МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ОРГАНІЗАЦІЇ МОНІТОРИНГУ ЗАГРОЗ В ЦЕНТРІ ОПЕРАТИВНОГО УПРАВЛІННЯ БЕЗПЕКОЮ (SOC)”

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

_____ Андрій КУЗЬКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Андрій КУЗЬКО
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЩАВІНСЬКИЙ
К.т.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: Юрій ПЕПА
К.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2025

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
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кузьку Андрію Володимировичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Інноваційні технології формування обізнаності й навчання персоналу з інформаційної безпеки”,
керівник кваліфікаційної роботи Щавінський Юрій, к.т.н., доцент,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.
3. Вихідні дані до кваліфікаційної роботи: *система інформаційної безпеки підприємства, організаційні методи моніторингу та засоби захисту, міжнародні стандарти, наукова та технічна література.*
4. Перелік питань, які мають бути розроблені:
   4.1. Проведення аналізу підходів до організації моніторингу загроз у Центрах оперативного управління безпекою (SOC).
   4.2 Дослідження та класифікація основних методів та технологій моніторингу кіберзагроз, включаючи SIEM-системи, IDS/IPS, Threat Intelligence та SOAR-платформи.
   4.3 Розроблення моделі моніторингу загроз у SOC, що враховує сучасні загрози, методи їх виявлення та реагування.

Перелік ілюстративного матеріалу: *презентація PowerPoint*

5. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	Виконано
2.	Збір та аналіз літератури.	29.03.2025	Виконано
3.	Аналіз особливостей управління інформаційною безпекою підприємства	08.04.2025	Виконано
4.	Дослідження основних характеристик технологій формування обізнаності й навчання персоналу.	15.04.2025	Виконано
5.	Вивчення інструментів та методів формування обізнаності й навчання персоналу з інформаційної безпеки	22.04.2025	Виконано
6.	Формулювання висновків за результатами проведеного дослідження.	10.05.2025	Виконано
7.	Оформлення роботи.	12.05.2025	Виконано
8.	Оформлення презентації.	25.05.2025	Виконано
9.	Отримання рецензії на роботу.	28.05.2025	Виконано
10.	Захист в ДЕК.	17.06.2025	

Здобувач вищої освіти _____ Андрій КУЗЬКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(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 здобувач Кузько А.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Інноваційні технології формування обізнаності й навчання персоналу з інформаційної безпеки"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач КУЗЬКО Андрій у кваліфікаційній роботі проаналізував особливості методи організації моніторингу загроз відділом SOC підприємства, дослідив основні системи захисту котрими забезпечується інформаційна безпека, вивчив інструменти та методи формування обізнаності й навчання персоналу з інформаційної безпеки, розробив відповідні методи організації моніторингу загроз відділом SOC за темою дослідження.

КУЗЬКО Андрій показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на двох конференціях.

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

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Кузько А.В. 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 КУЗЬКА Андрія

на тему “Методи організації моніторингу загроз в Центрі оперативного управління безпекою (SOC)”

Актуальність. Кваліфікаційна робота присвячена аналізу та розробці ефективних методів моніторингу кіберзагроз у Центрах оперативного управління безпекою (SOC), що є вкрай актуальним у сучасних умовах зростання кількості кіберінцидентів. Питання своєчасного виявлення, класифікації та реагування на загрози має критичне значення для забезпечення стійкості інформаційних систем. Робота відповідає сучасним науково-практичним тенденціям у сфері кібербезпеки.

Позитивні сторони.

Робота має логічну структуру. При проведенні аналізу підходів до моніторингу загроз у SOC автор охопив сучасні методології організації моніторингу, описав архітектурні моделі SOC різних рівнів, проведено систематизацію засобів SIEM, IDS/IPS, Threat Intelligence, SOAR, надано їх порівняльну характеристик, Особливої уваги заслуговує практична частина, де автор запропонував структуровану модель інтеграції різних систем (SIEM, TI, SOAR) у єдиний процес моніторингу та реагування. Високий рівень технічної грамотності та володіння термінологією.

Недоліки.

Було б доцільно глибше описати механізми інтеграції з зовнішніми Threat Intelligence-джерелами. У практичному розділі можна було б подати приклад впровадження моделі на базі конкретного програмного забезпечення (наприклад, AlienVault, QRadar, або Splunk). Варто було б розширити аналіз кейсів реагування на конкретні типи атак. Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент: Юрій ПЕПА

к.т.н., доцент *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів організації моніторингу загроз в центрі оперативного управління безпекою (SOC). Робота

складається зі вступу, трьох розділів, що містять 5 рисунків, висновків і списку використаних джерел із 50 найменувань. Загальний обсяг роботи становить 71 аркуші, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є розробка та обґрунтування ефективних методів організації моніторингу загроз у Центрі оперативного управління безпекою (SOC) для виявлення, аналізу та реагування на кіберзагрози в режимі реального часу.

Об'єктом дослідження є процес організації моніторингу інформаційної безпеки та кіберзагроз у Центрі оперативного управління безпекою (SOC).

Предмет дослідження **–** методи та інструменти моніторингу загроз у SOC, зокрема використання SIEM-систем, систем виявлення вторгнень (IDS/IPS), аналітики загроз (Threat Intelligence) та автоматизованих засобів реагування (SOAR).

Методи дослідження. У ході дослідження питань, що стосуються моніторингу кіберзагроз у SOC, були використані такі основні методи дослідження:

– аналіз літературних джерел – вивчення стандартів безпеки (ISO 27001, NIST), технічної документації (IBM QRadar, Splunk, Zeek, Suricata, Snort, тощо), наукових публікацій і звітів про інциденти для розуміння архітектури та функціоналу SOC;

– порівняльний аналіз – системне порівняння SIEM-, IDS/IPS-, SOAR-систем та платформ Threat Intelligence за критеріями продуктивності, масштабованості, інтеграції, функціоналу й ефективності виявлення загроз;

– метод моделювання – побудова узагальненої моделі SOC, алгоритмів моніторингу загроз, структури реагування на інциденти та інтеграції між компонентами (SIEM, SOAR, Threat Intelligence, IDS/IPS);

– системний підхід – дослідження SOC як цілісної системи, де взаємодіють технології, персонал, політики безпеки, інструменти реагування й аналітика;

– емпіричне дослідження (огляд кейсів) – розгляд реальних сценаріїв використання Snort, Suricata, Zeek, IBM Resilient SOAR, Splunk SOAR, тощо, в контексті Security Operations Center;

Галузь застосування. Отримані результати дослідження та розглянуті технології мають практичне значення в наступних сферах:

– кібербезпека в корпоративному секторі – впровадження SOC у великих організаціях для захисту критичних активів, реагування на інциденти, моніторингу аномальної активності та зниження ризиків порушення безпеки;

– фінансові установи та банки – захист від фішингових атак, шахрайських транзакцій, забезпечення відповідності регуляторним вимогам (наприклад, PCI DSS, ISO 27001);

– державні органи та критична інфраструктура – контроль за інформаційною безпекою об’єктів енергетики, транспорту, зв’язку, охорони здоров’я, що є об’єктами потенційних кібератак;

– хмарні провайдери та дата-центри – реалізація централізованого моніторингу трафіку, подій доступу, виявлення бот-мереж, шкідливих навантажень та загроз нульового дня;

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

ABSTRACT

The qualification work is devoted to the study of technologies for creating awareness and training of information security personnel. The work consists of an introduction, three chapters containing 5 figures, conclusions and a list of 50 references. The total volume of the work is 71 pages, of which 6 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to develop and substantiate effective methods for organizing threat monitoring in the Security Operations Center (SOC) to detect, analyze and respond to cyber threats in real time.

The object of research is the process of organizing information security and cyber threat monitoring in the Security Operations Center (SOC).

The subject of the study is the methods, technologies and tools for monitoring threats in the SOC, including the use of SIEM systems, intrusion detection systems (IDS/IPS), threat intelligence and automated response tools (SOAR).

Research methods. In the course of working on topics related to monitoring cyber threats in SOC, the following main research methods were used:

– literature analysis – study of security standards (ISO 27001, NIST), technical documentation (IBM QRadar, Splunk, Zeek, Suricata, Snort, etc.), scientific publications and incident reports to understand the architecture and functionality of the SOC;

– comparative analysis – a systematic comparison of SIEM, IDS/IPS, SOAR systems and Threat Intelligence platforms by the criteria of performance, scalability, integration, functionality, and threat detection efficiency;

– modeling method – building a generalized SOC model, threat monitoring algorithms, incident response structure, and integration between components (SIEM, SOAR, Threat Intelligence, IDS/IPS);

– systems approach – studying the SOC as an integrated system where technologies, personnel, security policies, response tools, and analytics interact;

– empirical research – consideration of real-life scenarios of using Snort, Suricata, Zeek, IBM Resilient SOAR, Splunk SOAR, etc. in the context of the Security Operations Center.

Field of application. The results of the study and the technologies reviewed are of practical importance in the following areas:

– cybersecurity in the corporate sector - implementation of SOC in large organizations to protect critical assets, respond to incidents, monitor anomalous activity, and reduce security risks.

– financial institutions and banks - protection against phishing attacks, fraudulent transactions, and compliance with regulatory requirements (e.g., PCI DSS, ISO 27001).

– government agencies and critical infrastructure - control over the information security of energy, transportation, communications, and healthcare facilities that are subject to potential cyberattacks.

– cloud providers and data centers - implementation of centralized monitoring of traffic, access events, detection of botnets, malicious loads, and zero-day threats.

– security solution integrators (MSSPs) - using SIEM/SOAR/IDS systems to provide monitoring and response services to third-party customers on an outsourced basis.

– The testing of the results of the qualification work took place at the All-Ukrainian Scientific and Practical Conference “Cyber Resilience Strategies: Risk Management and Business Continuity” on February 27, 2025.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ІС	Інформаційна система
ПЗ	Програмне забезпечення
SOC	Security operation center
ШПЗ	Шкідливе програмне забезпечення
ПЗ	Програмне забезпечення
EDR	Endpoint detection and response
ML	Machine learning
SOAR	Security Orchestration, Automation and Response
SIEM	Security information and event management
NDR	Network detection and response
XDR	Extended detection and response
IDS	Intrusion detection system
IPS	Intrusion prevention system
MSG	Mail security gateway
DLP	Data leak prevention
Splunk ES	Splunk Enterprise Security
TIP	Threat Intelligence Platform

ВСТУП

Актуальність теми. Щосекунди у різного роду ІС зберігають, оброблюють, передають головний об’єкт сучасності – інформацію. Вона є в багатьох форматах, будь-то повідомлення в месенджері чи транзакція в банку, або взагалі транслюванням музики до ваших навушників. У зв’язку з великим обсягом використання цифровізованої інформації у компаній виникає очевидне питання, яким чином організувати не просто контроль над інформацією, а повноцінний моніторинг подій, що відбуваються в ІС, реагування під час кібератак, використання перевірених документів та ПЗ та інші функції котрі виконує Центр оперативного управління безпекою (SOC).

З огляду на вищезазначене, моніторингу інформаційної безпеки та кіберзагроз у Центрі оперативного управління безпекою (SOC) є актуальним науковим завданням.

Метою роботи є розробка та обґрунтування ефективних методів організації моніторингу загроз у Центрі оперативного управління безпекою (SOC) для виявлення, аналізу та реагування на кіберзагрози в режимі реального часу.

Об’єктом дослідження є процес організації моніторингу інформаційної безпеки та кіберзагроз у Центрі оперативного управління безпекою (SOC).

Предмет дослідження – методи, технології та інструменти моніторингу загроз у SOC, зокрема використання SIEM-систем, систем виявлення вторгнень (IDS/IPS), аналітики загроз (Threat Intelligence) та автоматизованих засобів реагування (SOAR).

Завдання дослідження є:

– проведення аналізу підходів до організації моніторингу загроз у Центрах оперативного управління безпекою (SOC);

– дослідження та класифікація основних методів та технологій моніторингу кіберзагроз, включаючи SIEM-системи, IDS/IPS, Threat Intelligence та SOAR-платформи;

– розроблення моделі моніторингу загроз у SOC, що враховує сучасні загрози, методи їх виявлення та реагування.

Методи дослідження. У ході роботи над темами, що стосуються моніторингу кіберзагроз у SOC, були використані такі основні методи дослідження:

– **аналіз літературних джерел** – вивчення стандартів безпеки (ISO 27001, NIST), технічної документації (IBM QRadar, Splunk, Zeek, Suricata, Snort, тощо), наукових публікацій і звітів про інциденти для розуміння архітектури та функціоналу SOC.

– **Порівняльний аналіз** – системне порівняння SIEM-, IDS/IPS-, SOAR-систем та платформ Threat Intelligence за критеріями продуктивності, масштабованості, інтеграції, функціоналу й ефективності виявлення загроз.

– **Метод моделювання** – побудова узагальненої моделі SOC, алгоритмів моніторингу загроз, структури реагування на інциденти та інтеграції між компонентами (SIEM, SOAR, Threat Intelligence, IDS/IPS).

– **Системний підхід** – дослідження SOC як цілісної системи, де взаємодіють технології, персонал, політики безпеки, інструменти реагування й аналітика.

– **Емпіричне дослідження** (огляд кейсів) – розгляд реальних сценаріїв використання Snort, Suricata, Zeek, IBM Resilient SOAR, Splunk SOAR, тощо, в контексті Security Operations Center.

Практичне значення одержаних результатів. Застосування результатів полягає у створенні цілісного підходу до побудови ефективної системи моніторингу кіберзагроз у рамках діяльності Security Operations Center (SOC). Отримані знання, аналітичні матеріали та моделі можна використовувати в реальних умовах для підвищення рівня інформаційної безпеки як в окремих організаціях, так і в масштабі галузі.

Основні аспекти практичного значення:

– **Вдосконалення архітектури SOC**

Запропоновані підходи до побудови SOC, з урахуванням використання SIEM, IDS/IPS, SOAR та платформ Threat Intelligence, дають змогу організаціям формувати гнучку й адаптивну інфраструктуру безпеки.

- **Оптимізація процесів моніторингу та реагування**

Побудовані моделі моніторингу та реагування на інциденти дають змогу скоротити час виявлення та нейтралізації загроз, знизити навантаження на аналітиків SOC і зменшити людський фактор у прийнятті рішень.

- **Інтеграція сучасних рішень безпеки**

Представлений аналіз і порівняння систем (QRadar, Splunk, Zeek, Suricata, SOAR) допомагає приймати обґрунтовані рішення щодо їх впровадження залежно від специфіки організації, бюджету й технічних вимог.

- **Підвищення ефективності реагування на інциденти**

Впровадження сценаріїв автоматизованого реагування (SOAR) дозволяє значно знизити час між виявленням загрози та виконанням захисних дій.

- **Навчання фахівців**

Матеріали дослідження можуть бути використані для підготовки аналітиків SOC, спеціалістів з кібербезпеки та IT-персоналу, сприяючи формуванню практичних навичок роботи з системами виявлення загроз.

- **Реалізація у різних галузях**

Результати дослідження можуть бути впроваджені у фінансовому секторі, держструктурах, енергетиці, охороні здоров’я, телекомі тощо, де потреба в надійному захисті інформаційних систем є критичною.

Розділ 1 АНАЛІЗ ПІДХОДІВ ДО ОРГАНІЗАЦІЇ МОНІТОРИНГУ КІБЕРЗАГРОЗ У SOC

SOC складається з багатьох направлень, але основними є саме моніторинг та аналіз подій пов’язаних зі зберіганням, обробкою, передачою інформації в кіберпросторі.

1.1 Поняття та функціональне призначення Центру оперативного управління безпекою (SOC)

SOC – це централізована команда людей, яка відповідає за покращення кібербезпеки організації та запобігання загрозам, виявлення й реагування на них. Команда SOC, яка може входити до складу організації або складатися із залучених зі сторони виконавців, моніторить стан кінцевих точок, серверів, баз даних, мережевого обладнання, веб-сайтів та інших систем, щоб виявляти потенційні кібератаки в режимі реального часу. Вона також виконує профілактичні заходи із безпеки, застосовуючи аналітику загроз, та спостерігає за актуальними новинами в світі кіберпростору, щоб залишатися в курсі груп загроз та стану інфраструктури, а також виявляти й усувати вразливості систем або процесів, перш ніж ними встигнуть скористатися зловмисники [1].

Більшість SOC працюють цілодобово сім днів на тиждень. Крім того, великі організації, які працюють в кількох країнах, також можуть мати глобальний операційний центр безпеки (GSOC), щоб залишатися в курсі загроз безпеці в усьому світі, а також координувати виявлення та реагування між кількома місцевими центрами оперативного кіберзахисту.

Основні функції SOC зображено на рис. 1.

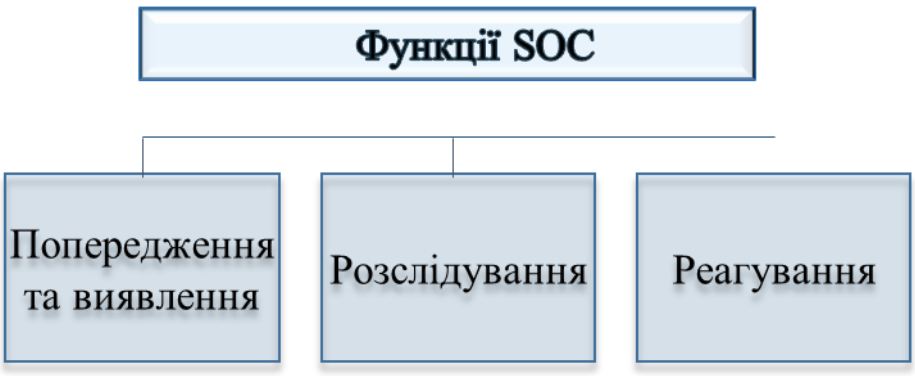

Рис.1. Основні функції SOC

1) Попередження та виявлення.

Коли мова йде про кібербезпеку, запобігання завжди буде більш ефективним, ніж реагування. Замість того, щоб реагувати на загрози, коли вони виникають, SOC працює над цілодобовим моніторингом мережі. Таким чином, команда SOC може виявити зловмисні дії та запобігти їм до того, як вони зможуть завдати шкоди.

Коли аналітик SOC бачить щось підозріле, він збирає якомога більше інформації для глибшого розслідування.

2) Розслідування.

На етапі розслідування SOC-аналітик аналізує підозрілу активність, щоб визначити характер загрози та ступінь її проникнення в інфраструктуру на основі наявних подій. Аналітик з безпеки розглядає мережу та операції організації з точки зору зловмисника, шукаючи ключові індикатори та вразливі місця до того, як вони будуть використані.

Аналітик ідентифікує та сортує різні типи інцидентів безпеки, розуміючи, як розгортаються атаки та як ефективно реагувати на них до того, як вони вийдуть з-під контролю. SOC поєднує інформацію про мережу організації з останніми даними про глобальні загрози, які включають специфіку інструментів, методів і тенденцій зловмисників, щоб виконати ефективне сортування.

3) Реагування.

Після розслідування команда SOC координує заходи з усунення проблеми. Як тільки інцидент підтверджено, команда виступає в ролі першої служби реагування, виконуючи такі дії, як ізоляція кінцевих точок, припинення шкідливих процесів, запобігання їх виконанню, видалення файлів тощо, тобто локалізації проблеми.

Після інциденту SOC працює над відновленням систем і відновленням будь-яких втрачених або скомпрометованих даних. Це може включати очищення та перезавантаження кінцевих точок, переконфігурацію систем або, у випадку атак зловмисників, розгортання життєздатних резервних копій, щоб обійти вірус-вимагач. У разі успіху цей крок поверне мережу до стану, в якому вона перебувала до інциденту.

1.2 Основні загрози та вектори атак, які контролює SOC

Вектори атаки - це різні способи використання існуючих вразливостей комп'ютера для отримання доступу до системи, встановлення шкідливе програмне забезпечення або вкрасти дані.

Хоча в кібербезпеці вивчається багато векторів атак, на практиці зазвичай використовуються кілька основних типів (рис.2) [3].

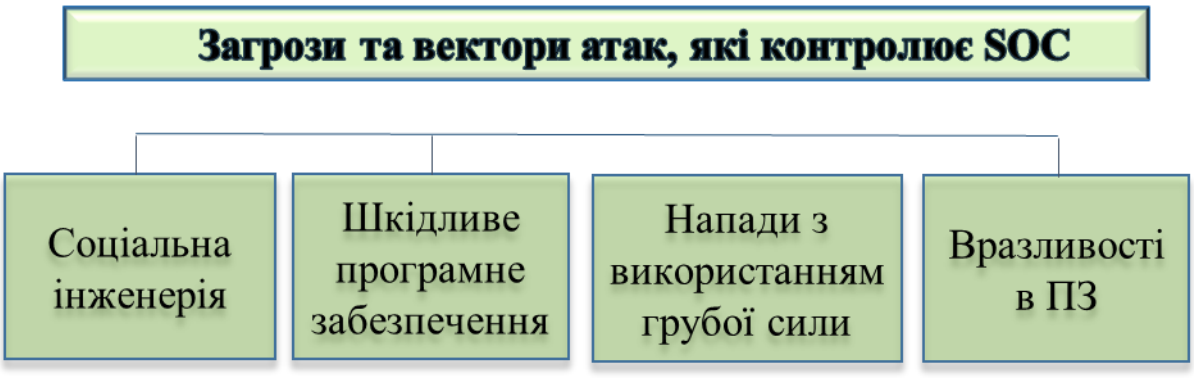

Рис.2. Основні загрози та вектори атак, які контролює SOC

1) Соціальна інженерія.

Соціальна інженерія ґрунтується на психологічному маніпулюванні людьми з метою отримання конфіденційної інформації або схиляння їх до небажаних дій. Деякі випадки включають фішинг (крадіжка особистих даних), а також вішинг (голосові атаки) та атаки через текстові повідомлення.

Щоб уникнути таких атак, необхідно дотримуватись наступних порад:

– Не переходити за підозрілими посиланнями та не завантажувати вкладення з невідомих джерел.

– Перевіряти автентичність та безпечність повідомлень, перш ніж надавати конфіденційну інформацію.

– Бути в курсі останніх тактик та новин щодо соціальної інженерії.

2) Шкідливе програмне забезпечення.

ШПЗ призначене для проникнення або пошкодження комп'ютерних систем. Як приклад, вразливості включають у себе завантаження заражених файлів з невідомих джерел, відкриття підозрілих вкладень листів електронної пошти та відвідування скомпрометованих веб-сайтів.

Для захисту від ШПЗ необхідно:

– Використовувати сучасне антивірусне програмне забезпечення та регулярно сканувати систему на наявність будь-яких зловмисних файлів/програм та підозрілої активності.

– Уникати завантаження програм або файлів з ненадійних сайтів.

– Підтримувати актуальну версію операційної системи та програм, включаючи найновіші патчи безпеки.

3) Напади з використанням грубої сили.

Атаки грубої сили передбачають багаторазові спроби вгадати паролі або ключі шифрування, поки не буде знайдено той, котрий надасть доступ до конфіденційних даних. Це може стосуватися онлайн-сервісів, систем входу або мереж Wi-Fi тощо.

Щоб запобігти атакам грубої сили необхідно:

– Використовувати надійні паролі, що містять комбінацію букв, цифр і спеціальних символів довжиною більше 8 символів, чим більше, ти краще для захисту системи/ОЗ і т.п..

– Використовувати додаткову функцію безпеки, а саме двофакторну автентифікацію, де це можливо.

– Обмежити кількість невдалих спроб входу та тимчасове блокування акаунтів після їх великої кількості.

4) Вразливості в програмному забезпеченні.

Вразливі місця ПЗ – це слабкі місця або недоліки в програмному забезпеченні або операційних системах, якими можуть скористатися кіберзлочинці. Ці вразливості зазвичай виправляються за допомогою оновлень безпеки, впровадження певних обмежень у системі або створенням запитів щодо їх виправлень безпосередньо на його вендора.

Для захисту від вразливостей ПЗ необхідно:

– Підтримувати актуальну версію програмного забезпечення шляхом встановлення найновіших патчів безпеки.

– Використовувати програмне забезпечення для захисту, яке виявляє та блокує відомі вразливості, наприклад антивірус чи EDR.

– Уникати використання програмного забезпечення котре вже застаріле або не підтримується розробниками.

1.3 Забезпечення моніторингу актуальних загроз

Загрози виявляються за допомогою наступних інструментів [4]:

1) Автоматизовані/пасивні інструменти

1.1) Алгоритми машинного навчання та штучний інтелект. Моделі ML аналізують великі обсяги історичних даних, щоб виявляти сучасні

загрози в режимі реального часу. Це дозволяє їм підвищити точність і ефективність процесу виявлення загроз.

1.2) Виявлення та реагування на кінцевих точках - EDR.

Просунуті інструменти виявлення загроз часто інтегруються з рішеннями EDR. Вони відстежують поведінку кінцевих точок в режимі реального часу, виявляють підозрілі дії та полегшують криміналістичний аналіз для виявлення загроз і швидкого реагування на інциденти безпеки, пов'язані з кінцевими точками.

1.3) Автоматизоване реагування на інциденти безпеки - SOAR.

Використовуйте доступні інструменти для прискорення реагування організації на кіберзагрози, зокрема: карантин/ізоляція заражених або скомпрометованих кінцевих точок і систем, блокування зловмисних IP-адрес і запуск робочих процесів усунення наслідків на основі встановлених критеріїв.

2) Активні/людиноцентричні стратегії

2.1) Методи поведінкового аналізу.

Виявлення аномальних патернів і відхилень у поведінці акаунтів, мережевому трафіку, активності додатків і системних процесах дозволяє виявляти компрометації та загрози, які традиційні підходи на основі сигнатур можуть пропустити.

2.2) Полювання на загрози (Threat hunting).

Це проактивний пошук прихованих загроз і ознак компрометації в мережі, який вимагає людського досвіду, розвідки загроз і спеціалізованих інструментів.

2.3) Обманні технології.

Ці технології, так названі «приманки» та «хлібні крихти», заманюють зловмисників до взаємодії з підробленими системами та збирають цінну інформацію про зловмисника. Обман може допомогти виявити вторгнення на ранній стадії, зібрати інформацію про тактику атаки і відвернути увагу супротивника від критично важливих активів.

2.4) Об'єднання розвідданих про загрози.

Агреговані дані про загрози з внутрішньої телеметрії, розвідданих з відкритих джерел (OSINT), галузевих каналів та власних каналів надають більш повне уявлення про ландшафт загроз, актуальних для вашої організації.

1.4 Використання SIEM-систем у SOC для аналізу подій безпеки

Майже кожна сучасна ІС, котра використовується в сфері ІТ, зберігає дані про кожні дії виконані в ній різними користувачами. SIEM – це рішення безпеки, яке за рахунок обробки інформації з інших систем захисту, допомагає організаціям розпізнавати та усувати потенційні загрози безпеці та вразливості, перш ніж вони матимуть шанс порушити роботу бізнесу.

На найпростішому рівні всі SIEM-рішення виконують певний рівень функцій агрегації, консолідації та сортування даних для виявлення загроз та дотримання вимог щодо відповідності даних. Хоча деякі рішення відрізняються можливостями, більшість пропонують однаковий основний набір функцій [5].

Керування журналами подій

SIEM отримує дані подій з широкого кола джерел, залежно від конфігурацій їх логування, по всій ІТ-інфраструктурі організації, включаючи локальні та хмарні середовища.

Дані журналу подій від користувачів, кінцевих точок, програм, джерел даних, хмарних робочих навантажень та мереж, а також дані з апаратного та програмного забезпечення безпеки, такого як брандмауери, антивірусне програмне забезпечення, EDR, NDR і т.д., збираються, корелюються та аналізуються за допомогою SIEM та співробітників SOC в режимі реального часу.

Деякі SIEM-рішення також інтегруються зі сторонніми каналами інформації про загрози, щоб зіставити свої внутрішні дані безпеки з раніше розпізнаними сигнатурами та профілями загроз. Інтеграція з каналами

інформації про загрози в режимі реального часу дозволяє командам блокувати або виявляти нові типи сигнатур атак.

Кореляція та аналітика подій

Кореляція подій є важливою частиною будь-якого SIEM-рішення. Використовуючи розширену аналітику для виявлення та розуміння складних шаблонів даних, кореляція подій надає інформацію для швидкого виявлення та пом'якшення потенційних загроз безпеці бізнесу.

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

Моніторинг інцидентів та сповіщення про безпеку

SIEM об'єднує свій аналіз в єдину централізовану панель інструментів, де команди безпеки відстежують активність, сортують сповіщення, виявляють загрози та ініціюють реагування або усунення наслідків.

Більшість панелей інструментів SIEM також включають візуалізацію даних у режимі реального часу, яка допомагає аналітикам безпеки виявляти сплески або тенденції підозрілої активності. Використовуючи налаштовувані, попередньо визначені правила кореляції, адміністратори можуть негайно отримувати сповіщення та вживати відповідних заходів для зменшення загроз, перш ніж вони перетворяться на більш серйозні проблеми безпеки.

Управління відповідністю нормативним вимогам та звітність

Рішення SIEM є популярним вибором для організацій, які підлягають різним формам дотримання нормативних вимог. Завдяки автоматизованому збору та аналізу даних, які він забезпечує, SIEM є цінним інструментом для отримання та перевірки даних про відповідність по всій бізнес-інфраструктурі.

Рішення SIEM можуть генерувати звіти про відповідність стандартам PCI-DSS, GDPR, HIPAA, SOX та іншим стандартам у режимі реального часу, що зменшує навантаження на управління безпекою та виявляє потенційні порушення на ранній стадії для їх усунення. Багато рішень SIEM постачаються з

попередньо вбудованими, готовими до використання додатками, які можуть генерувати автоматизовані звіти, розроблені для відповідності вимогам.

1.5 Підходи до організації структури відділу SOC

SOC як своєрідна структурна одиниця в архітектурі організації, потребує свого упорядкування, ієрархії. Хоч і досягається одна ціль, але існують різні підходи для реалізації даного завдання.

1) Поділ на аналітиків L1, L2, L3 [6].

Рівень 1 (Line 1).

Основні обов'язки:

– безперервний моніторинг сповіщень безпеки в реальному часі.

– первинна класифікація інцидентів за ступенем серйозності та потенційним впливом.

– детальна документація виявлених загроз.

– ескалація інцидентів, що потребують більшої уваги.

– застосування стандартизованих протоколів реагування.

Необхідні навички:

– базові знання мереж та операційних систем.

– фундаментальне розуміння поширених векторів атак.

– здатність працювати під тиском і в змінному режимі.

– відмінні навички документування та комунікації.

– аналітичний склад розуму та увага до деталей.

Рівень 2 (Line 2):

Основні обов'язки:

– глибокий аналіз складних інцидентів, ескальованих від L1.

– попереднє форензік розслідування скомпрометованих систем.

– координація з іншими відділами для реалізації рішень.

– активне стримування поточних загроз.

– розробка і поліпшення процедур виявлення.

Необхідні навички:

– просунуті знання мережевих протоколів та архітектури систем.

– досвід роботи з інструментами цифрової форензики.

– знайомство з тактиками, техніками і процедурами (TTPs) котры використовують зловмисники.

– здатність корелювати дані з декількох джерел.

– сертифікації, такі як GCIH, Security+ або CySA+.

Рівень 3 (Line 3).

Основні обов'язки:

– проактивний пошук загроз, не виявлених автоматизованими системами.

– аналіз кіберрозвідки та її застосування до безпеки організації.

– розробка нових правил виявлення і методологій аналізу.

– просунуте форензичне розслідування критичних інцидентів.

– стратегічне консультування керівництва з питань безпеки.

Необхідні навички:

– глибокі знання безпеки з боку Red team та Blue team.

– досвід у програмуванні та автоматизації (Python, PowerShell).

– розуміння просунутих технік обходу захисту і персистентності.

– здатність до аналізу першопричин.

– сертифікації, такі як SANS GIAC, OSCP або CISSP.

2) Поділ аналітиків SOC згідно сфер діяльності.

Тут поділ відбувається не аналітичними рівнями, а сферами діяльності, наприклад:

– аналітики для проведення розслідувань;

– malware аналітики;

– SOC інженери.

3) Без як такого поділу.

Висновки до розділу 1

SOC є важливою частиною IT-інфраструктури будь-якої діджіталізованої організації, адже саме саме за допомогою нього забезпечується як моніторинг усіх подій, так і виявлення загроз, кібератак, реагування тощо. У процесі діяльності, співробітники відділу ІБ можуть взаємодіють з багатьма інструментами захисту, наприклад SIEM, EDR, NDR, XDR, IDS, IPS, MSG, DLP. Інформація, отримувана зі всіх систем використовується для вищеперерахованих дій та дає можливість розслідувати можливі інциденти ІБ в організації, забезпечуючи повноцінний захист її кіберпростору.

Розділ 2 ІНСТРУМЕНТИ ТА ТЕХНОЛОГІЇ ДЛЯ ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ В SOC

2.1 SIEM-системи (QRadar, Splunk, Elasticsearch): можливості та функціонал

2.1.1 IBM QRadar SIEM

IBM QRadar SIEM – це потужна платформа для управління інформаційною безпекою та подіями (SIEM), яка забезпечує централізований моніторинг, аналіз та реагування на загрози в реальному часі. Вона допомагає організаціям виявляти, розслідувати та реагувати на кіберзагрози, а також дотримуватися вимог нормативного регулювання [6].

Основні функції та можливості IBM QRadar SIEM розглянуті в таблиці 1[7, 8, 9].

Таблиця 1

Основні функції та можливості системи QRadar SIEM

Категорія	Опис
Збір даних	Консолідація логів, мережевого трафіку, подій безпеки та даних про активи з різних джерел.
Нормалізація	Перетворення різнорідних даних у стандартизований формат для подальшого аналізу.
Кореляція подій	Виявлення складних атак шляхом аналізу взаємозв'язків між подіями з різних джерел на основі кореляційних правил.
Аналіз поведінки	Виявлення аномалій у поведінці користувачів та систем для виявлення потенційних загроз.

Продовження таблиці 1

Інтеграція з Threat Intelligence	Використання зовнішніх джерел інформації про загрози для покращення виявлення та реагування на атаки.
Автоматизація реагування	Автоматичне створення інцидентів, оповіщень та запуск відповідних дій у відповідь на виявлені загрози.
Звітування та дотримання нормативних вимог	Генерація звітів для аудиту та відповідності стандартам безпеки (наприклад, GDPR, HIPAA, PCI DSS). Звіти можуть бути створені для їх генерації користувачами, так і автоматичного генерування.
Масштабованість	Підтримка розгортання в хмарі, на локальних серверах або в гібридному середовищі.
Дослідження загроз	Автоматизований процес, ініційований модулями Threat Investigator і Case Management, визначає випадки, які потребують подальшого вивчення. Він знаходить артефакти, пов'язані зі спрацюваннями і запускає операцію з видобування даних для складання детальної хронології інциденту, що включає тактику і методи MITRE ATT&CK з візуальним ланцюговим графіком.
Є центром виявлення та реагування	Централізує управління сценаріями використання виявлення та реагування, полегшуючи впровадження нових заходів безпеки. Допомагає командам безпеки керувати різноманітним набором протоколів безпеки, дозволяючи створювати, переглядати та коригувати правила виявлення за допомогою інтуїтивно зрозумілого редактора правил.

Продовження таблиці 1

Має уніфікований користувацький інтерфейс	Забезпечує узгодженість між користувацьким інтерфейсом з іншими продуктами IBM (EDR, XDR, Log Insights, SOAR), що дає можливість інтуїтивного сприйняття та легкого користування інтерфейсу для користувача, якщо він працював якимось з інших раніше.
Дашборди	У системі можна створювати різного роду дашборди, на основі спрацювань та їх даних, користувачів, пошуків.
Можливість категоризації спрацювань	Для пріорітизації та визначення критичності спрацювань у системі (Offenses) у системі є показники Severity, Credibility, Relevance

IBM QRadar SIEM вирішує основні проблеми, котрих стосується даний вид систем захисту.

– Зменшення кількості хибнопозитивних спрацювань.

Завдяки кореляції подій та аналізу поведінки система зменшує кількість помилкових оповіщень, дозволяючи аналітикам зосередитися на реальних загрозах.

– Швидке виявлення та реагування на загрози.

Реальний час обробки даних дозволяє оперативно виявляти та реагувати на інциденти безпеки.

– Централізований моніторинг.

Об'єднання даних з різних джерел в єдину консоль забезпечує повну видимість ситуації з безпекою в організації.

– Дотримання нормативних вимог.

Автоматизоване створення звітів та аудитів допомагає організаціям відповідати вимогам різних стандартів безпеки.

2.1.2 Splunk Enterprise Security.

Splunk ES - провідна на ринку система SIEM, яка забезпечує комплексну видимість, точне виявлення та підвищує операційну ефективність, що має вирішальне значення для забезпечення роботи SOC майбутнього [10].

Основні функції та можливості Splunk ES розглянуті в таблиці 2[11, 12]:

Таблиця 2

Основні функції та можливості системи Splunk ES

Категорія	**Опис**
Збір даних	Консолідація логів, мережевого трафіку, подій безпеки та даних про активи з різних джерел.
Нормалізація	Перетворення різнорідних даних у стандартизований формат для подальшого аналізу.
Кореляція подій	Виявлення складних атак шляхом аналізу взаємозв'язків між подіями з різних джерел на основі кореляційних пошуків.
Аналіз поведінки	Виявлення аномалій у поведінці користувачів та систем для виявлення потенційних загроз.
Інтеграція з Threat Intelligence	Використання зовнішніх джерел інформації про загрози для покращення виявлення та реагування на атаки.
Автоматизація реагування	Автоматичне створення інцидентів, оповіщень та запуск відповідних дій у відповідь на виявлені загрози.
Звітування та дотримання нормативних вимог	Генерація звітів для аудиту та відповідності стандартам безпеки (наприклад, GDPR, HIPAA, PCI DSS). Звіти можуть бути створені для їх генерації користувачами, так і автоматичного генерування.

Продовження таблиці 2

Масштабованість	Підтримка розгортання в хмарі, на локальних серверах або в гібридному середовищі.
Дашборди	У системі можна створювати різного роду дашборди, на основі спрацювань та їх даних, користувачів, пошуків.
Можливість категоризації спрацювань	Для пріорітизації та визначення критичності спрацювань у системі (Incident) у системі є показники згідно з міжнародними фреймворками, а саме: - CIS 20 (топ 20 базових контролів ІБ рекомендовані організацією: Center for Internet Security [13]); - Kill Chein (модель визначає, що саме повинні зробити противники, щоб досягти своєї мети [14]); - MITTR ATTACK (база знань, котра містить у собі інформацію щодо найпоширеніших тактик та технік, котрі використовують зловмисники при проведенні. різного роду кібератак як на системи, так і користувачів [15]).

Splunk ES як і IMB QRadar SIEM, вирішує ті ж проблеми в організаціях бо вони є одним і тим же типом систем захисту, але при цьому, вони мають певні відмінності між собою, що описано в таблиці 3 [16, 17, 18, 19, 20].

Таблиця 3

Порівняння Splunk ES та IBM QRadar SIEM

Критерій	**Splunk Enterprise Security (ES)**	**IBM QRadar SIEM**
Основна перевага	Потужна аналітика даних, гнучкість у налаштуванні, розширені можливості інтеграції.	Інтегрована система безпеки з автоматизованим збором логів, виявленням аномалій та інцидентів.
Масштабованість	Висока; підходить для великих організацій з великими обсягами даних.	Підходить для середніх та великих підприємств; добре інтегрується з іншими продуктами IBM.
Аналітика та ML	Розширені можливості аналітики з використанням машинного навчання; гнучке налаштування правил та дашбордів.	Вбудовані можливості аналітики; фокус на автоматизації та спрощенні процесів безпеки.
Інтеграція	Широкий спектр інтеграцій з різними сторонніми рішеннями; підтримка великої кількості джерел даних.	Глибока інтеграція з екосистемою IBM; підтримка стандартних джерел даних.
Складність навчання	Вища; вимагає більше часу на освоєння та налаштування.	Нижча; більш інтуїтивно зрозумілий інтерфейс та налаштування.

Продовження таблиці 3

Ціна	Базується на обсязі індексованих даних; може бути дорогим при великих обсягах.	Базується на кількості користувачів та оброблених подій; більш передбачуване ціноутворення.
Відповідність нормативним вимогам	Підтримка широкого спектру стандартів безпеки та відповідності (наприклад, GDPR, HIPAA, PCI DSS).	Вбудовані шаблони та звіти для відповідності стандартам безпеки.
Розгортання	Підтримка хмарних, локальних та гібридних розгортань.	Підтримка локальних та хмарних розгортань; добре підходить для організацій, що вже використовують продукти IBM.

2.1.3 Elasticsearch

Elasticsearch, як частина Elastic Stack (раніше відомого як ELK Stack), є потужним інструментом для реалізації SIEM-рішень (Security Information and Event Management). Завдяки своїй масштабованості, гнучкості та інтеграції з іншими компонентами Elastic Stack, Elasticsearch дозволяє ефективно збирати, аналізувати та візуалізувати дані безпеки.

Сам Elasticsearch не такий сильний інструмент, якщо не використовується у взаємозв’язку з іншими системами, як приклад це може бути конструкція описана в таблиці 4 [21].

Таблиця 4

Компоненти для повної реалізації Elasticsearch як SIEM

Компонент	**Опис**
Elasticsearch	Ядро для зберігання та пошуку даних.
Logstash	Інструмент для обробки та трансформації даних перед їх зберіганням.
Beats	Легкі агенти для збору даних з різних джерел.
Kibana	Інтерфейс для візуалізації та аналізу даних.

Основні функції та можливості Elasticsearch описано в таблиці 5[22].

Таблиця 5

Основні функції та можливості системи Elasticsearch

Категорія	**Опис**
Збір даних	Консолідація логів, мережевого трафіку, подій безпеки та даних про активи з різних джерел.
Нормалізація	Перетворення різнорідних даних у стандартизований формат для подальшого аналізу.
Кореляція подій	Виявлення складних атак шляхом аналізу взаємозв'язків між подіями з різних джерел на основі кореляційних пошуків.
Аналіз поведінки	Виявлення аномалій у поведінці користувачів та систем для виявлення потенційних загроз.

Продовження таблиці 5

Звітування та дотримання нормативних вимог	Генерація звітів для аудиту та відповідності стандартам безпеки (наприклад, GDPR, HIPAA, PCI

	DSS). Звіти можуть бути створені для їх генерації користувачами, так і автоматичного генерування.
Масштабованість	Підтримка розгортання в хмарі, на локальних серверах або в гібридному середовищі.
Дашборди	У системі можна створювати різного роду дашборди, на основі спрацювань та їх даних, користувачів, пошуків.
Можливість категоризації спрацювань	Для пріорітизації та визначення критичності спрацювань у системі (Incident) у системі є показники згідно з MITTR ATTACK (база знань, котра містить у собі інформацію щодо найпоширеніших тактик та технік, котрі використовують зловмисники при проведенні

2.2 Використання систем IDS/IPS (Snort, Suricata, Zeek) для виявлення вторгнень

Snort – це відкрита система виявлення та запобігання вторгненням (IDS/IPS), розроблена для аналізу мережевого трафіку в реальному часі [23]. Вона здатна виявляти різноманітні загрози, такі як:

- атаки типу DoS/DDoS;
- сканування портів;
- SQL-ін'єкції;
- шкідливе ПЗ;
- підозрілі шаблони трафіку.

Snort може працювати в трьох основних режимах [24]:

1. Sniffer Mode.

Захоплення та відображення мережевих пакетів у реальному часі.

2. Packet Logger Mode.

Запис пакетів на диск для подальшого аналізу.

3. Network Intrusion Detection System (NIDS) Mode.

Аналіз трафіку на основі заданих правил для виявлення підозрілої активності.

Suricata – це відкрита система виявлення та запобігання вторгненням (IDS/IPS), яка також виконує функції мережевого моніторингу безпеки (NSM) [25]. Вона здатна аналізувати мережевий трафік у реальному часі, виявляти загрози та, за потреби, блокувати шкідливу активність.

Zeek – це відкрита система моніторингу мережевої безпеки (NSM), яка також виконує функції системи виявлення вторгнень (IDS) [26]. Вона здатна аналізувати мережевий трафік у реальному часі, виявляти загрози та надавати детальну інформацію для подальшого аналізу.

Основні можливості IDS/IPS зображено на рис. 3 та детальніше описано в таблиці 6.

Рис.3. Основні функції IDS/IPS системи

Таблиця 6

Основні можливості IDS/IPS

Категорія	**Опис**

Аналіз протоколів	Підтримка TCP, UDP, ICMP, HTTP, FTP, DNS та інших протоколів.
Пошук за вмістом	Виявлення загроз на основі сигнатур та шаблонів у трафіку.
Гнучкі правила	Можливість створення власних правил для специфічних потреб.
Інтеграція з SIEM	Передача логів та сповіщень до систем управління інформацією про безпеку.
Підтримка спільноти	Велика база готових правил та активна спільнота користувачів.

Переваги та недоліки IDS/IPS на прикладі Snort, Suricata, Zeek описано в таблиці 7.

Таблиця 7

Основні переваги та недоліки IDS/IPS на прикладі Snort, Suricata, Zeek

Переваги	**Недоліки**
Відкритий вихідний код	Потребує глибоких знань для налаштування та підтримки
Гнучкість та масштабованість	Може бути складним у великих мережах з високим трафіком
Широка підтримка спільноти	Потребує регулярного оновлення правил для ефективності

Продовження таблиці 7

Інтеграція з іншими інструментами безпеки	Може потребувати додаткових ресурсів для обробки великого обсягу даних

Використання IDS/IPS у SOC

У центрах моніторингу безпеки (SOC) IDS/IPS використовується для:

– моніторингу мережевого трафіку в реальному часі;

– виявлення та сповіщення про підозрілу активність;

– інтеграції з системами управління подіями безпеки (SIEM)) та відповідно розширеного моніторингу загроз;

– аналізу інцидентів та реагування на загрози.

2.3 Роль платформ Threat Intelligence у моніторингу загроз

Threat Intelligence Platform (TIP) – це програмне забезпечення або набір інструментів, призначених для збору, аналізу та управління даними про потенційні кіберзагрози. TIP автоматизує процеси обробки великої кількості даних з різних джерел, надаючи аналітикам структуровану та актуальну інформацію для прийняття рішень [27].

Інтеграція TIP у SOC дозволяє [28]:

– ідентифікувати та реагувати на загрози до настання наслідків;

– корелювати сповіщення з відомими індикаторами компрометації (IOC) та тактиками, техніками і процедурами (TTP);

– автоматизувати виявлення та реагування на загрози за допомогою TIP та рішень SOAR;

– підвищити ефективність аналітиків SOC, зменшуючи кількість хибнопозитивних сповіщень та пріоритезуючи критичні загрози.

Приклади популярних TIP наведено у таблицы 8[29, 30, 31, 32].

Таблиця 8

Популярні TIP

Платформа	**Особливості**

Anomali ThreatStream	Оцінка загроз за допомогою машинного навчання, інтеграція з EDR, SIEM та фаєрволами, підтримка різних джерел загроз.
Recorded Future	Збір даних з відкритих, глибоких та темних веб-джерел, використання машинного навчання для аналізу загроз.
MISP	Відкрите програмне забезпечення для збору, зберігання та обміну індикаторами загроз, підтримка стандартів STIX/TAXII.
Cisco Talos	Надає інформацію про останні кіберзагрози, зокрема шкідливе ПЗ та активність загрозливих акторів.
ANY.RUN	Інтерактивна пісочниця для аналізу шкідливого ПЗ, інтеграція з іншими інструментами безпеки.

Переваги систем TIP наступні: проактивний захист, зменшення кількості хибнопозитивних сповіщень, покращують ефективності SOC, інтегруються з іншими інструментами безпеки. Окрім вищеперерахованих плюсів, вони мають і недоліки, наприклад: можуть бути складними у впровадженні та налаштуванні, потребують регулярного оновлення даних про загрози, можуть вимагати додаткових ресурсів для обробки великого обсягу даних, потребують навчання персоналу для ефективного використання.

2.4 Автоматизація SOC за допомогою SOAR-рішень (IBM Resilient SOAR, Splunk SOAR)

Реакції на спрацювання та інциденти, які моніторить SOC, можливо автотизувати за допомогою рішень SOAR що є ключовим кроком до підвищення ефективності та швидкості реагування на кіберзагрози. Серед провідних платформ у цій галузі – IBM Resilient SOAR та Splunk SOAR, які широко використовуються в більшості відділів SOC.

SOAR – це набір інструментів, які дозволяють автоматизувати та оркеструвати процеси реагування на інциденти безпеки. Вони інтегруються з різними системами безпеки, такими як SIEM, EDR, фаєрволи та інші, забезпечуючи централізоване управління інцидентами та зменшуючи навантаження на аналітиків SOC.

У контексті SOC, SOAR-рішення виконують такі функції:

– автоматизація рутинних завдань: наприклад, обробка фішингових листів або блокування шкідливих IP-адрес;

– оркестрація процесів: координація дій між різними системами безпеки для ефективного реагування на загрози;

– збагачення інцидентів: додавання контекстної інформації до подій безпеки для кращого розуміння ситуації;

– стандартизація реагування: використання шаблонів (playbooks) для уніфікованого реагування на типові загрози.

Переваги впровадження SOAR у SOC [33, 34]:

– швидше реагування на інциденти: автоматизація дозволяє зменшити час реагування з годин до хвилин;

– зменшення навантаження на аналітиків: автоматизація рутинних завдань дозволяє фокусуватися на складніших загрозах;

– покращення якості розслідувань: збагачення інцидентів контекстною інформацією сприяє більш точному аналізу;

– стандартизація процесів: використання шаблонів забезпечує уніфіковане реагування на типові загрози.

Проблеми, котрі виникнуть при впровадженні SOAR у SOC:

– складність впровадження: необхідність ретельного планування та налаштування інтеграцій;

– потреба в навчанні персоналу: аналітики повинні бути навчені ефективному використанню SOAR-платформ;

– вартість: висока початкова інвестиція;

– підтримка та документація: деякі платформи мають обмежену документацію та потребують покращення технічної підтримки.

Ключові кроки при впровадженні SOAR системи:

– оцінка потреб: визначення основних завдань, які потребують автоматизації;

– вибір платформи: аналіз доступних рішень з урахуванням специфіки організації;

– інтеграція з існуючими системами: налаштування взаємодії з SIEM, EDR та іншими інструментами;

– розробка playbooks: створення шаблонів для автоматизованого реагування на типові інциденти;

– навчання персоналу: підготовка аналітиків до роботи з новими інструментами;

– моніторинг та оптимізація: постійне вдосконалення процесів на основі отриманих результатів.

Порівняння IBM Resilient SOAR та Splunk SOAR описано в таблиці 9.

Таблиця 9

Порівняння IBM Resilient SOAR та Splunk SOAR

Характеристика	**IBM Resilient SOAR**	**Splunk SOAR**
Інтеграція	Швидка інтеграція з існуючими системами	Підтримка понад 300 сторонніх інструментів
	безпеки та IT-інфраструктурою.	та понад 2800 автоматизованих дій.

Автоматизація	Можливість створення кастомних playbooks для автоматизації процесів.	Візуальний редактор playbooks для спрощення створення автоматизованих сценаріїв.
Масштабованість	Підходить для середніх та великих організацій.	Висока масштабованість, підходить для організацій будь-якого розміру.
Підтримка та документація	Потребує покращення технічної підтримки та документації.	Деякі користувачі відзначають недостатню деталізацію документації.
Вартість	Конкурентоспроможна ціна для корпоративного сегменту.	Висока вартість, що може бути обмеженням для малих організацій.

Висновки до розділу 2

Сучасна архітектура системи моніторингу в SOC (Security Operations Center) потребує комплексного підходу до виявлення, аналізу та реагування на кіберзагрози. Основою такого підходу є інтеграція інструментів, що доповнюють одне одного у виконанні ключових функцій безпеки – від збирання подій до автоматизованого реагування. Зокрема, SIEM-системи, IDS/IPS-рішення,

платформи Threat Intelligence і засоби автоматизації SOAR утворюють єдину екосистему для ефективного управління інцидентами інформаційної безпеки.

SIEM-платформи, такі як IBM QRadar, Splunk та Elasticsearch, виконують роль центрального вузла збору, нормалізації, кореляції та збереження логів і подій з різних джерел. Вони забезпечують гнучкий пошук, побудову дашбордів, генерацію оповіщень і звітів, що є критично важливим для раннього виявлення інцидентів та забезпечення відповідності політикам безпеки. Завдяки глибокій інтеграції з іншими інструментами, SIEM виступає основою для централізованого моніторингу в SOC.

На рівні мережевого аналізу важливу роль відіграють IDS/IPS-системи – Snort, Suricata та Zeek. Вони дозволяють виявляти аномальні мережеві активності, підозрілу поведінку, відомі атаки, а також проводити детальний аналіз трафіку. Snort і Suricata забезпечують потужний сигнатурний та поведінковий аналіз, а Zeek (раніше Bro) фокусується на глибшому мережевому моніторингу з можливістю збагачення інцидентів контекстною інформацією. Їх використання забезпечує видимість того, що відбувається на мережевому рівні, що значно підвищує ефективність виявлення загроз.

Доповненням до внутрішнього моніторингу виступають платформи Threat Intelligence, які постачають інформацію про актуальні зовнішні загрози. Вони надають аналітикам SOC можливість зіставляти внутрішні події з відомими індикаторами компрометації (IOC), тактиками та техніками атак. Завдяки впровадженню платформ TI зростає контекстуальність аналізу подій, покращується точність пріоритезації інцидентів і підвищується швидкість реагування на загрози ззовні.

Насамкінець, автоматизація SOC за допомогою SOAR-рішень, таких як TheHive або Shuffle, дозволяє значно зменшити час реагування на інциденти, мінімізувати людський фактор і стандартизувати процедури обробки подій. Вони дають змогу створювати сценарії (playbooks), що автоматизують типові дії – наприклад, ізоляцію хостів, інформування користувачів, блокування IP-адрес або відкриття тикетів для розслідування. Автоматизація не лише підвищує

ефективність SOC, але й оптимізує використання людських ресурсів, звільняючи час аналітиків для розслідування складніших інцидентів.

Отже, побудова надійної системи моніторингу в SOC потребує цілісного підходу, де SIEM-системи виступають центром збору і кореляції, IDS/IPS – першою лінією оборони в мережі, Threat Intelligence – джерелом знань про зовнішні загрози, а SOAR – інструментом ефективної автоматизації реагування. Така синергія технологій дозволяє створити стійку, гнучку й адаптивну систему кіберзахисту, здатну протистояти сучасним викликам у сфері безпеки.

Розділ 3 РОЗРОБКА МЕТОДІВ ОРГАНІЗАЦІЇ МОНІТОРИНГУ В SOC

3.1 Архітектура SOC та вимоги до побудови моніторингової системи

Проаналізовано архітектуру центру оперативної безпеки (Security Operations Center, SOC) та визначено вимоги до системи моніторингу. SOC являє собою централізований підрозділ, що цілодобово (24/7) відстежує IT-інфраструктуру організації з метою своєчасного виявлення, аналізу та реагування на інциденти безпеки [36]. Основною метою SOC є забезпечення раннього виявлення кібератак і оперативного реагування на них шляхом об'єднання всіх технологій кібербезпеки та процесів в єдину скоординовану систему [36]. Дослідження підтверджують, що наявність належної системи моніторингу активів і інфраструктури є критичною для швидкого виявлення інцидентів; зокрема, впровадження SOC із використанням системи управління подіями та інформацією безпеки (Security Information and Event Management, SIEM) у поєднанні з іншими засобами значно підвищує видимість загроз та ефективність реагування [37, 38]. Таким чином, архітектура SOC покликана забезпечити повну видимість стану безпеки у всіх ключових вузлах мережі та системах організації [37, 38].

Основні компоненти архітектури SOC умовно поділяються на три категорії: люди, процеси та технології. До компонента «люди» належить команда фахівців з кібербезпеки – аналітики моніторингу, інженери з безпеки, спеціалісти з реагування на інциденти, мисливці за загрозами (threat hunters) тощо – які володіють належними навичками для аналізу та нейтралізації загроз. Процеси – це регламентовані процедури та політики SOC, що описують порядок дій під час інцидентів, інтеграцію розвідки загроз, забезпечення відповідності стандартам тощо. Процеси повинні бути чітко задокументовані, регулярно переглядатися та покращуватися на основі досвіду і постінцидентного аналізу. Технологічна складова охоплює інструменти та платформи, необхідні для реалізації

моніторингу й реагування. Ключовими технологічними компонентами сучасного SOC є:

– **Система SIEM**.

SIEM є центральним вузлом моніторингу: збирає журнали подій і дані безпеки з різних джерел, зберігає їх, аналізує в режимі наближеному до реального часу та виявляє підозрілі дії [37, 38]. SIEM корелює події між собою, генерує оповіщення про потенційні інциденти та надає засоби для проведення поглибленого аналізу. Дані до SIEM можуть надходити через стандартні журнали (наприклад, Syslog) або за допомогою агентів збору логів. Цей компонент забезпечує централізований збір даних, їхню кореляцію, зберігання для потреб цифрової криміналістики та формування звітності.

– **Системи виявлення вторгнень (IDS/IPS) та засоби розширеного виявлення й реагування (EDR/XDR).**

IDS (Intrusion Detection System) аналізує мережевий трафік і системні логи, порівнюючи їх зі шаблонами відомих атак або відхиленнями від норми, з метою виявлення зловмисної активності [37, 38]. Система запобігання вторгнень (IPS) може автоматично блокувати виявлені атаки. EDR (Endpoint Detection and Response) зосереджується на моніторингу кінцевих пристроїв (робочих станцій, серверів) та виявленні ознак компрометації на них. Інструменти XDR (eXtended Detection and Response) об’єднують дані з різних джерел (мережа, кінцеві точки, хмара) для ширшого огляду та виявлення складних загроз. Згідно з результатами експериментального впровадження SOC, використання відкритого ПЗ на зразок Wazuh (платформа SIEM+XDR) у поєднанні з IDS (наприклад, Suricata) дозволяє успішно виявляти різні типи атак (brute-force, шкідливе ПЗ, DoS тощо) та проводити відповідне реагування [37, 38].

– **Платформа розвідки загроз (Threat Intelligence Platform).**

Цей компонент накопичує та аналізує дані про актуальні кіберзагрози з зовнішніх і внутрішніх джерел. Інтеграція розвідки загроз дозволяє корелювати активність, виявлену в інфраструктурі, з відомими тактиками та індикаторами компрометації (IoC) [37, 38]. Наприклад, при спрацюванні оповіщення SIEM

аналітик SOC може звірити підозрілі IP-адреси або хеші файлів із базою відомих IoC. За рекомендаціями профільних організацій, підвищити якість виявлення допомагає використання таксономій атак на кшталт MITRE ATT&CK, що структурує відомі техніки зловмисників і слугує базисом для побудови моніторингових випадків [39]. Регулярне оновлення даних про загрози та тенденції атак є обов'язковим для підтримання актуальності системи моніторингу.

– **Інструменти керування вразливостями та конфігураціями.**

SOC також виконує превентивні функції: проводить сканування вразливостей у вузлах мережі, перевіряє відповідність налаштувань систем рекомендованим безпечним конфігураціям та вимогам політик [37, 38]. Ці засоби не лише виявляють слабкі місця (незакриті вразливості, неправильні налаштування), а й відстежують зміни конфігурацій, щоби запобігти відхиленням від політик безпеки. Результати регулярного аудиту вразливостей та відповідності (compliance) передаються команді SOC для оцінки ризиків і планування заходів захисту.

– **Засоби оркестрації та автоматизації реагування (SOAR) і системи управління інцидентами.**

SOAR дає змогу автоматизувати рутинні операції: фільтрацію незначних оповіщень, збір додаткових даних при інциденті, виконання стандартних реакцій (блокування IP, ізоляція хоста тощо). Інтеграція SOAR зі SIEM та іншими інструментами дозволяє суттєво скоротити час реакції та зменшити навантаження на аналітиків [40]. Для ведення випадків інцидентів застосовуються спеціалізовані платформи (наприклад, системи керування інцидентами та розслідуваннями, такі як TheHive), де фіксуються всі дії по інциденту, відповідальні особи, статус і результати розслідування [37, 38]. Це забезпечує контроль за повним життєвим циклом інциденту – від виявлення до закриття – та накопичення бази знань для подальшого навчання.

Для успішного функціонування SOC висуваються такі вимоги до моніторингової системи:

– **Повнота покриття джерел даних.**

Система повинна збирати телеметрію з усіх критичних елементів IT-інфраструктури: мережевого обладнання, серверів, баз даних, робочих станцій, хмарних сервісів, застосунків тощо. Чим ширше покриття – тим вища ситуаційна обізнаність SOC щодо потенційних загроз. Недостатність даних може призвести до пропущених інцидентів. Тому організація має підтримувати актуальний реєстр активів і джерел логів, які потрібно моніторити [36].

– **Оперативність і постійність моніторингу.**

SOC повинен функціонувати безперервно, забезпечуючи неперервний моніторинг подій безпеки у режимі, близькому до реального часу [37]. Виявлення загрози має відбуватися якомога раніше після її виникнення, аби мінімізувати час перебування зловмисника в системі. Для цього архітектура SOC передбачає високу пропускну здатність для обробки потоків подій та масштабованість рішень (можливість обробляти зростаючі обсяги даних) [41]. Також важливо мати резервні механізми збору й аналізу логів на випадок збоїв окремих компонентів.

– **Точність виявлення та мінімізація хибних спрацювань.**

Моніторингова система повинна мати налаштовані правила кореляції та моделі аномалій, що забезпечують надійне виявлення реальних інцидентів і зменшують кількість false positives (помилкових тривог). Використання кількох методів детектування (сигнатурного, поведінкового, статистичного) та контекстного збагачення подій (даними про активи, користувачів, загрози) підвищує точність спрацьовувань. Наприклад, впровадження UEBA (User and Entity Behavior Analytics) дозволяє виявляти аномалії у поведінці користувачів, які можуть свідчити про компрометацію облікового запису. При цьому важливо, щоб налаштування порогів і правил виявлення регулярно переглядались з урахуванням актуальних даних, аби алгоритми залишались чутливими до нових типів атак, але стійкими до шумів.

– **Інтеграція та сумісність компонентів.**

Всі елементи SOC мають бути тісно інтегровані між собою, утворюючи єдину екосистему. Це означає, що інструменти моніторингу, аналітики та реагування повинні обмінюватись даними в автоматизованому режимі. Наприклад, SIEM має отримувати дані з усіх сенсорів, SOAR – автоматично забирати контекст з SIEM і запускати скрипти реакції, платформа розвідки загроз – збагачувати події в SIEM зовнішніми даними тощо. Відсутність інтеграції призводить до розрізненості та втрати часу на ручне об'єднання інформації. Сучасні підходи передбачають використання єдиних консолей (наприклад, об'єднані консолі XDR) та відкритих API для взаємодії різнорідних засобів безпеки [40].

– **Автоматизація рутинних дій.**

Автоматизація моніторингу та реагування є критичним чинником швидкодії SOC. Повторювані операції – фільтрація спам-алертів, збір стандартних артефактів, первинна діагностика – повинні виконуватися автоматично за наперед визначеними сценаріями (плейбуками). Завдяки SOAR платформи виконують ці дії на машинній швидкості, вивільняючи час аналітиків для складніших завдань [40]. Автоматизація прискорює реакцію, зменшує людський фактор і допомагає масштабувати захист під зростаючий потік атак [40]. Разом з тим, критично важливо мати можливість ручного контролю та втручання фахівця у нетипових ситуаціях.

– **Кваліфікований персонал та налагоджені процеси.**

Технології не принесуть користі без професійної команди та чітких процедур. Вимога до SOC – укомплектувати штат компетентними аналітиками та інженерами, забезпечити їх навчання і тренінги. Має бути налагоджена система управління знаннями (обмін досвідом, база інцидентів). Процеси реагування повинні бути відпрацьовані і підтримуватись керівництвом. Відсутність достатньої кількості навчених кадрів та слабка організаційна підтримка є одними з найбільших перешкод для ефективності SOC [42]. За даними досліджень, понад 57% опитаних SOC назвали дефіцит кваліфікованого

персоналу головною проблемою, а близько 50% вказали на брак автоматизації як серйозний бар’єр [42]. Таким чином, при побудові SOC необхідно приділити увагу не лише вибору технологій, але й інвестиціям у персонал та оптимізацію процесів.

Загалом, правильно спроєктована архітектура SOC поєднує людей, процеси й технології таким чином, щоб забезпечити проактивний захист організації. Вона повинна бути масштабованою, інтегрованою та адаптивною – з можливістю впровадження нових інструментів та методів по мірі еволюції кіберзагроз [41]. Постійний моніторинг ефективності SOC та внесення удосконалень (наприклад, тренування команди, оновлення процедур, впровадження штучного інтелекту) є необхідним для підтримання високого рівня кіберстійкості організації [43, 44].

3.2. Вибір оптимального підходу до виявлення загроз.

У цьому підрозділі розглянуто підходи до виявлення кіберзагроз та обґрунтовано вибір оптимальної стратегії для SOC. Існують дві базові методології детектування: **сигнатурна** (правилорієнтована) та **аномалійна** (поведінкова). Сигнатурний підхід полягає у порівнянні мережевих пакетів чи подій із наперед відомими паттернами атак або сигнатурами шкідливих програм. Якщо ознаки події співпадають з шаблоном відомої загрози – система генерує тривогу. Натомість поведінковий підхід відстежує відхилення від нормальної поведінки користувачів чи систем і сигналізує при виявленні незвичних, потенційно шкідливих дій [44]. Наприклад, різке збільшення обсягу вихідного трафіку з сервера або нестандартні дії користувача о 3:00 ночі можуть бути розцінені як аномалія, що вимагає уваги аналітика.

Кожен з підходів має сильні та слабкі сторони. **Сигнатурні** (IDS, в тому числі антивіруси, системи аналізу трафіку на основі правил) ефективні для швидкого розпізнавання відомих атак і практично не дають хибних спрацювань на легітимну активність. Їхній головний недолік – нездатність виявляти нові, ще не відомі науці атаки або модифіковані експлойти, для яких немає наперед підготовлених сигнатур. **Аномалійні методи** (поведінковий аналіз, машинно-навчальні моделі) здатні розпізнати невідомі раніше атаки, оскільки спираються не на сигнатури, а на відхилення від базових ліній (baseline) нормальної активності. Це дає шанс виявити навіть «нульові» атаки або внутрішніх зловмисників, чия поведінка не відповідає типовій. Ціна такої чутливості – більша кількість помилкових тривог, адже будь-яка нестандартна, але легітимна дія (наприклад, нетипове використання прав адміністрування) також може бути позначена як аномалія. Крім того, поведінкові системи потребують достатнього обсягу якісних даних для навчання моделей і можуть бути складнішими у налаштуванні.

З огляду на вказані особливості, **оптимальним підходом** до виявлення загроз у SOC визнано **комбінований**, багаторівневий підхід, що поєднує переваги обох методологій. Гібридні системи здійснюють базове фільтрування за сигнатурами відомих атак (щоб відсіювати очевидні загрози з мінімальними витратами ресурсів) та передають нестандартні випадки на глибший аналіз аномалійними моделями [44]. Така двоступенева схема дозволяє зменшити навантаження на алгоритми поведінкового аналізу і знизити частку хибних спрацювань, не втративши при цьому невідомі атаки. Сучасні дослідження підтверджують ефективність гібридного підходу: зокрема, у роботі Квона та ін. (2022) продемонстровано, що об’єднання сигнатурного та поведінкового методів перевершує за точністю чисто поведінкові моделі (на основі автоенкодера) і зменшує обчислювальні витрати на аналіз аномалій. Іншими словами, використання комбінованих алгоритмів виявлення підвищує загальну

результативність SOC, дозволяючи знаходити більше реальних атак при меншому рівні шуму.

Практична реалізація оптимальної стратегії виявлення у SOC включає декілька взаємодоповнюваних напрямів.

– **Правила кореляції та IoC.**

На рівні SIEM і мережевих сенсорів впроваджуються набори кореляційних правил, які реагують на відомі шаблони атак та індикатори компрометації. Наприклад, правила виявлення брутфорсу, сканування портів, відомих сигнатур експлойтів, а також зіставлення вхідних даних з базами скомпрометованих IP-адрес, хешів шкідливих файлів тощо. Такі правила постійно оновлюються на основі останніх повідомлень про вразливості та розвідданих про загрози. Для ефективності сигнатурного методу важливо налагодити оперативне надходження Threat Intelligence до SOC (через автоматичні фіди або API), щоби нові IoC потрапляли в систему одразу після їх появи в спільноті кібербезпеки.

– **Моделі поведінки та аномалій.**

Паралельно налаштовуються системи поведінкового аналізу – це може бути модуль UEBA в межах SIEM, окремі рішення для аналізу мережевих потоків (Network Traffic Analysis) з алгоритмами машинного навчання, або власноруч налаштовані скрипти аналізу логів. Вони формують профілі нормальної активності для користувачів та систем (baseline) і відстежують статистично значущі відхилення. При виявленні аномальної події (наприклад, нестандартне підвищення привілеїв процесу, нетипова послідовність команд) в SOC генерується оповіщення для детального розгляду. Важливим аспектом є тюнінг моделей – визначення порогів чутливості, часового вікна для аналізу, винятків для відомих легітимних аномалій – щоб мінімізувати false positive. Поведінкові методи часто використовують штучний інтелект: наприклад, нейромережі для класифікації трафіку, алгоритми кластеризації для виявлення аномальних груп подій тощо. Як зазначається у тенденціях, впровадження

AI/ML у SOC дозволяє знаходити складні патерни атак і скорочувати час реакції [41].

– **Threat hunting (проактивне «полювання» на загрози).**

Окрім автоматизованих методів, оптимальна стратегія включає ручний проактивний пошук прихованих загроз аналітиками SOC. Threat hunting передбачає висування гіпотез про можливі присутні в системі загрози і їх перевірку шляхом поглибленого аналізу даних (журнали, трафік, пам'ять) поза рамками рутинних оповіщень. Мисливці за загрозами можуть виявити атаки, що пройшли повз автоматичні фільтри, шляхом виявлення слабких сигналів або незвичних взаємозв'язків. Наприклад, аналіз ланцюжків подій за матрицею MITRE ATT&CK допомагає виявити певну техніку атакуючого навіть за відсутності прямої сигнатури. Хоча threat hunting виходить за межі суто «моніторингових» завдань, результати такого пошуку (виявлені нові IoC, патерни) потім включаються в базу знань SOC і впроваджуються у правила детектування надалі.

– **Оцінка ризиків та пріоритизація сповіщень.**

Зважаючи на великий обсяг оповіщень, що генеруються в SOC, критично важливим є механізм пріоритизації – визначення, на які тривоги реагувати насамперед. Оптимальний підхід до виявлення передбачає застосування ризик-орієнтованого аналізу: кожному інциденту або оповіщенню присвоюється оцінка критичності (бали ризику) залежно від впливу на бізнес, важливості задіяного активу, впевненості спрацьовування тощо [45]. Наприклад, спрацювання, що вказує на можливий витік даних з критичного серверу, отримає високий пріоритет, тоді як

одинична підозріла дія на звичайному ПК – нижчий. Для цього SOC може впроваджувати системи User and Entity Behavior Risk Scoring та аналогічні метрики. Пріоритизація дозволяє зосередити зусилля команди на найбільш небезпечних загрозах і зменшити навантаження від малозначущих подій.

На основі наведеного, оптимальний підхід до виявлення загроз у SOC – це багатошарова система, де сигнатурні методи швидко відпрацьовують відоме,

поведінкові – виловлюють нове, а люди-експерти доповнюють автоматизацію творчим аналізом складних загроз. Важливо, що всі ці рівні взаємопов’язані: результати розвідки та ручного пошуку інтегруються в автоматичні правила, а автоматичні оповіщення перевіряються і довіряються тільки після експертного підтвердження. Таким чином, SOC реалізує циклічний процес навчання і вдосконалення: кожен виявлений інцидент поповнює базу знань, що підвищує ефективність майбутнього виявлення загроз.

3.3 Розробка алгоритму моніторингу загроз у SOC

Для забезпечення систематичного моніторингу кіберзагроз у межах SOC розроблено алгоритм (послідовність дій), що охоплює повний цикл від збору даних до реагування. Алгоритм моніторингу загроз у SOC можна представити у вигляді таких етапів:

1) Збір та агрегування даних.

На першому кроці відбувається **моніторинг джерел даних** безпеки по всій інфраструктурі. Встановлені агенти та сенсори збирають журнали подій з серверів, мережевих пристроїв, систем безпеки (фаєрволів, IDS/IPS), кінцевих точок, хмарних сервісів тощо. Дані передаються в централізоване сховище (модуль збору логів) у структурованому вигляді [38]. При цьому здійснюється початкова обробка: фільтрація дубльованих або несуттєвих подій, приведення до єдиного формату, мітки часу та джерела. Метою цього етапу є забезпечити цілісність і повноту вхідних даних для подальшого аналізу.

2) Аналіз та кореляція подій.

Зібрані дані надходять до модуля аналізу (ядра SOC, зазвичай реалізованого засобами SIEM). **SIEM проводить кореляцію подій** між собою, застосовуючи правил набори і аналітичні модулі: співставляє події з різних систем за часовими та контекстними ознаками, виявляючи послідовності, що вказують на атаку. Також на цьому етапі функціонують **модулі виявлення**

аномалій: вони аналізують потік даних з використанням встановлених статистичних моделей і алгоритмів ML, відмічаючи відхилення від норми. Результатом аналізу є сформований набір безпекових подій (security events) – агрегованих записів, що потенційно мають відношення до безпеки (наприклад, «невдала авторизація admin 10 разів поспіль» або «виявлено malware-зразок на хості»). Ці події зберігаються у базі даних SIEM та постійно оновлюються в режимі реального часу [37, 38].

3) Збагачення та контекстуалізація даних.

Паралельно з аналізом, система **збагачує події контекстною інформацією**. Через інтеграцію з **платформою Threat Intelligence** кожна подія перевіряється на наявність відомих IoC: до неї додаються відомості, чи фігурують відповідні IP, домени, хеші в базах загроз [38]. Також підтягується інформація з довідників про активи (Asset Management): важливість сервера, геолокація IP, привілеї облікового запису користувача тощо. Метою є надати максимально повні дані для ухвалення рішення – аналітик або автоматизований модуль на виході отримує подію з усіма відповідними атрибутами (тегами загроз, оцінкою критичності). Наприклад, якщо SIEM зафіксував підозрілу команду на хості, система додасть, що цей хост – сервер баз даних високої важливості, команда відповідає відомій техніці ATT&CK, а файл, який запускався, відомий як шкідливий (згідно з TI). Це значно прискорює подальше розслідування.

4) Моніторинг та виявлення інцидентів.

На цьому етапі відбувається **безпосереднє спостереження за проаналізованими подіями** з метою **виявлення інцидентів**. Умовно кажучи, SIEM-консоль та інші інтерфейси виступають «панеллю моніторингу», де відображаються всі значущі події і тривоги. Аналітики рівня L1 безперервно відстежують цю панель, реагуючи на спрацьовування, що приходять з правил кореляції та аномалій. Важлива частина алгоритму – **тріаж оповіщень**: визначення, чи є тривога істинною (означає реальну атаку) чи хибною. На основі напрацьованих процедур аналітик перевіряє деталізацію події, за потреби робить

швидкий пошук додаткових логів (наприклад, по IP-адресі або імені файла в інших джерелах) і приймає рішення. Якщо тривога помилкова (false positive), вона закривається з відповідною відміткою. Якщо ж подія справді виглядає як інцидент безпеки, алгоритм переходить до наступного кроку.

5) Ескалація і розслідування інциденту.

Виявлений інцидент ескалується на вищий рівень опрацювання (L2/L3) або безпосередньо до команди реагування (CERT/CIRT). Цей етап включає **глибоке розслідування**: залучені спеціалісти аналізують всі аспекти інциденту, встановлюють першопричину, масштаб розповсюдження, вплив на системи. Може проводитися додаткова форензика (аналіз пам'яті, дампів дисків, мережевих сесій), якщо це передбачено сценарієм. Важливим завданням є також визначити ланцюжок атаки (kill chain) – які кроки виконав зловмисник від початкового проникнення до поточного стану. На основі розслідування підтверджується або спростовується факт інциденту. Якщо підтверджується, паралельно слід негайно активувати заходи реагування.

6) Реагування на інцидент.

Алгоритм моніторингу тісно інтегрований з алгоритмом реагування (див. підрозділ 3.4). На цьому кроці виконуються дії для стримування та ліквідації загрози. **Інцидентна команда** або автоматизовані скрипти здійснюють заходи: ізоляція уражених хостів від мережі, блокування облікових записів або трафіку, застосування патчів, видалення шкідливого ПЗ тощо. Метою є **локалізувати інцидент**, запобігти подальшому розвитку атаки та звести до мінімуму збитки. У межах алгоритму моніторингу передбачається, що для типових категорій інцидентів реалізовані **автоматизовані сценарії реагування** (SOAR playbooks) [38]. Наприклад, при виявленні шкідливого файлу на кінцевій станції система може автоматично запустити скрипт ізоляції цього хоста від мережі і сповіщення адміністратору. Автоматизація на цьому етапі суттєво скорочує MTTR (Mean Time to Respond) і не дає зловмиснику закріпитися чи поширитися глибше по мережі.

7) Відновлення та завершення інциденту.

Після нейтралізації загрози здійснюються роботи з **відновлення нормальної роботи систем**: перевстановлення скомпрометованих вузлів із чистих резервних копій, зміна скомпрометованих паролів, повторна перевірка цілісності даних. SOC моніторить інфраструктуру на предмет повторних проявів інциденту під час відновлення. Інцидент вважається закритим лише після повного відновлення працездатності та впевненості, що загрозу усунуто. Всі дії детально фіксуються в системі керування інцидентами (case management) зі зазначенням часу, відповідальних та результатів.

8) Післяінцидентний аналіз і вдосконалення.

Завершальний крок алгоритму – **ретроспективний аналіз** інциденту (post-incident review). Команда SOC проводить розбір: що було виявлено, які методи використовував противник, чи можна було запобігти або виявити раніше, наскільки ефективно спрацювали процедури реагування. Результати оформлюються у вигляді звіту з висновками та рекомендаціями [38]. Ці рекомендації можуть включати оновлення правил моніторингу (щоб у майбутньому швидше ловити такі атаки), додаткове навчання персоналу, покращення конфігурації систем безпеки, внесення змін до планів реагування. Таким чином, цикл моніторингу замикається: уроки, отримані з інциденту, **впроваджуються в систему моніторингу**, що підвищує її ефективність надалі [30]. SOC постійно самонавчається на основі власних кейсів, що є запорукою актуальності та живучості моделі моніторингу.

Варто зазначити, що описаний алгоритм є спрощеною узагальненою моделлю. У реальності окремі етапи можуть виконуватися ітеративно або паралельно. Наприклад, розслідування (крок 5) часто йде одночасно з реагуванням (крок 6), коли потрібно терміново ізолювати систему ще до завершення повного аналізу. Так само автоматичні скрипти можуть виконуватися на різних стадіях без залучення людини. Проте загальна структура залишається незмінною: **моніторинг – виявлення – підтвердження – реагування – покращення**. Дотримання цього алгоритму забезпечує

комплексний підхід до протидії загрозам та замикання циклу кібербезпеки в організації.

3.4 Опис моделі реагування на інциденти безпеки

Ефективне реагування на інциденти є невід'ємною складовою моделі SOC та тісно пов'язане з процесом моніторингу. **Модель реагування на інциденти** визначає етапи і заходи, яких слід вжити від моменту виявлення інциденту до повного відновлення роботи і впровадження покращень. У світовій практиці широко використовується «цикл реагування на інциденти» за рекомендаціями NIST, що складається **з чотирьох основних фаз** [47, 48] (іноді детальніше розбивається на 6 фаз). ці етапи згідно з класичною моделлю NIST SP 800-61 [38] наведено на рисунку 4.

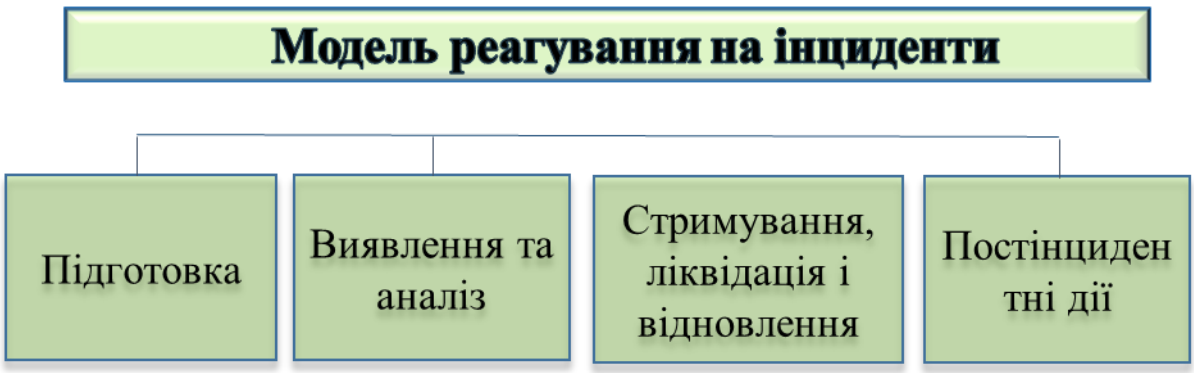

Рис.4. Модель реагування на інциденти згідно NIST

Підготовка (Preparation).

На цьому докризовому етапі організація готується до можливих інцидентів. Розроблено та впроваджено план реагування на інциденти (Incident Response Plan) – документ, що визначає політики, ролі і обов'язки, процедури дій у разі різних типів інцидентів. Створено команду реагування (CIRT/CERT), призначено відповідальних осіб. Проводяться регулярні навчання персоналу

(кібер-вчення, імітації інцидентів), щоб відпрацювати навички і виявити прогалини. Забезпечено необхідні інструменти: середовища для аналізу шкідливого ПЗ, засоби резервного копіювання, контакти зовнішніх експертів (наприклад, правоохоронних органів, якщо планується їх залучення). Фаза підготовки також включає заходи захисту, що зменшують імовірність інцидентів: підтримка актуальності патчів, резервування даних, налаштування журналювання тощо [36]. Якісна підготовка визначає здатність організації швидко й ефективно реагувати, коли інцидент станеться.

Виявлення та аналіз (Detection & Analysis).

Ця фаза розпочинається безпосередньо з моменту, коли моніторингові засоби SOC зафіксували підозрілу подію і кваліфікували її як інцидент (відповідно до алгоритму 3.3). Ключове завдання – **ідентифікувати інцидент, оцінити його природу і масштаб**. Аналітики збирають всю доступну інформацію: журнали, артефакти, дані системного моніторингу, і намагаються встановити відповіді на питання: що сталося, на яких системах, коли почалося, як було виявлено, хто або що є джерелом атаки. Проводиться первинна пріоритизація – визначається критичність інциденту (наприклад, компрометація критичного сервера – високий пріоритет). Якщо інцидент підтверджено, відповідальна команда офіційно реєструє його (заведення кейсу) та переходить до активних дій. На етапі аналізу можуть залучатися сторонні ознаки: індикатори з Threat Intelligence, результати пошуку схожих випадків у базі минулих інцидентів. Важливо також подбати про **сповіщення керівництва та зацікавлених осіб** (в рамках політики повідомлень) – на цьому етапі приймається рішення, кого потрібно інформувати негайно (наприклад, СТО, відділ захисту даних, партнери, якщо інцидент їх стосується, тощо).

Стримування, ліквідація і відновлення (Containment, Eradication & Recovery).

Це ядро процесу реагування, коли вживаються практичні заходи для нейтралізації загрози. Спершу виконується стримування: дії, що зупиняють розповсюдження атаки та мінімізують шкоду. Залежно від ситуації, це може бути

відключення заражених систем від мережі, блокування скомпрометованих акаунтів, встановлення тимчасових правил фаєрвола, що відтинають трафік з IP атакуючого, тощо. Стримування є критичним кроком, оскільки дає виграш у часі на подальші кроки та не дозволяє інциденту ескалувати. Далі команда переходить до ліквідації (ерикації) – видалення самого джерела загрози. Це може включати: очищення шкідливого коду, видалення або ізоляцію уражених файлів, закриття уразливостей (встановлення патчів), припинення шкідливих процесів. Паралельно слід знайти root cause – первинну причину проникнення – і усунути її (наприклад, відключити викрадені облікові дані, через які зловмисник отримав доступ). Відновлення передбачає повернення систем до штатного режиму роботи. Якщо машини було вимкнено чи перевстановлено – їх слід підключити назад, перевіривши, що повторної компрометації не сталося. Можливо, доведеться відновити дані з резервних копій (у разі їх пошкодження або шифрування). Перед поверненням у експлуатацію кожен компонент тестується на відсутність слідів присутності зловмисника. Ця фаза може тривати від кількох годин до днів і тижнів – залежно від складності інциденту. Важливо мати документовані процедури на кожен тип інциденту, щоб дії були швидкими і вивіреними. Добре побудована модель реагування включає заздалегідь розроблені playbooks (сценарії) для типових ситуацій, що значно пришвидшує роботи. За потреби, на етапі ліквідації/відновлення залучаються зовнішні спеціалісти – наприклад, якщо інцидент дуже серйозний (attack APT- англ. Advanced persistant threat) або потрібна експертиза правоохоронців.

Постінцидентні дії (Post-Incident Activity).

Після завершення робіт з ліквідації загрози проводиться підсумковий етап – аналіз і уроки інциденту. Команда реагування спільно з командою моніторингу збираються для розбору: що спрацювало добре, де були проблеми, як покращити процеси надалі. Готується формальний звіт про інцидент, який містить хронологію подій, вжиті заходи, оцінку збитків, витрачені ресурси, а також рекомендації щодо запобігання аналогічним інцидентам у майбутньому [38]. Наприклад, може бути вирішено посилити моніторинг певного сегмента мережі,

оновити правила кореляції, провести додаткове навчання персоналу або змінити політики безпеки. Дуже важливо впровадити результати цього аналізу на практиці – модель реагування передбачає зворотній зв’язок до фази Preparation, таким чином утворюється циклічний процес покращення. Крім того, на постінцидентному етапі можливі юридичні кроки: повідомлення регуляторів (якщо того вимагає закон при витоку даних), взаємодія з правоохоронними органами, судові позови проти зловмисників (якщо їх ідентифіковано) тощо. Ці аспекти також повинні бути враховані моделлю (наприклад, чи готова організація надати цифрові докази в прийнятному вигляді).

Описана модель реагування є узагальненою і може коригуватися залежно від специфіки організації та типів інцидентів. Проте дотримання цієї структури (підготовка – виявлення – стримування – відновлення – аналіз) дозволяє побудувати чіткий процес, який охоплює всі необхідні кроки. В академічній літературі і стандартах наголошується, що реагування на інциденти повинно бути тісно інтегроване з загальною системою управління кіберризиками організації [48]. Це означає, що навіть на етапах **ідентифікації та захисту** (які передують інциденту) вже враховується майбутнє реагування – наприклад, впроваджуються засоби журналювання, що забезпечать потрібні докази. Навпаки, уроки, винесені з інцидентів, впливають на стратегію захисту і моніторингу в подальшому. Таким чином, модель реагування не існує ізольовано, а є частиною єдиного циклу безперервного вдосконалення кібербезпеки.

Правильна організація процесу реагування дає відчутні результати. За даними NIST, впровадження рекомендацій з incident response дозволяє **зменшити кількість та вплив інцидентів**, а також підвищити ефективність виявлення та відновлення [49]. Іншими словами, чим більш зрілою є функція реагування, тим менше шкоди приноситимуть атаки, оскільки вони швидше локалізуються і усуваються. Для SOC це означає менші простої сервісів, захист репутації компанії та економію коштів на ліквідацію наслідків. Саме тому

побудова зрілої моделі реагування – один із головних пріоритетів при розробці комплексної моделі моніторингу безпеки.

3.5 Модель моніторингу загроз у SOC

Згідно вищенаведеної інформації було побудовано наступну модель моніторингу загроз у SOC:

Рис.5. Модель моніторингу загроз у SOC

Висновки до розділу 3

У третьому розділі курсової роботи розроблено модель організації моніторингу кібербезпеки в рамках SOC, що включає архітектуру системи, підходи до виявлення загроз, алгоритм моніторингу та модель реагування на інциденти. На основі аналізу сучасних практик встановлено, що ефективний SOC має багаторівневу архітектуру, яка поєднує інструменти збору й аналізу даних (SIEM, IDS/IPS, EDR), платформи розвідки загроз, засоби автоматизації та команду фахівців, які діють за чітко регламентованими процесами. Оптимальний підхід до виявлення загроз грунтується на комбінації сигнатурних і поведінкових методів, підтримується інтеграцією актуальної розвідки загроз і проактивним пошуком аномалій. Розроблений алгоритм моніторингу забезпечує безперервний цикл від збору подій до реагування та навчання на інцидентах, що дозволяє системі самовдосконалюватись. Запропонована модель реагування на інциденти охоплює всі фази – від підготовки до післяінцидентного аналізу – і тісно інтегрована з процесом моніторингу. Застосування описаної моделі в організації підвищить її кіберстійкість, забезпечить своєчасне виявлення атак і мінімізує збитки від інцидентів за рахунок швидкого та скоординованого реагування.

Загальні висновки

У результаті проведеного комплексного дослідження було здійснено глибокий аналіз теоретичних та практичних аспектів побудови системи моніторингу загроз у рамках функціонування Центру оперативного управління безпекою (SOC). У роботі розкрито значення SOC як центрального елементу сучасної кіберзахисної інфраструктури, що забезпечує безперервний моніторинг, аналіз та реагування на кіберзагрози. Особливу увагу було приділено визначенню ролі SOC у протидії актуальним загрозам, таким як фішинг, атаки нульового дня, DDoS, зловмисне ПЗ, а також інцидентам, пов’язаним із людським фактором або помилками конфігурації.

Проаналізовано функціонал та можливості найпоширеніших SIEM-систем – зокрема IBM QRadar, Splunk Enterprise Security та Elasticsearch. Встановлено, що саме ці платформи дозволяють автоматизовано збирати, корелювати та аналізувати великі обсяги подій з різноманітних джерел. У поєднанні з системами виявлення та запобігання вторгненням (Snort, Suricata, Zeek) SIEM-системи значно підвищують точність виявлення інцидентів і допомагають формувати повну картину атак у реальному часі. Кожна з IDS/IPS систем має свої сильні сторони: Snort вирізняється стабільністю та поширеністю, Suricata – високою продуктивністю, а Zeek – глибоким контекстним аналізом мережевої поведінки.

Додаткову цінність для SOC створюють платформи Threat Intelligence, що забезпечують централізований обмін даними про загрози з перевірених джерел. Вони допомагають покращити якість реагування на новітні атаки, знижуючи ймовірність пропуску критичних загроз. Інтеграція Threat Intelligence у SIEM та SOAR-рішення дозволяє автоматично перевіряти IOC (Indicators of Compromise), виявляти повторювані шаблони атак, а також посилювати можливості аналізу в контексті глобальних загроз.

Окремий фокус було спрямовано на аналіз SOAR-рішень (IBM Resilient, Splunk SOAR, TheHive, Shuffle), які виступають фундаментом для автоматизації

процесів реагування. SOAR значно зменшує час, необхідний для обробки інцидентів, автоматизує стандартні процедури, дозволяє будувати робочі процеси (playbooks) і зменшує навантаження на аналітиків, одночасно підвищуючи ефективність їхньої роботи

На основі проведеного аналізу було розроблено модель організації моніторингу в SOC, яка включає архітектуру компонентів, алгоритм виявлення загроз, послідовність дій у разі виявлення інциденту безпеки та механізми реагування. Запропонований підхід орієнтований на гнучкість, масштабованість та інтегрованість, що дозволяє ефективно реагувати на широкий спектр загроз у мінливому кіберпросторі

Усі поставлені завдання дослідження були виконані в повному обсязі. Визначено сучасні підходи до організації моніторингу, обґрунтовано вибір інструментів, досліджено можливості інтеграції рішень, а також представлено практичну модель побудови SOC. На основі виконаного аналізу зроблено висновок, що ефективний SOC – це результат синергії технологій, процесів і кваліфікованих спеціалістів.

Перспективи подальшого розвитку у цій сфері пов’язані з активним впровадженням елементів штучного інтелекту та машинного навчання для поведінкового аналізу користувачів і аномалій у мережевому трафіку. Також важливими напрямками є уніфікація стандартів обміну інформацією про загрози (наприклад, STIX/TAXII), розвиток Zero Trust архітектури та забезпечення адаптивної безпеки в умовах гібридного IT-середовища (локальні ресурси + хмара). У цілому, майбутнє систем моніторингу кіберзагроз полягає в побудові самонавчальних SOC-платформ, здатних проактивно і ефективно протидіяти загрозам нового покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Micrososft Corp. Що таке операційний центр безпеки (SOC)?. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-security-operations-center-soc.

2. Check Point. What is a Security Operations Center (SOC)?. URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/.

3. Durán A. Основні вектори атак, які використовують кіберзлочинці: Вразливості та поради щодо запобігання. URL: https://masterbase.com/uk/основні-вектори-атак-які-використову/майстер-база/.

4. A Comprehensive Guide to Threat Detection | AppOmni. AppOmni. URL: https://appomni.com/what-is-threat-detection/.

5. IBM. What is SIEM? | IBM. IBM - United States. URL: https://www.ibm.com/think/topics/siem.

6. Аналітик безпеки і SOC (Центр інформаційної безпеки) » CyberSecureFox. CyberSecureFox. URL: https://cybersecurefox.com/ru/analitik-bezopasnosti-i-soc-vashi-strazhi-v-mire-kiberbezopasnosti/.

7. IBM QRadar SIEM. IBM - United States. URL: https://www.ibm.com/products/qradar-siem.

8. IBM QRadar Security Intelligence Platform. IBM - United States. URL: https://www.ibm.com/docs/en/qsip/7.5?topic=started-qradar-overview.

9. IBM QRadar: Key Modules, Features, Architecture, and Limitations. All-in-One Cybersecurity Platform - Cynet. URL: https://www.cynet.com/siem/ibm-qradar-key-modules-features-architecture-and-limitations/.

10. IBM QRadar on Cloud. IBM - United States. URL: https://www.ibm.com/docs/en/qradar-on-cloud?topic=rules-creating-custom-rule.

11. Splunk Enterprise Security | Splunk. Splunk. URL: https://www.splunk.com/en_us/products/enterprise-security.html.

12. Splunk Enterprise Security Features | Splunk. Splunk. URL: https://www.splunk.com/en_us/products/splunk-enterprise-security-features.html.

13. Configure correlation searches - Splunk Documentation. Documentation - Splunk Documentation. URL: https://docs.splunk.com/Documentation/PCI/5.3.3/Install/Correlationsearches.

14. The CIS Top 20 Controls Explained. CyberSaint | Cyber Risk Management Software & Platform. URL: https://www.cybersaint.io/blog/the-cis-top-20-controls.

15. Cyber Kill Chain®. Lockheed Martin. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

16. MITRE ATT&CK®. URL: https://attack.mitre.org/.

17. IBM Security QRadar SIEM vs Splunk Enterprise 2025 | Gartner Peer Insights. URL: https://www.gartner.com/reviews/market/security-information-event-management/compare/product/ibm-security-qradar-siem-vs-splunk-enterprise.

18. Splunk Enterprise Security vs IBM Security QRadar | SoftwareReviews | Security Information and Event Management. SoftwareReviews. URL: https://www.infotech.com/software-reviews/categories/security-information-and-event-management/compare/splunk-enterprise-security-vs-ibm-security-qradar-siem.

19. Splunk vs QRadar: A SIEM Solution Comparison. Kinney Group. URL: https://kinneygroup.com/blog/splunk-vs-qradar/.

20. Okeke F. QRadar vs Splunk (2024): SIEM Tool Comparison. URL: https://www.techrepublic.com/article/qradar-vs-splunk/.

21. Splunk vs IBM QRadar: Security Information And Event Management (SIEM) Comparison. 6sense. URL: https://6sense.com/tech/security-information-and-event-management-siem/splunk-vs-ibmqradar.

22. Hannachi H. Elastic–Elastic SIEM Fundamentals. Medium. URL: https://hassen-hannachi.medium.com/elastic-elastic-siem-fundamentals-3337d580fafe.

23. Explore and analyze | Elastic Docs. Elastic – The Search AI Company | Elastic. URL: https://www.elastic.co/docs/explore-analyze.

24. Snort - Network Intrusion Detection & Prevention System. Snort. URL: https://www.snort.org/.

25. SNORT–Network Intrusion Detection and Prevention System | Fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/snort.

26. Home – Suricata. Suricata. URL: https://suricata.io/.

27. The Zeek Network Security Monitor. Zeek. URL: https://zeek.org/.

28. What Is A Threat Intelligence Platform? Capabilities, Benefits & More | Analyst1. Analyst1. URL: https://analyst1.com/threat-intelligence-platform/.

29. Building a Threat Intelligence-Driven SOC: Frameworks, Tools, and Best Practices | by Scott Bolen | RONIN OWL CTI | Medium. Scott Bolen. URL: https://medium.com/@scottbolen/building-a-threat-intelligence-driven-soc-frameworks-tools-and-best-practices-0143fd2ac9b7.

30. Top 7 Threat Intelligence Platforms & Software in 2025. eSecurity Planet. URL: https://www.esecurityplanet.com/products/threat-intelligence-platforms/.

31. MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. URL: https://www.misp-project.org/.

32. Cisco Talos Intelligence Group - Comprehensive Threat Intelligence. Cisco Talos Intelligence Group - Comprehensive Threat Intelligence. URL: https://talosintelligence.com/categories.

33. Threat Intelligence Lookup, a searchable database of IOCs and events for threat hunting. ANY.RUN - Interactive Online Malware Sandbox. URL: https://any.run/threat-intelligence-lookup.

34. Benefits and Challenges of SOAR Platforms. SEI Blog. URL: https://insights.sei.cmu.edu/blog/benefits-and-challenges-of-soar-platforms/.

35. 2021 Volume 2 Benefits of Using a SOAR Solution. ISACA. URL: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/benefits-of-using-a-soar-solution.

36. IBM Resilient: Pros and Cons 2025. Buying Intelligence and Reviews for Enterprise Technology. URL: https://www.peerspot.com/products/ibm-resilient-pros-and-cons.

37. IBM Knowledge Center. What is a Security Operations Center (SOC)? – IBM, 15 March 2024. – URL: https://www.ibm.com/think/topics/security-operations-center.

38. (PDF) Building a Scalable Security Operations Center: A Focus on Open-Source Tools https://www.researchgate.net/publication/381613928_Building_a_Scalable_Security_Operations_Center_A_Focus_on_OpenSource_Tools.

39. Bassey C., Chinda E.T., Idowu S. Building a Scalable Security Operations Center: A Focus on OpenSource Tools. Journal of Engineering Research and Reports. с. 196–209. DOI: 10.9734/jerr/2024/v26i71203.

40. Best practices for setting up a security operations centre (SOC) - ITSAP.00.500 - Canadian Centre for Cyber Security https://www.cyber.gc.ca/en/guidance/best-practices-setting-security-operations-centre-soc-itsap00500.

41. CHAPTER-11: SOC Reference Architecture https://www.linkedin.com/pulse/chapter-11-soc-reference-architecture-shahab-al-yamin-chawdhury-ctunc.

42. SOC Architecture: Designing an Efficient Security Operations Center https://www.cadosecurity.com/wiki/soc-architecture-designing-an-efficient-security-operations-center.

43. Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-socsurvey-39060.pdf.

44. Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods https://www.mdpi.com/2079-9292/11/6/867.

45. Kwon H.-Y., Kim T., Lee M.-K. Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods. Electronics. DOI: 10.3390/electronics11060867.

46. Guidepoint security. SOC: The Next Generation. URL: https://www.guidepointsecurity.com/wp-content/uploads/2021/07/Next-Gen-SOC_WP.pdf

47. NIST Incident Response: 4-Step Life Cycle, Templates and Tips https://www.cynet.com/incident-response/nist-incident-response/.

48. Incident Response Lifecycle: Stages and Best Practices | Atlassian https://www.atlassian.com/incident-management/incident-response/lifecycle.

49. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

50. SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile | CSRC https://csrc.nist.gov/pubs/sp/800/61/r3/final.