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 НА АУТСОРСИНГОВІЙ ОСНОВІ: ПЕРЕВАГИ І НЕДОЛІКИ"

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

_____ Максим ХАРИТОНЧУК

(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Максим ХАРИТОНЧУК

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 Харитончуку Максиму Михайловичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "ЦЕНТР БЕЗПЕКИ SOC НА АУТСОРСИНГОВІЙ ОСНОВІ: ПЕРЕВАГИ І НЕДОЛІКИ"

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, загрози кібербезпеці, центр безпеки (Security Operation Center, SOC), SOC на аутсорсинговій основі.
4. Перелік питань, які потрібно розробити:
   1. З'ясувати роль і функції центру безпеки (SOC) у забезпеченні кібербезпеки підприємства.
   2. Дослідити етапи розробки й розгортання SOC
   3. Встановити переваги й недоліки аутсорсингу SOC і запропонувати рекомендації щодо впровадження SOC для різних організацій.
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 ролі і функцій центру безпеки SOC у забезпеченні кібербезпеки підприємства.	27.10.2023	
4.	Дослідження етапів розробки й розгортання центру безпеки SOC.	10.11.2023	
5.	Встановлення переваг і недоліків аутсорсингу SOC і розробка відповідних рекомендацій.	15.11.2023	
6.	Формулювання висновків за результатами проведеного 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.	19.01.2024	

Здобувач вищої освіти _____ Максим ХАРИТОНЧУК
(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 Харитончук М.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 НА АУТСОРСИНГОВІЙ ОСНОВІ: ПЕРЕВАГИ І НЕДОЛІКИ"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **ХАРИТОНЧУК Максим** у кваліфікаційній роботі з'ясував роль і функції центру безпеки (SOC) у забезпеченні кібербезпеки підприємства, дослідив етапи розробки й розгортання SOC, встановив переваги й недоліки аутсорсингу SOC і запропоновував рекомендації щодо впровадження SOC для різних організацій.

ХАРИТОНЧУК Максим оволодів методами наукового дослідження, опрацював достатню джерельну базу за предметом дослідження. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено згідно з планом, зроблено відповідні висновки. Ключові положення роботи представлено у вигляді зображень.

Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу".

Це дозволяє оцінити виконану кваліфікаційну роботу здобувача **ХАРИТОЧНУКА Максима** 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 Харитончук М.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 Харитончука Максима Михайловича
на тему "ЦЕНТР БЕЗПЕКИ SOC НА АУТСОРСИНГОВІЙ ОСНОВІ: ПЕРЕВАГИ І НЕДОЛІКИ"

Актуальність

Як свідчить практика, кількість кібератак зростає, незважаючи на появу нових інструментів безпеки. Очікується, що загрози кібербезпеці зростатимуть щонайменше на 15% на рік, і під загрозу потраплять компанії будь-якого розміру.

Щоб усунути мінливий ландшафт загроз, одних лише точкових рішень недостатньо, оскільки команди безпеки все ще перевантажені помилковими спрацьовуваннями, навіть за наявності найкращих технологій і процесів. Одним із варіантів вирішення цих проблем є створення центру безпеки SOC, який забезпечить виявлення, аналіз, стримування та усунення загроз та інцидентів кібербезпеці.

Завдяки швидкій ідентифікації, реакції та співпраці компанії, які мають власний або використовують послуги аутсорсингового SOC, мають набагато більше шансів успішно та ефективно відреагувати на кібератаки.

Позитивні сторони

У кваліфікаційній роботі з'ясовано роль і функції центру безпеки (SOC) у забезпеченні кібербезпеки підприємства, досліджено етапи розробки й розгортання SOC, встановлено переваги й недоліки аутсорсингу SOC і запропоновано рекомендації щодо впровадження SOC для різних організацій.

Здобувач оволодів методами наукового дослідження, опрацював достатню джерельну базу за предметом дослідження. Кваліфікаційна робота оформлена у відповідності з вимогами, а її структура забезпечує досягнення мети і завдань.

Недоліки

1. Доцільно було б навести більше прикладів практичного використання послуг аутсорсингового SOC.

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 Харитончук Максим Михайлович заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Рецензент:

_____
підпис *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 81 стор., 18 рис., 62 джерела.

Метою роботи є дослідження переваг і недоліків центру безпеки SOC на аутсорсинговій основі.

Об'єктом дослідження є засади розробки і функціонування центру безпеки SOC.

Предмет дослідження – переваги і недоліки центру безпеки SOC на аутсорсинговій основі.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використано методи системного аналізу, синтезу, порівняння й теоретичного узагальнення, класифікації.

Короткий зміст роботи. Як результат у роботі з'ясовано роль і функції центру безпеки (SOC) у забезпеченні кібербезпеки підприємства; досліджено етапи розробки й розгортання SOC; встановлено переваги й недоліки аутсорсингу SOC і запропоновано рекомендації щодо впровадження SOC для різних організацій.

Галузь застосування. Розроблені підходи можуть бути використані для прийняття обґрунтованого рішення щодо вибору варіанту центру безпеки SOC: власного або аутсорсингового, а також при плануванні, реалізації та забезпеченні функціонування корпоративного центру безпеки SOC обох видів.

КЛЮЧОВІ СЛОВА : КІБЕРБЕЗПЕКА ПІДПРИЄМСТВА, ЗАГРОЗИ КІБЕРБЕЗПЕЦІ, ЦЕНТР БЕЗПЕКИ (SECURITY OPERATION CENTER, SOC), SOC НА АУТСОРСИНГОВІЙ ОСНОВІ.

ABSTRACT

The text part of the qualification work for obtaining the master's degree: 81 pages, 18 figures, 62 sources.

The purpose of the work is to study the advantages and disadvantages of the SOC security center on an outsourced basis.

The object of research is the principles of development and operation of the SOC security center.

Subject of research is to solve the above-mentioned scientific task, methods of system analysis, synthesis, comparison and theoretical generalization, classification were used in the work.

Research methods. Methods of system analysis, synthesis, comparison and theoretical generalization, classification were used in the work.

Brief content of research. As a result, the work clarified the role and functions of the security center (SOC) in ensuring the cyber security of the enterprise; the stages of SOC development and deployment were investigated; advantages and disadvantages of SOC outsourcing are identified and recommendations for SOC implementation for various organizations are proposed.

Field of research. The developed approaches can be used to make an informed decision regarding the choice of an SOC security center option: own or outsourced, as well as when planning, implementing and ensuring the functioning of a corporate SOC security center of both types.

KEYWORDS: CYBER SECURITY OF ENTERPRISES, CYBER SECURITY THREATS, SECURITY OPERATION CENTER (SOC), OUTSOURCED SOC.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service
DLP	Data Leak Prevention
DoS	Denial-of-Service
EDR	Endpoint detection and response
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IoT	Internet of Things
MDM	Mobile Device Management
MSSP	Managed Security Service Provider
NAC	Network Access control
NGAV	Next Generation Antivirus
NGFW	Next Generation Firewall
NTP	Network Time Protocol
SEM	Security Event Management
SIEM	Security Information & Event Management
SLMS	Security Log Management Service
SNMP	Simple Network Management Protocol
SOC	Security Operation Center
SOAR	Security Operation Orchestration and Response
UEBA	User & Entity Behavior Analytics
WAF	Web Application Firewall
XEDR	Extended Endpoint Detection and Response

ВСТУП

Актуальність теми. Інформація завжди була як найважливішим об'єктом, так і засобом боротьби між людьми. Неможливо заперечувати факти здійснення інформаційного впливу на широку аудиторію протягом усіх етапів історичного розвитку, хоча в різні періоди інтенсивність застосування тих чи інших способів впливу, як і досконалість його організації, значною мірою відрізнялися.

На сучасному етапі різноманітні засоби інформаційного впливу активно застосовуються конкуруючими фірмами та корпораціями в конкурентній боротьбі за встановлення контролю на ринку та домінування у відповідній сфері.

Тому політика забезпечення інформаційної безпеки підприємства має буде побудована з урахуванням потреби запобігати і протидіяти загрозам, що виникають внаслідок застосування методів інформаційного протиборства, захищати потенційно важливі інформацію, інфраструктуру та персонал як стратегічний ресурс підприємства.

З огляду на зазначене тема кваліфікаційної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки суб'єктів підприємницької діяльності в умовах інформаційного протиборства.

Мета роботи полягає є дослідження переваг і недоліків центру безпеки SOC на аутсорсинговій основі.

Об'єкт дослідження є засади розробки і функціонування центру безпеки SOC.

Предмет дослідження – переваги і недоліки центру безпеки SOC на аутсорсинговій основі.

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

1. З'ясувати роль і функції центру безпеки (SOC) у забезпеченні кібербезпеки підприємства.

2. Дослідити етапи розробки й розгортання SOC

3. Встановити переваги й недоліки аутсорсингу SOC і запропонувати рекомендації щодо впровадження SOC для різних організацій.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використано методи системного аналізу, синтезу, порівняння й теоретичного узагальнення, класифікації.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані для прийняття обґрунтованого рішення щодо вибору варіанту центру безпеки SOC: власного або аутсорсингового, а також при плануванні, реалізації та забезпеченні функціонування корпоративного центру безпеки SOC обох видів.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформації, інфраструктури та персоналу підприємства у відповідності до цілей бізнесу, корпоративних можливостей та ресурсів в умовах інформаційного протиборства.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науковій конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу”.

РОЗДІЛ 1
ЦЕНТР БЕЗПЕКИ (SOC) У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

1.1 Теоретичні засади кібербезпеки

Інформація є невід'ємною частиною навколишнього світу та нашої свідомості.

Інформаційна безпека своєю назвою вказую на важливість інформації в суспільстві та показує цінність інформації на рівні з багатством, як гроші та дорогоцінні метали.

Метою інформаційної безпеки є захист інформації та інфраструктури, яка її підтримує, від будь-якого випадкового чи зловмисного втручання, яке може призвести до втрати або накопичення інформації в Інтернеті, пошкодження її безпосередніх власників та інфраструктури, яка підтримує її зберігання та існування. Інформаційна безпека виконує завдання, пов'язані з передбаченням і запобіганням можливих подібних дій, а також мінімізацією можливої шкоди.

Основні аспекти інформаційної безпеки можна побачити на рис. 1.1.

Рис. 1.1. Тріада інформаційної безпеки

Доступність (Availability) – це можливість за прийнятний час одержати необхідну інформаційну послугу.

Інформаційні системи створюються для отримання певних інформаційних послуг. Якщо з тих чи інших причин надання цих послуг користувачам стає неможливим, це, очевидно, завдає шкоди всім сторонам інформаційних відносин, оскільки нові клієнти не можуть отримати інформацію про послуги, що надаються сервісом. Тому цей аспект слід виділити як найважливіший.

Головна роль доступності особливо яскраво проявляється в різних системах управління – виробництві, транспорті тощо. Зовні менш драматичні, але й дуже неприємні наслідки – як матеріальні, так і моральні – може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та авіаквитків, банківські послуги тощо).

Цілісність (Integrity) – це актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни.

Цілісність є певним аспектом ІБ у тих випадках, коли вона служить «керівництвом до дії». Рецептурні препарати, медичні процедури, набір і характеристики компонентів, хід технологічного процесу - все це приклади інформації, цілісність, яку можна оцінити як, буквально, смертельну. Також неприємно спотворювати офіційну інформацію в тексті закону, на сторінці веб-сервера інформації чи десь у державній організації, де інформація є важливою.

Конфіденційність (Confidentiality) – це захист інформації від попадання до рук тих осіб, які не повинні мати доступ до неї.

Конфіденційні моменти є у багатьох організаціях. Закрита інформація про СУІБ, документи що регламентують оцінку ризиків, діяльність співробітників, розписані карти мережі, списки серверів тощо. Виток хоча б одного з них для людини що не має доступу до них може полегшити завдання для зловмисників при побудові плану дії після експлуатації вразливості [12].

Кібербезпека стосується всіх аспектів захисту організації, її співробітників і активів. Оскільки кібератаки стають все більш поширеними та складними, а

корпоративні мережі стають все більш розмежованими, для зменшення корпоративного кіберризику потрібні різноманітні рішення кібербезпеки.

Кібербезпека - це широка галузь, яка охоплює кілька напрямів (Рис. 1.2).

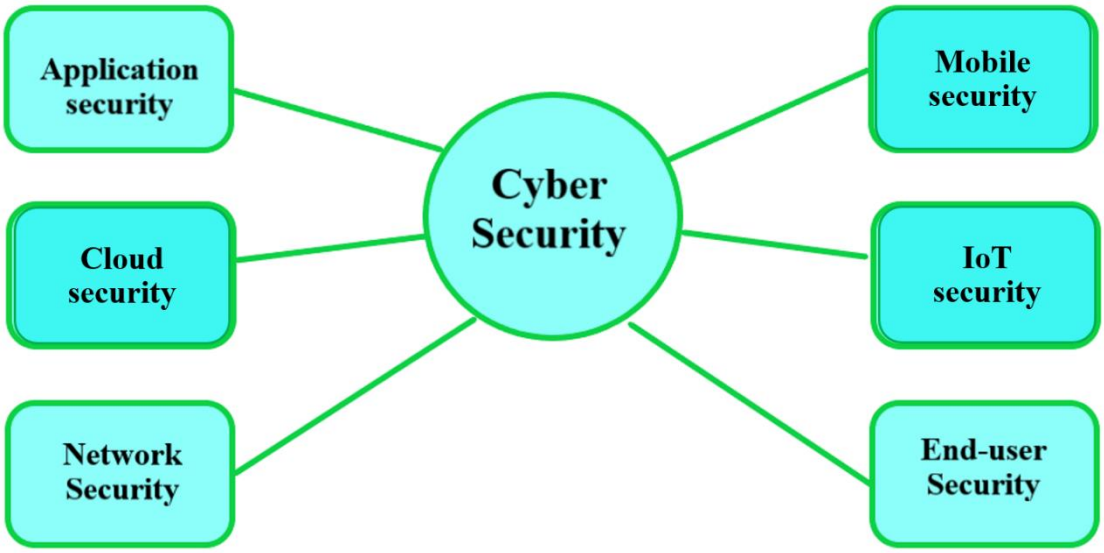

Рис. 1.2. Складові кібербезпеки

Безпека мережі. Більшість атак відбувається через мережу і рішення для захисту мережі розроблені для виявлення та блокування цих атак. Ці рішення включають елементи управління даними та доступом, такі як запобігання втраті даних (DLP), IAM (управління доступом до ідентифікаційної інформації), NAC (контроль доступу до мережі) і NGFW (мережевий екран наступного покоління) для дотримання правил безпечного використання Інтернету.

Передові та багаторівневі технології запобігання мережевим загрозам включають IPS (систему запобігання вторгненням), NGAV (антивірус наступного покоління), ізольоване програмне середовище та CDR (зняття з охорони та відновлення вмісту). Також важливими є мережева аналітика, полювання на загрози та автоматизовані технології SOAR (Security Orchestration and Response).

Хмарна безпека. Оскільки організації все частіше використовують хмарні обчислення, безпека хмари стає головним пріоритетом. Стратегія хмарної безпеки включає рішення, елементи керування, політики та служби

кібербезпеки, які допомагають захистити від атак усе хмарне розгортання організації (програми, дані, інфраструктуру тощо).

Незважаючи на те, що багато постачальників хмарних послуг пропонують рішення безпеки, вони часто не відповідають завданням досягнення рівня корпоративної безпеки у хмарі. Для захисту від витоку даних і цілеспрямованих атак у хмарних середовищах необхідні додаткові сторонні рішення.

Безпека кінцевих точок. Модель безпеки з нульовою довірою передбачає створення мікросегментів навколо даних, де б вони не були. Один зі способів зробити це за допомогою мобільної робочої сили – це захист кінцевої точки. Завдяки безпеці кінцевих точок компанії можуть захистити пристрої кінцевих користувачів, як-от настільні комп'ютери та ноутбуки, за допомогою засобів керування безпекою даних і мережі, передового захисту від загроз, таких як захист від фішингу та програм-вимагачів, а також технологій, які забезпечують криміналістику, наприклад виявлення кінцевих точок і реагування на них (EDR) [39].

Мобільна безпека. Часто забувають про те, що мобільні пристрої, такі як планшети та смартфони, мають доступ до корпоративних даних, наражаючи компанії на загрози з боку шкідливих програм, нульового дня, фішингу та атак миттєвих повідомлень. Мобільна безпека запобігає цим атакам і захищає операційні системи та пристрої від рутингу та джейлбрейка. Якщо це включено до рішення MDM (Mobile Device Management), це дає змогу підприємствам забезпечити доступ до корпоративних активів лише сумісним мобільним пристроям [39].

Безпека IoT. Хоча використання пристроїв Інтернету речей (IoT) безсумнівно підвищує продуктивність, воно також наражає організації на нові кіберзагрози. Зловмисники шукають уразливі пристрої, випадково підключені до Інтернету, для зловмисного використання, наприклад для доступу до корпоративної мережі або іншого бота в глобальній мережі.

Безпека IoT захищає ці пристрої за допомогою виявлення та класифікації підключених пристроїв, автоматичної сегментації для контролю мережевих дій і

використання IPS як віртуального патча для запобігання експлойтам проти вразливих пристроїв IoT. У деяких випадках мікропрограму пристрою також можна доповнити невеликими агентами, щоб запобігти експлойтам і атакам під час виконання.

Безпека програм. Веб-програми, як і будь-що інше, безпосередньо підключене до Інтернету, є цілями для зловмисників. З 2007 року OWASP відслідковує 10 найпоширеніших загроз критичних недоліків безпеки веб-додатків, таких як ін'єкція, несправна автентифікація, неправильна конфігурація та міжсайтовий сценарій.

Завдяки безпеці програми можна зупинити атаки OWASP Top 10. Безпека програм також запобігає атакам ботів і припиняє будь-яку зловмисну взаємодію з програмами та API. Завдяки постійному навчанню програми залишатимуться захищеними, навіть якщо DevOps випускає новий вміст.

Модель нульової довіри. Традиційна модель безпеки зосереджена на периметрі, будуючи стіни навколо цінних активів організації, як замок. Однак цей підхід має кілька проблем, таких як потенціал внутрішніх загроз і швидке розпад периметра мережі.

Оскільки корпоративні активи переміщуються за межі підприємства в рамках впровадження хмари та віддаленої роботи, потрібен новий підхід до безпеки. Нульова довіра використовує більш деталізований підхід до безпеки, захищаючи окремі ресурси за допомогою поєднання мікросегментації, моніторингу та застосування контролю доступу на основі ролей [39].

1.2 Еволюція ландшафту загроз кібербезпеці

Сучасні кіберзагрози вже не такі, як кілька років тому. Оскільки ландшафт кіберзагроз змінюється, організаціям потрібен захист від поточних і майбутніх інструментів і методів кіберзлочинців.

Ландшафт загроз кібербезпеці постійно розвивається, і інколи ці досягнення представляють нове покоління кіберзагроз. На сьогоднішній день людство зіткнулося з п’ятьма поколіннями кіберзагроз і рішень, розроблених для їх пом’якшення, зокрема (Рис. 1.3):

Gen I (вірус): наприкінці 1980-х років вірусні атаки на автономні комп’ютери надихнули на створення перших антивірусних рішень.

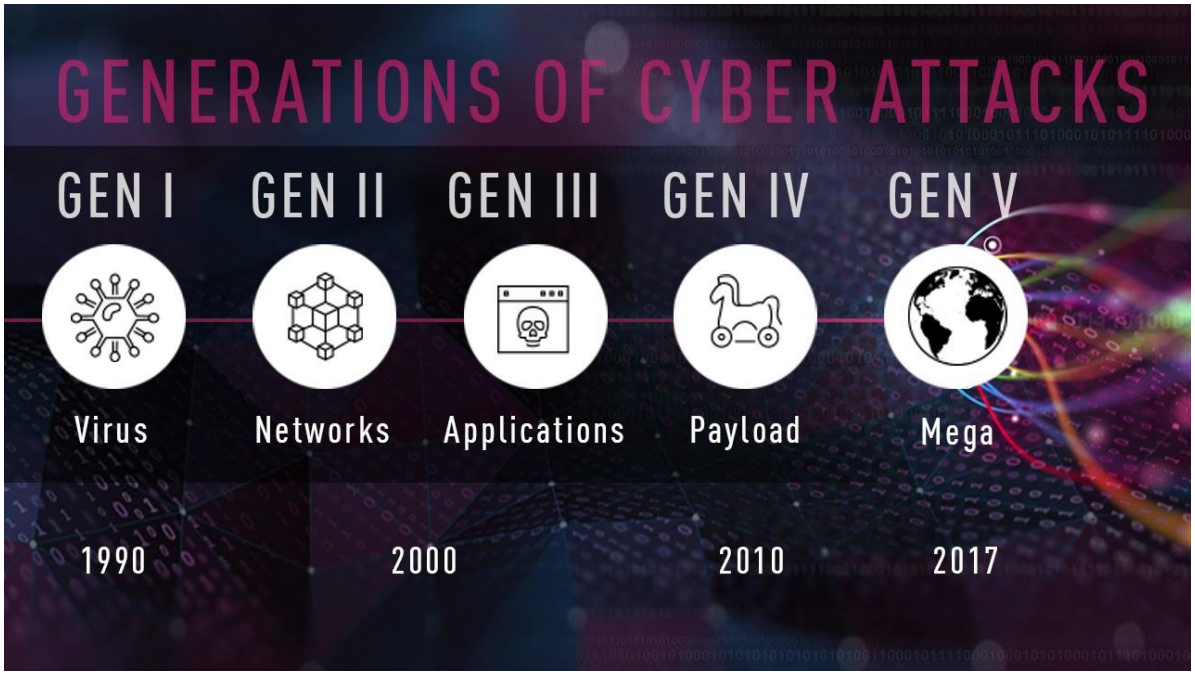

Рис. 1.3. Покоління кібератак

Gen II (мережа): Коли кібератаки почали відбуватися через Інтернет, був розроблений брандмауер, щоб ідентифікувати та блокувати їх.

Gen III (програми): використання вразливостей у програмах спричинило масове впровадження систем запобігання вторгненням (IPS).

Gen IV (корисне навантаження): оскільки зловмисне програмне забезпечення стало більш цілеспрямованим і здатним обійти захист на основі сигнатур, для виявлення нових загроз знадобилися рішення для захисту від ботів і ізольованого програмного середовища.

Gen V (мега): останнє покоління кіберзагроз використовує широкомасштабні багатовекторні атаки, що робить передові рішення для запобігання загрозам пріоритетом [39].

Кожне покоління кіберзагроз робило попередні рішення кібербезпеки менш ефективними або фактично застарілими. Для захисту від сучасної кіберзагрози потрібні рішення з кібербезпеки V покоління.

До найбільш поширених сучасних кіберзагроз відносять (Рис. 1.4):

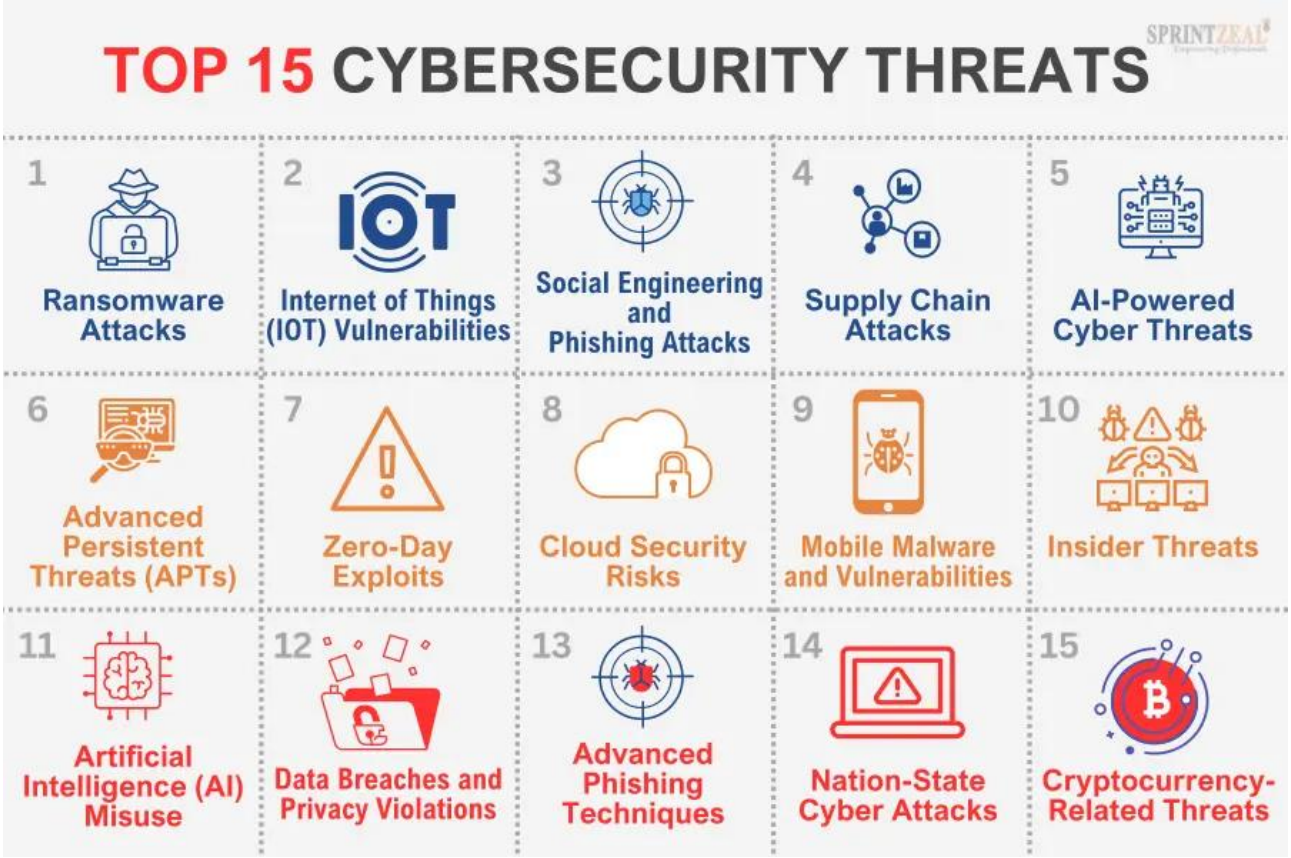

Рис. 1.4. Найбільш поширені кіберзагрози

1. Атаки програм-вимагачів

Атаки програм-вимагачів залишаються поширеною загрозою у 2023 році. Кіберзлочинці продовжують вдосконалювати свої методи, використовуючи передове шифрування та цільові стратегії. Ці атаки можуть паралізувати організації, що призведе до значних фінансових втрат і репутаційної шкоди.

З метою протидії таким загрозам доцільно використовувати розширене шифрування та цільові стратегії, а також надійні стратегії резервного копіювання, навчання обізнаності персоналу і регулярних виправлень безпеки.

2. Уразливості Інтернету речей (IoT)

З поширенням пристроїв IoT поверхня атаки для кіберзлочинців розширюється. У 2023 році вразливості IoT становлять значні ризики, оскільки

багато пристроїв не мають належних заходів безпеки. Хакери можуть використовувати ці слабкі місця, щоб отримати несанкціонований доступ або запустити розподілені атаки типу «Відмова в обслуговуванні» (DDoS). За рахунок поширення пристроїв IoT розширюється поверхня атаки, а відсутність адекватних заходів безпеки в багатьох пристроях IoT робить їх ще більш вразливими.

Пом'якшити вразливості IoT можна за допомогою надійних паролів, регулярного оновлення прошивки та сегрегації мережі.

3. Соціальна інженерія та фішингові атаки

Соціальна інженерія та фішингові атаки залишаються дуже успішними у 2023 році. Кіберзлочинці використовують складні методи та персоналізовану інформацію, щоб обдурити людей. Велика кількість персональних даних, доступних у соціальних мережах і на онлайн-платформах, робить ці атаки більш успішними.

Боротьба з соціальною інженерією та фішинговими атаками здійснюється за допомогою навчання обізнаності про кібербезпеку, двофакторної автентифікації й дотримання правил безпечного обміну інформацією.

4. Атаки на ланцюжки поставок

Атаки на ланцюжки поставок набули популярності в останні роки, і 2023 рік не став винятком. Проникаючи в системи надійних постачальників або надавачів послуг, хакери компрометують весь ланцюжок поставок, потенційно впливаючи на кілька організацій. Найчастіше порушники вставляють шкідливий код або бекдори в оновлення програмного забезпечення, які несвідомо розповсюджуються серед користувачів.

Запобігти атакам на ланцюжок поставок можна за допомогою ретельної перевірки постачальників, регулярних оцінок безпеки й використання надійних протоколів реагування на інциденти.

5. Кіберзагрози із застосуванням штучного інтелекту (ШІ)

У 2023 році кіберзлочинці використовують штучний інтелект для організації складних атак. Загрози, керовані штучним інтелектом, автоматизують атаки, уникають виявлення й обходять традиційні заходи безпеки.

Для запобігання і протидії таким атакам необхідно впроваджувати підходи і рішення безпеки, що також базуються на основі штучного інтелекту, впливаючи на зловмисника його ж засобами [30].

6. Розширені постійні загрози (APT)

APT – це складні довгострокові кібератаки, спрямовані на конкретні організації, такі як уряди або великі організації. У 2023 році APT продовжують становити серйозну загрозу, використовуючи приховані методи для отримання несанкціонованого доступу та підтримки стійкості в мережах.

Пом'якшення наслідків APT можливе за допомогою надійного контролю доступу, регулярних оцінок безпеки й передових технологій виявлення й реагування на загрози.

7. Експлойти нульового дня

Експлойти нульового дня націлені на раніше невідомі вразливості програмного забезпечення без доступних виправлень або захисту. У 2023 році експлойти нульового дня дуже затребувані серед кіберзлочинців і хакерів, спонсорованих державами.

Для захисту від експлойтів нульового дня необхідно оновлювати виправлення програмного забезпечення, використовуючи системи виявлення вторгнень і відстежуючи бази даних вразливостей.

8. Ризики хмарної безпеки

Широке впровадження хмарних сервісів створює нові ризики для безпеки. У 2023 році неправильні конфігурації, витоки даних і несанкціонований доступ до хмарних середовищ викликають серйозне занепокоєння фахівців з кібербезпеки.

Для захисту хмарних обчислень необхідно надавати пріоритет безпечним хмарним конфігураціям, надійній автентифікації та шифруванню, а також постійному моніторингу хмарних середовищ.

9. Шкідливе програмне забезпечення і вразливості мобільних пристроїв

Мобільні пристрої все частіше стають мішенню для кіберзлочинців через їх широке використання та доступ до конфіденційної інформації. У 2023 році шкідливе програмне забезпечення та вразливості мобільних пристроїв становлять значні ризики, включаючи витік даних і крадіжку особистих даних.

Захистити мобільні пристрої можна за допомогою надійних програм безпеки, регулярних оновлень операційної системи й безпечного завантаження програм [30].

10. Внутрішні загрози

Внутрішні загрози – це зловмисні або недбалі дії окремих осіб в організації. У 2023 році внутрішні загрози залишаються серйозною проблемою, оскільки співробітники з привілейованим доступом можуть навмисно чи ненавмисно скомпрометувати корпоративні дані та системи.

Доцільно запобігати й виявляти внутрішні загрози за допомогою суворого контролю доступу, моніторингу активності співробітників і регулярних тренінгів з кібербезпеки.

11. Неправильне використання штучного інтелекту

Хоча штучний інтелект має багато сфер для корисного застосування, його не рідко використовують для зловмисних цілей. У 2023 році зловживання штучним інтелектом становить зростаючу загрозу кібербезпеці. Кіберзлочинці можуть використовувати алгоритми штучного інтелекту для автоматизації атак, покращення тактики соціальної інженерії або обходу систем безпеки.

Для пом'якшення неправомірного використання штучного інтелекту доречним буде впровадження систем етики ШІ, проведення аудиту моделей ШІ та моніторингу систем ШІ на предмет підозрілої діяльності.

12. Витік даних і порушення конфіденційності

У 2023 році витоки даних і порушення конфіденційності, як і раніше, залишаються серйозною проблемою кібербезпеки. Щоб отримати конфіденційні

дані, кіберзлочинці націлені на бізнес, що може завдати величезної фінансової та репутаційної шкоди.

З огляду на це компанії повинні приділяти першочергову увагу захисту даних через законодавчі обмеження, пов'язані з конфіденційністю даних, захист від витоків даних і порушень конфіденційності за допомогою надійного шифрування, контролю доступу й регулярних аудитів безпеки.

13. Передові методи фішингу

У 2023 році фішингові атаки еволюціонували за допомогою більш складних методів. Кіберзлочинці використовують передові тактики соціальної інженерії, добре продумані електронні листи й реалістичні підроблені веб-сайти, щоб обманом змусити людей розкрити конфіденційну інформацію. Ці атаки націлені як на окремих осіб, так і на організації, тому дуже важливо залишатися пильними.

Захиститися від передових методів фішингу можливо за допомогою фільтрації електронної пошти, навчання користувачів і антифішингового програмного забезпечення.

14. Кібератаки національних держав

Уряди, організації та ключова інфраструктура перебувають у зоні серйозного ризику кібератак національних держав. Ці атаки плануються й реалізуються добре фінансованими і висококваліфікованими кіберпідрозділами з наміром порушити або проникнути в мережі для отримання комерційної, військової або політичної вигоди.

Для протидії кібератакам національних держав необхідно використовувати надійні засоби мережевої безпеки, планувати реагування на інциденти й обмінюватися розвідувальною інформацією про загрози з партнерами й державними органами.

15. Загрози, пов'язані з криптовалютою

Зростання криптовалют створило нові загрози кібербезпеці у 2023 році. Кіберзлочинці націлені на криптовалютні біржі, гаманці та транзакції, щоб викрасти кошти або запустити атаки криптоджекінгу. Децентралізований та

анонімний характер криптовалют ускладнює відстеження й повернення вкрадених активів.

Щоб захиститися від загроз, пов'язаних з криптовалютою, використовують засоби безпечного управління гаманцями, двофакторної автентифікації безпечної участі в первинних пропозиціях монет (ICO) [30].

Крім великої кількості різноманітних кіберзагроз, які постійно вдосконалюються і розширюють спектр своєї деструктивної дії, завдання забезпечення кібербезпеки ускладнюють ще низка чинників, серед яких:

Складні атаки: сучасні кібератаки більше не можна виявити за допомогою застарілих підходів до кібербезпеки. Щоб виявити кампанії передових постійних загроз (APT) та інших складних суб'єктів кібернетичної загрози, необхідні більш глибока видимість і дослідження.

Складне середовище: сучасна корпоративна мережа розповсюджується на локальну інфраструктуру та численні хмарні середовища. Це значно ускладнює послідовний моніторинг безпеки й застосування політики в IT-інфраструктурі організації.

Неоднорідні кінцеві точки: IT більше не обмежується традиційними настільними та портативними комп'ютерами. Технологічна еволюція та політика використання власного пристрою (BYOD) роблять нагальною необхідність захистити низку пристроїв, деякими з яких компанія навіть не володіє.

Розширення масштабів: відповідь на пандемію COVID-19 продемонструвала, що моделі віддаленої та гібридної роботи є життєздатними для багатьох компаній. Зараз організаціям потрібні рішення, які дозволять їм ефективно захистити віддалену робочу силу, а також співробітників на місці.

Спроба вирішити всі ці проблеми за допомогою низки відключених рішень є немасштабованою та нежиттєздатною. Лише шляхом консолідації й оптимізації своїх структур безпеки компанії можуть ефективно забезпечувати кібербезпеку.

1.3 Центр безпеки (SOC): етапи розвитку і сучасні риси

1.3.1 Історія SIEM та зародження операційного центру безпеки

Акроніми SEM, SIM і SIEM іноді використовуються в контексті взаємозамінності. Сегмент систем управління безпекою, що має справу з моніторингом в реальному часі, кореляцією подій, повідомленнями й відображенням на кінцевих пристроях, зазвичай називають управлінням подіями (SEM).

Друга галузь забезпечує довготривале зберігання, аналіз і звітність за накопиченими даними, відома як управління інформацією (SIM). У міру зростання потреб в додаткових можливостях безперервно розширюється і доповнюється функціональність даної категорії продуктів. Наприклад, потреба в безпеці голосових даних (vSIEM).

Поняття управління подіями й інформацією безпеки (SIEM), введене Марком Ніколеттом і Амрітом Вільямсом з компанії Gartner в 2005 році, описує функціональність збору, аналізу та подання інформації від мережевих пристроїв і пристроїв безпеки, додатків ідентифікації (управління обліковими даними) та управління доступом, інструментів підтримки політики безпеки й відстеження вразливостей, операційних систем, баз даних і журналів — додатків, а також відомостей про зовнішні загрози. Основна увага приділяється управлінню привілеями користувачів і служб, сервісів директорій та іншим змінам конфігурації, а також забезпечення аудиту та огляду журналів, реакцій на інциденти.

SIEM дозволяє здійснювати збір подій з практично будь-яких джерел, уніфікуючи їх, роблячи придатним для подальшого аналізу. SIEM дозволяє агрегувати однотипні події, дозволяючи використовувати їх при аналізі ситуації.

При цьому картина того, що відбувається, залишається не розмитою. Рішення класу SIEM автоматизують процес зіставлення подій між собою за різними критеріями, дозволяючи в автоматичному режимі виявляти складні для

розпізнавання інциденти. SIEM здійснює збір подій із практично будь-яких джерел та дозволяє зберігати визначений час, при цьому використовує стиснення та вирішує завдання централізованого архівного зберігання.

Термін аутсорсинговий операційний центр безпеки (Security Operation Center, SOC), або центр безпеки, вперше з'явився на початку 2000-х років. У той час багато компаній передавали різні IT-функції стороннім постачальникам. Однак із розвитком ландшафту загроз стало зрозуміло, що кібербезпека надто важлива, щоб довіряти її зовнішньому постачальнику. У результаті компанії почали відходити від аутсорсингу SOC і натомість створили власні групи експертів з безпеки.

Сьогодні аутсорсингові SOC стають популярними серед підприємств будь-якого розміру. Це просто: управління комплексною програмою безпеки є складним і трудомістким завданням. Передаючи цю функцію сторонньому постачальнику, компанії можуть зосередитися на своїх основних компетенціях, зберігаючи при цьому високий рівень безпеки. Але повний перехід на аутсорс несе за собою фінансові наслідки, оскільки цей сервіс не є дешевим [45].

1.3.2 Програмні компоненти, які використовуються в SOC

Центр безпеки SOC – структурний підрозділ організації, що відповідає за оперативний моніторинг IT-середовища та запобігання кіберінцидентам. Він поєднує технології, людей та процеси що в сукупності працює як система, що збирають та аналізують дані з різних об'єктів інфраструктури організації, та при виявленні підозрілої активності вживають заходів для запобігання атакам.

Зловмисники, що мають високу кваліфікацію, здатні виконувати складні атаки на IT-структуру підприємства. Для того, щоб вчасно виявляти і реагувати на можливі загрози необхідні засоби, які нададуть аналітикам можливість виявити, відреагувати на атаки. Але можливість тверезо відреагувати на загрози перекриває кількість джерел, які потребують моніторингу, кожне джерело може мати різну форму звітності, різну кількість логів [20].

Таким чином можливості SIEM-системи дозволяють перетворити величезні обсяги даних в важливу інформацію, на основі якої далі приймаються рішення. Використання таких систем на практиці допомагає зробити більш ефективним обмін інформацією про загрози та ризики інформаційної безпеки підприємства. Типові функції SIEM-системи показані на рисунку 1.5.

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

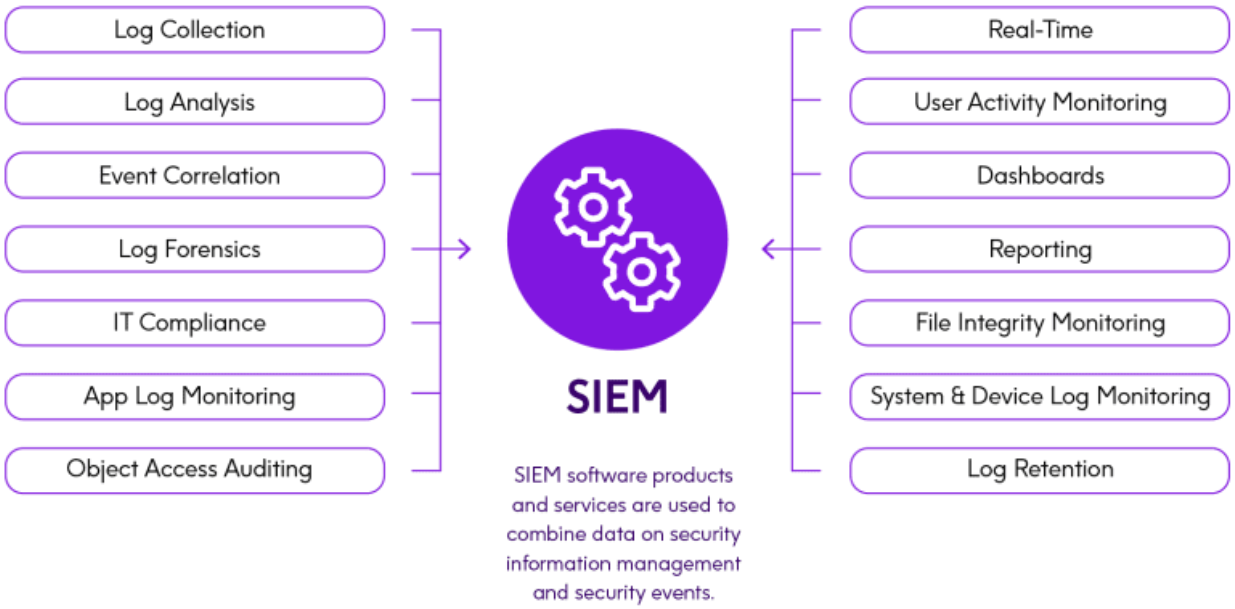

Рис. 1.5. Функції SIEM системи

На базі даних зібраних SIEM-системами також проводиться аналіз поведінки користувача в мережі - User and Entity Behavior Analytics (UEBA).

UEBA – тип процесів в кібербезпеці, який враховує нормальну поведінку користувача та виявляє аномальну поведінку або випадки відхилення від «нормальних» моделей. Наприклад, якщо конкретний користувач регулярно завантажує файл розміром 10 МБ, але раптово завантажує гігабайти файлів, система зможе виявити цю аномалію і негайно попередити аналітиків [49]. Функціонал систем UEBA представлений на рисунку 1.6.

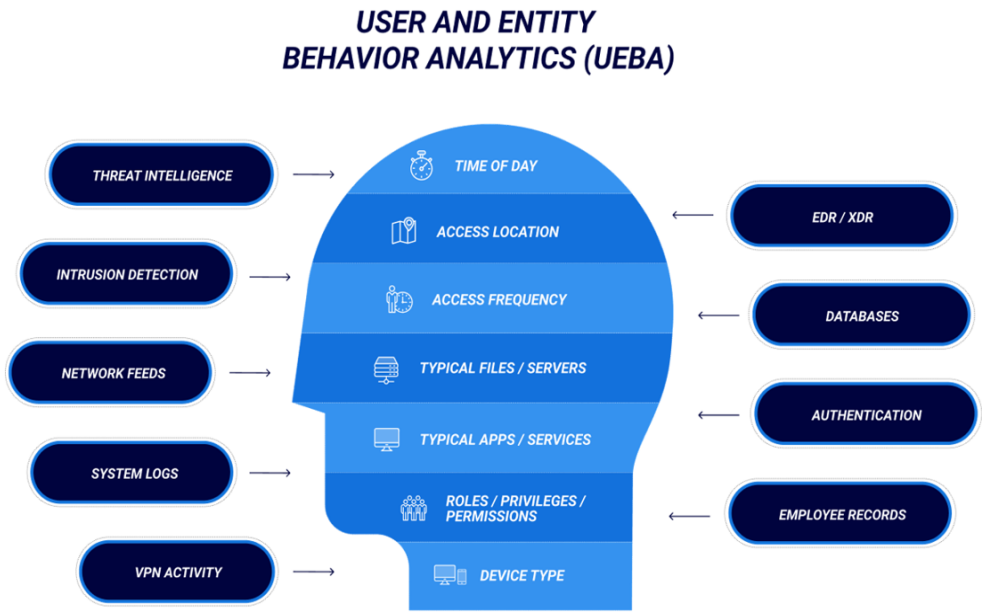

Рис. 1.6. Функції UEBA

Для того, щоб виявляти події на кінцевих вузлах користувачів і серверах в IT-інфраструктурі, також може бути використано засіб класу Endpoint Detection and Response (EDR).

EDR – це платформа, яка здатна виявляти складні і цільові атаки в системі, сервері, будь-якому комп'ютерному пристрої (кінцеві точки) і швидко на них реагувати. Платформа EDR не просто захищає комп'ютерну систему від шкідників, вона вміє моментально помічати нові загрози високої складності і одночасно проявляти реакцію на ситуацію, що виникла.

EDR не тільки має вбудовані механізми журналювання, але і детально аналізує те, що відбувається на рівні операційної системи. Зокрема, EDR-система може виступати джерелом подій для SIEM-системи.

Типові функції EDR показані на рисунку 1.7 [50].

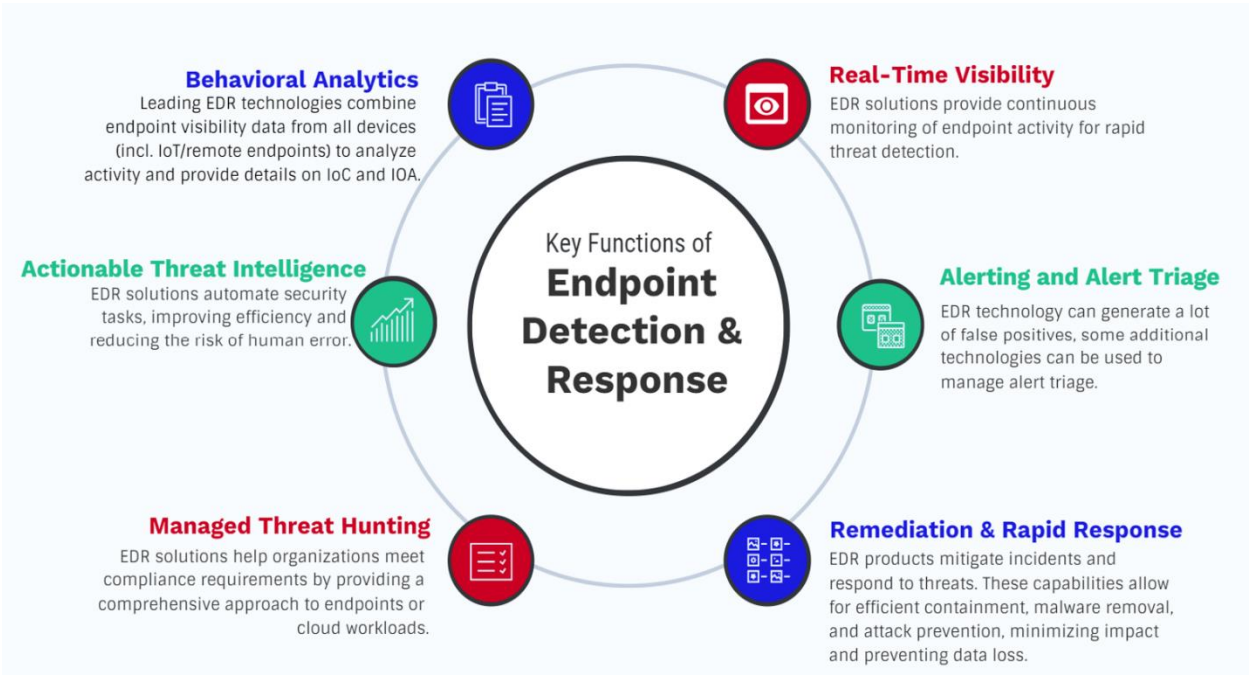

Рис. 1.7. Функції EDR

Важливим джерелом інформації слугує мережевий трафік. Для автоматизації збору і аналізу подій всередині трафіку використовуються засоби класу Network Traffic Analysis (NTA). NTA безперервно аналізують мережеву телеметрію і / або записи потоків (Рис. 1.8).

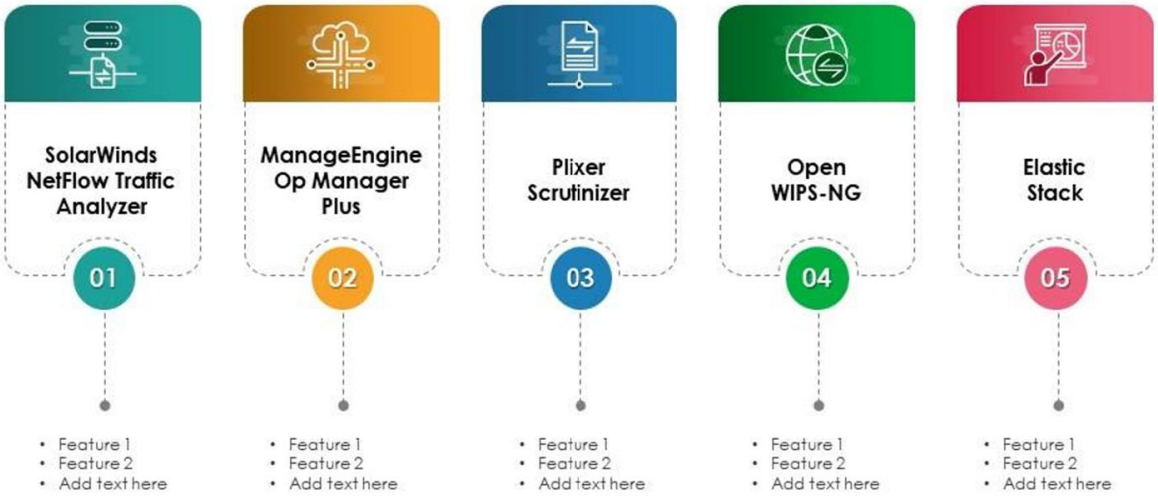

Рис. 1.8. Основні інструменти NTA

Дана система приймає дані телеметрії від безлічі мережевих пристроїв, таких як маршрутизатори, комутатори і брандмауери, щоб визначити, як виглядає «нормальна» поведінка цих пристроїв. При виявленні аномального

трафіку або нерегулярної мережевої активності ці інструменти попереджають групу безпеки про потенційну загрозу [51].

1.3.3 Функції SOC

Функції SOC можуть відрізнятися залежно від масштабу підприємства та його організаційної структури. Найчастіше у сферу відповідальності операційного центру безпеки входить (Рис. 1.9):

1. Активний моніторинг IT-середовища та збір даних про інциденти. Зазвичай оператори SOC збирають інформацію з робочих місць працівників, мережевих пристроїв та інших об'єктів комп'ютерної інфраструктури в режимі 24/7, щоб якомога раніше виявити та зупинити можливу атаку. Для моніторингу та збору даних фахівці можуть використовувати SIEM-рішення та EDR-продукти.

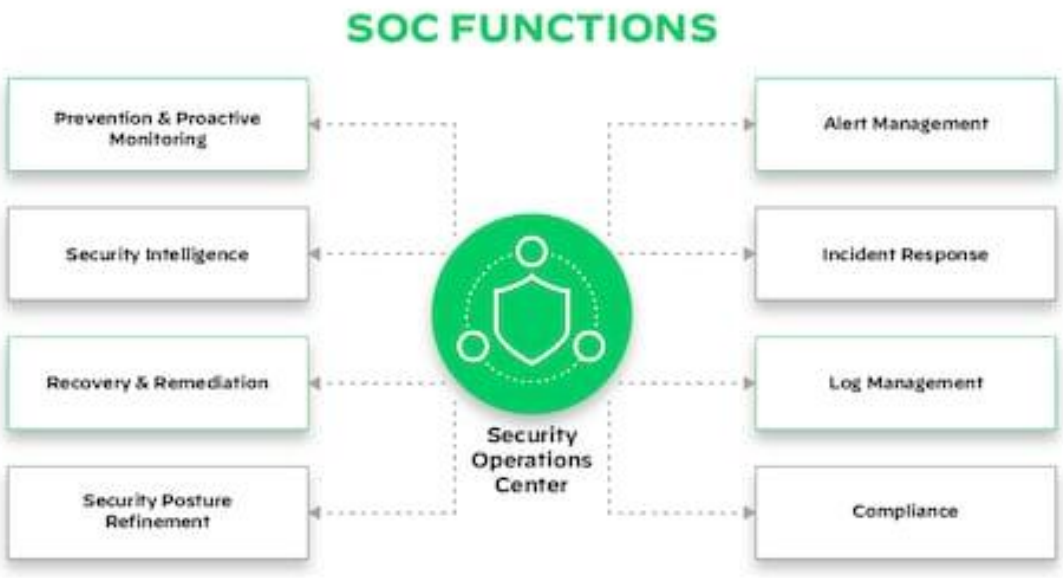

Рис. 1.9. Функції SOC

2. Аналіз підозрілих подій. Отримавши повідомлення про можливий інцидент, фахівці SOC визначають, чи є загроза, і якщо є її характер і ступінь небезпеки.

3. Реагування на небезпеку. При виявленні кіберінциденту команда SOC вживають заходів щодо його усунення та мінімізації збитків.

4. Відновлення після інциденту. Фахівці SOC можуть брати участь в усуненні наслідків інциденту, зокрема у відновленні постраждалих систем, файлів з бекапу тощо.

5. Розслідування інцидентів. Експерти SOC можуть брати участь у пошуку причин кіберінциденту. Результати розслідування допоможуть організації запобігти подібним інцидентам у майбутньому.

6. Веде реєстр ресурсів. Для успішного виконання своїх обов'язків співробітникам SOC необхідно знати, які об'єкти входять до контуру безпеки підприємства та які ІБ-продукти можуть бути використані для їх захисту. Тому нерідко саме вони ведуть реєстр ресурсів компанії.

7. Менеджмент відповідності до вимог. Оскільки співробітники SOC відповідають за безпеку даних компанії, досить часто вони займаються питаннями відповідності державним і міжнародним вимогам, нормативним документам у сфері безпеки даних, таких як GDPR, HIPAA, CPPA тощо [25].

1.4 Розподіл повноважень спеціалістів SOC

У SOC ролі розділяються на три основні рівні: сортування, реагування на інциденти й активний пошук загроз. Окрему позицію займає менеджер SOC. Вимоги до зазначених категорій фахівців показані на рис. 1.10.

Спеціалісти 1 рівня (сортування): в основному відповідають за збір необроблених даних, а також за перегляд тривог і попереджень. Вони повинні підтверджувати, визначати або коригувати критичність сповіщень і збагачувати їх відповідними даними. Для кожного попередження фахівець з сортування повинен визначити, чи є воно обґрунтованим чи помилковим спрацьовуванням.

Додатковою відповідальністю на цьому рівні є виявлення інших подій високого ризику та потенційних інцидентів. Все це потрібно пріоритезувати відповідно до їх критичності. Якщо проблеми, що виникають, не можуть бути вирішені на цьому рівні, вони переходять до аналітиків рівня 2. Крім того,

фахівці з сортування часто керують та налаштовують інструменти моніторингу [17].

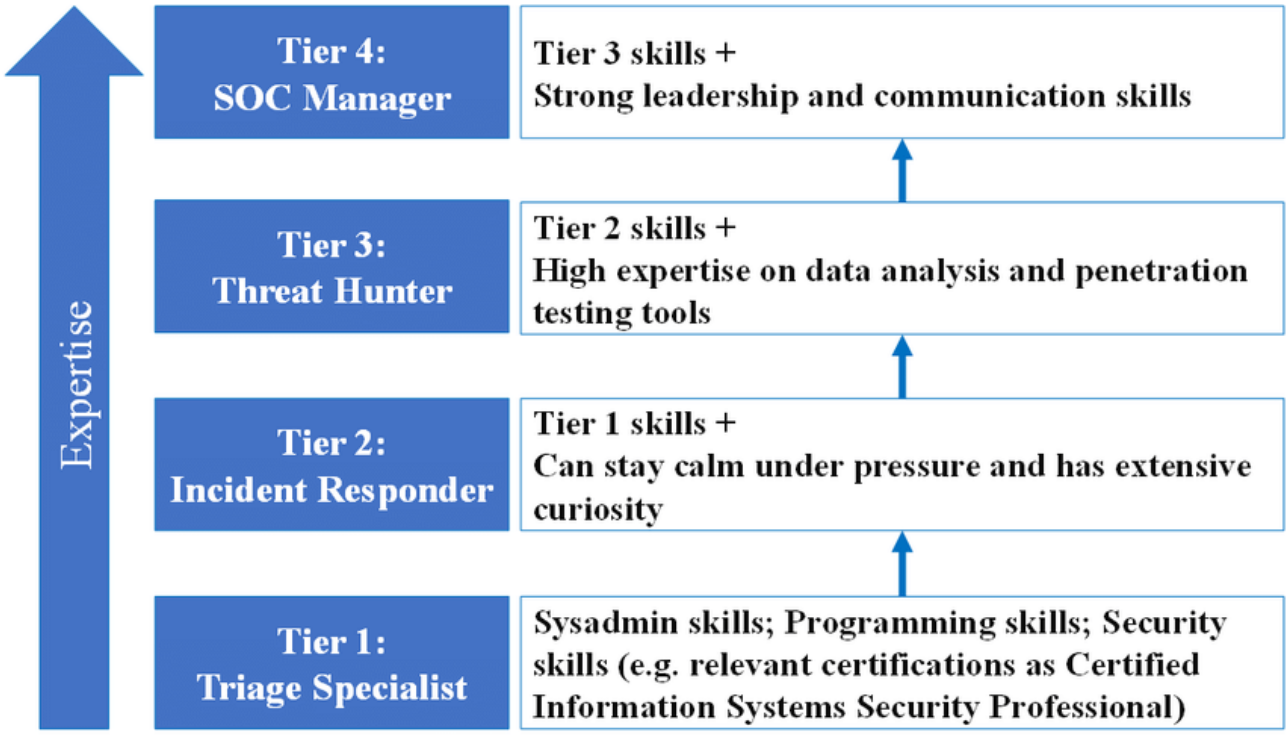

Рис. 1.10. Вимоги до спеціалістів SOC

Спеціалісти 2 рівня (реагування на інциденти): на рівні 2 аналітики розглядають більш критичні інциденти безпеки, передані фахівцями з сортування, і проводять більш глибоку оцінку за допомогою розвідки загроз (індикатори компрометації, оновлені правила тощо). Вони повинні розуміти масштаби атаки та знати про уражені системи. Необроблені дані телеметрії атак, зібрані на рівні 1, перетворюються на дієву розвідку загроз на рівні 2.

Служби реагування на інциденти несуть відповідальність за розробку та реалізацію стратегій стримування та відновлення після інциденту. Якщо аналітик рівня 2 стикається з серйозними проблемами з виявленням або пом'якшенням атаки, проводяться консультації з додатковими аналітиками рівня 2 або інцидент переходить на рівень 3 [17].

Спеціалісти 3 рівня («мисливці за загрозами»): аналітики рівня 3 є найдосвідченішою робочою силою в SOC. Вони займаються серйозними інцидентами, які їм надходять від служб реагування на інциденти. Вони також проводять або, принаймні, контролюють оцінку вразливостей і тести на

проникнення, щоб виявити можливі вектори атак. Їхнім найважливішим обов'язком є завчасне виявлення можливих загроз, прогалин у безпеці та вразливостей, які можуть бути невідомими.

Отримуючи обґрунтовані знання про можливу загрозу системам, вони також повинні рекомендувати шляхи оптимізації розгорнутих інструментів моніторингу безпеки. Крім того, будь-які критичні сповіщення безпеки, аналіз загроз та інші дані безпеки, надані аналітиками рівнів 1 і 2, повинні бути переглянуті на цьому рівні.

Менеджери SOC: менеджери контролюють команду SOC. Вони надають технічні вказівки, якщо це необхідно, але найголовніше, вони відповідають за адекватне управління командою. Це включає найм, навчання та оцінку членів команди, оцінку звітів про інциденти, а також розробку та впровадження необхідних планів кризових комунікацій.

Вони також контролюють фінансові аспекти SOC, підтримують аудити безпеки та звітують перед директором з інформаційної безпеки (CISO) або відповідною керівною посадою вищого рівня. Кожна з цих основних ролей повинна мати певний набір навичок. Основні ролі можна знайти в SOC незалежно від їх розміру. Однак у меншому SOC обов'язки кожної ролі ширші, і вони звужуються, щоб бути більш конкретними, коли SOC зростає.

Наприклад, у невеликому SOC, де всього кілька аналітиків, кожен повинен бути обізнаний з кількома навичками, тому що кілька співробітників мають охопити всі завдання команди. У більшому SOC ролі можуть бути більш конкретними, оскільки, наприклад, деякі аналітики можуть бути зосереджені на моніторингу мережі, тоді як інші є експертами зі специфіки Windows або Linux.

Це має багато переваг, таких як краща та швидша реакція на загрози або кращий розподіл завдань [17].

Основні завдання SOC. Кожен операційний центр безпеки повинен складатися із основних складових, які представлені на рис. 1.11.

Рис. 1.11. Основні завдання SOC

1. Огляд активів: щоб центр безпеки допомагав компанії залишатися в безпеці, вони повинні мати повне розуміння того, які ресурси їм потрібно захистити. Інакше вони не зможуть захистити всю мережу.

Обстеження активів має ідентифікувати кожен сервер, маршрутизатор, брандмауер під контролем підприємства та будь-які інші інструменти кібербезпеки, які активно використовуються [34].

2. Збір журналів: дані є найважливішим чинником для належного функціонування SOC, а журнали служать ключовим джерелом інформації щодо мережевої активності. Центр безпеки має налаштувати прямі канали з корпоративних систем, щоб дані збиралися в режимі реального часу.

Люди не можуть перетравлювати такі великі обсяги інформації, тому інструменти сканування журналів, що працюють на основі алгоритмів штучного інтелекту, є такими цінними для SOC. Однак вони створюють деякі цікаві побічні ефекти, які людство все ще намагається виправити [34].

3. Профілактичне обслуговування: SOC може запобігти кібератакам, будучи активним у своїх процесах. Це включає встановлення патчів безпеки та регулярне коригування політик брандмауера.

Оскільки деякі кібератаки починаються як внутрішні загрози, центр безпеки також повинен шукати ризики всередині організації.

4. Безперервний моніторинг: щоб бути готовим реагувати на інцидент кібербезпеки, SOC має бути пильним у своїй практиці моніторингу. Кілька хвилин можуть бути різницею між блокуванням атаки та дозволом їй зруйнувати всю систему чи веб-сайт.

Інструменти SOC сканують мережу компанії, щоб виявити потенційні загрози та іншу підозрілу активність.

5. Керування сповіщеннями: автоматизовані системи чудово знаходять шаблони та слідують сценаріям. Але людський фактор SOC доводить свою цінність, коли справа доходить до аналізу автоматичних сповіщень і їх ранжування на основі серйозності та пріоритету.

Співробітники центру безпеки повинні знати, які відповіді вживати та як перевірити законність попередження.

6. Аналіз першопричини: після того, як інцидент стався і був усунений, робота SOC тільки починається. Експерти з кібербезпеки проаналізують першопричину проблеми та діагностують, чому вона взагалі виникла.

Це сприяє безперервному вдосконаленню за допомогою інструментів безпеки та правил, змінених для запобігання повторенню аналогічних інцидентів у майбутньому.

7. Аудит відповідності: Компанії хочуть знати, що їхні дані та системи безпечні та керуються ними законним чином.

Постачальники SOC повинні проводити регулярні аудити, щоб підтвердити свою відповідність у регіонах, де вони працюють [34].

Висновки до розділу 1

Встановлено, що кібербезпека має на меті забезпечення комплексного захисту організації, її активів і персоналу від кіберзагроз. Кібербезпека – це широка галузь, яка охоплює кілька напрямів, зокрема безпека інформації, операцій, програм, мереж, кінцевих точок і планування відновлення після інцидентів.

Дослідження показало, що основними загрозами кібербезпеці є атаки програм-вимагачів, уразливості Інтернету речей (IoT), соціальна інженерія та фішингові атаки, атаки на ланцюжок поставок, кіберзагрози із застосуванням штучного інтелекту, розширені постійні загрози (APT), експлойти нульового дня, загрози хмарній безпеці й мобільним пристроям, шкідливе ПЗ, внутрішні загрози, загрози, пов'язані з криптовалютою тощо.

Оскільки складність і масштаби кіберзагроз зростають, а корпоративні ІКС стають все більш розмежованими, організації стикаються з потребою у реалізації комплексних рішень кібербезпеки, одним із яких є центр безпеки (SOC).

SOC є структурним підрозділом організації, що відповідає за оперативний моніторинг IT-середовища й запобігання кіберінцидентам і поєднує технології SIEM, UEBA, EDR, NTA та інші. Функції SOC включають активний моніторинг IT-середовища та збір даних про інциденти; аналіз підозрілих подій; реагування на загрози; розслідування інцидентів й відновлення після них; ведення реєстру ресурсів; управління відповідністю.

Повноваження фахівців SOC розділяють на три основні рівні: спеціалісти 1 рівня (сортування), які переважно відповідають за збір необроблених даних, а також за перегляд тривог і попереджень; спеціалісти 2 рівня (реагування на інциденти), які опрацьовують більш критичні інциденти безпеки і проводять поглиблену оцінку за допомогою розвідки загроз; спеціалісти 3 рівня (пошук загроз), які займаються серйозними інцидентами, а також завчасним виявленням можливих загроз і невідомих вразливостей.

РОЗДІЛ 2
ЕТАПИ РОЗРОБКИ Й РОЗГОРТАННЯ SOC

2.1 Підготовчий етап створення центру безпеки

Для багатьох організацій створення центру безпеки може здатися нездійсненним завданням. З обмеженими ресурсами (часом, персоналом і бюджетом) створення SOC, що підтримується безліччю технологій моніторингу безпеки й оновлень загроз майже в реальному часі, здається не таким вже й легким.

Насправді, незважаючи на сумніви у наявності достатньої кількості штатних і кваліфікованих членів команди, щоб впроваджувати й керувати різними інструментами SOC на постійній основі, важливо шукати способи спростити й уніфікувати моніторинг безпеки, щоб оптимізувати процеси і команду SOC.

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

Тому слід зробити управління інцидентами чітко та поетапно, як рекомендує міжнародний стандарт ISO/IEC 27035-1:2023 з управління інцидентами інформаційної безпеки, який є основою багатокомпонентного міжнародного стандарту. В ньому представлені основні концепції і етапи управління інцидентами безпеки, які об’єднані з принципами в структурованому підході до виявленню, оцінці і реагуванні на інциденти. Принципи, які викладені в стандарті є загальними та призначені для використання всіма організаціями.

Отже, згідно з стандартом ISO/IEC 27035-1:2023 [55], управління інцидентами ІБ складається з:

1. Планування і підготовки.

2. Виявлення і звітності.

3. Оцінки та прийняття рішення.

4. Реагування.

5. Аналізу отриманого досвіду й коригування подальших дій.

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

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

- координація і зв'язок між сторонами;

- повідомлення керівництва й інших зацікавлених сторін прозначні інциденти;

- обмін інформацією між зацікавленими сторонами: внутрішніми і зовнішніми співробітниками, такими як постачальники.

Після обрамування процесу управління ризиками, можна приступити до основних етапів створення SOC. Процес створення SOC складається з таких етапів (Рис. 2.1): розробка стратегії SOC; створення індивідуального рішення SOC; створення процесу, процедури та навчання; підготовка середовища; впровадження рішення; розгортання наскрізних сценаріїв використання; підтримка та розвиток індивідуального рішення SOC [56].

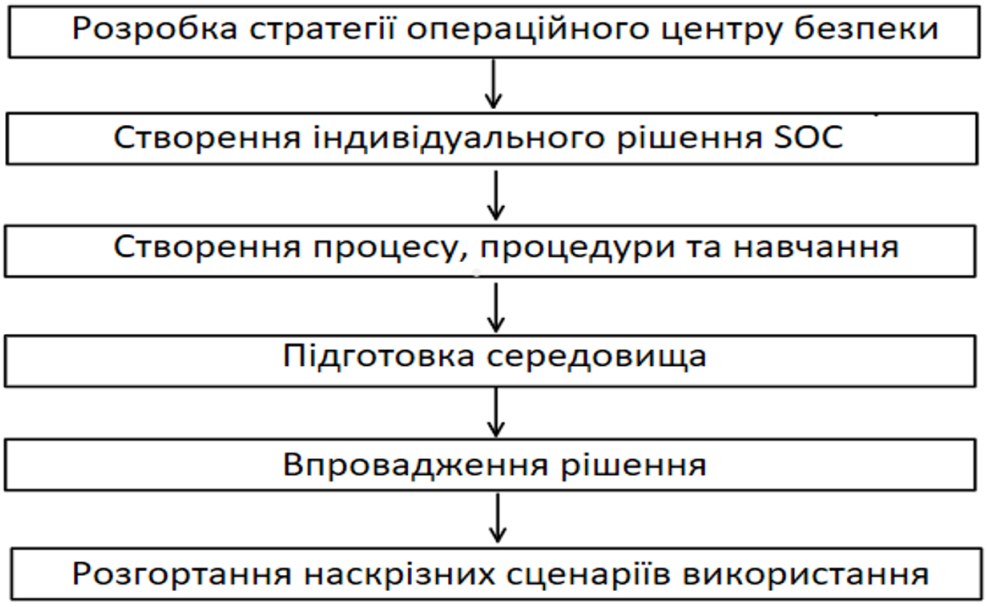

Рис. 2.1. Етапи створення SOC

2.2 Розробка стратегії та вибір рішення як основи для SOC

Першим кроком є уточнення бізнес-цілей для створення SOC.

Хибним буде створення центру безпеки тільки для покращення корпоративної безпеки без урахування загальних бізнес-цілей, що може призвести до неузгодженості й навіть до того, що SOC пропустить ключову загрозу, яка завершиться руйнівним кіберінцидентом.

Насамперед треба розглянути динамічний ландшафт загроз і те, як це стосується конкретної організації чи бізнесу. З розвитком таких технологій, як 5G, IoT, хмарні технології та штучний інтелект, у кіберзлочинців з'явилися нові шляхи для їх використання, щоб виконувати масивні атаки.

Взаємопов'язаний характер цифрових екосистем організації робить можливими масштабні атаки, серед яких DDOS атаки з великим обсягом трафіку.

Інвестиції в численні інструменти безпеки без належної інтеграції, розуміння процесу та контексту, а також необхідного досвіду є недоцільними. Хоча кожен інструмент може досягти успіху у своїй конкретній галузі, проблема полягає в необхідності агрегування й аналізу даних з різних джерел.

Замість того, щоб додавати більше інструментів, треба оптимізувати й інтегрувати існуючі для створення єдиної системи захисту.

Наступним кроком є оцінка наявних можливостей центру безпеки компанії з точки зору людей, процесів і технологій. Якщо процес створення починається з нуля, початкова сфера застосування SOC повинна бути обмежена основними функціями, тобто моніторингом, виявленням, реагуванням і відновленням. Хоча повноцінні SOC підтримують більш просунуті функції, такі як управління вразливостями, варто відкласти їх до тих пір, поки основні функції не стануть достатньо зрілими [33].

Розробляючи рішення SOC, яке відповідає вимогам та очікуванням конкретної організації, доцільно почати з вибору кількох критично важливих для

бізнесу варіантів і з них обрати оптимальне рішення SOC, пам'ятаючи, що його потрібно буде масштабувати для додаткових майбутніх потреб.

Почати потрібно з побудови фундаменту на основі унікального профілю загроз, схильності до ризику та бюджету організації, а також узгодження стратегії з бізнес-цілями й рівнями прийнятності ризиків. У подальшому рішення SOC буде поступово розвиватися, зосереджуючись на людях, процесах і технологіях, які відповідають конкретним потребам.

Варто розуміти, що лише деяким організаціям потрібен великий, ретельно продуманий центр безпеки або всі найновіші інструменти безпеки. Така громіздка структура насправді може перешкоджати продуктивності.

Консервативний дизайн початкового рішення SOC на ранніх стадіях скоротить час, необхідний для його впровадження та отримання результатів. У рамках обраного рішення мають бути визначені джерела даних журналів і подій, які будуть відстежуватися, інформації про загрози й вимоги до продуктивності, наприклад, часу реагування.

Джерелами даних можуть бути не тільки сервери, але і маршрутизатори, фаєрволи, NGFW, IDS, IPS, EDR, XEDR, NTA, продукти власного написання, які мають можливість створення і відправки логів безпеки, криміналістичний аналіз зразків шкідливих програм і носіїв, повний аналіз сеансу мережевих даних [33].

Проектування технічної архітектури

Наступним кроком є проектування технічної архітектури, що включає визначення складу та конфігурації компонентів рішення, включаючи платформу SIEM. Потрібно буде уточнити, які бізнес- та інформаційні системи потрібно інтегрувати з організаційною SIEM-платформою.

Інші дії включають визначення робочих процесів для подій та інцидентів таким чином, щоб вони відповідали процесам, які вже є в організації. Потрібно буде вирішити, до якої міри вбудовувати автоматизацію у своє рішення, щоб отримати оптимальну видимість ландшафту загроз і запобігти атакам на ранніх стадіях життєвого циклу атаки.

Перш ніж вкладати гроші в SIEM-проект, необхідно розглянути деякі передумови, зокрема, коли SOC:

- вже має інструменти збору логів; його потреби в аналітиці та кореляції даних більші, ніж пропонують поточні інструменти.

- виконує значну частину своїх повноважень з аналізу даних в реальному часі.

- виділяє крім IDS / IPS ще кілька потоків даних, які необхідно передавати в SIEM в режимі реального часу.

- бере участь у процесі регулярного управління й налаштування датчиків, для чого є визначений персонал, що свідчить про готовність команди взяти на себе функції управління SIEM.

SIEM-проекти мають доволі складну схему обслуговування, а їх остаточна ціна зазвичай залежить від: кількості джерел даних; обсягів даних, які обробляє система; кількості користувачів, що мають доступ до мережі.

Ретельне планування має ключове значення для купівлі SIEM-систем, тому що операційного центру безпеки повинен прогнозувати щорічні виплати в рамках загальної вартості підтримки. Щорічна плата за обслуговування та підтримку складає від 20-30% від початкової вартості придбання. При роботі з SIEM-системами необхідно чітко розуміти головні вимоги до неї [5]. Тому насамперед слід оглянути ключові параметри архітектури й реалізації SIEM-систем (Рис. 2.2).

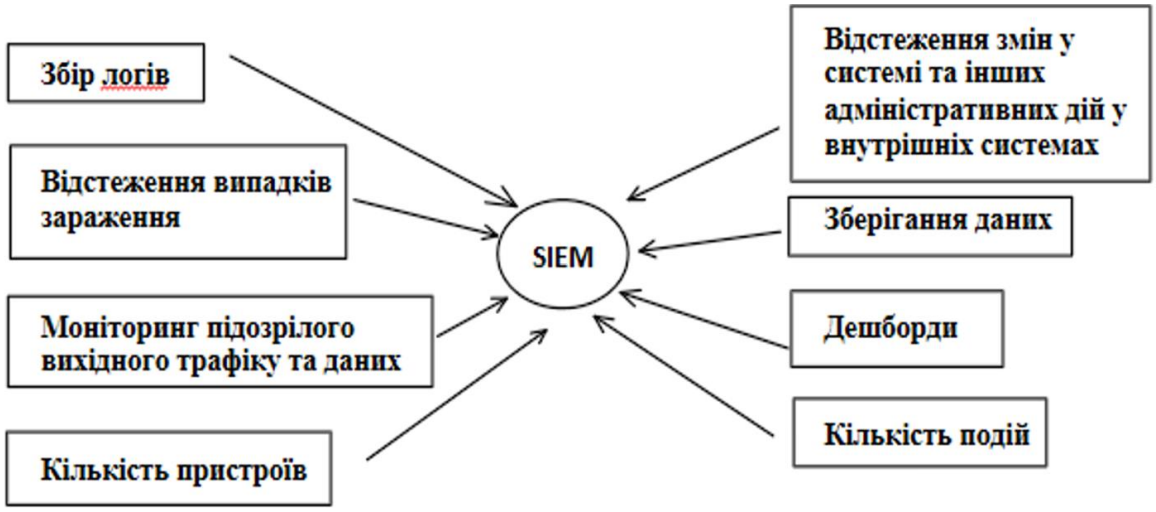

Рис. 2.2. Ключові параметри архітектури й реалізації SIEM-систем

- Збір логів. Пакети розгортання існують декількох типів:

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

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

- Відстеження випадків зараження. Виявлення шкідливих програм із використанням вихідних журналів брандмауерів та журналів веб-проксі, а також внутрішніх журналів підключення та мережевих потоків.

- Моніторинг підозрілого вихідного трафіку та даних, що передаються в мережі, з використанням журналів брандмауеру та журналів веб-проксі і NetFlow. Виявлення крадіжки даних та інших підозрілих зовнішніх з'єднань.

- Відстеження змін у системі та інших адміністративних дій у внутрішніх системах та їх відповідність політиці дозволів підприємства.

- Відстеження атак на веб-додатки та їх наслідків з використанням журналів веб-серверів, WAF (Web Application Firewall, екран для захисту веб-додатків) і логів додатків. Виявлення спроб компрометації веб-додатків шляхом аналізу різних звітів.

- Зберігання даних. Продукти SIEM теоретично здатні зберігати події, зібрані за багато років. Але тривалість зберігання зазвичай обмежується періодом роботи з моменту першої ітерації. У деяких випадках SOC може віддати перевагу новій інсталяції SIEM, щоб почати з чистого аркуша. Це може стати проблематичним, оскільки SOC буде міняти безліч поколінь продуктів SIEM, водночас продовжуючи прагнути до довгострокового зберігання даних аудиту. У міру розвитку і більшої стабільності продуктів, оновлення ПЗ краще підтримує зберігання даних про події і призначені для користувача дані.

- Кількість пристроїв. SIEM повинна мати можливість обробляти десятки або навіть сотні тисяч кінцевих пристроїв з використанням різних каналів передачі даних. SIEM також повинна мати можливість розпізнавати декілька потоків даних з однієї і тієї ж кінцевої точки. Добре спроектоване ПЗ агента має справлятися з багатьма пристроями (можливо, десятками тисяч), чий сумарний потік подій може підтримувати понад тисячу подій за секунду.

- Кількість подій. Правильна реалізація SIEM зазвичай обробляє події, що надходять зі швидкістю на рівні тисяч подій за секунду, що відповідає десяткам або сотням мільйонів подій за день. Це оптимальна цифра для SIEM. Хоча багато постачальників SIEM рекламують швидкість прийому від 10 000 до 100 000 або більше подій за секунду. Слід звернути увагу, чи покращиться робота аналітиків завдяки розподілу даних за рівнями, або чи не занадто багато даних вони збирають.

- Можливість створення інформативних панелей управління, які можна гнучко налаштувати для надання інформації під запити підрозділів.

Перед впровадженням SIEM-проекту в SOC слід визначити, які пристрої будуть слугувати джерелами даних і виділити окремі правила кореляції, для того щоб аналітики не губили потрібну інформацію серед ‘‘шуму’’. Тому слід почати з інвентаризації активів інформаційної безпеки організації.

Для цього можна використовувати сканери вразливостей, які дозволять за короткий час зібрати всю потрібну інформацію про наявні компоненти інфраструктури компанії та про їх вразливості, а також допоможуть в майбутньому відстежувати стан мережі. Коли вся необхідна інформація зібрана, пріоритезують, тобто надають кожній події ступінь критичності й вирішують, які дані доцільно збирати, обробляти і зберігати. Найбільш важливі та критичні джерела потрібно підключати до SIEM-систем [19].

Варто також пам’ятати, що кожне робоче місце в центрі безпеки по-різному використовує дані і функції SIEM.

Лінія 1 буде зацікавлена в сортуванні даних в реальному часі і конкретних сценаріях використання, під які вони можуть написати інструкції. Лінія 2

швидше за все буде зацікавлена в зборі якомога більшої кількості деталей про потенційний інцидент, тобто вони будуть виконувати запити довільної форми протягом тривалих періодів часу .

Ті, хто відповідають за виявлення та попередження атак або за відстеження тенденцій, ймовірно, будуть агрегувати різні джерела даних, багаторазово виконуючи довгі ресурсомісткі запити. Менеджери будуть зацікавлені в координації роботи і метриках, які дає інструмент, щоб переконатися, що відповідні підрозділи центру безпеки виконують інструкції, відстежують аномальну активність, коли система її вловлює, і не допускають простою системи.

Розподіл механізмів за рівнями ієрархії зображений на рисунку 2.3. при переході до механізмів більш високого рівня такі як формування звітів, проведення кореляції, прийняття рішень, кількість оброблюваних подій зменшується, а складність їх обробки збільшується [29].

Рис. 2.3 Ієрархія механізмів SOC

Формування штату працівників.

Далі для формування центру безпеки треба розглядати штат. Команда SOC може варіюватися від п’яти працівників до розмірів національних координаційних центрів. Надійна структура управління має важливе значення для ефективного SOC. Для кожного члена команди визначаються ролі, обов'язки

і лінії звітності, щоб забезпечити безперебійну роботу й підзвітність. Незалежно від того, чи буде обрано модель побудови власного SOC, MSSP, MDR або гібридну модель, наявність чітко визначеної структури створює основу для успіху.

Власний центр безпеки означає використання SIEM системи і допоміжних програмних засобів безпосередньо в організації. SOC не надає свої послуги на аутсорс, тільки в саму компанію.

MDR (Managed Security Service Provider) – це керована служба кібербезпеки, яка допомагає швидко виявляти та усувати різні загрози, зокрема вторгнення, віруси, інші шкідливі програми та шкідливі дії в мережі. MDR зазвичай враховує структуру, посади та ролі компанії, покладається на власний стек технологій і залучає призначену команду криміналістичних аналітиків, а також внутрішню команду безпеки. Це суттєво скорочує час на виявлення й усунення інцидентів. У багатьох випадках скорочення становить від місяців до літературних годин, що робить MDR ефективним рішенням з кібербезпеки. MDR – це реагування, яке не просто автоматизоване, а здійснюється людиною або штучним інтелектом.

MSSP (Managed Detection and Response) - це рішення безпеки, яке покладається на технології автоматизації. Воно дозволяє повністю передати кібербезпеку на аутсорсинг постачальнику послуг безпеки. Традиційно немає потреби у власній команді з кібербезпеки замовника, але його технологічний стек братиме участь. Це робить пропозицію MSSP дешевшою, ніж MDR, і передбачає, що команда підтримки буде внутрішньою для клієнта.

Зазначимо, що MSSP досить гнучкі у відносинах із клієнтом, адаптуються до його IT-середовища та відстежують події безпеки в ньому, надсилаючи сповіщення про виявлені аномалії. Однак MSSP, як правило, не розслідують їх і не реагують на загрози. Ці функції можуть бути доступні за допомогою спеціального фіксатора [16].

Зазвичай SOC поділяє аналітиків на три лінії:

- Перша лінія займається оперативним реагуванням на інцидент;

- Друга лінія – це аналітики, що ведуть розслідування, аналізують дані та створюють звітність.

- Третя лінія – це найдосвідченіші аналітики, вони займаються серйозними інцидентами, які їм надходять від служб реагування на інциденти. Вони також проводять або, принаймні, контролюють оцінку вразливостей і тести на проникнення, щоб виявити можливі вектори атак.

Менеджери SOC: менеджери контролюють команду операцій безпеки. Вони надають технічні вказівки, якщо це необхідно, але найголовніше, вони відповідають за адекватне управління командою [15].

На рисунку 2.4 показано схему взаємодії персоналу SOC.

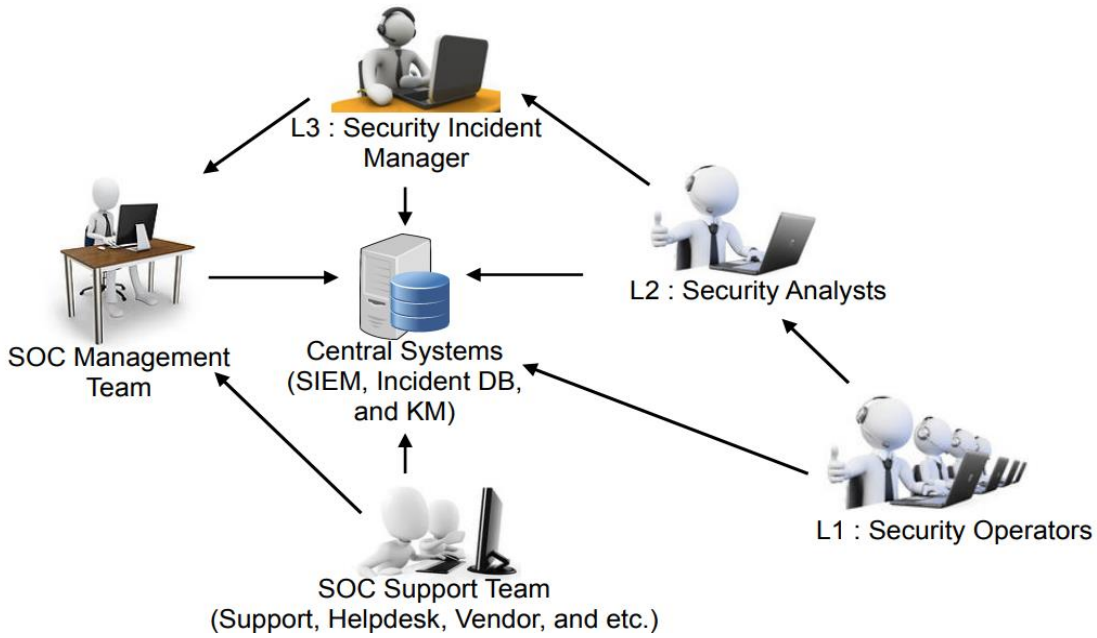

Рис. 2.4. Взаємодія працівників команди SOC

Для кожного рівня центру безпеки аналітика є основним набором вмінь, якими мають володіти його фахівці. Найголовніше – це знати архітектуру операційних систем як Unix-подібних, так і Windows.

Оскільки пошук загроз може доходити до систем і без орієнтації в системі, аналітик може загубитися і витратити більше часу, що є критичним. SOC аналітики повинні знати мови програмування для написання правил кореляції або правил для API, щоб забирати оповіщення або логи з систем захисту для подальшої обробки.

2.3 Розробка процесів виявлення, реагування і навчання персоналу

Для досягнення максимального результату дій із реагування слід зробити цей процес чітким та поетапним, але перед тим як робить будь-які дії потрібно переконатися, що дії SOC не призведуть до переривання нормальних процесів і не вплинуть на виконання завдань клієнта більше, ніж на сам інцидент; сформоване розуміння масштабу і ступеня серйозності вторгнення. Спостереження за зловмисником, іноді є більш ефективним, ніж виконання статичного експертного розслідування на скомпрометованих системах за його відсутності.

В ідеалі, SOC повинен виявити інцидент до того, як буде завдано значної шкоди. Ідеальним сценарієм є виявлення події в ході розвідки або фактичної атаки, коли доступ до системи здійснюється через експлуатацію вразливості.

Ознаки атаки можуть виникати одночасно в декількох місцях: в мережевому трафіку, BIOS-хості, на жорсткому диску, знімних носіях, ПЗ, системному ПЗ і додатках у пам'яті. Усвідомлення цієї інформації впливає на вибір датчиків для установки і розуміння того, коли і як ці датчики можна обійти, нейтралізувати або відключити. Аналітики починають з первинних індикаторів (наприклад, високорівневого попередження про інцидент або спрацьованого правила кореляції) і далі збирають додаткові дані для підтвердження виявлених подій.

Достовірність цих даних може бути покращена за допомогою засобів кореляції і автоматизованої фільтрації, а також дедублікації даних в SIEM-системах. Спеціалісти центру не можуть бути на 100% впевнені в тому, що насправді сталося, через неповні, непереконливі або неоднозначні дані. Команда SOC має це враховувати, особливо, при виборі сценарію реагування. Підозри на інциденти допомагають аналітику зорієнтуватися, на які події слід звернути увагу в першу чергу. Контекст необхідний для того, щоб точно встановити, що насправді сталося (наприклад, незаперечні факти наявності шкідливої активності на хості і в мережі).

Якщо SOC не буде охоплювати цей спектр, аналітики не зможуть ефективно виявляти й аналізувати передбачувані інциденти.

Інформацію про інциденти аналітики отримують з різних джерел, які поділяють зовнішні і внутрішні (Рис. 2.5).

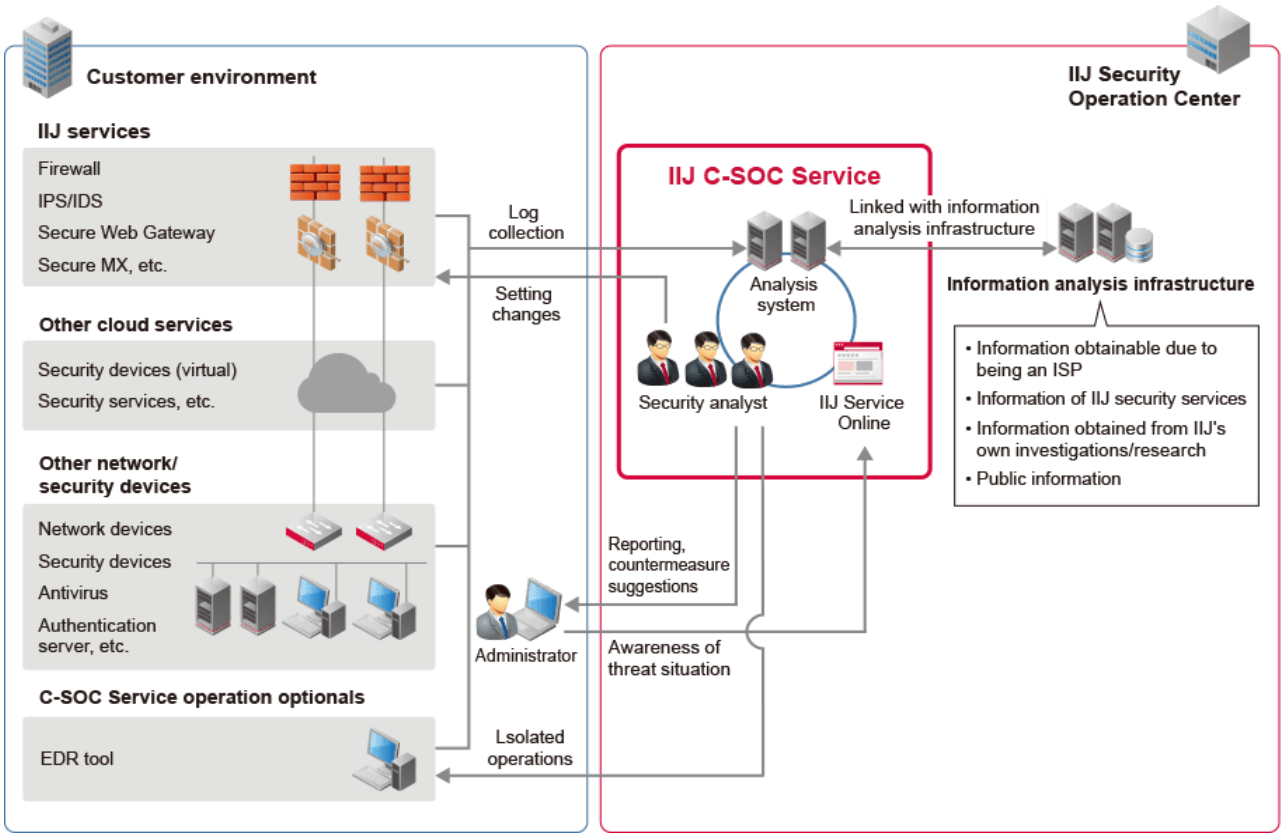

Рис. 2.5. Зовнішні і внутрішні джерела інформації для SOC

До зовнішніх джерел відносять такі, як:

- клієнти зі звичайним непривілейованим доступом до системи;
- системні адміністратори й адміністратори мереж клієнта;
- служби технічної підтримки клієнта;
- менеджери і керівники систем інформаційної безпеки клієнта;
- інші SOC (того ж рівня або підлеглі, координаційні або національні);
- правоохоронні органи або інші слідчі підрозділи;
- інші організації, які причетні до інциденту.

Дані про інцидент можуть бути отримані різними способами, включаючи:

- електронні листи;
- телефонні дзвінки;
- звіти при особистому спілкуванні;

- заповнення форми про інцидент на веб-сайті SOC;

- інформація від інших SOC.

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

SOC також отримує інформацію з внутрішніх джерел, таких як:

- системи виявлення та запобігання атак (IDS/IPS);

- системи виявлення / запобігання вторгнень на хостах (HIDS / HIPS);

- системи аналізу мережевого трафіку (NetFlow);

- журнали ОС, додатків і мережевих пристроїв, таких як веб-сервери, веб-проксі, DNS і попередження антивірусу (AV);

- інструменти менеджменту й аналізу логів та SIEM, які збирають, аналізують, зіставляють і інформують ці дані;

- криміналістичний аналіз зразків шкідливих програм і носіїв, наприклад жорстких дисків;

- системи автоматичного збору та оповіщення про дані кіберрозвідки;

- повний аналіз сеансу мережевих даних (PCAP).

Що стосується виявлення самих вторгнень, то існує два основних підходи: сигнатурне виявлення та виявлення аномалій.

- Сигнатурне виявлення, також називається виявленням несанкціонованої активності. Тобто система самостійно може виявити та розрізнити шкідливу активність в мережі.

- Виявлення аномалій означає, що система розпізнає звичну активність і попереджає аналітиків про відхилення.

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

Важливим елементом навчання є розуміння актуальних загроз та методів їх виявлення. Спеціалісти центру безпеки повинні вивчати нові типи атак, техніки обходу захисту і зразки зловмисного ПЗ. Також важливо навчати персоналу користуватися інструментами аналізу і системами виявлення вторгнень.

Додатковий акцент робиться на тренування з реагування на інциденти. Це включає в себе симуляції кібератак, вправи з виявлення та ізоляції загроз, а також тренування з відновлення роботи після інциденту. Заняття такого роду допомагають команді SOC вдосконалювати свої навички й реагувати швидше та ефективніше в реальних сценаріях.

Навчання персоналу центру безпеки має бути неперервним процесом, оскільки кіберзагрози постійно змінюються. Постійне оновлення знань і навичок є важливим для забезпечення високої ефективності та готовності команди SOC до викликів кібербезпеки.

2.4 Підготовка середовища і впровадження рішення

Перш ніж розгортати SOC, потрібно перевірити, чи всі компоненти відповідають призначенню та гарантують безпечне середовище, а передача логів підтримується в захищеному вигляді для унеможливлення сценарію перехоплення. Це має включати забезпечення захисту пристроїв персоналу SOC, а також надійні механізми управління доступом і автентифікації.

Для підготовки середовища, потрібно спланувати, як журнали безпеки будуть потрапляти до SOC:

- через SIEM систему тобто з використанням її агента, який збирає інформацію з кінцевих систем або кінцеві системи будуть самі надсилати логи напряму до SIEM;

- шляхом надсилання логів за допомогою лог-сервера, при якому розгортається сервер, на якому налаштовується лог-сервер, який буде збирати

логи і частину зберігати в собі, для подальшої передачі, якщо кількість логів дуже велика;

- гібридний варіант позиціонує і лог-сервера, і агентів системи SIEM.

У рамках впровадження обраного рішення здійснюється такий перелік заходів для початкового розгортання SOC:

1. Створення інфраструктуру управління журналами.

По-перше, необхідно розглядати впровадження систем журналювання, які автоматично збирають та аналізують дані з різних джерел, таких як системи безпеки, мережеві пристрої та додатки. Це дозволяє спеціалістам SOC вчасно виявляти аномалії та потенційні загрози, а також реагувати на їхні подальші розвиток [45].

По-друге, важливо мати централізовану систему управління журналами, яка дає можливість аналізувати й візуалізувати дані в реальному часі. Це включає використання спеціалізованих інструментів для пошуку, фільтрації та кореляції подій, а також для генерації звітів та аналітичних матеріалів. Забезпечення інфраструктури управління журналами в рамках SOC допомагає командам з безпеки створювати ефективні стратегії виявлення та реагування на потенційні кіберзагрози, підвищуючи загальний рівень безпеки організації [45].

2. Увімкнення мінімальної колекції критично важливих джерел даних.

Спочатку слід ідентифікувати ключові джерела даних, які найбільше релевантні для безпеки організації, такі як системні журнали, дані від антивірусних програм, файєрволів і систем виявлення вторгнень. При включенні цих критичних джерел даних в мінімальну колекцію SOC можливо забезпечити постійний потік інформації, необхідної для вчасного виявлення та відповіді на потенційні загрози [45].

Далі, у зв'язку з увімкненням мінімальної колекції, необхідно налаштувати системи для ефективного моніторингу й аналізу цих даних. Це включає створення правил і сценаріїв, які спрямовані на виявлення аномалій і потенційно небезпечної активності. Такий підхід дозволяє SOC реагувати на інциденти швидше й ефективніше, забезпечуючи високий рівень безпеки для інформаційної

інфраструктури організації. Увімкнення мінімальної колекції критичних джерел даних стає фундаментальним кроком у зміцненні кібербезпеки та зменшенні ризиків для бізнес-процесів.

3. Активація аналітики безпеки й можливостей автоматизації та оркестрування безпеки.

Запровадження аналітичних інструментів дозволяє збирати, аналізувати та інтерпретувати великі обсяги даних для виявлення аномалій та потенційних загроз у реальному часі. Інтеграція автоматизованих рішень та оркестрація безпекових заходів робить можливим автоматичний відгук на інциденти, що прискорює час реакції та допомагає уникнути ручного втручання.

Більше того, активна аналітика безпеки та автоматизація можуть бути оркестровані для створення повноцінної екосистеми кібербезпеки. Це включає інтеграцію різних систем безпеки, взаємодію між ними й автоматизацію виконання складних завдань безпеки. Цей підхід дозволяє організації ефективно впоратися з розмаїттям загроз і забезпечити високий рівень захисту, зменшуючи трудомісткість та підвищуючи швидкість реагування на інциденти [45].

4. Розгортання кількох варіантів використання, які зосереджені на комплексному виявленні загроз і реагуванні на них. Перш за все, важливо впроваджувати системи виявлення вторгнень/аномалій (IDS/ADS), які можуть ефективно моніторити мережевий трафік і системну активність для виявлення невідомих чи непередбачених змін, що можуть свідчити про кіберзагрози [43].

Другий аспект включає в себе розгортання систем SIEM, які інтегрують дані з різних джерел, таких як системи журналювання, фаєрволи та антивіруси. Це дозволяє створювати повний образ безпекового ландшафту та виявляти нестандартні або погано помічені шаблони атак. Комбінування цих варіантів використання надає комплексний погляд на кібербезпеку, забезпечуючи не лише виявлення потенційних загроз, а й швидке та координоване реагування на них для забезпечення безпеки інформаційної інфраструктури організації.

5. Інтеграція каналів розвідки загроз та інших джерел розвідувальної інформації, наприклад автоматизованих вхідних даних для підвищення точності

виявлення. По-перше, цей процес передбачає впровадження систем, які можуть автоматично збирати, обробляти та аналізувати дані з різноманітних джерел, таких як відкриті джерела інформації, форуми з кібербезпеки, темні веб-ресурси та інші ресурси розвідки. Це дозволяє забезпечити повний спектр інформації про потенційні загрози, враховуючи їхні характеристики та особливості.

Другий аспект інтеграції каналів розвідки полягає в розробці механізмів автоматизованого аналізу та обробки цієї інформації. Використання технологій штучного інтелекту та машинного навчання дозволяє автоматизовано класифікувати та оцінювати рівень загроз, роблячи висновки про можливий вплив на організаційну безпеку. Цей підхід допомагає вчасно реагувати на нові загрози, забезпечуючи вищу точність виявлення і знижуючи ризики безпеки.

Після розгортання основних можливостей обраного рішення SOC переходять до етапу впровадження сценаріїв використання на різних функціональних рівнях. На рівні аналітики, команди безпеки активно використовують сценарії для проведення глибокого аналізу подій та виявлення нестандартних чи підозрілих активностей. Інтелектуальні сценарії дозволяють виявляти та класифікувати загрози швидше та ефективніше, забезпечуючи підвищену відповідь на інциденти.

На рівнях автоматизації безпеки й оркестрування, сценарії грають ключову роль у впровадженні автоматичних відповідей на інциденти та оркестрації заходів забезпечення безпеки. Автоматизація дозволяє швидше реагувати на загрози та виконувати стандартні заходи безпеки, в той час як оркестрація забезпечує координований підхід до взаємодії різних систем безпеки. Це сприяє покращенню ефективності команд SOC та забезпеченню високого рівня захисту в інтенсивному кіберпросторі.

2.5 Підтримка та вдосконалення індивідуального рішення

Кіберзагрози постійно розвиваються, тому стратегія SOC також повинна розвиватися. Обов'язковим є регулярне оцінювання ефективності заходів безпеки, які впроваджуються командою SOC, проведення ретельної оцінки і вдосконалення стратегії безпеки організації з урахуванням нових загроз, кращих галузевих практик та уроків, отриманих з інцидентів. Таким чином буде сформовано загальноорганізаційну культуру постійного вдосконалення безпеки.

Оцінка та вдосконалення стратегії безпеки повинні бути інтегрованими процесами, що враховують кращі галузеві практики, аналіз останніх трендів у кібербезпеці, а також вивчення уроків, отриманих з попередніх інцидентів. Важливо відзначити, що цей цикл постійного вдосконалення також включає в себе забезпечення освітленості персоналу та створення загальноорганізаційної культури, спрямованої на активне виявлення та запобігання кіберзагрозам. Тільки такий гнучкий та вдосконалюваний підхід може забезпечити ефективний захист в умовах невпинної еволюції кіберзагроз.

Дотримуючись вищезазначених вимог, організація зможе закласти базу для ефективної стратегії SOC, яка відповідає організаційним цілям, враховує рівні толерантності до ризику, зменшує кіберризики та дозволяє впевнено орієнтуватися в мінливому ландшафті загроз.

Після того, як SOC розпочне своє функціонування, він потребуватиме постійного технічного обслуговування, зокрема оновлення параметрів конфігурації та коригування для підвищення точності виявлення. З часом доцільно буде розглянути можливість додавання до рішення допоміжних систем.

Варто наголосити, що інвестиції в розвиток скоординованої команди кваліфікованих спеціалістів SOC, які можуть успішно використовувати обраний стек технологій безпеки, інтерпретувати дані, приймати обґрунтовані рішення та оперативно і якісно реагувати на загрози, сприятимуть формуванню ефективної системи забезпечення кібербезпеки організації.

Висновки до розділу 2

Дослідження показало, що процес побудови центру безпеки є послідовним і комплексним процесом, який складається з таких етапів: розробка стратегії центру безпеки; створення індивідуального рішення SOC; створення процесу, процедури та навчання; підготовка середовища; впровадження рішення; розгортання наскрізних сценаріїв використання; підтримка та розвиток індивідуального рішення SOC.

У рамках *розробки стратегії і створення індивідуального рішення центру безпеки* здійснюється уточнення бізнес-цілей для створення SOC, оцінка наявних можливостей SOC і визначення функціональних вимог, проектування технічної архітектури, визначення робочих процесів для подій безпеки, формування штату.

Навчання та розвиток персоналу також відіграють ключову роль у виявленні та запобіганні кіберзагрозам, забезпечує високий рівень обізнаності персоналу у галузі кібербезпеки. Програми навчання повинні бути адаптивними й охоплювати найновіші методики виявлення загроз, а також враховувати конкретні характеристики інфраструктури та бізнес-процесів організації.

На етапі *підготовки середовища* перевіряють, чи всі компоненти відповідають призначенню та гарантують безпечне середовище, обрати канали і забезпечити захищену передачу логів. У ході *впровадження обраного рішення* здійснюється початкове розгортання SOC, зокрема: створення інфраструктури управління журналами; увімкнення мінімальної колекції важливих джерел даних; активацію засобів аналітики, автоматизації та оркестрування безпеки; розгортання кількох варіантів комплексного виявлення і реагування на загрози.

Підтримка та вдосконалення індивідуального рішення центру безпеки передбачає регулярне оцінювання ефективності заходів безпеки, проведення ретельної оцінки і вдосконалення стратегії безпеки організації на основі нових ризиків і загроз, впровадження кращих галузевих практик і врахування уроків, отриманих з інцидентів.

РОЗДІЛ 3
ПЕРЕВАГИ Й НЕДОЛІКИ АУТСОРСИНГУ SOC ДЛЯ РІЗНИХ ПІДПРИЄМСТВ

3.1 Внутрішній чи керований SOC: чинники прийняття рішення

У сучасному цифровому ландшафті організації стикаються з дедалі більшою кількістю кіберзагроз. Для ефективної боротьби з цими загрозами компанії повинні створити надійний центр безпеки SOC. Однак критично важливе рішення виникає під час визначення того, чи будувати власний SOC чи вибрати керовані послуги SOC [23].

Перш ніж заглибитися в процес прийняття рішень, важливо зрозуміти фундаментальну різницю між створенням власного SOC і передавання послуг безпеки на управління постачальнику [25].

Так, упровадження внутрішнього центру безпеки на базі компанії передбачає створення спеціальної групи аналітиків безпеки, придбання необхідної інфраструктури й налаштування інструментів і технологій безпеки. Ця опція пропонує повний контроль, налаштування й широкі можливості узгодити SOC з конкретними потребами організації. Однак це вимагає значних вкладень часу, грошей і досвіду.

З іншого боку, центр безпеки, управління яким здійснює постачальник, включає передачу функцій моніторингу безпеки та реагування на інциденти спеціалізованому сторонньому постачальнику. Ця опція дозволяє організаціям використовувати знання та досвід зовнішніх професіоналів, які добре знаються на найновіших методах безпеки. Керовані служби SOC часто забезпечують цілодобовий моніторинг, розвідку загроз і можливості реагування на інциденти, зменшуючи навантаження на внутрішні ресурси.

Для прийняття оптимального рішення щодо того, який вид центру безпеки обрати, організація має врахувати низку основних чинників (Рис. 3.1):

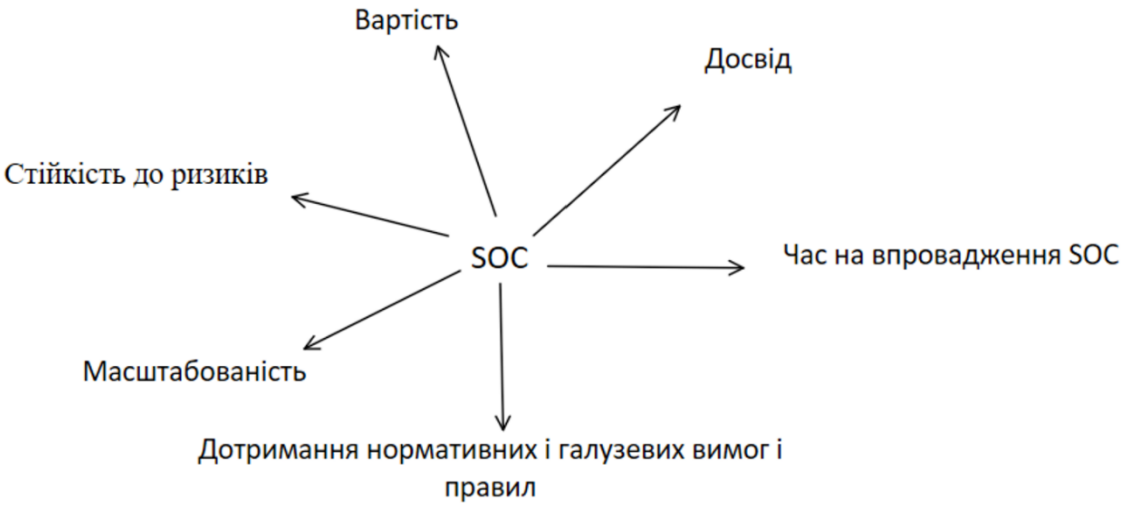

Рис. 3.1. Чинники прийняття рішення: внутрішній чи аутсорсинговий SOC

Вартість: слід оцінити фінансові наслідки створення та підтримки внутрішнього SOC у порівнянні з поточними витратами, пов'язаними з керованими послугами безпеки, а також врахувати такі фактори, як персонал, інфраструктура, навчання та модернізація технологій.

Досвід: необхідно оцінити наявний набір навичок фахівців з кібербезпеки, які зможуть забезпечити виконання функцій SOC в організації. Адже, у випадку їх нестачі, виникне потреба у найманні й утриманні кваліфікованих аналітиків безпеки, тоді як керовані послуги центру безпеки надають доступ до команди зовнішніх експертів із різноманітним досвідом.

У той час, як при аутсорсингу центру безпеки, постачальник послуг зможе залучити більш широкий спектр кваліфікованих спеціалістів, наприклад укладаючи контракти з незалежними операторами і наймаючи людей з різними спеціальностями та кваліфікаціями, які зможуть вирішити конкретні вузькоспеціалізовані проблеми безпеки. Цей кадровий резерв також заощаджує час, оскільки не потрібно шукати персонал.

Масштабованість: потрібно врахувати вимоги конкретної організації до розширення масштабів діяльності SOC. Якщо у планах передбачене швидке

зростання або коливання потреб у безпеці, керовані послуги безпеки можуть запропонувати більшу гнучкість і масштабованість порівняно з власним SOC.

Крім цього аутсорсинг стає цінним інструментом подолання кадрових, фінансових та інших потенційних проблем організації, пов'язаних з розробкою і впровадження власного центру безпеки. Використовуючи стороннього постачальника послуг SOC, компанія перекладає на нього відповідальність за персонал, постачання технологій і уникає разового виділення значних коштів.

Дотримання нормативних і галузевих вимог і правил: оскільки функціонування внутрішнього SOC має здійснюватися в рамках діючого законодавства і нормативних документів, слід добре знати вимоги, що стосуються галузі кібербезпеки, і в подальшому цілком їх дотримуватися. Постачальники послуг керованого SOC часто спеціалізуються на управлінні відповідністю, забезпечуючи дотримання нормативних стандартів.

Час на впровадження SOC: створення внутрішнього центру безпеки може зайняти багато часу, вимагаючи ретельного планування, найму та налаштування інфраструктури. Керовані послуги SOC пропонують швидший графік впровадження, що дозволяє організаціям швидко підвищити рівень безпеки.

Стійкість до ризиків: необхідно ретельно проаналізувати потенційні ризики кібербезпеці і встановити рівні їх прийнятності для організації. Незважаючи на те, що створення внутрішнього SOC забезпечує більший контроль над операціями безпеки, це також означає взяти на себе повну відповідальність за будь-які потенційні інциденти. Натомість керовані послуги центру безпеки забезпечують розподіл ризиків між організацією та надавачем послуг і надають додаткові рівні захисту [5].

Отже, рішення побудувати власний центр безпеки або вибрати послуги SOC на аутсорсинговій основі є критично важливим і вимагає ретельного розгляду різних факторів. Оцінюючи вартість, досвід, масштабованість, вимоги до відповідності, час впровадження та толерантність до ризику, організації можуть прийняти обґрунтоване рішення, яке відповідає їхнім унікальним потребам і ресурсам. Водночас, слід пам'ятати, що універсального рішення не

існує, а оптимальний вибір залежатиме від конкретних обставин і цілей конкретної організації.

Таким чином, основною перевагою внутрішнього центру безпеки є забезпечення безпосереднього внутрішньо-організаційного контролю за функціонуванням SOC і виконанням його завдань, оскільки не потрібно покладатися на стороннього постачальника. Завдяки цьому організація матиме:

– власних експертів із кібербезпеки, які займаються виключно захистом корпоративних ресурсів, систем і мереж. У такому випадку забезпечується високий рівень обізнаності персоналу SOC із внутрішніми системами й мережевою архітектурою, який важко зрівняти з зовнішнім постачальником;

– можливість зберігати всі файли журналів та інші дані безпеки на місці. Це допомагає компанії підтримувати видимість і контролювати свої дані безпеки;

– повний контроль з питань вибору та розгортання рішень безпеки. У той час, як зовнішній постачальник SOC матиме попередньо вибраний стек безпеки, яким він керує [21].

3.2 Переваги центру безпеки на аутсорсингу

Дослідження показало, що вибір варіанту передачі функцій центру безпеки на аутсорсинг має багато переваг для організації-замовника (Рис. 3.2). Розглянемо кожну з них детальніше.

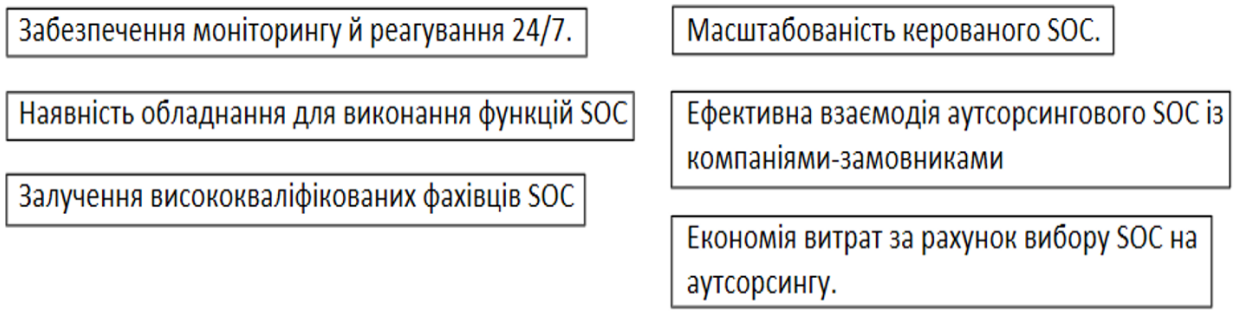

Рис. 3.2. Переваги SOC на аутсорсинговій основі

Наявність обладнання для виконання функцій центру безпеки. Перша перевага, пов'язана з аутсорсинговими послугами SOC, полягає в тому, що встановлення всього супутнього обладнання, необхідного для оснащення команди, вже виконано. Якщо створюється центр безпеки, потрібно буде придбати обладнання і встановити його належним чином. Аутсорсингові фірми SOC вже мають налаштоване обладнання і готові мінімізувати час простою.

Аутсорсинговий SOC використовує ряд технологій для ефективного моніторингу, виявлення та реагування на потенційні загрози безпеки:

– SIEM – забезпечують централізований збір, аналіз і відображення даних про події безпеки з різних джерел, виявлення аномалій і вразливостей.

– Міжмережеві екрани - контролюють трафік в мережі та запобігають несанкціонованому доступу до систем. Фаєрволи використовуються разом з системами IDS/IPS для точного виявлення загроз і швидкого реагування на них.

– Антивірусні рішення – виявляють і блокують віруси, троянські програми, шпигунське ПЗ та інші загрози.

– Засоби виявлення й реагування на загрози кінцевим точкам (EDR) - відстежують активність на кінцевих пристроях і реагують на підозрілі події і вторгнення.

– Платформи розвідки загроз (Threat Intelligence) - надають інформацію про поточні загрози, зокрема дані про вторгнення, вразливості й методи атак.

– Засоби управління вразливостями (Vulnerability Management) – виявляють і управляють вразливостями в інформаційних системах та мережах.

– Системи координації, автоматизації і реагування на події безпеки (SOAR) - автоматизують і координують процеси реагування на інциденти безпеки.

– Засоби аналітики безпеки (Security Analytics) – обробляють великі обсяги даних і виявляють складні атаки.

– Системи поведінкової аналітики (UEBA) - аналізують поведінку користувачів та об'єктів для виявлення аномалій.

– Панелі управління та засоби візуалізації – унаочнюють дані та стан безпеки для зручного моніторингу та прийняття рішень.

Аутсорсингові SOC зазвичай належать до висококваліфікованих експертів у сфері кібербезпеки. Вони мають доступ до передових технологій та ресурсів, що дозволяє їм надавати високий рівень захисту.

Залучення висококваліфікованих фахівців SOC. Експертні знання та компетентність в аутсорсинговому центру безпеки становлять важливу основу для ефективного виявлення, аналізу та протидії кіберзагрозам.

Глибокі технічні знання є критичним елементом для аутсорсингового SOC, який відповідає за ефективне виявлення та реагування на кіберзагрози. Вони охоплюють широкий спектр областей, включаючи кібербезпеку, мережеву безпеку, інформаційну безпеку, розуміння алгоритмів шифрування та їхнє використання для захисту конфіденційної інформації, знання процесів аналізу та інтерпретації інформації з різних журналів та лог-файлів, вміння вести моніторинг активності, використовуючи засоби управління інформацією про безпеку.

Головні аспекти, в яких повинен розбиратися спеціаліст центру безпеки, – це актуальні та поширені кіберзагрози та популярні тактики вторгнення. Кіберзагрози включають різні типи шкідливих програм:

– Віруси (Viruses): Вони прикріплюються до інших програм або документів і виконуються при їх запуску. Вони можуть руйнувати чи модифікувати файли та програми.

– Черв'яки (Worms): Вони поширюються самостійно, використовуючи мережі та комунікаційні канали. Черв'яки можуть швидко розповсюджувати свої копії через інтернет чи локальні мережі.

– Троянські коні (Trojans): Вони приховуються в корисних програмах, але виконують зловмисні функції без відома користувача, такі як збір конфіденційної інформації.

– Шпигунські програми (Spyware): Збирають інформацію про користувача без його дозволу. Це може включати перегляд введеної інформації, паролів, історію перегляду тощо.

– Рекламне програмне забезпечення (Adware): Відображає рекламу на комп'ютері користувача без його згоди. Деякі можуть бути досить нав'язливими та впливати на продуктивність системи.

– Програми-вимагачі (Ransomware): Зашифровує файли користувача і вимагає викуп за їх розкодування. Користувачам часто доводиться платити кількасот або навіть тисячі доларів у криптовалюті.

– Ботнети (Botnets): Збирають велику кількість комп'ютерів під контроль зловмисника для використання у шкідливих діях, таких як атаки на мережу або розсилання спаму.

– Пупси (PUPs - Potentially Unwanted Programs): Невеликі програми, які можуть встановлюватися разом з іншим ПЗ і виконувати небажані дії, такі як зміна налаштувань браузера.

– Фішингові програми (Phishing Software): Спроектовані для викрадання особистої інформації, шляхом імітації надійних веб-сайтів чи використання соціальної інженерії.

Розуміння різних типів шкідливого ПЗ, їхніх методів поширення та впливу на системи сприяє їх вчасному виявленню і застосуванню превентивних заходів.

Також фахівці центру безпеки мають бути глибоко обізнаними про основні тактики вторгнення, які можуть бути задіяні:

– Фішинг: атаки фішингу включають надсилання підроблених електронних листів, повідомлень чи перенаправлення на фейкові веб-сайтів, щоб спонукати користувача ввести конфіденційні дані, такі як паролі чи банківську інформацію.

– Шкідливі програми: зловмисники намагаються впровадити шкідливе ПЗ у систему жертви, використовуючи віруси, черв'яки, троянські коні та інші види шкідливих програм.

– Брутфорс-атаки: використовують програми для автоматичної спроби вгадати паролі, шляхом спроби всіх можливих комбінацій.

– Атаки на слабкі місця в мережі: порушники прагнуть експлуатувати слабкі місця в мережевих пристроях чи ПЗ для вторгнення в систему.

– DDoS-атаки: атаки, спрямовані на перевантаження мережі чи серверів, щоб зробити їх недоступними для законних користувачів.

– Викрадення ідентифікаційних даних (Credential Theft): здобуття імен і паролів користувачів для нелегального доступу до системи чи інформації.

– Маніпулювання векторами атаки: використання різних методів для введення шкідливого коду або отримання несанкціонованого доступу, таких як вразливості в ПЗ, застарілі програми чи слабкі конфігурації.

– Соціальна інженерія: зловмисники використовують маніпуляції та обман, щоб отримати від користувачів конфіденційну інформацію або доступ до системи.

– Атаки на програмне забезпечення: експлуатація вразливостей у програмному забезпеченні, яке використовується на цільовій системі.

– Використання анонімізації: порушники намагаються залишати мінімум слідів та приховувати свою ідентичність, використовуючи анонімізаційні сервіси та інші засоби.

Здатність аналізу та реагування в аутсорсинговому SOC визначає його ефективність у забезпеченні безпеки та відновленні роботи після кіберінцидентів. Така глибока компетентність дозволяє швидко й точно взаємодіяти з кіберзагрозами для мінімізації збитків та захисту організації.

Постійне оновлення навичок в аутсорсинговому SOC є стратегічно важливим, оскільки дозволяє ефективно реагувати на швидкозмінний ландшафт кіберзагроз і залишатися на передовому фронті кібербезпеки. Існує велика кількість платформ, на яких можна тренуватися, типу Hack The Box, Try hack me, vulnhub. Фахівці, які активно працюють над своїм професійним розвитком, мають змогу ефективно впроваджувати інноваційні стратегії та гарантувати високий рівень захисту інформації.

Ефективна взаємодія аутсорсингового SOC *із компаніями-замовниками.* Співпраця між аутсорсинговим центром безпеки і замовниками визначається високим рівнем довіри, гнучкістю та спільним бажанням досягти високих результатів у сфері кіберзахисту. Це стратегічне партнерство спрямоване на забезпечення безпеки та стійкості інформаційних систем замовників у зростаючому ландшафті кіберзагроз. Така взаємодія забезпечує визначення чіткої архітектури і надає перевагу у вигляді «прив`язки» спеціалістів SOC до інфраструктури замовника з метою більш ефективного виявлення інцидентів.

Регулярна звітність перед клієнтами щодо стану кібербезпеки відіграє критичну роль у забезпеченні взаєморозуміння та довіри між аутсорсинговим SOC та його замовниками. Цей процес не лише вказує на прозорість та відповідальність центру безпеки, але й стає ефективним інструментом для спільної роботи над постійним покращенням заходів безпеки.

Взаємодія SOC і замовників включає також консультації та тренінги з питань кібербезпеки для поліпшення власного захисту компаній-клієнтів, активний обмін інформацією про виявлені кіберзагрози й методи боротьби з ними з іншими SOC. Співпраця з іншими галузевими гравцями, участь у спільних ініціативах і групах для розвитку нових методів захисту забезпечують суттєве підвищення компетентності спеціалістів надавача послуг безпеки.

Використання ефективних комунікаційних інструментів для оперативного обміну інформацією між командами SOC та з клієнтами таких як Slack, Microsoft Teams чи Telegram, дозволяє оперативно й ефективно спілкуватися в режимі реального часу. Зручність інтерфейсу та можливість створення окремих каналів для різних завдань полегшують координацію робіт.

Актуальність знань і технологій, які застосовуються в роботі зовнішнього SOC підтримуються шляхом інтегрування й використання новітніх рішень від провідних виробників засобів кіберзахисту. Це може включати в себе впровадження нових інструментів для виявлення загроз, використання продуктів з хмарної безпеки та впровадження інших інновацій. Гнучкість у використанні новітніх рішень дозволяє зовнішньому SOC швидко адаптуватися до змін у

кіберзагрозах та удосконалювати свої практики для забезпечення максимальної ефективності в галузі кібербезпеки.

Невід'ємною частиною ефективного вирішення інцидентів та координації роботи команд центру безпеки є використання систем тікетінгу й управління проектами. Системи тікетінгу – це програмне забезпечення служби підтримки, яке використовується для обробки, управління та відстеження проблем клієнтів від подання заявки до вирішення. Таке ПЗ дозволяє структурувати й відстежувати кожен етап вирішення інциденту, роблячи процес більш прозорим та ефективним. Кожен інцидент отримує унікальний тікет, який містить всю необхідну інформацію, таку як опис проблеми, пріоритет, стан вирішення, призначених відповідальних осіб та інші ключові деталі.

Системи управління проектами допомагають управляти різноманітними завданнями та ініціативами в межах SOC. Засоби цієї категорії дозволяють призначати та розподіляти завдання між фахівцями, визначати пріоритети й терміни виконання. Вони надають можливість створення і відстеження проектів, що допомагає забезпечити систематичний та організований підхід до управління ресурсами, часом і виконанням завдань. У результаті використання цих інструментів команди SOC можуть ефективно співпрацювати, забезпечуючи структуроване та вчасне вирішення інцидентів, а також оптимальне виконання завдань для підвищення кібербезпеки.

Економія витрат за рахунок вибору SOC на аутсорсингу. Внутрішній центр безпеки вимагає значних витрат на наймання й підтримку персоналу, впровадження технічних засобів і постійне оновлення знань. Аутсорсинг дозволяє економити кошти, перекладаючи ці витрати на зовнішнього постачальника.

Економія ресурсів є важливим аспектом діяльності аутсорсингового центру безпеки, оскільки це сприяє оптимізації витрат і забезпечує ефективність заходів з кібербезпеки. Так, керований SOC економить на використанні комплексних рішень (SIEM, IDS/IPS, EDR/XDR, сканер вразливостей), а також моделей оплати відповідно до обсягу послуг, який дозволяє оптимізувати витрати й надавати клієнтам гнучкість у виборі пакетів послуг. Такі моделі

оплати замість фіксованого тарифу пропонують клієнтам платити лише за той обсяг та рівень послуг, які вони фактично використовують.

Це особливо актуально в сфері кібербезпеки, де потреби можуть різнитися в залежності від розміру компанії, її інфраструктури та особливостей ризиків. Таким чином клієнти можуть ефективно відповідати на змінні умови й витрати ресурсів на забезпечення необхідного рівня кіберзахисту, адаптувати свій обсяг послуг відповідно до зростаючих чи спадаючих потреб, що робить цей підхід більш ефективним і економічно вигідним для отримувачів послуг.

Економія ресурсів у аутсорсинговому SOC не тільки допомагає знизити витрати, але й сприяє більш ефективному використанню обмежених ресурсів, щоб досягти максимального рівня захисту інформації й оптимальної функціональності безпекових систем. Це важливий аспект стратегії кібербезпеки, оскільки дозволяє компаніям зосередитися на своїх основних функціях, уникнути витрат на розгалужені та складні структури, і в той же час, отримувати високий рівень захисту від кіберзагроз.

Забезпечення моніторингу й реагування 24/7. Зовнішні центри безпеки можуть забезпечувати постійний моніторинг та реагування на кіберзагрози у будь-який час, що є особливо важливим у світлі постійної еволюції кіберзагроз.

Безперервний моніторинг та реагування як основний елемент керованого SOC є критичним для забезпечення постійного захисту інформації клієнтів від кіберзагроз і включає не лише пошук і виявлення потенційних загроз, а й оперативне реагування на них. Автоматизовані системи для виявлення аномальної поведінки й атак дозволяють підвищити ефективність процесу моніторингу, оскільки вони здатні оперативно реагувати на події, які можуть бути непоміченими людським оком.

Використання алгоритмів, які аналізують зміни в поведінці користувачів і систем, стає ключовим для виявлення підозрілих дій. Ці алгоритми дозволяють виявляти відхилення від нормальної активності, які можуть свідчити про можливі кіберзагрози, а також передбачати можливі інциденти і розробляти

детальні плани реагування, спрямовані на підготовку SOC до вирішення потенційних загроз.

Системи управління інцидентами грають важливу роль в організації та відслідковуванні всіх етапів вирішення проблеми, починаючи від виявлення інциденту та закінчуючи його виправленням. Це включає в себе документування, аналіз та вдосконалення процесів реагування на інциденти.

Окрім того, використання автоматизованих систем, які допомагають аналітикам у швидкому виявленні та відповіді на інциденти, сприяє зниженню часу реакції й оперативному прийняттю рішень у відповідь на кіберзагрози. Це робить центр безпеки більш витрато-ефективним і здатним до вирішення складних кібербезпекових викликів.

Миттєва відповідь на критичні загрози стає необхідною для негайного усунення ризиків і запобігання подальшим пошкодженням. Автоматичні системи SOC можуть вживати різні заходи, такі як призупинення аномальної активності, блокування IP-адрес чи видалення заражених файлів, щоб запобігти поширенню атак і забезпечити безпеку інформаційних ресурсів.

Однак важливо зазначити, що автоматизоване реагування має бути правильно налаштованим і супроводжуватися постійним моніторингом. Неналежне налаштування або неправильне розпізнавання загроз може призвести до некоректних рішень або навіть втрати доступу до легітимних ресурсів. Таким чином, автоматичне реагування має бути інтелектуальним і гнучким, враховувати специфіку середовища та потреби конкретної організації.

Масштабованість керованого центру безпеки. Здатність до швидкого масштабування є ключовим аспектом для аутсорсингового SOC, оскільки дозволяє ефективно адаптуватися до коливань у навантаженні, випадкових або сезонних збільшень робочого обсягу та нових викликів у сфері кіберзахисту.

Зовнішній SOC може оперативно реагувати на зростання обсягів роботи й забезпечити швидку масштабованість відповідно до потреб клієнта. Це особливо важливо в умовах динамічного кіберсередовища, де зміни в загрозах і ризиках можуть бути різкими.

Використання хмарних платформ є одним із ключових засобів для забезпечення гнучкості й можливості швидко масштабувати інфраструктуру центру безпеки в залежності від обсягів роботи. Це дозволяє ефективно використовувати ресурси та зменшує час на впровадження нових систем. Хмарні рішення допомагають легко масштабувати рішення SOC, забезпечуючи еластичність, необхідну для ефективної роботи в динамічному середовищі.

Важливу роль у швидкому створенні й розгортанні нових ресурсів центру безпеки відіграє використання технології віртуалізації, яка дозволяє гнучко управляти обчислювальними ресурсами, швидко реагуючи на зміни в потребах клієнта або обсягах роботи. Віртуалізація сприяє ефективному використанню апаратних ресурсів та забезпечує швидку реакцію на зростання навантаження.

Застосування автоматизованих засобів для швидкого розгортання нових систем і сервісів допомагає зменшити людський вплив на процес масштабування та забезпечити ефективність у вирішенні завдань. Це включає в себе автоматичну конфігурацію, розгортання й налаштування нових компонентів SOC.

Для оптимального реагування на збільшення навантаження доцільно впроваджувати системи, які автоматично реагують на ці зміни та відповідно масштабують інфраструктуру, зокрема автоматичне вмикання додаткових ресурсів, розширення обчислювальних кластерів чи інші заходи, спрямовані на підтримку ефективного функціонування SOC на час підвищених навантажень.

За потреби зовнішній центр безпеки може забезпечити співпрацю з резервними командами й залучення додаткових фахівців для вирішення кризових ситуацій або великих інцидентів.

3.3 Недоліки зовнішнього центру безпеки

Передача журналів безпеки третім особам. Аутсорсинг SOC, безсумнівно, є відмінним варіантом для організацій з конкретними потребами. Водночас такий варіант має декілька недоліків, на які варто звернути увагу.

Примітно, що найбільшим недоліком аутсорсингу для такого важливого завдання як операції безпеки корпоративної мережі є відсутність безпосереднього нагляду. Завдяки внутрішнім підрозділам SOC організація може прямо взаємодіяти з персоналом і бути мати впевненість, що все працює відповідно до встановлених вимог і очікувань. Крім того, конфіденційні дані, які належать або обробляються організацією, зберігаються за межами офісу на серверній платформі постачальника послуг, а не всередині компанії. Отже, функції резервного копіювання й доступу до даних можуть залежати від здатності фірми-постачальника надавати швидкі послуги.

Незважаючи на те, що передача корпоративних журналів клієнта фірмі-постачальнику здійснюється у реальному часі через захищений тунель під наглядом висококваліфікованих спеціалістів SOC, аутсорсингове рішення має негативні аспекти. Зокрема, через некомпетентність фахівців зовнішнього центру безпеки можливою є передача потенційних вразливостей третім особам з подальшим проникненням у корпоративну мережу і витоком конфіденційної інформації клієнта.

Недостатня кастомізація послуг керованого SOC. Також є питання щодо налаштування пакету послуг безпеки під потреби й можливості конкретної організації. З одного боку, компанія-клієнт отримує увагу команди, яка спеціалізується на безпеці, з іншого боку – надається широкий спектр послуг, аналогічний для багатьох різних компаній. Отже, типові послуги і впровадження безпеки від постачальника налаштовані так, щоб працювати для будь-якої системи, а не бути спеціально адаптованими до потреб організації.

Універсальний підхід може призвести до нестачі глибини знань про специфічні галузі або особливості конкретного бізнесу клієнта. Аутсорсинговий SOC може не мати достатньої експертизи щодо особливостей діяльності клієнта, а це може негативно впливати на якість індивідуального кіберзахисту.

Відсутність індивідуального підходу може також призвести до труднощів у збереженні контексту щодо історії інцидентів та особливостей мережі клієнта. При вирішенні інцидентів або аналізі загроз важливо мати повний контекст, щоб ефективно взаємодіяти з унікальними викликами конкретного бізнесу.

Аутсорсингові центри безпеки часто використовують стандартизовані інструменти для моніторингу й виявлення загроз. Однак така стандартизація може не враховувати специфічні технічні особливості або внутрішні стандарти певної компанії.

Умови обмеженої кастомізації можуть вплинути на рівень взаємодії між аутсорсинговим SOC та внутрішньою командою безпеки компанії. Не враховані індивідуальні потреби можуть стати перешкодами для ефективної комунікації та співпраці між усіма сторонами. Для вирішення цього питання в межах команди операційного центру безпеки доцільно виділити для кожного замовника окремого фахівця, який буде добре знайомий з особливостями клієнта, орієнтуватися в його інфраструктурі та ландшафті загроз, а отже, зможе коригувати зусилля з кіберзахисту відповідно до потреб даної компанії.

Труднощі управління та контролю центру безпеки. Однією з основних проблем управління аутсорсинговим SOC є обмежений внутрішній контроль над процесами безпеки. В таких умовах організація може втратити можливість негайно втручатися в безпекові операції та приймати стратегічні рішення, що впливає на спроможність реагувати на нові загрози або зміни в інфраструктурі.

Однією з важливих складових віддаленого управління є комунікація. Компанії повинні розробляти чіткі механізми обміну інформацією з аутсорсинговим SOC, враховуючи різницю у місцях розташування. Використання сучасних засобів зв'язку, таких як відеоконференції, чат та

електронна пошта, стає критичним для забезпечення ефективного обміну інформацією та вирішення завдань на віддаленій основі.

Однак разом із вигодами віддаленого управління виникають і виклики. Відсутність фізичної присутності може призвести до труднощів у плануванні та нагляді за процесами безпеки. Необхідно активно розробляти стратегії ефективного контролю, щоб уникнути можливих непорозумінь, забезпечити відповідність стандартам безпеки і зберегти високий рівень захисту ІКС.

Управління відповідальністю також може бути проблематичним у контексті аутсорсингу, якщо відповідальність за різні аспекти кібербезпеки між замовником і аутсорсинговим партнером не буде належним чином визначена і розподілена. Це може вплинути на ефективність реагування на інциденти і знизити рівень впевненості в безпеці інформації.

Часто є досить важко врахувати всі аспекти послуги і включити їх у контрактні зобов'язання. Недостатня чіткість у специфікаціях може призвести до конфліктів і непорозумінь між сторонами. Особливо важливо забезпечити чіткість і однозначність у визначенні рівня послуг, обсягів відповідальності та процедур взаємодії.

Визначення й вимірювання продуктивності аутсорсингового SOC також може бути викликом. Організація-замовник і постачальник послуг безпеки повинні визначити ключові індикатори продуктивності, які відображають рівень ефективності й безпеки, а також розробити механізми для систематичного відслідковування цих показників. Такий контроль важливий для забезпечення якості послуг центру безпеки та відповідності стратегічним цілям організації.

Використання стандартних інструментів SOC. Стандартизація інструментів кіберзахисту може призвести до недостатньої гнучкості при реагуванні на нові чи унікальні загрози. Встановлені засоби можуть виявитися неефективними у випадку, коли потрібно швидко адаптуватися до різноманітних кіберзагроз або використовувати нові технології.

Крім того, засоби безпеки не завжди ідеально відповідають специфіці бізнес-процесів і потребам конкретної компанії. Кожна організація має свої

унікальні вимоги й особливості, і використання стандартизованих інструментів може не задовольнити всі ці потреби. Коли компанія зупиняється на конкретних інструментах, вона може втратити можливості використання нових рішень, які сприятимуть покращенню її кібербезпеки.

3.4 Рекомендації щодо впровадження SOC для різних організацій

Оскільки організації стикаються з неминучою необхідністю використання центру безпеки як з міркувань безпеки, так і з огляду на обов'язок дотримуватися дедалі жорсткіших нормативних вимог, більшість із них постають перед вибором: створювати власний SOC чи скористатися рішенням від стороннього постачальника.

Розглянемо, яким організація підходить кожне із рішень.

Внутрішній центр безпеки

Впровадження внутрішнього центру безпеки підходить організаціям, яким потрібні надзвичайно спеціалізовані або налаштовані процеси. Як правило, це дуже великі підприємства з кількома суворими нормативними вимогами в різних місцях розташування. Власний SOC також необхідний для організацій, які зберігають величезну кількість конфіденційної інформації.

Саме в таких компаніях внутрішній SOC працюватиме найкраще, оскільки вони потребують повного контролю над своїми процесами та продуктивністю послуг безпеки. Якщо його правильно налаштувати, він може забезпечити надзвичайно високий рівень безпеки.

Водночас, у прийняття внутрішнього центру безпеки є багато вже перелічених вище недоліків, зокрема: початкове налаштування та конфігурація SOC може коштувати мільйони доларів і вимагати 6-12 місяців для досягнення повної готовності. Тому згадані організації описаного вище характеру нерідко змушені звертатися до зовнішнього SOC як посередника.

Після налаштування внутрішньому центру безпеки потрібно кілька років, щоб досягти бажаного рівня ефективності, адже членам команди потрібно буде навчитися злагоджено працювати разом, адаптувати робочі процеси під потреби організації. На цьому шляху не уникнути помилок, які треба буде виправляти й запобігати їх повторні появі. Цей період навчання та ітерації часто обходиться організаціям навіть дорожче, ніж початкове налаштування.

Необхідність цілодобового моніторингу та підтримки є ще одним каменем спотикання для внутрішніх SOC. Ця потреба виникла лише протягом останніх кількох років і ще більше збільшує поточні витрати.

Аутсорсинг/керований центр безпеки

На відміну від впровадження власного рішення, вибір аутсорсингового центру безпеки надає компаніям можливість майже одразу отримати повний доступ до всього спектра послуг і відчути переваги керованого SOC. Від замовника очікується здійснити лише незначні процедури зі встановлення і налаштування, оскільки всю основну роботу виконує постачальник SOC.

Такий підхід усуває значні перешкоди для започаткування центру безпеки і дозволяє компаніям із набагато меншими бюджетами отримати доступ до професійно реалізованих послуг із застосуванням найсучасніших технологій та залученням провідних спеціалістів із кібербезпеки.

Використовуючи аутсорсинг SOC, організації не потрібно турбуватися про персонал, забезпечення програмним і апаратним забезпеченням, оренду місця для операційного центру безпеки, технічне обслуговування й оновлення чи будь-які інші витрати, пов’язані з управлінням власним центром безпеки.

Однак, на відміну від внутрішнього центру безпеки, замовник майже не впливає на повсякденну роботу SOC. Процесами та процедурами боротьби з кіберзагрозами керує виключно постачальник. Це може ускладнити роботу організацій, які мають обов’язки жорсткого дотримання нормативних вимог, оскільки багато постачальників не захочуть або не зможуть адаптувати свій підхід для одного клієнта.

Тим не менше, для багатьох компаній це не буде проблемою, і фінансові вигоди від використання аутсорсингу SOC значно переважують недоліки, коли йдеться про гнучкість, контроль і адаптивність. У поєднанні з конкурентоспроможними та комплексними угодами про рівень послуг між постачальником послуг і користувачем (Service-level agreement, SLA) це означає, що аутсорсингові центри безпеки часто є некладною проблемою для багатьох компаній [23].

Висновки до розділу 3

З'ясовано, що створення центру безпеки є актуальним завданням майже кожної сучасної компанії. Однак критично важливим є зробити вірний вибір між розбудовою внутрішнього SOC і передавання послуг безпеки на управління постачальником. Для прийняття оптимального рішення організація має врахувати такі основні чинники: вартість реалізації кожного з варіантів; наявність у фахівців організації навичок, необхідних для виконання функцій SOC; перспективи масштабування центру безпеки; потреба у дотриманні нормативних і галузевих вимог; час на впровадження SOC; рівень стійкості компанії до ризиків.

Дослідження показало, що вибір варіанту передавання функцій центру безпеки на аутсорсинг має багато переваг для організації-замовника, зокрема: наявність у постачальника обладнання й високо-кваліфікованих фахівців для виконання функцій SOC; ефективна взаємодія аутсорсингового SOC із компаніями-замовниками; забезпечення моніторингу безпеки й реагування 24/7; економія витрат за рахунок вибору SOC на аутсорсингу; масштабованість керованого центру безпеки.

До недоліків зовнішнього SOC відносять: підвищення ризиків безпеці даних і систем внаслідок передачі журналів безпеки третім особам; недостатня

кастомізація послуг керованого SOC, труднощі управління та контролю SOC з боку компанії-замовника; використання стандартних інструментів у рамках керованого SOC, що не завжди відповідає потребам конкретної організації.

За підсумками роботи запропоновано рекомендації щодо впровадження центру безпеки для різних організацій. Встановлено, що впровадження внутрішнього SOC підходить потужним компаніям, які потребують повного контролю над своїми процесами і продуктивністю послуг безпеки з огляду на зберігання й обробку великої кількості конфіденційної інформації.

Натомість, користування послугами аутсорсингового SOC є прийнятним варіантом для компаній з набагато меншими бюджетами і потребою отримати швидкий доступ до професійних послуг безпеки. Використовуючи керований SOC, організації не потрібно турбуватися про залучення кваліфікованого персоналу з безпеки, оренду приміщень, впровадження технологій, технічне обслуговування й будь-які інші витрати, пов’язані з управлінням SOC.

ВИСНОВКИ

Встановлено, що кібербезпека - це широка галузь, яка охоплює кілька напрямів, зокрема безпека інформації, операцій, програм, мереж, кінцевих точок і планування відновлення після інцидентів. Основними загрозами кібербезпеці є атаки програм-вимагачів, уразливості Інтернету речей (IoT), соціальна інженерія та фішингові атаки, атаки на ланцюжок поставок, кіберзагрози із застосуванням штучного інтелекту, розширені постійні загрози (APT), експлойти нульового дня, загрози хмарній безпеці й мобільним пристроям, шкідливе ПЗ, внутрішні загрози, загрози, пов'язані з криптовалютою тощо.

Оскільки складність і масштаби кіберзагроз зростають, а корпоративні ІКС стають все більш розмежованими, організації стикаються з потребою у реалізації комплексних рішень кібербезпеки, одним із яких є центр безпеки (SOC), який відповідає за оперативний моніторинг IT-середовища й запобігання інцидентам кібербезпеки і поєднує технології SIEM, UEBA, EDR, NTA та інші.

З'ясовано, що функції SOC включають активний моніторинг IT-середовища та збір даних про інциденти; аналіз підозрілих подій; реагування на загрози; розслідування інцидентів й відновлення після них; ведення реєстру ресурсів; управління відповідністю. Повноваження фахівців SOC розділяють на три основні рівні: спеціалісти 1 рівня, які відповідають за збір необроблених даних, а також за перегляд тривог і попереджень; спеціалісти 2 рівня, які опрацьовують більш критичні інциденти безпеки і проводять поглиблену оцінку за допомогою розвідки загроз; спеціалісти 3 рівня, які займаються серйозними інцидентами, а також завчасним виявленням можливих загроз і невідомих вразливостей.

Дослідження показало, що процес побудови SOC є послідовним і комплексним процесом, який складається з етапів розробки стратегії центру; створення індивідуального рішення SOC; розробка процесу, процедури і навчання; підготовка середовища; реалізація рішення; розгортання наскрізних сценаріїв використання; підтримка і розвиток індивідуального рішення SOC.

З’ясовано, що створення центру безпеки є актуальним завданням майже кожної сучасної компанії. Однак критично важливим є зробити вірний вибір між розбудовою внутрішнього SOC і передавання послуг безпеки на управління постачальником. Для прийняття оптимального рішення організація має врахувати такі основні чинники: вартість реалізації кожного з варіантів; наявність необхідних навичок у фахівців організації; перспективи масштабування центру безпеки; потреба у дотриманні нормативних і галузевих вимог; час на впровадження SOC; рівень стійкості компанії до ризиків.

Дослідження показало, що вибір варіанту передавання функцій центру безпеки на аутсорсинг має багато переваг для організації-замовника, зокрема: наявність у постачальника обладнання і кваліфікованих фахівців для виконання функцій SOC; ефективна взаємодія аутсорсингового SOC із компанією-замовником; забезпечення моніторингу безпеки й реагування 24/7; економія витрат за рахунок вибору SOC на аутсорсингу; масштабованість керованого центру.

До недоліків зовнішнього SOC відносять: підвищення ризиків безпеці даних і систем внаслідок передачі журналів безпеки третім особам; недостатня кастомізація послуг керованого SOC, труднощі управління та контролю SOC з боку компанії-замовника; використання стандартних інструментів у рамках керованого SOC, що не завжди відповідає потребам конкретної організації.

За підсумками роботи запропоновано рекомендації щодо впровадження центру безпеки для різних організацій. Встановлено, що впровадження внутрішнього SOC підходить потужним компаніям, які потребують повного контролю над своїми процесами і продуктивністю послуг безпеки з огляду на зберігання й обробку великої кількості конфіденційної інформації.

Натомість, користування послугами аутсорсингового SOC є прийнятним варіантом для компаній з набагато меншими бюджетами і потребою отримати швидкий доступ до професійних послуг безпеки. Використовуючи керований SOC, організації не потрібно турбуватися про залучення кваліфікованого персоналу з безпеки, оренду приміщень, впровадження технологій, технічне обслуговування й будь-які інші витрати, пов’язані з управлінням SOC.

СПИСОК ПОСИЛАНЬ

1. 7 Types of Cyber Security Threats. URL: https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/
2. AI in Cyber Security: Pros and Cons. URL: https://terranovasecurity.com/blog/ai-in-cyber-security/
3. An Ultimate Guide to Cyber Security for Beginners. URL: https://www.simplilearn.com/tutorials/cyber-security-tutorial/cyber-security-for-beginners
4. Artificial Intelligence (AI) Cybersecurity. URL: https://www.ibm.com/ai-cybersecurity
5. Building Your Own SOC or Opting for Managed SOC Services: A Guide to Making the Right Decision. URL: https://www.linkedin.com/pulse/building-your-own-soc-opting-managed-services-guide-making-kwulc
6. Comparative Study of Ontologies Based ISO 27000 Series Security Standards. URL: https://www.sciencedirect.com/science/article/pii/S187705091931662X
7. Cryptography and its Types. URL: https://www.geeksforgeeks.org/cryptography-and-its-types/
8. Cryptography. URL: https://www.synopsys.com/glossary/what-is-cryptography.html
9. Cyber Attack. URL: https://www.imperva.com/learn/application-security/cyber-attack/
10. Cyber Risks to Financial Stability. URL: https://www.lawfaremedia.org/article/cyber-risks-financial-stability
11. Cyber security failure one of biggest risks facing countries and businesses, warns WEF. URL: https://www.computerweekly.com/news/252511811/Cyber-security-failure-one-of-biggest-risks-facing-countries-and-businesses-warns-WEF
12. Cybersecurity Best Practices. URL: https://www.cisa.gov/topics/cybersecurity-best-practices
13. IDS vs. IPS: Definitions, Comparisons & Why You Need Both | Okta. URL: https://www.okta.com/identity-101/ids-vs-ips/

14. ISO 27000 Family of Standards. URL: https://isocertificationexperts.com.au/iso-27000-family-of-standards/

15. How SOC Teams Can Master Collaboration Security with Both Efficiency and Risk Management. URL: https://technative.io/soc-teams-collaboration-security/

16. MDR vs MSSP: defining both solutions and uncovering key differences. URL: https://www.crowdstrike.com/cybersecurity-101/mdr-vs-mssp/

17. Necessary skills among SOC roles. URL: https://www.researchgate.net/figure/Necessary-skills-among-SOC-roles-54-66-75-100-101_fig3_347520429

18. Online RSA Encryption, Decryption and Key Generator Tool. URL: https://www.devglan.com/online-tools/rsa-encryption-decryption

19. OWASP Top Ten. URL: https://owasp.org/www-project-top-ten/

20. Risk, Threat, or Vulnerability? How to Tell the Difference. URL: https://www.kennasecurity.com/blog/risk-vs-threat-vs-vulnerability/

21. Security Operation Centers. Outsourced Or Internal? Which Is Better? URL: https://www.clearnetwork.com/outsourced-soc-vs-internal-soc/

22. SHA-256 Cryptographic Hash Algorithm. URL: https://www.movable-type.co.uk/scripts/sha256.html

23. Simon Lipscombe. In house vs outsourced SOC. What should you choose. URL: https://wizardcyber.com/in-house-vs-outsourced-soc-what-should-you-choose/

24. SOC: що це таке і навіщо воно потрібне? URL: https://indevlab.com/uk/blog-ua/soc-scho-tse-take-%D1%96-nav%D1%96scho-vono-potr%D1%96bne/

25. SOC-as-a-Service Provider. URL: https://underdefense.com/services/soc/

26. SOC-as-a-Service. URL: https://www.ontinue.com/soc-as-a-service/

27. SOC-звіти – нові інструменти підтвердження якості процесів у компаніях | «Делойт» в Україні. URL: https://www2.deloitte.com/ua/uk/pages/press-room/press-release/2019/soc-reports.html

28. The AI and Cybersecurity Handbook – Past the hype and onto the ROI. URL: https://www.freecodecamp.org/news/ai-and-cybersecurity-handbook/

29. The Definition of SOC-cess? SANS 2018 Security Operations Center Survey. URL: https://www.sans.org/reading-room/whitepapers/analyst/definition-soc-cess-2018- security-operations-center-survey-38570

30. Top cybersecurity threats. URL: https://www.sprintzeal.com/blog/top-cybersecurity-threats

31. Using Artificial Intelligence in Cybersecurity. URL: https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

32. What are the series of ISO 27000 standards? URL: https://bestpractice.biz/what-are-the-series-of-iso-27000-standards/

33. What is a Security Operations Center (SOC)? URL: https://www.opentext.com/what-is/security-operations-center

34. What is a Security Operations Center (SOC)? URL: https://www.trellix.com/en-us/security-awareness/operations/what-is-soc.html

35. What is an Outsourced SOC? Everything you need to know before outsourcing your Security Operations Center. URL: https://www.ngnetserv.com/what-is-outsourced-soc/

36. What is Cryptography? How algorithms keep information secret and safe. URL: https://www.csoonline.com/article/3583976/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html

37. What is Cyber Attack? URL: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/

38. What is Cyber Security? Definition & Best Practices. URL: https://www.itgovernance.co.uk/what-is-cybersecurity

39. What is cybersecurity. URL: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/

40. What is Cybersecurity? URL: https://www.comptia.org/content/articles/what-is-cybersecurity

41. What is Cybersecurity?. URL: https://www.ibm.com/id-en/topics/cybersecurity

42. What is Data Loss Prevention (DLP)? A Definition of Data Loss Prevention. URL: https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

43. What is IDS and IPS? URL: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

44. What is Security Operation Center – Javatpoint. URL: https://www.javatpoint.com/ what-is-security-operation-center

45. What is SIEM. URL: https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

46. What is SIEM? URL: https://www.imperva.com/learn/application-security/siem/

47. What is SOC as a Service (SOCaaS)? Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/soc-as-a-service

48. What is the OWASP Top 10 and how does it work? URL: https://www.synopsys.com/ glossary/what-is-owasp-top-10.html

49. What is User and Entity Behavior Analytics? A Definition of UEBA, benefits, how it works, and more. URL: https://www.digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more

50. What is EDR? URL: https://www.openedr.com/blog/what-is-edr/

51. What is Network Traffic Analysis (NTA). URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-network-traffic-analysis-nta/

52. Why is cybersecurity important? URL: https://www.upguard.com/blog/cybersecurity-important

53. ISO/IEC 27001:2022 Preview. URL: https://cdn.standards.iteh.ai/samples/82875/726bcf58250e43d9a666b4d929c8fbdb/ISO-IEC-27001-2022.pdf

54. ISO/IEC 27035-1:2023. Information technology. Information security incident management. Part 1: Principles and process. URL: https://www.iso.org/standard/78973.html

55. 7 Steps to Building A Security Operations Center (SOC). URL: https://logrhythm.com/blog/7-steps-to-build-your-security-operations-center/

56. Все що ви хотіли дізнатися про XDR. URL: https://habr.com/en/post/551128/

57. Заплотинський Б.А. Основи інформаційної безпеки. URL: http://surl.li/dbndh

58. Захист від витоку інформації. URL: http://integritysys.com.ua/security/dlp/

59. Качан О. І., Інформаційна безпека підприємства в умовах глобалізації. URL: https://conf.ztu.edu.ua/wp-content/uploads/2017/09/234.pdf

60. Основні терміни та поняття у сфері інформаційної безпеки. URL: https://www.znanius.com/3849.html

61. Поняття інформації. URL: https://step.org.ua/konspekt/info/tema1

62. Програмні засоби захисту. URL: https://studfile.net/preview/6012701/page:42/