НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
В.о. завідувача кафедри

_____ **Микола ГРАЙВОРОНСЬКИЙ**
(підпис)

«_____»_____2021 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною программою «Системи, технології та математичні методи кібербезпеки»
спеціальності: 125 «Кібербезпека»

на тему: Soc як послуга на основі SIEM

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-74

Харламова Катерина Олександрівна
(підпис)

Керівник к.е.н, доц кафедри ІБ,Ткач Володимир Миколайович
(підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ - 2021 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Микола ГРАЙВОРОНСЬКИЙ
(підпис)
«___»_____2021 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Харламової Катерини Олександрівни

1. Тема роботи Soc як послуга на основі SIEM,

керівник роботи к.е.н, доц кафедри ІБ, Ткач Володимир Миколайович,

затверджені наказом по університету від « » _____ 2021 р. №

2. Термін подання здобувачем вищої освіти роботи 07 червня 2021 р.

3. Вихідні дані до роботи : Існуючі дані про операційні центри безпеки, дані про інфраструктуру компанії для побудови класифікації.

4. Зміст роботи

1. Загальний опис архітектури SOC as a Service, SOC та загальна проблематика SIEM-систем.
2. Створення моделі SOC для подальшого аналізу.
3. Практична частина – створення класифікації на основі даних про інфраструктуру компанії для моделей операційного центру безпеки: внутрішнього та зовнішнього

4. Висновки

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

6. Дата видачі завдання 1 грудня 2020 року.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	01.12.2020	Виконано
2	Огляд літератури з відповідної теми	10.01.2021	Виконано
3	Аналіз архітектури операційного центру безпеки	13.02.2021	Виконано
4	Розробка моделі операційного центру безпеки	20.03.2021	Виконано
5	Проходження переддипломної практики	12.04 - 16.05.2021	Виконано
6	Розробка класифікацій	26.05.2021	Виконано
7	Висновки	28.05.2021	Виконано

Здобувач вищої освіти _____ Катерина ХАРЛАМОВА
(підпис)

Керівник роботи _____ Володимир ТКАЧ
(підпис)

РЕФЕРАТ

Дипломна робота містить: 67 сторінок, 12 ілюстрацій, 7 таблиць та 22 літературних посилань.

В роботі розглянуто проблеми впровадження систем моніторингу подій, види операційних центрів, методи побудови внутрішніх операційних центрів безпеки.

Об’єктом дослідження є створена модель операційного центру безпеки.

Предметом досліджень є класифікація операційних центрів безпеки по типам підприємств.

Метою даної дипломної роботи є дослідження методів, моделей та видів побудови операційних центрів безпеки. Для цього на основі аналізу даних з відкритих джерел була побудована класифікаційна таблиця для подальшого вибору виду операційного центру безпеки.

Як результат у роботі проведена створена модель операційного центру безпеки, а також розроблена класифікація для різних видів підприємств.

Ключові слова: Операційний центр безпеки, операційний центр безпеки як послуга, SEIM-системи.

ABSTRACT

Thesis project contains: 67 pages, 12 figures, 7 tables, 22 references.

The problems of implementing of event monitoring systems, types of security operation centers, methods of construction of internal SOC are considered in the work.

The object of research is the created model of internal SOC.

The subject of research is the SOC's classification by the type of enterprise.

The aim of this thesis is to research the methods, models and types of SOC's construction. For this project, based on the analysis of data from published source, a classification table was built for further selection of the type of SOC.

As a result of this work is a created model of security operation center and developed classification for various types of enterprises.

Keywords: SOC, SOC as a Service, SIEM-system.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CSOC/SOC - Cybersecurity Operations Center (операційний центр безпеки).

ІБ - Інформаційна безпека

SIEM - Security information and event management (системи управління інформацією і подіями безпеки).

IRP - Incident Response Platform (платформа реагування на інциденти).

UEBA - User and entity behavior analytics (поведінковий аналіз користувачів і сутностей).

EDR - Endpoint detection and response (виявлення загроз на кінцевих точках та реагування на них).

NTA - Network traffic analysis (Аналізатори мережевого трафіку).

SOAR - Security Orchestration, Automation and Response (технології оркестрації, автоматизації та реагування).

SGRC - Security Governance, Risk-management and Compliance (управління безпекою, ризиками і відповідністю законодавству).

PCAP AV - Packet Capture Antivirus (повний аналіз сеансу мережевих даних антивірусу).

IDS/IPS - Intrusion Detection System/Intrusion Prevention System (системи виявлення та запобігання атак).

SLA - Service Level Agreement (угода про рівень надання послуги).

TCO - Total cost of ownership (сукупна вартість володіння).

ВСТУП

У зв'язку з розвитком кібератак, їх масштабом і впливом, організаціям будь-якого розміру доводиться приймати важливі рішення про те, як економічно ефективно управляти операціями щодо забезпечення безпеки. Таким чином багато організацій починають звертати увага на операційні центри безпеки, але часто через неправильний підхід до побудови власного SOC або ж неправильно вибору виду даного центру підприємства втрачають кошти та час на реалізаціє даного проекту.

Актуальність даної дипломної роботи полягає у визначені факторів, що впливають на підприємства при виборі типу SOC, тому в даній роботі побудована класифікаційна таблиця на основі якої підприємства зможуть надалі робити вибір операційного центру безпеки.

Операційний центр безпеки (SOC, Security Operations Center) – команда аналітиків, що за допомогою спеціальних систем та технологій вирішують завдання з безпеки. Таких як виявлення та аналіз кібербезпеки, оперативне реагування, запобігання їх виникненню та складання звітності.

При побудові SOC важливо пам'ятати кілька моментів. Security Operation Center - це не тільки технічні засоби. Це команда, завдання якої виявляти, аналізувати, реагувати, повідомляти про виникнення і запобігати інцидентам інформаційної безпеки. Ще один важливий компонент SOC - це процеси, оскільки мається на увазі взаємодію між співробітниками підрозділу, відповідального за моніторинг і реагування на інциденти, а також між різними підрозділами. Від того, наскільки якісно збудовані ці процеси, буде залежати ефективність роботи SOC. Технічні засоби є лише інструментами, які дозволяють автоматизувати частину процесів, які функціонують в SOC. При великому потоці подій досить важко обійтись без SIEM-системи, оскільки швидкість реакції на інциденти буде низькою. Таким чином,

формула ідеального SOC виглядає так: SOC = Персонал + Процеси + Технічні засоби.

Метою даної дипломної роботи є дослідження методів, моделей та видів побудови операційних центрів безпеки. Для цього на основі аналізу даних з відкритих джерел була побудована класифікаційна таблиця для подальшого вибору виду операційного центру безпеки.

Об’єктом дослідження є створена модель операційного центру безпеки.

Предметом досліджень є класифікація операційних центрів безпеки по типам підприємств.

1 АНАЛІЗ ОПЕРАЦІЙНОГО ЦЕНТРУ БЕЗПЕКИ. ПРОБЛЕМАТИКА СИСТЕМ МОНІТОРИНГУ ПОДІЙ

1.1 Засоби управління інформаційною безпекою

Політики або засоби управління ІБ самі по собі не гарантують повний захист інформації, інформаційних систем, служб або мереж. Після того як засоби управління безпекою були реалізовані, існує можливість того, що залишилися уразливості, які можуть стати причиною зниження ефективності ІБ і виникнення інцидентів ІБ. Дана обставина потенційно може мати прямий і непрямий вплив на бізнес-діяльність організації. Недостатня підготовка організації до вирішення таких інцидентів призведе до менш ефективного відповідного реагування і збільшить ступінь потенційного несприятливого впливу на її діяльність.

Внаслідок цього для будь-якої організації, зацікавленої в ефективній програмі ІБ, необхідно мати структурований і спланований підхід до:

- виявлення, звітності та оцінки інцидентів ІБ;
- реагування на інциденти ІБ, включаючи активізацію відповідних засобів управління для запобігання, зменшення і відновлення після несприятливих наслідків інцидентів;
- звітності по вразливостям ІБ для вжиття відповідних заходів щодо їх оцінки та вирішення;
- вилучення досвіду з інцидентів і вразливостей ІБ, впровадження превентивних засобів управління і вдосконалення загального підходу до управління інцидентами ІБ

Тому в організації слід впроваджувати операційні центри безпеки – SOC, які забезпечують :

- інвентаризація та контроль інфраструктури;
- консолідація (зміцнення, об'єднання, інтеграція) інформації про інциденти інформаційної безпеки;

- координація та автоматизація реагування на інциденти;
- аналіз даних, які були отримані з джерел зовні ;

Операційний центр безпеки також контролює мережі і кінцеві точки на наявність вразливостей, щоб захистити конфіденційні дані і дотримуватися галузевих або урядових постанов.

1.2 Аналіз компонентів операційного центру безпеки

Операційний центр безпеки – структура, що забезпечує захист активів компанії від сучасних атак. Він об’єднує технології, людей та процеси. Операційний центр безпеки – структура, що забезпечує захист активів компанії від сучасних атак. Він об’єднує технології, людей та процеси.

1.2.1 Технології

Технології SOC – це можливості, які необхідні для забезпечення видимості та надання аналітикам можливості для захисту від атак. Зловмисники, що володіють високою кваліфікацією в області інформаційних технологій і володіють різними методами злому здатні реалізувати складні атаки на IT-інфраструктуру. Це можуть бути масові атаки (самий гучний приклад - вірусні епідемії WannaCry і NotPetya) або цільові, спрямовані на конкретну компанію або галузь[3]. Для того, щоб вчасно зрозуміти, що зловмисники знаходяться в мережі організації необхідно збирати дані про події з великої кількості джерел. Чим більше джерел, тим більше шансів деактивувати атаку, але такий об’єм даних позводить до появи декількох проблем:

- Складно одночасно проглядати всі дані про події, що надходять з джерел.
- Кожне джерело має свою форму звітності про подію.
- Події з різних джерел можуть бути зв’язані, тому потрібно поставити їх в правильну послідовність.

- Журнали аудити періодично видаляють події, які зберігаються там протягом довгого періоду, тому важко відновити дані за довгий період.

Для вирішення цих проблем використовують системи моніторингу подій – **security information and event management (SIEM).** Основними задачами SIEM є:

• Збір та обробка даних;

• Цілодобова реєстрація інцидентів в режимі реального часу;

• Оперативна оцінка захищеності критично важливих ресурсів;

• Аналіз подій безпеки;

• Формування звітів.

Таким чином можливості SIEM - системи дозволяють перетворити величезні обсяги даних в важливу інформацію на основі якої далі приймаються рішення. Використання таких систем на практиці допомагає зробити більш ефективним обмін інформацією про загрози та ризики інформаційної безпеки підприємства.

Для вирішення проблем з встановлення зв’язку між подіями, які були отримані з різних джерел, використовують правили кореляції. При грамотному налаштуванні правил кореляції подій SIEM – система помітить підозрілу активність.

На базі даних зібраних SIEM – системами також проводиться аналіз поведінки користувача в мережі - **user and entity behavior analytics (UEBA)**.
UEBA – тип процесів в кібербезпеці, який враховує нормальну поведінку користувача та виявляє аномальну поведінку або випадки відхилення від
” нормальних ” моделей. Наприклад, якщо конкретний користувач регулярно завантажує файл розміром 10 МБ, але раптово завантажує гігабайти файлів, система зможе виявити цю аномалію і негайно попередити аналітиків [4].

Для того щоб детектувати події на кінцевих вузлах користувачів і серверах в IT-інфраструктурі, також може бути використано засіб класу **endpoint detection and response (EDR)**. EDR – це платформа, яка здатна виявляти складні і цільові атаки в системі, сервері, будь-якому комп'ютерному пристрої (кінцеві точки) і

швидко на них реагувати. Платформа EDR не просто захищає комп'ютерну систему від шкідників, вона вміє моментально помічати нові загрози високої складності і одночасно проявляти реакцію на ситуацію, що виникла. EDR не тільки має вбудовані механізми журналювання, але і детально аналізує те, що відбувається на рівні операційної системи. Зокрема, EDR-система може виступати джерелом подій для SIEM-системи.

Важливим джерелом слугує мережевий трафік. Для автоматизації збору і аналізу подій всередині трафіку використовуються засоби класу **network traffic analysis (NTA)**. NTA безперервно аналізують мережеву телеметрію і / або записи потоків. Дана система приймає дані телеметрії від безлічі мережевих пристроїв, таких як маршрутизатори, комутатори і брандмауери, щоб визначити, як виглядає «нормальна» поведінку цих пристроїв. При виявленні аномального трафіку або нерегулярної мережевої активності ці інструменти попереджають групу безпеки про потенційну загрозу. [5]

1.2.2 Процеси

Головними задачами SOC є виявлення та реагування на інцидент, але окрім цих процесів є інші і при побудові SOC нерідко неправильно вибудовують процеси, тобто їх життєвий цикл може виявитися, наприклад нежиттєздатним. В результаті аналітики не мають чіткого уявлення про задачі, які лежать перед ними, а також не мають грамотного побудування інструкцій щодо виконання цих задач.

Для підвищення ефективності SOC слід створити процеси рівня управління та операційного рівня.

1. Перший рівень забезпечує управління розвитком, підвищенням ефективності, управлінням звітністю та ресурсами.
2. Другий рівень базується безпосередньо над роботою з інцидентами, тобто їх реєстрацією, ідентифікацією, реагуванням та аналізом.

3. Останні служать для підключення джерел подій, розвитку кореляційної логіки, і актуалізації переліку інформаційних активів в області моніторингу та даних про ці активи [8].

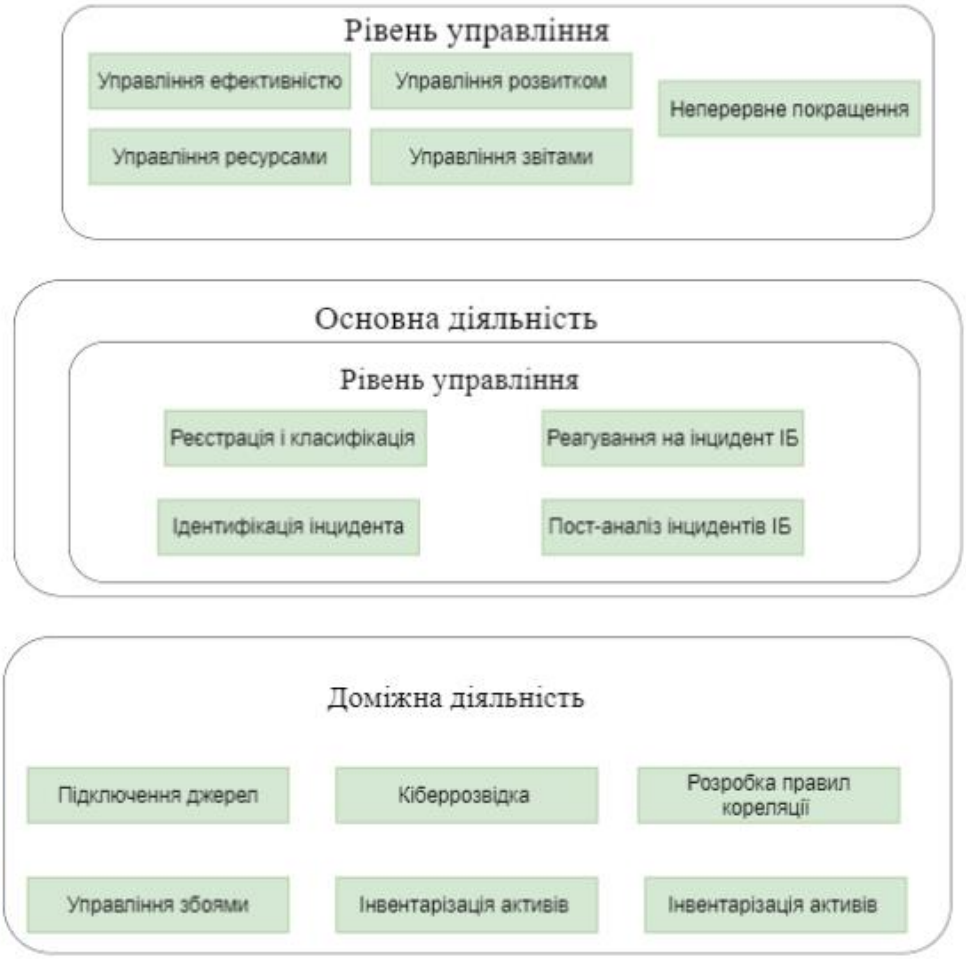

Рисунок 1.1 - Типова карта процесів SOC [8]

Якщо підсумувати зазначені вище рівні, то можна виділити такі процеси SOC:

- Інвентаризація;
- Аналіз загроз та ризиків;
- Виявлення вразливостей;
- Тестування на проникнення;
- Контроль виявлених раніше вразливостей;

- Аналіз коду;
- Управління інцидентами.

1.2.3 Люди

Центр SOC - це не тільки технічні системи, які в режимі реального часу передають аналітикам SOC повідомлення від засобів захисту, а й самі люди - експерти, які можуть відрізнити істинно позитивну подію від хибно позитивної, і здатні зрозуміти, чи є кілька явно не пов'язаних між собою повідомлень з джерел подій. Персонал SOC складається в основному з аналітиків безпеки, які працюють разом, щоб виявляти, аналізувати, реагувати, повідомляти і запобігати інцидентам, будь-яким подіям, які є непередбаченими або небажаними та можуть порушити діяльність організації або інформаційну безпеку. В прийнятті рішень
їм допомагають додаткові системи, які застосовуються для спрощення такого роду аналізу:

- SIEM
- Incident Response Platform (IRP) - платформи реагування на інциденти інформаційної безпеки;
- Security Orchestration, Automation and Response (SOAR) - системи управління, автоматизації та реагування на інциденти;
- Security Governance, Risk-management and Compliance (SGRC) - системи управління інформаційною безпекою, ризиками і відповідністю законодавству.

1.3 SOC as a Service

SOC-as-a-Service - це підключення до вже наявного центру моніторингу і реагування одного з ключових провайдерів ринку ІБ. Глобально це і є модель

керованих сервісів, які в більшості випадків замовник отримує з хмари. Зазвичай це - найпростіший і найменш витратний варіант реалізації SOC.

Провайдерів можна розділити на два типи:

- послуги гібридного SOC (центр моніторингу організований на базі інфраструктури замовника)

- хмарний SOC. Цей варіант буде кращий для невеликих організацій, що не мають власного SIEM-рішення, або для високотехнологічних компаній, яким потрібен швидкий результат і які готові використовувати в роботі аутсорсинг.

Отже, «віртуальний SOC», це коли функції кіберзахисту покладаються на наявний персонал, виділеного приміщення може і не бути, а під SOC розуміються швидше процеси забезпечення безпеки. Гібридний варіант, коли частина функцій захисту забезпечується на місці, а інші передаються на аутсорсинг в який-небудь комерційний SOC.

Комерційні SOC також називаються провайдерами керованого сервісу безпеки (Managed Security Service, MSS). Gartner [13] визначає MSS як моніторинг або управління функціями IT-безпеки, що надаються через загальні служби з віддалених операційних центрів безпеки, а не через персонал на місці. MSS повинен задовільняти трьом вимогам:

- цілодобовий віддалений моніторинг подій і джерел даних, що мають відношення до безпеки;
- забезпечення захисту віддалено з SOC, а не співробітниками на місці, і як комерційно доступний сервіс, а не послуга для єдиного споживача;
- адміністрування та управління технічними засобами IT-безпеки.

Крім моніторингу подій, SOC може надавати інші послуги. Наприклад, управління мережевими екранами, системами IDS / IPS і іншими пристроями, реагування на інциденти (віддалено або з виїздом на місце), оцінку вразливостей з супутніми діями (сканування, аналіз і вироблення рекомендацій). У міру того як компанії впроваджують хмарні технології систем безпеки, розширюється і

охоплення послуг віддаленого моніторингу, який тепер поширюється на послуги, що надаються з хмари і на середовище «Інтернету речей».

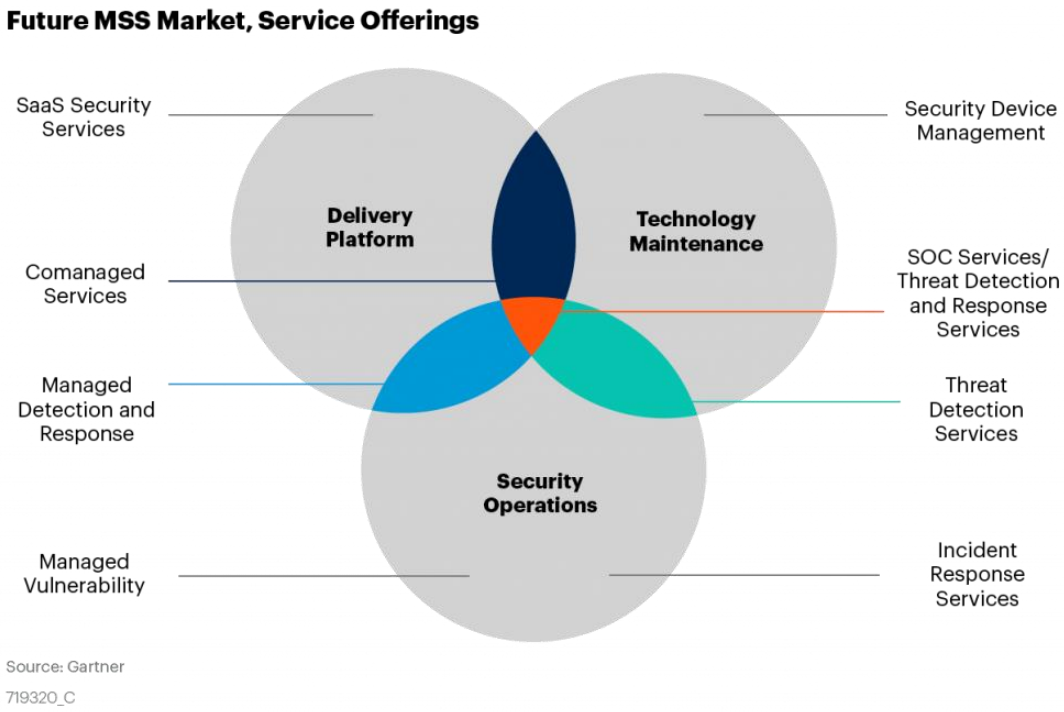

Рисунок 1.2 - Складові ринку MSS [14]

Центр ринку MSS складається з трьох основних функціональних областей:

1. Платформи доставлення (Delivery Platforms) -Saas, хмарні / локально розміщені,
2. Технічне обслуговування (Technology Maintenance) - доставлення контенту і підтримка технологій
3. Операції із забезпечення безпеки (Security Operations) – сервіс реагування на інциденти та сканери вразливостей. [14]

1.4 Аналіз архітектури SIEM-систем

SIEM-системи складаються з двох рішень:

- SIM (Security information management) – це управління інформаційною безпекою. Комплекс рішень, які спрямовані на створення та підтримку стабільної роботи системи, яка повинна забезпечувати зберігання важливої інформації, доступ до неї, а також проводити облік даних.
- SEM (Security event managemen) – це управління подіями безпеки. Забезпечує збір даних про загрози та впровадження засобів захисту, а також забезпечує рішення необхідні для прийняття конкретних заходів по пріоритизації, розслідуванню та усуненню загроз.

SIEM-система має розподілену архітектуру, яка передбачає більш високий рівень ефективності та дозволяє системі масштабуватися. Компоненти SIEM-системи представлені на різних платформах, і декілька компонентів можуть взаємодіяти один з одним для досягнення конкретної мети. Процес обробки інформації націлений на використання в різних організаційних моделях операційного центру безпеки. Ціль SIEM-проекту – це збір великої кількості даних та їх обробка, для того, щоб аналітики мали змогу використовувати цю інформацію для роботи.

Завдяки своїй архітектурі та набору функцій SIEM-система має декілька варіантів розвитку [9] :

1. Відстеження автентифікації і виявлення компрометації облікових записів користувачів і адміністраторів.
2. Відстеження випадків зараження. Виявлення шкідливих програм з використанням вихідних журналів брандмауера і журналів веб-проксі, а також внутрішніх журналів підключення і мережевих потоків.

3. Моніторинг підозрілого вихідного трафіку і переданих по мережі даних з використанням журналів брандмауера, журналів веб-проксі і NetFlow. Виявлення крадіжки даних і інших підозрілих зовнішніх з'єднань.
4. Відстеження системних змін і інших адміністративних дій у внутрішніх системах і їх відповідності дозволеної політиці.
5. Відстеження атак на веб-додатки та їх наслідків з використанням журналів веб-сервера, WAF (Web Application Firewall, екран для захисту веб-додатків) і логів програм. Виявлення спроб компрометації веб-додатків шляхом аналізу різних звітів.
6. Аналіз інцидентів, відстеження та зберігання даних журналу аудиту.

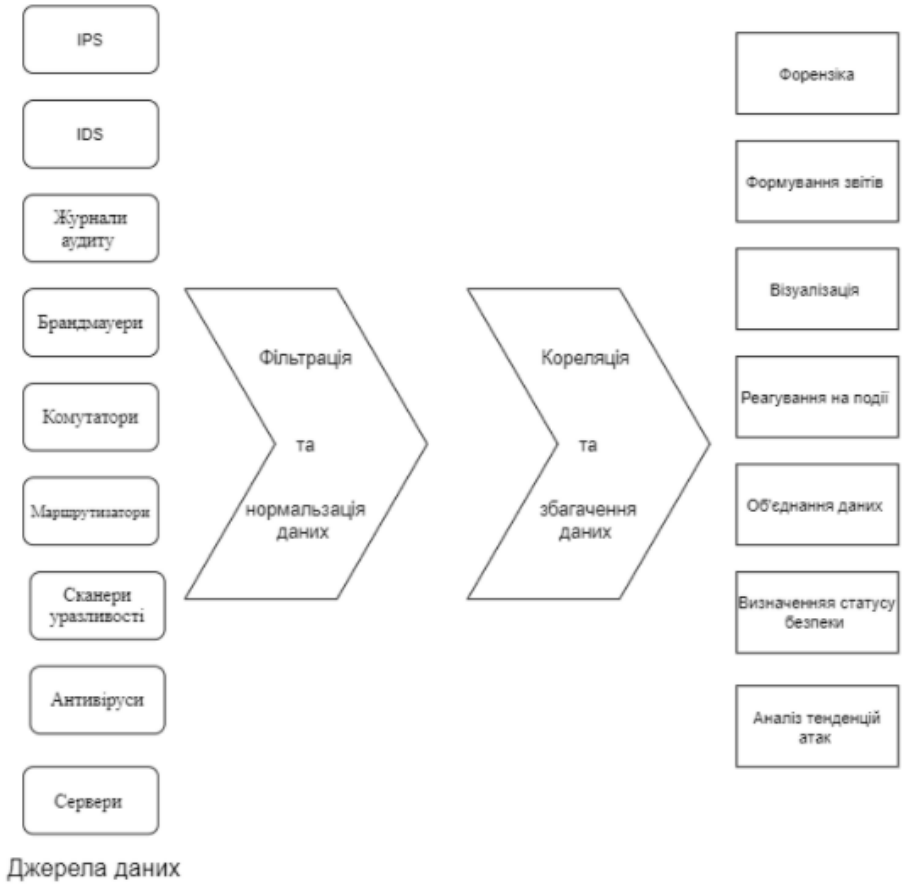

Рисунок 1.3 - Архітектура SIEM-систем [1]

1.5 Аналіз впровадження SIEM-систем на підприємство

Процес впровадження складається з багатьох етапів [10]:

1. Оцінка масштабу та інфраструктури;
2. Прийняття рішення про спосіб впровадження
3. Формування та затвердження технічного завдання;
4. Установка та базове налаштування SIEM-системи, тобто необхідно налаштувати SIEM-сервер, прописати логи, виконати специфічні налаштування відносно мережі підприємства;
5. Налаштування джерел подій;
6. Написання можливих додаткових правил реагування на інциденти, тому що “з коробки” SIEM-система не буде працювати належним чином;
7. Тестова експлуатація і накопичення статистики. В загальному слід відвести на цей пункт декілька місяців;
8. Корегування та доповнення правил кореляції. Нерідко виконується паралельно з попереднім етапом;
9. Завершення тестової експлуатації. Слід залишити декілька днів на фінальні корективи;
10. Підготовка до об'єднання SIEM-систем з системами, які знаходяться на підприємстві.

На сьогоднішній день проблема впровадження виникають на перших пунктах, так як вони потребують найбільшої уваги та врахування всіх необхідних параметрів режиму їх функціонування і мають обмеження на технічне забезпечення, а також визначення великої кількості конфігураційних атрибутів, які налаштовуються в SIEM-системі. Первинне налаштування проєкту являє собою набір дій по редагуванню конфігураційних файлів системи.

Складність побудови SIEM-системи пов’язана з необхідністю збору та аналізу подій різних типів, тому потребує:

1. Високої кваліфікації спеціалістів по налаштуванню правильної конфігурації.
2. Виділення неоднорідних апаратних платформ, що може обмежити впровадження SIEM-системи в вже існуючу інформаційну структуру підприємства.
3. Окрім цього, також достатньо високі вимоги до технічних характеристик апаратних платформ, що може призвести до того, що первинна цінна проекту буде збільшена.
4. Велика трудомісткість розробки технічної документації на багатокомплексну SIEM-систему і, відповідно, наявність великої кількості помилок може призвести до збільшення терміну впровадження системи.

1.6 Основні проблеми при інтеграції SIEM

1.6.1 Оцінка масштабу

Масштаб системи лежить в основі подальшого планування, впровадження та росту SIEM-проекту. Правильна оцінка впливає на вибір рішення, архітектурні вимоги, необхідну кількість співробітників. Перед купівлею, а згодом і впровадженням SIEM-системи на підприємство, слід оцінити [11]:

- Об'єм даних, які оброблює система протягом дня (вимірюються в гігабайтах в день),
- Кількість приладів, що надсилають дані в систему,
- Кількість співробітників, які мають доступ до системи.

1.6.2 Надлишкова інформація

Велика кількість логів безпеки збільшить навантаження на SIEM-систему. SIEM отримує інформацію з різних джерел, таких як:

- IDS,
- IPS,
- Журнали аудиту,
- Брандмауери,
- Комутатори,
- Маршрутизатори,
- Сканери уразливості,
- Антивіруси.

Одна з найважливіших задач для систем виявлення атак - отримання високого проценту істинно позитивних подій. Істинно позитивні події - коли відбувся негативний інцидент і система виявила це. Цей процент досягається за рахунок потоку хибно позитивних спрацювань, де хибно позитивні спрацювання - коли система генерує попередження, але активність насправді не була зловмисною, тому до SIEM-системи буде надходити надлишкова кількість подій, яка призводить до того, що аналітикам буде важко знайти важливу інформацію. Систему слідує налаштовувати так, щоб вона була орієнтована на результат.

1.6.3 Кваліфікація співробітників

Для успішного впровадження і роботи SIEM-проекту співробітники повинні бути компетентні та підготовлені до роботи з SIEM. SIEM-системи сам по собі працювати не можуть. Вони потребують постійного налаштування і обслуговування для правильно реагування на події, які виникають в системі, та вхідні дані. Окрім цього, є необхідність розслідувати інциденти і усувати проблеми, які будить виникати в процесі[1].

1.6.4 Час виділений на впровадження

Початкове налаштування SIEM досить просте. На те щоб підключити і налаштувати перші декілька джерел даних виділяється пару місяців і, на перший погляд, це забезпечує великі успіхи. Однак забезпечення системи потрібними даними, її налаштування, написання конфігураційних файлів та повна інтеграція в роботу може зайняти рік або навіть більше. Як правило, чим надійніше SIEM-система, тим більше часу повинен витратити аналітик на вивчення матеріалу, тому що потрібен час на те щоб освоїти інструмент

Висновки до розділу 1

Отже, в даному розділі було розглянуто архітектуру операційного центру безпеки та системи моніторингу подій. Описано засоби управління безпекою та основні проблеми при впровадженні SIEM-систем. Також було розглянуто етапи впровадження SIEM-проекту. Окрім цього було розглянуто види та загальні функції SOC-as-a-Service для подальшого аналізу.

2 СТВОРЕННЯ МОДЕЛІ SOC ЯК ПОСЛУГИ НА ОСНОВІ SIEM

2.1 Етапи управління інцидентами ІБ згідно ISO/IEC 27035-1:2016

Насамперед слід визначити етапи управління інцидентами, так як головними задачами операційного центру безпеки є виявлення та реагування на інциденти. Чітке розуміння поставленої задачі допоможе аналітикам краще орієнтуватися у роботі. Часто буває так, що основні задачі задокументовано розпливчато і при виконанні своєї роботи члени групи безпеки можуть вийти за деякі рамки при реагуванні на інцидент. Тому слід зробити управляння інцидентами чітко та поетапно.

ISO/IEC 27035-1:2016 – Методи і засоби забезпечення безпеки - Менеджмент інцидентів інформаційної безпеки - Частина 1: Принципи менеджменту інцидентів, є основою багатокомпонентного міжнародного стандарту. В ньому представлені основні концепції і етапи управляння інцидентами ІБ, які об’єднані з принципами в структурованому підході до виявленню, оцінці і реагуванні на інциденти. Принципи, які викладені в стандарті є загальними та призначені для використання всіма організаціями[12].

Отже, згідно з стандартом ISO/IEC 27035-1:2016, управляння інцидентами ІБ складається з:

1. Планування і підготовки;
2. Виявлення і звітності;
3. Оцінки та прийняття рішення;
4. Реагуванні;
5. Отриманому досвіді.

Деякі дії можуть відбуватися в кілька етапів або протягом усього процесу обробки інцидентів. До таких видів діяльності належать такі дії:

- Документування подій та інцидентів і ключової інформації, вжитих заходів реагування та подальших дій в рамках процесу обробки інцидентів;

- Координація і зв'язок між сторонами;
- Повідомлення керівництва та інших зацікавлених сторін про значні інциденти;
- Обмін інформацією між зацікавленими сторонами: внутрішніми і зовнішніми співробітниками, такими як постачальники.

Таблиця 2.1 - Етапи управління інцидентами ІБ

ПІДГОТОВКА ТА ПЛАНУВАННЯ
• оновити регламент інформаційної безпеки; • план управління інцидентами ІБ; • створення групи реагування на інциденти інформаційної безпеки (ГРІІБ) – це група аналітиків, що виконує, координує та підтримує реагування на порушення ІБ; • взаємодія з внутрішніми і зовнішніми організаціями; • технічна та інша підтримка (включаючи супровід); • оперативні наради та навчання з підвищення кваліфкації; • тестування плану управління інцидентами інформаційної безпеки.
⬇
ВИЯВЛЕННЯ ТА ЗВІТНІСТЬ
• узагальнення інформації про ситуативну обізнаності з внутрішніх і зовнішніх джерел даних і новинних стрічок; • моніторинг безперервності системних і мережевих процесів; • виявлення і сигналізація про аномальні, підозрілі або шкідливі активності; • формування звітів про інциденти від різних джерел або співробітників;

• звітність щодо подій ІБ.

ОЦІНКА І ПРИЙНЯТТЯ РІШЕНЬ

• загальна оцінка ІБ і визначення інциденту ІБ.

РЕАГУВАННЯ

• визначення місця знаходження інциденту ІБ;

• локалізація і ліквідація інциденту ІБ;

• відновлення діяльності після інциденту ІБ;

• висновок щодо інциденту ІБ і його аналіз.

• при необхідності подальше розслідування

ОТРИМАНИЙ ДОСВІД

• визначення досвіду, отриманого під час реагування на інциденти і вразливості ІБ;

• визначення та удосконалення ІБ;

• визначення та удосконалення системи управління інформаційною безпекою;

• формування та покращення управління інформаційною безпекою;

• оцінка ефективності ГРІІБ.

2.2 Формування моделі SOC

2.2.1 Формування ключових задач та параметрів SOC

Насамперед слід почати з опрацювань основних параметрів та задач створюваної моделі.

Отже, при розгляданні зазначених вище головних задач операційного центру безпеки більш детально, то до його завдань входять:

1. Запобігання інцидентів кібербезпеки.
2. Моніторинг, виявлення і аналіз потенційних вторгнень в режимі реального часу.
3. Реагування на підтверджені інциденти.
4. Надання відповідним організаціям актуальної інформації про поточну ситуацію, а також звітів про статус кібербезпеки, інциденти та тенденції в поведінці зловмисників.
5. Розробка і управління засобами захисту комп'ютерних мереж, такими як IDS або системи збору / аналізу даних.

Додаткові можливості деяких SOC можуть включати розширений криміналістичний аналіз, криптоаналіз і зворотне проектування шкідливих програм для аналізу інцидентів.

До ключових параметрів SOC можна віднести:

1. Організаційну модель. Дана модель створюється для малих, середніх та великих підприємств, які визначаються як: маленьке – до 50 співробітників, а середнє – від 50 до 500, великі – більше ніж 500. Тому організаційна модель ствоюємого SOC буде попадати в область між командою безпеки та внутрішньо розподіленим SOC, де:
   - Команда безпеки визначається відсутністю окремої одиниці для виявлення або реагування на інциденти. У разі виникнення інциденту комп'ютерної безпеки, збираються ресурси (як правило, з числа

споживачів послуг SOC) для вирішення проблеми, відновлення систем, після чого команда припиняє свою роботу. Цю модель, як правило, вибирають клієнти, що складаються з менше ніж 1000 користувачів або IP-адрес.

- Внутрішній розподілений SOC. Постійний SOC існує, але в основному складається з співробітників, що знаходяться за межами SOC, їх основна робота пов'язана з IT або безпекою, але не обов'язково пов'язана із захистом комп'ютерних мереж. Одна людина або невелика група відповідає за координацію дій щодо забезпечення безпеки, але складні завдання виконуються особами, залученими з інших організацій. Цю модель, як правило, вибирають клієнти, що складають діапазон від 500 до 5000 користувачів або IP-адрес.

2. Виконувані функції, які виходять із завдань.
3. Рівень повноважень. SOC може володіти трьома рівнями повноважень:
   - Без повноважень, тобто SOC може намагатися впливати на дії, які споживачі його послуг повинні зробити. Однак у SOC немає ні формальних засобів для чинення тиску, ні вищої організаційної одиниці, здатної це зробити. Тільки замовник вирішує, розглянути або ігнорувати рекомендації SOC.
   - Спільні повноваження. SOC може давати рекомендації керівництву замовника , у якого є повноваження для реалізації запропонованих змін. Ці рекомендації порівнюються з пропозиціями інших зацікавлених сторін до прийняття рішення, даючи SOC можливість «висловитися».

- Повні повноваження. SOC може давати споживачам своїх послуг вказівки на певні дії, не чекаючи схвалення або підтримки з боку учасників вищого рівня.

2.2.2 Формулювання групи безпеки

Команда SOC може варіюватися від п’яти співробітників до розмірів національних координаційних центрів. Зазвичай організаційний центр безпеки поділяє аналітиків на 3 Лінії:

- 1-ша Лінія займається оперативною реакцією на інцидент;
- 2-га та 3-тя Лінії – це аналітики, що ведуть розслідування, аналізують дані та створюють звітність.

Перша Лінія - це інженери моніторингу, які відповідають за своєчасну реакцію на інцидент, його аналіз, фільтрацію помилкових спрацювань. Якщо фахівець 1-ї Лінії визначає, що подія досягла встановленої заздалегідь межі, то подія передається на 2-гу Лінію та створюється детальна аналітична довідки про інцидент. Дана межа визначається в залежності від різних типів потенційної “небезпеки” , тобто різновиду інциденту про актив, який атакують або інформації про порушений процес. Співробітники 1-ї Лінії опрацьовують кожну подію протягом 15 хвилин. Їм не рекомендується виконувати поглиблений аналіз, оскільки вони не повинні відволікатися від подій, що надходять в режимі реального часу. У випадку, коли на опрацювання інциденту потрібно більше зазначеного часу, він переводиться на 2-гу Лінію. Перша Лінія працює позмінно і, таким чином, забезпечую реагування та розбір інцидентів в режимі 24/7.

Завдання 1-ї Лінії:

1. Пріоритизація подій в режимі реального часу.
2. Розбір телефонних дзвінків від користувачів.
3. Іншими рутинними завданнями.

Друга Лінія - це спеціалісти з певних напрямів в інформаційній безпеці, які обробляють нетипові інциденти у відповідності до сфери їх відповідальності. Кандидат на роботу в 2-й Лінії повинен досконало володіти основним функціоналом SIEM-системи. Друга Лінія отримує аналітичні довідки про

інциденти від 1-ї Лінії, щоб визначити, що насправді відбулось і чи потрібні подальші дії. Для визначення масштабу і важливості події може знадобитися декілька тижнів, для перевірки всіх необхідних даних. Для реагування на інцидент і подальшого відновлення SOC використовує зовнішні та внутрішні ресурси.

Менеджери SOC управляють групой безпеки та звітують зазвичай перед директором з ІБ. Вони є свого роду ланкою між вищим керівництвом та аналітиками. Контролюють групу безпеки, забезпечують технічне керівництво та керують фінансовою складовою. Менеджер SOC спостерігає за діяльністю команди SOC, включаючи прийом на роботу, навчання і оцінку персоналу. Додаткові обов'язки включають створення процесів, оцінку звітів про інциденти. Вони створюють звіти про відповідність, підтримують процес аудиту, вимірюють показники продуктивності SOC і звітують про операції із забезпечення безпеки перед керівниками ІБ [16].

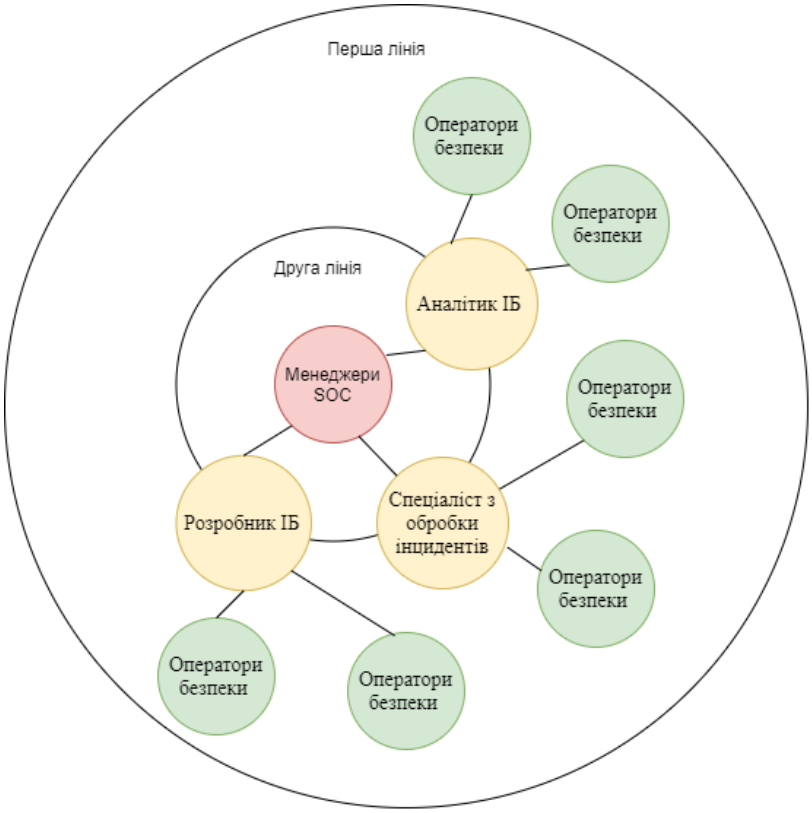

Рисунок 2.1 - Діаграма взаємодії персоналу

2.2.3 Реагування на інцидент

Як вже будо зазначено вище в пункті 2.1, для досягнення максимального результату на реагування, слід зробити цей процес чітким та поетапним, але перед тим як робить будь-які дії потрібен ряд причин:

1. SOC повинен бути впевнений, що його дії не призведуть до переривання нормальних процесів.
2. Відповідні дії можуть вплинути на виконання завдань клієнта більше, ніж на сам інцидент.
3. Розуміти масштаб і серйозність вторгнення. Спостереження за зловмисником, іноді більш ефективно, ніж виконання статичного експертного розслідування на скомпрометованих системах в його відсутність.

В ідеалі, SOC повинен виявити інцидент до того, як буде завдано значної шкоди. Ідеальний сценарій: виявлення інциденту під час розвідки або під час фактичної атаки, коли доступ до системи здійснюється через експлуатацію вразливості. Ознаки атаки можуть виникати одночасно в декількох місцях: в мережевому трафіку, BIOS-хості, на жорсткому диску, знімних носіях, ПО, системних ПО і додатках в пам'яті. Усвідомлення цієї інформації впливає на вибір датчиків для установки і розуміння того, коли і як можна ці датчики можна обійти, нейтралізувати або відключити.

Аналітики починають з первинних індикаторів (наприклад, високорівневого попередження про інцидент або спрацьоване правило кореляції) і далі збирають додаткові дані для підтвердження виявлених подій. Достовірність цих даних може бути покращена за допомогою засобів кореляції і автоматизованої фільтрації, а також дедублікації даних в SIEM-системах.

Спеціалісти SOC не можуть бути на 100% впевнені в тому, що насправді сталося, через неповні, непереконливі або неоднозначні дані. SOC повинен це враховувати, особливо, при виборі сценарію реагування. Підозри на інциденти

допомагають аналітику зорієнтуватися, на які події слід звернути увагу в першу чергу. Контекст необхідний для того, щоб точно встановити, що насправді сталося (наприклад, незаперечні «факти» наявності шкідливої активності на хості і в мережі). Якщо SOC не буде охоплювати цей спектр, аналітики не зможуть ефективно виявляти і проаналізувати передбачувані інциденти.

Саму інформацію про інцидент аналітики отримують з різних джерел таких як:

- Клієнтів зі звичайним непривілейованим доступом до системи;
- Системних адміністраторів і адміністраторів мереж клієнта;
- Служб технічної підтримки клієнта;
- Від менеджерів і керівників систем інформаційної безпеки клієнта;
- Інших SOC (того ж рівня або підлеглих, які координують або національних);
- Правоохоронних органів або інших слідчих підрозділів;
- Інших організацій, які причетні до інциденту;

Ці дані можуть бути отримані різними способами включаючи:

- Електронні листи;
- Телефонні дзвінки;
- Звіти при особистому спілкуванні;
- Заповнення форми про інцидент на веб-сайті SOC;
- Інформацію від інших SOC.

Інциденти, виявлені за допомогою цих засобів, слід розглядати як найбільш цінні, особливо в порівнянні з непідтвердженими повідомленнями від IDS. Оскільки вони оцінювалися з точки зору власних завдань і систем які повідомили про інцидент сторін, вони майже напевно заслуговують на увагу.

SOC також отримує інформацію з внутрішніх джерел, таких як:

- Системи виявлення та запобігання атак (IDS/IPS)
- Системи виявлення / запобігання вторгнень на хостах (HIDS / HIPS);
- Збір і аналіз мережевого трафіку (NetFlow);
- Журнали ОС, додатків і мережевих пристроїв, такі як журнали веб-сервера, журнали веб-проксі, журнали DNS і попередження антивіруса (AV);
- Інструменти лог-менеджменту та аналізу і SIEM, які збирають, аналізують, зіставляють і інформують про ціх логах;
- Криміналістичний аналіз зразків шкідливих програм і носіїв, наприклад жорстких дисків;
- Системи автоматичного збору та оповіщення про дані кіберрозвідки;
- Повний аналіз сеансу мережевих даних (PCAP).

Що стосується виявлення самих вторгнень, то існує декілька підходів – це сигнатурне виявлення та виявлення аномалій.

- Сигнатурне виявлення, також називається виявленням несанкціонованої активності. Тобто система самостійно може виявити та розрізнити шкідливу активність в мережі.
- Виявлення аномалій означає, що система розпізнає привичну активність і попереджає аналітиків про аномалію.

Сигнатурний підхід більш розповсюджений тому, що він вимагає наявність даних та знань про інциденти та атаки, для того щоб сповіщати групу безпеки не раніше того, як загроза стане відомою. З іншого боку, виявлення аномалій часто вимагає наявності вже базового рівня «нормальної поведінки», що теж потребує часу для збору даних.

2.2.4 Системи моніторингу подій.

Ефективна система моніторингу безпеки включає в себе дані, які були зібрані в результаті неперервного моніторингу кінцевих точок: комп'ютерів, ноутбуків, серверів тощо, а також мережі та журналів аудиту.

На рис 2.2 зображена загальна модель технологій виявлення подій, яка складається з різних даних, що потрапляють в систему моніторингу та процесів, які дана система має змогу згодом виконати:

- Видимість. Завдяки централізації джерел даних в системі, то SOC має змогу отримувати інформацію про можливі аномалії, загрози та інциденти.
- Аналіз. Спеціалісти з безпеки можуть аналізувати дані з різних джерел, відкидати хибно позитивні та будувати ряд подій для виявлення масштабу інциденту.
- Дії. На основі отриманих даних може бути проведене автоматичне або мануальне реагування, включно з установкою виправлень, модифікацією параметрів або відправленням системи чи файлу на карантин

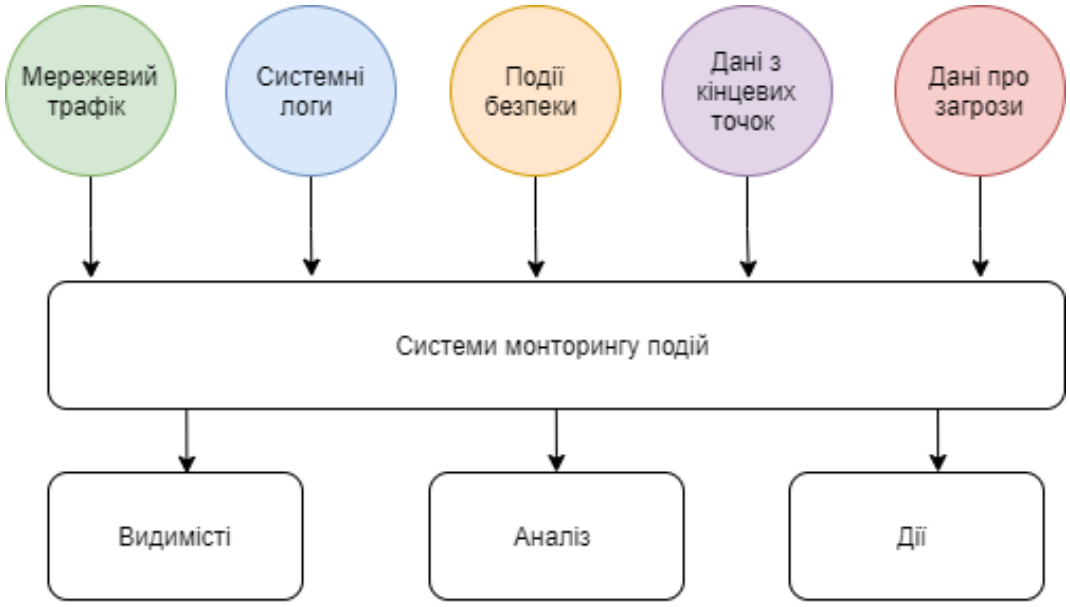

Рисунок 2.2 - Загальна модель технологій виявлення

Найпоширенішим прикладом такого класу систем є SIEM-системи, архітектура яких вже була описана в розділі 1.

2.3 SIEM-системи: передумови для впровадження , характеристики та механізми роботи

Перш ніж вкладати гроші в SIEM-проект необхідно деякі передумови, такі як [1]:

- У SOC вже є інструменти збору логів; його потреби в аналітиці та кореляції даних більше, ніж пропонують поточні інструменти.
- SOC виконує значну частину своїх обов'язків з аналізу даних в реальному часі.
- SOC виділив крім IDS / IPS ще кілька потоків даних, які необхідно передавати в SIEM в режимі реального часу.
- SOC бере участь в процесі регулярного управління і настройки датчиків, для чого є виділений персонал, тим самим демонструючи, що він готовий взяти на себе управління SIEM

SIEM- проекти мають доволі складну схему обслуговування і їх остаточна ціна зазвичай залежить від:

- Кількості джерел даних
- Об’єму даних, які оброблює система
- Кількості користувачів, що мають доступ до мережі.

Ретельне панування має ключове значення для купівлі SIEM-систем, тому що SOC повинен планувати щорічні виплати в рамках загальної вартості підтримки. Щорічна плата за обслуговування та підтримку складає від 20-30% від початкової вартості придбання.

При роботі з SIEM-системами необхідно чітко розуміти головні вимоги до неї. Тому насамперед слід оглянути ключові параметри архітектури та реалізації SIEM-систем.

Характеристики:

- **Пакет розгортання.** Пакети розгортання існують декількох типів:

  1.Коллектори- пакети в вигляді ПО, які можна встановити на кінцевий пристрій в єдиній точці збору, наприклад на сервері бази даних IDS. Вони мають декілька параметрів конфігурації параметрів, що дозволяють адміністраторам оптимізувати ресурси: ЦП, пам’ять, об’єм дискового простору і багатопотоковість.

  2.Менеджери(головний вузол) – пакети у вигляді ПО(у вигляді традиційно встановлюваного ПО або у вигляді віртуального пристрою) та апаратного пристрою. Менеджер повинен бути багатопотоковим, щоб підтримувати паралельне виконання запитів і ефективну кореляцію.

- **Зберігання даних.** Продукти SIEM теоретично здатні зберігати події, зібрані за багато років і навіть десятиліття. Але тривалість зберігання зазвичай обмежується періодом роботи з моменту першої ітерації. У деяких випадках SOC може віддати перевагу нову інсталяцію SIEM, щоб почати з чистого аркуша. Це може стати проблематичним, оскільки SOC буде міняти безліч поколінь продуктів SIEM, в той же час продовжуючи прагнути до довгострокового зберігання даних аудиту. У міру розвитку і більшої стабільності продуктів, оновлення програмного забезпечення краще підтримує зберігання даних про події і призначених для користувача даних.
- **Кількість пристроїв.** SIEM повинна мати можливість обробляти десятки або навіть сотні тисяч кінцевих пристроїв по різних каналах передачі даних. SIEM також повинна мати можливість розпізнавати декілька потоків даних з однієї і тієї ж кінцевої точки. Добре спроектована програмне забезпечення агента має справлятися з

багатьма пристроями (можливо, десятками тисяч), чий сумарний потік подій може підтримувати більше тисячі подій в секунду.

- **Кількість подій.** Правильна реалізація SIEM зазвичай обробляє події, що надходять зі швидкістю на рівні тисяч подій в секунду, що відповідає десяткам або сотням мільйонів подій в день. Це оптимальна цифра для SIEM. Хоча багато постачальників SIEM рекламують швидкість прийому від 10 000 до 100 000 або більше подій в секунду. При цьому слід звернути увагу чи покращиться робота аналітиків завдяки розподілу даних за рівнями, або не занадто ми нерозбірливі щодо того, які дані ми збираємо?

Перед впровадженням SIEM- проекту в інфраструктуру SOC слід визначити, які пристрої будуть слугувати джерелами даних та виділити окремі правила кореляції, для того щоб аналітики не губили потрібну інформацію серед ‘‘шуму’’. Тому слід почати з інвентаризації ІБ-активів організації, для цього можна використовувати сканери вразливостей. Це допомагає за короткий час зібрати всю потрібну інформацію про наявні компоненти інфраструктури компанії та про їх вразливості, а також допоможе в майбутньому відстежувати стан мережі. Коли вся необхідна інформація зібрана слід її приоритизувати, тобто надати кожній події ступінь критичності та вирішити, які дані слід збирати, оброблювати та зберігати. Найбільш важливі та критичні джерела потрібно підключати до SIEM-систем.

Коли SOC купує SIEM-проект, важливо звернути увагу на функції, які припускають, що продукт спочатку був сконструйований як SIEM корпоративного рівня, а не як разовий або домашній проект, який згодом перетворився в комерційну пропозицію. Багато продуктів класу SIEM, представлені на сьогоднішньому ринку, були спочатку спроектовані з дуже вузьким набором функцій і варіантів використання в порівнянні з тим, про що вони заявляють зараз. Хороший продукт SIEM повинен бути сконструйований з надійним механізмом кореляції і розширюваними можливостями прийому даних.

Початкове налаштування SIEM досить просте, його можна виконати за один або два дні. Через кілька тижнів або місяців можна підключити і налаштувати перші кілька каналів даних і почати створення контенту, що забезпечує швидкі успіхи. Однак забезпечення системи потрібними даними, її налаштування, написання контенту для клієнтських організацій і повна інтеграція в роботу займає рік або більше - за політичними і технологічних причин, а не через технічні причини. У багатьох випадках отримання власниками даних надійних і стійких каналів журналів аудиту може бути політично складним процесом.

Слід також пам’ятати, що кожне робоче місце в SOC по-різному використовує дані і функції SIEM. Лінія 1 буде зацікавлена в сортуванні даних в реальному часі і конкретних сценаріях використання, під які вони можуть написати інструкції. Лінія 2 швидше за все буде зацікавлена в зборі якомога більшої кількості деталей про потенційний інцидент, тобто вони будуть виконувати запити довільної форми протягом тривалих періодів часу. Ті, хто відповідають за виявлення та попередження атак або за відстеження тенденцій, ймовірно, будуть агрегувати різні джерела даних, багаторазово виконуючи довгі ресурсомісткі запити. Менеджери будуть зацікавлені в координації роботи і метриках, які дає інструмент, щоб переконатися, що відповідні підрозділи SOC виконують інструкції, відстежують аномальну активність, коли система її вловлює, і не допускають простою системи.

Розподіл механізмів по рівням ієрархії зображений на рисунку 2.3. при переході до механізмів більш високого рівня моделі, показаної на кількість оброблюваних подій зменшується, а складність їх обробки збільшується

Рисунок 2.3 - Ієрархія механізмів[18]

- Одним з ключових механізмів, які використовує SIEM, є механізм збору та агрегації логів. Ця інформація надходить з безлічі різних джерел - мережеве обладнання, засоби захисту інформації, додатки, СУБД. Інформація потрапляє в SIEM або на пряму з систем, що відслідковуються, або через парсинг лог-файлів. У загальному випадку інформація про ту чи іншу подію містить позначку про час (timestamp), код події, а також набір довільних полів даних, частина яких зустрічається дуже часто (IP адреса джерела події, ім'я користувача і т.д.). Задавши в правилах парсинга формат логів і призначення полів даних, ми зможемо використовувати ці дані в SIEM системі. Після обробки інформація стає доступна оператору, який може її використовувати для розслідування інцидентів, статистичного аналізу роботи IT систем або аудиту
- **Кореляція подій.** При підключені великої кількості джерел подій постає питання їх аналізу. Мануальна обробка даних не кращий варіант, тому для моніторингу системи використовують кореляцію

подій, що забезпечує автоматизований аналіз подій, які надходять до системи, та повідомляє оператора безпеки про загрозу тільки при необхідності. Виділяють два способи кореляції:

1. Кореляція на базі правил (Rule based correlation);

В цьому випадку при впровадженні системи ми описуємо певну послідовність логічних дій, які характеризують дії зловмисника. Наприклад, велика кількість спроб входу в якусь систему, що нагадує процес підбору пароля, яке закінчується успішним входом в цю систему. Перевагою цього способу є висока точність виявлення зловмисника. До недоліків можна віднести необхідність періодичного оновлення правил кореляції і неможливість реагувати на послідовність подій, що не описану в правилах.

2. Кореляція без використання правил (Rule-lesscorrelation).

Використовує ризик орієнтований підхід подібний банківським скоринговими системам. В рамках цього підходу всі події мають певний рейтинг, і, коли рівень рейтингу послідовності подій з одним параметром (вихідний IP адреса, цільової IP адреса, користувач і т.д.) перевищує встановлений, відбувається оповіщення оператора. Перевагою цього способу є відсутність залежності від написаних правил і можливість виявлення нових векторів атак. До недоліків відноситься менший рівень точності, тому що існує ймовірність того, що незвичайні дії виконує легітимний користувач. Також можна виділити статистичний аналіз подій, коли працюють системи створюють стандартний профіль подій (наприклад, велика кількість успішних авторизації в Active Directory вранці в будній день). Таким чином, нестандартна подія (наприклад, авторизація вночі або спроба віддаленого доступу з території іншої держави) також може означати ймовірність інциденту ІБ.

- **Розслідування інцидентів.** Так як SIEM система є центром агрегації всіх даних, обсяг подій, що вимагають додаткового аналізу, в ній завжди вище, ніж в звичайних засобах ІБ. У зв'язку з цим, SIEM системи мають у своєму розпорядженні вбудованим механізмом побудови процесів розслідування інцидентів ІБ. Наприклад, в разі появи інциденту, пов'язаного з роботою мережного обладнання, буде створений інцидент і призначений відповідальний співробітник.
- **Нормалізація.** Приведення форматів записів журналів, зібраних з різних джерел, до єдиного внутрішнього формату, який потім буде використовуватися для їх зберігання і подальшої обробки.
- **Фільтрація** подій безпеки полягає у видаленні надлишкових подій з вступників в систему потоків.
- **Класифікація.** Дозволяє для атрибутів подій безпеки визначити їх приналежність певним класам.
- **Пріоритезація.** Визначає значимість і критичність подій безпеки на підставі правил, визначених у системі.
- **Аналіз подій.** Включає процедури моделювання подій, атак і їх наслідків, аналізу вразливостей і захищеності системи, визначення параметрів порушників, оцінки ризику, прогнозування подій та інцидентів.
- **Прийняття рішень.** Визначає вироблення заходів по зміні конфігураційних правил засобів захисту з метою запобігання атак або відновлення безпеки інфраструктури.
- **Візуалізація.** Передбачає подання до графічному вигляді даних, що характеризують результати аналізу подій безпеки і стан захищеності системи та її елементів

2.4 Функціональна модель SOC та SIEM - систем

Базуючись на розглянутих вище даних, визначивши основні функції, задачі, напрями роботи та види діяльності, було побудовано модель організаційного центру безпеки, яка зображена на рисунок 2.4.

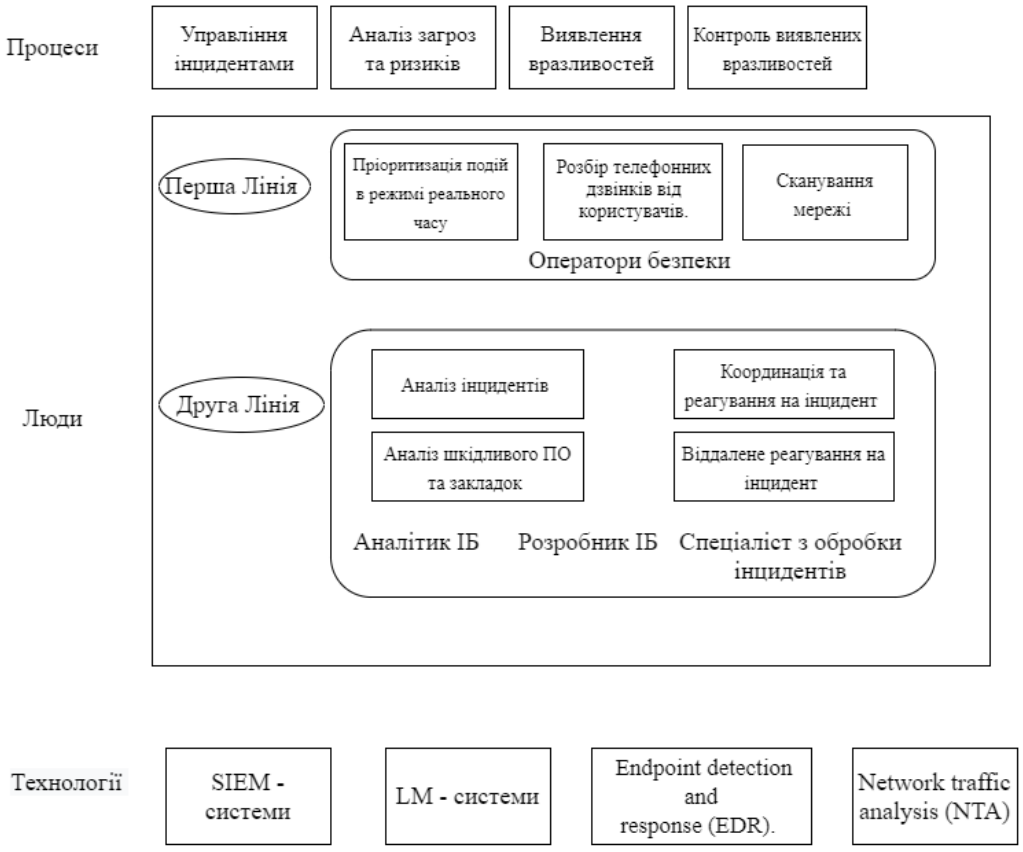

Рисунок 2.4 - Модель операційного центру безпеки

На даній моделі представленні основні компоненти SOC:

- Процеси
- Люди
- Технології

Кожна з цих складових відіграє важливу ролі у роботі SOC. Без визначених процесів аналітики не зможуть правильно організувати свою діяльність та будуть або перевищувати свої повноваження, або працювати не в повну силу.

SOC – це люди, тому немає сенсу в першокласних технологіях. Які будуть визначати інциденти, якщо не буде аналітиків, які зможуть реагувати на них та будувати подальші плани дій та аналізувати отримані дані. Цих даних навіть на малому підприємстві може налічуватися до декількох десятків в хвилину в журналах аудиту, тому навіть самий кваліфікований співробітник не має змогу в ручному режимі проаналізувати всі дані в короткий період, в такій ситуації на допомогу приходять технології, які можуть проводити моніторинг в режимі реального часу, визначати аномальну поведінку в мережі та допомагати аналітикам відтворювати та поєднувати події в один ряд, для того щоб визначити рівень загрози.

Функціональна модель SIEM-систем об’єднує такі функціональні підсистеми як [18]:

- Збір даних;
- Попередня обробка даних;
- Зберігання;
- Аналіз;
- Представлення в зрозумілому вигляді.

Зальний вигляд представлений на рисунок 2.5

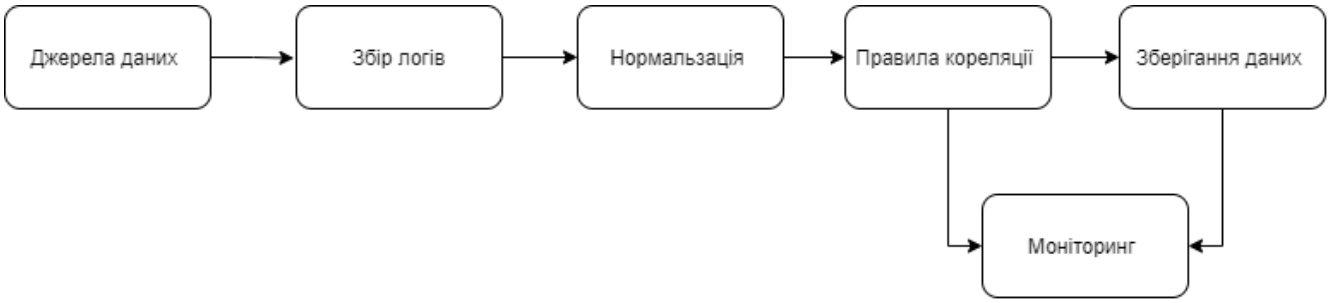

Рисунок 2.5 - Загальна послідовність обробки подій [19]

Висновки до розділу 2:

В даному розділі була розроблена модель операційного центру безпеки, операційна модель якого знаходиться в область між командою безпеки та

внутрішньо розподіленим SOC, має повні повноваження та функціонує як окрема група безпеки. Було визначено головні параметри функції та задачі SOC. Побудовано функціональну модель операційного центру безпеки та системи моніторингу подій, що полегшило розуміння системи в цілому та окремі її частини. Визначено основні механізми роботи SIEM-систем за допомогою ієрархічної моделі.

3 КЛАСИФІКАЦІЯ ДЛЯ ПІДПРИЄМСТВ ЩОДО ВИБОРУ МОДЕЛІ ОПЕРАЦІЙНОГО ЦЕНТРУ БЕЗПЕКИ

3.1 Внутрішній SOC

Насамперед слід визначити, що основний тип компаній, що будують внутрішній SOC це великі компанії. Дані компанії мають достатню кількість кваліфікованих співробітників, власні кошти та визначені задачі. Базою для операційного центру безпеки є:

- Персонал;
- Наповнення;
- Процеси;
- Ліцензії (наприклад для SIEM-систем або інших пристроїв, які використовуються у роботі).

Для вирішення питання з потужністю на підприємстві потрібно задіяти лише фінансову сферу компанії, але для вирішення питання з персоналом, процесами та наповненням потрібен не тільки гроші, але й час та сили.

На сьогоднішній день, на ринку праці для IT-спеціалістів існує великий дефіцит кандидатів високого рівня. Пошук одного ідеального кандидата загалом займає декілька місяців, а потом необхідно ще пів року для того, щоб співробітник повністю освоївся на своєму робочому місці, особливо якщо у компанії існує потреба в моніторингу в режимі 24x7. Ідеальним кандидатом є спеціаліст з досвідом роботи від 5 років, з достатньо високим рівнем англійської мови та без звички змінювати місце роботи кожні 3 роки. Такий спеціаліст отримує близько 50 пропозицій про роботу в день, що робить роботу HR-менеджера ще складнішою, а пропозиції від повинні бути компаній більш привабливими.

Наповнення та визначення процесів – камнем спотикання для побудови операційного центру безпеки та систем моніторингу подій. Наповнення SIEM-системи контентом є основною та найважливішою задачею тому, що набір правил

‘‘з коробки’’ не здатні здійснити повномасштабне реагування на інцидент, визначити потенційну вразливість або правильно побудувати ряд подій, які були зафіксовані з різних джерел подій. Для вирішення поставленої задачі, компанії необхідно мати в своєму штаті архітектора SIEM-систем, який буде налаштовувати правила в залежності від поставлених цілей, адаптувати їх під інфраструктуру та реалізовувати сценарії виявлення інцидентів.

Окрім цього, не менш важливою задачею є чітке визначення процесів та процедур, які необхідно не тільки забезпечити тим, що будуть отримані повідомлення про кожну атаку, а ще й виконання регламенту SLA.

3.2 SOC as a Service

Для великої компанії, яка має на меті побудувати внутрішній SOC, даний процес може зайняти деякий час, зазвичай цей період продовжується півтори роки. Таким чином бажання керівництва швидко побачити результат, може занапастити побудову операційного центру безпеки, тому що на збір бази знань для подальшої роботи необхідно від 6 місяців до року. Керівництво часто не готово чекати так довго. Тому у таких випадках слід звернути увагу на комерційний SOC.

SOC as a Service був розроблений, щоб допомогти в роботі з величезним обсягом інформації, моніторингом в режимі реального часу та реагуванням на атаки. Служба аналізує інформацію, аналізує дані і корелює події, при необхідності перетворюючи всю інформацію в події, що вимагають вживання заходів. При цьому компанія ефективно використовуєте внутрішні IT-служби, дозволяючи їм діяти на основі конкретної інформації з урахуванням їх місцевих особливостей найбільш ефективним чином. У регламенті визначається чіткий поділ обов’язків між замовником і підрядником.

3.3 Порівняльний аналіз критерій та вимоги для SOC as a Service та SOC

Отже, говорячи про кількість персоналу для внутрішнього SOC, то згідно з результатами опитування інституту SANS, які показані на рисунку 3.1, оптимальна кількість співробітників – 2-5.

Відсутність кваліфікованого персоналу - найбільш часта причина, яка стримує можливості SOC. Аналітик SOC повинен мати великі знання і необхідний досвід, щоб правильно інтерпретувати дані, одержувані від SIEM та інших засобів захисту, а також розуміти поведінку і розбиратися в бізнес-контексті, щоб точно встановити, що відбувається щось несанкціоноване.

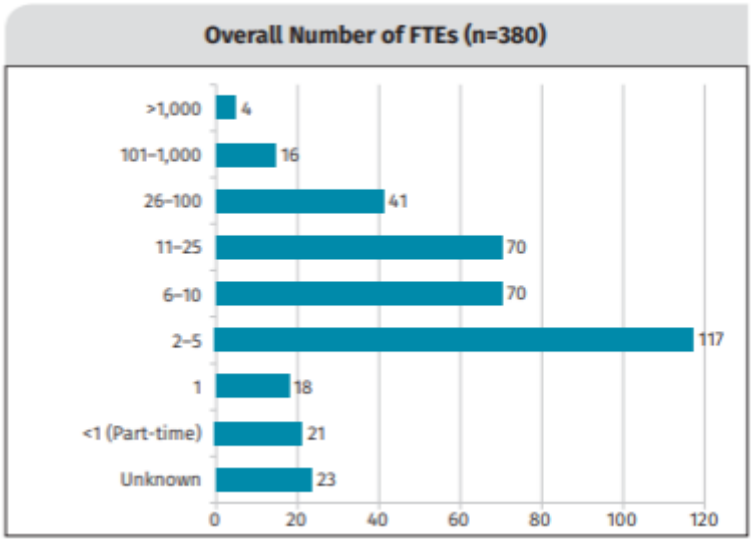

Рисунок 3.1 - Кількість співробітників на повний день

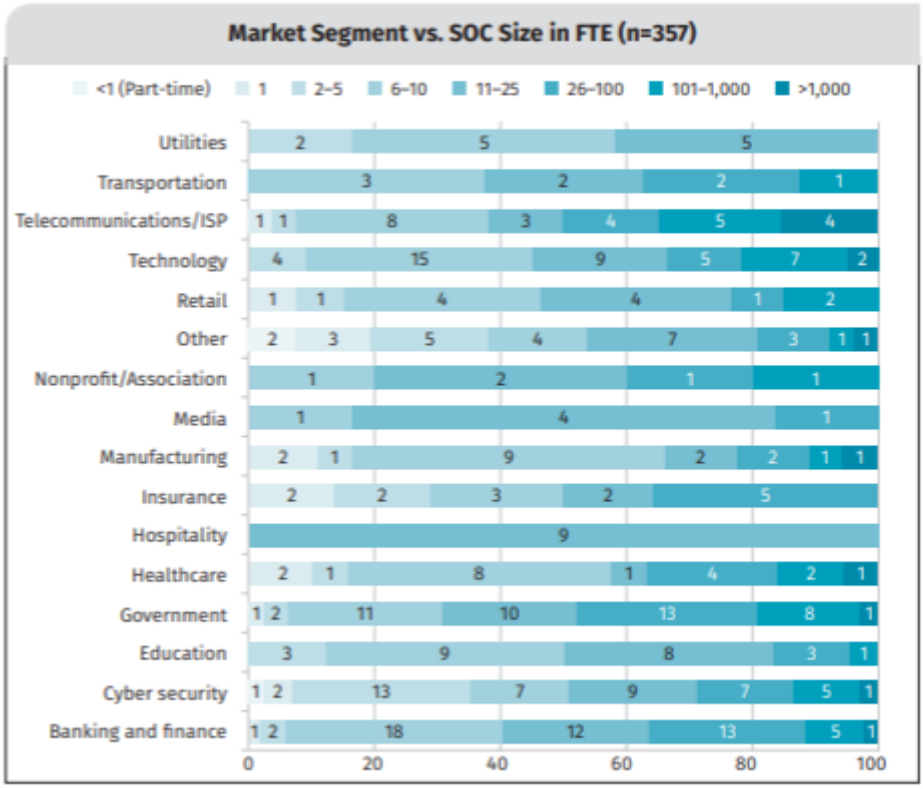

Рисунок 3.2 - Залежність штату SOC від сфери діяльності компанії

Розглядаючи сфери діяльності, можна виділити компанії, що надають послугу в сфері телекомунікацій та надання інтернет послуг. На 4-х підприємствах кількість співробітників залучених на повний день перевищую 1000. Якщо подивитися на сферу кібербезпеки, то можна побачити, що

- 1 компанія немає співробітників на повну ставку
- 2 мають лише одного
- 13 компаній штат складає 2-5 співробітників
- 7 компаній мають 6-10 співробітників
- 9 компаній мають 11-25 співробітників
- 7 компаній мають 26-100 співробітників
- 5 компаній мають 101-1000 співробітників
- 1 компанія має більше 1000 співробітників

Фактори, що впливають на розмір SOC

- Ступінь зрілості IT в компанії;
- Чутливість компанії до впливу на конфіденційність, цілісність і доступність;
- Очікування від керівництва і організації в цілому щодо швидкості та можливостей SOC;
- Вимоги з надання послуг іншим організаціям;
- Частота внесення змін до операційні системи і додатки;
- Доступний бюджет.

IT та інформаційна безпека все частіше стають споживаної послугою, тому що багато компаній намагаються обмежити розмір штату, зберігаючи власний персонал тільки на ключових бізнес-напрямки. Більшість (54% респондентів) вважають свій SOC внутрішнім постачальником послуг для своєї компанії. 53% з 102 респондентів відповіли, що використання внутрішнього SOC є обов'язковим, а 29% заявили, що можуть використовувати послуги зовнішнього SOC.

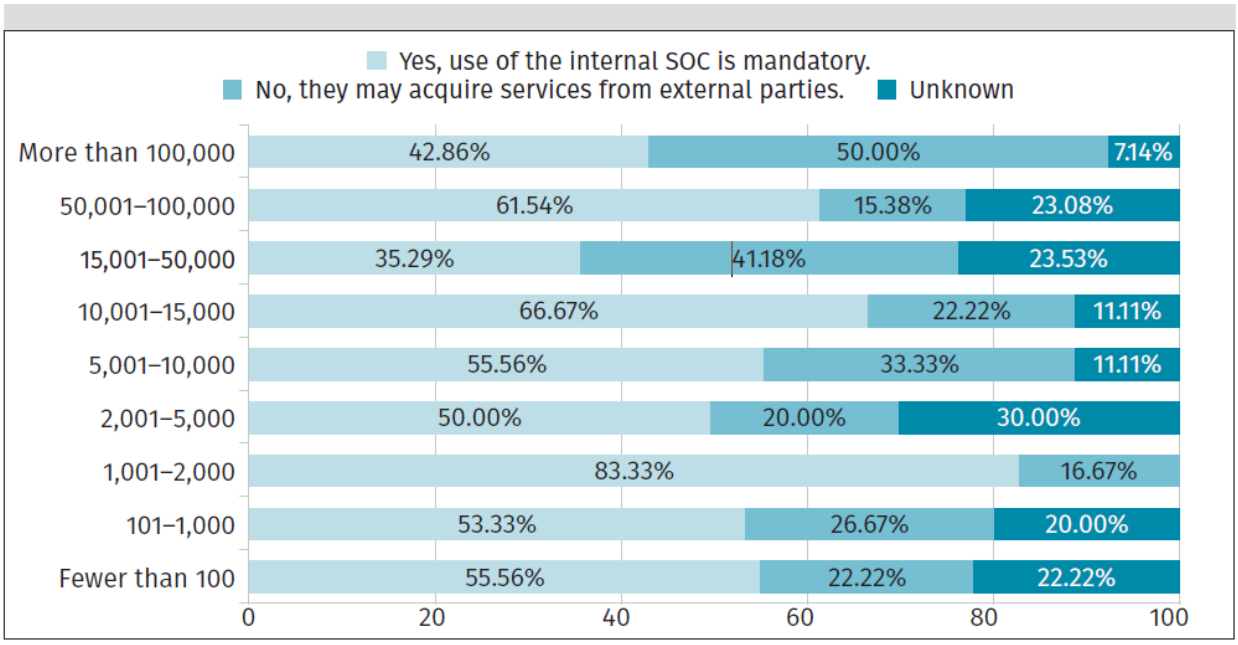

Рисунок 3.3 - Внутрішній чи зовнішній SOC

Таблиця 3.1 – Порівняльний аналіз для SOC as a Service та SOC

Критерій	SOC	SOC as a Service
Розмір організації	50 000 користувачів / IP-адрес. Обслуговують компанії з Fortune 500 і Global 2000 і великі урядові агентства.	1000 користувачів / IP-адрес. Обслуговують малий і середній бізнес, коледжі та місцеві органи влади.
Персонал	Даний SOC має вигідні умови для роботи кваліфікованого спеціаліста.	Даний SOC немає вигідних умов для роботи кваліфікованого спеціаліста.
Наповнення	Для повномасштабної робити даного виду SOC, необхідно мати великий потік трафіку, щоб наповнювати SIEM-системи контентом. У великих компаній наповнення журналу аудиту подіями починається з десятків тисяч в секунду та можуть мати високий рівень критичності, тому для даних компаній необхідно мати внутрішній SOC, який має повний доступ до всієї інформацій	У малих компаній наповнення журналу аудиту подіями досягається до сотні в секунду. Моніторингом подій займаються аутсорсингові компанії, що надають підприємству важливі витяги по даним подіям.
Ступінь важливості	Інциденти відбуваються часто та ступінь їх критичності	Інциденти відбуваються не дуже часто та ступінь їх критичності не

	достатньо висока для постійного моніторинга. При географічно розподілених організаціях великий централізований SOC може використовувати «гібридну» домовленість з окремими співробітниками на віддалених об'єктах для виконання ряду функцій з моніторингу та реагування.	достатньо висока для постійного моніторинга та необхідності будувати внутрішній SOC.

Малі підприємства, як правило, потребують SOC as a Service для виконання всіх функцій SOC, великі підприємства, як правило, використовують групи аналітиків SOC as a Service як доповнення до внутрішніх командам, в той час як організації середнього розміру зазвичай знаходяться десь посередині між цими крайнощами.

Постачальники SOC as a Service, що спеціалізуються на малих і середніх підприємствах, будуть вдосконалювати свої пропозиції, щоб забезпечити розуміння і рекомендації, які дозволять організаціям спільно управляти своєю безпекою з зовнішніми командами SOC, в той час як постачальники, орієнтовані на середні, великі і дуже великі підприємства , будуть розширювати свої можливості щодо ризиків і безпеки IoT.

Більшість великих організацій мають внутрішні SOC, в той час як компанії, що не мають персоналу або ресурсів для їх обслуговування, можуть вирішити передати деякі чи всі обов'язки SOC на аутсорсинг провайдеру керованих послуг, хмари або розміщеному віртуальному SOC.

3.4 Оцінка вартості SOC as a Service та SOC

Для оцінки витрат на побудову SOC було взято такі дані як:

1.Технічне оснащення:

1.1 SIEM-системи - Вартість ліцензій залежить від очікуваного потоку подій (розглядаємо ~ 50 джерел подій)

1.2 Інфраструктура для SIEM-системи – програмне та апаратне забезпечення, резервне копіювання, середа віртуалізації, мережеве обладнання;

2. Роботи на старті :

2.1 Витрати на впровадження технічних коштів (вартість робіт)- обстеження і проектування, впровадження та налаштування SIEM- системи,
підключення 50 джерел, розробка і реалізація правил кореляції для 30 сценаріїв виявлення інцидентів.

2.2 Витрати на ПЗ - визначення ключових ролей, термінів підключення, типових налаштувань, розробка регламенту розслідування і реагування на інциденти ІБ, розробка інструкцій оператора / аналітика / користувача.

Отже, кінцева сума для розгортання архітектури SOC буде варіюватися від 800 000 грн. на дану суму впливає вартість SIEM платформи різних виробників , трудомісткість робіт по налаштуванню, а також частину роботи по налаштуванню компанія може взяти на себе. Для подальшої оцінки була взята середня вартість в обсязі $B_{арх}$= 1 000 000 грн.

Основні витрати і організаційні складності, як правило, припадають саме на операційну частину. В першу чергу це кадрова проблема. Необхідний штат SOC залежить від масштабу підключається інфраструктури та обсягу робіт. При оцінці необхідної кількості фахівців, що займаються безпосередньо операційною діяльністю по обробці подій ІБ, потрібно орієнтуватися на планову навантаження.

Кількість спеціалістів (С) визначається як:

$$C = T / (250 * 0.7), \qquad (3.1)$$

де Т - планова трудомісткість групи,

250 - це кількість робочих днів у році 1 фахівця,

0,7 - коефіцієнт враховує 70% продуктивну завантаження фахівців (відпустки, хвороби, час на самоосвіту та ін.).

Для оцінки чисельності групи моніторингу береться очікуваний потік подій ІБ (N_i) і середній час обробки однієї події ІБ (t_i), далі розраховується загальна планова трудомісткість групи (Т):

$$T = N_i * t_i \qquad (3.2)$$

Приблизна кількість очікуваних потік подій ІБ для 50 джерел складає 2000-3500 подій в рік, середній час обробки події аналітиками складає 30 хвилин = 0.0625 людино-дня; Для знаходження показника людина-дня була використана формула:

$$Л\text{-}Д = \frac{Л}{8}, \qquad (3.3)$$

де Л-Д – показник людина-день,

Л – кількість годин витрачених на роботу(в даному випадку на аналіз однієї події),

8 – кількість робочих годин в день.

Розрахуємо максимальну планову трудомісткість групи:

$$T = 3500*0.065 = 227,5$$

Необхідна кількість спеціалістів:

$$C = \frac{227,5}{250*0.7} = 2$$

Для режиму 5х8 двох фахівця було б цілком достатньо, але при роботі в цілодобовому режим двох спеціалістів буде мало. Для складання графіка змінності з урахуванням вимог Трудового кодексу про нормативи робочого часу фахівців моніторингу і реагування доведеться наймати в кількості не менше 5.

Таким чином штат аналітиків SOC складається з

- Аналітиків першої лінії,
- Керівника SOC,
- Адміністратора SIEM,
- Інженер ІБ.

Таблиця 3.2 – Оцінка вартості штату SOC

Посада	Кількість, чол	Зарплата, грн	Загальна вартість ($В_з$), грн
Керівника SOC	1	80 000	80 000
Адміністратора SIEM	1	50 000	50 000
Інженер ІБ	1	40 000	40 000
Аналітик SOC	5	25 000	125 000
Загальна сума ($В_с$), грн			295 000

Загальна сума заробітної плати в рік для штату SOC є:

$$В_с = В_з * 12 = 295\,000 * 12 = 3\,540\,000 \text{ грн.} \quad (3.4)$$

Таким чином, загальна сума розгортання SOC буде

$$В_{впровадження} = В_с + В_{арх} = 3\,540\,000 + 1\,000\,000 = 4\,540\,000 \text{ грн.} \quad (3.5)$$

До цієї суми також додаються різні фактори вартість технічної підтримки, вартість навчання та підвищення кваліфікації співробітників, організація та обслуговування робочих місць, тощо.

Маючи загальну вартість розгортання операційного центру безпеки, слід визнчити загальну вартість володіння SOC (TCO)

$$TCO = B_{впровадження} * X, \qquad (3.6)$$

де X - термін планування, середній період впровадження складає 2 роки.

$$TCO = 4\ 540\ 000 * 2 = 9\ 080\ 000 \text{ грн}$$

Мінімальна цінова політика для послуг SOC as a Service починається від 56000 грн в місяць. Таким чином вартість послуг для SOC as a Service в рік складає:

$$B_{SIEM} = 56000 * 12 = 672\ 000 \text{ грн.} \qquad (3.7)$$

3.5 Побудова класифікації для підприємств

Насамперед, головною умовою для вибору виду операційного центру безпеки є сам розмір компанії. На основі цього вже розглядається більш детальна класифікація з урахуванням кількості та критичності подій, сферою діяльності компанії та розробкою регламентації для побудови процесів.

Згідно дослідженням Ponemon Institute, близько 70% малих і середніх підприємств зазнали кібератаки що призвело до витоку даних приблизно в 58% опитаних компаній. Експерти кажуть, що малий і середній бізнеси (SMB) стають головними мішенями для онлайн-злочинців, перш за все тому, що їм не вистачає людей, навичок, інструментів і бюджетів більш великих підприємств. Ці слабкі місця представляють собою головну мету для хакерів-зловмисників, що призводить до катастрофічних порушень, що означало кінець для 60% малих і середніх підприємств, які стали жертвами. На жаль, професіонали в галузі безпеки, які мають навички для виконання наскрізних завдань, таких як пошук загроз,

виявлення і криміналістичний аналіз, не ростуть на деревах. Це погана новина для малих і середніх підприємств, які найбільше постраждають від цього ідеального шторму - небезпечного ландшафту загроз, повного кримінальних хакерів в поєднанні з нестачею необхідних експертів для захисту цих підприємств від згаданих злочинних хакерів. Розвиток SOC as a Service може стати відповіддю для малих і середніх підприємств, які все частіше піддаються атакам.

Брак ресурсів спонукає малі і середні підприємства в сфері безпеки звертатися до SOC як послуги для боротьби з цією хвилею атак за допомогою аутсорсингу

Таблиця 3.3 – Характеристика підприємств

Розмір організації	Кількість співробітників	Характеристика
Мала	До 50	Малі і середні підприємства (SMEs (medium-sized entities) це підприємства, які: не є публічно підзвітними, і публікують фінансову звітність загального призначення для зовнішніх користувачів. Приклади зовнішніх користувачів включають власників, поки не беруть участі в управління бізнесом, існуючих і потенційних кредиторів, а також кредитні рейтингові агентства.
Середня	Від 50 до 500	
Велика	Більше ніж 500	Характерні стандартизована і складна структура і механістичний спосіб управління. Складність структури обумовлює наявність працівників різних спеціальностей. Більш того, велика організація, одного разу

		з'явившись, може стати фактором, який стабілізує ринок праці на довгі роки.

Окрім розміру підприємства слід звертати увагу на річний дохід, від нього залежать можливості компанії забезпечення SOC.

Таблиця 3.4 – Річний дохід

Розмір організації	Мала	Середня	Велика
Річний дохід	До 10 млн євро	Компанії, що можуть бути або малими або великими в залежності від своїх властивостей.	Більше 50 млн євро

На кількість персоналу впливає сфера діяльності компанії, але при розгляді різних сфер немає чіткої кореляції між специфікою та розміром компанії.

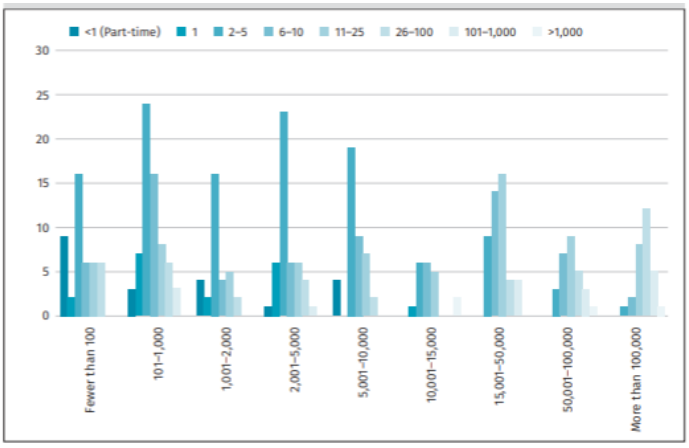

Рисунок 3.4 - Залежність штату SOC від розміру організації

Види діяльності підприємства діляться на 4 підгрупи:

- Виробництво - характеризується випуском готової продукції або сировини.
- Надання послуг - характеризується наданням різного роду допомоги замовникам. Від ремонту житла і побутової техніки, до надання послуг моніторингу безпеки.
- Інтелектуальне виробництво - випуск різного роду продуктів розумової праці. Починаючи від статей і анекдотів, і, закінчуючи серйозними дослідженнями.
- Зовнішньоекономічна діяльність - діяльність, пов'язана з впливом і впливом на зовнішній простір і конкурентів. У масштабах країни - це торгівля з іншими державами, вихід на міжнародний ринок товарів або інвестицій. У масштабах фірми - це діяльність, спрямована на надання впливу на конкурентів, за рахунок управління вторинними ознаками.

Залежно від сфери діяльності є рівень актуальності атак на підприємство.

Таблиця 3.5 - Категорії компаній

Сфера діяльності	Рівень актуальності атаки, %
Державне підприємство	16
Промисловість	15
Торгівля	7
Медична установа	7
Фінансова організація	6
IT-компанія	6
Онлайн-сервіси	5
Без прив'язки до галузі	21
Інші сфери діяльності	18

Отже, ґрунтуючись на отриманих вище факторах була побудована класифікація для різних підприємств. В даній таблиці співставленні розмір підприємства та його дохід.

Таблиця 3.6 – Критерій важливості

Розмір компанії ——————— Сфера діяльності	Мала	Середня	Велика
Державне підприємство	2	4	6
Промисловість	2	4	6
Торгівля	1	3	5
Медична установа	1	3	5
Фінансова організація	1	3	5
IT-компанія	1	3	5
Онлайн-сервіси	1	3	5

Таблиця 3.7 – Значення шкали для класифікованих підприємств

Рівень критичності	Характеристика	
	Розмір підприємства	Рівень актуальності атак, %
1	Мале	0 - 10
2	Мале	10 - 25
3	Середнє	0 - 10
4	Середнє	10 - 25
5	Велике	0 - 10
6	Велике	10 - 25

3.6 Компанії, що надають послуги операційного центру безпеки

- Information Systems Security Partners

ISSP – міжнародна компанія, що надає своїм клієнтам послуги в сфері кібербезпеки. Має офіси в Грузії, Казахстані, Канаді, Польщі та США. Компанія допомагає своїм клієнтам в різних сферах боротися з кібератаками та їх наслідками. Компанія має широкий спектр послуг починаючи від оцінки та аналізу вразливостей до моніторингу та реагування на інциденти. Обслуговує більш великі компанії з кількістю співробітників від двох до чотирьох тисяч.

- «Октава Кіберзахист»

Розрахована на клієнтів малого та середнього бізнесу, рівня SMB. В якості технологій, використовує “пастки” TrapX, що дозволяють за допомогою розгортаємої архітектури забезпечити виявлення та запобігання атакам в режимі реального часу, також використовує SIEM “Splunk”, безагентне рішення для захисту кінцевих точок Promisec Endpoint Manager та в якості детекторів використовує брандмауери Cisco.

- Infopulse

Компанія що надає аутсорсингові послуги в сфері IT в Україні. Заснована в 1991 та має представництва в декількох країнах Європи. Займається будівництвом операційних центрів безпеки у замовників та надає послуги зовнішнього SOC. Infopulse займається аналізом поведінки користувача, захистом від атак нульового дня та іншими функціями. В 2020 році увійшла в «The 2020 Global Outsourcing 100» світовий топ-100 компаній, що надають аутсорсингові послуги.

- Omega Security Service

Компанія пропонує комплексний захист мережевою інфраструктури, SOC нового покоління, захист від DOS/DDOS, сканує мережу на вразливості і випробування на проникнення, в тому числі з використанням методів соціальної інженерії. Також

компанія встановлює системи відеоспостереження та надає сервіс відеоаналітики. Крім України, компанія має офіс в Канаді.

Висновки до розділу 3

В даному розділі були розглянуті води операційного центру безпеки: внутрішній, зовнішній та гібридний. Був проведений аналіз критеріїв для SOC та SOC as a Service. Розглянуто різновиди підприємств та їх класифікації. Побудовано шкалу на основі отриманих даних для подальшої побудови класифікації

Таким чином підприємствам з критерієм важливості в діапазоні від 1 до 3 слід звернути увагу на SOC as a Service, тому що рівень атаки на компанію низький, так само як і рівень критичності інцидентів. Ризик побудови внутрішнього SOC достатньо великий, тому що річного доходу не вистачить на утримання, налаштування та впровадження SOC. Це дозволить забезпечити швидкий старт та отримати передбачувану якість послуг. Але в цьому варіанті, є чимало ризиків і про них потрібно пам'ятати, тому що залежність від постачальника послуг - 100%. Необхідно сформувати список резервних компаній, щоб максимально скоротити час на пошук нового аутсорсера, чітко сформулювати вимоги до термінів передачі і повноти документації тощо.

Для компаній з критерієм важливості від 4 до 6,навпаки невигідно залучати зовнішній SOC, так як вони потребують цілодобового моніторингу та повноти даних про подію, а зовнішні операційні центри безпеки надають витяги з події. Для таких компаній, на початковому слід звернути уваги на гібридний SOC і поетапно будувати власний організаційний центр безпеки.

ВИСНОВКИ

Дана робота аналізує фактори, що впливають на підприємства при виборі типу SOC. Під час виконання були проаналізовані моделі та типи операційних центрів безпеки, їх архітектуру та методи побудови. В результаті був побудована модель SOC та класифікаційна таблиця за допомогою якої підприємства зможуть надалі робити вибір операційного центру безпеки.

Вибір моделі SOC залежить від:

- Розміру підприємства;
- Сфери діяльності;
- Річного доходу;
- Рівня кваліфікації співробітників;
- Глобальне розташування.

Результати дослідження можуть буди використані на підприємстві під час вибору моделі операційного центру безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. What is a Security Operations Center (SOC)? [Електронний ресурс] – Режим доступу до ресурсу: https://digitalguardian.com/blog/what-security-operations-center-soc

2. Zimmerman Carson. MITRE. Ten Strategies of a World-Class Cybersecurity Operations Center. — 2014.

3. Как выявить кибератаку и предотвратить кражу денег [Електронний ресурс] – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/knowledge-base/

4. What is User and Entity Behavior Analytics? A Definition of UEBA, Benefits, How It Works, and More [Електронний ресурс] – Режим доступу до ресурсу: https://digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more

5. What Is Network Traffic Analysis [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/security/what-is-network-traffic-analysis.html

6. Behavioral Monitoring [Електронний ресурс] – Режим доступу до ресурсу: https://www.techcesscyber.com/behavioral-monitoring/

7. What is Network Detection and Response? [Електронний ресурс] – Режим доступу до ресурсу: https://www.gartner.com/reviews/market/network-detection-and-response

8. Чек-лист: проверьте, все ли «умеет» ваш SOC? [Електронний ресурс] – Режим доступу до ресурсу: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B5%D0%BA-%D0%BB%D0%B8%D1%81%D1%82:_%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D1%80%D1%8C%D1%82%D0%B5,_%D0%B2%D1%81%D0%B5_%D0%BB%D0%B8_%D1%83%D0%BC%D0%B5%D0%B5%D1%82_%D0%B2%D0%B0%D1%88_SOC#.C2.AB.D0.9F.D1.80.D0.BE.D1.86.D0.B5.D1.81.D1.81.D1.8B.C2.BB:_.D0.BA.D0.B0.D0.BA.D0.B8.D0.B5_.D0.BF.D1.80.D0.BE.D1.86.D0.B5.D1.81.D1.81.D1.8B_.D0.BD.D1.83.D0.B6.D0.BD.D1.8B_.D0.B4.D0.BB.D1.8F_.D1.8D.D1.84.D1.84.D0.B5.D0.BA.D1.82.D0.B8.D0.B2.D0.BD.D0.BE.D0.B9_.D1.80.D0.B5.D0.B0.D0.BB.D0.B8.D0.B7.D0.B0.D1.86.D0.B8.D0.B8_.D1.84.D1.83.D0.BD.D0.BA.D1.86.D0.B8.D0.B9_SOC

9. Що таке SIEM-системи і для чого вони потрібні? [Електронний ресурс] – 2017. – Режим доступу до ресурсу: https://uk.conservationdatasystems.com/2410-what-are-siem-systems-and-what-are-they-for.html

10. SIEM: ответы на часто задаваемые вопросы [Електронний ресурс] – 2013. – Режим доступу до ресурсу: https://habr.com/ru/post/172389/

11. Overcoming Common Causes for SIEM Solution Deployment Failures [Електронний ресурс] – 2017. – Режим доступу до ресурсу: https://www.gartner.com/en/documents/3732517/overcoming-common-causes-for-siem-solution-deployment-fa

12. ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами (ISO/IEC 27035-1:2016, IDT)

13. Managed Security Services (MSS), Worldwide Reviews and Ratings [Електронний ресурс] – Режим доступу до ресурсу: https://www.gartner.com/reviews/market/managed-security-services-worldwide

14. The Managed Security Services Landscape Is Changing [Електронний ресурс] – Режим доступу до ресурсу: https://blogs.gartner.com/pete-shoard/the-managed-security-services-landscape-is-changing/

15. SANS: Building a World-Class Security Operations Center: A Roadmap [Електронний ресурс] – Режим доступу до ресурсу: https://sibertor.com/wp-content/uploads/2016/07/building-world-class-security-operations-center-roadmap-35907.pdf

16. Security Operations Center Roles and Responsibilities [Електронний ресурс] – Режим доступу до ресурсу: https://www.exabeam.com/security-operations-center/security-operations-center-roles-and-responsibilities/

17. SANS: Building a World-Class Security Operations Center: A Roadmap [Електронний ресурс] – Режим доступу до ресурсу: https://www.rsa.com/en-us/offers/sans-building-a-world-class-security-operations-center

18. The Definition of SOC-cess? SANS 2018 Security Operations Center Survey (https://www.sans.org/reading-room/whitepapers/analyst/definition-soc-cess-2018-security-operations-center-survey-38570) [Електронний ресурс] – Режим доступу до ресурсу: https://www.sans.org/reading-room/whitepapers/analyst/membership/38570

19. И. В. Котенко, И. Б. Саенко, О. В. Полубелова, А. А. Чечулин, Применение технологии управления информацией и событиями безопасности для защиты

информации в критически важных инфраструктурах, Тр. СПИИРАН, 2012, выпуск 20, с. 27–56

20. DEFINITION security operations center (SOC) [Електронний ресурс] – Режим доступу до ресурсу: https://searchsecurity.techtarget.com/definition/Security-Operations-Center-SOC?_gl=1*1e1zmol*_ga*MTgyMjgyOTQ1OC4xNjIyNTgwMzY3*_ga_RRBYR9CGB9*MTYyMjU4MDM2Ni4xLjEuMTYyMjU4MDg1Mi4w&_ga=2.196789740.1301875822.1622580367-1822829458.1622580367

21. Growing Threats, Shrinking Talent Pool: Is SOC as a Service the Answer? [Електронний ресурс] – Режим доступу до ресурсу: https://www.channelfutures.com/mssp-insider/growing-threats-shrinking-talent-pool-is-soc-as-a-service-the-answer

22. Why your business needs SOC as a service [Електронний ресурс] – Режим доступу до ресурсу: https://www.computerweekly.com/opinion/Why-your-business-needs-SOC-as-a-service