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: “ТЕХНОЛОГІЇ ТА ПРОДУКТИ В АРХІТЕКТУРІ SOC ОРГАНІЗАЦІЇ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

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

_____ Максим ОРЛЕНКО

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
Максим ОРЛЕНКО

Керівник:
д.е.н., професор Світлана ЛЕГОМІНОВА

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освітимагістр
Спеціальність125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____” _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Орленку Максиму Євгеновичу

Тема кваліфікаційної роботи: “Технології та продукти в архітектурі SOC організації”

керівник кваліфікаційної роботи Світлана ЛЕГОМІНОВА *доктор економічних наук, професор*

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “30” жовтня 2025 р. № 467.

1. Строк подання кваліфікаційної роботи“25” грудня 2025 р.
2. Вихідні дані до кваліфікаційної роботи:.
3. Перелік питань, які потрібно розробити:
   1. Вивчити теоретичні засади побудови SOC, включаючи нормативно-правові та методологічні підходи.
   2. Проаналізувати технології, компоненти та продукти, які використовуються в архітектурі SOC, з урахуванням їх функцій та взаємодії.
   3. Сформулювати практичні рекомендації щодо подальшого розвитку SOC та оптимізації його роботи.
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання “02” жовтня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Вивчити теоретичні засади побудови SOC, включаючи нормативно-правові та методологічні підходи.	27.10.2025	
4.	Проаналізувати технології, компоненти та продукти, які використовуються в архітектурі SOC, з урахуванням їх функцій та взаємодії.	10.11.2025	
5.	Сформулювати практичні рекомендації щодо подальшого розвитку SOC та оптимізації його роботи.	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Максим ОРЛЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(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 магістра

Направляється здобувач Орленко М.Є. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програмиУправління інформаційною та кібернетичною безпекою
(назва)
на тему: "Технології та продукти в архітектурі SOC організації"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **ОРЛЕНКО Максим** у кваліфікаційній роботі проаналізував теоретичні аспекти та підходи до побудови SOC організації, проаналізував різні архітектури та продукти що використовуються в SOC . **ОРЛЕНКО Максим** показав високу теоретичну і практичну підготовку, володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення проблеми дослідження. Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **ОРЛЕНКО Максим** на оцінку "добре" та присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи_____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Орленко М.Є. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Орленка Максима Євгеновича
на тему "Технології та продукти в архітектурі SOC організації"

Актуальність Різноманітні засоби впливу зараз активно застосовуються у кіберпросторі з метою дестабілізації конкурентів чи привласнення коштів компаній шляхом вимагання. Тому важливим завданням сучасного підприємства є його захист від різноманітних кібератак, запобігання і протидія загрозам, що виникають внаслідок використання компаніями технологій для побудови власних мереж. З огляду на зазначене дослідження проблеми дослідження технологій та продуктів в SOC організації є актуальним науковим завданням.

Позитивні сторони

1. У роботі досліджено технології та продукти в архітектурі SOC типової середньої комерційної організації. Розглянуто різні архітектури SOC та їх рівні, технологічні компоненти, методи аналітики й автоматизації та як вони застосовуються на практиці, представлено концептуальну модель побудови центру обробки даних.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді таблиць та рисунків. Автор опрацював джерельну базу близько 20 публікацій, книжок та електронних джерел, в основному англомовних.
3. За результатами дослідження запропоновано рекомендації щодо побудови SOC середньої комерційної організації з використанням конкретних технологій та продуктів з обґрунтуванням запропонованих варіантів.

Недоліки

1. Доцільно було б приділити більше уваги розгляду якоїсь конкретної організації для більш наглядного прикладу, а також зазначенню найкращих світових практик для вирішення поставлених задач.

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

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Орленко Максим Євгенович заслуговує присвоєння кваліфікації "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Рецензент: завідувач кафедри
Систем та технологій кібербезпеки,

д.т.н, професор _____ *підпис* Галина ГАИДУР

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 86 стор., 5 рис., 4 табл., 21 джерел.

Метою роботи полягає у розробці науково-обґрунтованої та практично орієнтованої моделі архітектури SOC для комерційної організації середнього масштабу в Україні.

Об'єктом дослідження – система кіберзахисту комерційної організації (середнього масштабу) в Україні з акцентом на центр операцій безпеки.

Предмет дослідження – технології та продукти в архітектурі SOC типової середньої комерційної організації.

Методи дослідження. Для вирішення завдань та процесів побудови центрів операційної безпекиSOC використовується аналіз наукових джерел і нормативної документації, порівняльний аналіз технологій та продуктів, системний аналіз архітектури SOC, функціонально структурне моделювання, методи сценарного аналізу, експертних оцінок, узагальнення і синтезу та проектно-аналітичний метод.

Короткий зміст роботи. Як результат у роботі проведено аналіз основних теоретичних засад побудови SOC, розглянуто основні технологічні архітектури та продукти що використовуються для побудови центрів операційної безпеки, зокрема розглянуто ролі персоналу для забезпечення належної роботи SOC організації, побудовано концептуальну модель архітектури центру операційної безпеки для організації середнього масштабу.

Галузь застосування. Розроблені підходи можуть бути використані при побудові систем операційної безпеки SOC, плануванні та реалізації системи управління інформаційною безпекою підприємства у контексті протидії кіберзагрозам.

КЛЮЧОВІ СЛОВА : ЦЕНТР ОПЕРАЦІЙНОЇ БЕЗПЕКИ, АРХІТЕКТУРА SOC, ТЕХНОЛОГІЧНІ КОМПОНЕТИ SOC, SIEM, КІБЕРЗАХИСТ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 86 pages, 5 figures, 4 tables, 21 sources.

The purpose of the work is to develop a scientifically sound and practically oriented SOC architecture model for a medium-sized commercial organization in Ukraine.

Object of research is the cyber security system of a commercial organization (medium-sized) in Ukraine with a focus on the security operations center.

Subjec*t ***of research is technologies and products in the SOC architecture of a typical medium-sized commercial organization.

Research methods. To solve the tasks and processes of building SOCs, we used analysis of scientific sources and regulatory documentation, comparative analysis of technologies and products, systematic analysis of SOC architecture, functional structural modeling, scenario analysis methods, expert assessments, generalization and synthesis, and the design and analytical method.

Brief content of research. . As a result, the work analyzes the basic theoretical principles of SOC construction, considers the main technological architectures and products used to build operational security centers, in particular, considers the role of personnel in ensuring the proper operation of the organization's SOC, and constructs a conceptual model of the architecture of an operational security center for a medium-sized organization.

Field of research. The developed approaches can be used in building SOC operational security systems, planning and implementing an enterprise information security management system in the context of countering cyber threats.

KEYWORDS: OPERATIONAL SECURITY CENTER, SOC ARCHITECTURE, SOC TECHNOLOGICAL COMPONENTS, SIEM, CYBER SECURITY.

ЗМІСТ

ВСТУП

Сьогодні більшість комерційних підприємств стикаються з постійно зростаючими ризиками кібербезпеки: кількість і складність кібератак продовжує збільшуватися, а методи атак стають більш цілеспрямованими, багаторівневими і технічно витонченими. Це безпосередньо впливає на безперебійність бізнес-процесів, надійність операційних моделей, репутацію та фінансову стабільність компаній. Оскільки бізнес все більше залежить від цифрових послуг та критичних IT-інфраструктур, кіберризики перетворюються з просто технічного питання на стратегічну, управлінську та економічну проблему.

У цьому контексті Центри операцій безпеки безпеки (англ. Security Operations Centers, SOC) стають основним елементом сучасної системи кіберзахисту. National Institute of Standards and Technology (NIST) окреслює SOC як "основну точку для операцій безпеки і захисту мережі компанії", підкреслюючи його роль як організаційного та технологічного центру, який відповідає за спостереження, аналіз, координацію та реагування на загрози. SOC надає постійний моніторинг, виявлення аномалій, зіставлення подій, формування інцидентів і оперативне реагування протягом 24/7, забезпечуючи замкнений цикл контролю ризиків.

Основною причиною підвищення ролі SOC є зміна в ландшафті загроз, включаючи активність APT-груп, поширення складних фішингових кампаній, експлуатацію вразливостей нульового дня і використання автономних зловмисних програм, які можуть адаптуватися до контрзаходів. Крім того, зростає кількість атак, що спрямовані на хмарні середовища, промислові системи (ICS/SCADA), технології віддаленої роботи та мобільні платформи.

Український бізнес функціонує в унікальних умовах, де технічні, економічні та безпекові ризики ускладнюються геополітичними обставинами, активністю державних і псевдодержавних кіберугрупувань, а також гібридними операціями проти критичних та комерційних секторах. В таких умовах

впровадження SOC стає не лише технологічною необхідністю, але й стратегічним інструментом для забезпечення організаційної резильєнтності – здатності підприємства підтримувати свою операційну діяльність, оперативно відновлюватися після інцидентів і мінімізувати негативний вплив атак на бізнес-безперервність.

SOC дозволяє компаніям не лише реагувати на загрози, але й формувати проактивну модель безпеки: прогнозувати ризики, виявляти поведінкові аномалії, своєчасно локалізувати інциденти, забезпечувати аудит, дотримання стандартів і розвивати культуру безпеки. Отже, створення SOC є критично важливим кроком в напрямку підвищення цифрової стійкості та конкурентоспроможності організації в умовах зростаючої складності кіберпростору.

Мета роботи полягає у розробці науково-обґрунтованої та практично орієнтованої моделі архітектури SOC для комерційної організації середнього масштабу в Україні, що включає технологічні рішення, продукти, організаційно-процесну модель і рекомендації для впровадження.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Провести аналіз теоретичних засад побудови SOC, включаючи нормативно-правові та методологічні підходи.
2. Проаналізувати технології, компоненти та продукти, які використовуються в архітектурі SOC, з урахуванням їх функцій та взаємодії.
3. Розробити організаційно-операційну модель SOC: ролі, процеси, метрики, політики.
4. Сконструювати концепцію впровадження SOC у типовій українській комерційній організації середнього масштабу, з вибором технологій, архітектури, етапів реалізації.
5. Сформулювати практичні рекомендації щодо подальшого розвитку SOC та оптимізації його роботи.

Об’єкт дослідження – система кіберзахисту комерційної організації (середнього масштабу) в Україні з акцентом на центр операцій безпеки.

Предмет дослідження – Технології та продукти в архітектурі SOC типовій середній комерційній організації.

У роботі використані такі методи: аналіз науково-технічної літератури і нормативної бази; системний аналіз архітектурних моделей SOC; порівняльний аналіз технологічних продуктів; моделювання архітектури SOC для комерційної організації; формування рекомендацій на основі отриманих результатів.

Наукова новизна одержаних результатів полягає в інтеграції організаційно-процесного, технологічного та продуктивного підходів до архітектури SOC, а також у розробці концептуальної моделі SOC, адаптованої до українських комерційних реалій середнього масштабу.

Практичне значення одержаних результатів – Результати роботи можуть бути використані IT-підрозділами та службами безпеки комерційних організацій середнього масштабу для планування, проектування та впровадження SOC. Крім того, рекомендації можуть бути корисними консалтинговим компаніям, що надають послуги в сфері кібербезпеки, а також викладачам профільних дисциплін.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ПОБУДОВИ SOC

1.1. Концепція Центру операцій безпеки (SOC)

1.1.1. Поняття SOC та його роль у сучасній системі кіберзахисту

Центр операцій безпеки (SOC) є ключовим елементом системи захисту інформації в будь-якій сучасній організації, оскільки він забезпечує постійний моніторинг, аналіз, реагування та попередження інцидентів безпеки. Основна мета його функціонування полягає у зменшенні ризиків компрометації інформаційних ресурсів, запобіганні неавторизованому доступу та забезпеченні цілісності, доступності й конфіденційності даних.

SOC інтегрує людські ресурси, технологічні рішення та процеси (PPT або PPTGC – Люди, Процеси, Технології, Управління та Відповідність) у єдину структуру, що дозволяє не лише реагувати на інциденти, а й передбачати та запобігати атакам. У час, коли загрози постійно змінюються, а кібератаки стають дедалі складнішими, SOC виступає в ролі нервової системи кібербезпеки, забезпечуючи незмінну обізнаність щодо стану IT-інфраструктури й оперативне реагування на будь-які аномалії.

Ключові ролі SOC у системі кіберзахисту:

1. Центральний елемент захисту – SOC не лише реагує на інциденти, але й координує всі процеси безпеки, зливаючи різноманітні технології (SIEM, IDS/IPS, EDR, UEBA, Threat Intelligence, SOAR тощо) в єдину систему моніторингу та реагування.
2. Імунна система організації – SOC здійснює постійний моніторинг систем, встановлюючи аномальну активність, що може вказувати на спробу атаки. Це формує проактивну стратегію – організація не чекає на раптовий напад, а передбачає його.
3. Координаційний та аналітичний центр – SOC виконує ролі головного органу безпеки, де аналітики, автоматизовані алгоритми та машинне навчання

співпрацюють для виявлення зв’язків між подіями, кореляції даних і формування глибокого розуміння загроз.

4. Механізм запобігання атакам. Швидке реагування SOC зменшує наслідки атак – від скорочення часу на виявлення (Mean Time to Detect, MTTD) до зменшення часу на реагування (Mean Time to Respond, MTTR). Це безпосередньо впливає на фінансові та репутаційні втрати[1].

1.1.2. Мета та завдання SOC

Основна мета SOC полягає в забезпеченні стабільної кіберстійкості організації, що означає здатність ефективно протистояти кібератакам, швидко відновлюватися після інцидентів і підтримувати безперервність бізнес-процесів.

Основною метою функціонування Центру операційної безпеки є забезпечення безперервного, централізованого і контрольованого процесу захисту інформаційних ресурсів організації. SOC є важливим компонентом системи управління інформаційною безпекою, що забезпечує своєчасне виявлення, аналіз та реагування на кіберінциденти, зважаючи на критичність активів для бізнесу. Робота SOC спрямована на зменшення наслідків кіберзагроз, зниження ймовірності витоку даних, порушення цілісності інформаційних систем, а також зникнення доступності сервісів.

SOC надає захист як для локальної, так і для хмарної інфраструктури, включаючи користувацькі комп'ютери, сервери, мережеві елементи, системи аутентифікації, корпоративну електронну пошту та бізнес-програми. Його діяльність націлена на зменшення фінансових, операційних і репутаційних ризиків, а також на підтримку безперервності бізнес-процесів.

До основних завдань SOC входять:

- Моніторинг та виявлення загроз інформаційної безпеки: постійний збір, обробка та аналіз подій безпеки з усіх джерел у мережі. На основі

отриманих даних SOC здійснює виявлення аномалій, підозрілої поведінки користувачів та ознак реалізації кіберзагроз.

- Реагування на інциденти: своєчасний аналіз і класифікація інцидентів з визначенням їх рівня критичності та можливого впливу на діяльність організації з подальшим усуненням або ізоляцією загроз для зменшення наслідків.
- Формування ситуаційної обізнаності: створення єдиного уявлення про стан кібербезпеки організації, яке дозволяє приймати обґрунтовані управлінські рішення.
- Забезпечення відповідності вимогам: дотримання нормативних документів, стандартів безпеки (ISO/IEC 27001, NIST, GDPR тощо) та внутрішніх політик контролю.
- Аналіз тенденцій та розвиток процесів: на базі звітності та зворотного зв’язку SOC оптимізує власні процедури, запроваджуючи нові методи виявлення та автоматизації[10].

Важливим моментом є те, що SOC виконує роль засобу (тобто механізму для досягнення безпеки), а не виступає самоціллю. Його результативність визначається його можливістю забезпечувати кіберстійкість – здатність організації прогнозувати, реагувати, відновлюватися та адаптуватися до кіберзагроз[17].

1.1.3. Основні функції SOC: моніторинг, аналіз, реагування, звітність

SOC здійснює свої функції в безперервному циклі управління інцидентами, що включає чотири основні етапи:

1. Моніторинг та виявлення (Monitoring and Detection) – SOC постійно здійснює моніторинг подій в інформаційних системах, збираючи дані з різних джерел, таких як мережеві сенсори, системи ведення журналів, антивірусні програми, файрволи, EDR/IDS/IPS та інші.

Основні аспекти:

- Моніторинг у реальному часі: використання SIEM-систем для централізованого збору журналів і виявлення індикаторів компрометації (IoC).
- Виявлення аномалій: застосування поведінкового аналізу (UEBA) для розпізнавання нетипових дій користувачів або систем.
- Зменшення шуму: оптимізація налаштувань для зменшення кількості хибних спрацьовувань (FP) і хибних негативів (FN), що покращує ефективність аналітиків[2].

2. Аналіз (Analysis) – ця функція встановлює, чи є конкретна подія реальною загрозою, шляхом детального дослідження отриманих даних та виконує наступні завдання:

- Кореляція подій: зіставлення різноманітних журналів для виявлення складних атак або ланцюгів компрометації (Kill Chain, Mitre ATT&CK).
- Аналіз першопричин: виявлення джерела атаки, способів вторгнення та методів їх усунення.
- Залучення контексту: аналітик здійснює оцінку даних не тільки з технічної точки зору, але й в контексті бізнес-процесів організації, аби зрозуміти реальний вплив загрози.
- Інтеграція з Threat Intelligence: застосування як зовнішніх, так і внутрішніх джерел інформації для оперативного виявлення відомих шкідливих індикаторів[1,2].

3. Реагування (Response) – після виявлення інциденту SOC реалізує дії для його ліквідації або ізоляції, проходячи наступні етапи:

- Ізоляція заражених елементів: швидке відключення від мережі задля запобігання подальшому розповсюдженню атаки.
- Автоматизація реакції: використання систем SOAR для ефективного виконання стандартних сценаріїв реагування (наприклад, блокування IP-адреси, видалення шкідливих компонентів).

- Відновлення та аналіз після інциденту: після усунення загрози SOC проводить детальний аналіз для удосконалення політик безпеки та підвищення готовності до аналогічних ситуацій[4].

4. Звітність (Reporting) – це документування інцидентів та створення аналітичних звітів є основою для стратегічного управління безпекою.

- Технічні звіти: реєструють усі деталі подій, що дозволяє відтворювати інциденти в майбутньому.
- Аналітичні звіти: надають огляд тенденцій, ключових показників SOC (MTTD, MTTR, кількість інцидентів тощо) і рекомендації щодо поліпшення.
- Регуляторна звітність: необхідна для підтвердження відповідності стандартам і вимогам аудиту.

SOC можна порівняти з центром управління авіарейсами або відділом швидкого реагування, який постійно моніторить тисячі «датчиків» – логів, трафіку, сигналів про аномалії – та миттєво реагує на інциденти. Якщо систему безпеки організації розглядати як «організм», то SOC є його центральною нервовою системою, яка сприймає, аналізує та координує дії проти загроз, забезпечуючи стабільність і життєздатність всієї інфраструктури[1,2,10].

1.2. Архітектурні принципи SOC

1.2.1. Базові елементи SOC: збір подій, аналітика, реагування, управління

Архітектура SOC функціонує як система, що об'єднує технологічні платформи, людські ресурси і управлінські процеси в єдину екосистему кібербезпеки. Її основа полягає в концепції PPTGC (People, Processes, Technology, Governance, Compliance), яка відображає всебічний підхід до безпеки: взаємодію між аналітиками, стандартизованими процедурами, технічними засобами, стратегічним управлінням і дотриманням норм.

Кожен окремий функціональний елемент архітектури виконує певну, але взаємопов'язану роль, формуючи замкнутий цикл управління інцидентами.

1. Збір подій (Data Collection / Ingestion) – процес збору даних є основою архітектури SOC, оскільки саме на цьому етапі створюється потік подій, на основі якого функціонують всі наступні етапи аналітики та реагування таких як:

- Джерела подій – SOC інтегрує інформацію з численних джерел – мережевих пристроїв (файерволів, UTM, IDS/IPS), серверів, систем віртуалізації, кінцевих пристроїв (endpoint agents), баз даних, хмарних платформ і систем автентифікації. Додатково враховуються контекстуальні дані – результати перевірок на вразливості, інформація про конфігурацію активів, геолокаційні дані, а також зовнішні потоки кіберрозвідки, що містять показники компрометації (IoC).
- Обробка і нормалізація – інформація надходить у великих обсягах з різною структурою та форматом, тому вона проходить етап нормалізації, перетворюючись у єдиний формат, який дозволяє подальшу кореляцію.На цьому етапі система SIEM виконує фільтрацію шуму, класифікацію подій і пріоритизацію у відповідності до їх критичності.
- Важливість збору – ефективність SOC безпосередньо залежить від повноти зібраних даних – неповна або неточна телеметрія може призвести до «сліпих зон», де атаки можуть залишитися непоміченими[8,12].

2. Аналітика (Analytics) – аналітичний рівень є центром SOC, де здійснюється перетворення даних у знання та прийняття рішень на кшталт:

- Кореляція подій (Event Correlation) – SIEM аналізує інформаційні потоки з різних джерел, співставляючи їх за часовими, поведінковими або контекстуальними характеристиками. Це сприяє виявленню складних, багатогранних атак, які неможливо ідентифікувати, якщо розглядати події окремо [1].

- Інтелектуальна аналітика (AI/ML) – впровадження алгоритмів машинного навчання дозволяє виявляти аномальні паттерни поведінки, створювати базові профілі активності користувачів, передбачати можливі вектори атак і зменшувати кількість помилкових спрацювань. У деяких архітектурах SOC застосовуються нейронні моделі, що навчаються на історичних даних для автоматичного виявлення відхилень у трафіку або логах[4].
- Поглиблений аналіз (Deep Analysis) – після виявлення підозрілих подій проводиться детальний кореляційний аналіз, що включає перевірку показників, зворотне трасування джерел загроз і перевірку в контексті MITRE ATT&CK для визначення фази атаки.

Результатом аналітичного етапу є створення ситуаційної обізнаності, яка представляє собою динамічне розуміння нинішнього стану безпеки в режимі реального часу[1,12,17].

3. Реагування (Response) – цей етап визначає, як швидко SOC може зупинити атаку і мінімізувати її наслідки. Реагування має наступні фази:

- Реакція зазвичай відбувається у трьох етапах:
  - Containment – локалізація інциденту (ізоляція уражених систем).
  - Eradication – усунення причин та шкідливих елементів.
  - Recovery – повернення систем до безпечного стану.
- Автоматизація реагування – SOAR-платформи розширюють функціональність SIEM, забезпечуючи оркестрацію процесів – узгодження дій між інструментами, аналітиками і системами. Завдяки сценаріям реагування, процеси виконуються частково або повністю автоматизовано, що значно скорочує середній час відновлення (MTTR).
- Людський чинник – навіть із високим рівнем автоматизації, ключові рішення (наприклад, підтвердження інциденту або масштаб ізоляції) залишаються за аналітиками, оскільки вони володіють здатністю інтерпретувати контекст подій[1,4,7].

4. Управління (Management / Governance) – цей етап визначає стратегічну основу для SOC, забезпечуючи контрольованість, узгодженість та відповідність усіх процесів. Цей етап забезпечується наступними пунктами:

- Стратегічне управління – розробляються місія, цілі, ключові показники ефективності (KPI) і політики SOC, які відповідають бізнес-стратегіям організації. Управлінські процедури охоплюють аудит, регулярну оцінку продуктивності, управління ризиками та постійне вдосконалення процесів.
- Відповідність та регуляція – SOC забезпечує виконання міжнародних стандартів (ISO/IEC 27001, NIST CSF, GDPR, SOC 2), а також національних вимог у сфері кібезпеки. Це формує довіру до організації з боку клієнтів, партнерів та контролюючих органів.
- Метрики – для оцінки ефективності SOC використовуються кількісні показники, зокрема:
  - MTTD (середній час виявлення);
  - MTTR (середній час реагування);
  - Рівень хибних спрацьовувань;
  - Рівень зрілості SOC у аспекті безпеки[11,12,17].

1.2.2. Принципи побудови SOC: централізація, безперервність, масштабованість

Архітектурні рішення SOC залежать від його типу, розміру та цілей. Серед ключових принципів побудови виділяють:

Централізація – традиційна архітектура SOC передбачає централізований контроль, у якому консолідуються всі події безпеки. Проте сучасні тенденції вказують на перехід до дистрибутивних або змішаних моделей, що усувають єдину точку відмови та покращують гнучкість реакцій. У глобалізованому середовищі SOC часто організовують на основі децентралізованої архітектури, де місцеві підрозділи SOC взаємодіють з центральним регіональним центром. Основна причина цього зсуву – уникнення єдиної точки відмови. Архітектура

інтегрованих центрів NOC та SOC також може бути багаторівневою та масштабованою [8,12].

Безперервність – SOC працює без перерви, забезпечуючи постійний моніторинг і реагування. Це досягається завдяки відмовостійким архітектурним рішенням, таким як резервні сервери, кластеризація SIEM, географічне дублювання і автоматизовані системи оповіщення про збої. Безперервність забезпечується також через ротацію аналітиків, внутрішнє навчання та проведення тестів готовності[11].

Масштабованість – SOC повинен бути здатним масштабуватися відповідно до обсягів трафіку, кількості джерел логів і складності кібератак. Це реалізується завдяки модульній архітектурі SIEM, розподіленій обробці даних і можливості динамічно додавати нові джерела без порушення роботи системи. Масштабованість є ключовою умовою для інтеграції нових технологій – платформ розвідки загроз, XDR або поведінкових аналітичних модулів. Сучасний SOC прагне до забезпечення високого рівня автоматизації та великої частки залученості людей, де ефективність досягається завдяки масштабованим технологіям, а успіх операцій забезпечується завдяки кіберстійкості та гнучким архітектурним моделям, які мінімізують вразливість, пов’язану з централізацією[5,7].

1.2.3. Мінімальна базова архітектура SOC (Core Model)

Мінімальна архітектура Центру операцій безпеки (SOC) визначає основні елементи, необхідні для ефективного функціювання безпекового центру. Вона складає основу операційної моделі, що забезпечує виявлення, аналіз, реагування та вдосконалення системи захисту організації. Незалежно від варіанту SOC – внутрішнього (Internal SOC), керованого зовнішнім постачальником (Managed Security Service Provider, MSSP) або гібридного (Hybrid SOC) – її структура базується на чотирьох взаємопов’язаних

компонентах моделі PPTGC (Люди, Процеси, Технології, Управління та Відповідність), технологічно інтегрованих через платформу SIEM.

1. Рамкова модель PPTGC

Люди – Ключовим елементом SOC є персонал, який відповідає за моніторинг, аналіз і реагування на інциденти. У типовій організаційній структурі SOC виділяються три рівні аналітиків (Tier 1–3), інженерів безпеки, менеджерів SOC та спеціалістів з розвідки загроз:

- Tier 1 (Аналітик сповіщень) – виконує початковий моніторинг, перевіряє тривоги, проводить базову фільтрацію шумів і передає події для подальшої обробки.
- Tier 2 (Реагування на інциденти) – детальніше аналізує інциденти, визначає характер загрози, масштаби впливу та координує дії для реагування.
- Tier 3 (Переслідувач загроз/Експерт з цифрової криміналістики) – займається розслідуванням складних інцидентів, кореляцією маловідомих подій, полюванням на загрози та цифровою криміналістикою.
- Менеджер SOC – відповідає за управління змінами, ефективність процесів, настановлення пріоритетів для реагування та здійснення зв'язку з керівництвом організації.
- Інженери безпеки – здійснюють підтримку інфраструктури SOC, оптимізують SIEM, SOAR, інтегрують джерела логів, а також оновлюють правила кореляції та плейбуки.

Отже, людський фактор визначає якість аналітики, швидкість реагування та загальну ефективність SOC.

Процеси – це стандартизовані та задокументовані дії, що забезпечують повторюваність, прозорість і передбачуваність функціонування SOC. Основні елементи процесного рівня:

- SOP (Стандартні операційні процедури) – визначають стандартизовані кроки для виконання типових операцій, таких як обробка подій або управління інцидентами.
- Плейбуки – структуровані сценарії реагування на певні типи атак (наприклад, фішинг, C2-комунікація, виявлення шкідливого програмного забезпечення). Вони можуть реалізовуватися вручну або через системи SOAR для автоматизації.
- Ескалація (Ескалаційний процес) – механізм передачі інцидентів на вищий рівень компетенції, коли аналітик не може самостійно вирішити питання.
- Управління тікетами (Ticket Management) – система, що обліковує інциденти, фіксуючи кожен випадок, його статус, виконавців та час реагування (MTTR – Середній час реагування).
- Звітність та аудит (Reporting & Audit) – документує виконані дії, оцінює ефективність SOC, забезпечує зворотний зв’язок та вдосконалення процесів.

Наявність стандартизованих процедур гарантує виконання дій у стресових ситуаціях, а також відповідність вимогам безпеки та аудиту.

Технології – технологічний шар є основою операційної потужності SOC. Він включає зв’язані між собою інструменти для збору, аналізу, кореляції, автоматизації та реагування:

- SIEM (Управління інформацією та подіями безпеки) – основний компонент, що здійснює збір, нормалізацію, кореляцію логів і створення подій безпеки.
- SOAR (Оркестрація, автоматизація та реагування на безпеку) – автоматизує процес реагування на інциденти, забезпечує інтеграцію між різними системами безпеки та зменшує час реагування.
- IDS/IPS (Системи виявлення/запобігання вторгнень) – контролює мережевий трафік для виявлення та блокування спроб вторгнення.

- EDR (Виявлення та реагування на кінцевих точках) – надає детальну видимість активності на кінцевих пристроях, підтримуючи їх ізоляцію або усунення шкідливих процесів.
- UEBA (Аналітика поведінки користувачів і сутностей) – застосовує машинне навчання для аналізу поведінки користувачів і пристроїв, виявляючи аномалії, що можуть свідчити про внутрішні загрози.

Цей рівень забезпечує технічну інтеграцію центру операцій безпеки (SOC) в рамках всієї інфраструктури кібербезпеки, створюючи єдину екосистему для моніторингу і реагування.

Управління та Відповідність – цей елемент забезпечує стратегічний контроль, ефективність і відповідність діяльності SOC міжнародним та галузевим стандартам. Основні завдання цього рівня:

- Стратегічне управління – визначення місії SOC, основних показників ефективності (KPI, KRI), метрик продуктивності, а також пріоритетів реагування.
- Аудит і контроль якості – регулярна перевірка ефективності процесів, тестування процедур реагування, а також проведення внутрішніх і зовнішніх аудиторських перевірок.
- Відповідність стандартам – виконання вимог таких нормативів, як ISO/IEC 27001, NIST SP 800-61, GDPR, PCI DSS.
- Управління ризиками – виявлення та оцінювання ризиків інформаційної безпеки, контроль залишкових ризиків після впровадження заходів.

Отже, Управління та Відповідність забезпечує, що SOC функціонує не лише технічно справно, а й у рамках регуляторних, етичних і корпоративних вимог[6,12,17].

2. Основи технологічної моделі SIEM

Архітектура SIEM (Управління інформацією та подіями безпеки) є основою SOC, забезпечуючи централізований збір, збереження, обробку та

аналіз подій безпеки. SIEM слугує технологічною основою всіх діяльностей SOC та складається з кількох взаємопов'язаних шарів:

Джерела даних – джерела логів і подій охоплюють:

- мережеві пристрої (файерволи, маршрутизатори, комутатори);
- системи виявлення вторгнень (IDS/IPS);
- кінцеві системи (EDR, антивірусні програми, операційні системи);
- сервери, бази даних, хмарні послуги;
- контекстуальні джерела – сканери вразливостей, системи управління активами (CMDB), платформи кіберрозвідки (Threat Intelligence Feeds).

Чим більше джерел охоплено, тим більш повноцінною є аналітика SOC.

Колектори відповідають за збирання, агрегацію та передачу логів до центрального сховища SIEM. Вони можуть бути агентами (встановленими на кінцевих точках) або безагентними шлюзами, що отримують дані через Syslog, API або системи обміну повідомленнями (наприклад, Kafka). Ключові функції:

- буферизація логів для уникнення втрат даних;
- початкова нормалізація та фільтрація шуму;
- шифрування даних під час передачі до SIEM[1].

Ядро обробки (ядро SIEM) – це аналітичний центр, який виконує:

- Нормалізацію – перетворення логів різних форматів у єдиний стандарт.
- Кореляцію – виявлення зв'язків між подіями для визначення складних атак.
- Класифікацію – категоризацію інцидентів за типом загрози.
- Пріоритизацію – оцінку критичності подій на базі контексту й ризику.

Цей шар закладає основу для ситуаційного усвідомлення та надає аналітикам дані для ухвалення рішень.

Зберігання та звітність – дані про події та інциденти зберігаються у сховищах для подальшого аналізу, аудиту або юридичних розслідувань. Сучасні SIEM системи підтримують:

- тривале архівування для відповідності вимогам комплаєнсу;

- аналітичні панелі, що демонструють основні метрики SOC в реальному часі;
- звітність для керівництва, аудиторів або регуляторів;
- інтеграцію з інструментами бізнес-аналітики для більш глибокого аналізу тенденцій атак.

Таким чином, SIEM є не лише технічним рішенням, а аналітичною платформою SOC, яка об’єднує всі компоненти PPTGC в єдину систему для виявлення, оцінювання та реагування на загрози[12].

1.3. Методологічні та нормативні засади функціонування SOC

Архітектура і діяльність Центру безпеки операцій (SOC) базуються на системному підході до управління інформаційною безпекою, де методологічні та нормативні стандарти становлять основи для організації узгоджених процесів моніторингу, реагування та постійного вдосконалення. Стандарти NIST, ISO/IEC та настанови ENISA формують загальну рамку, яка визначає вимоги до процесів, документації, комунікацій та результативності роботи SOC[12].

1.3.1. SOC у контексті міжнародних стандартів NIST CSF, ISO/IEC 27035, ENISA SOC Guidelines

Міжнародні стандарти створюють єдине концептуальне середовище, в рамках якого SOC може систематизувати політики, оцінювати рівні зрілості процесів і забезпечувати можливість порівняння показників результативності.

Національний інститут стандартів і технологій (NIST) – SOC, що діє згідно з рамками NIST Cybersecurity Framework (CSF), реалізує п’ять основних функцій: Identify, Protect, Detect, Respond, Recover, які відображають повний цикл управління кіберризиками і ґрунтується на:

- Публікація NIST SP 800-61 Rev.2 "Посібник з обробки інцидентів комп'ютерної безпеки" є основоположною для розвитку процесу управління інцидентами (Incident Response Lifecycle). Вона визначає ролі, етапи реагування, комунікаційну політику, методи ескалації та вимоги до документації інцидентів.
- Стандарти NIST також передбачають категоризацію подій, класифікацію рівнів серйозності та впровадження механізмів оцінки зрілості SOC через моделі зрілості[1].

Стандарт ISO/IEC 27035:2016 пропонує цілісний підхід до управління інцидентами інформаційної безпеки в рамках системи менеджменту безпеки (ISMS) базою якого слугують:

- Частина 1 ("Принципи управління інцидентами") визначає загальні принципи організації процесу, ролі та відповідальність учасників, а також процедури обміну інформацією.
- Частина 2 ("План дій в разі інциденту та структури") описує формування команд реагування (CSIRT/SOC), їхні взаємодії з керівництвом і механізми обміну інформацією між організаціями.
- Узгодженість SOC із стандартом ISO/IEC 27035 забезпечує інтеграцію його процесів в загальну політику управління ризиками компанії (Risk Management), що є критично важливим для дотримання вимог стандарту ISO/IEC 27001[12].

Рекомендації ENISA (Агентство Європейського Союзу з кібербезпеки) – ENISA розробляє рекомендації для національних та корпоративних SOC, що ґрунтуються на принципах "кращих практик":

- У "Посібнику з управління інцидентами" агентство формулює структуру процесів SOC, механізми ескалації, класифікації інцидентів і координації з CERT/CSIRT.

- Рекомендації ENISA підкреслюють важливість розподілу функцій на рівні (Tier 1–3) і необхідність застосування автоматизованих засобів кореляції подій, що забезпечує відповідність моделі PPTGC.
- ENISA також встановлює принципи етичного збору та використання кіберрозвідданих (Threat Intelligence), включаючи їхнє фіксування та оцінювання достовірності[20].

Отже, ці стандарти та рекомендації забезпечують нормативну цілісність SOC, сприяють згідності політик безпеки та створюють основу для аудиту відповідності.

1.3.2. Підходи до оцінки ефективності SOC (KPI, MTTD, MTTR)

Оцінка ефективності SOC визначає його спроможність до швидкого виявлення, класифікації та усунення загроз. Це критично важливо для стратегічного управління ризиками та вдосконалення операційних процесів.

Ключові показники ефективності (Key Performance Indicators, KPI) – система KPI в SOC використовується не тільки для вимірювання швидкості реагування, а також для кількісного та якісного аналізу зрілості процесів.

- Кількісні метрики включають:
  - Кількість виявлених інцидентів – загальна кількість підтверджених інцидентів за визначений період;
  - Кількість закритих інцидентів – відсоток інцидентів, завершених без ескалації;
  - Рівень хибних спрацьовувань (FPR) – відсоток неправильно виявлених інцидентів;
  - Середній час на створення та призначення тікета – середній часовий період для оформлення тікета;
  - MTTD (Середній час виявлення) та MTTR (Середній час реагування).

- Якісні метрики оцінюють складність аналізу, глибину дослідження першопричин (root cause analysis), рівень автоматизації, точність класифікації та якість підготовлених звітів.
- Обмеження традиційних KPI: кількісні показники можуть вводити в оману щодо реальної ефективності. SOC з низьким показником MTTD може одночасно демонструвати значну частку пропущених інцидентів. З цієї причини сучасні практики включають інтеграцію "метрик якості виконання", які враховують контекст і пріоритетність подій.

Часові показники:

- MTTD (середній час до виявлення) – ілюструє швидкість виявлення загроз безпеки; низьке значення свідчить про ефективність кореляційних правил SIEM.
- MTTR (середній час реагування/відновлення) – вимірює тривалість між підтвердженням інциденту та повним відновленням функціональності.
- MTTT (середній час до класифікації) – показник швидкості первинного аналізу та категоризації; має важливе значення для SOC рівня Tier 1.
- MTTFV (середній час до виправлення вразливості) – метрика для оцінки взаємодії SOC та команд з управління вразливостями[17].

Автоматизація через платформи SOAR та UEBA здатна значно зменшити MTTD, MTTR і TTI (час до розслідування), що безпосередньо покращує можливості SOC для превентивних дій.

Методологія SOC-AAM (SOC Analyst Assessment Method) пропонує багатовимірну оцінювальну систему, яка враховує не лише швидкість, але й якість ухвалених рішень, докладність аналізу та ефективність комунікацій під час реагування[2].

1.3.3. Процесна модель SOC

Функціонування SOC визначається процесним підходом, який представляє собою послідовність етапів від підготовки до дій після інциденту.

Життєвий цикл реагування на інциденти (модель NIST) поділяються на такі етапи:

1. Підготовка – розробка процедур реагування на інциденти інформаційної безпеки, політик, резервних планів реагування на інциденти ІБ, навчання співробітників, забезпечення резервування інфраструктури та визначення каналів основної та резервної комунікації.
2. Виявлення та аналіз: використання SIEM, IDS/IPS, UEBA для збору даних, вивчення закономірностей поведінки та виявлення аномалій, сортування спрацювань системи SIEM, поглиблене дослідження ескальованих інцидентів, включаючи аналіз логів, мережевих пакетів та контекстуальних даних для визначення масштабу атаки та уражених систем.
3. Локалізація, усунення, відновлення: обмеження впливу інциденту, очищення систем, перевірка цілісності даних, проведення перевірки після відновлення.
4. Постінцидентна діяльність: проведення ретроспективного аналізу, складання звіту, проведення сесії "уроки навчання", коригування політик[1].

Додаткові моделі управління інцидентами:

- SANS PICERL: застосовується в багаторівневих SOC, передбачає постійний зворотний зв'язок між етапами.
- OODA Loop (Observe, Orient, Decide, Act): впроваджується в аналітичних SOC, інтегруючи інформацію про загрози в процес ухвалення рішень.
- Плейбуки: забезпечують стандартизацію реагування; можуть бути адаптованими та автоматизованими (динамічні плейбуки) на SOAR-платформах.

Управління процесами – SOC впроваджує централізовану систему управління інцидентами через модулі керування випадками, які охоплюють створення тікетів, автоматичну ескалацію, моніторинг дій аналітиків та зберігання історії розслідувань[1,4].

Ця структура забезпечує прозорість, повторюваність і відтворюваність процесів, а також слугує основою для подальшого вдосконалення за моделлю безперервного покращення.

1.4. Організаційні аспекти SOC

Ефективність функціонування SOC залежить від його внутрішньої структури, розподілу ролей, комунікаційних шляхів та зрілої системи управлінських процесів. Організаційна схема повинна забезпечувати відповідний баланс між оперативною ефективністю, адаптивністю у реагуванні та контролем за відповідністю стандартам безпеки.

1.4.1. Основні ролі персоналу SOC (Tier 1–3, SOC Manager)

Типова структура SOC базується на трирівневій моделі компетенцій, яка охоплює глибину технічних знань, рівень аналітичної відповідальності та швидкість реагування. Це розділення дає змогу знизити навантаження на старших аналітиків, упорядковувати потік інцидентів і забезпечувати неперервність моніторингу[10].

Таблиця 1.1

Основні ролі персоналу SOC рівня Tier 1-3

Рівень	**Роль**	**Основні обов'язки**
Tier 1	Аналітик/ Фахівець з Тріажу (Triage Specialist)	Збір необроблених даних, перегляд сигналізації та сповіщення. Їм потрібно підтвердити, визначити, або налаштувати критичність сповіщень і збагатити їх відповідні дані. На кожне сповіщення фахівець із сортування щоб визначити, чи є він виправданим чи хибним позитивним результатом. Додатковою відповідальністю на цьому рівні є ідентифікація інших подій високого ризику та потенційних інцидентів. Усім цим необхідно розставити пріоритети відповідно до їх критичності. Якщо виниклі проблеми не можуть бути вирішені на цьому рівні, їх передають до аналітиків рівня 2.

Продовження табл. 1.1

Рівень	Роль	Основні обов'язки
Tier 2	Фахівець з Реагування на Інциденти (Incident Responder)	Переглядають більш критичні інциденти безпеки, викликані ескалацією спеціалістів із сортування та проводять більш поглиблену оцінку використання аналізу загроз (індикатори компрометації, оновлені правила тощо). Вони повинні розуміти масштаби атаки та знати про уражені системи. Необроблені дані телеметрії про атаки, зібрані на рівні 1, перетворюються на дієві дані про загрози на цьому рівні. Якщо виниклі проблеми не можуть бути вирішені на цьому рівні, їх передають до аналітиків рівня 3.
Tier 3	Мисливець за Загрозами (Threat Hunter) / Експерт з Аналізу Загроз	Найбільш досвідчена робоча сила в SOC. Вони справляються з основними інцидентами, переданих їм від служб реагування на інциденти. Вони також виконують або принаймні контролюють уразливість оцінки та тести на проникнення для виявлення можливих векторів атаки. Їх найважливіший обов’язок для проактивного виявлення можливих загроз, прогалин у безпеці, і вразливості, які можуть бути невідомі. Вони також повинні рекомендувати способи оптимізації моніторингу безпеки. Також, будь-які критичні сповіщення про безпеку, аналіз загроз та інші безпекові дані, надані аналітиками рівня 1 і 2, повинні бути перевірено на цьому рівні.

Менеджери SOC контролюють команду безпеки. Вони забезпечують технічне керівництво, якщо потрібно, але найголовніше, вони відповідають за адекватне управління командою. Це включає наймання, навчання та оцінку членів команди, створення процесів, оцінку звітів про інциденти, а також розробку та реалізацію необхідних планів комунікацій у кризових ситуаціях. Вони також контролюють фінансові аспекти SOC, підтримують перевірки безпеки та звітують перед керівником інформаційної безпеки (CISO) або відповідною керівною посадою найвищого рівня. Основні напрямки діяльності SOC Manager:

- Керування персоналом – формування змін, моніторинг ефективності, сертифікація, реалізація програми безперервного навчання.
- Організація процесів – оптимізація сценаріїв реагування, контроль SLA, координація заходів у разі масових інцидентів.
- Звітність і комунікації – підготовка виконавчих звітів, участь у стратегічних нарадах з питань кіберстійкості.
- Виконання регуляторних вимог – інтеграція стандартів ISO/IEC 27001, NIST CSF, SOC 2 у внутрішні процедури SOC[17].

1.4.2. Взаємодія SOC з іншими підрозділами IT та кібербезпеки

SOC не може функціонувати в ізоляції – це інтегрована частина корпоративної кіберекосистеми. Якість співпраці з іншими командами прямо впливає на швидкість реагування, точність аналізу та ефективність запобігання атакам. Приклад схеми взаємодії ріхних підрозділів з SOC на (рис. 1.1).

Рис. 1.1 Взаємодія SOC з іншими підрозділами

Взаємодія з IT-операціями (NOC / NetOps) – історично, SOC і NOC діяли окремо, що призводило до конфліктів в операціях. Сучасні методи розвивають концепцію NetSecOps, яка інтегрує безпекові та мережеві процеси.

Переваги інтеграції:

- усунення повторення функцій та скорочення часів реагування;
- спільне використання інструментів для моніторингу, аналізу журналів та систем управління запитами;
- швидке інформування SOC про заплановані зміни в інфраструктурі, що зменшує число хибнопозитивних подій;
- створення єдиного SLA для забезпечення інтеграції процесів доступності, продуктивності та безпеки.

Взаємодія у сфері кібербезпеки – SOC активно співпрацює з такими підрозділами:

- Incident Response (IR) – спільне реагування та розслідування інцидентів;
- Threat Intelligence (TI) – збір і використання індикаторів компрометації;
- Vulnerability Management – обмін даними про вразливості;
- Forensics / Digital Investigation – детальний аналіз інцидентів та збір доказів.

Співпраця з іншими бізнес-підрозділами – у випадках критичних інцидентів SOC координує дії з:

- Юридичним відділом – визначення юридичних наслідків та підготовка доказів;
- Відділом корпоративних комунікацій – управління публічними заявами задля запобігання втраті репутації;
- Кадровим відділом – у ситуаціях внутрішніх інцидентів або порушень політики доступу.

Співпраця із зовнішніми організаціями (MSSP, CERT, Vendors) – у рамках моделі MSSP SOC функціонує як сервісна платформа для різних клієнтів. Така взаємодія передбачає – обмін розвідданими через міжнародні

платформи (Threat Sharing Communities), використання стандартизованих протоколів для сповіщень (STIX/TAXII) та участь у національних або корпоративних CERT/CSIRT ініціативах[12,17].

1.4.3. Основні політики SOC: реагування, ескалація, аудит, управління

Політики реагування на інциденти та плейбуки – плейбуки деталізують кроки дій для різних категорій інцидентів (наприклад, фішинг, компрометація облікових записів, lateral movement). Кожен плейбук містить наступні компоненти:

1. Тип інциденту і його джерело (endpoint, мережевий трафік, cloud-сервіс).
2. Алгоритм аналізу та ескалації.
3. Критерії рівня критичності.
4. Осіб, відповідальних за реагування, і очікуваний час реагування.

Сучасні SOC використовують системи SOAR для реалізації плейбуків, автоматизуючи дії – від ізоляції елементів до генерації звітів, що зменшує вплив людського фактора та прискорює процеси MTTD/MTTR[8,12].

Процеси ескалації забезпечують вертикальну комунікацію між рівнями SOC та між SOC і менеджментом. Кожен інцидент має чітко визначений Service Level Agreement (SLA), який встановлює часовий поріг для реагування. Якщо інцидент не вирішується у встановлений термін, система автоматично ескалює його на вищий рівень.

Важливо зберегти баланс між надмірною ескалацією (що може перевантажити Tier 2/3) та недооціненням подій (що може призвести до відсутності реакції на атаку)[10].

Політика аудиту та управління (Governance & Compliance) – управління в SOC включає необхідність забезпечення наступних пунктів для забезпечення роботи усього SOC належним чином:

- розробку політик доступу, контролю змін, ведення журналів;

- регулярні внутрішні аудити для перевірки ефективності процесів реагування;
- дотримання нормативних вимог (GDPR, ISO 27001, NIS2);
- аналіз результативності технологій за допомогою KPI та оцінки зрілості SOC (SOC Maturity Model).

Зокрема важливою є зміна управлінських документів – система фіксації змін у мережевих або програмних середовищах, що допомагає уникнути неправомірних спрацьовувань і забезпечує можливість історичного відстеження.

Структура SOC визначає його здатність та ефективність у протидії кібератакам. Оптимальний баланс між людьми, процесами, технологіями і управлінням (PPTGC) дозволяє центру швидко реагувати на інциденти, запобігаючи дублюванню функцій і підтримуючи постійний процес вдосконалення. SOC, завдяки розвиненій системі комунікації, автоматизації процесів реагування і ефективному управлінню політиками, здатен забезпечити кіберстійкість організації навіть у швидко змінюваному загрозливому середовищі[12,17].

Висновки до розділу 1

У даний розділі узагальнені ключові теоретичні засади побудови Центру операцій безпеки та демонструє його значущість у формуванні кіберстійкості організації, а саме:

1. Проведено аналіз поточного стану створення та функціонування центрів операцій безпеки (SOC), що дозволило оцінити їх значення як основного елемента у забезпеченні кіберстійкості організації. Визначено, що SOC є ключовим інституційним компонентом системи захисту від кіберзагроз, що забезпечує постійний моніторинг, виявлення загроз, оперативну відповідь та координацію заходів безпеки.

2. Встановлено концептуальні основи моделі PPTGC, яка об’єднує підготовлених співробітників, стандартизовані процеси, інтегровані технології, належне управління та контроль за відповідністю. Вивчено структуру взаємодії цих складових, що дозволяє підтримувати цілісність та узгодженість SOC як організаційно-технічної системи.

3. Вивчено ролі та компетенції фахівців SOC, включаючи рівні Tier 1–3 і управлінські обов’язки. Встановлено, що продуктивність SOC прямо залежить від кваліфікації аналітиків, здібностей до ескалації інцидентів, проведення детальних розслідувань, виконання операцій з виявлення загроз (Threat Hunting) та стратегічного управління на безпековому рівні.

4. Проведено аналіз процесного аспекту SOC, який включає стандартні операційні процедури (SOP), плейбуки реагування, механізми ескалації, звітності та взаємодії з зовнішніми структурами. Визначено критичну важливість стандартизації процесів, яка гарантує передбачуваність дій і скорочує час реакції на інциденти.

5. Проаналізовано технологічну основу SOC, зосереджуючи увагу на системах SIEM, і визначено їх роль як центрального елемента всієї архітектури. Окреслена функціональна структура SIEM: джерела даних, агрегатори подій, модулі кореляції та аналітики, а також системи зберігання та звітності. Підтверджено, що наявність такої багатошарової архітектури є мінімальною вимогою для ефективної функції SOC.

6. Встановлено взаємозв'язок між архітектурою SOC та вимогами управління та відповідності (Governance & Compliance). Підкреслено необхідність дотримання стандартів, аудиторських процедур, регуляторних вимог та політик з інформаційної безпеки для забезпечення контролю та якості функціонування SOC.

7. Обґрунтовано важливість створення мінімальної базової архітектури SOC у контексті реальних умов України, враховуючи необхідність адаптації до обмежених ресурсів, високих рівнів загроз і потребу в масштабованості рішень.

РОЗДІЛ 2 ТЕХНОЛОГІЧНА АРХІТЕКТУРА ТА ПРОДУКТИ SOC

2.1. Архітектура SOC і її рівні

Центр операцій безпеки (SOC) є основним елементом захисту кіберзахисту в організації, що забезпечує постійний моніторинг, виявлення, аналіз, реакцію та попередження про інциденти, пов'язані з інформаційною безпекою. Архітектура SOC визначає не тільки технічні аспекти, а й організаційні, процедурні та управлінські елементи, які складають єдину систему безпеки[1].

SOC може бути розглянуто як багаторівнева, інтегрована структура, де людські ресурси, процеси, технології, управлінські функції та дотримання норм складають взаємопов'язану систему, що націлена на забезпечення стійкості, оперативної реакції та зменшення ризиків, пов’язаних з кіберінцидентами[12].

2.1.1. Загальний архітектурний каркас SOC (PPTGC)

Архітектура SOC зазвичай представлена за допомогою концептуальної моделі PPTGC (People, Processes, Technology, Governance and Compliance), яка відображає основні компоненти діяльності SOC, як соціотехнічної системи:

- Люди (People): складають кадровий склад SOC – аналітики різних рівнів, фахівці з безпеки, архітектори, організатори реагування на інциденти, менеджери SOC, а також hunting-спеціалісти. Вони керують та налаштовують засоби моніторингу, розробляють стратегії стримування та відновлення, контролюють оцінку вразливостей та надають рекомендації щодо оптимізації моніторингу безпеки. Їхня майстерність впливає на швидкість, точність і глибину проведеного аналізу[17].
- Процеси (Processes): представляють стандартизовані робочі процедури - від моніторингу подій до аналізу після інциденту. Ці процедури, для прискорення реагування, детально документуються у вигляді playbooks,

стандартних операційних процедур (SOP) та угод про рівень обслуговування (SLA).

- Технології (Technology): охоплюють інструменти SOC, такі як SIEM, SOAR, EDR/XDR, IDS/IPS, UEBA, платформи для збору інформації про загрози тощо. Вони забезпечують автоматизацію збору, кореляції, аналізу та реакцій на загрози[1,4].
- Управління (Governance): встановлює стратегічні цілі SOC, визначає політики контролю доступу, відповідальність та узгодженість з корпоративною стратегією безпеки. Управління ризиками ІБ вимагає впровадження міжнародного стандарту ISO/IEC 27005.
- Відповідність (Compliance): регулює дотримання міжнародних і національних стандартів безпеки ISO27001, NIST CSF, GDPR, SOC 2 та проведення регулярного моніторингу та перевірки ефективності програми управління кіберризиками, включаючи регулярні аудити безпеки.

Ця модель створює основи для розбудови SOC, де технологічна ефективність не може бути досягнута без кадрових компетенцій, стандартизованих процесів і легального дотримання норм[12].

2.1.2. Типи архітектури SOC

Архітектурний аспект SOC визначається масштабами організації, географічним розташуванням, вимогами регуляторів та бюджетними обмеженнями. Основні архітектурні моделі за розташуванням включають:

- Централізований SOC: всі дані з різних філій надходять до єдиної центральної платформи (Data Lake/SIEM Core), де виконується аналітика. Цей підхід забезпечує контроль, але створює єдину точку можливого збою (Single Point of Failure).
- Розподілений SOC (Distributed SOC, DSOC): об'єднує декілька SOC з різних регіонів, синхронізованих через єдину архітектуру даних шляхом

отримування, обробки, об’єднання та надання інформації про безпеку. Це збільшує відмовостійкість і масштабованість.

- Децентралізований SOC (Federated або Grid SOC): ця модель є комбінацією централізованої та розподіленої архітектур, вона має автономні SOC з власними наборами інструментів, які взаємодіють через стандартизовані API або обмін інформацією про загрози. Така архітектура поширена в міжнародних компаніях або MSSP.

В даний час спостерігається тенденція до переходу від централізованих до гібридних SOC, що поєднують централізовану кореляцію подій із розподіленим збором даних та локальною реакцією, з метою зменшення ризиків відмов та затримок в передачі телеметрії[8,12].

За організаційною моделлю управління типи архітектур поділяються на:

1. Внутрішній SOC (In-house SOC) – модель внутрішнього SOC, що передбачає повноцінну організацію, управління та підбір кадрів для центру операцій безпеки силами самої компанії. У цій архітектурі основні процеси — від збору логів до реагування на інциденти та підготовки звітності — виконуються внутрішніми експертами. Це забезпечує щільну інтеграцію SOC з корпоративною IT-інфраструктурою, бізнес-процесами та внутрішніми нормами.

Головною перевагою внутрішнього SOC є глибоке осмислення контексту організації. Аналітики мають прямий доступ до інфраструктури, що дозволяє швидшою інтерпретацію подій безпеки та ухвалення виважених рішень з урахуванням важливості активів. Ця модель також надає максимальний контроль над даними, що є критично важливим для компаній з підвищеними вимогами до конфіденційності або відповідності законодавству.

Проте внутрішній SOC вимагає суттєвих початкових та постійних вкладень. До таких витрат належать кошти на впровадження технологічного забезпечення, утримання інфраструктури, наймання та підготовку висококваліфікованих співробітників, а також забезпечення цілодобової

роботи. Тому ця модель, як правило, характерна для великих або зрілих організацій, які мають стабільний бюджет на кіберзахист.

2. Аутсорсинговий SOC (Outsourced SOC/MSSP) – аутсорсингова модель SOC передбачає залучення постачальника послуг у сфері безпеки (MSSP), який виконує функції моніторингу, аналізу і первинного реагування на інциденти. У такій ситуації організація делегує частину або більшість операційних функцій зовнішній команді, зберігаючи стратегічний контроль і ухвалення основних рішень за собою.

Головною причиною вибору цієї моделі є економія коштів та нестача внутрішньої експертизи. Аутсорсинговий SOC дозволяє швидко отримати доступ до досвідчених аналітиків, готових технологічних рішень та цілодобового моніторингу, без необхідності створювати власну команду. Це особливо актуально для організацій середнього розміру або тих, хто лише розпочинає будувати свою систему інформаційної безпеки.

Однак аутсорсингова модель має певні обмеження. Видимість інфраструктури клієнта для MSSP часто регулюється умовами угод щодо рівня обслуговування, політиками доступу або вимогами захисту конфіденційних даних. Це може ускладнити повноцінне підтвердження сповіщень та аналіз інцидентів. Додатково, аналітики MSSP зазвичай обслуговують кілька клієнтів одночасно, що іноді призводить до формального підходу до ескалації подій та зростання кількості повідомлень з низькою впевненістю, щоб не порушити умови угоди.

3. Комбінований SOC (Hybrid SOC) – комбінована модель SOC об'єднує внутрішні можливості організації з послугами зовнішнього MSSP, вважається найгнучкішою альтернативою для організацій середнього розміру. У цій архітектурі внутрішня команда відповідає за стратегічні рішення, управління інцидентами, роботу з важливими активами та взаємодію з бізнесом, тоді як MSSP забезпечує додаткові функції, включаючи цілодобовий моніторинг, збори інформації про загрози, підтримку форензики або аналіз складних атак.

Перевагою гібридного підходу є оптимальний баланс між контролем і економічною ефективністю. Організація зберігає результативну експертизу у своїй команді, водночас компенсуючи нестачу ресурсів або часу за рахунок зовнішніх партнерів. Ця модель також дозволяє поступово підвищити зрілість внутрішнього SOC, використовуючи MSSP як засіб передачі знань і підтримки в критичних ситуаціях[1].

2.1.3. Архітектура SIEM у контексті SOC

Система SIEM (Security Information and Event Management) є центральним елементом SOC, яка забезпечує забезпечуючи виконання критично важливих функцій: збір, нормалізацію, кореляцію, зберігання та візуалізацію безпекових подій. Її архітектура включає:

- Збирачі даних (Data Collectors) – агенти, які відповідають за отримання, агрегацію та фільтрацію необроблених даних з мережевих, серверних та хмарних джерел (firewalls, proxies, OS logs, vulnerability scanners, endpoint telemetry).
- Нормалізаційний шар (Normalization Layer) – уніфікує формати логів у єдиний стандартний формат, що забезпечує їхню сумісність для подальшого аналізу.
- Кореляційний механізм (Correlation Engine) – застосовую правила кореляції та виявляє закономірності поведінки або ланцюжків подій, які можуть вказувати на інцидент безпеки. Ці правила можуть бути спеціально розроблені аналітиками SOC для конкретних сценаріїв загроз організації. Кореляція допомагає виявити потенційні загрози, пов'язуючи розрізнені події, що поодинці не мали б значення.
- Аналітичний та AI шар (Analytics and AI Layer) – сучасні SIEM використовують моделі машинного навчання для зменшення кількості хибних спрацювань та для виявлення аномальної поведінки, також це допомагає аналітикам зосередитись на найбільш критичних інцидентах.

- Звітність та інформаційні панелі (Reporting and Dashboards) – забезпечують аналітику для управління, звітність з KPI (MTTD, MTTR, FP, TP) та інтеграцію з SOAR.

Таким чином, SIEM є ядром SOC, яке централізує керування даними про безпеку, але цей інструмент лише підтримує аналітиків у складній задачі виявлення та реагування, оскільки обчислення пріоритетів, вбудовані в SIEM, можуть виконувати "важку роботу", але фахівці все одно повинні вирішувати, які тривоги є реальними загрозами. Ефективність SIEM залежить від якості зібраних даних, обсягу телеметрії, правил кореляції та ступеня автоматизації[1,4].

2.1.4. **Архітектура SOAPA (Архітектура Платформи Операцій Безпеки та Автоматизації)**

SOAPA являє собою концептуальний підхід, що описує спосіб інтеграції різних систем безпеки через єдину архітектуру та розглядається як архітектура «знизу вгору» (bottom-up architecture), що має програмований верхній рівень, який може бути інструментований для виконання автоматизованих дій. Ця архітектура забезпечує інтеграцію процесів збору, аналізу, оркестрації, автоматизації та реагування. SOAPA складається з п’яти основних компонентів:

- Шар послуг даних – цей рівень відповідає за управління сирими даними, зібраними з усієї мережі. Включає генерацію даних, їхню агрегацію, захист та можливості зберігання.
- Шар інтеграції: функціонує як посередник між різними системами (SIEM, EDR, IDS, SOAR) через API, шини даних або брокери повідомлень, та слугує для полегшення функцій зазначених у шарі послуг даних.
- Шар аналітики: використовує штучний інтелект та машинне навчання для проведення поведінкових аналізів, прогнозування можливих атак (прогнозування загроз), оцінки ризиків і встановлення кореляцій між джерелами.

- Шар операцій безпеки – відповідає за безпосереднє виконання завдань з оркестрації, автоматизації та реагування на інциденти. Його мета – виявляти, класифікувати та усувати загрози, перетворюючи їх на дієві сповіщення чи розвідувальні дані
- Консоль управління– об’єднує всі функції в інтерфейс аналітиків SOC, надаючи SOC-командам інтегрований робочий простір, що включає дашборди, ключові показники ефективності, карти загроз та системи оповіщення.

SOAPA зміцнює інтеграцію між технологіями, зменшує розрізненість екосистеми SOC і забезпечує єдність між різними рівнями реагування[4].

2.1.5. Рівні SOC (Багаторівнева структура)

Стандартна структура SOC має багаторівневу ієрархію, яка забезпечує ефективний розподіл обов'язків і компетенцій.

Таблиця 2.1

Стандартна структура SOC

Рівень	**Роль**	**Основні обов'язки**
Tier 1	Triage Specialist (Спеціаліст з тріажу)	Моніторинг у реальному часі та конфігурування системних інструментів. Збір сирих даних, перегляд та збагачення (enrichment) тривог та сповіщень. Визначення, чи є сповіщення хибним спрацьовуванням (FP) чи справжньою тривогою. Ескалація інцидентів, які виходять за межі їхньої компетенції, до Tier 2.
Tier 2	Incident Responder (Фахівець із реагування на інциденти)	Поглиблений аналіз інцидентів, переданих з Tier 1. Огляд звітів, визначення постраждалих систем та обсягу атаки. Розробка та впровадження стратегій стримування та відновлення. Перетворення сирих даних на дієву інформацію.

Продовження табл. 2.1

Рівень	Роль	Основні обов'язки
Tier 3+	Threat Hunter (Мисливець за загрозами)	Найдосвідченіший персонал SOC. Обробка великих інцидентів, переданих з Tier 2. Проактивне виявлення можливих, ще невідомих загроз, прогалин безпеки та вразливостей (Threat Hunting). Нагляд за оцінкою вразливостей та тестуванням на проникнення. Надання рекомендацій щодо оптимізації інструментів моніторингу.

У сучасних SOC можуть також існувати спеціалізовані ролі:

- Аналітик розвідувальної інформації про загрози – займається інтеграцією зовнішніх інформаційних джерел TI.
- Фахівець у сфері криміналістики – аналіз після інцидентів.
- Інженер з автоматизації – відповідальний за розробку плейбуків з реагування на інциденти ІБ для системи SOAR.
- Спеціаліст з дотримання вимог – в його обов’язки входить перевірка політик та відповідності стандартам[1,12,17].

2.1.6. Специфіка взаємодії рівнів SOC

Ієрархічна модель передбачає висхідну ескалацію інцидентів, де кожен рівень забезпечує поглиблений аналіз ситуації. Проте дієздатний SOC також передбачає зворотний обмін знаннями, коли досвід аналітиків вищого рівня трансформується в правила, шаблони, автоматизацію і навчання для нижчих рівнів.

Серед ключових показників зрілості архітектури SOC можна виділити:

8. Формування правил і плейбуків – аналітики SOC, зокрема фахівці третього рівня, пропонують методи для покращення моніторингу безпеки. Використовуючи свій досвід і знання про конкретне середовище, аналітики

розробляють правила кореляції (випадки використання) для системи SIEM, які представляють собою форму явного знання. Результати аналізу загроз, що проводиться на високих рівнях, перетворюються у плейбуки – покрокові інструкції, необхідні для ефективної реакції на певні інциденти.

9. Налаштування та усунення хибних спрацьовувань – аналітики регулярно переглядають і коригують налаштування сигналізації з метою подальшого удосконалення і усунення хибних спрацьовувань (FP). Цей процес часто виконується вручну і вимагає постійного вдосконалення інструментів, що відображає інтеграцію досвіду аналітиків у технологічну систему.

10. Автоматизація (SOAR) – Рішення SOAR автоматизують і координують процеси реагування на інциденти, застосовуючи ті ж плейбуки, які створені на основі експертного досвіду. Ефективна автоматизація дозволяє аналітикам першого рівня зосередитися на завданнях, що потребують критичного мислення, замість виконання рутинних і монотонних операцій. Архітектура SOC є не лише технічною структурою, але й цілісною операційною моделлю, що об'єднує людей, процеси і технології в одну систему для досягнення кіберстійкості.

Ефективність SOC визначається його здатністю адаптуватися до загроз, рівнем автоматизації, глибиною інтеграції і узгодженістю управлінських процесів. Розвиток SOC проходить шлях від централізованих систем до інтелектуально-розподілених, орієнтованих на дані, автоматизованих платформ, спроможних забезпечити неперервну безпеку в режимі реального часу[1,4,7].

2.2. Технологічні компоненти SOC

Архітектура Центру операцій безпеки (SOC) спирається на набір взаємопов’язаних інструментів, які забезпечують повний процес моніторингу, виявлення, аналізу, ескалації та реагування на кіберінциденти. У контексті

постійно зростаючих кіберзагроз ефективність функціонування SOC визначається не тільки рівнем компетенції фахівців, але і ступенем автоматизації та інтеграції технологічних елементів.

Оскільки ніякий продукт не може покрити всі аспекти захисту, SOC зазвичай представлений у формі екосистеми, яка об'єднує SIEM, EDR/XDR, SOAR, Threat Intelligence (TI) та додаткові підсистеми, такі як NDR, UEBA, IDS/IPS.

2.2.1. SIEM-системи (Security Information and Event Management)

SIEM виступає головним елементом SOC, функціонуючи як "нервова система", що збирає події безпеки з різноманітних джерел: мережевих пристроїв, серверів, робочих станцій, програм, хмарних сервісів, систем доступу, антивірусного програмного забезпечення та інших.

Основна мета SIEM полягає у формуванні єдиної картини подій в організації для своєчасного виявлення аномалій та загроз.

Основні функції SIEM включають:

- Збір та агрегація подій – отримання даних у реальному часі через протоколи Syslog, API або агентські рішення.
- Нормалізація та парсинг – перетворення різнорідних логів у єдиний формат (Common Event Format, JSON, XML), що дозволяє створювати універсальні аналітичні правила.
- Кореляція подій – зв'язування окремих індикаторів (таких як спроби входу з різних IP-адрес, модифікація реєстру, запуск невідомих процесів) в актуальну аналітичну подію.
- Пріоритезація інцидентів – автоматичне визначення критичності на основі контексту, рівня загрози, цінності активів та історичних даних.

- Звітність і дашборди – візуалізація метрик безпеки для аналітиків SOC та керівництва (KPI, MTTR, індикатори відповідності стандартам ISO 27001, NIST)[1].

На ринку існує багато пропозицій різноманітних SIEM систем:

- Splunk Enterprise Security – надає потужні можливості аналітики та машинного навчання завдяки Machine Learning Toolkit (MLTK), використовується для виявлення поведінкових аномалій, аналітики користувачів (UEBA) та прогнозування інцидентів[4].
- Microsoft Sentinel – це хмарне SIEM/SOAR-рішення, що інтегрується з екосистемою Microsoft 365 Defender, Azure та GitHub Advanced Security.
- IBM QRadar – має вбудований аналіз потоків NetFlow та можливість інтеграції з XDR-компонентами.
- Micro Focus ArcSight – орієнтований на великі корпоративні мережі, пропонує гнучку побудову кореляційних правил і розширену аналітику подій.

Актуальною тенденцією у розвитку SIEM є перехід до XSIEM (Extended SIEM), де платформи об'єднують функції UEBA, SOAR та Threat Intelligence в єдиному аналітичному середовищі[1,4].

2.2.2. EDR/XDR-рішення (Endpoint / Extended Detection and Response)

EDR є системами для моніторингу, виявлення та реагування на загрози на кінцевих пристроях, таких як робочі станції, сервери і віртуальні машини. Вони надають детальну телеметрію про процеси, мережеву активність, доступ до файлів і зміни системних параметрів.

Основна відмінність XDR від традиційного EDR полягає в інтеграції даних не лише з кінцевих точок, але також з мережевих сенсорів, поштових шлюзів і хмарних середовищ, що забезпечує цілісну видимість загроз у всякій інфраструктурі(рис.2.1.)[4].

Таблиця 2.2

Порівняльна характеристика технологій EDR та XDR

Характеристика	EDR	XDR
Фокус	Кінцеві точки	Широка інфраструктура
Джерело даних	Логи кінцевих точок, події безпеки	Логи кінцевих точок, логи хмарного середовища, данні SIEM
Виявлення загроз	Локальні атаки, шкідливе ПЗ	Складні атаки, ланцюги атак, загрози нульового дня
Реагування	Ізоляція пристроїв, видалення шкідливого ПЗ	Автоматизовані дії, оркестрація реагування

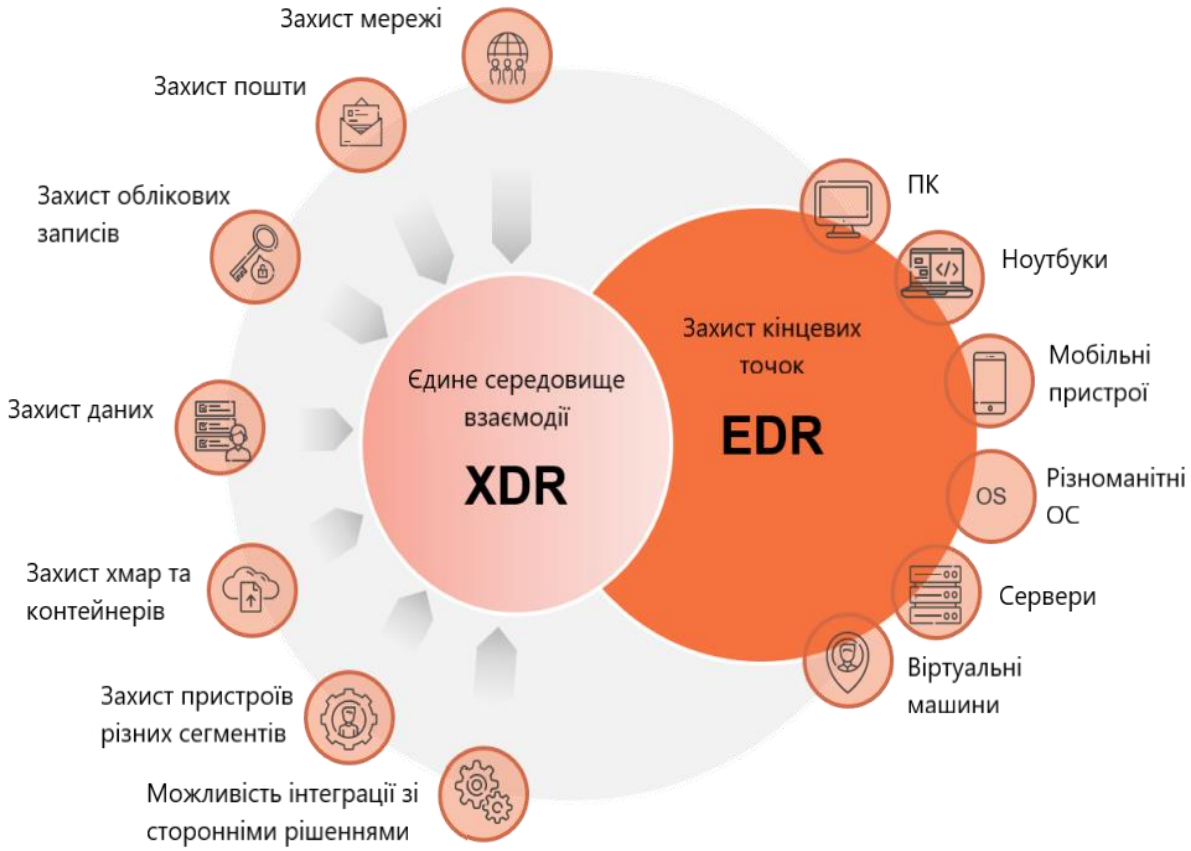

Рис. 2.1 Ключові можливості EDR/XDR

Ключові можливості EDR/XDR:

- Безперервний моніторинг активності процесів – реєстрація кожного запуску, створення файлів, змін у реєстрі та мережевих з’єднаннях.

- Виявлення аномалій – виявлення нетипової поведінки (таких як виконання PowerShell-скриптів без підпису).
- Автоматичне реагування – ізоляція пристрою, завершення роботи процесу або видалення шкідливого файлу.
- Інтеграція з SOC-процесами – пересилання сповіщень в SIEM/SOAR для подальшої автоматизації реагування.

Приклади рішень EDR/XDR:

- CrowdStrike Falcon – забезпечує можливості віддаленого ізолювання пристроїв, проведення аналізу з форензики та інтеграції з Cortex XSOAR.
- Microsoft Defender for Endpoint – об’єднує телеметрію з Windows, macOS, Android і Linux, використовуючи моделі машинного навчання для виявлення протиправних атак.
- SentinelOne Singularity XDR – використовує поведінкові моделі для автономного реагування без втручання оператора.

EDR діє як "очі" SOC на рівні кінцевих пристроїв, надаючи детальний контекст для розслідувань, що сприяє зменшенню середнього часу виявлення (MTTD) і часу реагування (MTTR)[17].

2.2.3. SOAR-платформи (Оркестрація, Автоматизація та Реакція на Загрози)

SOAR виступає основою для автоматизації процесів SOC. Його метою є зменшення навантаження на аналітиків через уніфікацію, оркестрацію й автоматизацію реакцій на інциденти. Основні елементи SOAR(табл 2.3)

Таблиця 2.3

Основні елементи SOAR

Термін	**Визначення та роль**
Оркестрація	Планування, інтеграція, співпраця та координація діяльності інструментів і експертів безпеки з метою оптимізації процесів та забезпечення автоматизації необхідних дій у відповідь на інциденти безпеки.

Продовження табл 2.3

Термін	Визначення та роль
Автоматизація	Використання інформаційних технологій для заміни ручних процесів під час реагування на кіберінциденти та управління подіями безпеки. Автоматизація реалізується за допомогою плейбуків.
Тріаж інцидентів	Класифікація подій за критичністю, типом та контекстом
Плейбуки та Ранбуки	Плейбук — це лінійний контрольний список кроків і дій (робочих процесів), необхідних для успішного реагування на конкретні типи інцидентів і загроз. Ранбук (runbook) складається з низки умовних кроків для автоматичного виконання дій, таких як збагачення індикаторів, стримування загрози та надсилання сповіщень[4].

Приклади платформ які можна знайти на ринку:

1. Cortex XSOAR (Palo Alto Networks) – підтримує створення складних сценаріїв реагування, а також інтеграцію із понад 700 API, включаючи джерела Threat Intelligence.
2. IBM Resilient – проводить аналіз минулих інцидентів для прогнозування ризиків і вибору найкращого способу реагування.
3. DFLabs IncMan SOAR – впроваджує технології supervised active intelligence для адаптивного автоматизованого реагування.
4. TheHive Project – з відкритим кодом, широко використовується для колективного управління інцидентами та співпраці з MISP.

Використання SOAR дозволяє досягти автоматизації до 70% стандартних завдань SOC, суттєво скорочуючи час реагування на інциденти.

2.2.4. Інтеграція Threat Intelligence (TI)

Threat Intelligence (TI) – це структурована інформація, що охоплює загрози, індикатори компрометації (IoC), а також тактики та техніки зловмисників (TTP), яка служить для підвищення обізнаності SOC і поліпшення точності виявлення. TI є каталізатором для трансформації сирих логів у дієву

інформацію, що дозволяє SOC перейти від реактивного до проактивного управління безпекою[1]. Основні напрямки застосування TI:

- Збагачення інцидентів – інформація про загрози використовується для доповнення подій, зафіксованих в SIEM або SOAR, додатковим контекстом. Це включає дані про відомі шкідливі IP-адреси, домени, URL, хеші файлів та вразливості (CVE). Таке збагачення сприяє швидшій оцінці реальної загрози, допомагає визначити її походження і пріоритет реагування, а також зменшує кількість хибних спрацювань, підтверджуючи або спростовуючи підозрілі індикатори.
- Проактивна оборона – дані про загрози використовуються для вивчення тактик, технік і процедур супротивника на основі фреймворка MITRE ATT&CK. Це дозволяє прогнозувати можливі вектори атак з урахуванням особливостей інфраструктури організації. Внаслідок цього SOC може заздалегідь розробляти і впроваджувати відповідні сценарії виявлення, посилювати контроль у найуразливіших зонах і підвищувати загальний рівень готовності до цільових атак.
- Автоматична класифікація та аналіз – використання методів обробки природної мови та машинного навчання дозволяє автоматично аналізувати великі обсяги неструктурованої інформації з відкритих джерел, таких як технічні звіти, публікації дослідників та повідомлення у спеціалізованих спільнотах. В результаті автоматично виділяються індикатори компрометації з текстових даних, що прискорює їх інтеграцію в процеси виявлення та реагування.
- Обмін розвідданими – інтеграція з міжнародними платформами через стандартизовані протоколи STIX/TAXII дозволяє отримувати актуальні та структуровані дані про загрози, а також ділитися власними спостереженнями. Такий обмін сприяє підвищенню загальної кіберстійкості, забезпечує швидше реагування на масові кампанії атак та дозволяє SOC діяти в контексті глобального ландшафту загроз[4].

Приклади джерел Threat Intelligence:

- MISP (Malware Information Sharing Platform) – забезпечує колективний обмін CTI та інтеграцію з SIEM/SOAR.
- VirusTotal Intelligence – надає API для перевірки хешів, доменів і IP-адрес на наявність у базах шкідливих об’єктів.
- AbuseIPDB, AlienVault OTX, Anomali ThreatStream – комерційні та відкриті TI-сервіси.
- NVD, CVE, CISA KEV Catalog – офіційні бази даних вразливостей, які інтегруються для оцінки ризиків і пріоритезації оновлень.

Якість TI оцінюється за принципами A.R.T. (Actionable, Relevant, Timely) – вона має бути практично застосовною, актуальною та своєчасною. Високий рівень інтеграції TI з SIEM і SOAR дозволяє розробляти динамічні плейбуки, які автоматично оновлюють правила кореляції та сценарії реагування при з’явленні нових загроз[17].

Загалом всі вищезгадані компоненти SOC взаємодіють між собою наступним чином:

- Інструменти SOC формують взаємопов’язану архітектуру:
- SIEM збирає та корелює події.
- EDR/XDR створює телеметричні дані з кінцевих точок.
- SOAR автоматизує реакцію, використовуючи дані з SIEM і TI.
- Threat Intelligence надає контекст і проактивну аналітику.

У комбінації ці елементи утворюють адаптивну систему, здатну до самонавчання та оборони, орієнтованої на загрози, що дозволяє організації переходити від реактивного до проактивного кіберзахисту[3].

2.3. **Аналітика та автоматизація SOC**

Функціонування Центру операцій безпеки (SOC) ефективно залежить не тільки від якості його технологічних складників, але також від можливості

аналітичної системи швидко аналізувати події, виявляти шаблони і автоматизувати реакцію на кіберінциденти. Сучасні SOC інтегрують аналітичні алгоритми, машинне навчання, поведінковий аналіз і автоматизовані сценарії реагування, утворюючи складну систему для виявлення, аналізу та нейтралізації загроз у режимі реального часу.

2.3.1. Методи кореляції подій та поведінковий аналіз

Кореляція подій є одним з основних механізмів SOC, що дозволяє поєднати різнобічні логи, отримані з різних систем, у відомі контекстуальні інциденти. Це дає змогу SOC зменшити тисячі несуттєвих сповіщень до декількох актуальних подій безпеки.

Основні цілі та значення кореляції:

- Зниження інформаційного шуму шляхом виділення лише важливих подій.
- Виявлення складних атак, що складаються з кількох етапів (наприклад, розвідка, компрометація, підвищення привілеїв, ексфільтрація).
- Створення причинно-наслідкових зв'язків дій зловмисника в просторі та часі.

Кореляційні методи представленні наступними видами:

- Структурна кореляція – аналіз зв’язків між подіями, виходячи з їхнього походження (IP-адреса, користувач, процес).
- Функціональна кореляція – визначення зв’язків між подіями, що мають спільну мету або результат, навіть якщо технічно вони не пов’язані.
- Поведінкова кореляція – фіксація відхилень у звичайній поведінці об'єктів (користувачів, систем, процесів)[5].

Роль аналітика у процесі кореляції – незважаючи на автоматизацію, людський елемент залишається ключовим. Досвідчений аналітик розробляє власні правила кореляції – індивідуальні сценарії для виявлення інцидентів, які відповідають певній інфраструктурі. Ці правила часто показують більшу

точність, аніж генералізовані шаблони SIEM-систем, та допомагають зменшити кількість хибно позитивних результатів.

Поведінковий аналіз та аналіз причин – поведінковий аналіз зосереджений на виявленні аномалій, які виходять за рамки нормальної діяльності системи або користувачів. Його мета – не тільки зафіксувати факт порушення, але й зрозуміти причини його виникнення.

Прикладом системи поведінкового аналізу є система NoDoze - інноваційний інструмент для зменшення втоми від сповіщень через створення графа причинно-наслідкових зв’язків між подіями. Алгоритм аналізує історію співпраці між процесами, файлами, сокетами та іншими елементами системи, створюючи чітку картину подій[7].

Основні переваги причинно-наслідкового аналізу:

- Збільшення точності розслідувань шляхом надання контексту інциденту.
- Можливість автоматичного визначення джерела загрози.
- Скорочення часу реагування через фокусування виключно на актуальних ланцюгах подій.

Застосування мережевих дифузійних алгоритмів та поведінкового розділення виконання дає змогу зменшити розмір графа залежностей у 100 разів у порівнянні з традиційними методами, послаблюючи навантаження на аналітиків SOC[11].

2.3.2. Інтеграція машинного навчання у SOC

Машинне навчання та штучний інтелект утворюють інтелектуальний шар SOC, який покращує точність і швидкість аналітичних процесів. Використання машинного навчання дозволяє системам вивчати історичні дані і автоматично виявляти шаблони атак, мінімізуючи втручання людини.

Основні напрямки, в яких застосовується машинне навчання у SOC:

1. Класифікація та пріоритезація інцидентів – алгоритми машинного навчання автоматично оцінюють серйозність інциденту, спираючись на контекст, історичні шаблони та наслідки. Наприклад, IBM Resilient використовує історичні дані для прогнозування важливості та часу вирішення інцидентів.
2. Виявлення аномалій – машинне навчання моделює "нормальну поведінку" системи і виявляє відхилення від неї. Наприклад, ServiceNow впроваджує автоматичне визначення аномалій у показниках продуктивності, використовуючи методи нелінійного регресійного аналізу.
3. Зменшення хибних спрацьовувань – на основі минулих рішень аналітиків алгоритми машинного навчання навчаються ідентифікувати події, які з великою ймовірністю не представляють загрозу, і автоматично їх відфільтровують. З часом коли SOC стає зрілим це дуже допомагає зменшити навантаження на аналітиків, залишаючи лише корисні спрацювання.
4. Контекстуальний аналіз ıграфа походження даних – системи, подібні до NoDoze, розраховують аномальний бал для кожної події в графі походження даних та історичному контексті мережевої активності підприємства. Це дозволяє автоматично виявляти найбільш підозрілі ланцюги дій.

Пояснювальна штучна інтелектуальна система (X-IDS) та вимоги до прозорості систем – проблема "чорної скриньки" у машинному навчанні полягає в тому, що система часто не здатна пояснити причини своїх рішень. Це є критичним для центру операцій з безпеки (SOC), оскільки аналітик повинен усвідомлювати логіку системи, щоб ухвалювати подальші рішення. Це є одним з факторів які гальмують процес провадження машинного навчання в архітектури SOC по всьому світу[4].

2.3.3. Модель REACT для штучного інтелекту та машинного навчання в SOC

Модель REACT – це система вимог, розроблена для підвищення корисності та практичної значущості систем безпеки, особливо тих, що

використовують технології штучного інтелекту (ШІ) та машинного навчання, у центрах операцій безпеки.

Ця модель була запропонована у відповідь на висновки дослідження про високу кількість і низьку якість сповіщень безпеки, які часто є недієвими. Мета впровадження вимог REACT полягає в тому, щоб допомогти аналітикам.

Вимоги, що складають модель REACT, такі: Reliable (Надійний), Explainable (Пояснюваний), Analytical (Аналітичний), Contextual (Контекстуальний), Transferable (Адаптивний/Передаваний):

- Надійність – система повинна забезпечувати стійкість результатів незалежно від вхідних даних. Вимога надійності виникла через те, що традиційні сповіщення часто є ненадійними (наприклад, через нечітко написані сигнатури), а також через залежність від ознак, які швидко змінюються (наприклад, доменні імена шкідливого програмного забезпечення). У контексті ШІ/МН-систем, надійність досягається шляхом оптимізації та зворотного зв'язку[1].
- Пояснюваність – кожне рішення має бути обґрунтованим і зрозумілим для людини. Вимога пояснюваності виникає через те, що комерційні інструменти безпеки часто є «чорними ящиками», які генерують тривоги без зрозумілого обґрунтування, що знижує довіру аналітиків та вимагає ручного дослідження сирих даних.
- Аналітичність – модель повинна підтримувати багаторівневий аналіз. Ця вимога підкреслює критичну роль когнітивних здібностей людини та таємного знання (досвіду) у процесі прийняття рішень, оскільки аналітики використовують свій досвід для формулювання гіпотез та розслідування загроз.
- Контекстуальність – врахування робочого середовища, графів знань, розкладу і бізнес-процесів. Вимога контекстуальності відображає необхідність збагачення повідомлень інформацією про мережі, системи,

бізнес-процеси та активи, оскільки брак контексту є однією з основних обмежень, що ускладнює фільтрацію хибних спрацювань.

- Передаваність – здатність адаптуватися до нових умов завдяки навчанням переносу. Ця вимога фокусується на адаптивності систем ШІ/МН до унікального середовища кожної організації, оскільки жоден інструмент не може бути «однаковим для всіх». Мережі та екосистеми швидко змінюються, і початкові дані можуть стати застарілими.

Такі системи називають X-IDS (пояснювальні системи виявлення вторгнень). Вони об'єднують аналітичні моделі та контекстуальні знання, що дозволяє пояснити кожне виявлення або рішення на основі логічних міркувань[1,4].

2.3.4. Автоматизовані сценарії реагування

Плейбуки і ранбуки є основними інструментами для автоматизації в SOC. Вони містять опис дій, які повинні бути виконані під час реагування на певний вид загрози.

Існує 2 основних видів псценаріїв реагування:

- Плейбук – це набір стандартних лінійних покрокових інструкцій, що можуть виконуватися автоматично через системи SOAR.Playbook створюється за процедурою поступового узгодження та перевірки(рис.2.2).
- Ранбук – це сценарій із умовними розгалуженнями, що змінює поведінку в залежності від ситуації. Вони використовується для позначення послідовності умовних кроків, які виконуються автоматично для забезпечення таких дій, як збагачення індикаторів, стримування загрози та надсилання сповіщень.

Кожен плуйбук поділяється на такі типові етапи :

Першим кроком є активація сповіщення, яке запускається моніторинговими системами, зокрема SIEM або EDR. Подія створюється на основі дії правила кореляції, виявлення поведінки або механізму підпису. На даному етапі фіксується основна інформація про інцидент, включаючи джерело події, час її виникнення, залучені активи та попередній рівень важливості.

Другий етап передбачає доповнення індикаторів компрометації для отримання додаткового контексту. Автоматизовані запити надсилаються до зовнішніх або внутрішніх джерел інформації про загрози, таких як платформи, які аналізують репутацію IP-адрес, доменів, хеш файлів або вразливостей. Результати цього збагачення допомагають підтвердити або спростувати злочинний характер події, а також уточнити її походження та можливий вплив.

Третій етап включає автоматичне стримування загрози. Залежно від типу інциденту та встановленої політики реагування, SOAR може ініціювати блокування IP-адреси на мережевому периметрі, ізоляцію скомпрометованої кінцевої точки, відключення облікового запису або обмеження доступу до ресурсів. Автоматизація цього етапу є критично важливою для скорочення часу, протягом якого зловмисник залишався в інфраструктурі.

Четвертий етап полягає в сповіщенні відповідних осіб про інцидент та вжиті заходи. Повідомлення надсилаються через корпоративні канали зв’язку, такі як системи миттєвих повідомлень або електронна пошта, і містять короткий опис події, статус реагування та рекомендації щодо подальших дій. Це забезпечує прозорість процесу та своєчасне залучення зацікавлених сторін.

Останнім етапом є завершення інциденту в системі управління випадками. На цьому етапі фіксуються результати розслідування, вжиті заходи, ухвалені рішення та кінцевий статус інциденту. Накопичена інформація використовується для подальшого аналізу, покращення якості виявлення та вдосконалення сценаріїв у рамках безперервного процесу розвитку SOC[14].

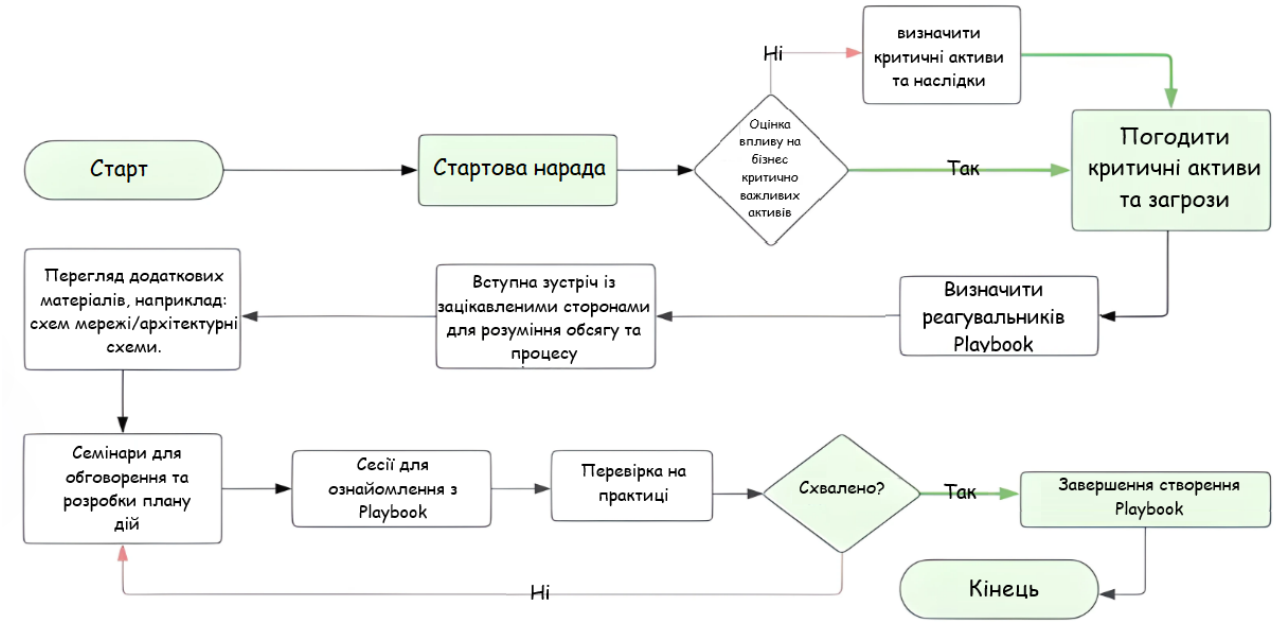

Рис.2.2 Етапи створення Playbook

2.3.5. MITRE ATT&CK як основа автоматизації:

Багато платформ SOAR, таких як D3 Security та Cortex XSOAR, використовують фреймворк MITRE ATT&CK для розробки плейбуків "Kill Chain", що відповідають тактикам і технікам атак. Це дозволяє стандартизувати процес реагування, роблячи його прозорим і відтворюваним.

Переваги застосування автоматизації в SOC:

- Суттєве скорочення середнього часу реагування на інциденти, відомого як MTTR. Автоматизоване виконання сценаріїв, збагачення даних подій і здійснення первинних заходів щодо стримування загроз дозволяє обробляти критичні інциденти протягом хвилин замість годин. Це безпосередньо скорочує тривалість присутності зловмисника в системі та обмежує можливості потенційних негативних наслідків атаки.
- Підвищення узгодженості та стандартизованості дій аналітиків. Автоматизовані сценарії реагування забезпечують послідовне виконання встановлених кроків, що відповідають внутрішнім політикам і процедурам, незалежно від досвіду конкретного співробітника або робочого навантаження в SOC. Це підвищує повторюваність результатів,

спрощує процеси аудиту і підвищує загальний рівень зрілості моделі операційної безпеки.

- Зменшення навантаження на працівників SOC та зниження ймовірності виникнення людських помилок. Автоматизація рутинних і повторюваних завдань, таких як первинна оцінка, збагачення індикаторів або створення інцидентів, дозволяє аналітикам зосередитись на більш складних справах, включаючи детальний аналіз і виявлення загроз. Це не тільки покращує якість реагування, але й знижує ризик прийняття помилкових рішень, пов'язаних з втомою чи перевантаженням працівників[5].

В цілому, автоматизація змінює SOC з переважно реактивної структури на ефективний, масштабований і надійний центр управління кіберінцидентами, що здатний швидко адаптуватися до змін у середовищі загроз.

У зрілому SOC найефективнішою є модель Quadrant 2 SOC Automation Matrix, що поєднує високий рівень кваліфікації аналітиків і великий ступінь автоматизації процесів. Цей баланс дозволяє організації досягати максимальної ефективності при збереженні гнучкості у реагуванні[15].

2.4. Захищеність і стійкість SOC

2.4.1. Захищеність та стійкість Центру управління безпекою

Захищеність та стійкість Центру управління безпекою являють собою критично важливі елементи архітектури інформаційної безпеки в організації. SOC служить центральним елементом для моніторингу, кореляції подій, виявлення інцидентів та реагування, формуючи останню лінію оборони. Будь-яке порушення функціонування SOC призводить до ризику втрати контролю над подіями безпеки, що може фактично позбавити організацію можливості виявити або зупинити кібератаку на ранніх стадіях. Саме тому концепція захищеності SOC включає не лише захист його елементів, але й забезпечення

операційної безперервності, надійності інфраструктури, цілісності даних та кадрової стійкості аналітичної команди[6].

Механізми резервування та ізоляції сегментів SOC:

1. Резервування та надлишковість – архітектура SOC повинна бути спроектована відповідно до принципів fault tolerance і high availability (HA), які гарантують безперервність моніторингу навіть у разі виходу з ладу основних компонентів. Резервні механізми включають:
   - Системи резервного збору та зберігання логів. Дані журналів є ключовим джерелом для аналітики, тому відмова компонентів збору (collectors, agents) чи бази даних SIEM не повинна призводити до втрати історії подій. Для цього застосовується реплікація баз даних (наприклад, Elasticsearch Clustering) і cold storage, де події зберігаються в зашифрованому вигляді на відокремлених носіях.
   - Надлишкова архітектура. Вона передбачає розподіл навантаження між кількома вузлами SIEM/SOAR з автоматичним переключенням (failover) у випадку відмови одного з них. Наприклад, реалізація активної-активної або активної-пасивної кластеризації для компонентів аналізу, а також балансування навантаження між collector-серверами дозволяє зменшити час простою.
   - Резервування аналітичних середовищ. У сучасних SOC використовується концепція "sandbox mirroring" – дублювання середовищ для аналізу шкідливих зразків, щоб у разі знищення однієї лабораторії інша зберігала повний набір артефактів для подальшого дослідження.
   - Тестування відмовостійкості. Однією з практик зрілих SOC є проведення симуляцій відмов (chaos testing) – навмисне відключення компонентів для перевірки реакції системи та персоналу[8].
2. Розподілена архітектура та ізоляція – традиційна централізована модель SOC (SOCBox) схильна до ризику утворення єдиної точки відмови (Single Point

of Failure). Для виправлення цього недоліку сучасні методи передбачають переходи до розподілених SOC (DSOC) або мережевих SOC-гридів (Grid SOC, GSOC), що забезпечують:

- Географічну ізоляцію сегментів SOC. Кожен вузол обробляє події конкретного регіону або підрозділу компанії, що знижує ймовірність значного збою.
- Сегментацію за рівнем довіри. Для зменшення ризику компрометації окремих компонентів SOC застосовується розділення на ізольовані домени – аналітичний, адміністративний і зберігання даних, між якими діє принцип мінімальної взаємодії.
- Використання Zero Trust Network Access (ZTNA). SOC повинен бути відокремлений від корпоративної мережі клієнта, навіть якщо відбувається моніторинг внутрішніх систем. Доступ до SOC надається тільки через контрольовані шлюзи з багатофакторною автентифікацією[9].

2.4.2. Контроль доступу та управління привілеями

Контроль доступу є одним із найбільш важливих аспектів забезпечення внутрішньої безпеки SOC. Оскільки SOC працює з найбільш чутливими даними, такими як журнали автентифікації, телеметрія EDR, мережеві діаграми, компрометація облікових записів аналітиків може спричинити катастрофічні наслідки.

Доступ до контекстуальних даних. Для правильного оцінювання спрацювань аналітику потрібно отримати доступ до контексту: топології мережі, основних ліній поведінки користувачів, переліку критично важливих активів. Нестача контексту знижує якість аналітики та подовжує час реагування. Водночас надмірний доступ створює ризики витоку, тому важливо забезпечити баланс між "достатнім знанням" і "мінімальним доступом".

Моделі контролю доступу. У функціонуванні SOC використовують комбінації RBAC (контроль доступу на основі ролей) та ABAC (контроль доступу на основі атрибутів). RBAC забезпечує базовий розподіл прав доступу відповідно до ролей (аналітик, старший аналітик, адміністратор), тоді як ABAC дозволяє враховувати додаткові атрибути (тип інциденту, чутливість даних, географічне походження користувача).

Принцип найменших привілеїв. Його реалізація через PAM (управління привілейованим доступом) та IAM-рішення забезпечує, що жоден внутрішній користувач не може виконати операції, що виходять за межі їхніх обов’язків. У поєднанні з моделлю Zero Trust це створює багаторівневу бар'єрну систему, яка ускладнює горизонтальне просування зловмисника після компрометації.

Аудит і моніторинг адміністративних дій. Усі дії, які виконуються користувачами з вищими правами, повинні бути задокументовані та відстежувані незалежно від команди SOC, наприклад, за допомогою правил SIEM/SOAR типу "виявлення дій співробітників"[15].

2.4.3. Стійкість і кібервідновлення SOC

Стійкість SOC полягає не лише у технічній відмовостійкості, але й у здатності оперативно відновлюватися після інцидентів, які є загрозою самому центру. На відміну від простого кіберзахисту, стійкість фокусується на забезпеченні того, щоб основні функції та послуги організації не припинялися, навіть якщо атака виявляється успішною. Для цього використовуються:

- Ізольовані резервні канали зв’язку. У випадках, коли корпоративна мережа стає уразливою або частково недоступною, SOC повинен мати доступ до альтернативних і попередньо протестованих маршрутів для координації дій реагування. До таких рішень відносяться захищені VPN-з'єднання з окремими точками виходу, ізольовані управлінські домени, а також альтернативні канали зв'язку, які не залежать від основної

інфраструктури. Це забезпечує можливість підтримки контролю над процесами реагування та комунікацією між аналітиками й відповідальними структурами в умовах криз.

- Оперативна стійкість персоналу. Вона досягається шляхом постійної підготовки аналітиків через освітні програми, такі як симуляції роботи Blue Team, відпрацювання сценаріїв великих інцидентів і кризового реагування. Крім того, реалізується ротація змін та резервування ключових ролей, що передбачає наявність підготовлених замін для кожної важливої функції. Такий підхід зменшує залежність SOC від окремих фахівців і забезпечує неперервність роботи у випадку перевантаження або відсутності персоналу.
- Захист інструментів SOC. Самі елементи SOC, включаючи SIEM, SOAR, TIP, EDR-консолі, повинні піддаватися постійному моніторингу для виявлення зловживань, несанкціонованих змін у налаштуваннях або спроб несанкціонованого доступу, оскільки вони є критично важливими активами. Це передбачає контроль доступу, аудит змін конфігурацій, виявлення аномальної активності та спроби несанкціонованого втручання. Забезпечення безпеки самих інструментів SOC допомагає уникнути ситуацій, коли зловмисник може приховати свою присутність або впливати на процеси реагування.

У результаті зазначені заходи створюють комплексний підхід до забезпечення стійкості SOC, що дозволяє не тільки боротися із зовнішніми загрозами, але і забезпечує безперервність функцій кіберзахисту в умовах кризових та надзвичайних ситуацій [11].

2.4.4. Підходи до тестування ефективності SOC

Оцінювання ефективності SOC виходить за межі простого підрахунку інцидентів. Зрілі SOC застосовують моделі, що оцінюють продуктивність та зрілість, які включають як кількісні, так і якісні показники.

Метрики ефективності(KPIs) – ключові показники продуктивності SOC охоплюють такі аспекти:

- MTTD (середній час виявлення) – середній період від моменту виникнення інциденту до його виявлення;
- MTTR (середній час реагування) – середній період, необхідний для реакції;
- FP Ratio (коефіцієнт хибних позитивів) – відношення хибних і підтверджених інцидентів;
- Time per Investigation – середній час, витрачений на одну перевірку;
- Quality Index of Incident Reports – показник якості аналітичних звітів, який може визначатися через експертну оцінку або через SOC-AAM (модель оцінки аналітиків SOC)[17].

Недоліком традиційних KPI є те, що вони не відображають контекстуальну складність інцидентів та глибину аналізу. Тому в сучасних підходах акцент робиться на комбінованих моделях: об'єднанні кількісних показників з якісними оцінками (аналіз сценаріїв реагування, точність класифікації інцидентів, повнота кореляційних зв’язків).

Кожен SOC має за собою моделі зрілості. Моделі зрілості дозволяють систематично оцінити еволюційний розвиток SOC. Типова SOC проходить через п’ять фаз:

- Non-Existent: відсутність централізованого моніторингу.
- Initial (Ad-hoc): реактивна обробка подій без стандартизованих процесів.
- Defined: формалізація процедур, початкова автоматизація.
- Managed: інтеграція з бізнес-процесами, застосування SOAR.
- Optimized: високий рівень автоматизації, аналітика на основі штучного інтелекту, проактивна оборона[7].

Однією з інноваційних моделей є SOC Automation Matrix, яка відображає рівень розвитку SOC за двома параметрами – ступенем автоматизації та людським залученням. Найбільш ефективним вважається Quadrant 2 (висока

автоматизація + високе людське залучення), де автоматизовані рутинні процеси синхронізуються з експертним аналізом складних випадків.

Для SOC на ранніх стадіях (низька автоматизація + низьке людське залучення) рекомендується спочатку рухатися вертикально (збільшення людської участі), а потім горизонтально (підвищення автоматизації). Цей підхід допомагає зберегти контроль якості аналітики під час цифрової трансформації SOC.

Захищеність і витривалість центру операцій безпеки (SOC) є не лише результатом технічних властивостей, але також ґрунтуються на системному підході, який інтегрує інфраструктуру, процеси, людей та політики. Резервування, сегментація з ізоляцією, контроль доступу, досконаліть аналітики і управління привілеями складають основу для забезпечення надійної архітектури SOC [22].

Висновки до розділу 2

Технологічна архітектура системи реагування на інциденти безпеки (SOC) формує багатогранну структуру, що поєднує організаційні аспекти, технологічні засоби, операційні заходи та управлінські механізми. Розгляд архітектурних підходів і технологічних рішень показує, що ефективність SOC залежить не лише від окремих інструментів, а й від рівня узгодженості компонентів, які функціонують у єдиному циклі діяльності.

По-перше, рамкова модель PPTGC створює основи для розбудови SOC. Вона доводить, що технології, без ретельно підготовленого персоналу, стандартизованих процедур та керівних механізмів, не здатні забезпечити надійний захист. Саме виважений баланс між процесами, технічними можливостями та управлінською структурою визначає ступінь зрілості SOC.

По-друге, аналіз архітектурних моделей свідчить про те, що сучасні організації переходять від строго централізованих схем до гібридних або

федеративних рішень. Це пов'язано зі зростанням обсягів телеметрії, глобальним розподілом інфраструктури, потребою в безперервності операцій та наростанням вимог до масштабованості. SOC еволюціонує у бік дистрибутивних, стійких платформ, які забезпечують локальні реакції та централізовану аналітику.

По-третє, SIEM виступає важливим аналітичним центром SOC, чия ефективність залежить від здатності обробляти великі обсяги телеметрії, якісного парсингу, кореляції даних та впровадження автоматизованих механізмів штучного інтелекту. Тенденція до переходу до XSIEM вказує на рух до інтегрованих екосистем, де аналітика, автоматизація та поведінкове моделювання поєднуються в єдиній системі.

По-четверте, технології EDR/XDR розширюють можливості SOC, надаючи видимість у середовищах кінцевих точок та хмар. Інтеграція телеметрії з різних сфер дозволяє виявляти ускладнені атаки та формує повний облік інцидентів. Важливою перевагою є здатність цих систем виконувати автономне реагування, що суттєво скорочує час відновлення (MTTR).

По-п’яте, платформи SOAR трансформують SOC з переважно ручної моделі на автоматизований, високоякісний центр. Оркестрація дій, формалізація сценаріїв відповіді, автоматизоване підвищення пріоритету та єдині процеси сприяють зменшенню впливу людського фактора, оптимізації навантаження на аналітиків та забезпеченню передбачуваності реагування.

Системна сукупність технічних компонентів SOC – SIEM, EDR/XDR, SOAR, NDR, UEBA, IDS/IPS – створює багатошарову екосистему, здатну виявляти та локалізувати загрози на різних етапах атаки. Зрілість SOC визначається ступенем інтеграції цих елементів, якістю даних, узгодженістю процесів та рівнем автоматизації.

Узагальнюючи, технологічна архітектура SOC є динамічною та гнучкою системою, що адаптується до збільшення складності кіберзагроз. Сучасні SOC орієнтуються на єдині платформи, що базуються на даних та автоматизації, де

аналітика, інтеграція та оперативна взаємодія між рівнями визначають можливості організації залишатися ефективною в умовах постійного кібертиску.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ВПРОВАДЖЕННЯ SOC У ТИПОВІЙ КОМЕРЦІЙНІЙ ОРГАНІЗАЦІЇ

3.1. Аналіз організації та потреб у SOC

Типова комерційна організація середнього розміру в Україні відповідно до Закону України «Про бухгалтерський облік та фінансову звітність в Україні» оперує в складному цифровому просторі, який об'єднує локальні IT-ресурси та хмарні сервісні рішення. У компанії, що має до 250 співробітників та має балансову вартість активів – до 20 мільйонів євро включно, формується широка інфраструктура, що включає головний офіс і кілька регіональних відділів. Значну частину таких підприємств представляють фірми в сфері послуг, фінансовому секторі, роздрібній торгівлі та логістиці, де бізнес-процеси мають критичну залежність від високої доступності сервісів та цілісності даних[18].

Інформаційні активи включають різноманітні робочі станції, мобільні пристрої та периферійні системи, а також серверну інфраструктуру, на якій працюють корпоративні системи, такі як CRM та ERP рішення. Багато організацій дедалі більше впроваджують хмарні технології для електронної пошти, документообігу та управління користувачами, інтегруючи їх із традиційними локальними ресурсами. Мережева архітектура містить маршрутизатори, комутатори різних класів, міжмережеві екрани, VPN-шлюзи та системи контролю доступу. В результаті формується складна, багатошарова екосистема мережевих та обчислювальних ресурсів, яка потребує постійного моніторингу та оперативної реакції на відхилення.

Сучасний стан інформаційної безпеки зазвичай характеризується наявністю основних засобів захисту, які функціонують автономно: антивірусних програм, систем логування подій операційних систем, стандартних інструментів мережевого обладнання та обмеженого моніторингу трафіку. Водночас організації стикаються з недоліками цього розрізненого підходу – різні джерела подій не з'єднані в єдину аналітичну систему, що

створює «сліпі зони» та затримує відповіді на інциденти. З огляду на зростаючу кількість фішингових атак, розповсюдження шкідливих програм, експлуатацію вразливостей у VPN-технологіях і постійні спроби аутентифікації способом перебору, ці обмеження стають особливо критичними. Інциденти можуть залишатися непоміченими протягом декількох годин або навіть днів, що дозволяє зловмисникам здійснювати атаки, пересуватися в системі або отримувати доступ до ключових бізнес-систем.

Зростання ризиків безпосередньо впливає на діяльність організації: ймовірність порушення доступності сервісів, виникнення інцидентів витоку даних, фінансових втрат і репутаційних збитків зростає. В таких умовах стає очевидною необхідність переходу від реактивних методів до структурованої, безперервної та централізованої моделі кібербезпеки.

Діяльність із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з п’яти функцій кібербезпеки (рис.3.1):

- ідентифікація ризиків;
- кіберзахист;
- виявлення кіберінцидентів;
- реагування;
- відновлення поточного стану кібербезпеки[21].

Компанія формулює чіткі цілі для створення SOC. По-перше, є потреба зменшити час виявлення атак шляхом впровадження цілодобового моніторингу подій, що дозволяє виявляти аномалії на ранніх стадіях. По-друге, важливо централізувати управління інцидентами, щоб усунути фрагментацію різних засобів захисту та забезпечити єдиний процес обробки подій. По-третє, важливим завданням є автоматизація реагування на поширені види атак – фішинг, спроби несанкціонованих доступів і поширення шкідливого програмного забезпечення, що знижує вплив людського фактора та

пришвидшує діяльність аналітиків. Нарешті, SOC дозволяє підвищити загальний рівень кібербезпеки компанії та забезпечити відповідність регуляторним нормам і вимогам галузі.

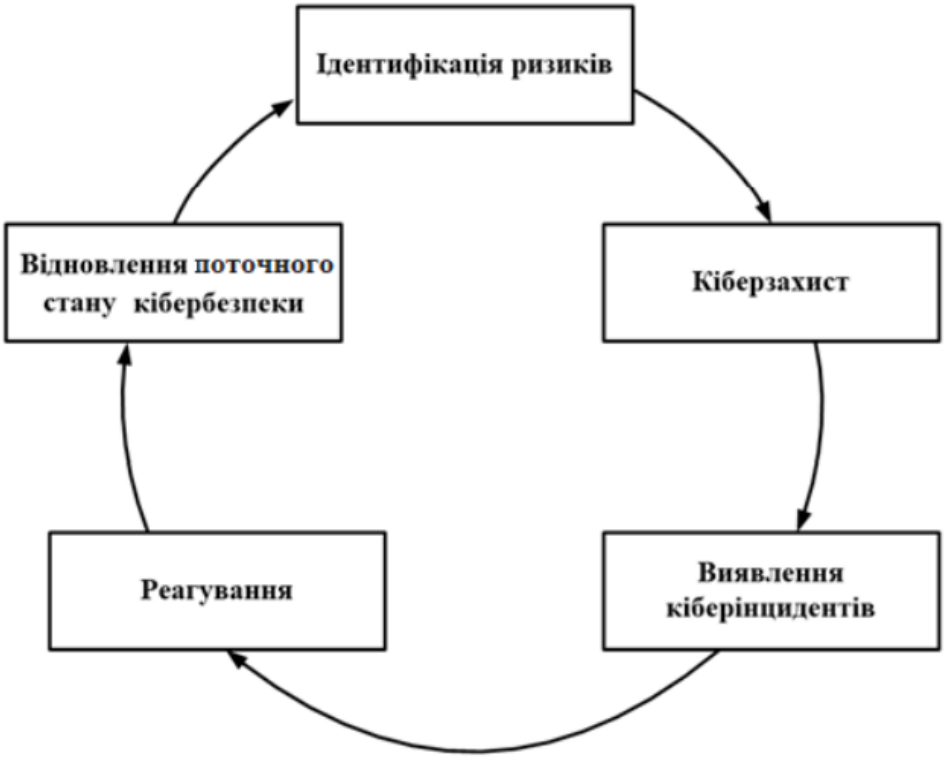

Рис 3.1. Цикл управління кібербезпекою

Таким чином, реалізація SOC є не лише технічним кроком, а стратегічним рішенням, яке створює основу для сталого, передбачуваного та адаптивного захисту інформаційного середовища. SOC стає ключовим елементом у посиленні операційної стійкості, дозволяючи організації ефективно протистояти сучасним загрозам і зменшувати їх негативний вплив на бізнес-процеси.

3.2. Оцінка поточної зрілості кібербезпеки

Оцінка рівня зрілості кіберзахисту є необхідним кроком перед впровадженням Центра оперативного управління безпекою, оскільки дозволяє отримати об'єктивне уявлення про актуальний стан захисту в організації,

усвідомити існуючі слабкі місця та розробити пріоритети для подальшого розвитку. У багатьох українських компаніях рівень зрілості зазвичай коливається між початковим і базовим етапами, коли різні елементи безпеки наявні, але не об'єднані в єдину структуру, і їх ефективність суттєво обмежена відсутністю централізованого управління та належного контролю.

Перший аспект, який розглядається під час оцінювання, стосується ведення журналів подій та логів в критичних інформаційних системах. У багатьох компаніях журнали дій насправді збираються, однак цей процес часто не має єдиного регламенту: деякі системи ведуть журнали в обмеженому режимі, інші – зберігають логи недостатньо тривалий час, а в деяких випадках відсутнє захист від видалення або зміни записів. Логи не аналізуються за допомогою автоматизованих інструментів, що призводить до накопичення інформації без практичної користі. З такою ситуацією швидке виявлення підозрілих дій стає неможливим, що значно ускладнює розслідування інцидентів, які могли б бути визначені на ранній стадії.

Другим ключовим елементом є управління вразливостями. Аудит більшості організацій показує, що регулярні перевірки вразливостей не проводяться або виконуються нерегулярно, без формалізованої процедури виявлення та усунення виявлених недоліків. Це призводить до накопичення серйозних ризиків для безпеки, зокрема на серверах, робочих станціях, мережевих пристроях і в хмарних сервісах. У багатьох компаніях патч-менеджмент виконується вручну, без центрального контролю і без чітко визначених термінів оновлення. Як результат, системи можуть залишатись уразливими протягом тривалого періоду після виходу публічних уксплойтів.

Третя область оцінки пов'язана з управлінням доступом та привілеями. Загальними проблемами є використання локальних акаунтів адміністратора, недостатнє використання багатофакторної автентифікації для критичних сервісів, надмірні привілеї на робочих станціях і відсутність контролю за змінами в правах доступу. Часто відсутня централізована система управління ідентифікацією, а політики доступу не відповідають принципу мінімально

необхідних прав. Слабий контроль за обліковими записами створює загрозу для несанкціонованих дій, зловживань чи компрометації акаунтів під час фішингових атак.

Також в оцінці враховується готовність організації до реагування на інциденти. Більшість компаній не мають формальної процедури реагування на кіберінциденти, або така процедура існує лише формально. Під час атаки співробітники, як правило, діють інтуїтивно, без структурованого підходу до ізоляції загрози, комунікацій, документування та відновлення. Відсутність готових сценаріїв і чітких ролей призводить до затримок та неефективних дій, що ускладнює зменшення шкоди.

Окремої уваги потребує захист мережевої інфраструктури, який включає в себе сегментацію мережі, захист зони DMZ, політики фаєрволів, використання рішень IDS/IPS та контроль трафіку. У багатьох організаціях сегментація реалізована недостатньо або відсутня зовсім, що дозволяє потенційному зловмиснику безперешкодно пересуватися мережею після початкового проникнення. IDS/IPS, зазвичай, або відсутні, або функціонують у режимі моніторингу без можливостей активної блокади.

Завдяки ретельному аналізу формується загальна оцінка рівня зрілості, яка вказує на те, що організація потребує не лише технічних вкладень, але й перегляду своїх процесів, політик та загального підходу до кібербезпеки. Ці обставини підкреслюють необхідність створення SOC як структурного елемента, що здатен інтегрувати різноманітні механізми в єдину керовану систему.

3.3. Проєктування концепції SOC

Основною метою створення SOC є встановлення контрольованого, стандартизованого та відтворюваного процесу моніторингу, виявлення, аналізу і реагування на кіберзагрози. SOC надає безперервний захист критичних сервісів організації, таких як Active Directory, корпоративна електронна пошта,

ERP/CRM, VPN-доступ, робочі станції і хмарні платформи. У компанії, що налічує , близько 250 співробітників, SOC функціонує як механізм для зменшення ризику фінансових втрат, компрометації конфіденційних даних, несанкціонованого доступу до інфраструктури та збоїв у діяльності сервісів, які підтримують бізнес-процеси.

Для організацій такого масштабу найефективнішою є гібридна модель SOC, яка інтегрує внутрішні операційні можливості з зовнішньою експертизою. Внутрішня структура складається з аналітиків рівня L1/L2, необхідних платформ для спостереження та розроблених playbooks, разом із архітектурними компонентами SIEM, SOAR та інструментами контролю подій. Зовнішні постачальники додатково зміцнюють SOC, пропонуючи послуги глибокої загрози розвідки, спеціалізованого аналізу з форензики, реверс-інженерії шкідливих програм і забезпечуючи цілодобове покриття. Поєднання 12×7-in-house-підтримки та цілодобової автоматизації або MDR/SOC-as-a-service дозволяє досягти оптимального балансу між якістю, вартістю та часом реагування.

Для забезпечення сталого функціонування потрібна принаймні мінімальна штатна структура що включає в себе SOC Manager, двох або трьох аналітиків рівня L1, одного L2/Incident Responder та одного Security Engineer, що відповідає за підтримку SIEM/SOAR та забезпечення якості механізмів виявлення. Додатково, залучається команда на контрактній основі для надання послуг з Threat Intelligence та DFIR. Така конструкція забезпечує чітке розподілення обов’язків: аналітики L1 здійснюють моніторинг, первинний тріаж та реєстрацію інцидентів; аналітики L2 досліджують складніші загрози, виконують відстеження загроз та ведуть технічні дослідження; Security Engineer відповідає за створення правил кореляції, оптимізацію сповіщень і інтеграцію джерел журналів. Зовнішній DFIR використовується як економічний варіант доступу до глибокої експертизи, яку не доцільно утримувати в штаті постійно.

3.3.1. Технологічна архітектура SOC

Архітектура SOC повинна забезпечувати збір, нормалізацію та кореляцію даних з основних компонентів корпоративної інфраструктури. Мінімальний набір включає журнали Active Directory, які фіксують події автентифікації, зміни в групових політиках і дії адміністраторів; журнали EDR/XDR, встановлених на всіх робочих станціях і серверах, які реєструють поведінку процесів, можливі ознаки шкідливої активності і спроби межового переміщення. Дані систем електронної пошти, журнали firewall/NGFW, що містять записи про VPN-з'єднання, події IDS/IPS і аналіз трафіку, журнали проксі чи веб фільтрів, записи WAF для публічних сервісів; журнали з хмарних платформ, журнали критично важливих додатків, таких як ERP та CRM.

Для забезпечення кореляції подій, аналітики та сповіщення доцільно використовувати SIEM системи, які виступають як центральний компонент SOC. Для середньої компанії доцільним є використання SIEM на основі ELK/OpenSearch, оскільки це забезпечує високий рівень контролю, гнучке масштабування та доступну вартість ліцензування. Система повинна підтримувати збагачення даними з зовнішніх та внутрішніх джерел, надавати можливості для створення аналітичних дашбордів, формувати правила кореляції для виявлення підозрілих поведінкових моделей і надавати сповіщення через SOAR або інші комунікаційні канали.

Для виконання функцій формування структурованих і повторюваних процесів реагування використовуються SOAR-системи. Централізоване управління дозволяє автоматично блокувати IP-адреси на прикордонних пристроях, ізолювати робочі станції або сервери у разі підтвердженої шкідливої активності, створювати та закривати інциденти відповідно до плану реагування на інциденти з кібербезпеки, а також обробляти фішингові повідомлення. Найкращим варіантом у співвідношенні ціна якість буде вибір комбінації TheHive + Cortex.

Для середнього бізнесу найкращими варіантами в захисті кінцевих пристроїв є Microsoft Defender for Endpoint та CrowdStrike Falcon. Обидва цих рішення пропонують функції поведінкового виявлення, автоматичну ізоляцію інфікованих пристроїв, аналіз взаємозв'язків між процесами та раннє виявлення lateral movement під час атаки. Проте з власного досвіду вважаю за доцільне обрати саме CrowdStrike Falcon, адже він за моїми спостереженнями виявляє нові види шкідливого програмного забезпечення швидше та краще за конкурентів на ринку, також присутня можливість докупляти необхідний функціонал не лише за допомогою підвищення рівня ліцензії а й окремими функціями, однією з таких що не входить до базової ліцензії, проте є дуже корисною є функція пісочниці (sandbox) що дозволяє швидко і зручно аналізувати підозрілі файли(рис 3.2).

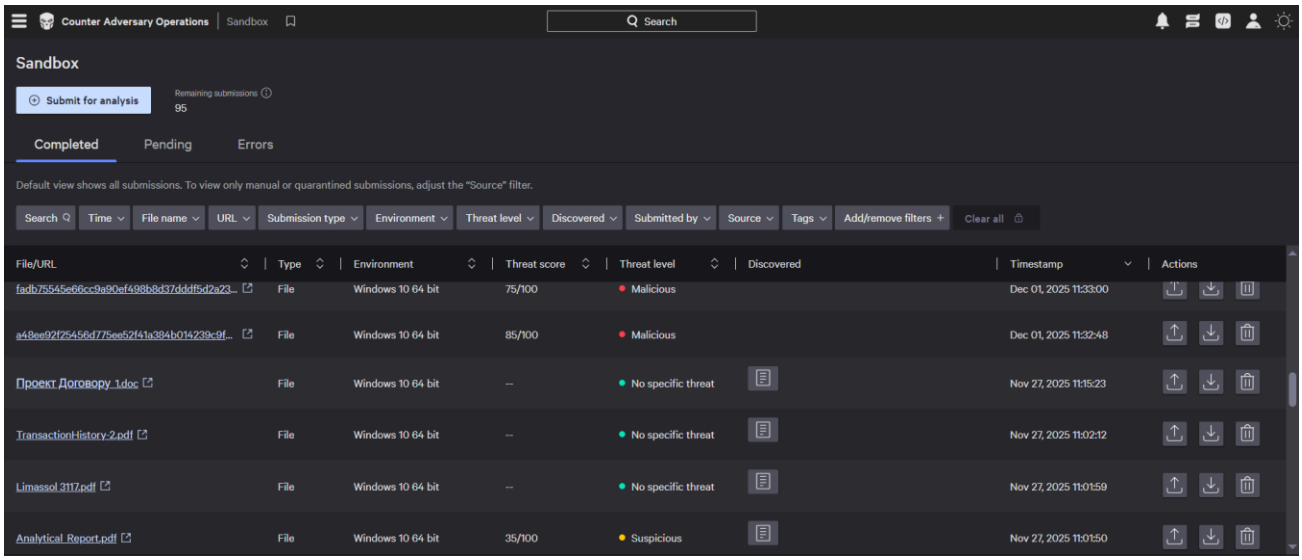

Рис 3.2 Демонстрація роботи функії Sandbox у системи CrowdStrike Falcon

Компоненти NDR створюють мережевий рівень виявлення. Найменша конфігурація передбачає наявність Suricata IDS або IPS-компонентів NGFW для ідентифікації мережевих атак. У додатковому використанні доцільним буде Zeek, який надає глибокий аналіз поведінки мережевих з'єднань та створює насичений контекст для кореляції в SIEM.

Для забезпечення функйцій Threat intelligence застосовують механізми TI які інтегрують дані як з комерційних, так і з відкритих джерел, серед яких

CERT-UA, VirusTotal Premium, HybridAnalysis і OSINT, оброблені інженером безпеки. TI застосовується для поглиблення інформації про інциденти, визначення пріоритетів реагування та підвищення точності виявлення загроз. Слід зазначити, що використання TI є дуже важливим адже дозволяє не лише завчасно запобігти ураженню системи, а й зменшити обсяг власної роботи використовуючи звіти різних DFIR команд які вже можуть бути на цих платформах.

Для забезпечення операційної діяльності SOC використовують план реагування на інциденти, який описує ролі, етапи реагування та основні процедури. Додатково створюються security operation protocols(SOPs) для виявлення, ескалації, блокування активності та комунікацій між SOC і IT-відділами. Каталог сценаріїв використання структурує всі випадки виявлення, а дорожня карта зрілості виявлення визначає пріоритети поліпшення виявлення.

Мінімальний набір сценаріїв охоплює кілька категорій. У сфері автентифікації виявляються brute force, перебір користувачів при відомому паролі (password spray), несанкціоновані зміни в групах адміністраторів та спроби підвищення привілеїв. Категорія Endpoint охоплює виявлення виконання підозрілих бінарних файлів, поведінкові патерни шкідливих програм, створення точок стійкості та руху вбік. Категорія електронної пошти включає шкідливі вкладення, URL-адреси та зловживання відкритою авторизацією. Мережеві сценарії використання зосереджуються на скануванні, C2-комунікаціях та можливій ексфільтрації даних. Хмарна категорія включає сценарії неможливої подорожі, зловживання токенами та ознаки обходу MFA.

Реагування на інциденти безпеки відбувається наступним чином – аналітик L1 отримує сповіщення від SIEM, виконує первинну верифікацію події, розглядає контекст, визначає рівень критичності і, за потреби, передає подію до L2. Аналітик L2 проводить детальне розслідування, визначає первинну причину, формує рекомендації щодо ізоляції, блокування або видалення облікових записів, координує дії з IT-відділами та виконує аналіз після інциденту. Інженер безпеки відповідає за вдосконалення механізмів

виявлення та зменшення кількості хибних позитивних сповіщень, а також за розробку нових сценаріїв. У складніших випадках залучається зовнішня DFIR-команда, яка здійснює детальну форензику і надає технічні висновки для керівництва.

У випадку інфраструктурної схеми то стандартний процес виглядає так: журнали передаються до лог-колекторів, після чого вони надходять у SIEM, який генерує сповіщення. SOAR реалізує автоматизовані дії та координує виконання сценаріїв. На етапі доповнення дані збагачуються TI. Інцидент проходить повний цикл плану реагування на інциденти: розслідування, відокремлення, відновлення та закриття, після чого відбувається вдосконалення правил. Мінімальна інфраструктура передбачає два вузли SIEM, один SOAR, один TheHive/IRP, мережеві NDR-сенсори та EDR на всіх пристроях.

Для успішного впровадження SOC уа стадії підготовки проводиться аудит джерел логів, класифікація активів, формування KPI та KRI. Перша фаза зосереджується на запуску SIEM, інтеграції основних джерел, налаштуванні первинних сценаріїв використання і навчанні аналітиків L1. У фазі розвитку впроваджується SOAR, розширюється набір випадків виявлення, інтегруються хмарні джерела та TI, а також здійснюється полювання на загрози. Фаза зрілості включає розробку виявлень на основі TTP, покриття MITRE ATT&CK та впровадження операційної інформаційної панелі.

Щоб впровадити SOC потрібно мати немаленький бюджет, що формується формується в залежності від конкретного технологічного стека, але зазвичай включає витрати на SIEM (1,5–6 тис. доларів щомісяця), EDR/XDR (10–20 доларів на пристрій), SOAR (від безкоштовних до 50 тис. доларів), NGFW та NDR (20–60 тис. доларів), заробітну плату персоналу (8–20 тис. доларів щомісяця) та зовнішню DFIR/TI-підтримку (1–4 тис. доларів).

Після впровадження SOC організація здобуває можливість виявляти до 90% критично важливих інцидентів на початкових етапах, що суттєво зменшує час, необхідний для реагування з кількох годин до кількох хвилин, встановлює

повний контроль над логами, централізує функції безпеки та формує зрілу, стандартизовану систему реагування.

Висновки до розділу 3

Вивчено актуальний стан кіберзагроз, що впливають на середні українські бізнеси, та виявлено необхідність створення центру операцій безпеки (SOC) як важливої складової захисної структури.

Проаналізовано сучасний рівень безпеки й визначено основні напрямки загроз, які потребують централізації моніторингу та автоматизації відповідей на них.

Обрано оптимальну архітектуру SOC – гібридну модель, яка поєднує локальні ресурси з хмарними технологіями, що забезпечує гнучкість і можливість масштабування.

Обґрунтовано вибір основних технологічних компонентів: SIEM для кореляції подій, SOAR для автоматизації процесів, EDR для моніторингу кінцевих пристроїв.

Встановлено логічну структуру потоків даних, що забезпечує безперервний збір логів, їх стандартизацію і подальший аналіз.

Виділено типові сценарії реагування на інциденти, які дозволяють запровадити стандартизовані та повторювані механізми захисту.

Досліджено етапи впровадження SOC і розроблено поетапну модель, яка охоплює етапи від проведення аудиту до створення цілодобового центру.

Вивчено результати діяльності SOC після реалізації: скорочення середнього часу відгуку (MTTR), зменшення кількості інцидентів, підвищення ефективності витрат.

Окреслено шляхи майбутнього розвитку SOC – перехід до розширених рішень (XDR), впровадження систем штучного інтелекту, підвищення автоматизації та інтеграція з глобальними системами обміну інформації про загрози.

Результати даного дослідження можуть бути використані для подальшого вдосконалення системи кіберзахисту організації, формування стратегії безпеки, планування ресурсів та проектування корпоративної моделі SOC відповідно до актуальних умов українського кіберпростору.

ВИСНОВКИ

Проведено всебічний аналіз та розробка науково обґрунтованої і практично спрямованої моделі архітектури Центру операцій безпеки для комерційного підприємства середнього розміру в Україні. Досягнуті цілі роботи підтверджуються послідовним виконанням усіх визначених завдань і отриманими результатами.

Виконано аналіз теоретичних основ створення SOC, включаючи сучасні методологічні підходи, міжнародні стандарти та законодавчі вимоги в галузі кібербезпеки. Виявлено, що SOC є критично важливим елементом системи кіберзахисту організації, який поєднує технічні, організаційні та процесуальні механізми для забезпечення вчасного виявлення і реагування на кіберінциденти. Проаналізовані підходи підтвердили доцільність застосування моделей управління безпекою, орієнтованих на ризики та процеси.

Здійснено дослідження технологій, компонентів і продуктів, які використовуються в архітектурі SOC. Розглянуто роль SIEM, SOAR, EDR/XDR, NDR, платформі з розвідки загроз та додаткових інструментів, а також їх взаємодію в рамках єдиного циклу моніторингу і реагування. Визначено, що ефективність SOC в значній мірі визначається не лише окремими продуктами, а й рівнем їх інтеграції, якістю кореляції подій і автоматизації процесів. Була розроблена організаційно-операційна модель SOC, що включає розподіл ролей і відповідальностей, опис основних процесів реагування, використання playbooks, а також впровадження метрик ефективності. Запропонована модель враховує реальні кадрові та фінансові обмеження середньої комерційної організації та забезпечує баланс між рівнем контролю, оперативністю реагування та економічною доцільністю.

Головним результатом роботи стала концепція впровадження SOC в типовій українській комерційній організації середнього розміру. Запропоновано поетапний підхід до реалізації SOC – від етапу підготовки до досягнення зрілої операційної моделі. Обґрунтовано доцільність використання гібридної архітектури SOC, що поєднує внутрішні ресурси із можливостями зовнішніх

сервісів, як найкращий варіант для українських умов. Сформульовано практичні рекомендації щодо подальшого розвитку SOC, зокрема в напрямках автоматизації реагування, розширення використання розвідки загроз, підвищення стійкості SOC та переходу до механізмів виявлення загроз, орієнтованих на TTP. Показано, що впровадження автоматизації та проактивних підходів дозволяє значно скоротити час реагування, знизити навантаження на персонал і збільшити загальний рівень кіберстійкості організації.

Наукова новизна отриманих результатів полягає в інтеграції організаційно-процесного, технологічного та продуктового підходів до створення архітектури SOC, а також у розробці концептуальної моделі SOC, що адаптована до умов діяльності середніх комерційних організацій в Україні. Практична цінність роботи полягає в можливості застосування отриманих результатів як методичної основи для проектування, впровадження та розвитку SOC у реальних умовах господарювання.

Таким чином, результати роботи підтверджують доцільність і ефективність запропонованої архітектури SOC і можуть бути використані як у наукових дослідженнях, так і в практичній діяльності фахівців у галузі кібербезпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bushra A. Alahmadi, Louise Axon, and Ivan Martinovic 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms 2022.URL: https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi

2. Enoch Agyepong∗ , Yulia Cherdantseva, Philipp Reinecke, Pete Burnap A systematic method for measuring the performance of a cyber security operations centre analyst 2023. URL: https://www.sciencedirect.com/journal/computers-and-security

3. Wajih Ul Hassan , Shengjian Guo‡ , Ding Li∗ , Zhengzhang Chen∗ , Kangkook Jee∗ , Zhichun Li∗ , Adam Bates NODOZE: Combatting Threat Alert Fatigue with Automated Provenance Triage 2019. URL: https://dx.doi.org/10.14722/ndss.2019.23349

4. Johnson Kinyua and Lawrence Awuah AI/ML in Security Orchestration, Automation and Response: Future Research Directions 2021. URL: https://www.techscience.com/iasc/v28n2/42057

5. Wenjun Xiong, Emeline Legrand, Oscar Åberg, Robert Lagerström Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix 2021. URL: https://doi.org/10.1007/s10270-021-00898-7

6. Chiba, D.; Akiyama, M.; Otsuki, Y.; Hada, H.; Yagi, T.; Fiebig, T.; Van Eeten, M. DomainPrio: Prioritizing Domain Name Investigations to Improve SOC Efficiency. IEEE Access 2022, 10, 34352–34368. Subash Neupane, Jesse Ables, (graduate student member, Ieee), William Anderson, Sudip Mittal, (member, Ieee), Shahram Rahimi , (member, Ieee), Ioana Banicescu, (Life Senior Member, Ieee), and Maria Seale Explainable Intrusion Detection Systems (X-IDS): A Survey of Current Methods, Challenges, and Opportunities 2022.

7. Tilbury, J.; Flowerday, S. Humans and Automation: Augmenting Security Operation Centers. J. Cybersecur. Priv. 2024, 4, 388–409. URL: https://doi.org/10.3390/ jcp4030020

8. Deepesh Shahjee and Nilesh Ware Integrated Network and Security Operation Center: A Systematic Analysis 2022.

9. Robert A. Bridges Letter to Computers & Security Editor & Reviewers 2023. URL:https://www.sciencedirect.com/science/article/pii/S0167404823001116

10. Faris Bugra Kokulu, Ananta Soneji, Tiffany Bao, Yan Shoshitaishvili, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. 2019. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), November 11–15, 2019, London, United Kingdom. ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3319535.3354239

11. Gwanghyun Ahn, Jisoo Jang, Seho Choi, and Dongkyoo Shin, (Member, Ieee) Research on Improving Cyber Resilience by Integrating the Zero Trust Security Model With the MITRE ATT&CK Matrix 2024.

12. Manfred Vielberth, Fabian Böhm, Ines Fichtinger, and Günther Pernul, (Member, Ieee) Security Operations Center: A Systematic Study and Open Challenges 2020.

13. Carson Zimmerman Ten Strategies of a World-Class Cybersecurity Operations Center 2014. URL: https://duikt.edu.ua/ua/lib/1/category/2132/view/1717

14. Ofte, H.J.; Katsikas, S. Understanding Situation Awareness in SOCs, a Systematic Literature Review. Comput. Secur. 2023, 126, 103069

15. https://socradar.io/create-more-effective-soc-with-the-mitre-attck-framework/

16. Joseph Muniz The Modern Security Operations Center 2021.

17. Oleg Dubetcky Як побудувати та запустити центр безпеки (SOC) URL:https://oleg-dubetcky.medium.com/%D1%8F%D0%BA-%D0%BF%D0%BE%D0%B1%D1%83%D0%B4%D1%83%D0%B2%D0%B0%D1%82%D0%B8-%D1%82%D0%B0-%D0%B7%D0%B0%D0%BF%D1%83%D1%81%D1%82%D0%B8%D1%82%D0%B8-%D1%86%D0%B5%D0%BD%D1%82%D1%80-

%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8-soc-504266cefa53

18. Закон України Про бухгалтерський облік та фінансову звітність в Україні (Відомості Верховної Ради України (ВВР), 1999, № 40, ст.365) URL: https://zakon.rada.gov.ua/laws/show/996-14#Text

19. SOAR – TheHive Project URL: https://blog.thehive-project.org/tag/soar/

20. HOW TO SETUP UP CSIRT AND SOC GOOD PRACTICE GUIDE 2020 URL:https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20How%20to%20setup%20CSIRT%20and%20SOC.pdf

21. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 06 жовтня 2021 року № 601. URL: https://share.google/5SNRpK8K6VBk1sUrR