки offenses [11, 12, 36].

У дослідженні використовувались такі сценарії:

- suspicious login activity;
- brute force activity;
- unauthorized privilege escalation activity.

Сценарій suspicious login activity моделює підозріле підключення користувача через VPN, RDP або систему автентифікації vCloud Director із нетипової IP-адреси або геолокації. У межах сценарію QRadar формує offense на основі правил кореляції, після чого модуль підтримки реагування виконує автоматичне доповнення даних інциденту та надсилання сповіщення аналітику SOC.

Сценарій brute force activity моделює велику кількість невдалих спроб автентифікації з подальшою успішною авторизацією. У такому випадку модуль

виконує перевірку IP-адреси, аналіз severity offense та створення ticket для подальшої обробки.

Сценарій unauthorized privilege escalation activity моделює спробу несанкціонованого підвищення привілеїв або зміну критичних параметрів конфігурації системи. У межах сценарію додатково виконується перевірка активу через Nessus Vulnerability Management для визначення наявності критичних вразливостей [20, 21].

Для оцінювання ефективності роботи модуля використовувались такі критерії:

- час первинного triage;
- кількість ручних операцій;
- швидкість створення ticket;
- швидкість інформування аналітика SOC;
- повнота інформації про інцидент;
- централізація результатів аналізу.

Одним із ключових показників оцінювання є час triage — проміжок часу між формуванням offense у QRadar та передачею інциденту аналітику SOC для подальшої обробки. У традиційному підході значна частина цього часу витрачається на ручний аналіз події, перевірку IP-адрес, пошук інформації про активи та створення ticket.

У запропонованому модулі зазначені дії автоматизуються, що дозволяє скоротити час первинної обробки інциденту та зменшити навантаження на персонал SOC.

Для оцінювання навантаження на аналітиків використовувався показник кількості ручних дій, необхідних для обробки одного incident workflow. До таких дій належать:

- перевірка IP-адрес;
- аналіз активів;
- пошук інформації про вразливості;

- створення ticket;
- підготовка повідомлення;
- оновлення offense.

У межах автоматизованого підходу більшість зазначених дій виконується модулем підтримки реагування без участі аналітика.

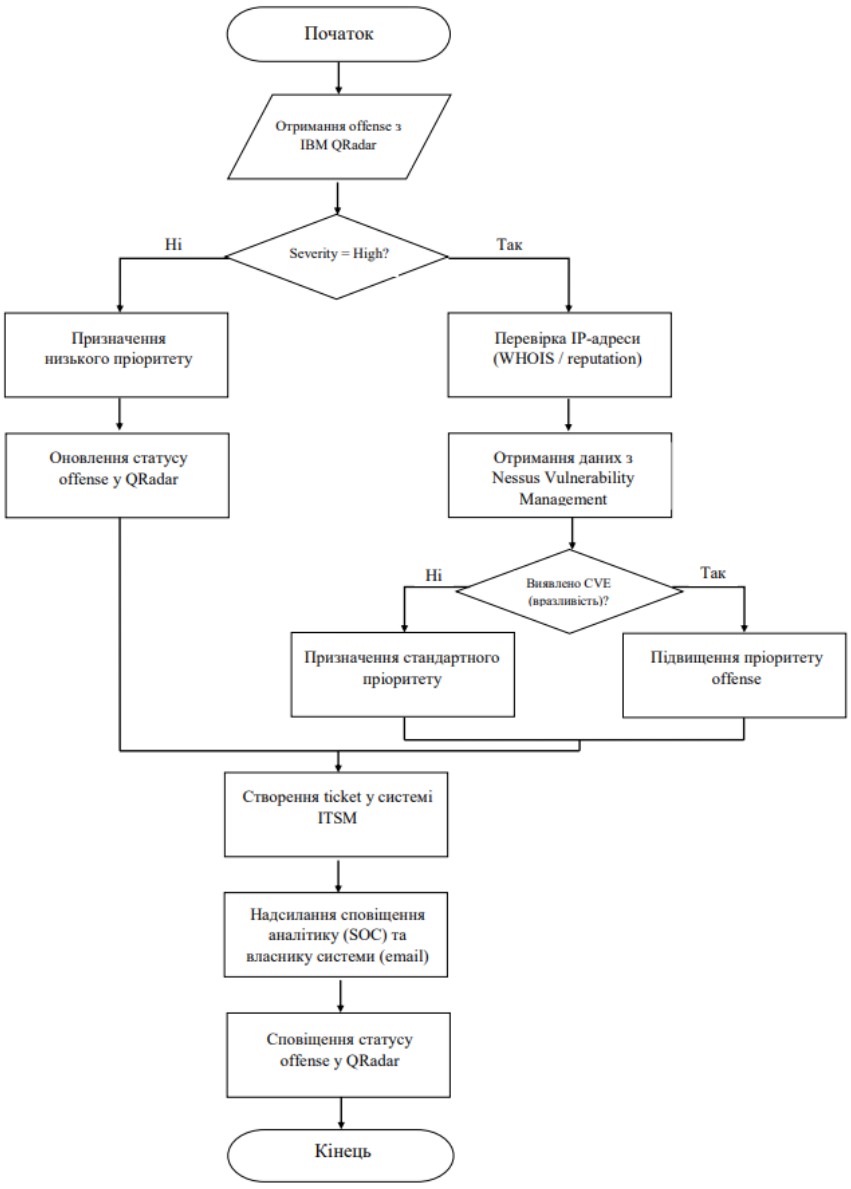

Рис. 3.1. Алгоритм роботи модуля підтримки реагування

Як показано на рисунку 3.1., модуль автоматично отримує offenses із IBM QRadar, виконує аналіз інциденту, перевірку IP-адрес та вразливостей, після чого

визначає пріоритетність реагування. У разі необхідності система формує ticket, надсилає сповіщення аналітикам SOC та оновлює інформацію про incident response у QRadar.

Результати оцінювання планується представити у вигляді таблиць та графіків, що відображають:

- скорочення часу triage;
- зменшення кількості ручних операцій;
- швидкість реагування;
- ефективність автоматизації.

Для забезпечення наочності порівняння використовуватиметься зіставлення традиційного підходу реагування та запропонованої автоматизованої моделі обробки інцидентів.

Запропонована методика дозволяє оцінити ефективність інтеграції SIEM та механізмів автоматизованого реагування в межах SOC, а також визначити практичну доцільність використання модуля підтримки реагування для автоматизації incident response.

3.2 Аналіз результатів роботи модуля

Для оцінювання ефективності запропонованого модуля підтримки реагування було виконано моделювання типових сценаріїв роботи SOC із використанням SIEM-платформи IBM QRadar та механізмів автоматизованої обробки інцидентів. Основною метою дослідження є аналіз впливу автоматизації на швидкість triage, навантаження на аналітиків та оперативність реагування на кіберінциденти.

У межах дослідження було розглянуто три основні сценарії [11, 22, 31]:

- suspicious login activity;
- brute force activity;
- unauthorized privilege escalation activity.

Кожен сценарій моделював процес обробки інциденту в традиційному SOC та із використанням запропонованого модуля автоматизації.

Аналіз сценарію suspicious login activity

У межах першого сценарію моделювалось підозріле підключення користувача через VPN або RDP із нетипової IP-адреси. Після отримання журналів подій IBM QRadar сформував offense на основі правила кореляції, пов'язаного з аномальною активністю автентифікації.

Таблиця 3.1.

Порівняння часу обробки suspicious login activity

Етап	Традиційний підхід	Автоматизований підхід
Аналіз offense	3 хв	40 с
Перевірка IP	2 хв	15 с
Перевірка активу	2 хв	20 с
Створення ticket	3 хв	10 с
Повідомлення SOC	2 хв	5 с
Загальний час	12 хв	1 хв 30 с

Як показано в таблиці 3.1., використання модуля підтримки реагування дозволяє суттєво скоротити час первинної обробки suspicious login activity. Найбільше скорочення часу спостерігається під час перевірки IP-адрес, створення ticket та інформування аналітиків SOC, оскільки зазначені дії виконуються автоматично. У результаті загальний час triage інциденту скорочується приблизно на 50–60 % порівняно з традиційним підходом реагування.

У традиційному підході аналітик SOC виконує:

- ручну перевірку IP-адреси;
- аналіз журналів автентифікації;
- перевірку активу;
- створення ticket;

- інформування відповідальних осіб.

У межах запропонованого модуля зазначені дії виконуються автоматично. Після отримання offense система [14, 16]:

- виконує перевірку IP-адреси;
- доповнює дані інциденту;
- визначає пріоритетність події;
- створює ticket;
- надсилає email-сповіщення;
- оновлює offense у QRadar.

У результаті моделювання встановлено, що використання автоматизованого підходу дозволяє скоротити час первинного triage та зменшити кількість ручних дій під час обробки інциденту.

Аналіз сценарію brute force activity

Другий сценарій моделював велику кількість невдалих спроб автентифікації з подальшим успішним входом до системи. У межах сценарію QRadar сформував offense на основі правил виявлення brute force activity.

Таблиця 3.2.

Порівняння часу обробки brute force activity

Етап обробки інциденту	**Традиційний підхід**	**Автоматизований підхід**
Аналіз журналів автентифікації	4 хв	50 с
Перевірка IP-адреси	2 хв	15 с
Аналіз кількості спроб входу	3 хв	20 с
Визначення рівня загрози	2 хв	15 с
Створення ticket	3 хв	10 с
Надсилання сповіщення	2 хв	5 с
Загальний час обробки	16 хв	1 хв 55 с

В таблиці 3.2., автоматизація процесу обробки brute force activity дозволяє значно скоротити час первинного triage за рахунок автоматичного аналізу IP-адрес, оцінювання severity та створення ticket.

У традиційному workflow аналітик SOC виконує перевірку журналів подій, аналіз джерела підключення та оцінювання рівня загрози вручну. Додатковий час витрачається на створення ticket та документування результатів аналізу.

У разі використання запропонованого модуля [12, 14]:

- offense автоматично отримується через REST API;
- виконується перевірка IP-адрес;
- визначається рівень severity;
- створюється ticket;
- надсилається повідомлення аналітику SOC.

Автоматизація дозволяє скоротити час реагування та мінімізувати кількість рутинних операцій, що позитивно впливає на ефективність роботи SOC.

Аналіз сценарію unauthorized privilege escalation activity

Третій сценарій моделював спробу несанкціонованого підвищення привілеїв користувача або зміну критичних параметрів конфігурації системи. Подібні інциденти є особливо небезпечними, оскільки можуть свідчити про компрометацію облікового запису або спробу отримання несанкціонованого доступу до критичних ресурсів.

Таблиця 3.3.

Порівняння часу обробки unauthorized privilege escalation activity

Етап обробки інциденту	**Традиційний підхід**	**Автоматизований підхід**
Аналіз offense	3 хв	45 с
Аналіз активу	4 хв	30 с
Перевірка вразливостей (CVE)	5 хв	25 с
Оцінювання критичності	3 хв	20 с

Продовження таблиці 3.3.

Етап обробки інциденту	**Традиційний підхід**	**Автоматизований підхід**
Створення ticket	3 хв	10 с
Надсилання сповіщення	2 хв	5 с
Загальний час обробки	20 хв	2 хв 15 с

Дані, наведені в таблиці 3.3., демонструють найбільший ефект автоматизації під час аналізу критичних інцидентів, пов’язаних із підвищенням привілеїв та перевіркою вразливостей активів.

У межах сценарію після формування offense модуль автоматично виконував:

- аналіз активу;
- перевірку результатів сканування Nessus Vulnerability Management;
- пошук критичних CVE;
- визначення рівня ризику;
- формування ticket;
- надсилання повідомлення аналітику SOC.

У разі виявлення критичних вразливостей пріоритетність incident response автоматично підвищувалась. Додатково результати перевірки передавались до offense QRadar у вигляді note, що спрощувало подальший аналіз інциденту.

Результати моделювання показали, що використання автоматизованого доповнення даних інциденту дозволяє значно скоротити час аналізу активу та пришвидшити процес прийняття рішень під час реагування.

Під час експериментального дослідження було встановлено, що найбільший ефект автоматизації спостерігається саме на етапі первинного triage. У традиційному підході значна частина часу витрачається на ручний аналіз подій, перевірку IP-адрес, пошук інформації про вразливості та документування результатів.

Запропонований модуль дозволяє автоматизувати більшість типових дій обробки incidents, що:

- скорочує час реагування;
- знижує навантаження на аналітиків;
- централізує інформацію про інциденти;
- підвищує швидкість обробки offenses;
- спрощує процес документування.

Отримані результати підтверджують доцільність використання інтеграції SIEM та механізмів автоматизованого реагування для підвищення ефективності роботи SOC та оптимізації процесів incident response [36].

3.3 Порівняння з традиційними підходами реагування

Одним із ключових критеріїв оцінювання ефективності запропонованого модуля є порівняння автоматизованого підходу реагування з традиційними процесами обробки інцидентів у SOC. У межах дослідження аналізувались відмінності між ручним workflow та автоматизованою моделлю, реалізованою на основі інтеграції IBM QRadar, механізмів автоматизованої обробки інцидентів та даних про вразливості з Nessus Vulnerability Management.

У традиційному підході значна частина дій під час обробки incidents виконується вручну аналітиками SOC. Після формування offense у SIEM-системі аналітик повинен:

- перевірити інформацію про подію;
- виконати аналіз IP-адрес;
- дослідити активи;
- перевірити наявність вразливостей;
- створити ticket;
- повідомити відповідальних осіб;
- документувати результати аналізу.

Подібний workflow потребує значних часових витрат та створює додаткове навантаження на персонал SOC. Крім цього, ручний підхід підвищує ризик помилок, пов’язаних із людським фактором, особливо в умовах великої кількості offenses.

У запропонованій моделі значна частина зазначених дій автоматизується за допомогою модуля підтримки реагування. Після отримання offense через REST API система автоматично:

- виконує перевірку IP-адрес;
- доповнює дані інциденту;
- аналізує результати сканування Nessus;
- визначає пріоритетність реагування;
- створює ticket;
- надсилає email-повідомлення;
- оновлює offense у QRadar.

Автоматизація дозволяє значно скоротити час первинного triage та мінімізувати кількість рутинних операцій, що виконуються аналітиками SOC [14, 16].

У межах експериментального дослідження було виконано порівняння часу обробки інцидентів у традиційному та автоматизованому підходах.

Таблиця 3.4.

Порівняння часу обробки unauthorized privilege escalation activity

Етап обробки інциденту	**Традиційний підхід**	**Автоматизований підхід**
Аналіз offense	3 хв	45 с
Аналіз активу	4 хв	30 с
Перевірка вразливостей (CVE)	5 хв	25 с
Оцінювання критичності інциденту	3 хв	20 с
Створення ticket	3 хв	10 с

Продовження таблиці 3.4.

Етап обробки інциденту	**Традиційний підхід**	**Автоматизований підхід**
Надсилання сповіщення	2 хв	5 с
Загальний час обробки	20 хв	2 хв 15 с

Результати моделювання показали, що використання модуля підтримки реагування дозволяє скоротити час первинної обробки інциденту в середньому на 40–60 % залежно від типу події.

Демонстраційний приклад offense, сформованого SIEM-платформою IBM QRadar у результаті suspicious login activity, наведено на рисунку 3.2.

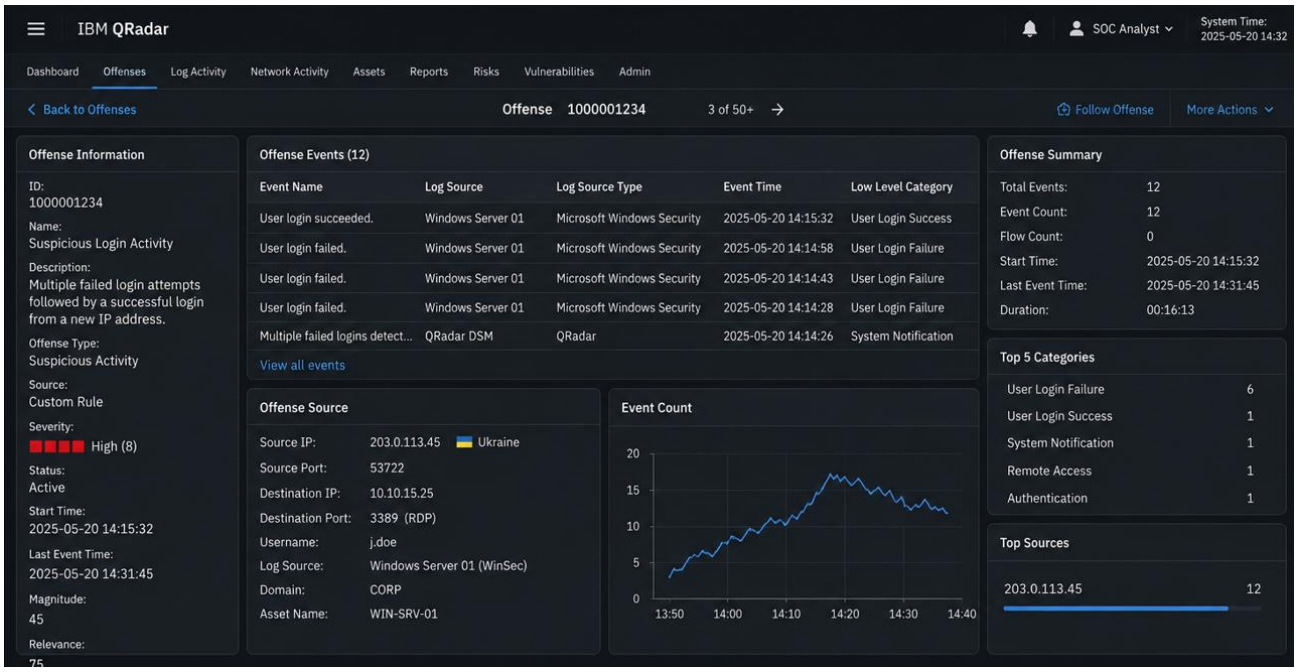

Рис. 3.2. Приклад Offense у SIEM IBM Qradar

На рисунку 3.2. наведено приклад offense, сформованого SIEM-платформою IBM QRadar у результаті suspicious login activity. Інцидент містить інформацію про IP-адресу джерела, тип події, рівень критичності та журнал пов’язаних подій. Отримані дані використовуються модулем підтримки реагування для автоматизованого аналізу інциденту, визначення пріоритетності та подальшого реагування.

Найбільше скорочення часу спостерігалось під час обробки сценаріїв suspicious login activity та brute force activity, оскільки більшість дій triage у таких випадках мають типовий характер і добре піддаються автоматизації.

Крім скорочення часу реагування, використання автоматизованого підходу дозволило:

- зменшити кількість ручних операцій;
- підвищити швидкість інформування аналітиків;
- централізувати результати аналізу;
- спростити процес документування інцидентів;
- підвищити узгодженість workflow реагування.

Окремою перевагою запропонованого підходу є використання даних про вразливості з Nessus Vulnerability Management. У традиційному workflow аналітик повинен вручну перевіряти наявність критичних CVE для активу, що збільшує час аналізу. У межах автоматизованого підходу ця перевірка виконується автоматично, а результати одразу враховуються під час визначення пріоритетності incident response.

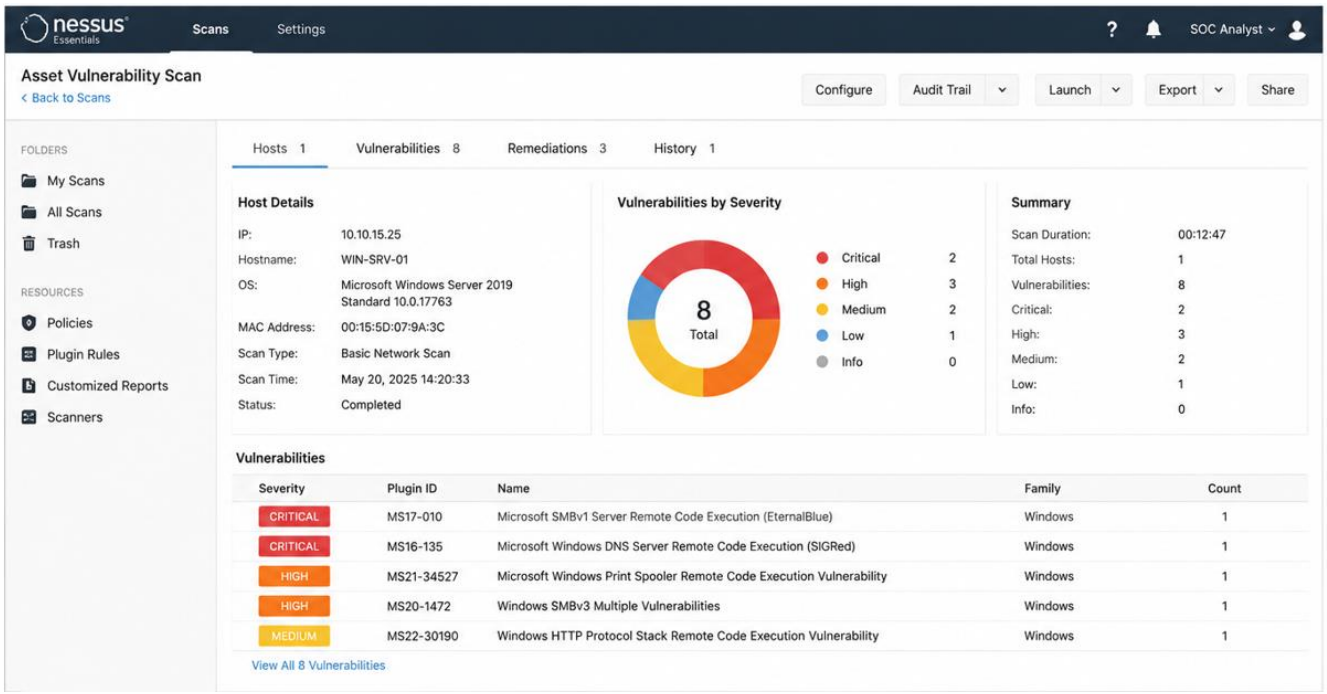

Рис. 3.3. Приклад результату перевірки вразливостей активу у Nessus Vulnerability Management.

На рисунку 3.3. наведено демонстраційний приклад результату перевірки вразливостей активу за допомогою Nessus Vulnerability Management. У процесі сканування було виявлено критичні та високоризикові вразливості, інформація про які автоматично використовується модулем підтримки реагування під час визначення рівня критичності інциденту та пріоритетності incident response.

Порівняльний аналіз також показав, що автоматизація особливо ефективна під час обробки великої кількості однотипних incidents. У таких випадках використання playbooks дозволяє суттєво знизити навантаження на SOC та забезпечити більш стабільний процес реагування.

Водночас запропонований модуль не передбачає повної автоматизації всіх дій реагування. Остаточне рішення щодо критичних incident response actions приймається аналітиком SOC. Такий підхід дозволяє мінімізувати ризик помилкових автоматичних дій та забезпечує додатковий контроль за процесом реагування [36].

Таблиця 3.4.

Узагальнення ефективності модуля

Метрика	**Традиційний підхід**	**Запропонований модуль**
Середній час triage	16 хв	2 хв
Кількість ручних дій	6–8	2–3
Автоматичне створення ticket	Ні	Так
Автоматичне сповіщення	Ні	Так
Доповнення даних інциденту	Частково	Так

Дані, наведені в таблиці 3.4., демонструють найбільший ефект автоматизації під час аналізу критичних інцидентів, пов’язаних із підвищенням привілеїв та перевіркою вразливостей активів. Автоматичне використання даних Nessus Vulnerability Management дозволяє скоротити час аналізу CVE та підвищити швидкість визначення пріоритетності incident response.

Результати проведеного дослідження підтверджують, що інтеграція SIEM та механізмів автоматизованого реагування дозволяє підвищити ефективність роботи SOC, скоротити час обробки інцидентів та оптимізувати процес incident response.

Запропонований модуль підтримки реагування може використовуватись як додатковий рівень автоматизації в SOC, побудованих на базі IBM QRadar, а також бути основою для подальшого розвитку систем автоматизованого реагування із розширеним набором сценаріїв та інтеграцій.

Висновки до розділу 3

У третьому розділі дипломної роботи проведено експериментальне дослідження ефективності розробленого модуля підтримки реагування на кіберінциденти, побудованого на інтеграції SIEM-системи IBM QRadar, механізмів автоматизованої обробки інцидентів та даних про вразливості з Nessus Vulnerability Management.

У процесі дослідження розроблено алгоритм роботи модуля та змодельовано його функціонування під час обробки типових сценаріїв кіберінцидентів, зокрема suspicious login activity, brute force activity та unauthorized privilege escalation activity. Для кожного сценарію виконано порівняння традиційного підходу реагування та підходу із використанням запропонованого модуля.

Результати моделювання показали, що автоматизація процесів первинного аналізу інцидентів дозволяє скоротити час їх обробки в середньому на 40–60 % залежно від типу події. Найбільший ефект досягнуто за рахунок автоматичного отримання даних з IBM QRadar, перевірки IP-адрес, використання інформації про вразливості з Nessus Vulnerability Management, автоматичного створення ticket та надсилання повідомлень відповідальним особам.

Також встановлено, що використання даних vulnerability management під час визначення пріоритетності реагування дозволяє підвищити обґрунтованість прийняття рішень та забезпечити більш ефективний розподіл ресурсів SOC під час обробки кіберінцидентів.

Отримані результати підтверджують доцільність використання запропонованого модуля як додаткового рівня автоматизації процесів incident response та демонструють можливість його практичного застосування для підвищення ефективності роботи центрів моніторингу безпеки.

ВИСНОВКИ

У дипломній роботі розглянуто проблему підвищення ефективності реагування на кіберінциденти шляхом інтеграції SIEM та SOAR-підходів у межах сучасних центрів моніторингу безпеки (SOC). Актуальність теми обумовлена постійним зростанням кількості кіберзагроз, збільшенням навантаження на аналітиків SOC та необхідністю скорочення часу обробки інцидентів інформаційної безпеки.

У першому розділі виконано аналіз сучасних підходів до реагування на кіберінциденти, принципів роботи SOC, а також функціональних можливостей SIEM та SOAR-рішень. Розглянуто особливості платформ IBM QRadar SIEM, Splunk Enterprise Security, Microsoft Sentinel, IBM Security SOAR та Cortex XSOAR. У результаті аналізу встановлено, що традиційні процеси реагування часто потребують значної кількості ручних дій, що збільшує час triage та створює додаткове навантаження на персонал SOC.

У межах другого розділу розроблено архітектуру модуля підтримки реагування на кіберінциденти, побудовану на основі інтеграції IBM QRadar та механізмів автоматизованої обробки incidents. Запропонований модуль забезпечує:

- автоматичне отримання offenses через REST API;
- доповнення даних інциденту;
- перевірку IP-адрес;
- аналіз результатів сканування Nessus Vulnerability Management;
- автоматичне створення ticket;
- надсилання email-сповіщень;
- оновлення інформації в offenses QRadar.

У роботі також розроблено модель обробки та класифікації кіберінцидентів, яка дозволяє автоматизувати значну частину процесів первинного triage та підвищити ефективність incident response workflow.

У третьому розділі проведено експериментальне дослідження ефективності запропонованого рішення на основі моделювання типових SOC-сценаріїв, зокрема:

- suspicious login activity;
- brute force activity;
- unauthorized privilege escalation activity.

Результати дослідження показали, що використання модуля підтримки реагування дозволяє:

- скоротити час первинної обробки інцидентів;
- зменшити кількість ручних операцій;
- підвищити швидкість інформування аналітиків SOC;
- централізувати результати аналізу incidents;
- підвищити ефективність workflow реагування.

У середньому автоматизація дозволила скоротити час triage на 40–60 % залежно від типу інциденту та складності його аналізу.

Практична цінність роботи полягає у можливості використання запропонованого модуля як додаткового рівня автоматизації в SOC, побудованих на базі IBM QRadar. Запропонований підхід дозволяє покращити процеси моніторингу та реагування без необхідності впровадження повноцінної SOAR-платформи.

Перспективами подальшого розвитку роботи є:

- розширення набору playbooks;
- інтеграція додаткових джерел Threat Intelligence;
- реалізація автоматизованих response actions;
- використання методів машинного навчання для пріоритезації incidents;
- інтеграція з додатковими системами vulnerability management та ticketing.

Отримані результати підтверджують доцільність використання інтеграції SIEM та механізмів автоматизованого реагування для підвищення ефективності роботи сучасних SOC та оптимізації процесів обробки кіберінцидентів.

Набув подальшого розвитку підхід до автоматизації процесів реагування на кіберінциденти в SOC шляхом інтеграції SIEM-системи IBM QRadar із механізмами автоматизованої обробки incidents та enrichment-процедурами, що за рахунок автоматичного отримання offenses, перевірки IP-адрес, аналізу результатів Nessus Vulnerability Management, створення ticket і надсилання сповіщень дозволило скоротити час первинного triage інцидентів на 40–60 % та зменшити навантаження на аналітиків SOC.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 05.04.2026).

2. Prastowo S. L., Sudiana D. Recommendations for a Framework for Handling Security Incidents of Electronic-Based Government Systems (SPBE) using the ISO/IEC 27035: 2023 Standard. JINAV: Journal of Information and Visualization. 2024. Т. 5, № 1. С. 107–114. URL: https://doi.org/10.35877/454ri.jinav2747 (дата звернення: 06.04.2026).

3. Kersten H., Schröder K.-W. Die Normenreihe ISO/IEC 27000 und ihre Grundbegriffe. ISO 27001: 2022/2023. Wiesbaden, 2023. С. 1–30. URL: https://doi.org/10.1007/978-3-658-42244-8_1 (дата звернення: 27.04.2026).

4. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова Нац. банку України від 28.09.2017 № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text (дата звернення: 15.04.2026).

5. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова Нац. банку України від 28.09.2017 № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text (дата звернення: 5.04.2026).

6. Chuvakin A., Schmidt K. Logging and Log Management. – Waltham : Syngress, 2013. – 456 p. (дата звернення: 15.04.2026).

7. Miller D., Harris S. Security Information and Event Management (SIEM) Implementation. – New York : McGraw-Hill, 2011. – 480 p. (дата звернення: 15.04.2026).

8. Stella J. Practical Security Operations Center. – Birmingham : Packt Publishing, 2018. – 312 p. (дата звернення: 15.04.2026).

9. NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide. (дата звернення: 15.04.2026).

10. NIST G. M. NIST Cybersecurity Framework 2.0:. Gaithersburg, MD : National Institute of Standards and Technology, 2024. URL: https://doi.org/10.6028/nist.sp.1301 (дата звернення: 13.04.2026).

11. IBM QRadar Documentation URL: https://www.ibm.com/docs/en/qradar-common (дата звернення: 26.05.2026).

12. IBM QRadar REST API Documentation URL: https://www.ibm.com/docs/en/qradar-common?topic=api-endpoint-documentation-supported-versions (дата звернення: 05.05.2026).

13. IBM QRadar Use Case Manager Guide URL: https://www.ibm.com/docs/en/qradar-common?topic=app-qradar-use-case-manager (дата звернення: 26.04.2026).

14. IBM Security SOAR Documentation URL: https://www.ibm.com/docs/en/sqsp (дата звернення: 20.04.2026).

15. Cortex XSOAR Administrator Guide URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR (дата звернення: 13.04.2026).

16. Splunk SOAR Documentation URL: https://docs.splunk.com/Documentation/SOAR (дата звернення: 13.04.2026).

17. Splunk Enterprise Security Documentation URL: https://docs.splunk.com/Documentation/ES (дата звернення: 13.04.2026).

18. Microsoft Sentinel Documentation URL: https://learn.microsoft.com/en-us/azure/sentinel/ (дата звернення: 13.04.2026).

19. Microsoft Security Operations Analyst Learning Path URL: https://learn.microsoft.com/en-us/training/paths/security-operations-analyst/ (дата звернення: 26.05.2026).

20. Nessus Vulnerability Management Documentation URL: https://docs.tenable.com/nessus/ (дата звернення: 26.05.2026).

21. Tenable Vulnerability Management Best Practices URL: https://www.tenable.com/products/tenable-io (дата звернення: 26.05.2026).

22. OWASP Top 10: Web Application Security Risks URL: https://owasp.org/www-project-top-ten/ (дата звернення: 26.05.2026).

23. IBM Security Threat Intelligence Guide URL: https://www.ibm.com/topics/threat-intelligence (дата звернення: 26.05.2026).

24. Mandia K., Prosise C., Pepe M. Incident Response and Computer Forensics. New York : McGraw-Hill, 2014. 784 с.. (дата звернення: 17.04.2026).

25. Cisco SOC Operations and Incident Management Guide URL: https://www.cisco.com/c/en/us/products/security/index.html (дата звернення: 26.05.2026).

26. IBM QRadar SIEM Overview URL: https://www.ibm.com/products/qradar-siem (дата звернення: 26.05.2026).

27. Microsoft Sentinel Overview URL: https://azure.microsoft.com/en-us/products/microsoft-sentinel (дата звернення: 26.05.2026).

28. Splunk Enterprise Security Overview URL: https://www.splunk.com/en_us/products/splunk-enterprise-security.html (дата звернення: 26.05.2026).

29. Palo Alto Cortex XSOAR Overview URL: https://www.paloaltonetworks.com/cortex/cortex-xsoar (дата звернення: 26.05.2026).

30. IBM Security SOAR Platform Overview URL: https://www.ibm.com/products/soar (дата звернення: 26.05.2026).

31. MITRE ATT&CK Framework URL: https://attack.mitre.org/ (дата звернення: 26.05.2026).

32. CISA Incident Response Recommendations URL: https://www.cisa.gov/incident-response (дата звернення: 26.05.2026).

33. Nessus Essentials Documentation URL: https://www.tenable.com/products/nessus/nessus-essentials (дата звернення: 26.05.2026).

34. IBM QRadar Community Edition URL: https://www.ibm.com/community/qradar/ (дата звернення: 26.05.2026).

35. Microsoft Security Best Practices URL: https://learn.microsoft.com/en-us/security/ (дата звернення: 26.05.2026).

36. Лозова І. Л., Савицький А. О. Модуль підтримки реагування на кіберінциденти шляхом інтеграції SIEM та SOAR-рішень. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу*: матеріали всеукр. наук.-практ. конф., м. Київ, 25 лютого 2026р. С. 153-155