МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ЦЕНТР БЕЗПЕКИ SOC: ОСОБЛИВОСТІ ЗАСТОСУВАННЯ НА ПІДПРИЄМСТВАХ ВЕЛИКОГО, СЕРЕДНЬОГО І МАЛОГО БІЗНЕСУ”

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

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

_____ Анатолій ВЕРШИГОРА

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Анатолій ВЕРШИГОРА

Керівник:
к. держ. упр., доц Тетяна МУЖАНОВА
Рецензент:

_____

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачу ВЕРШИГОРІ Анатолію Миколайовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "ЦЕНТР БЕЗПЕКИ SOC: ОСОБЛИВОСТІ ЗАСТОСУВАННЯ НА ПІДПРИЄМСТВАХ ВЕЛИКОГО, СЕРЕДНЬОГО І МАЛОГО БІЗНЕСУ"

керівник кваліфікаційної роботи Тетяна МУЖАНОВА, к. держ. упр., доц.
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. № 145.

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р.
3. Вихідні дані до кваліфікаційної роботи: кібербезпека підприємства, центр безпеки (Security Operation Center, SOC), застосування SOC на підприємствах великого, середнього і малого бізнесу.
4. Перелік питань, які потрібно розробити:
   1. Встановити основні характеристики центру безпеки (SOC), зокрема місію і функції.
   2. Проаналізувати особливості застосування SOC для великих і середніх підприємств.
   3. Дослідити засади реалізації SOC на підприємствах малого бізнесу.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	23.10.2023	
3.	Вивчення основних характеристик центру безпеки (SOC).	27.10.2023	
4.	Аналіз особливостей застосування SOC для великих і середніх підприємств.	10.11.2023	
5.	Дослідження засад реалізації SOC на підприємствах малого бізнесу.	15.11.2023	
6.	Формулювання висновків за результатами дослідження.	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	17.01.2024	

Здобувач вищої освіти _____ Анатолій ВЕРШИГОРА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Вершигора А.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "ЦЕНТР БЕЗПЕКИ SOC: ОСОБЛИВОСТІ ЗАСТОСУВАННЯ НА ПІДПРИЄМСТВАХ ВЕЛИКОГО, СЕРЕДНЬОГО І МАЛОГО БІЗНЕСУ"
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **ВЕРШИГОРА Анатолій** у кваліфікаційній роботі встановив основні характеристики центру безпеки (SOC), зокрема місію і функції; проаналізував особливості застосування SOC для великих і середніх підприємств; дослідив засади реалізації SOC на підприємствах малого бізнесу.

ВЕРШИГОРА Анатолій показав хороші теоретичні знання, вміння проводити наукове дослідження і самостійно вирішувати наукові завдання, довів володіння практичними навичками у процесі аналізу специфіки застосування SOC на підприємствах різного розміру.

Результати дослідження апробовані на Всеукраїнській науково-практичній конференції "Актуальні проблеми кібербезпеки" 2023 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **ВЕРШИГОРИ Анатолія** на позитивну оцінку та присвоїти йому кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач ВЕРШИГОРА А.М. допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

Здобувача вищої освіти ВЕРШИГОРИ Анатолія Миколайовича
На тему: ЦЕНТР БЕЗПЕКИ SOC: ОСОБЛИВОСТІ ЗАСТОСУВАННЯ НА ПІДПРИЄМСТВАХ ВЕЛИКОГО, СЕРЕДНЬОГО І МАЛОГО БІЗНЕСУ

Актуальність: В умовах інтеграції ІТ практично в усі аспекти бізнес-діяльності, що має наслідком не тільки отримання переваг, пов'язаних з доступністю та швидкістю обробки й передавання даних, автоматизацією бізнес-процесів, але й поглиблення негативних тенденцій, таких як зростання кількості кіберзагроз та ускладнення методів деструктивного впливу.

У зв'язку з цим більшість підприємств зіткнулися з нагальною потребою у комплексному і скоординованому підході до забезпечення корпоративної кібербезпеки. Сьогодні практично в усіх компаніях великого і середнього бізнесу функцію забезпечення кібербезпеки виконує центр операцій безпеки (SOC), а малі підприємства все частіше задумуються про створення власного SOC або передачу операцій кібербезпеки на аутсорсинг.

З огляду на це дослідження особливостей застосування центру безпеки SOC на підприємствах великого, середнього і малого бізнесу.

Позитивні сторони. У кваліфікаційній роботі встановлено основні характеристики центру безпеки (SOC), зокрема місію і функції; проаналізовано особливості застосування SOC для великих і середніх підприємств; досліджено засади реалізації SOC на підприємствах малого бізнесу, запропоновано .

Кваліфікаційна робота засвідчила розуміння здобувачем наукової проблеми та напрямів її вирішення, володіння методами дослідження. Здобувач опрацював достатню джерельну базу за темою, засвідчив наявність практичних знань і навичок роботи за фахом. Робота оформлена відповідно до вимог. Виклад матеріалу здійснено згідно з планом, надано практичні рекомендації.

Недоліки

Не враховує обмеження ресурсів компанії. Вартість обладнання та програмного забезпечення та персонал і навчання можуть бути значними.

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

Висновок: Кваліфікаційна робота виконана на достатньому науково-методичному рівні, заслуговує позитивної оцінки і рекомендується до захисту, а здобувач ВЕРШИГОРА Анатолій Миколайович заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Рецензент:

_____ _____
підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 75 стор.,17 рис., 2 табл., 60 джерел.

Метою роботи є дослідження особливостей застосування центру безпеки SOC на підприємствах великого, середнього і малого бізнесу.

Об'єктом дослідження є засади застосування центру безпеки SOC на підприємстві.

Предмет дослідження - особливості застосування центру безпеки SOC на підприємствах великого, середнього і малого бізнесу.

Методи дослідження. Для вирішення завдань дослідження використовувалися Офіційні документи виробників обладнання та програмного забезпечення. Ці документи містять інформацію про функціональні можливості обладнання та програмного забезпечення.

Короткий зміст роботи. Як результат у роботі встановлено основні характеристики центру безпеки (SOC), зокрема місію і функції; проаналізовано особливості застосування SOC для великих і середніх підприємств; досліджено засади реалізації SOC на підприємствах малого бізнесу.

Галузь застосування. Банківська справа та фінанси. Ці галузі є особливо вразливими до кібератак, оскільки вони обробляють великі обсяги чутливої інформації.

Сервіси. Ці галузі, такі як хостинг, хмарна інфраструктура та IT-аутсорсинг, є важливими цілями для кібератак, оскільки вони надають доступ до критичної інфраструктури.

Ключові слова : КІБЕРБЕЗПЕКА ПІДПРИЄМСТВА, ЦЕНТР БЕЗПЕКИ (SECURITY OPERATION CENTER, SOC), ЗАСТОСУВАННЯ SOC НА ПІДПРИЄМСТВАХ ВЕЛИКОГО, СЕРЕДНЬОГО І МАЛОГО БІЗНЕСУ.

ABSTRACT

Textual part of the qualification work for obtaining the degree of Master: 75 pages, 17 figures, 2 tables, 60 sources.

The purpose of the work is to study the features of the application of the SOC security center in large, medium and small businesses.

The object of the study is the principles of application of the SOC security center at the enterprise.

The subject of the study is the features of the application of the SOC security center in large, medium and small businesses.

Research methods. To solve the research problems, the Official documents of the manufacturers of equipment and software were used. These documents contain information about the functional capabilities of equipment and software.

Cybersecurity reference materials. These materials contain information about modern cyber threats and methods of their detection and blocking.

Practical experience in cybersecurity.

Short content of the work. As a result of the work, the basic characteristics of the security center (SOC) were established, including the mission and functions; the features of the application of SOC for large and medium-sized enterprises were analyzed; the principles of implementation of SOC in small businesses were investigated.

Field of application. Banking and finance. These industries are particularly vulnerable to cyberattacks as they process large amounts of sensitive information.

Services. These industries, such as hosting, cloud infrastructure, and IT outsourcing, are important targets for cyberattacks as they provide access to critical infrastructure.

Keywords: ENTERPRISE CYBERSECURITY, SECURITY CENTER (SECURITY OPERATION CENTER, SOC), APPLICATION OF SOC IN LARGE, MEDIUM AND SMALL BUSINESSES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ADS	Anomaly Detection System
AI	Artificial Intelligence
APT	Advanced Persistent Threat
CIO	Chief Information Officer
CRM	Customer Relationship Management
DLP	Data Leakage Prevention
EDR	Endpoint Detection and Response
ERP	Enterprise Resource Planning
HRM	Human Resource Management
IAM	Identity and Access Management
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ITOPS	Information Technology Operations and Security
ML	Machine Learning
NTA	Network Traffic Analysis
SaaS	Security as a Service
SA&T	Security Awareness and Training
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operation Center
TTP	Tactics, Techniques and Procedures
UBA	User Behavior Analytics
UEBA	User and Entity Behavior Analytics

ВСТУП

Актуальність теми. В умовах інтеграції ІТ практично в усі аспекти бізнес-діяльності, що має наслідком не тільки отримання переваг, пов'язаних з доступністю та швидкістю обробки й передавання даних, автоматизацією бізнес-процесів, але й поглиблення негативних тенденцій, таких як зростання кількості кіберзагроз та ускладнення методів деструктивного впливу.

У зв'язку з цим більшість сучасних підприємств зіткнулися з нагальною потребою у комплексному і скоординованому підході до забезпечення корпоративної кібербезпеки, одним із найважливіших елементів якого є операції з кібербезпеки: моніторинг, аналіз, реагування та відновлення після кібератак.

Оперативним координаційним центром із забезпечення кібербезпеки підприємства є центр операцій безпеки (Security Operation Center, SOC), який сьогодні є практично у всіх компаніях великого і середнього бізнесу, а малі підприємства все частіше задумуються про створення власного SOC або передачу операцій кібербезпеки на аутсорсинг.

З огляду на зазначене дослідження особливостей застосування центру безпеки SOC на підприємствах великого, середнього і малого бізнесу є актуальним науковим завданням.

Метою роботи є дослідження особливостей застосування центру безпеки SOC на підприємствах великого, середнього і малого бізнесу.

Об'єктом дослідження є засади застосування центру безпеки SOC на підприємстві.

Предмет дослідження - особливості застосування центру безпеки SOC на підприємствах великого, середнього і малого бізнесу.

Для досягнення цієї мети в роботі необхідно виконати наступні *завдання:*

1. Встановити основні характеристики центру безпеки (SOC), зокрема місію і функції.

2. Проаналізувати особливості застосування SOC для великих і середніх підприємств.

3. Дослідити засади реалізації SOC на підприємствах малого бізнесу.

Методи дослідження. Для вирішення завдань дослідження використовувалися Офіційні документи виробників обладнання та програмного забезпечення. Ці документи містять інформацію про функціональні можливості обладнання та програмного забезпечення.

Довідкові матеріали з кібербезпеки. Ці матеріали містять інформацію про сучасні кіберзагрози та методи їх виявлення та блокування.

Наукова новизна одержаних результатів. Наукова новизна дипломної роботи "Центр безпеки SOC: особливості застосування на підприємствах середнього та великого бізнесу" полягає в дослідженні та вивченні нових аспектів застосування SOC на підприємствах цільового розміру. Дослідження включає в себе аналіз впливу сучасних технологій, таких як штучний інтелект та машинне навчання, на функціонування SOC та можливість підвищення рівня безпеки. Також робота порівнює ефективність та результативність SOC на підприємствах різних розмірів, виявляючи різниці у їхньому впровадженні та функціонуванні. Крім того, вона спрямована на розробку практичних рекомендацій для підприємств середнього та великого бізнесу з метою покращення їхньої безпеки та ефективності в галузі кібербезпеки. Ці аспекти роблять важливий внесок у розвиток знань у сфері кібербезпеки та ролі SOC на підприємствах.

Практичне значення одержаних результатів. Банківська справа та фінанси. Ці галузі є особливо вразливими до кібератак, оскільки вони обробляють великі обсяги чутливої інформації.

Сервіси. Ці галузі, такі як хостинг, хмарна інфраструктура та IT-аутсорсинг, є важливими цілями для кібератак, оскільки вони надають доступ до критичної інфраструктури.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», жовтень 2023 року.

РОЗДІЛ 1.
ОСНОВНІ ХАРАКТЕРИСТИКИ ЦЕНТРУ БЕЗПЕКИ (SOC)

1.1 Сутність і місія SOC

Забезпечення конфіденційності, цілісності та доступності сучасного цифрового підприємства є важким завданням, виконання якого охоплює багато паралельних і пов'язаних зусиль, від розробки надійних систем до ефективної політики кібербезпеки й комплексного навчання персоналу. Одним із найважливіших елементів є операції з кібербезпеки: моніторинг, аналіз, реагування та відновлення після всіх кібератак.

Центр операцій безпеки (Security operation Center, SOC) є оперативним координаційним центром для виявлення, аналізу й реагування на інциденти кібербезпеки. Практично всі середні й великі компанії мають SOC різної форми, а їхня важливість зростає, оскільки кібербезпека стає все більш невід'ємною частиною будь-якої організації, включаючи комерційні й некомерційні підприємства, державні та наукові установи.

Поява SOC і зростання їх ролі були викликані низкою чинників, серед яких:

• зростання числа розширених постійних загроз (APT) [1] і прискорення розвитку тактики, техніки і процедур кіберзлочинців;

• цифрова трансформація, тобто інтеграція IT практично в усі аспекти бізнес- та урядової діяльності, включаючи ті, що традиційно не пов'язані з комп'ютерами;

• розмивання організаційних меж підприємства з появою як мобільних, так і хмарних обчислень, включаючи раптовий перехід до віддаленої роботи і роботи з дому внаслідок глобальної пандемії COVID 19;

• інтеграція й поширення нетрадиційних IT, наприклад із вбудованими обчислювальними засобами та системами промислового управління (Industrial

Control Systems ICSs) / системами диспетчерського контролю та збору даних Supervisory Control and Data Acquisition (SCADA);

• перехід від мережевих атак переповнення буфера до атак на боці клієнта;

• зростання ролі кібербезпеки до першочергової, визнання керівниками галузевих вертикалей і в усьому світі важливості кібербезпеки для бізнес-операцій та інтеграції кібербезпеки в корпоративне управління ризиками [2].

SOC - це команда, яка складається переважно з фахівців з кібербезпеки, організована для запобігання, виявлення, аналізу, реагування та звітування інциденти кібербезпеки. SOC виконує централізовану функцію в організації, яка використовує людей, процеси та технології для постійного моніторингу й покращення стану безпеки організації, одночасно запобігаючи, виявляючи, аналізуючи та реагуючи на інциденти кібербезпеки [3]. Відповідно до визначення Комітету систем національної безпеки (CNSS) це є функція кіберзахисту (Cyber Defense) [4].

SOC можуть бути таких типів:

• центр, який забезпечує виконання невеликих операцій із лише декількома фахівцями, кожен з яких працює неповний робочий день;

• центр, де кожен член команди «робить усе»;

• національний (або корпоративний) координаційний центр із сотнями аналітиків і служб реагування, де кожна особа зазвичай виконує дуже спеціалізовану роль.

Основною місією SOC є виявлення потенційних кіберзагроз і реагування на них. Це включає розуміння того, як SOC переходить від обізнаності про загрози до реагування на них, а також розуміння того, як знання супротивника формує ці дії.

Типова місія SOC середнього розміру зазвичай включає такі елементи (Рис. 1.1):

• Запобігання інцидентам кібербезпеки за допомогою профілактичних заходів, зокрема:

◦ Постійний аналіз загроз

◦ Сканування на вразливості

◦ Розгортання скоординованих контрзаходів

◦ Консультації щодо політики та архітектури безпеки

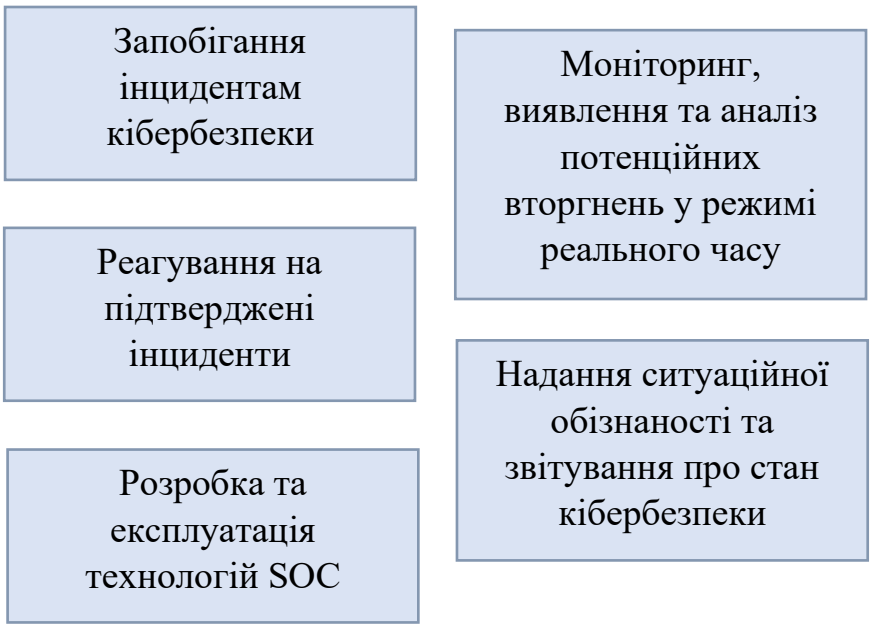

Рис. 1.1 Елементи типової місії SOC

• Моніторинг, виявлення та аналіз потенційних вторгнень у режимі реального часу та шляхом пошуку зловмисників із використанням різноманітних джерел даних, що стосуються безпеки

• Реагування на підтверджені інциденти шляхом координації ресурсів і вказівок щодо використання своєчасних і відповідних контрзаходів

• Надання ситуаційної обізнаності та звітування про стан кібербезпеки, інциденти та тенденції в поведінці противника для відповідних організацій

• Розробка та експлуатація технологій SOC, таких як головні датчики, мережеві датчики, системи збору журналів і аналізу [2, 5].

Місію SOC також можна розглядати з точки зору інфраструктури та даних, які SOC захищає. Так, функціонування SOC невеликої компанії буде спрямоване лише на наявні локальні цифрові активи й дані. Однак для команд більшості SOC їхні обов’язки також включатимуть моніторинг, виявлення й реагування на потенційні інциденти у віддалених системах, системах і даних у хмарі та мобільній інфраструктурі групи. Деякі SOC також можуть інтегрувати моніторинг і захист операційних технологій (OT) у місію SOC. Загалом, SOC

може відповідати за багато різних аспектів безпеки: IT (локальні та віддалені), операційні технології, хмара та мобільні пристрої.

1.2 Функції SOC

SOC задовольняє потреби групи в кібермоніторингу і захисті, виконуючи комплекс таких функцій, розподілених за категоріями [2] (Рис. 1.2) . Водночас, варто зауважити, що, зазвичай, не всі функції знаходять своє місце в конкретному SOC. Кожна організація обирає перелік функцій, який забезпечить досягнення обраних нею цілей кібербезпеки і відповідає організаційним можливостям.

Крім цього при виборі функцій необхідно звернути увагу на таке:

• Категорія функцій «Управління вразливостями» включена до цього списку послуг для повноти. Хоча в багатьох організаціях є окрема команда, яка виконує окремі або всі ці функції. Водночас, в багатьох компаніях ці обов’язки покладаються на фахівців власне SOC.

• Функціональна сфера «Симуляція й оцінювання атак» включає тестування на проникнення (Pentesting). Однак тестування на проникнення нерідко тісно пов’язане з програмою управління вразливостями й може здійснюватися фахівцями, відповідальними за функції віртуальної машини, якщо вони не є членами команди SOC.

• Такі функціональні сфери, як «Ситуаційна обізнаність і комунікація», «Метрики», «Навчання» та «Вдосконалення процесів», як правило, будуть включені до виконання багатьох інших сервісів. Їх називають унікальними функціональними сферами, щоб показати необхідність створення механізму для інтеграції цих зусиль у SOC.

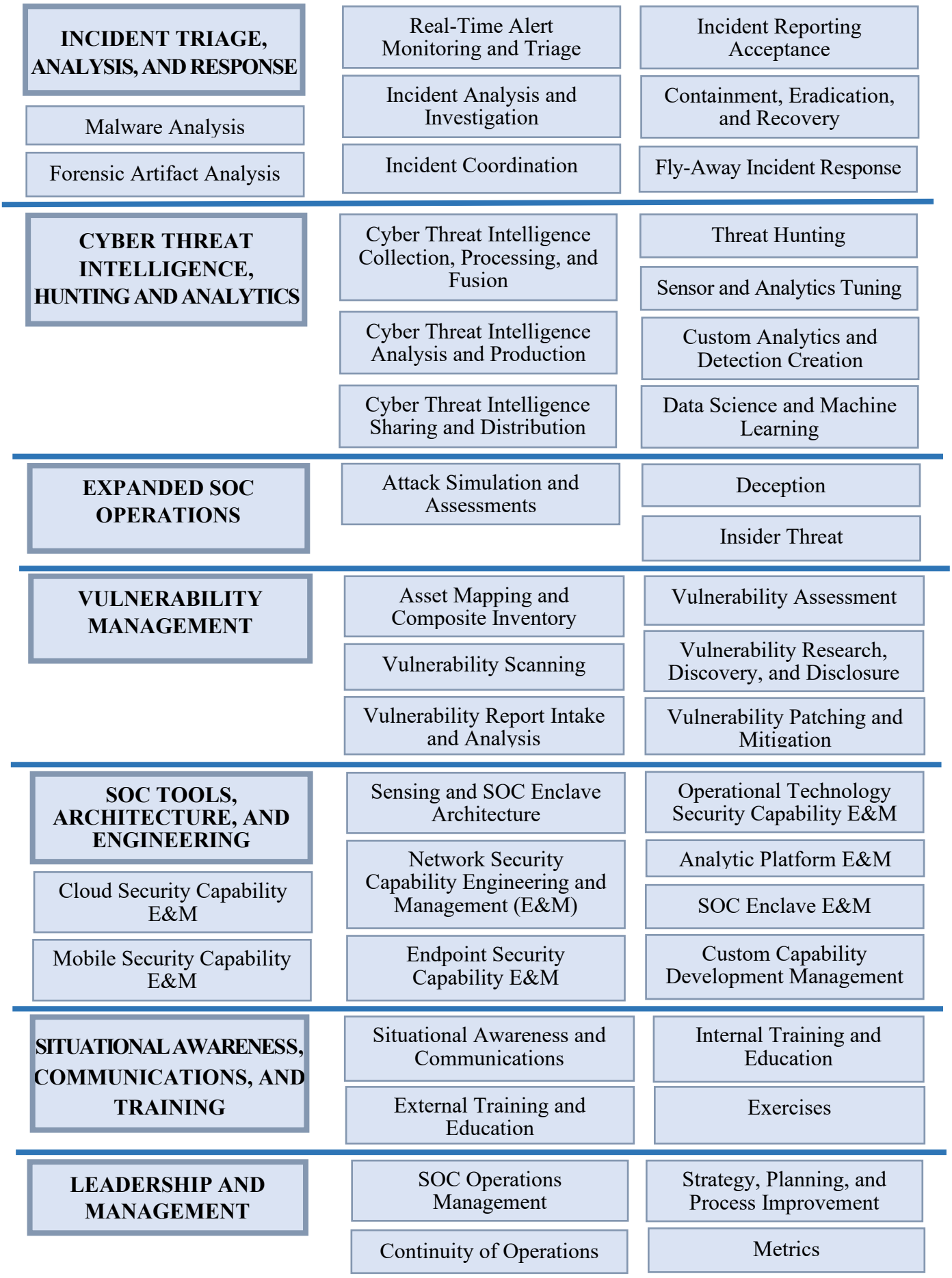

Рис. 1.2 Функції SOC

• «Архітектура безпеки, розробка й адміністрування» включають розгортання й управління для різних технічних середовищ. Як і в інших функціональних сферах, не всі середовища можна застосувати до всіх SOC. Крім того, з часом можуть з'явитися нові середовища.

• Функція «Внутрішні загрози» зазвичай поєднує фізичну безпеку, обізнаність персоналу та принципи, орієнтовані на інформацію [6]. Залежно від запитів організації SOC може відігравати більшу чи меншу роль у виявленні цієї загрози та захисті від неї.

З'ясуємо сутність окремих функцій у рамках категорій.

Категорія «*Сортування, аналіз і реагування на інциденти*» включає функції:

Моніторинг і сортування сповіщень у режимі реального часу, що передбачає виконання сортування й короткочасного аналізу потенційних інцидентів безпеки, створених за допомогою каналів сповіщень безпеки практично в реальному часі.

Прийняття повідомлень про інциденти, в рамках якого аналітики отримують і обробляють звіти про потенційні інциденти безпеки від учасників, інших SOC та третіх сторін. Ці звіти можуть надходити в письмовій (наприклад, електронною поштою) або в усній формі.

Аналіз і розслідування інцидентів передбачає виконання поглибленого детального аналізу підозрюваних інцидентів, зокрема визначення таких деталей, як походження, масштаби й наслідки інциденту, а також перевірку достовірності цих висновків.

У межах функції стримування, ліквідації наслідків та відновлення після інцидентів фахівці SOC впроваджують заходи щодо стримування інциденту або зловмисника, управління збитками, видалення зловмисника й відновлення системи для зменшення поточного впливу й переходу до стану, в якому створено умови для запобігання майбутнім інцидентам.

Координація інцидентів включає збір і розповсюдження інформації, а також оповіщення на підтримку поточного інциденту. Крім цього обов'язковим є управління й координація процесів реагування у партнерстві з аналітиками

власного SOC, зацікавленими сторонами реагування на інциденти, іншими SOC та третіми сторонами.

Криміналістичний аналіз доказів передбачає вивчення зразків носіїв інформації і цифрових артефактів (жорстких дисків, файлів, пам'яті) для детальних спостережень і висновків щодо підозрілої діяльності, наприклад аналіз вмісту та реконструкція часової шкали.

Аналіз зловмисного програмного забезпечення має на меті зрозуміти походження, родовід, функції та призначення підозрілих зразків зловмисного програмного забезпечення через вивчення підозрілих файлів. Для цього використовують різні методології, в тому числі статичного зворотного проектування коду й динамічного аналізу часу виконання [7].

У ході реагування на віддалені (Fly-Away) інциденти застосовують інструменти, процедури та механізми координація для швидкого переміщення й надання послуг реагування на інциденти на місці його виникнення, де аналітики SOC зазвичай не перебувають.

До категорії «*Розвідка, пошук і аналітика кіберзагроз*» [8] відносять такі функції:

Аналітики SOC забезпечують збір, обробку й інтеграцію даних про кіберзагрози, отриманих у результаті пошуку й розвідки загроз. Така інформація має містити відомості про канали отримання даних і звіти. Необхідним є також обробка й інтеграція даних розвідки загроз у системи SOC, аналіз і фільтрація інформації для її подальшого використання SOC та його підрозділами.

Аналіз і формування систематизованої інформації про кіберзагрози включає використання аналітичних методів для відстеження, визначення тенденцій і кореляції поведінки зловмисника з плином часу та підтримки прийняття рішень про ризик. Це включає створення звітів за результатами аналізу загроз з описом конкретних об'єктів атак, їхніх тактик, методів і процедур - TTP [9] і кампаній. Це може включати використання платформи аналізу кіберзагроз або інших інструментів для покращення аналізу.

Обов’язковою функцією SOC є забезпечення обміну й розповсюдження інформації про кіберзагрози, зокрема даними розвідки загроз і звітами про інциденти, зі партнерами організації, іншими SOC і ширшою спільнотою у галузі кібербезпеки.

Пошук загроз (Threat Hunting) передбачає здійснення профілактичних операцій для виявлення потенційно зловмисної діяльності поза межами встановлених сповіщень SOC, заснованих на гіпотезах про те, що зловмисник діє в найближчому для організації оточенні або проти неї [8]. Ця функція включає також розробку та вдосконалення власних аналітичних можливостей SOC.

Функція налаштування датчиків і аналітики має на меті здійснення контролю, налаштування й оптимізації засобів виявлення підозрілих подій, аналітики, сигнатур, правил кореляції і реагування, що використовуються в системах виявлення та аналітики SOC, таких як EDR, SIEM і SOAR.

Створення системи виявлення й аналітики інцидентів, адаптованої під потреби організації, має забезпечити використання знань про TTP і системи, що використовуються зловмисниками, для глибокого розуміння й ефективного виявлення різноманітної активності в датчиках і аналітичних системах SOC.

Використання методів і засобів науки про дані і машинного навчання необхідні для підтримки функцій SOC, зокрема побудови індивідуальних моделей машинного навчання, адаптованих до місії SOC.

У межах категорії «*Розширені операції SOC»* реалізуються такі функції:

Симуляція й оцінювання атаки передбачає діяльність т.зв. «червоних команд» (Red team), які збирають інформацію про цілі атаки, шукають актуальні вектори атак і вразливостей, експлуатують вразливості; формують відповідну звітність [10], тестування на проникнення, емуляцію противника і власне симуляцію атак, діяльність фіолетової команди, яка поєднує наступальну й оборонну тактику для виявлення, оцінювання та пом’якшення ризиків безпеці [11], а також інші види тестування з метою покращення операцій та загальної оборонної позиції команди SOC.

Використання технологій введення в оману (Deception), які є прийнятними засобами в арсеналі аналітиків SOC, включають здійснення заходів з метою приховування мереж і активів, створення невизначеності та плутанини, дезорієнтуючого впливу на зловмисника, що матиме наслідком хибне сприйняття ним реальної ситуації та прийняття неправильних рішень [12].

Запобігання і протидія внутрішнім загрозам передбачає підтримку заходів виявлення, аналітики та розслідувань, зосереджених на виявленні зловмисних або аномальних дій, які здійснюються користувачами з авторизованим доступом до систем організації.

У рамках великої категорії «*Управління вразливостями*» здійснюються такі функції:

Класифікація активів та їх загальна інвентаризація, які мають на меті збір і контроль інформації про активи, мережі та сервіси організації, відображення їх взаємозалежностей і обчислення критичності та ризиків.

Сканування вразливостей є важливим завданням команди SOC і включає перевірку активів організації щодо статусу вразливості, в тому числі рівня виправлення і встановленого програмного забезпечення, а також важливої для безпеки конфігурації з метою розрахунку ризиків безпеки і статусу відповідності нормативним вимогам.

Оцінювання вразливостей є здійсненням систематичної перевірки інформаційної системи або продукту для визначення адекватності заходів безпеки, виявлення недоліків безпеки, надання даних, на основі яких можна передбачити ефективність запропонованих заходів безпеки, і підтвердження адекватності таких заходів після їх впровадження [13].

Прийняття й аналіз звіту про вразливості входить у функціонал фахівців SOC і передбачає отримання, сортування й аналіз звітів про вразливості від дослідників уразливостей, щоб зрозуміти їх і знайти засоби пом’якшення для продуктів або активів компанії.

У рамках функції дослідження, виявлення та розкриття вразливостей здійснюється проактивне виявлення вразливостей безпеки, які раніше не були

відомі SOC (наприклад, «вразливість нульового дня»), шляхом аналізу внутрішніх інцидентів, збору даних про кіберзагрози і зворотного проектування програмного забезпечення. Ця діяльність також включає обмін інформацією про вразливості з постачальниками, іншими SOC, підрозділами організації, щоб вони могли діяти на основі цієї інформації.

Виправлення і пом'якшення вразливостей безпеки відбувається шляхом застосування патчів або зменшення ризику використання вразливості внаслідок мінімізації впливу вразливостей, таких як зміни конфігурації системи або служби, на самих зловмисників.

Наступна категорія «*Інструменти, архітектура й інженерія SOC*» містить такі функції:

Створення інтегрованої архітектури SOC відбувається шляхом визначення її складових для середовищ виявлення, аналітики та функціонування SOC, включаючи інтеграцію між різними компонентами і планування управління даними. Це може включати оцінку комерційних продуктів для використання за призначенням.

Інженерія й управління мережевою безпекою включає створення, розгортання, експлуатацію та підтримку можливостей виявлення та захисту мережевих і корпоративних служб, включаючи брандмауери, проксі браузера та електронної пошти, фільтри контенту. Також ця функція включає створення і підтримку з’єднань і потоків даних, які поєднують технічні засоби та дані.

Інженерія й управління можливостями захисту кінцевих точок, в межах якої здійснюється розробка, розгортання, експлуатація та підтримка інструментів виявлення та захисту кінцевих точок, таких як EDR, а також створення і підтримка з’єднань і потоків даних, які з’єднують інструменти та дані. Варто зауважити, що кінцевою точкою є будь-який віддалений обчислювальний пристрій, який підключений і взаємодіє з мережею, наприклад ПК, ноутбук, смартфон, планшет, сервер, робоча станція, пристрій IoT [14], що визначає великий фронт роботи для фахівців SOC.

Інженерія й управління можливостями хмарної безпеки передбачає розробку, розгортання, експлуатацію та підтримка можливостей хмарного виявлення та захисту, таких як CASB – програмне рішення, яке виступає у якості посередника між користувачами й постачальниками хмарних послуг [15] та інших хмарних інструментів, які захищають хмарні служби, а також з'єднань і потоків даних, які з'єднують інструменти та дані.

Інженерія й управління можливостями мобільної безпеки охоплює розробку, розгортання, експлуатацію і підтримку можливостей виявлення й захисту корпоративних і кінцевих точок для мобільних пристроїв, а також створення й підтримку з'єднань і потоків даних, які з'єднують інструменти й дані.

Інженерія й управління можливостями безпеки операційних технологій - розробка, розгортання, експлуатація та підтримка можливостей кібервиявлення та захисту для оперативних технологій, а також створення та підтримку з'єднань і потоків даних, які з'єднують інструменти та дані.

Інженерія й управління аналітичною платформою є комплексом заходів із розробки, розгортання, експлуатації та підтримки платформ SIEM, SOAR, CTI, UEBA, Big Data Platform та інших технологій, а також з'єднань і потоків даних, які з'єднують інструменти та дані.

Інженерія й управління анклавами (розмежованими середовищами) SOC

Розгортання, експлуатація та підтримка технологій поза межами функціоналу SOC і сенсорів, які підтримують операції SOC, включаючи дослідницькі середовища, сервери, робочі станції, принтери, спільні файли та системи розмежованих мереж.

Розвиток можливостей/потужностей, адаптованих під запити конкретної організації, зокрема створення власних інструментів і систем, необхідних для виконання різноманітних вимог SOC, коли жодна відповідна комерційна чи відкрита можливість не відповідає потребам.

До категорії «*Ситуаційна обізнаність, комунікація та навчання*» відносять такі функції:

Формування ситуаційної обізнаності й комунікація, що мають на меті узагальнення та перерозподіл знань SOC про активи, ризики, загрози, інциденти та вразливі місця для окремих підрозділів та організацію загалом, покращення стану та практики кібербезпеки. Взаємодія з зацікавленими сторонами компанії та іншими організаціями для надання й обміну інформацією, налагодження співпраці.

Внутрішнє навчання та розвиток персоналу включає збір, формулювання та проведення тренінгів для аналітиків SOC, щоб підвищити їхні знання у функціональних сферах SOC.

Зовнішнє навчання та розвиток фахівців SOC передбачає збір, формулювання та проведення тренінгів із залученням спеціалістів і тренерів зі сторонніх навчально-тренінгових центрів, щоб розширити знання команди аналітиків з більш широких питань кібербезпеки.

Проведення практичних занять і вправ, що базуються на сценаріях, означає моделювання реальної ситуації, наприклад, виявлення загрози чи реалізації кіберінцидента, в нестресовому симуляційному середовищі, для надання учасникам можливостей отримати практичний досвід за фахом [16].

Остання категорія «*Лідерство й управління*» об’єднує функції, безпосередньо пов’язані з управлінням безпекою, зокрема:

Здійснення операційного управління SOC, тобто виконання повсякденних функцій управління SOC, включаючи управління фінансами та персоналом.

Впровадження стратегії SOC, планування та вдосконалення процесів її реалізації - визначення майбутнього стану SOC і спрямування організації до цих результатів. Ця функція також включає аналіз попереднього досвіду і виявлення недоліків для внесення покращень, оцінювання поточного стану і виявлення нових можливостей.

Забезпечення безперервності операцій досягається за рахунок розробки й оцінювання планів діяльності SOC з метою підтримання місії організації і бізнес-процесів під час і після інцидентів.

Розробка і використання метрик є засобом визначення, вимірювання та звітування щодо ключових показників ефективності операційних процесів SOC, результатів операцій та ситуаційну обізнаність у межах SOC та організації загалом.

1.3 Еволюція центрів безпеки

Під час третьої промислової революції поширення цифровізації та широке проникнення Інтернету спричинили появу нових викликів і породили нові форми атак, яких раніше не існувало. Це охоплювало шкідливі віруси, експлойти нульового дня, DDoS-атаки тощо.

У відповідь на ці зростаючі загрози виникла потреба в комплексній централізованій інфраструктурі безпеки для моніторингу, аналізу й реагування на виникаючі інциденти. Цей попит призвів до створення центрів операційної безпеки SOC, які спочатку використовувалися для цілей захисту і сприяли централізованому моніторингу, обробляли попередження про віруси та протидіяли спробам вторгнення. Оснащені традиційними технологіями, ці центри переважно користувалися аналізом на основі сигнатур.

По мірі трансформації ландшафту кібербезпеки SOC довелося розвиватися та включати передові інструменти для моніторингу операцій безпеки, наприклад рішення SIEM. Ці доповнення зміцнили їхні захисні можливості від загроз APT і дозволили їм аналізувати різні види зловмисного програмного забезпечення. Крім того, SOC адаптували для виконання нормативних вимог динамічної галузі кібербезпеки.

SOC почали створювати в середині 70-х років і створювали в основному для оборонних організацій, які зосереджувалися на шкідливому коді з низьким рівнем впливу.

У 90-х роках SOC почали з’являтися на комерційних підприємствах. Оскільки технології та Інтернет зростали разом із шкідливими вірусами, DDOS-атаками та арміями бот-мереж, наступне покоління породило такі можливості, як виявлення та запобігання вторгненням. Тоді функція SOC включала регулятивну діяльність та діяльність із забезпечення нормативної відповідності [17].

Приблизно у 2007 році спостерігався ріст APT «низьких і повільних», які призвели до ексфільтрації даних (несанкціонованого передавання даних за межі організації вручну або за допомогою зловмисного програмного забезпечення [18]). Приблизно тоді система управління інформацією та подіями безпеки (SIEM) стала центральною технологією, яка збирала журнали, інтегрувала IT та генерувала сповіщення на основі визначених правил. Пройшло кілька років, і кіберпрофесіонали почали використовувати розвідку загроз разом із евристичними методами, щоб увімкнути попередні індикатори компрометації.

Створення та управління SOC сьогодні є жорстким процесом із розширенням поверхні атак, впровадженням хмарних технологій, врахування геополітичних ризиків, складністю сторонніх розробників і ланцюжків поставок, розширенням переліку інструментів і браком кадрів. Глобальні інциденти продовжують підкреслювати швидко мінливий ландшафт загроз, що створює підвищений цифровий/кібернетичний ризик.

Отже, реагуючи на розвиток всесвітньої мережі Інтернет та паралельне зростання загроз кіберзлочинності, SOC формувався поступово, і його еволюцію умовно розділять на чотири покоління [19] (Рис. 1.3).

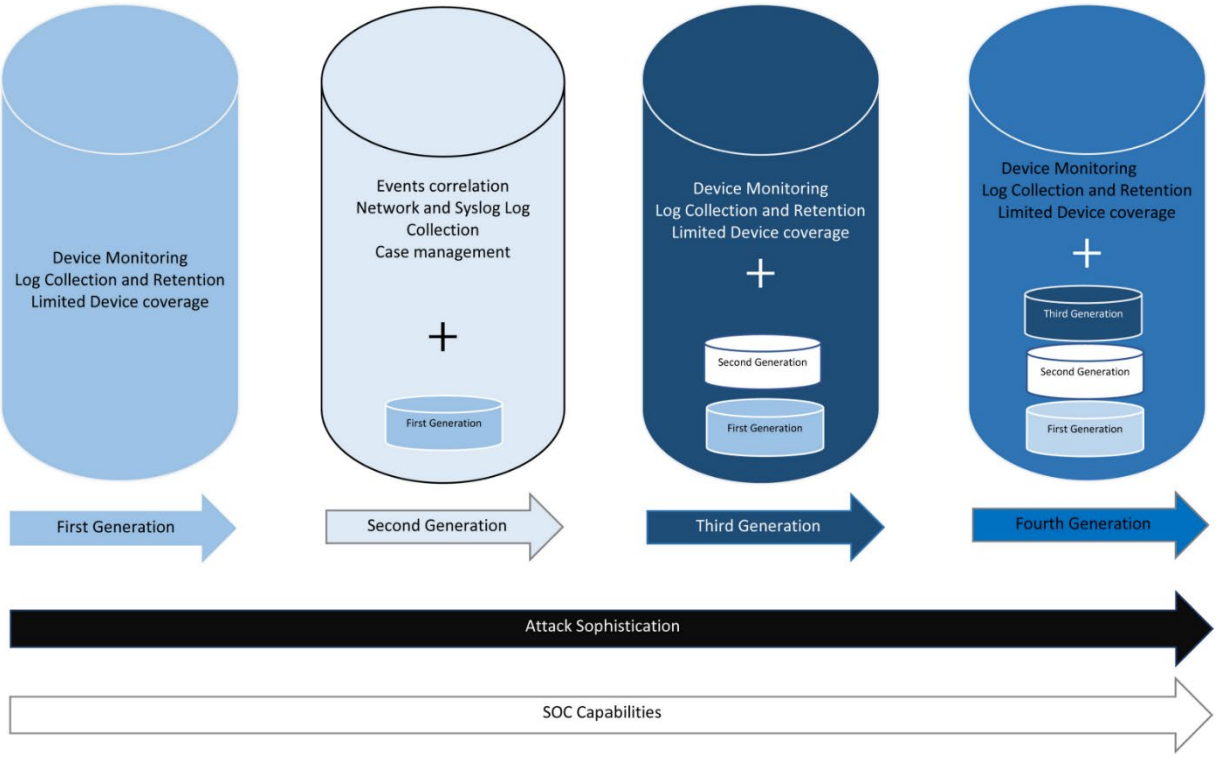

Рис. 1.3 Чотири покоління SOC

SOC першого покоління

У першому поколінні SOC, також відомому як традиційний SOC, IT-команда надавала послуги та функції SOC. Ця команда не завжди мала необхідний набір навичок, щоб робити те, що робить SOC сьогодні. Команда Центру зазвичай працювала над безліччю різних завдань, наприклад, забезпечувала антивірусну безпеку в компанії та збирала дані з реєстраційних журналів.

Для першого покоління SOC збір журналів обмежувався даними про джерело запису й тип пристрою. Часто повідомлення журналу зберігалися локально. В інших випадках центральний засіб реєстрації було налаштовано для прийому даних журналів, переважно у формі незашифрованого системного журналу або повідомлень протоколу простого керування мережею (SNMP).

Повідомлення й дані з журналів рідко аналізувалися. Як правило, повідомлення журналу зберігалися локально в кожній системі, на відміну від зберігання в централізованій системі, такій як сучасна SIEM.

SOC другого покоління

Інструменти SIEM почали з’являтися на ринку під час впровадження SOC другого покоління. Провайдери SIEM першого покоління представили методи виявлення мережевих загроз, звільнивши адміністраторів від важких завдань ручного управління й аналізу великих обсягів реєстраційних даних.

Перші постачальники цих інструментів зосереджувалися на управлінні подіями безпеки (Security Event Management, SEM), в рамках якого здійснювали аналіз журналів, що використовувалися для виявлення загроз у режимі реального часу. SEM приймав дані журналу, згенеровані різними джерелами в різних форматах, що робило його ефективнішим у пошуку інцидентів безпеки.

Основна ідея SEM полягала в об’єднанні реєстраційних даних з різних джерел, таких як пристрої безпеки та програми, що дозволяло пов’язати події безпеки. Пізніше SEM було посилено за допомогою засобів управління інформацією про безпеку (Security Information Management, SIM), які зосереджені на пошуку великих обсягів даних журналу, які можна було б додатково проаналізувати. У результаті поєднання двох зазначених продуктів створено комплексне рішення SIEM (Security Information and Event Management).

SOC другого покоління мав ще одну перевагу, а саме управління випадками інцидентів безпеки. Управління випадками інцидентів безпеки (Security Incidents Case Management) - це коли оператори SIEM можуть обробляти випадки різних інцидентів безпеки, про які повідомляють різні пристрої та програми [20].

SOC третього покоління

Інструменти SIEM продемонстрували свою справжню цінність у SOC третього покоління, запровадивши нові служби безпеки. Команда SOC цього покоління відповідала за завдання управління вразливостями, яке включало виявлення й перевірку вразливостей системи. Потім оцінювався вплив уразливостей, визначалися та впроваджувалися коригувальні дії, а також відстежувався їх статус закриття.

SOC четвертого покоління

У четвертому поколінні SOC з'явилися численні сучасні та прогресивні служби безпеки, які впоралися з новими інцидентами безпеки. У результаті відзначено зростання обмеженої кореляції подій, яке можна було спостерігати в старих поколіннях захисту великих даних SIEM. Безпека великих даних забезпечується шляхом аналізу великих обсягів даних протягом тривалого часу, щоб знайти загрози та аномалії, які потім використовуються для візуалізації результатів у зручний спосіб. Ще одна концепція, яка прийшла з цим поколінням, - це збагачення даних, які надходять із різних джерел, наприклад дані DNS, географічні дані та багато інших [20].

Обмеження традиційного SOC

Традиційний SOC має свої обмеження в порівнянні з тим, що пропонує його сучасний варіант. Здатність оцінювати й аналізувати широкий спектр даних і співвідносити численні інші типи подій з точки зору кібербезпеки є однією з ключових характеристик продуктивного SOC. У більшості ситуацій традиційні SOC не можуть виявити раніше невиявлені вразливості, а це не відповідає вимогам сучасного ландшафту безпеки. Щоб забезпечити ефективне виявлення та реагування у 2020 році й надалі, слід використовувати переваги машинного навчання, аналітики поведінки користувачів та автоматизації безпеки.

Існує кілька проблем зі стандартною багаторівневою моделлю центру безпеки.

• Аналітик вивчає нові сповіщення та передає важливі події старшим аналітикам. Ця техніка базується майже виключно на правилах і попередньо встановлених діях внаслідок чого користувачі покладаються на процедуру й знання про попередні події для оцінки інцидентів безпеки, закриваючи очі на нові небезпеки.

• Більшість сповіщень SOC є двійковими. Поява X, де X представляє час/дані/вікно. Потім аналітик повинен контекстуалізувати і пов'язати дані з середовищем. Однак аналітик, який працює з цими даними, не може управляти

всіма джерелами реєстраційних даних, а, отже, забезпечення надійного співвіднесення сигналів із різних джерел є проблематичним.

• Втома від тривоги є, ймовірно, найбільш критичною проблемою традиційного SOC. Щоразу, коли спостерігається інцидент, аналітик звертає на нього пильну увагу. У ситуації багаторазового повторення ця дія стає рутинною, і працівникам стає важко сортувати сповіщення від систем послідовно та з однаковим ступенем аналізу [21].

Актуальною є концепція розвитку SOC, представлена у статті Т. Поттера [22] (Рис. 1.4), відповідно до якої Центри безпеки пройшли 6 етапів розвитку, яким характерні такі риси:

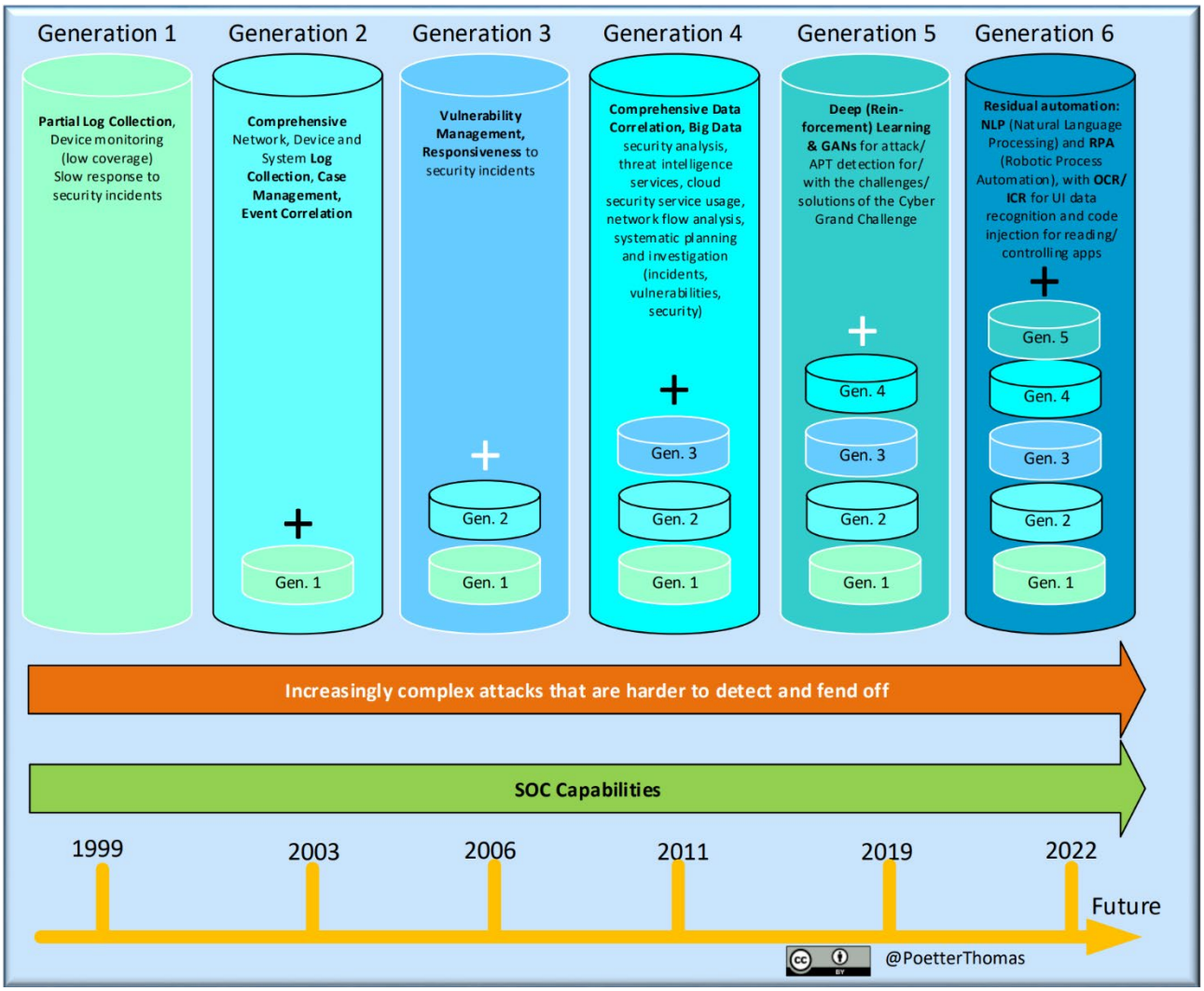

Рис. 1.4. Покоління SOC (за Т. Поттером)

Покоління 1. Часткове збирання логів, моніторинг пристроїв з низьким рівнем охоплення, повільне реагування на інциденти безпеки.

Покоління 2. Комплексне збирання логів (включаючи мережі, пристрої та системи), управління випадками безпеки, кореляція подій + активності 1 покоління.

Покоління 3. Управління вразливостями, здатність реагувати на інциденти безпеки + активності 1, 2 поколінь.

Покоління 4. Комплексна кореляція даних, аналіз безпеки великих даних, сервіси розвідки загроз і хмарної безпеки, аналіз мережевих потоків, системне планування і розслідування (інцидентів, вразливостей, заходів безпеки) + активності 1-3 поколінь.

Покоління 5. Глибоке (посилене) навчання і використання генеративних змагальних мереж (Generative adversarial networks, GANs - це клас алгоритмів штучного інтелекту, що використовуються в некерованому навчанні, реалізовані системою двох штучних нейронних мереж, які змагаються одна з одною в рамках гри з нульовою сумою [23]) для виявлення звичайних і APT-атак з використанням рішень Cyber Grand Challenge (змагання, започатковане Агентством передових оборонних дослідницьких проектів (DARPA) з метою розробки систем автоматичного захисту, які можуть виявляти, підтверджувати й виправляти недоліки програмного забезпечення в режимі реального часу) [24] + активності 1-4 поколінь.

Покоління 6. Залишкова автоматизація: обробка природної мови (Natural Language Processing, NLP) і автоматизація роботизованих процесів (Robotic Process Automation, RPA), з оптичним та інтелектуальним розпізнаванням символів (Optical Character Recognition, OCR / Intelligent Character Recognition, ICR) для розпізнавання даних інтерфейсу користувача та впровадження коду для читання/управління програмами.

Виклики для сучасних SOC

Сучасні SOC, як і їхні попередники також стоять перед новими викликами і мають вирішувати безліч питань безпеки, одночасно захищаючи організацію за допомогою меншої кількості кваліфікованих практиків.

Ризики і стійкість. Світ перейшов у стадію цифрової економіки, що мало наслідком підвищення критичності кібербезпеки для всіх організацій. І сьогодні вже не йдеться про захист від кібератак, а про захист систем від компрометації, і даних - від підробки та витоку. Крім того, зловмисники, які реалізують загрози, мають структурну перевагу: щоб досягти успіху, їм потрібно лише знайти одну слабку сторону, яку можна використати.

Особливе занепокоєння викликає зростання й популярність геополітичної складової кіберзлочинності, а також складності ланцюга поставок, що посилює сферу ризиків. Так, в останньому звіті Всесвітнього економічного форуму «Перспективи глобальної безпеки» відзначено, що «лідери більшості організацій вважають, що глобальна геополітична нестабільність помірно або дуже ймовірно призведе до катастрофічної кіберподії в найближчі два роки».

Віддалене управління й автоматизація операцій SOC. Зіткнувшись із пандемією, багато традиційних SOC розпустили, перейшовши до розподіленого режиму роботи. Пандемія показала, що створення розподіленого SOC є реальним і потенційно перспективним завданням. Сьогодні SOC нерідко керуються дистанційно, з місця проживання кіберспеціалістів, багато з яких працюють у звичайний робочий час.

Сучасний SOC еволюціонував так, що «центр» означає «центр передового досвіду» із сукупною експертизою разом із централізованим контролем і координацією, що виконується у розподілений спосіб. Ключовим елементом для розвитку корпоративного SOC у «центр передового досвіду» є автоматизація за допомогою штучного інтелекту (AI) і машинного навчання (ML). Це дає змогу організаціям ефективніше обробляти дані, зменшувати «шум» і швидко знаходити й усувати проблеми. Зазначені складові є невід'ємною частиною сучасного SOC, що дозволяє йому швидко реагувати на загрози, значно знижуючи ризики. Це також дозволяє проводити процедури стандартизації й масштабування, запроваджуючи послідовний, повторюваний процес.

З автоматизованою обробкою більшості загроз і сповіщень зараз не потрібні цілодобові зміни. Персонал за викликом потрібен лише для вирішення критичних,

підтверджених інцидентів, які не можуть бути оброблені за допомогою автоматизації. Вивільнення аналітиків дає їм більше часу для моделювання і прогнозування, творчої ініціативи. Вмотивована праця підвищує моральний дух персоналу й утримує його, водночас сприяючи вдосконаленню [25, 26].

Нульова довіра. SOC є втіленням нульової довіри – стратегії високого рівня, яка передбачає, що особам, пристроям і службам, які хочуть отримати доступ до ресурсів компанії, навіть тих, що знаходяться в мережі, не можна автоматично довіряти. Для посилення безпеки ці користувачі перевіряються щоразу, коли вони запитують доступ, навіть якщо вони були автентифіковані раніше [27]. Нульова довіра підсумовується тезою «довіряй, але перевіряй».

SOC дозволяє постійно відстежувати й підтверджувати конкретні рішення про довіру, використовуючи розширену телеметрію для створення унікального глобального уявлення про всі події. Це надає перевагу контексту - тому, чого не вистачає інструментам запобігання й іншим технологіям.

У рамках SOC є можливість ще раз перевірити попередні рішення про довіру, використовуючи інструменти, орієнтовані на аналітику поведінки, пошук загроз, виявлення аномалій та інші правила кореляції. SOC також використовує автоматизацію, щоб задіяти повну систему засобів управління для забезпечення дотримання принципів нульової довіри і надає додатковий рівень перевірки для подальшого зниження ризиків.

Брак талановитого персоналу. Нестача обдарованих спеціалістів продовжує залишатися важливою проблемою для більшості організацій і тим більше для SOC. У всьому світі кібербезпека відчуває зростаючий дефіцит – на галузевому ринку праці бракує близько 3,4 мільйона кіберфахівців [28]. Хоча зафіксовано потребу в професіоналах як на технічних, так і на загальних посадах, SOC складається, переважно, з практиків, тобто здібного і кваліфікованого персоналу, здатного якісно виконувати свою роботу.

Модель розподіленого SOC значно спрощує набір персоналу, дозволяючи наймати фахівців там, де вони є, ефективно розширюючи кадровий резерв, оскільки географічні обмеження більше не грають визначальної ролі. Акцент

робиться саме на навичках, а не на ієрархії, що є перевагою для організацій, які працюють в епоху гострої нестачі практиків.

SOC у цифровій трансформації бізнесу. Завдяки цифровій трансформації та іншим революційним технологіям, які розширюють зони атаки, обсяг і тип даних, які потрібно отримувати, аналізувати та щодо яких треба вживати захисних заходів, збільшуються в рази. Наявність ефективного SOC є обов'язковим для організацій будь-якого розміру, щоб забезпечити швидке виявлення та реагування на інциденти безпеки.

Традиційні SOC, які покладаються на фахівців-аналітиків, мають труднощі з масштабуванням для задоволення сучасних вимог. Це означає, що автоматизацію, штучний інтелект і машинне навчання слід розглядати як для корпоративного SOC, так і для SOC на аутсорсинговій основі.

Значення SOC досягло значно вищого рівня, зробивши його критично важливим засобом для організацій, що працюють у глобалізованій цифровій економіці. Зараз SOC виконує дуже важливу місію забезпечення цифрової трансформації і стійкості бізнесу. Оптимально налаштований, добре сконфігурований і керований SOC дозволяє підприємствам брати на себе нові ініціативи й ефективно прораховувати ризики кібербезпеки [25, 26].

Висновки до розділу 1

Встановлено, що центр безпеки (SOC) є оперативним координаційним центром для виявлення, аналізу й реагування на інциденти кібербезпеки. Типова місія SOC включає такі елементи: запобігання інцидентам; моніторинг безпеки; реагування на підтверджені інциденти; ситуаційне інформування та звітування про стан кібербезпеки; розробка й експлуатація технологій SOC.

Аналіз джерел показав, що SOC виконує багато різних функцій, які умовно можна поділити на сім категорій: сортування, аналіз і реагування на інциденти;

розвідка, пошук і аналітика кіберзагроз; розширені операції SOC; управління вразливостями; інструменти, архітектура й інженерія SOC; ситуаційна обізнаність, комунікація та навчання; лідерство й управління. Вибір функцій SOC залежить від потреб і можливостей організації.

З'ясовано, що перші центри операційної безпеки були створені для сектору оборони. У відповідь на зростаючі загрози, пов'язані з цифровізацією та розвитком Інтернету, й потребу в комплексній централізованій інфраструктурі для моніторингу, аналізу й реагування на виникаючі інциденти, в 90-х роках SOC почали з'являтися на комерційних підприємствах.

У наукових працях виділяють чотири покоління SOC. Центри 1-го покоління здійснювали моніторинг пристроїв, збирання логів і мали обмежене охоплення пристроїв; 2-му поколінню SOC притаманні такі функції як кореляція подій, збирання логів з системних журналів і мережевих пристроїв, управління випадками інцидентів безпеки, поява перших SIEM; SOC 3-го покоління впровадили нові сервіси безпеки, зокрема управління вразливостями й реагування на інциденти; на 4-му етапі розвитку SOC з'явилися численні сучасні сервіси безпеки: аналіз великих даних; збагачення даних, які надходять із різних джерел; розвідка загроз; розслідування інцидентів тощо.

Викликами для сучасних SOC є поява нових ризиків і потреба у забезпеченні кіберстійкості; віддалене управління; автоматизація операцій з використанням штучного інтелекту й машинного навчання; брак кваліфікованого персоналу; масштабність і мультифункціональність SOC, а також критична важливість кібербезпеки в забезпеченні цифрової трансформації і стійкості бізнесу.

РОЗДІЛ 2
ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ SOC ДЛЯ ВЕЛИКИХ І СЕРЕДНІХ ПІДПРИЄМСТВ

2.1 Специфіка SOC для великого бізнесу

На підприємствах великого бізнесу SOC виконує більш широкий спектр функцій, ніж на середніх та малих фірмах. Це пов'язано з тим, що такі підприємства мають більш складну структуру, більшу кількість інформаційних систем та мереж, а також вищі вимоги до безпеки.

Для підприємств великого бізнесу характерні такі особливості впровадження SOC: великий обсяг даних і мережевої активності; наявність значних ресурсів та інвестицій; масштабування діяльності з інформаційної безпеки; комплексність систем виявлення та реагування на інциденти безпеки; наявність власних кваліфікованих фахівців; централізований моніторинг; автоматизація завдань; інтеграція з іншими системами безпеки; інтеграція з бізнес-процесами; вищий рівень забезпечення безпеки [29] (Рис. 2.1).

Розглянемо їх детальніше.

Ресурси та інвестиції

Великі компанії зазвичай мають більше ресурсів для інвестицій у SOC, що дозволяє їм використовувати більш складні технології та підходи. Наприклад, великі компанії можуть дозволити собі придбати більш потужні системи виявлення вторгнень (IDS), системи виявлення аномалій (ADS) і системи виявлення витоків інформації (DLP). Вони також можуть дозволити собі найняти більше фахівців з безпеки, які мають досвід роботи з цими складними технологіями. Можливості компаній середнього розміру, звичайно, є меншими, ніж у потужних компаній, але значно більшими ніж у малих фірм.

Рис. 2.1. Особливості впровадження SOC для великого бізнесу

Масштабування

Великі компанії мають більший обсяг даних і мережевої активності, ніж малі компанії. Це вимагає більшого масштабування SOC. Наприклад, великі компанії можуть потребувати використання більшої кількості серверів для зберігання даних моніторингу, а також більшу кількість фахівців для обробки цих даних.

Комплексність

Великі підприємства часто стикаються з більш складними і різноманітними кіберзагрозами підприємства. Це потребує більш складних систем виявлення та реагування. Наприклад, великі компанії можуть потребувати використання систем машинного навчання для виявлення загроз, які неможливо виявити за допомогою традиційних методів.

Внутрішня експертиза

Великі компанії здатні працевлаштовувати більше внутрішніх фахівців для SOC. Це дозволяє їм краще розуміти свої особливості та потреби, а також краще інтегрувати SOC з іншими бізнес-процесами [30].

Централізований моніторинг.

SOC на підприємствах великого, а також частково середнього бізнесу зазвичай здійснюється централізований моніторинг всіх інформаційних систем та мереж організації. Це дозволяє виявляти загрози й інциденти безпеки на ранніх етапах, що підвищує ефективність реагування.

Автоматизація завдань.

На великих і середніх підприємствах SOC часто використовують автоматизовані інструменти для виявлення загроз та реагування на інциденти безпеки. Це дозволяє звільнити персонал SOC для більш складних завдань.

Інтеграція з іншими системами.

SOC на підприємствах великого бізнесу зазвичай інтегрується з іншими системами інформаційної безпеки, такими як системи управління доступом, системи виявлення та запобігання вторгненням (IDS/IPS) та системи управління інформаційною безпекою (SIEM). Це дозволяє отримувати більш точну інформацію про стан безпеки організації та підвищує ефективність реагування на інциденти безпеки [31].

Інтеграція з бізнес-процесами

У великих компаніях SOC більш тісно інтегрований з загальною стратегією безпеки й бізнес-операціями, такими як DevOps, управління ризиками й управління активами. Це дозволяє SOC краще розуміти бізнес-потреби й ефективніше реагувати на кіберзагрози.

Вплив на безпеку

Ці відмінності в застосуванні SOC мають значний вплив на безпеку великих компаній. Вони дозволяють краще виявляти й реагувати на кіберзагрози, що знижує ризик витоку інформації та інших кіберінцидентів.

Оскільки великі компанії, такі як технологічні гіганти Google, OpenAI, мають складні потреби безпеки, вони використовують SOC для виявлення та

реагування на широкий спектр кіберзагроз, включаючи DDoS-атаки, атаки «нульового дня» й атаки на інтелектуальну власність. А, отже, використовують широкий спектр технологій та підходів, зокрема:

- Системи виявлення вторгнень (IDS).
- Системи виявлення аномалій (ADS).
- Системи виявлення витоків інформації (DLP).
- Системи штучного інтелекту (AI) й машинного навчання (ML).
- Аналіз поведінки користувачів (UBA).
- Аналіз мережевої активності (NTA) [32].

На нашу думку, для подальшого розвитку SOC великої компанії доцільно зосередитися на таких напрямках як: застосування засобів штучного інтелекту й машинного навчання; покращення інтеграції з бізнес-процесами; розвиток кібербезпеки як послуги.

Розвиток AI та ML

Штучний інтелект (AI) має потенціал для вдосконалення кібербезпеки. Засоби можуть аналізувати великі обсяги даних моніторингу й виявляти нові та складні кіберзагрози, які неможливо виявити за допомогою традиційних методів. AI та ML доцільно використовувати не тільки для автоматизації завдань моніторингу й виявлення загроз, а також для виявлення нових і складних кіберзагроз.

Покращення інтеграції з бізнес-процесами

SOC повинен бути тісно інтегрований з іншими бізнес-процесами, щоб краще розуміти бізнес-потреби і ефективніше реагувати на кіберзагрози. Для цього необхідно розробити стратегію інтеграції SOC з бізнес-процесами, яка враховуватиме особливості бізнес-діяльності конкретної компанії, її можливості і потреби у галузі безпеки [33].

Розвиток кібербезпеки як послуги (Security as a Service, SaaS)

SaaS – це модель надання кібербезпеки як послуги. CaaS може бути корисним для середніх підприємств, які не мають ресурсів для створення власного SOC.

На Рис 2.2 показано типову структуру моделі «Кібербезпека як послуга» [34].

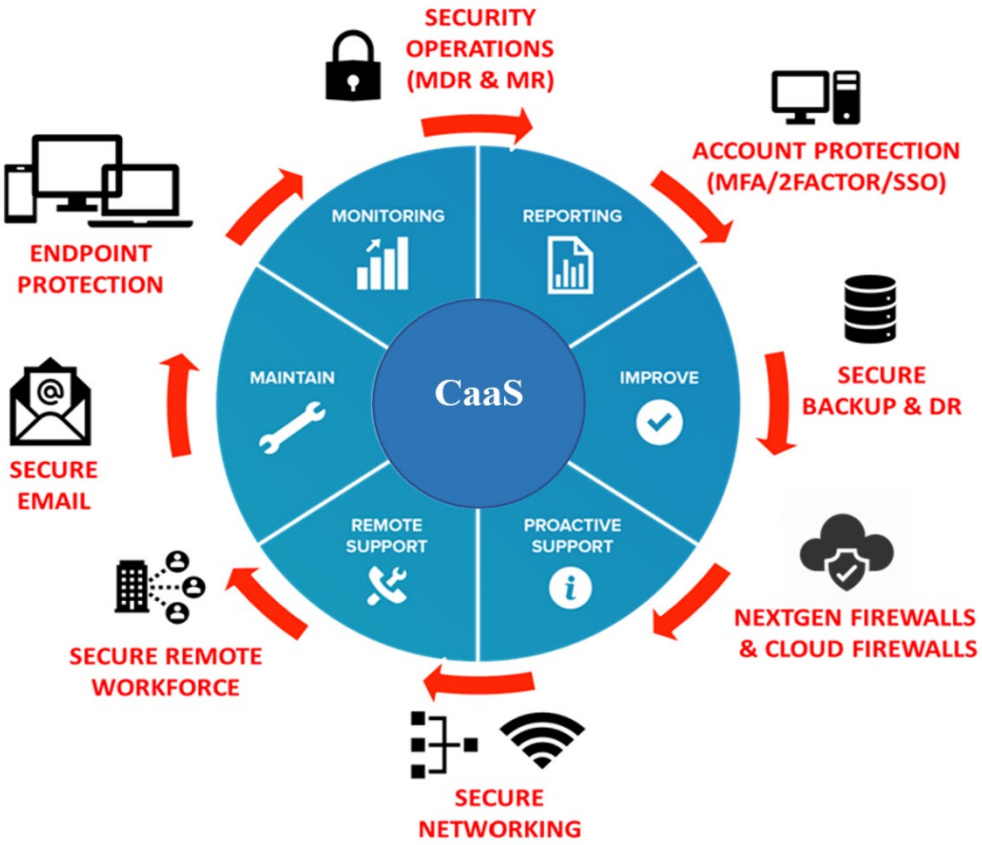

Рис 2.2. Типова структура моделі SaaS.

Навчання та розвиток персоналу SOC

Персонал SOC повинен постійно навчатися й розвиватися, щоб відповідати мінливим загрозам безпеки. Компанії мають інвестувати в навчання та розвиток персоналу SOC, щоб забезпечити їхню високу кваліфікацію й ефективність праці.

Співпраця з іншими підрозділами компанії

SOC повинен тісно співпрацювати з іншими підрозділами компанії, такими як IT, юридичний відділ, відділи безпеки, що забезпечити ефективне виявлення й реагування на кіберзагрози.

2.2 Аналіз використання SOC на підприємствах середнього бізнесу

Слід зазначити, що впровадження центрів безпеки на великих і середніх підприємствах також можуть відрізнятися. Так, якщо центри безпеки SOC є необхідним інструментом для забезпечення кібербезпеки великих компаній, то представники середнього бізнесу можуть обирати, чи створювати власний SOC.

Тим не менше, останнім часом SOC все частіше використовуються і на підприємствах середнього бізнесу. За даними дослідження компанії Gartner, у 2023 році 40% підприємств середнього бізнесу використовуватимуть SOC [35]. Так ситуація викликана наступними факторами:

– Зростання кількості кіберзагроз, які становлять загрозу не лише великим компаніям, але й підприємствам середнього бізнесу.

– Усвідомлення необхідності належного забезпечення кібербезпеки керівниками середнього бізнесу.

– Поява нових технологій і послуг, які дозволяють середнім компаніям створювати і підтримувати SOC.

Аналіз використання SOC на підприємствах середнього бізнесу показує, що такі компанії найчастіше використовують SOC для:

– моніторингу стану інформаційних систем і виявлення загроз безпеці;

– реагування на інциденти безпеки;

– здійснення аналізу безпеки;

– розробки й реалізації заходів безпеки.

SOC на підприємствах середнього бізнесу, як правило, мають менший масштаб, ніж SOC великих компаній. Вони також використовують менш складні технології і підходи. Однак, навіть SOC невеликого масштабу може бути ефективним інструментом для забезпечення кібербезпеки.

Водночас, впровадження SOC у великих і середніх компаніях є досить складним завданням, яке вимагає ретельного планування і реалізації.

Впровадження SOC здійснюється у відповідності з такою схемою (Рис. 2.3) [36].

На першому етапі необхідно провести аналіз потреб компанії в сфері безпеки, зокрема визначити такі аспекти:

– Типи інформаційних систем, які необхідно захищати.

– Рівень безпеки, який необхідно забезпечити.

– Ресурси, які треба виділити на впровадження SOC.

Рис. 2.3 Етапи впровадження SOC.

Другий етап передбачає розробку плану впровадження SOC, який визначає наступні елементи:

– Структура та функції SOC.

– Персонал, залучений до виконання завдань SOC.

– Інструменти та технології, які будуть використовуватися в SOC.

На третьому етапі необхідно реалізувати план впровадження SOC, у рамках якого здійснюють такі дії:

– Придбання обладнання і програмного забезпечення.

– Набір персоналу.

– Впровадження процедур і процесів безпеки.

Останній четвертий етап охоплює завдання із забезпечення експлуатації SOC, зокрема:

– Моніторинг стану інформаційних систем.

– Визначення загроз.

– Реагування на інциденти безпеки.

– Аналіз безпеки.

Як показав аналіз прикладів впровадження SOC на підприємствах середнього і великого бізнесу, ключовими факторами успіху є:

– Підтримка керівництва, яка є необхідною для реалізації такого складного і дороговартісного проекту.

– Залучення досвідчених фахівців, оскільки впровадження SOC вимагає знань і досвіду в сфері кібербезпеки.

– Постійне навчання та розвиток персоналу, завдяки якому фахівці SOC постійно оновлюють свої професійні знання і навички у відповідь на зміни в галузі кібербезпеки [36].

Приклад успішного впровадження SOC на підприємстві середнього бізнесу

Прикладом успішного впровадження SOC на підприємстві середнього бізнесу є компанія - виробник електротехнічної продукції "Альфа". У 2022 році компанія "Альфа" стала жертвою кібератаки, в результаті якої були втрачені важливі дані, після чого керівництво компанії вирішило впровадити SOC.

Компанія "Альфа" залучила до впровадження SOC досвідчену компанію-консультанта. У рамках проекту було розроблено план впровадження SOC, який передбачав:

1. Формування структури SOC.

SOC компанії "Альфа" складається з таких підрозділів (Рис. 2.4):

Рис. 2.4. Структура SOC компанії «Альфа»

Центр моніторингу відповідає за відстеження стану систем і виявлення загроз. Центр моніторингу використовує широкий спектр інструментів і технологій для виявлення кіберзагроз, зокрема: системи виявлення вторгнень (IDS), аномалій (ADS) та витоку інформації (DLP), машинного навчання (ML), аналізу поведінки користувачів (UBA), мережевої активності (NTA).

Центр реагування на інциденти відповідає за надання своєчасної та якісної відповіді на інциденти безпеки. Центр реагування на інциденти використовує процедури і процеси виявлення й оцінювання інциденту, реагування і повідомлення про інцидент

Центр аналізу безпеки відповідає за дослідження стану безпеки і використовує такі інструменти й технології: системи управління інформаційною безпекою (SIEM), управління конфіденційністю, цілісністю та доступністю (CIEM), управління загрозами (TM), управління інцидентами (IM).

Центр розробки і реалізації заходів безпеки відповідає за планування і впровадження заходів безпеки з використанням таких інструментів і технологій: систем управління безпекою (ISMS), управління ризиками (RMS), управління активами (IAM), управління персоналом (HRMS).

2. Наймання персоналу SOC і розподіл повноважень.

Відповідно до структури SOC компанії "Альфа" персонал складається з таких фахівців: інженери з моніторингу, аналітики безпеки, експерти з

реагування на інциденти, фахівців з аналізу безпеки, фахівці з розробки і реалізації заходів безпеки.

3. Застосування інструментів і технологій.

Для виконання своїх завдань SOC компанії "Альфа" використовує інструменти й технології від перевірених і надійних виробників:

– Системи виявлення вторгнень (IDS): Snort, Suricata.
– Системи виявлення аномалій (ADS): Bro, OSSEC.
– Системи виявлення витоків інформації (IDS): NetFlow, Splunk.
– Системи машинного навчання: IBM QRadar, Splunk.
– Аналіз поведінки користувачів (UBA): IBM QRadar, Splunk.
– Аналіз мережевої активності (NTA): IBM QRadar, Splunk [37].

Таким чином, можна скласти умовний перелік кращих виробників програних і апаратних рішень для SOC (Рис. 2.5).

Рис. 2.5. Виробники технологій SOC компанії "Альфа"

Архітектура SOC компанії "Альфа" представлена на рисунку 2.6.

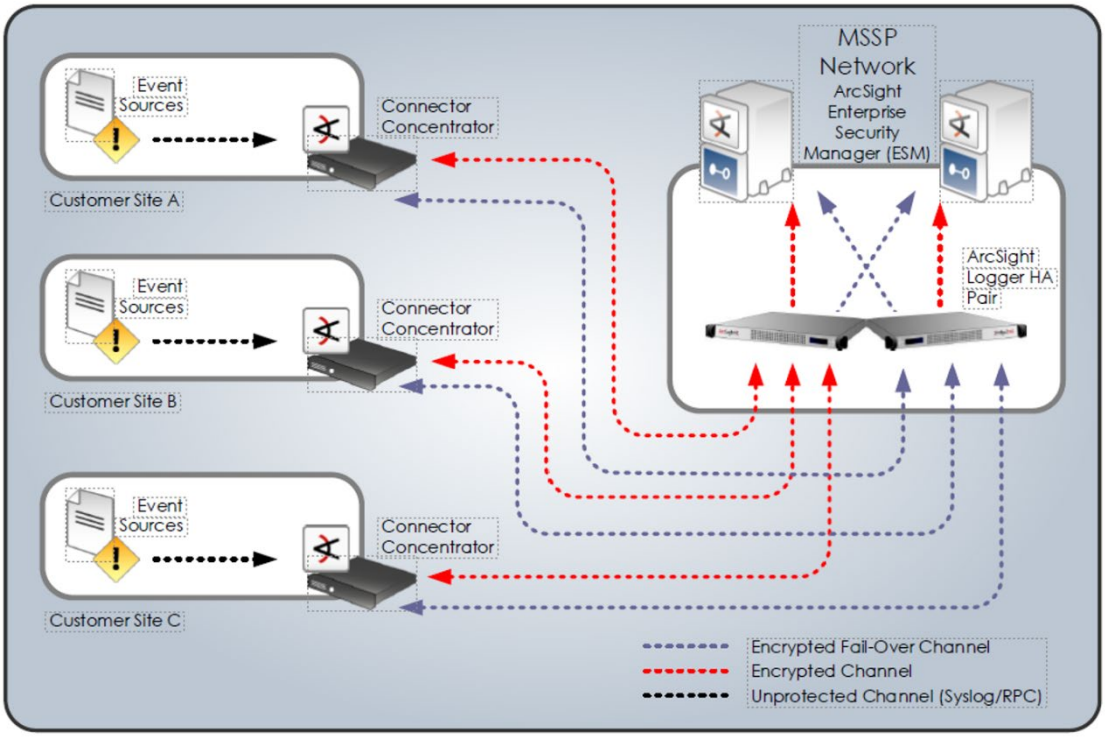

Рис. 2.6. Архітектура SOC компанії "Альфа".

Реалізація плану впровадження SOC компанії "Альфа" була завершена в 2023 році. Після впровадження SOC компанія "Альфа" зафіксувала наступні позитивні результати:

– Зниження кількості кібератак.
– Скорочення часу реагування на інциденти безпеки.
– Покращення ефективності заходів безпеки.

2.3 Використання технологій AI та ML для підвищення ефективності великих і середніх SOC

Штучний інтелект (Artificial Intelligence, AI) і машинне навчання (Machine Learning, ML) та є потужними технологіями, які можуть бути використані для підвищення ефективності забезпечення інформаційної безпеки підприємства. Використання AI та ML дає низку переваг для галузі кібербезпеки:

пришвидшення процесів обробки інформації, забезпечення просунутої аналітики, автоматизація рутинних і повторюваних процесів, розпізнавання шаблонів у даних, розробка прогнозів, підвищення ефективності систем безпеки (Рис. 2.7) [38].

Програми безпеки, керовані AI, можуть реагувати на підозрілу активність у режимі реального часу і запобігати атакам до того, як вони відбудуться. Такі рішення можуть швидко обробляти величезні неструктуровані та гібридні набори даних, аналізувати дані, знаходити закономірності й навіть робити прогнози.

Рис. 2.7. Переваги AI та ML для рішень кібербезпеки

Штучний інтелект може автоматизувати рутинні та повторювані завдання, скоротити час на розслідування атак і видавати менше помилкових спрацьовувань порівняно з традиційними системами кібербезпеки. Крім того, алгоритми машинного навчання розроблені для вдосконалення своєї продуктивності з часом, покращуючи загальну ефективність системи.

Впровадження AI та ML в рішення з кібербезпеки підвищує їх ефективність, дозволяючи таки інструментам безпеки краще захищати компанії від існуючих і невідомих загроз. Крім того, ці інноваційні технології мають потенціал для вдосконалення традиційних рішень і процесів кібербезпеки.

Завдяки здатності AI та ML обробляти великі обсяги як структурованих, так і неструктурованих даних, виявляти закономірності й навчатися, застосування AI та ML в інструментах кібербезпеки може їх істотно покращити.

Розглянемо детальніше, для яких напрямів забезпечення інформаційної безпеки використання AI та ML матиме найбільшу користь (Рис. 2.8).

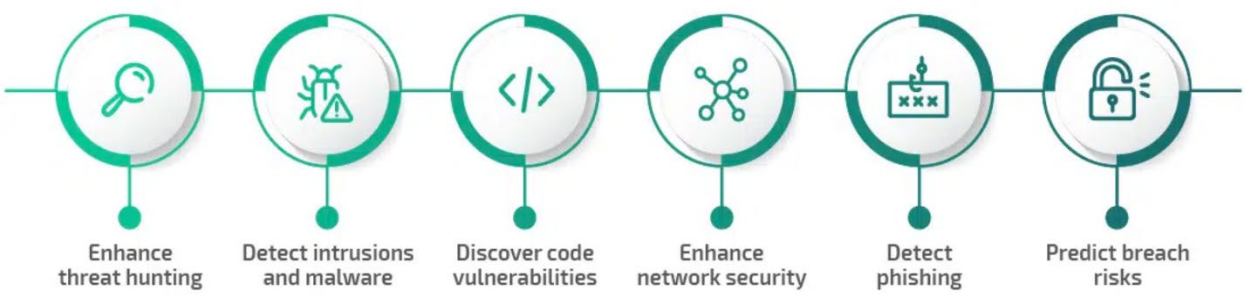

Рис. 2.8. Напрями інформаційної безпеки, в яких доцільно використовувати AI та ML

1. Розвідка загроз. Розвідка загроз передбачає проактивний пошук кіберзагроз в мережі організації, який раніше був ручним і трудомістким процесом. Однак завдяки застосуванню ML, розширеної аналітики та аналітики поведінки користувачів (UBA) розвідку загроз можна частково автоматизувати, таким чином підвищивши її ефективність [39].

2. Виявлення вторгнень та зловмисного програмного забезпечення. Методи ML доцільно використовувати для вдосконалення систем виявлення шкідливих програм на основі сигнатур. Наприклад, зловмисники часто створюють варіанти зловмисного ПЗ, щоб уникнути виявлення під час повторного використання того самого шкідливого коду. Оскільки традиційні методи на основі сигнатур не можуть виявити невідомі варіанти зловмисного ПЗ, аналітики безпеки пропонують виявлення на основі поведінки: метод, який аналізує характеристики та поведінку файлу, щоб визначити, чи він справді є шкідливим.

Однак традиційне сканування та аналіз даних займає надто багато часу, що робить такий підхід неефективним. З розширеними можливостями ML

інструмент кібербезпеки зможе обробляти великі обсяги даних, таким чином прискорюючи аналіз і ефективно розрізняючи зловмисне ПЗ [40].

3. Виявлення вразливостей програм. І зловмисники, і розробники додатків шукають уразливості коду. Перемагає той, хто першим виявить вразливість. Одним із сучасних способів пошуку небезпечних недоліків у коді є використання алгоритмів AI та ML, які можуть швидко сканувати величезні обсяги коду й виявляти відомі вразливості до того, як хакери помітять і використають їх.

Ідея виявлення недоліків у коді за допомогою штучного інтелекту не нова, але все ще є предметом досліджень. Деякі дослідники автоматизують виявлення вразливостей ПЗ за допомогою гібридних нейронних мереж. Незважаючи на те, що цей підхід довів свою ефективність, все ще існують певні обмеження, пов’язані з мовою, якою написано ПЗ, і відсутністю позначених наборів даних про вразливості.

4. Мережева безпека. Застаріле ПЗ, мікропрограми та політики безпеки є поширеними ризиками безпеки, які збільшують зону атаки. Щоб подолати ці проблеми, варто використовувати можливості штучного інтелекту для покращення корпоративних рішень мережевої безпеки шляхом управління всіма підключеними пристроями в мережевому середовищі; дослідження моделей мережевого трафіку з метою виявлення аномалій; функціональне групування робочих навантажень і політик безпеки на основі конкретних потреб.

5. Виявлення фішингових атак. Рішення для аналізу електронної пошти на основі ML зазвичай працюють швидше й ефективніше, ніж традиційні. Так, використовуючи величезну колекцію як фішингових, так і безпечних електронних листів, можна навчити алгоритми ML аналізувати контекст повідомлення, розуміти, як користувачі спілкуються, і знаходити відхилення та конкретні шаблони [41].

Наприклад, варто використати цей підхід, щоб побудувати систему, яка буде помічати підроблених відправників, визначаючи адреси електронної пошти, подібні до тих, з яких особа вже отримувала електронні листи (наприклад, адреса генерального директора чи головного бухгалтера), або

реагувати на термінові слова, що є типовою ознакою фішингових електронних листів.

6. Прогнозування ризиків порушення даних. Компанія може покращити своє рішення кібербезпеки за допомогою розширеної аналітики (AA), яка передбачає автономну обробку даних з використання методів AI й алгоритмів ML для пошуку глибоких кореляцій, прогнозування та надання рекомендацій [40, 41].

Розглянемо ряд технічних рішень, які можуть бути використані для імплементації передових технологій ML та AI в моніторингу безпеки.

Системи управління інформаційною безпекою (SIEM): SIEM збирають та аналізують дані з різних джерел, таких як мережі, системи та пристрої. ML можна використовувати для виявлення аномалій у даних SIEM, які можуть вказувати на потенційні кібератаки [42].

Системи виявлення вторгнень (IDS): IDS використовують різні методи для виявлення вторгнень у мережу. ML можна використовувати для підвищення точності IDS.

Системи управління подіями безпеки (SOAR): SOAR автоматизують процеси реагування на інциденти безпеки. AI можна використовувати для підвищення ефективності SOAR [43].

Наведемо кілька прикладів реалізації передових технологій ML та AI в моніторингу безпеки:

Компанія Google Cloud Security Command Center (SCC) використовує ML для виявлення аномалій у даних SIEM. SCC може виявляти аномалії, які неможливо виявити вручну.

Компанія CrowdStrike Falcon використовує AI для виявлення та реагування на кібератаки. Falcon може виявляти кібератаки на ранніх етапах, що дозволяє їм бути більш ефективно зупиненими.

Компанія IBM Security QRadar використовує ML для виявлення аномалій у даних IDS. QRadar може виявляти аномалії, які неможливо виявити вручну [44].

Передові технології ML та AI мають потенціал для значного підвищення ефективності моніторингу безпеки. Компанії, які інтегрують ці технології у свої стратегії безпеки, можуть отримати конкурентну перевагу та краще захистити свої активи від кібератак.

Одним із основних способів використання ML у моніторингу безпеки є виявлення аномалій у даних. ML можна використовувати для навчання моделі на наборі даних, який містить нормальні дані. Потім модель можна використовувати для виявлення аномалій у нових даних, які не відповідають моделі.

Наприклад, компанія може використовувати ML для виявлення аномалій у даних мережевого трафіку. Модель може бути навчена на наборі даних, який містить нормальний мережевий трафік. Потім модель можна використовувати для виявлення аномалій у нових даних мережевого трафіку, таких як незвичайний трафік із невідомого джерела.

AI також можна використовувати для автоматизації завдань моніторингу. Це може звільнити персонал для більш складних завдань, таких як аналіз загроз та реагування на інциденти.

Наприклад, компанія може використовувати AI для автоматизації процесу виявлення аномалій у даних SIEM. AI може використовуватися для аналізу даних SIEM та виявлення аномалій, які можуть вказувати на потенційні кібератаки.

Висновки до розділу 2

Дослідження показало, що великі компанії, які мають більше даних, ресурсів і впливу, стикаються з більш складними кіберзагрозами і є більш привабливими цілями для хакерів. Крім цього великі підприємства також мають більш складну інфраструктуру, що ускладнює виявлення й реагування на кібератаки.

Водночас, компанії великого бізнесу мають можливість інвестувати в більш розвинені SOC з внутрішніми командами. Ці SOC оснащені найновішими технологіями й інструментами, а також мають кваліфікований персонал, що дозволяє ефективно виявляти та реагувати на складні й витончені кібератаки.

Середні підприємства, як правило, мають менші бюджети та ресурси, ніж великі компанії. Тому вони можуть покладатися на аутсорсинг і стандартизовані рішення для забезпечення кібербезпеки. Аутсорсинг дозволяє середнім підприємствам отримати доступ до спеціалізованих знань та досвіду, не інвестуючи у власні ресурси. Стандартизовані рішення можуть допомогти середнім підприємствам зменшити витрати і полегшити масштабування.

Для підприємств середнього і великого бізнесу важливо, щоб реалізація SOC було частиною комплексної стратегії кібербезпеки, яка відповідає конкретним потребам компанії, враховує її розмір, ресурси і специфіку роботи.

При реалізації великих і середніх SOC доцільно використовувати засоби машинного навчання і штучного інтелекту, які дозволяють пришвидшити процеси обробки інформації, забезпечити просунуту аналітику, автоматизувати рутинні й повторювані процеси, розпізнавати шаблони в даних, розробляти прогнози і підвищити ефективність корпоративних систем безпеки загалом. Встановлено, що використання AI та ML матиме найбільшу користь для таких напрямів кібербезпеки як: розвідка загроз, виявлення вторгнень та зловмисного ПЗ, виявлення вразливостей програм, мережевої безпеки, виявлення фішингових атак, прогнозування ризиків порушення даних.

РОЗДІЛ 3
РЕАЛІЗАЦІЯ SOC НА ПІДПРИЄМСТВАХ МАЛОГО БІЗНЕСУ

Центри безпеки (SOC) відіграють вирішальну роль у стратегії кібербезпеки сучасних організацій. Вони виконують критично важливу функцію, забезпечуючи неперервний моніторинг, виявлення та реагування на інциденти безпеки. Особливо це важливо для малих підприємств, які часто мають обмежені ресурси та бюджети для впровадження комплексних заходів кібербезпеки. На відміну від великих корпорацій, малі підприємства часто не мають доступу до великої команди IT-фахівців або передових технологій, але SOC може стати ключем до ефективного управління кіберзагрозами.

Отже, основними чинниками, які визначають підходи малих підприємств до організації SOC є: невеликі обсяги даних, які потребують захисту; обмежений фінансові можливості компанії; наявність невеликої кількості персоналу.

Невеликий обсяг даних: для малих підприємств важливо вибрати SOC, що ефективно обробляє обмежені обсяги даних, забезпечуючи високу точність виявлення та аналізу інцидентів без надмірних вимог до зберігання даних.

Обмежений бюджет: Малі підприємства шукають економічно ефективні рішення для SOC, включаючи аутсорсинг, використання хмарних сервісів та відкритих програмних рішень Open source.

Невелика кількість персоналу: SOC повинен бути простим у використанні, інтуїтивно зрозумілим, з мінімальними вимогами до технічних знань персоналу. Ключовими є автоматизація процесів моніторингу й реагування на інциденти [45].

3.1 Інформаційні системи, мережева й серверна інфраструктура SOC малого підприємства

Основні інформаційні системи малого бізнесу, які потребують захисту

Основні інформаційні системи малого бізнесу України не відрізняються від основних інформаційних систем малого бізнесу в інших країнах. До них зазвичай відносять (Рис. 3.1):

Рис. 3.1. Інформаційні системи малого бізнесу, які потребують захисту

Системи управління ресурсами підприємства (ERP), такі як 1C, SAP і Oracle, використовуються для управління всіма аспектами бізнесу, включаючи фінанси, виробництво, логістику та продажі.

Системи управління продажами та маркетингом (CRM), такі як Salesforce і HubSpot, використовуються для управління взаємовідносинами з клієнтами, включаючи продажі, маркетинг та обслуговування клієнтів.

Електронна пошта, така як Gmail і Outlook, використовується для спілкування з клієнтами, співробітниками та іншими партнерами.

Телефонія, така як VoIP і мобільні телефони, використовується для голосового спілкування.

Відеоконференції, такі як Zoom і Microsoft Teams, використовуються для відеозв'язку.

Системи управління доступом (IAM), такі як Active Directory і Okta, використовуються для контролю доступу до конфіденційної інформації та систем.

Системи резервного копіювання, такі як Veeam і Veritas, використовуються для резервного копіювання даних для відновлення в разі втрати даних [46, 47].

Мережева й серверна інфраструктура малого підприємства

Для забезпечення функціонування базових IT-сервісів на малому підприємстві необхідно спроектувати та впровадити відповідну мережеву й серверну інфраструктуру (Рис. 3.2). Ця інфраструктура повинна забезпечувати надійну передачу даних, доступ до Інтернету та інших ресурсів, а також захист даних від несанкціонованого доступу.

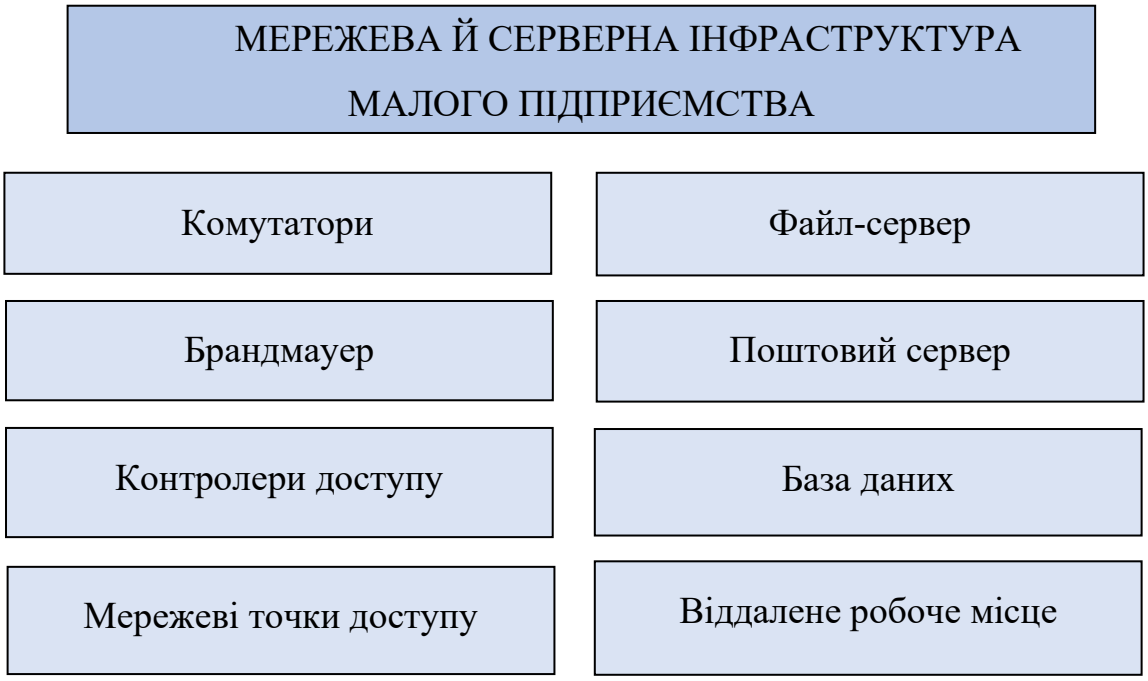

Рис. 3.2. Мережева й серверна інфраструктура малого підприємства

Мережева інфраструктура повинна включати в себе такі елементи:

– Комутатори, які забезпечують зв'язок між кінцевими пристроями і серверами.

– Брандмауер, який захищає мережу від несанкціонованого доступу.

– Контролери доступу, які контролюють доступ до мережі.

– Мережеві точки доступу, які забезпечують бездротовий доступ до мережі.

Серверна інфраструктура повинна включати в себе такі елементи:

– Файл-сервер, який забезпечує спільний доступ до файлів.

– Поштовий сервер, який забезпечує відправку й отримання повідомлень електронної пошти.

– База даних - організована структура, призначена для зберігання, зміни й обробки взаємопов'язаної інформації, важливої для підприємства.

– Віддалене робоче місце, яке дозволяє співробітникам працювати з будь-якого місця [48].

Наведений перелік IT-систем є базовим набором, який може бути використаний для побудови IT-інфраструктури малого підприємства. Кожен елемент цього набору має свою роль у забезпеченні функціонування IT-сервісів.

Active Directory - це система управління каталогами, яка забезпечує централізоване управління обліковими записами користувачів і комп'ютерів.

Windows File Server - це файловий сервер, який забезпечує спільний доступ до файлів.

Microsoft Exchange або Office 365 - це поштовий сервер, який забезпечує відправку та отримання електронної пошти.

MS SQL - це сервер баз даних, який зберігає важливі дані.

VMware Sphere - це платформа віртуалізації, яка дозволяє створювати та керувати віртуальними машинами.

Мережеві пристрої забезпечують зв'язок між різними елементами IT-інфраструктури. Система/сервери резервного копіювання забезпечують захист даних від втрати.

При виборі та впровадженні мережевої та серверної інфраструктури для малого підприємства необхідно враховувати такі фактори, як: розмір і складність бізнесу; бюджетні обмеження; потреби бізнесу в функціональності. Для малого бізнесу з невеликим бюджетом можуть бути доступні безкоштовні або недорогі варіанти мережевих і серверних пристроїв. Однак для більш складних бізнесів знадобляться дорожчі пристрої з більшою функціональністю.

Український малий бізнес часто використовує безкоштовні або недорогі варіанти основних інформаційних систем, що пов'язано з обмеженими обсягами бюджету. Вітчизняний малий бізнес часто має обмежений доступ до фахівців з інформаційної безпеки, що ускладнює реалізацію заходів щодо захисту основних

інформаційних систем від кібератак. Загалом, українські малий бізнес стикається з тими ж викликами в галузі безпеки, що й малий бізнес в інших країнах [49].

Важливо провести класифікацію розташування ресурсів і місць знаходження даних для їх подальшого захисту (Таблиця 3.1) [50].

Таблиця 3.1.

Ресурси й місця знаходження даних для їх подальшого захисту

Тип	Опис	Системи
Дані	Дані, які охоплюють конфіденційну інформацію про клієнтів, працівників, фінансові показники тощо, є найціннішим активом для будь-якого бізнесу, а також першочерговими цілями для кібератак. Фінансові дані (номери кредитних карток, банківські рахунки та особисті доходи).	Кінцеві пристрої, такі як комп'ютери, ноутбуки, планшети та смартфони, можуть зберігати дані про користувачів (імена, паролі, контактну інформацію). Сервери, які використовують для зберігання й обробки даних, можуть зберігати великі обсяги інформації, такі як фінансові дані, дані клієнтів та дані працівників. Мережі, що з'єднують комп'ютери й інші пристрої, містять електронні листи, файли та веб-сторінки.

Продовження табл. 3.1.

Тип	Опис	Системи
Дані	Дані клієнтів (імена, адреси, номери телефонів, електронні адреси). Власні інтелектуальні права (патенти, торгові марки й авторські права).	Мережі, що з'єднують комп'ютери й інші пристрої, містять електронні листи, файли та веб-сторінки. Хмарні платформи, такі як AWS, Azure та Google Cloud Platform, зберігають великі обсяги конфіденційних даних компанії.

Системи	Системи, які зберігають та обробляють конфіденційні дані (комп'ютери, сервери, мережі та хмарні платформи), є цінними бізнес-активами і важливими цілями для кібератак. Інфраструктура, яка підтримує бізнес: фізичні об'єкти (будівлі й обладнання), віртуальна інфраструктура (хмарні сервіси).	Системи CRM зберігають дані про клієнтів (імена, контактну інформацію, історію покупок та обслуговування). Системи ERP зберігають дані про бізнес (фінансові дані, дані про виробництво та продажі). Системи HRM зберігають дані про персонал (персональні дані, інформація у сфері охорони здоров’я і трудової діяльності. Системи електронної пошти зберігають повідомлення, які містять конфіденційні дані. Системи зберігання файлів зберігають файли з конфіденційними даними. Веб-сайти містять конфіденційну інформацію (персональні дані користувачів, фінансова інформація).

3.2 Розмежування обов'язків команди SOC

Розмежування обов'язків є важливим аспектом забезпечення інформаційної безпеки будь-якої організації. Чим чіткіше визначені ролі та обов'язки кожного співробітника, тим менший ризик виникнення конфліктів і незахищених ділянок в інформаційному ландшафті.

На практиці розмежування обов'язків часто не є чітко визначеним, що може призвести до конфліктів між групами персоналу з інформаційної безпеки. Наприклад, IT-спеціалісти можуть вважати, що відповідальність за безпеку покладається на них, а власники активів можуть вважати, що це їхня

відповідальність. Це може призвести до того, що ділянки в інформаційному ландшафті залишаться незахищеними.

Існує кілька інструментів, які можна використовувати для узгодження та документування ролей і обов'язків усіх співробітників, залучених до забезпечення безпеки корпоративного середовища.

Одним із таких інструментів є RACI-таблиця. RACI-таблиця - це матриця, в якій для кожної задачі або проекту визначено перелік ролей: відповідальна особа (Responsible), підзвітна особа (Accountable), консультант (Consulted) та інформована особа (Informed) (Рис. 3.3) [51].

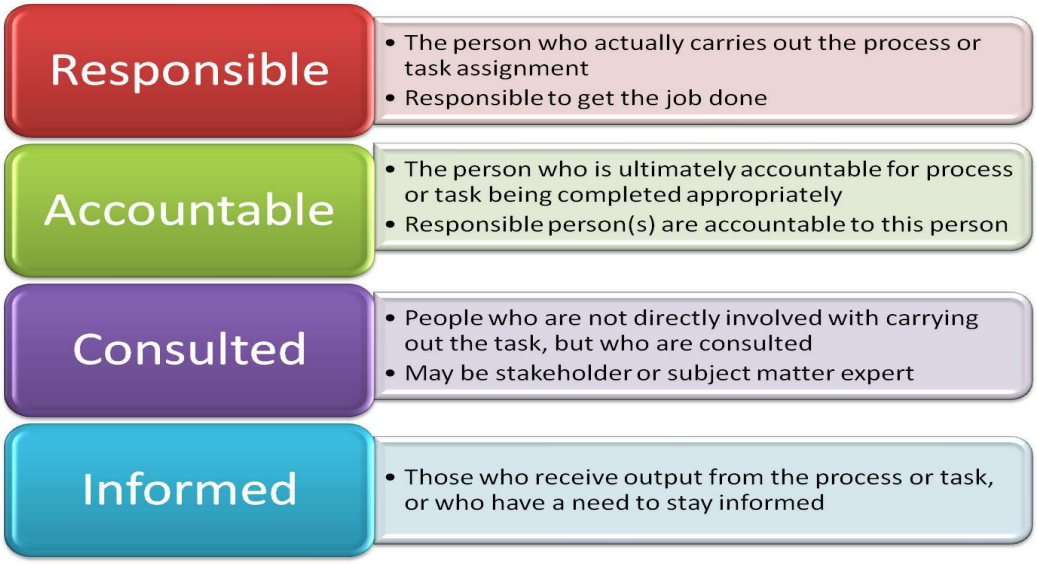

Рис. 3.3. RACI-таблиця

A (Accountable) - відповідає за виконання завдання. Ця особа має остаточну відповідальність за те, щоб завдання було виконано належним чином.

R (Responsible) - відповідає за виконання конкретного аспекту завдання. Ця особа має виконати завдання або забезпечити його виконання.

C (Consulted) - консультується щодо виконання завдання. Ця особа може надати інформацію, експертні знання або поради, але не несе відповідальності за виконання завдання.

I (Informed) - інформується про виконання завдання. Ця особа повинна бути поінформована про прогрес у виконанні завдання, але не несе відповідальності за його виконання.

Однією з найпоширеніших форм RACI-таблиць є Purdue RACI. У Purdue RACI відповідальним є працівник, який безпосередньо виконує задачу або проект. Підзвітним є співробітник, який має остаточну відповідальність за успіх задачі або проекту. Консультантом є співробітник, який надає поради й рекомендації щодо виконання задачі або проекту. Інформованим є співробітник, якого необхідно інформувати про стан задачі або проекту.

Generic RACI є більш гнучкою формою RACI-таблиці, ніж Purdue RACI. У Generic RACI можна використовувати інші ролі, крім чотирьох основних. Наприклад, можна використовувати роль виконавчого секретаря (Executive Secretary), який відповідає за організацію та проведення зустрічей, або роль координатора (Coordinator), який відповідає за координацію дій різних груп персоналу.

Використання RACI-таблиці є ефективним способом узгодження та документування ролей і обов'язків усіх співробітників, залучених до забезпечення безпеки компанії. Це допомагає уникнути конфліктів, забезпечити ефективну співпрацю між різними групами персоналу та підвищити рівень інформаційної безпеки організації [52].

На рисунку 3.4 показана структура посадових осіб, залучених у процес забезпечення інформаційної безпеки підприємства малого бізнесу.

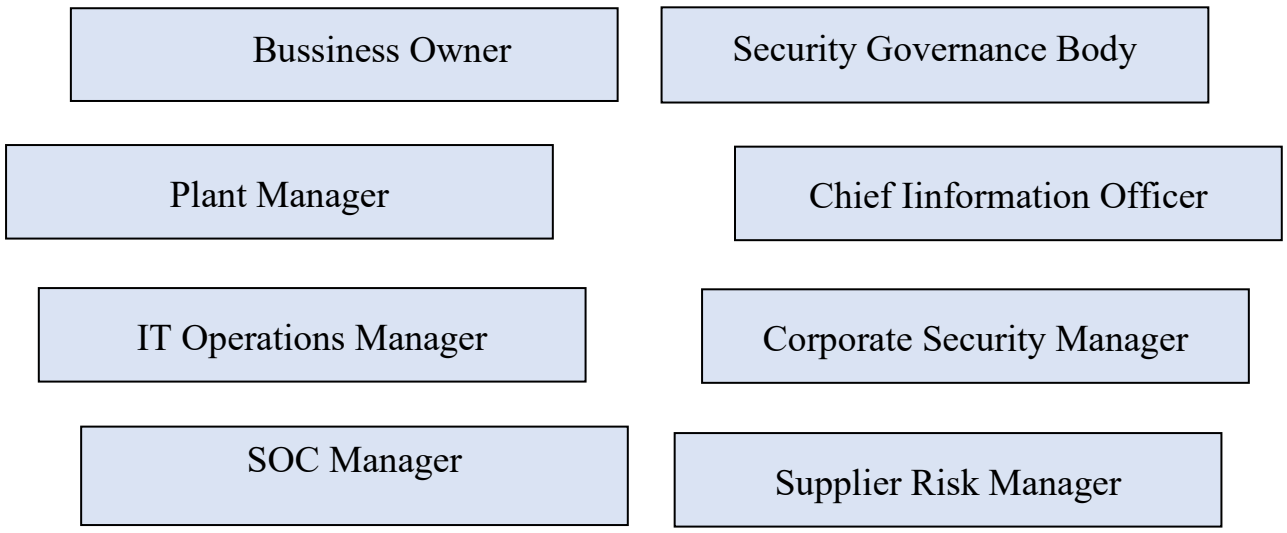

Рис. 3.4. Посадові особи, залучені у процес забезпечення інформаційної безпеки малого підприємства

У таблиці 3.2 представлений розподіл основних ролей і обов'язків з безпеки відповідно до концепції RACI [53].

Таблиця 3.2.

Розподіл основних ролей і обов'язків з безпеки відповідно до RACI

Роль	Відповідальність	Обґрунтування
Власник бізнесу (Bussiness Owner)	Відповідальний	Відповідальний за безпеку своїх бізнес-додатків і даних
Наглядовий орган з безпеки (Security Governance Body)	Інформований	Наглядає за загальним станом безпеки в організації
Керівник компанії (Plant Manager)	Відповідальний	Відповідальний за безпеку фізичних активів та безпеку місцевого об'єкта
Директор з IT (CIO)	Відповідальний	Визначає загальну стратегію та управління IT-безпекою
Менеджер операцій безпеки (ITOPS)	Відповідальний	Впроваджує та підтримує засоби безпеки в різних технологічних доменах

Продовження табл. 3.2.

Роль	Відповідальність	Обґрунтування
Менеджер корпоративної безпеки (Corporate Security Manager)	Відповідальний	Виконує конкретні функції безпеки: IAM, EDR, управління загрозами, підключення третіх сторін, реагування на інциденти, пентестинг, SA&T, підтримка політики й моніторинг відповідності
Менеджер SOC (SOC Manager)	Відповідальний	Моніторинг подій і інцидентів безпеки

Менеджер ризиків, пов’язаних із постачальниками (Supplier Risk Manager)	Консультант	Консультує щодо управління ризиками, пов'язаними з підключенням третіх сторін

Дослідження показало, що до основних напрямів забезпечення інформаційної безпеки малого підприємства у рамках SOC відносять:

– Виконання процедур управління ідентифікацією та доступом (IAM).

– Оновлення, впровадження безпеки і моніторинг кінцевих точок.

– Оновлення, впровадження безпеки і моніторинг додатків.

– Оновлення, впровадження безпеки і моніторинг баз даних.

– Оновлення, впровадження безпеки і моніторинг серверів.

– Оновлення мережевого обладнання, впровадження безпеки мережі, моніторинг мережевого трафіку.

– Ведення реєстру активів.

– Виконання процедур управління вразливостями.

– Виконання процедур управління загрозами.

– Управління підключеннями третіх сторін.

– Управління реагуванням на інциденти безпеки.

– Проведення тестування на проникнення.

– Впровадження програми обізнаності й навчання з безпеки (SA&T).

– Ведення політики безпеки.

Моніторинг відповідності нормативним вимогам [54, 55].

3.3 Проблеми впровадження та перспективи розвитку SOC

Незважаючи на всі переваги і безліч прикладів успішної реалізації центрів безпеки, при впровадженні SOC спостерігається низка типових проблем, серед яких: брак ресурсів, недостатня підготовка персоналу, недосконалі процеси і процедури, недостатня комунікація [56].

З огляду на те, що впровадження SOC вимагає значних ресурсів, включаючи обладнання, ПЗ, персонал і послуги, компанії мають ретельно оцінити свої потреби в ресурсах, перш ніж приймати рішення про впровадження SOC.

Недостатня підготовка персоналу SOC є серйозною проблемою, оскільки некваліфіковані фахівці без досвіду у сфері кібербезпеки не зможуть ефективно виконувати свої функціональні обов'язки. Тому компанії повинні забезпечити належну підготовку свого персоналу SOC або найняти професіоналів ззовні.

Для того, щоб корпоративний SOC функціонував і успішно виконував свої завдання, компанія повинна розробити і впровадити ефективні процеси і процедури, зокрема для моніторингу, виявлення загроз, реагування на інциденти та аналізу безпеки.

SOC має здійснювати якісну і своєчасну комунікацію з іншими підрозділами компанії, такими як відділи IT, корпоративної безпеки, юридичний та управління персоналом, щоб забезпечити обізнаність і координацію дій із захисту бізнесу від кібератак.

Для вирішення окреслених вище проблем компаніям необхідно вжити таких заходів для вирішення проблем, пов'язаних з впровадженням SOC:

– Розробити план впровадження SOC, який визначає цілі, завдання, ресурси та терміни впровадження SOC і допоможе компанії ефективно впровадити SOC і уникнути проблем.

– Передати деякі функції SOC на аутсорсинг, щоб звільнити ресурси для інших пріоритетних завдань.

– Використовувати більш прості технології і підходи, які, тим не менше, забезпечують достатньо високий рівень безпеки.

– Залучити досвідчених консультантів з кібербезпеки, які поділяться цінним досвідом і знаннями щодо успішного впровадження SOC і уникнення типових проблем.

– Регулярно навчати персонал SOC, щоб фахівці команди центру володіли актуальними знаннями і практичними навичками за напрямами діяльності SOC і могли ефективно виконувати свої обов'язки.

– Переглядати процеси та процедури SOC регулярно та у разі виникнення нагальної потреби, щоб вони залишалися ефективними і відповідали поточним тенденціям розвитку галузі кібербезпеки, змінам ландшафту загроз і технологій кіберзахисту.

– Удосконалювати комунікацію між SOC і іншими підрозділами компанії з використанням ефективних каналів комунікації, щоб забезпечити належний обмін інформацією і скоординовану взаємодії [57, 58].

На рис 2.7 представлено проблеми реалізації SOC і заходи їх запобігання.

Рис 2.7. Проблеми впровадження SOC і заходи щодо їх запобігання.

Перспективи розвитку SOC

У міру того, як кіберзагрози стають все більш складними, роль SOC також зростає, а ключовою вимогою є здатність SOC виявляти і реагувати на кібератаки в реальному часі, а також розробляти і впроваджувати заходи для захисту від майбутніх загроз. Крім того SOC має адаптуватися до нових тенденцій розвитку підходів і методів забезпечення кібербезпеки.

Так, SOC повинні бути інтегровані з іншими системами і процесами компанії, такими як інформаційні системи, системи управління ризиками та системи управління бізнес-процесами, що допоможе забезпечити ефективний захист бізнесу від кібератак. Наприклад, SOC можуть бути інтегровані з системами управління інформаційною безпекою (ISMS), щоб забезпечити ефективний моніторинг і управління ризиками безпеки. SOC також можуть бути інтегровані з системами управління бізнес-процесами (BPM), щоб забезпечити ефективне реагування на інциденти безпеки, які можуть вплинути на бізнес-процеси.

Автоматизація може допомогти підвищити продуктивність і ефективність SOC за рахунок використання автоматизованих інструментів для моніторингу, виявлення загроз і реагування на інциденти. Наприклад, SOC можуть використовувати автоматизовані інструменти для моніторингу мережевого трафіку, щоб виявляти аномалії, які можуть вказувати на кібератаки, а також автоматизовані засоби реагування на інциденти, щоб скоротити час реагування і мінімізувати збитки.

Використання штучного інтелекту (AI) і машинного навчання (ML) може допомогти SOC у виявленні і реагуванні на кібератаки. AI використовують для аналізу великих наборів даних і виявлення аномалій, які можуть вказувати на кібератаки. Наприклад, SOC можуть використовувати AI для аналізу даних про мережевий трафік, щоб виявляти приховані загрози, і розробки нових методів їх виявлення і реагування. Також SOC можуть використовувати AI для виявлення кібератак, які використовують нові і складні методи. SOC також можуть

використовувати AI і ML для розробки нових методів реагування на кібератаки, які є більш ефективними і менш витратними.

Кібербезпека як послуга (Security as a Service, SaaS) - це нова модель надання кіберпослуг. SaaS дозволяє компаніям отримувати доступ до кіберпослуг від постачальника без необхідності інвестувати у власні ресурси та обладнання. SaaS може бути хорошим варіантом для компаній, які не мають достатніх ресурсів для створення власного SOC. SaaS також може бути хорошим варіантом для компаній, які хочуть отримувати доступ до найновіших технологій кібербезпеки [59].

Кібербезпека в реальному часі (Real-time Cybersecurity) - це нова парадигма кібербезпеки, яка фокусується на виявленні і реагуванні на кібератаки в реальному часі. SOC будуть відігравати ключову роль у розвитку кібербезпеки в реальному часі. Наприклад, SOC можуть використовувати AI і ML для виявлення й реагування на кібератаки в реальному часі, щоб мінімізувати збитки.

Співпраця між SOC, насамперед тими, що захищають критичну інфраструктуру, є обов'язковою, щоб обмінюватися інформацією про кібератаки, формувати повне уявлення про кіберзагрози й розробити більш ефективні заходи захисту. Ця співпраця може бути організована в рамках державних або приватних ініціатив [60].

3.4 Принципи впровадження SOC на підприємствах малого бізнесу

Для ефективного впровадження центру безпеки SOC у малих підприємствах необхідно дотримуватися кількох основних принципів.

Перший принцип: малі підприємства повинні починати з малого. Не потрібно намагатися побудувати повнофункціональний SOC з самого початку. Замість цього, малі підприємства мають починати з базових функцій, таких як

моніторинг безпеки та виявлення інцидентів. Потім вони можуть поступово розширювати SOC у міру зростання своїх потреб.

Цей принцип важливий, оскільки він допомагає малим підприємствам уникнути непотрібних витрат і труднощів. Повнофункціональний SOC може бути дорогим і складним для управління. Малі підприємства часто не мають ресурсів для підтримки повнофункціонального SOC.

Другий принцип: малі підприємства повинні використовувати доступні інструменти й технології, щоб не перевищувати свій бюджет. Існує багато доступних інструментів і технологій, які можуть допомогти побудувати SOC.

Цей принцип важливий, оскільки він допомагає малим підприємствам отримати доступ до необхідних функцій SOC без надмірних витрат. Існує багато відкритого програмного забезпечення та інших безкоштовних інструментів, які можуть бути використані для побудови SOC.

Третій принцип: малі підприємства повинні забезпечити навчання і тренування персоналу SOC. Персонал SOC має бути належим чином фахово підготовленим до виконання своїх функцій. Малі компанії повинні забезпечити, щоб їхній персонал SOC залучався до регулярного навчання з актуальних питань інформаційної безпеки.

Цей принцип важливий, оскільки він допомагає забезпечити ефективне функціонування SOC. Персонал SOC має бути знайомий з останніми загрозами й методами захисту, а також ефективно реагувати на інциденти безпеки.

Четвертий принцип: малі підприємства повинні регулярно оцінювати роботу центру безпеки і впроваджувати необхідні вдосконалення. Регулярне оцінювання допоможе забезпечити ефективне функціонування SOC.

Цей принцип важливий, оскільки він допомагає SOC залишатися актуальним у мінливому ландшафті кібербезпеки. SOC повинні регулярно оцінюватися, щоб визначити, чи відповідають вони поточним потребам компанії.

Висновки до розділу 3

У результаті дослідження встановлено, що основними чинниками, які визначають підходи малих підприємств до організації SOC є: невеликі обсяги даних, які потребують захисту; обмежений фінансові можливості компанії; наявність невеликої кількості персоналу.

Інформаційними системами малого бізнесу, які потребують захисту, є системи управління ресурсами підприємства (ERP), системи управління продажами і маркетингом (CRM), електронна пошта, телефонія, відеоконференції, системи управління доступом (IAM) і резервного копіювання.

Для забезпечення функціонування базових IT-сервісів на малому підприємстві необхідно спроектувати та впровадити відповідну мережеву й серверну інфраструктуру, яка забезпечить надійну передачу даних, доступ до Інтернету та інших ресурсів, а також захист даних від порушень безпеки. Мережева інфраструктура включає комутатори, брандмауер, контролери доступу, мережеві точки доступу. Базова серверна інфраструктура складається з файл-сервера, поштового сервера, бази даних і віддаленого робочого місця.

Важливим аспектом забезпечення кібербезпеки будь-якої компанії є розмежування обов'язків, завдяки якому зменшується ризик появи незахищених ділянок в інформаційному ландшафті. Існує кілька інструментів узгодження й документування ролей і обов'язків персоналу, залученого до забезпечення безпеки корпоративного середовища, одним із яких є RACI-таблиця.

Дослідження показало, що при впровадженні SOC на малому підприємстві спостерігається низка типових проблем, серед яких: брак ресурсів, недосконалі процеси і процедури, недостатня підготовка персоналу, неефективна комунікація. Для вирішення окреслених проблем компаніям необхідно: розробити план впровадження SOC з чітким визначенням цілей, завдань, ресурсів і термінів; передати деякі функції SOC на аутсорсинг; використовувати простіші технології і підходи безпеки; залучити досвідчених консультантів з

кібербезпеки ззовні; регулярно навчати персонал SOC з питань безпеки; переглядати процеси та процедури SOC періодично або за потреби; вдосконалювати комунікацію між SOC і іншими підрозділами компанії.

Встановлено, що для ефективного впровадження центру безпеки SOC підприємства малого бізнесу повинні: починати з впровадження базових функцій, використовувати доступні інструменти й технології, забезпечити навчання і тренування персоналу, регулярно оцінювати роботу SOC і впроваджувати необхідні вдосконалення.

ВИСНОВКИ

Встановлено, що центр безпеки (SOC) є оперативним координаційним центром для виявлення, аналізу й реагування на інциденти кібербезпеки. Типова місія SOC включає такі елементи: запобігання інцидентам; моніторинг безпеки; реагування на підтверджені інциденти; ситуаційне інформування та звітування про стан кібербезпеки; розробка й експлуатація технологій SOC.

Аналіз джерел показав, що SOC виконує багато різних функцій, які умовно можна поділити на сім категорій: сортування, аналіз і реагування на інциденти; розвідка, пошук і аналітика кіберзагроз; розширені операції SOC; управління вразливостями; інструменти, архітектура й інженерія SOC; ситуаційна обізнаність, комунікація та навчання; лідерство й управління. Вибір функцій SOC залежить від потреб і можливостей організації.

З’ясовано, що перші центри операційної безпеки були створені для сектору оборони. У відповідь на зростаючі загрози, пов’язані з цифровізацією та розвитком Інтернету, й потребу в комплексній централізованій інфраструктурі для моніторингу, аналізу й реагування на виникаючі інциденти,.

У наукових працях виділяють чотири покоління SOC, перші комерційні зразки яких були творені в 90-х роках. Сучасні SOC використовують комплекс сервісів безпеки: аналіз великих даних; збагачення даних, які надходять із різних джерел; розвідка загроз; розслідування інцидентів тощо. Викликами для сучасних SOC є поява нових ризиків і забезпеченні кіберстійкості; віддалене управління; автоматизація операцій з використанням AI та ML; брак кваліфікованого персоналу; масштабність і мультифункціональність SOC.

Дослідження показало, що великі компанії, які мають більше даних, ресурсів і впливу, стикаються з більш складними кіберзагрозами і є більш привабливими цілями для хакерів. Крім цього великі підприємства також мають більш складну інфраструктуру, що ускладнює виявлення й реагування на кібератаки. Водночас, компанії великого бізнесу мають можливість інвестувати

в більш розвинені SOC з внутрішніми командами, новітніми технологіями й інструментами, щоб ефективно виявляти та реагувати на ускладнені кібератаки.

Середні підприємства, як правило, мають менші бюджети та ресурси, ніж великі компанії, тому вони можуть використовувати аутсорсинг і стандартизовані рішення для забезпечення кібербезпеки. Аутсорсинг дозволяє середнім підприємствам отримати доступ до спеціалізованих знань та досвіду, не інвестуючи у власні ресурси. Стандартизовані рішення можуть допомогти середнім підприємствам зменшити витрати і полегшити масштабування.

Для підприємств середнього і великого бізнесу важливо, щоб реалізація SOC було частиною комплексної стратегії кібербезпеки, яка відповідає конкретним потребам компанії, враховує її розмір, ресурси і специфіку роботи.

При реалізації великих і середніх SOC доцільно використовувати засоби AI та ML, які дозволяють пришвидшити процеси обробки інформації, забезпечити просунуту аналітику, автоматизувати рутинні й повторювані процеси, розпізнавати шаблони в даних, розробляти прогнози і підвищити ефективність корпоративних систем безпеки загалом.

Встановлено, що основними чинниками, які визначають підходи малих підприємств до організації SOC є: невеликі обсяги даних, які потребують захисту; обмежений фінансові можливості компанії; наявність невеликої кількості персоналу.

Дослідження показало, що при впровадженні SOC на малому підприємстві спостерігається низка типових проблем, серед яких: брак ресурсів, недосконалі процеси і процедури, недостатня підготовка персоналу, неефективна комунікація. Для вирішення окреслених проблем компаніям необхідно: розробити план впровадження SOC з чітким визначенням цілей, завдань, ресурсів і термінів; передати деякі функції SOC на аутсорсинг; використовувати простіші технології і підходи безпеки; залучити досвідчених консультантів з кібербезпеки ззовні; регулярно навчати персонал SOC з питань безпеки; переглядати процеси та процедури SOC періодично або за потреби; вдосконалювати комунікацію між SOC і іншими підрозділами компанії.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cisco, “What Is an Advanced Persistent Threat (APT)?,” 29 October 2021. URL: https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html.
2. Kathryn Knerler, Ingrid Parker, Carson Zimmerman. 11 Strategies of a World-Class Cybersecurity Operations Center. URL: https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf
3. What Is a Security Operations Center? URL: https://www.trellix.com/security-awareness/operations/what-is-soc/
4. Committee on National Security Systems (CNSS), “CNSS Instruction No. 4009 Glossary,” 6 April 2015. URL: https://www.cnss.gov/CNSS/openDoc.cfm?YV5eCARxrtHkRwkrYRARpQ==
5. Natalia G. Miloslavskaya. Security Operations Centers for Information Security Incident Management. URL: https://www.researchgate.net/publication/306938995_Security_Operations_Centers_for_Information_Security_Incident_Management
6. CISA Insider Threat Mitigation. Cybersecurity and Infrastructure Security Agency (CISA), November 2021. URL: https://www.cisa.gov/insider-threatmitigation
7. Static vs Dynamic Analysis. URL: https://rahulsinghinfosec.github.io/hackme/reverse-engineering/static-vs-dynamic-analysis.html
8. Threat Intelligence vs Threat Hunting. URL: https://www.sapphire.net/managed-security-services/threat-intelligence-vs-threat-hunting/
9. Threat tactics, techniques, and procedures (TTP). URL: https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures/
10. Red Teaming. URL: https://www.synopsys.com/glossary/what-is-red-teaming.html
11. Purple teaming explained. URL: https://www.crowdstrike.com/cybersecurity-101/purple-teaming/
12. Deception technology: a critical component of a modern cyber security stack. Attivo Networks, 2021. URL: https://www.attivonetworks.com/wp-content/

uploads/sites/13/documentation/Attivo_Networks-Understanding_Deception_Technology.pdf

13. Security and Privacy Controls for Information Systems and Organizations. NIST, December 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

14. Cyberpedia. What is an Endpoint? URL: _https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint

15. What is a Cloud Access Security Broker (CASB)? URL: https://www.skyhighsecurity.com/cybersecurity-defined/what-is-a-casb.html

16. Planning and Executing Scenario Based Simulation Exercises: Methodological Lessons. URL: https://www.degruyter.com/document/doi/10.1515/jhsem-2013-0077/html

17. Evolution Of Security Operations. URL: https://www.cioandleader.com/article/2023/08/23/evolution-security-operations

18. Computer Security Resource Center. NIST Glossary. URL: https://csrc.nist.gov/glossary/term/exfiltration

19. E. Ayhan, M. Tannous. Modeling a Security Operations Center, 2022. URL: https://www.diva-portal.org/smash/get/diva2:1703746/FULLTEXT01.pdf

20. A. N. Muniz J, Mclntyre G. Security Operations Center Building, Operating and Maintaining Your SOC. Cisco Press, San Jose, CA, 2015.

21. M. Smith. The SOC is dead, long live the SOC! URL: https://ieeexplore.ieee.org/document/9104585

22. T. Pötter. Security Operations Center (SOC): SOC Generations 1-6 and OpenSource SOC Architecture. URL: https://www.researchgate.net/publication/333682708_Security_Operations_Center_SOC_SOC_Generations_1-6_and_OpenSource_SOC_Architecture_Graphics_DEEN

23. GANs: Generative Adversarial Networks - An Advanced Solution for Data Generation. URL: https://towardsdatascience.com/gans-generative-adversarial-networks-an-advanced-solution-for-data-generation-2ac9756a8a99

24. Cyber Grand Challenge. Defense Advanced Research Projects Agency. URL: https://www.darpa.mil/about-us/timeline/cyber-grand-challenge

25. What is a Security Operations Center (SOC)? URL: https://www.opentext.com/what-is/security-operations-center#related-products
26. L. Kleinman. The Evolution Of The Modern Security Operations Center. URL: https://www.forbes.com/sites/forbestechcouncil/2023/06/16/the-evolution-of-the-modern-security-operations-center/?sh=75cfea3b1062
27. Zero Trust Model - Modern Security Architecture – Microsoft. URL: https://www.microsoft.com/en-us/security/business/zero-trust
28. ISC2 Cybersecurity Workforce Study. How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, 2023. URL: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e
29. R. Bidou. Security Operation Center Concepts & Implementation. URL: https://www.researchgate.net/publication/228587242_Security_Operation_Center_Concepts_Implementation
30. Manfred Vielberth Security Operations Center (SOC). URL: https://www.researchgate.net/ publication/349312209_Security_Operations_Center_SO
31. Why Every Company Needs A SOC. URL: https://www.ek.co/publications/why-every-company-needs-a-soc/ 14 July 2021
32. Behrad Shaporzade. Building a Security Operations Center (SOC). URL: https://www.academia.edu/33355557/Building_a_Security_Operations_Center_SOC
33. G. Jarpey and R. Scott McCoy. Security Operations Center Guidebook. A Practical Guide for a Successful SOC. 2017. 186 p.
34. Cybersecurity as a Service. URL: https://www.sophos.com/en-us/cybersecurity-explained/what-is-cybersecurity-as-a-service-csaas
35. SOC Model Guide: Gartner Research. URL: https://www.gartner.com/en/documents/4851731
36. 5 Steps to Building and Operating an Effective Security Operations Center (SOC). URL: https://www.ciscopress.com/articles/article.asp?p=2460771

37. Tools and technologies used in SOCs. URL: https://www.manageengine.com/log-management/siem/soc-tools-technologies.html

38. Implementing Artificial Intelligence and Machine Learning in Cybersecurity Solutions. URL: https://www.apriorit.com/dev-blog/474-ai-ml-cybersecurity

39. What is cyber threat hunting? URL: https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

40. Machine learning (ML) in cybersecurity. URL: https://www.sailpoint.com/identity-library/how-ai-and-machine-learning-are-improving-cybersecurity/

41. Shouq Alnemari, Majid Alshammari. Detecting Phishing Domains Using Machine Learning. URL: https://www.mdpi.com/2076-3417/13/8/4649

42. SOC and SIEM: The Role of SIEM Solutions in the SOC. URL: https://www.exabeam.com/explainers/siem-security/the-soc-secops-and-siem/

43. Gaurav Jagadeesh. Importance of SOAR in SOC team. URL: https://www.linkedin.com/pulse/importance-soar-soc-team-gaurav-jagadeesh

44. IBM Security QRadar Suite. URL: https://www.ibm.com/qradar

45. SOC for Small & Medium Size Businesses. URL: https://www.issp.com/post/soc-for-small-medium-size-businesses

46. 4 Qualities of an Efficient Security Operations Center for Telecom. URL: https://www.infopulse.com/blog/soc-telecom-implementation

47. Mark Roy Long. A Small Business Guide to the Security Operations Center (SOC). URL: https://www.fool.com/the-ascent/small-business/it-management/articles/soc/

48. SOC for Small & Medium Size Businesses. URL: https://www.issp.com/post/soc-for-small-medium-size-businesses

49. Центр безпеки (SOC) як сервіс. URL: https://www.h-x.technology/ua/services/soc-service-ua

50. How To Build A Soc With Limited Resources: White Paper. URL: https://www.scribd.com/document/434733689/How-to-Build-a-Soc-With-Limited-Resources-White-Paper

51. Samuel Christopher Dixon What Is a RACI Chart? Definition, Template, and Examples. URL: https://www.wrike.com/blog/what-is-a-raci-chart/

52. Lauren Good What Is a RACI Matrix? URL: https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/
53. Security Operations Center RACI Matrix Template. URL: https://clickup.com/ templates/raci-matrix/security-operations-center
54. How to Build a Security Operations Center for Small Companies. URL: https://www.exabeam.com/security-operations-center/how-to-build-a-security-operations-center/
55. Securing Success: Why Small and Medium Enterprises (SMEs) Need a Security Operations Center (SOC). URL: https://www.linkedin.com/pulse/securing-success-why-small-medium-enterprises
56. Top Security Operations Center Challenges. URL: https://www.iiot-world.com/ics-security/cybersecurity/top-challenges-soc-are-facing/
57. John Burke. 8 challenges every security operations center faces. URL: https://www.techtarget.com/searchsecurity/tip/8-challenges-every-security-operations-center-faces
58. M. Saraiva, N. Mateus-Coelho. CyberSoc Framework a Systematic Review of the State-of-Art. URL: https://www.researchgate.net/publication/363471986_CyberSoc_Framework_a_Systematic_Review_of_the_State-of-Art
59. The SOC of the Future - Infosecurity Magazine. URL: https://www.infosecurity-magazine.com/magazine-features/the-soc-of-the-future/
60. Security Operation Center. URL: https://www.reply.com/contents/COMVR11_SOC_eng.pdf