Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та кібербезпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

СИСТЕМА ОПЕРАТИВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ НА ФІРМІ

CYBER SECURITY OPERATIONAL MANAGEMENT SYSTEM AT THE COMPANY

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Шворак Максим Станіславович

(підпис)

Керівник:
к.т.н., доцент
Бортник Катерина Яківна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« _____ » червня 2023 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2023 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та кібербезпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ проф. Н.Чернящук
«_____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Швораку Максиму Станіславовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Система оперативного управління кібербезпекою на фірмі*

Керівник роботи *Бортник Катерина Яківна, к.т.н., доцент*

затверджені наказом закладу вищої освіти від «28» грудня 2022 року № 982/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 01.06.2023р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Архітектура і функції SOC
Рекомендації для підприємства при побудові SOC
Порівняльна система управління інформаційною безпекою
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Існуючі рішення
Використані технології
Архітектура системи
Інтерфейс системи
Схема роботи програмного продукту

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз проблеми за темою роботи та постановка завдань дослідження	*Бортник К.Я.*		
Теоретичне дослідження та практична реалізація	*Бортник К.Я.*		
Практична реалізація об'єкта проектування	*Бортник К.Я.*		
Висновки			

7. Дата видачі завдання 01.11.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Обгрунтування теми*	До 15.11.2022 р.	Виконано
2.	*Огляд літератури із досліджуваної проблеми*	До 15.12.2022 р.	Виконано
3.	*Розділ 1*	До 02.03.2023 р.	Виконано
4.	*Розділ 2*	До 02.03.2023 р.	Виконано
5.	*Висновки та пропозиції*	До 02.04.2023 р.	Виконано
6.	*Формування списку використаних джерел*	До 02.05.2023 р.	Виконано
7.	*Формування додатків*	До 15.05.2023 р.	Виконано
	Оформлення ілюстративного матеріалу	До 25.05.2023 р.	Виконано
	Нормоконтроль	До 01.06.2023 р.	Виконано
8.	*Інструментальна перевірка на академічний плагіат*	До 07.06.2023 р.	Виконано
9.	*Представлення кваліфікаційної роботи бакалавра до захисту*	До 02.03.2023 р.	Виконано

Здобувач вищої освіти _____ Шворак М.С.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Бортник К.Я.
(підпис) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 58 с., 7 табл., 11 рис., 15 джерел.

Об’єктом дослідження цієї дипломної роботи є процес розслідування інцидентів кібербезпеки в умовах функціонування сучасного підприємства.

Мета роботи полягає у проведенні аналізу існуючих моделей та методів побудови системи розслідування інцидентів кібербезпеки. На основі цього аналізу необхідно розробити комплексний процес розслідування різних типів інцидентів у структурі Центру Оперативного Управління Безпекою (Security Operation Center, SOC) підприємства.

В основній частині роботи досліджено ключові фактори, які визначають вибір моделі та архітектурних характеристик SOC. На основі цього аналізу розроблено практичні рекомендації щодо вибору оптимальної моделі Центру безпеки для конкретного підприємства.

Додатково було проведено порівняльний аналіз SIEM-продуктів [5], які пропонуються для корпоративного сегмента, з метою обґрунтування вибору найбільш ефективної системи для забезпечення функціонування SOC.

Практична цінність дослідження полягає у створенні розроблених деталізованих процесів розслідування різноманітних інцидентів. Результати цієї роботи можуть бути безпосередньо впроваджені на українських підприємствах для підвищення їхньої кіберстійкості.

Ключові слова: Security Operation Center, SOC, SIEM.

ABSTRACT

Explanatory note: 58 pages, 7 tables, 11 figures, 15 sources.

The object of this thesis is the process of investigating cybersecurity incidents in the context of a modern enterprise.

The purpose of the work is to analyze existing models and methods for building a cybersecurity incident investigation system. Based on this analysis, it is necessary to develop a comprehensive process for investigating various types of incidents within the structure of the enterprise's Security Operation Center (SOC).The main part of the thesis examines the key factors that determine the choice of SOC model and architectural characteristics.

Based on this analysis, practical recommendations have been developed for selecting the optimal security center model for a specific enterprise.

In addition, a comparative analysis of SIEM products [5] offered for the corporate segment was conducted to justify the choice of the most effective system for ensuring the functioning of the SOC.

The practical value of the research lies in the creation of detailed processes for investigating various incidents. The results of this work can be directly implemented in Ukrainian enterprises to increase their cyber resilience.

Keywords: Security Operation Center, SOC, SIEM.

ЗМІСТ

ВСТУП

З початком повномасштабної війни кібератаки на Україну суттєво зросли. Основні дані про статистику кібер-атак за 2023 рік надає Державна служба спеціального зв'язку та захисту інформації України та Служба безпеки України.

Загальна кількість зареєстрованих кіберінцидентів, даними Держспецзв'язку, у 2023 році зросла на 15,9% (до 2543 інцидентів), порівняно з 2022 роком. Інші джерела Держспецзв'язку також вказували на зростання на 62,5% у порівнянні з 2022 роком, але цифра 15,9% та 2543 інциденти була оприлюднена пізніше.

СБУ зафіксувала приблизно 4500 потужних кібератак у 2023 році, що на рівні 2022 року (з 1400 у 2021 році).

Цілеспрямовані атаки були переважно спрямовані на такі сектори:

– державні органи (міністерства та інші органи державної влади);

– критична інфраструктура (телекомунікаційний сектор, енергетичний сектор, фінансовий сектор (наприклад, DDoS-атаки на українські банки), оборонний сектор);

– інші (місцеві органи влади, ІТ, ПЗ та дані).

Переважна більшість кібератак і кіберінцидентів пов'язана зі спецслужбами та хакерськими угрупованнями Російської Федерації (наприклад, Sandworm, APT29 та інші).

Відзначається тренд на зростання активності нових хакерських угруповань.

Методи атак, які було зафіксовано за 2022-23 роки наступні: фішинг, програми-вимагачі, DDoS-атаки тощо.

Для їх виявлення застосовують різні перевірки.

Сканування мереж можна здійснювати ODS (сканування на вимогу) – функція, яка використовується в програмному забезпеченні для кібербезпеки. Вона дозволяє користувачеві або системі ініціювати повне або часткове сканування мережі або окремих комп'ютерних ресурсів. ODS запускається тоді,

коли це потрібно, наприклад, після отримання попередження про загрозу або перед важливим оновленням системи.

OAS – стандарт, який використовується для автоматичної валідації даних в API (інтерфейсах прикладного програмування).

Intrusion Detection Scan (IDS) – це діяльність або процес, який є складовою частиною роботи системи виявлення вторгнень. Це не окремий інструмент, а спосіб, яким система перевіряє мережевий трафік або файли на наявність ознак шкідливої активності або несанкціонованого доступу. IDS-сканування дозволяє здійснювати безперервний або періодичний моніторинг і аналіз даних з метою ідентифікації загроз.

Web Anti-Virus – це компонент або функція антивірусного програмного забезпечення, що застосовується для захисту комп’ютера або мережі від загроз, що походять з Інтернету (веб-сайтів, завантажень, електронної пошти та сценаріїв, що виконуються у браузері). Це перший рубіж оборони під час серфінгу в Інтернеті.

Botnet Activity Detection здійснює моніторинг у сфері кібербезпеки, спрямований на ідентифікацію пристроїв у мережі (комп’ютерів, серверів, IoT-пристроїв), які були скомпрометовані та контролюються зловмисниками як частина ботнету. Botnet Activity Detection (Виявлення активності ботнетів) — це критично важливий процес у сфері кібербезпеки, спрямований на ідентифікацію пристроїв у мережі (комп'ютерів, серверів, IoT-пристроїв), які були скомпрометовані та контролюються зловмисниками як частина ботнету. Виявлення активності ботнету переважно покладається на поведінковий аналіз мережевого трафіку, оскільки традиційні сигнатурні методи часто не можуть впоратися з унікальними та мінливими C2-протоколами.

Створення центру моніторингу та оперативного реагування на кібератаки (SOC) обумовлене необхідністю переходу від пасивного захисту до активної оборони та проактивного реагування в режимі реального часу.

Сучасні кібератаки, особливо автоматизовані, відбуваються значно швидше, ніж традиційні методи захисту можуть на них відреагувати. Ручні процеси виявлення та реагування занадто повільні. Центр моніторингу

використовує автоматизовані інструменти (SIEM, SOAR) для миттєвого виявлення та початкової нейтралізації загрози.

Сучасна корпоративна мережа генерує величезні обсяги журналів і мережевого трафіку. Жодна людина не здатна вручну проаналізувати мільярди подій на день. SOC використовує системи кореляції (SIEM), щоб відфільтрувати «шум» і виявити лише ті події, які дійсно вказують на інцидент.

Без централізованого центру моніторингу, захисні інструменти (антивіруси, фаєрволи, IDS) працюють ізольовано. Це створює «сліпі зони». SOC об’єднує дані з усіх цих інструментів, надаючи єдину, повну картину безпеки всієї інфраструктури.

Забезпечення комплексного підходу моніторингу і реагування на кіберзагрози здійснюється відповідними нормативними документами, які регулюють кібербезпеку: ISO IEC 27035, ISO IEC 27001 [7] тощо. Їх реалізація дозволяє організації створити комплексну, системну та ефективну систему управління інформаційною безпекою, що охоплює як проактивний захист, так і реактивне реагування на інциденти.

Мета роботи: провести аналіз моделей і методів організації розслідування інцидентів кібербезпеки на фірмі та розробити процеси розслідування різноманітних інцидентів у SOC.

З метою забезпечення кібербезпеки на фірмі з використанням SOC потрібно вирішити низку питань:

− провести аналіз архітектури та функцій SOC;

− проаналізувати чинники, які впливають на прийняття рішення;

− визначити шляхи реагування на виявлені інциденти;

− сформувати процедуру збору доказів.

РОЗДІЛ 1 АРХІТЕКТУРА І ФУНКЦІЙ SOC

1.1 Реалізації SOC

Створення центру операційної безпеки (Security Operations Center, SOC) – це не просто купівля програмного забезпечення; це перетворення культури та процесів фірми. Це як побудова надійного командного центру, де висококваліфіковані фахівці цілодобово стежать за периметром і готові блискавично реагувати на будь-яку кіберзагрозу. Шлях реалізації SOC можна уявити як подорож, що проходить через три основні етапи: підготовка, будівництво та експлуатація.

На етапі підготовки здійснюється визначення місії та основи безпеки. Потрібно визначитися з тим, що потрібно захищати і від чого.

Спочатку потрібно чітко визначити обсяг і місію SOC. Необхідно проаналізувати критичні бізнес-активи (сервери, дані клієнтів, інтелектуальну власність) та оцінити пов’язані з ними ризики. SOC має будуватися навколо захисту саме цих активів. Слід сформулювати модель зрілості, тобто зрозуміти, чи буде це «SOC рівня 1» (лише базовий моніторинг) чи «SOC рівня 3» (проактивний пошук загроз, інтеграція зі штучним інтелектом).

Далі йде організаційний дизайн. Тут вирішується, яким буде SOC за своєю природою: внутрішній (повністю свій), аутсорсинговий (керований стороннім постачальником, так званий MSSP), чи гібридний. Внутрішній SOC дає повний контроль, але вимагає значних інвестицій у найм і навчання високооплачуваних аналітиків, яких важко знайти. Аутсорсинг швидше запускається і є економічно вигіднішим для невеликих фірм, але передбачає передачу частини контролю.

Після вибору моделі починається формування фундаменту даних – потрібно інвентаризувати мережу та IT-інфраструктуру, визначити джерела журналів подій, які будуть збиратися для аналізу.

На етапі будівництва перетворюються плани на дію, оснащуючи центр операційної безпеки «очима» та «руками».

Центральною технологією тут є SIEM-система (Security Information and Event Management), яка слугує мозком SOC. Вона збирає мільйони логів з усіх куточків мережі (сервери, фаєрволи, робочі станції) і використовує складні алгоритми для кореляції подій – виявлення аномальних послідовностей, які вказують на кібератаку, що розвивається. Наприклад, вхід у систему о третій ночі з незвичної країни з подальшим копіюванням великого обсягу даних.

Паралельно розробляються операційні процеси. Це «інструкції з виживання» для аналітиків. Ключові серед них: процес управління інцидентами та процес управління вразливостями.

Процес управління інцидентами – чіткий, покроковий план, що робити, коли SIEM спрацював (хто реагує, як ізолюється заражений комп'ютер, як документується інцидент). Це вимагає розробки так званих плейбуків – готових сценаріїв дій для типових загроз.

Процес управління вразливостями – регулярне сканування IT-активів, оцінка ризиків виявлених «дірок» і пріоритизація їхнього усунення, щоб SOC знав, де ймовірне буде втручання.

Останнім часом набуває поширення впровадження SOAR-систем (Security Orchestration, Automation and Response), які є автоматизованими «руками» SOC. SOAR дозволяє автоматично запускати плейбуки. Наприклад, якщо виявлено вірус-шифрувальник, SOAR може автоматично заблокувати користувача у мережі та створити запит на антивірусну перевірку, звільняючи аналітика для складнішої роботи.

На етапі експлуатації відбувається навчання та постійне вдосконалення SOC. Це означає, що навіть ідеально побудований SOC швидко може застаріти, якщо його не підтримувати і не розвивати. Цей етап – це безперервний цикл вдосконалення.

Персонал є найціннішим активом SOC. Необхідно інвестувати у постійне навчання аналітиків, оскільки кіберзагрози еволюціонують щодня. Вони повинні брати участь у симуляціях реальних атак, щоб відточувати навички реагування в умовах стресу.

Крім того, справжній SOC переходить від пасивного реагування до проактивного пошуку загроз. Це означає, що аналітики не просто чекають, поки SIEM подасть сигнал, а активно, на основі новітніх даних про загрози, шукають ознаки компрометації, які ще не були виявлені автоматизованими засобами.

Регулярне переоцінювання ефективності є важливим. Керівництво SOC повинно постійно вимірювати ключові показники, такі як MTTD (Mean Time To Detect – середній час виявлення) та MTTR (Mean Time To Respond – середній час реагування). Чим менші ці показники, тим ефективніший SOC. На основі цих метрик проводяться коригувальні дії для оптимізації процесів та налаштування інструментів, забезпечуючи, що SOC залишається гнучким і надійним щитом проти кіберзлочинності.

Успішний SOC функціонує як злагоджений оркестр, де кожен фахівець має свою унікальну партію. Ефективність SOC залежить від чіткого розмежування обов'язків та тісної співпраці між рівнями.

Зазвичай, персонал SOC поділяється на три ключові рівні (Tier), а також керівну та інженерну ланки.

Операційний персонал це аналітики (Tiers 1, 2, 3).

Це своєрідна «передова» SOC, яка безпосередньо взаємодіє із загрозами. Їхня робота вимагає високої концентрації, швидкості реакції та постійного навчання.

Аналітик SOC прешого рівня займається моніторингом. Його обов'язок полягає у моніторингу SIEM-системи та інших засобів безпеки. Він приймає та сортує попередження, відфільтровуючи хибні спрацювання від справжніх загроз. Його завдання – швидко провести початкову верифікацію інциденту, зібрати базові дані (IP-адреси, час, тип атаки) і, якщо інцидент підтверджено, передати його на вищий рівень.

Аналітики цього рівня повинні мати знання основ мережевих протоколів, вміння працювати з інтерфейсом SIEM, уважність і дотримання процедур.

Аналітики SOC другого рівня займається обробкою інцендентів. Вони отримують підтверджені тривоги від аналітика першого рівня шляхом глибокого дослідження інцидентів та керування процесом реагування.

Вони використовують спеціалізовані інструменти (наприклад, системи для аналізу мережевого трафіку або кінцевих точок) для повного розуміння масштабу компрометації. Вони локалізують загрозу, розробляють та впроваджують заходи щодо її усунення та відновлення систем. Вони також створюють детальні звіти про інцидент.

Аналітики SOC другого рівня повинні мати поглиблене розуміння операційних систем, мережевої архітектури, знання криміналістичного аналізу та вміння писати запити для SIEM.

Аналітик SOC третього рівня це експерт, основний обов'язок якого – розробка нових методів виявлення, проактивний пошук прихованих загроз та оптимізація інструментів. Він не чекає на алерти. На основі Threat Intelligence (даних про нові тактики зловмисників) вони активно шукають ознаки компрометації, які «проскочили» автоматичні системи. Вони створюють нові кореляційні правила для SIEM, пишуть автоматизовані сценарії для SOAR та надають експертну підтримку аналітикам другого рівня у найскладніших випадках.

Аналітик цього рівня повинен мати глибоке знання тактик, технік та процедур зловмисників, програмування, реверс-інжиніринг шкідливого програмного забезпечення та досвід пентесту (Penetration Testing).

Керівна та підтримуюча ланка забезпечують стратегічний розвиток та безперебійну роботу технічної інфраструктури SOC.

Менеджер SOC – лідер команди та зв'язкова ланка між SOC та вищим керівництвом фірми. Його обов'язок пов'язаний зі стратегічним плануванням, управлінням бюджетом, персоналом та забезпечення відповідності SOC бізнес-цілям.

Він встановлює KPI для команди (MTTD, MTTR), звітує про рівень кіберризику, керує інцидентами високої критичності, забезпечує безперервне навчання команди та розвиток інструментарію.

У сою чергу, інженер безпеки – це будівельник та наладчик технічної інфраструктури SOC. Його основний обов'язок полягає у проектуванні, розгортанні та обслуговуванні всіх технологій безпеки.

Інженер безпеки відповідає за встановлення та налаштування SIEM, SOAR, IDS/IPS, забезпечують якісний збір логів з усіх джерел, оптимізують продуктивність систем та впроваджують нові інструменти. Він є технічною основою, що дозволяє аналітикам виконувати свою роботу.

Аналітик Threat Intelligence збирає та інтерпретує зовнішні дані про загрози на практичні дії. Він моніторить форуми зловмисників, державні та комерційні звіти про кібератаки, виявляють нові «індикатори компрометації» (IoC) та інтегрують ці дані в SIEM, щоб захисні механізми фірми були готові до атак, які ще не відбулися.

Комплексне поєднання навичок – від рутинного моніторингу до глибокого хакерського мислення та стратегічного управління робить SOC динамічним і життєздатним інструментом у боротьбі з кіберзагрозами.

1.2 Основні задачі SOC

Корпоративний захист інформації має бути комплексним і охоплювати не лише технології, але й людей та процеси. Ці вимоги ґрунтуються на трьох стовпах інформаційної безпеки: конфіденційність, цілісність та доступність.

Мережева та периметрова безпека зосереджені на захисті меж корпоративної мережі та її внутрішніх сегментів. Фаєрволи та системи виявлення/запобігання вторгнень (IDS/IPS) здійснюють фільтрацію вхідного та вихідного трафіку, блокування несанкціонованих з’єднань і проактивне виявлення та запобігання відомим атакам. Сегментація мережі відповідає за розділення мережі на ізольовані зони (наприклад, зона для серверів, зона для розробників, гостьова мережа). Це запобігає поширенню атаки у разі компрометації одного сегмента. Захист віддаленого доступу (VPN/SLA) передбачає використання захищених каналів (VPN) та суворих правил контролю доступу для працівників, що працюють віддалено.

Захист кінцевих точок та пристроїв висуває вимоги до захисту комп’ютерів, ноутбуків та мобільних пристроїв, які є найчастішою точкою входу для кіберзлочинців. Антивірусне ПЗ та EDR-системи дають сучасні рішення, що

не лише виявляють відоме шкідливе ПЗ, але й контролюють поведінку (EDR – Endpoint Detection and Response) для виявлення атак нульового дня та складних загроз. Управління патчами здійснює впровадження систематичного та швидкого процесу встановлення оновлень безпеки на всі операційні системи та прикладне ПЗ для усунення вразливостей. Контроль пристроїв та носіїв інформації накладає заборону або суворий контроль підключення неавторизованих зовнішніх пристроїв (наприклад, USB-накопичувачів).

Управління доступом та ідентифікацією відповідає за контроль – хто має доступ до яких ресурсів і як він його отримує. Принцип мінімальних привілеїв реалізує надання користувачам та системам лише тих прав доступу, які абсолютно необхідні для виконання їхніх функціональних обов'язків. Багатофакторна автентифікація передбачає обов'язкове використання двох або більше факторів для підтвердження особи для доступу до критичних систем, а централізоване управління доступом – використання єдиних систем для управління обліковими записами, що спрощує моніторинг та швидке блокування облікового запису.

Управління ризиками та безперервність описують вимоги, що стосуються стратегічного підходу до безпеки та забезпечення функціонування бізнесу. Це передбачає оцінку ризиків та аудити шляхом регулярного проведення аналізу вразливостей та оцінки ризиків для визначення найважливіших активів та загроз.

Планування безперервності бізнесу та аварійного відновлення передбачає розробку та тестування планів дій для швидкого відновлення критичних бізнес-функцій після інциденту. Сама політика резервного копіювання забезпечує регулярне, перевірене та ізольоване резервне копіювання даних.

Основні процеси SOC наступні.

Робота SOC – це безперервний, циклічний процес, який можна описати як чотирифазний життєвий цикл управління загрозами: моніторинг і виявлення, реагування та усунення, аналіз і вдосконалення, а також проактивна безпека. Це не просто послідовність кроків, а цілісний механізм, що забезпечує стійкість фірми.

Моніторинг та виявлення є фундаментом, на якому будується вся діяльність SOC. Він починається з безперервного збору інформації, що надходить з усіх куточків корпоративної мережі. SOC агрегує мільярди подій із серверів, мережевого обладнання, фаєрволів та кінцевих точок за допомогою SIEM-системи. Тут відбувається кореляція подій – аналітики та автоматизовані системи шукають взаємозв'язки між, здавалося б, непов'язаними подіями, які разом можуть свідчити про кібератаку. Наприклад, невдала спроба входу вночі, за якою слідує успішне підключення до нетипового сервера.

Після спрацювання попередження відбувається сортування. Аналітики першого рівня швидко оцінюють критичність події та визначають, чи є вона хибним спрацюванням чи справжнім інцидентом. Це вимагає швидкого прийняття рішень, оскільки час є критичним для запобігання збиткам.

Коли інцидент підтверджено, SOC переходить до фази активної протидії. Це найдраматичніший етап, де важлива кожна секунда. Процес починається з локалізації, тобто швидкої ізоляції скомпрометованої системи, щоб запобігти поширенню загрози на інші частини мережі. Далі йде розслідування, під час якого аналітики другого рівня проводять аналіз, щоб зрозуміти повний обсяг вторгнення – як зловмисник потрапив всередину, що він робив і які дані були скомпрометовані.

Кульмінацією є усунення загрози – видалення шкідливого програмного забезпечення, виправлення використаної вразливості та блокування облікових записів, які могли бути скомпрометовані. Фінальний крок – відновлення, коли системи повертаються до нормальної роботи, але вже з посиленими заходами безпеки.

Після усунення інциденту робота не закінчується. Ця фаза перетворює негативний досвід на позитивний урок. Проводиться постійний аналіз причинно-наслідкових зв'язків: чому система захисту не спрацювала вчасно? Це призводить до перегляду та оновлення правил кореляції в SIEM, а також до вдосконалення плейбуків (сценаріїв реагування).

Керівництво SOC аналізує ключові показники ефективності, зокрема MTTD та MTTR, щоб виявити «вузькі місця» у процесах. На основі цього аналізу

приймаються рішення щодо оптимізації технологій та додаткового навчання персоналу.

Моніторинг інформаційної безпеки – це безперервний, життєво важливий процес, який можна порівняти із системою спостереження на стратегічно важливому об'єкті. Його головна місія полягає в забезпеченні того, щоб ніщо небезпечне не пройшло непоміченим. Це не просто збір даних, а інтелектуальна діяльність із постійного збору, агрегації, аналізу та аудиту інформації, що надходить з усієї корпоративної IT-інфраструктури, з метою виявлення та попередження кіберзагроз у режимі реального часу.

Основною метою моніторингу є забезпечення ранньої видимості компрометації. У сучасних умовах атаки розвиваються блискавично, і можливість виявити підозрілу активність на її початковому етапі – це вирішальний фактор, що визначає, чи закінчиться інцидент невеликим збоєм, чи катастрофічним витоком даних. Якісний моніторинг безпосередньо впливає на MTTD, прагнучи звести його до мінімуму. Таким чином, моніторинг забезпечує оперативну підтримку тріади конфіденційності, цілісності та доступності інформації.

Система аудиту дій користувачів виконує завдання, що є важливими для забезпечення підзвітності, прозорості та цілісності функціонування корпоративного середовища. Її можна розглядати як інформаційну пам’ять організації, яка ретельно фіксує кожну взаємодію людини з інформаційними ресурсами.

Рішення Qualys Scanner є ключовим компонентом потужної хмарної платформи безпеки Qualys (Qualys Security Cloud Platform). Це високоточний, масштабований інструмент для безперервного виявлення та оцінки вразливостей в IT-інфраструктурі будь-якої складності.

Основна ідея Qualys полягає в тому, що сканування безпеки повинно бути постійним процесом, а не лише періодичною перевіркою, і це досягається завдяки хмарній архітектурі.

Основні модулі та види сканування Qualys Scanner:

– Vulnerability Management, Detection and Response (VMDR) (основний інструмент, який використовує сканери для постійного виявлення вразливостей та помилок конфігурації на всіх IT-активах);

– Web Application Scanning (WAS) (спеціалізований сканер для динамічного аналізу безпеки вебдодатків, який автоматизовано сканує вебсайти та API для виявлення вразливостей із переліку OWASP Top 10);

– CyberSecurity Asset Management (CSAM) (дозволяє сканеру шукати вразливості й автоматично інвентаризувати усі IT-активи в гібридному середовищі, надаючи єдине, актуальне уявлення про всю атакуючу поверхню).

Інше рішення – Symantec Data Loss Prevention (DLP), тепер частина Broadcom, це комплексне програмне рішення, призначене для запобігання витоку конфіденційної інформації за межі корпоративного периметра. Воно забезпечує видимість, моніторинг та контроль за даними, незалежно від їхнього стану: у спокої (Data-at-Rest), у русі (Data-in-Motion) та у використанні (Data-in-Use).

Symantec DLP використовує уніфіковану платформу (DLP Enforce Platform) для керування політиками у всьому середовищі фірми. Він допомагає фірмам захистити інтелектуальну власність, зменшити фінансові ризики та підтримувати репутацію, мінімізуючи як зловмисні, так і випадкові витоки даних.

Автоматизація реакції на інциденти кібербезпеки підвищує ефективність сучасного SOC. Цей процес відомий як SOAR і являє собою перехід від ручного, повільного реагування до миттєвого, стандартизованого та масштабованого.

Автоматизація звільняє висококваліфікованих аналітиків SOC від рутинних і повторюваних завдань, що підвищує загальну продуктивність команди, та забезпечує послідовність у застосуванні захисних заходів, що є важливим для управління та відповідності нормативним вимогам.

Повідомлення також надходять із зовнішніх джерел через API або сповіщення електронною поштою. Головне, щоб вони працювали за певними правилами, заснованими, наприклад, на регулярних виразах або тегах.

1.3 Аналіз моделей SOC

Основні моделі організації та функціонування Центру оперативного реагування SOC визначають, хто саме керує центром, де він розташований і який обсяг функцій він виконує.

Існує чотири ключові моделі SOC: внутрішня, аутсорсингова, гібридна і віртуальна.

Внутрішній SOC являє собою найбільш традиційну модель, де центр безпеки повністю належить та управляється самою організацією. Усі фахівці (аналітики, інженери, архітектори) є штатними співробітниками компанії, а вся інфраструктура (SIEM, SOAR, обладнання) розташована на об’єктах компанії.

До переваг цієї моделі належить: повний контроль над даними та процесами; глибоке знання внутрішньої мережі та бізнес-процесів; швидка інтеграція з внутрішніми командами (IT, розробка). До недоліків – високі витрати на створення та підтримку, складнощі з наймом та утриманням висококваліфікованого персоналу.

Дана модель SOC підходить великим корпораціям, фінансовим установам, державному сектору та об’єктам критичної інфраструктури, де конфіденційність даних є найвищим пріоритетом.

У аутсорсинговій моделі SOC організація повністю або частково передає функції моніторингу та реагування зовнішньому постачальнику послуг. Послуги надає Managed Security Service Provider (MSSP). MSSP відповідає за інструменти, персонал та цілодобовий моніторинг інфраструктури клієнта.

До переваг аутсорсинговій моделі SOC належить нижчі початкові витрати (немає потреби купувати дороге обладнання), доступ до висококваліфікованих експертів 24/7, швидке розгортання та масштабованість. З точки зору недоліку можна відзначити – менший контроль над даними та процесами, потрібна висока довіра до MSSP, може бути складніше узгодити реакцію з внутрішніми бізнес-процесами.

Ця модель підходить до малого та середнього бізнесу, компаній, які не мають ресурсів для створення власного цілодобового центру.

Модель гібридного SOC поєднує елементи внутрішнього та аутсорсингового підходів. Тут такі функції як управління вразливостями, реагування на високорівневі інциденти залишаються всередині компанії, а рутинні функції, такі як моніторинг 24/7 та управління SIEM, передаються зовнішньому MSSP.

У даній моделі забезпечується оптимальний розподіл ресурсів, компанія зберігає контроль над найбільш чутливими даними та процесами, а MSSP бере на себе навантаження рутинних задач, але виникають складнощі у визначенні чітких зон відповідальності між внутрішньою командою та MSSP.

Ця модель підходить великим компаніям, які прагнуть оптимізувати витрати, але зберегти внутрішній контроль над ключовими компетенціями.

Віртуальний SOC ця модель характеризується відсутністю фізичного, єдиного центру. У цьому випадку персонал може бути розподілений географічно віддалено, але використовує єдину хмарну або програмну платформу (SIEM, SOAR) для збору та аналізу даних. Часто це повністю або майже повністю аутсорсинг, але з акцентом на хмарних технологіях.

Даній моделі властиві низькі операційні витрати на інфраструктуру, гнучкість у наймі фахівців з усього світу, висока доступність та масштабованість. Зрозуміло, що ця модель залежить від хмарних провайдерів і якості інтернет-з'єднання та підходить компаніям, що працюють повністю або переважно у хмарі.

Порівняння місця розміщення технічного оснащення (серверів, систем SIEM/SOAR, фаєрволів, систем аналізу трафіку тощо) між основними моделями SOC є фактором, що впливає на витрати, контроль та безпеку.

Порівняльна характеристика, що відображає місце розміщення технічного оснащення для кожної моделі подано у таблиці 1.1:

Кількість та оптимальний склад персоналу Центру оперативного реагування (SOC) залежать від розміру та складності інфраструктури, рівня ризику компанії (це фінансовий сектор чи критична інфраструктура) та обраної моделі SOC.

Оптимальна команда має забезпечувати цілодобовий моніторинг (24/7/365), оскільки кібератаки не мають робочого графіку.

Таблиця 1.1 – Порівняння місця розміщення технічного оснащення основних моделей SOC

Модель SOC	Місце розміщення технічного оснащення	Власник та оператор оснащення	Ключовий фактор безпеки
Внутрішній SOC	Фізично на об'єктах організації (власний дата-центр або серверна)	Організація-власник	Фізичний контроль доступу та інфраструктури
Аутсорсинговий SOC	На об'єктах MSSP (дата-центри постачальника послуг безпеки)	MSSP (Стороння організація)	Безпечний канал зв'язку (VPN) для передачі логів клієнта та надання доступу до консолі
Гібридний SOC	Розподілене: Критичне оснащення (SIEM, DLP) на об'єктах клієнта, а аналітичні інструменти або вторинні системи – на об'єктах MSSP (або у хмарі)	Спільна відповідальність (частина – клієнт, частина – MSSP)	Необхідність складної інтеграції та розмежування мереж
Віртуальний SOC	У хмарі на серверах хмарних провайдерів (AWS, Azure, Google Cloud)	Хмарний провайдер (фізичне обладнання) та організація/MSSP (програмне забезпечення)	Контроль доступу до хмарного середовища та правильність конфігурації хмарних сервісів

Як було зазначено вище, персонал SOC зазвичай поділяють на рівні (Tiers) за рівнем складності виконуваних завдань.

Для забезпечення повноцінного цілодобового покриття (24/7) та підтримки процесів потрібна певна мінімальна кількість людей (табл. 1.2).

Щоб забезпечити роботу 24/7, необхідно мати 4 повні зміни по 8 годин кожна (з урахуванням вихідних, відпусток та лікарняних).

Мінімальна команда (для малої/середньої компанії): кількість на зміну 1xTier1+1xTier2, а загальна мінімальна кількість:

(1+1)x4зміни+1xTier3+1xМенеджер=10 осіб.

Оптимальна команда (для великої компанії): кількість на зміну: 2xTier1+1xTier2, а загальна оптимальна кількість:

(2+1)x4 зміни +2xTier3 +1x Менеджер +1x Адміністратор SIEM = 16-20 осіб.

Ключовий чинник – це співвідношення аналітиків.

Оптимальне співвідношення між рівнями має бути приблизно 3:2:1 (Tier1 : Tier2 : Tier3). Це забезпечує, що рутинні завдання не перевантажують дорогих і висококваліфікованих фахівців.

Таблиця 1.2 – Ключові ролі та функціональний розподіл персоналу

Рівень (Tier)	Позиція	Основна відповідальність	Необхідна кількість
Tier 1	Аналітик реагування (Alert Analyst)	Первинний моніторинг. Фільтрує та триажує (сортує) автоматичні сповіщення від SIEM. Відкидає помилкові спрацьовування. Відповідає за швидкість виявлення.	Найбільша. Мінімум 3–4 особи для покриття 24/7.
Tier 2	Фахівець з реагування на інциденти (Incident Responder)	Поглиблений аналіз та ізоляція. Розслідує підтверджені інциденти, виконує форензику, визначає корінь проблеми, керує процесом реагування.	Середня. Мінімум 2–3 особи для покриття 24/7.
Tier 3	Мисливець за загрозами (Threat Hunter) / Старший інженер	Проактивна діяльність. Шукає приховані загрози, які оминули автоматичні системи. Розробляє нові правила виявлення для SIEM/IDS/EDR.	Найменша. 1–2 висококваліфіковані особи.
Керівництво	Менеджер SOC / CISO (Chief Information Security Officer)	Керує командою, визначає стратегію, бюджет, звітує вищому керівництву.	1 особа (повна або часткова зайнятість).

Стандарт COBIT (Control Objectives for Information and Related Technology) [16] є одним із провідних фреймворків у сфері управління IT та його невід'ємною частиною є модель зрілості (Maturity Model), яка дозволяє оцінити рівень розвитку та контролю кожного IT-процесу в організації.

Модель зрілості COBIT (яка в нових версіях, зокрема COBIT 5 та COBIT 2019, базується на стандарті ISO/IEC 15504 SPICE та моделі CMMI) розрізняє шість рівнів зрілості (табл. 1.3).

Модель зрілості дозволяє організації:

– оцінити поточний стан (зрозуміти, наскільки ефективно кожен IT-процес виконується сьогодні);

– визначити прогалини (чітко побачити, які процеси є слабкими і потребують негайної уваги);

– скласти дорожню карту (на основі оцінки розробити план дій для підвищення рівня зрілості критичних процесів до бажаного рівня);

– виміряти прогрес (періодично проводити повторну оцінку для вимірювання успіху впроваджених поліпшень).

Таблиця 1.3 – Характеристика моделей зрілості COBIT

Рівень	Назва	Характеристика процесу
Рівень 0	Незавершений (Incomplete)	Процес або не впроваджений, або не досягає своєї мети. Доказів його виконання немає.
Рівень 1	Виконаний (Performed)	Процес виконується і досягає своєї мети, але він не формалізований, не добре визначений і є непередбачуваним (залежить від окремих осіб).
Рівень 2	Керований (Managed)	Процес планується, моніториться та коригується на рівні окремих проектів. Результати контролюються.
Рівень 3	Встановлений (Established)	Процес добре визначений, документований і стандартизований у межах організації. Використовуються єдині керівництва та процедури.
Рівень 4	Прогнозований/Кількісно керований (Predictable/Quantitatively Managed)	Процес контролюється та вимірюється за допомогою статистичних та кількісних методів. Він працює у визначених межах для досягнення цілей ефективності.
Рівень 5	Оптимізований (Optimizing)	Процес постійно вдосконалюється на основі кількісного розуміння його ефективності. Фокус на інноваціях та реакції на зміни.

Для ефективного та успішного створення власного Центру моніторингу та оперативного реагування (SOC) за методологією COBIT, організація має досягти мінімум Рівня 3 (Встановлений) зрілості IT-процесів. Це є оптимальною базою, оскільки він забезпечує необхідну стандартизацію та надійність для функціонування SOC.

Це означає, що всі ключові IT-процеси (включаючи управління інцидентами, управління вразливостями та управління конфігураціями) будуть формалізовані та документовані. У всій організації будуть використовуються єдині процедури та інструменти, а персонал буде навчений і дотримується цих стандартів.

В ідеалі потрібний Рівень 4 (Кількісно керований). Хоча SOC може успішно функціонувати на Рівні 3, прагнення до Рівня 4 дозволяє йому стати по-справжньому ефективним і проактивним. Це означає, що процеси безпеки будуть

вимірюватися за допомогою кількісних показників, а наявність якісних даних дозволить прогнозувати ризики та оптимізувати захист. У такому випадку SOC переходить до проактивного «полювання за загрозами», базуючись на статистичних даних та аналізі ефективності.

Таким чином, приведений аналіз основних типів архітектури SOC дозволить нам у подальшому обрати потрібну модель SOC і відповідне її забезпечення та сформувати рекомендації для її побудови [1] на фірмі.

РОЗДІЛ 2 РЕКОМЕНДАЦІЇ ДЛЯ ПІДПРИЄМСТВА ПРИ ПОБУДОВІ SOC

2.1 Аналіз факторів, що впливають на вибір рішення

Вибір архітектурного рішення – це завжди пошук балансу між потребами бізнесу, технологічними можливостями та наявними ресурсами. Розглянемо ключові фактори, що формують цей вибір.

Першочерговим і найбільш визначальним фактором є місія та сфера діяльності організації. SOC для великого фінансового конгломерату, що працює в режимі 24/7/365, матиме кардинально іншу архітектуру, ніж SOC для державного органу чи невеликої IT-компанії.

Якщо компанія оперує критично важливою інфраструктурою (енергетика, фінанси, телеком), архітектура має відповідати найвищим стандартам відмовостійкості, надмірності та географічної розподіленості. Необхідність дотримання жорстких регуляторних вимог (GDPR, ISO 27001, PCI DSS) також безпосередньо впливає на вимоги до зберігання, обробки та конфіденційності даних, що є основою архітектурного вибору.

Для деяких загроз, критична кожна секунда. Якщо пріоритетом є оперативне реагування (наприклад, зупинка DDoS-атаки чи ізоляція скомпрометованого хоста), архітектура повинна забезпечувати мінімальну затримку між виявленням події та активацією автоматичних або напівавтоматичних інструментів реагування (SOAR). Це часто вимагає розміщення певних компонентів ближче до кінцевих точок.

Прогноз на зростання об’ємів даних (логи, трафік) та кількості контрольованих об’єктів є вирішальним. Монолітна архітектура може бути швидкою для невеликого SOC, але вона швидко стане вузьким місцем. Мікросервісна або розподілена архітектура, хоч і є складнішою у впровадженні, надає безмежну горизонтальну масштабованість, дозволяючи додавати обчислювальні потужності чи сховища даних без зупинки всієї системи.

Архітектура SOC – це не лише програмне забезпечення, а складна екосистема, яка повинна гармонійно функціонувати з уже наявними технологіями.

SOC збирає дані з тисяч джерел: фаєрволів, EDR/XDR, хмарних сервісів, систем автентифікації. Архітектура повинна мати надійні, гнучкі та уніфіковані механізми прийому даних. Вибір на користь певної платформи SIEM або Data Lake залежить від того, наскільки легко вона інтегрується з цими різноманітними джерелами. Наприклад, якщо більшість інфраструктури в хмарі, архітектура повинна бути «cloud-native».

Якість виявлення загроз прямо залежить від можливостей обробки даних. Сучасний SOC вимагає не лише кореляції подій, а й Machine Learning (ML) для виявлення аномалій та поведінкового аналізу. Це вимагає потужних обчислювальних кластерів і, відповідно, архітектурних рішень, здатних підтримувати паралельні обчислення та роботу з великими обсягами «гарячих» та «холодних» даних.

Вибір між хмарою, приміщенням та гібридом – це фундаментальне архітектурне рішення. Хмарна архітектура (SaaS/PaaS-based SOC) пропонує швидке розгортання, майже необмежену масштабованість і менші операційні витрати на підтримку інфраструктури, але вимагає довіри до постачальника послуг. Локальна архітектура надає повний контроль над даними та інфраструктурою, що критично для деяких галузей, але вимагає значних капітальних інвестицій та постійного обслуговування. Гібридна модель намагається поєднати переваги обох.

Навіть ідеальна технологічна архітектура не буде успішною без урахування економічних та кадрових аспектів.

Початкові інвестиції в інфраструктуру (сервери, сховища, ліцензії) часто є меншою частиною загальних витрат. Архітектурне рішення має враховувати операційні витрати на підтримку, оновлення, електроенергію, а також вартість кваліфікованого персоналу. Складна, високоспеціалізована архітектура може вимагати дорожчих експертів.

Немає сенсу будувати SOC на базі мікросервісів та Kubernetes, якщо в команді немає спеціалістів з їх підтримки. Архітектура повинна бути реалістичною з точки зору доступності та рівня кваліфікації інженерів та аналітиків. Вибір на користь поширених та стандартизованих рішень (наприклад, відкритих фреймворків) може спростити набір персоналу та його навчання.

Складна архітектура, хоч і потужна, підвищує ризик людської помилки та ускладнює усунення несправностей. Архітектура повинна забезпечувати прозорість та можливість аудиту всіх компонентів. Принцип простоти та зрозумілості часто перемагає над надмірною технологічною складністю, оскільки операційна ефективність SOC напряму залежить від того, наскільки швидко аналітик може зрозуміти, що сталося і чому система це виявила.

Таким чином, вибір архітектури SOC – це не просто купівля «найкращого» обладнання чи програмного забезпечення, а стратегічне рішення, яке є відображенням потреб, ризиків та ресурсів організації. Це баланс між масштабованістю, надійністю, швидкістю, вартістю та людським потенціалом.

Для оцінки наслідків втрати основних властивостей активів – які в кібербезпеці зазвичай представлені тріадою CIA (Confidentiality, Integrity, Availability – конфіденційність, цілісність, доступність), а також часто розширюються до CIAA (конфіденційність, цілісність, доступність, автентичність) та спостережливість – використовуються критерії, що охоплюють фінансові, операційні, репутаційні та регуляторні аспекти.

Оцінка наслідків є важливою частиною управління ризиками.

Наслідки порушення безпеки активу оцінюються за кількома основними напрямками.

1. Фінансові Збитки. Це найбільш прямий і кількісно вимірюваний критерій. Втрати можуть включати:

– прямі втрати доходу (внаслідок простою критичних систем виникає втрата доступності);

– витрати на відновлення (кошти на усунення інциденту, відновлення систем, заміну обладнання, наймання зовнішніх експертів);

– штрафи та санкції (фінансові стягнення за порушення регуляторних вимог (GDPR, PCI DSS) або умов контрактів призводить до втрати конфіденційності чутливих даних);

– зниження вартість акцій/ринкова капіталізація (довгострокові фінансові наслідки репутаційної шкоди).

2. Операційні Втрати (втрата ефективності). Цей критерій оцінює вплив на здатність організації виконувати свої основні функції:

– простій критичних функцій (час, протягом якого бізнес-процеси зупинені або функціонують некоректно через втрату доступності активу);

– порушення роботи бізнес-процесів (ситуації, коли дані чи системи скомпрометовані (втрата цілісності), що призводить до прийняття невірних рішень, затримок у виробництві або некоректної роботи сервісів(;

– втрата контролю та спостережливості (нездатність моніторити стан системи унеможливлює своєчасне виявлення та реагування на інциденти, що продовжує час простою та підвищує загальні збитки);

– втрата довіри до даних (якщо системи звітують про скомпрометовані або неправдиві дані, це призводить до значних операційних витрат на їх перевірку та виправлення).

3. Репутаційні та довіра клієнтів.

Наслідки, що мають непрямий, але часто довготривалий вплив на бізнес:

– втрата довіри клієнтів та партнерів (особливо критично при витоку персональних даних або інформації про транзакції);

– погіршення іміджу бренду (негативне висвітлення у ЗМІ, яке відлякує нових клієнтів і впливає на лояльність існуючих);

– конкурентна позиція (якщо інцидент дає перевагу конкурентам або розкриває комерційну таємницю).

4. Регуляторні та юридичні наслідки.

Оцінка відповідності законодавчим та нормативним вимогам:

– невиконання законодавчих вимог (порушення законів про захист даних, яке призводить до юридичних позовів та штрафів;

– порушення контрактних зобов'язань (недотримання угод про рівень обслуговування (SLA) з клієнтами чи партнерами, що може призвести до розірвання контрактів);

– вимоги про обов'язкове повідомлення (необхідність публічного оголошення про порушення безпеки, що посилює репутаційні збитки).

Оцінка наслідків завжди прив'язана до конкретного порушення властивості активу (табл. 2.1).

Таблиця 2.1 – Наслідки порушення властивості активу

Властивість активу (порушення)	Ключові оціночні критерії наслідків
Конфіденційність (розкриття даних)	Фінансові (штрафи, позови), репутаційні (втрата довіри), регуляторні (порушення GDPR/PCI DSS)
Цілісність (несанкціонована зміна даних)	Операційні (некоректні рішення, помилки в обліку), фінансові (потреба у виправленні, шахрайство), юридичні (недостовірність звітів)
Доступність (недоступність системи/даних)	Операційні (простій, втрата продуктивності), фінансові (втрата доходу, витрати на відновлення)
Автентичність (несправжність користувача/системи)	Операційні (дії зловмисника під виглядом легітимного користувача), фінансові (шахрайство), юридичні
Спостережливість (недоступність логів/моніторингу)	Операційні (подовження часу виявлення інциденту), фінансові (зростання загальних витрат на відновлення)

Оцінка зазвичай проводиться за шкалою (наприклад, від низького до критичного) для кожного критерію окремо, а потім комбінується для визначення загального рівня ризику для активу.

4) Бюджет і фінансова готовність.

Бюджет і фінансова готовність є факторами, які безпосередньо визначають рівень зрілості та ефективності системи кібербезпеки на будь-якому підприємстві. Це питання, по суті, про управління ризиками та інвестиції.

Підприємства, які досягають високої кіберстійкості, розглядають витрати на безпеку не як «центр витрат», а як стратегічну інвестицію у безперервність бізнесу та захист активів.

Оптимальний бюджет не є фіксованим відсотком від загальних IT-витрат. Він визначається на основі оцінки ризиків. Підприємство аналізує, які саме

активи є критичними (IP, клієнтські дані, операційні системи), яка ймовірність їх компрометації та якою буде фінансова ціна найгіршого сценарію (аналіз наслідків, про який ми говорили раніше). Бюджет має бути достатнім для зниження найбільш критичних ризиків до прийнятного рівня.

Підприємства, що працюють у високорегульованих галузях (фінанси, охорона здоров'я, державний сектор), зобов'язані виділяти значні кошти для відповідності стандартам PCI DSS, GDPR, HIPAA тощо. Бюджет тут є обов'язковим мінімумом для легального ведення діяльності.

У свою чергу компанії, що володіють критично важливою інфраструктурою або мають великі обсяги персональних даних, повинні інвестувати більше у відмовостійкість та захист периметру.

Таким чином, готовність підприємства витрачати кошти на кібербезпеку – це пряме відображення його толерантності до ризику. Чим критичніші активи та чим менша толерантність до простою, тим більшими будуть і більш обґрунтованими витрати на забезпечення безпеки.

2.2 Рекомендації щодо вибору архітектури та типу SOC

Створення Центру моніторингу та оперативного реагування (SOC) необхідне, коли рівень кіберризику, вимоги законодавства чи масштаб бізнес-операцій перевищують можливості стандартних, розрізнених інструментів безпеки.

Розглянемо ключові ситуації та умови, за яких створення SOC стає важливим або обов'язковим.

Створення SOC є обов'язковим, якщо інцидент кібербезпеки може призвести до катастрофічних наслідків для бізнесу:

– захист критичної інфраструктури (якщо підприємство належить до секторів фінансів, енергетики, телекомунікацій, транспорту чи охорони здоров'я. Порушення роботи цих систем має прямі наслідки для національної безпеки або життя та здоров'я людей);

– обробка надзвичайно чутливих даних (коли організація працює з великими обсягами персональних даних клієнтів (GDPR), комерційною таємницею, інтелектуальною власністю (IP) або військовими/державними секретами. Втрата вонфіденційності цих активів є неприпустимою);

– висока ймовірність цілеспрямованих атак (якщо компанія є привабливою мішенню для висококваліфікованих, фінансово мотивованих або підтримуваних державою хакерських груп. У цьому випадку потрібен проактивний моніторинг та Threat Hunting, що є основними функціями SOC);

– складна IT-екосистема (наявність гібридної або складної розподіленої інфраструктури, що включає операційні технології чи Інтернет речей (IoT). Управління безпекою такого ландшафту неможливе без централізованої спостережливості).

У багатьох випадках рішення про SOC диктується не внутрішніми потребами, а зовнішніми регуляторними та контрактними вимогами:

– регуляторний комплаєнс (законодавство вимагає мати постійний моніторинг та документовану процедуру реагування на інциденти. Наприклад, стандарти ISO 27001, PCI DSS (для обробки платіжних карток) та місцеві закони про захист даних часто вимагають можливостей, які може надати лише SOC);

– вимоги страхових компаній (для отримання поліса страхування кіберризиків компанія повинна продемонструвати високий рівень контролю, включаючи 24/7 моніторинг, що є синонімом роботи SOC;

– контрактні зобов’язання (великі корпоративні клієнти чи державні організації можуть вимагати від своїх підрядників наявності SOC як обов’язкову умову співпраці для забезпечення безпеки ланцюга постачання).

Створення SOC є логічним кроком еволюції кібербезпеки:

– потреба в централізації та автоматизації (коли існуючі інструменти безпеки (IDS/IPS, фаєрволи) генерують таку велику кількість сповіщень, що команда безпеки не встигає їх обробляти (проблема «шуму»). SOC використовує SIEM для кореляції та SOAR для автоматизації, що дозволяє швидко виявляти справжні загрози);

– неможливість ефективного реагування (якщо середній час виявлення та середній час реагування на інциденти є занадто довгими, що призводить до значних збитків. SOC створюють для зменшення цих показників через стандартизовані процедури та цілодобову готовність;

– перехід від реактивного до проактивного захисту, це коли підприємство хоче не просто «залатати діри» після атаки, а проактивно шукати загрози у своїй мережі. Це вимагає спеціалізованих навичок, постійного аналізу загроз та інструментів, що консолідуються в SOC.

Отже, рішення про створення SOC є точкою перетину між рівнем бізнес-ризику, ціною інциденту та фінансовою можливістю його запобігання. Якщо потенційні збитки від кібератаки значно перевищують вартість створення та підтримки SOC, то його створення є необхідністю.

Створення Enterprise SOC (Центру оперативного реагування на загрози рівня підприємства) необхідне, коли масштаби, складність та критичність інформаційних активів організації виходять за рамки можливостей стандартних засобів захисту. Enterprise SOC потрібен, коли звичайні заходи безпеки вже не можуть ефективно захистити організацію, і потрібна централізація та професіоналізація функції кібербезпеки.

Це рішення обумовлене такими основними факторами: високий рівень ризику та критичність, масштаб та складність інфраструктури, вимоги до часу реагування та комплаєнсу.

Enterprise SOC стає необхідним, коли компанія оперує великою, розподіленою та надзвичайно складною IT-інфраструктурою. Це стосується великих банків, глобальних телекомунікаційних провайдерів, виробничих гігантів або енергетичних компаній, чиї операції розподілені по різних регіонах і країнах. У таких випадках кількість згенерованих даних вимірюється терабайтами щодня. Аналіз такого обсягу інформації, кореляція подій між віддаленими філіями, хмарними та локальними середовищами та, найголовніше, скорочення часу виявлення до хвилин, а не годин, неможливе без спеціалізованого центру. По суті, SOC стає життєво необхідним інтелектуальним фільтром, що перетворює хаос даних на конкретні інциденти.

Якщо діяльність компанії перебуває під суворим державним або міжнародним регулюванням, створення Enterprise SOC є практично обов'язковим. Це стосується, наприклад, фінансових установ, які підпадають під вимоги Національного банку щодо стійкості та захисту даних, або компаній, які працюють з персональними даними громадян ЄС (GDPR). Ці регулятори часто вимагають не просто наявності захисних механізмів, а й формалізованих, документованих та цілодобових процесів моніторингу та управління інцидентами. Enterprise SOC може забезпечити таку повну прозорість, контрольованість та звітність перед регуляторами.

Для компаній, чий основний капітал полягає в унікальних технологіях, комерційній таємниці, патентах або даних клієнтів (фармацевтика, IT-розробники, оборонний сектор), ризик економічного шпигунства є реальністю. Цілі атак у цьому випадку не фінансова вигода, а крадіжка інтелектуальної власності. Оскільки такі атаки часто є високоцільовими та використовують «нульові дні», вони не виявляються стандартними антивірусами. Enterprise SOC потрібен для проактивного полювання за загрозами, тобто для пошуку прихованих зловмисників, які вже проникли в мережу, використовуючи експертизу внутрішніх фахівців, які досконало знають, які саме дані є найціннішими і де їх шукати.

Якщо компанія надає послуги, життєво важливі для суспільства або для безперервності власного бізнесу, ціна простою через кібератаку є катастрофічною. Enterprise SOC створюється для мінімізації часу простою і забезпечення безперервності бізнесу. Зовнішній MSSP може добре відреагувати, але лише внутрішня команда SOC може миттєво приймати бізнес-рішення (наприклад, відключити цілий сегмент виробництва, щоб запобігти поширенню вірусу) з повним розумінням всіх операційних ризиків.

Рішення про створення Enterprise SOC суттєво залежить від кількості працівників фірми, але непрямо. Кількість співробітників є важливим індикатором масштабу, складності та поверхні атаки організації, що, у свою чергу, і обумовлює необхідність власного SOC.

Кількість працівників корелює з кількома ключовими факторами, що вимагають Enterprise SOC. Чим більше співробітників – тим більше пристроїв підключається до мережі, тим більше облікових записів та прав доступу потрібно керувати і тим більше взаємодій відбувається з хмарними сервісами, що розширює мережевий периметр.

Це призводить до експоненційного зростання кількості подій безпеки, які потрібно аналізувати. Обробка цього обсягу даних вимагає автоматизації та централізації (функцій SOC).

Управління безпекою в такому складному, гетерогенному середовищі вимагає встановлених процесів (COBIT Рівень 3+) та постійного цільового моніторингу (функції Enterprise SOC).

Мала фірма (до 100 працівників) зазвичай може обійтися аутсорсингом SOC (MSSP), оскільки витрати на створення внутрішнього центру не виправдані. У свою чергу, велика корпорація (від 1000+ працівників), як правило, потребує Enterprise SOC через величезну поверхню атаки, високу складність інфраструктури та критичність бізнес-процесів.

Створення SOC-as-a-Service (SOC як послуга), що є формою аутсорсингу (MSSP), стає найкращим стратегічним вибором, коли організація потребує високоякісного, цілодобового кіберзахисту, але не має внутрішніх ресурсів або не вважає доцільним створювати і підтримувати власний корпоративний центр.

Прийняття рішення про використання SOC-as-a-Service є наслідком тверезої оцінки внутрішніх можливостей та зовнішніх загроз.

SOC-as-a-Service дає миттєвий доступ до глибокої, широкої та актуальної експертизи, якою володіє провайдер. Ці команди постійно працюють з десятками клієнтів, обробляючи різні типи загроз і накопичуючи унікальні знання про сучасні тактики зловмисників. Організація отримує таку експертизу, не обтяжуючи себе процесами найму, навчання та заміни персоналу.

SOC-as-a-Service може бути розгорнутий значно швидше, часто за лічені тижні, без необхідності встановлення та інтеграції маси обладнання. Крім того, ці послуги легко масштабуються: якщо компанія подвоїла кількість серверів чи

співробітників, провайдер просто адаптує обсяг моніторингу, тоді як внутрішній SOC потребував би нових інвестицій та персоналу.

Багато компаній можуть підтримувати моніторинг безпеки лише протягом робочого дня (5/8), залишаючи себе вразливими у вечірні та нічні години та на вихідних, коли більшість інцидентів починаються або розвиваються. SOC-as-a-Service за своєю природою надає цілодобове покриття (24/7), гарантуючи, що хтось спостерігає за системою і готовий реагувати, навіть коли внутрішні співробітники відпочивають.

SOC-as-a-Service потрібно обирати організаціям, які розглядають кібербезпеку як стратегічну послугу, що повинна бути високоякісною та надійною, а не як внутрішній IT-проект, який поглинає дефіцитні ресурси та час.

У свою чергу, Hybrid SOC рекомендовано обирати організації, що знаходяться на перетині потреби у внутрішньому контролі та необхідності оптимізації ресурсів. Ця модель не виникає від простої економії, а від розуміння того, що різні функції безпеки вимагають різних підходів.

Гібридний SOC стає оптимальним рішенням у випадках, коли організація є занадто великою та критичною, щоб повністю покладатися на зовнішній аутсорсинг, але недостатньо великою або забезпеченою ресурсами, щоб підтримувати власний, повноцінний, цілодобовий Enterprise SOC.

Найпоширеніша причина для вибору гібридної моделі – це досягнення цілодобового покриття (24/7) без колосальних витрат на штат. Підтримка власної команди, що працює у чотири зміни (мінімум 10-12 штатних одиниць), є дуже дорогою. У таких випадках компанія вирішує аутсорсити рутинні, базові функції Tier 1 (первинний моніторинг, фільтрація помилкових спрацьовувань) зовнішньому постачальнику послуг безпеки (MSSP). Це дозволяє MSSP, який вже має інфраструктуру та персонал, виконувати «нічні чергування» та «святкові зміни», тоді як внутрішня команда може зосередитися на робочому графіку (наприклад, 8 годин на день, 5 днів на тиждень). Таким чином, компанія «купує» час і економію, делегуючи найбільш ресурсоємний аспект моніторингу.

Для багатьох організацій існують унікальні та високочутливі дані або системи (наприклад, критично важливі фінансові сервери, інструменти

інженерної розробки), інформацію про які вони не можуть або не хочуть передавати сторонній компанії. У гібридній моделі компанія створює внутрішню команду Tier 2 та Tier 3, яка бере на себе поглиблене розслідування інцидентів, що стосуються цих чутливих активів. MSSP надсилає лише «сигнал тривоги» (підтверджений інцидент), а подальше розслідування, яке вимагає доступу до конфіденційних внутрішніх даних, проводиться власними фахівцями. Це дозволяє зберегти суверенітет даних та контролювати найважливіші фази реагування.

2.3 Порядок розміщення SOC на підприємстві

Створення Центру оперативного реагування (SOC) являє собою багатоетапний проект, який вимагає глибокої трансформації корпоративної культури безпеки. Етапи впровадження SOC забезпечують, що новий центр не стане просто дорогою «чорною дірою» для логів, а буде ефективно інтегрований у бізнес-процеси.

Процес впровадження SOC зазвичай поділяють на три великі фази: планування та обстеження, створення та впровадження, й оптимізація та управління.

На перші фазі закладаються цілі, обсяг робіт і визначається, що саме буде захищатися і як це буде вимірюватися.

Під час обстеження підприємства, здійснюючи визначення обсягу та цілей, команда проводить ретельну інвентаризацію та аналіз поточного стану безпеки. Це схоже на медичне обстеження: ми повинні знати, де у пацієнта болить, перш ніж призначати лікування.

Спершу необхідно визначити, які активи є найціннішими для бізнесу. Далі проводиться аналіз ризиків для цих активів, щоб зрозуміти, які саме загрози є найімовірнішими та найруйнівнішими. Це дає чітке розуміння, які інциденти SOC повинен запобігати та виявляти в першу чергу.

Під час аналізу поточної зрілості (COBIT) оцінюється поточний рівень зрілості IT-процесів (як було сказано вище, мінімум Рівень 3). Це включає оцінку

того, як зараз ведеться управління активами, управління конфігураціями та управління інцидентами. Якщо ці процеси незрілі, SOC не матиме якісних даних для роботи.

Також чітко окреслюється, які сегменти мережі (локальні офіси, хмара, виробничі системи) будуть під моніторингом SOC. Це рішення безпосередньо впливає на вибір технологій і кількість персоналу.

У подальшому, на основі ризиків, бюджету та наявної експертизи приймається рішення про модель, що обумовлює подальше розміщення технічного оснащення та найм персоналу. Встановлюються ключові показники ефективності, які SOC буде зобов'язаний демонструвати, наприклад, середній час виявлення та середній час реагування.

На другій фазі впровадження технологій та створення процесів відбувається фізичне створення центру та його інтеграція.

Створення технічної бази передбачає закупівлю, розгортання та налаштування ключових технологічних комплексів:

– SIEM-системи (для агрегації та кореляції логів);

– SOAR-платформи (для автоматизації);

– сенсорів і агентів EDR (на кінцевих точках);

– інтеграція з Threat Intelligence (для отримання актуальних даних про загрози).

На етапі розробки процедур створюються стандартизовані алгоритми дій для найпоширеніших та найкритичніших інцидентів (наприклад, фішинг, витік даних, DDoS). Це гарантує, що незалежно від того, хто з аналітиків на чергуванні, реакція буде однаковою та ефективною.

Набір та навчання персоналу передбачає формування команди аналітиків (Tier 1, Tier 2, Tier 3). Персонал проходить навчання з використання нових ПТК та обов'язково – практичні тренування з реагування на змодельовані інциденти.

Рекомендації, що до кількості потрібних фахівці, які необхідні для впровадження SOC, подано у таблиці 1.2 даної роботи.

Після запуску SOC на фазі експлуатації, оптимізація та вдосконалення переходить у безперервний цикл покращення.

Коли SOC починає працювати в режимі 24/7, то основна увага приділяється калібруванню SIEM – зниженню кількості помилкових спрацьовувань, які можуть паралізувати роботу аналітиків [3].

Команда Tier 3 починає активно шукати приховані загрози, ґрунтуючись на нових індикаторах та аналізі логіки атак, а не просто чекаючи сповіщень.

Згідно з принципом ISO 27035, після кожного великого інциденту проводиться аналіз «винесених уроків». Ці уроки використовуються для оновлення Playbooks, покращення правил SIEM та вимог до персоналу, забезпечуючи, що SOC стає кращим із кожним новим викликом.

У сценаріях подій певний набір правил [9], який ви розглядаєте, найчастіше називається Playbook або Runbook.

Playbook – це формалізований, детальний набір інструкцій та процедур, який автоматично або вручну виконується командою SOC для реагування на конкретний тип інциденту чи загрози. Він охоплює весь сценарій події, від виявлення (наприклад, SIEM спрацював на несанкціоновану спробу доступу) до відновлення (очищення системи та повернення до нормальної роботи).

Кожен великий виробник, який продає системи для моніторингу та реагування (наприклад, Microsoft, Palo Alto Networks, Splunk, IBM), має власні портали. Вони публікують Playbooks, які максимально інтегровані та оптимізовані для роботи з їхнім програмним забезпеченням.

Окрім офіційних порталів, існують також спеціалізовані ресурси та спільноти, часто створені за підтримки виробників або незалежних експертів, де фахівці обмінюються цими сценаріями:

– форуми та репозиторії на GitHub (хоча це не завжди офіційні сайти, вони є важливим джерелом сценаріїв, адаптованих спільнотою, часто з урахуванням досвіду використання продуктів конкретних виробників);

– державні ресурси (такі організації, як CISA (Cybersecurity and Infrastructure Security Agency) у США, створюють та публікують Playbooks, які виробники також інтегрують у свої продукти для підвищення національної кіберстійкості).

Як було зазначено вище, виробники мають власні сайти для публікації сценаріїв подій.

Palo Alto Networks, Inc. – це американська багатонаціональна компанія, яка є світовим лідером у сфері кібербезпеки. Вона розробляє та надає комплексні рішення для інформаційної безпеки, захищаючи мережі, кінцеві точки, а також хмарні середовища. Їхня продукція об'єднана в єдину платформу безпеки, але більшість продуктів Palo Alto Networks не є вільно доступними. Компанія часто пропонує безкоштовні пробні версії (free trials) своїх програмних рішень, особливо для хмарних продуктів та віртуальних міжмережевих екранів. Це дає можливість протестувати функціонал протягом обмеженого часу (наприклад, 30 днів).

Кількість сценаріїв подій або випадків використання Palo Alto Networks є дуже великою і охоплює практично всі аспекти сучасної кібербезпеки. Кожна з трьох платформ закриває десятки конкретних потреб (табл. 2.2).

Таблиця 2.2 – Сценарії використання Palo Alto Networks

Платформа	Приклади сценаріїв використання
Strata	Запобігання нульовим атакам (Zero-Day Attacks): використання WildFire для аналізу невідомих файлів. Контроль додатків (App-ID): дозвіл/заборона трафіку на основі фактичних додатків, а не лише портів. Захист IoT: ідентифікація та сегментація всіх пристроїв Інтернету речей у мережі.
Prisma	Безпека DevSecOps: сканування коду на вразливості до розгортання в хмарі (Shift Left). Zero Trust Network Access (ZTNA): надання доступу до корпоративних програм лише після ретельної перевірки користувача та пристрою. Cloud Security Posture Management (CSPM): безперервний аудит конфігурації хмарних ресурсів на відповідність стандартам безпеки (Compliance).
Cortex	Автоматичне реагування на інциденти: Використання XSOAR для автоматичного блокування шкідливих IP-адрес та ізоляції уражених пристроїв. Розширене виявлення загроз (XDR): Об'єднання даних з кінцевих точок, мережі та хмари для швидкого виявлення складних атак. Управління поверхнею атаки (ASM): Виявлення незахищених або невідомих зовнішніх активів (тіньовий IT).

HPE ArcSight Marketplace стосується інтегрованого онлайн-ресурсу, який є частиною екосистеми продуктів ArcSight – однієї з провідних платформ у сфері SIEM [10]. Це централізований каталог (магазин), де користувачі платформи

ArcSight можуть знаходити, завантажувати та інтегрувати готовий контент для підвищення ефективності своєї системи безпеки.

Він надає «будівельні блоки» для SIEM-системи, які допомагають швидко реагувати на нові загрози та вимоги комплаєнсу. Кількість сценаріїв подій, доступних для платформи ArcSight, є динамічною і вимірюється сотнями офіційних та партнерських пакетів.

IBM Security App Exchange – це онлайн-репозиторій (маркетплейс) та екосистема для спільного використання програмних розширень, додатків та контенту, які посилюють можливості основних продуктів IBM Security [11]. Exchange дозволяє користувачам завантажувати й встановлювати розширення, що додають нові функції, інтеграції та аналітику до їхніх рішень IBM Security.

Splunk – це американська транснаціональна компанія, яка розробила однойменну потужну програмну платформу, призначену для пошуку, моніторингу, аналізу та візуалізації величезних обсягів машиногенерованих даних (log files, метрики, траси, конфігурації). Це універсальний інструмент, який збирає дані в реальному часі з практично будь-якого джерела (сервери, мережеве обладнання, програми, хмарні сервіси) та перетворює їх на аналітичні інсайти.

Цей онлайн-маркетплейс, подібний до IBM App Exchange, який містить понад 2000 застосунків, додаткових модулів та пакетів контенту, розроблених Splunk, партнерами та спільнотою. Це дозволяє користувачам легко розширювати функціонал платформи для конкретних джерел даних або галузевих потреб.

Розробка ефективних правил співвідношення (correlation rules) є ядром роботи будь-якої системи SIEM [9]. Це процес перетворення необроблених даних (логів) на дієздатні інциденти.

Основними методами (або стратегіями/техніками) співвідношення подій, які використовуються в SIEM, можна виділити наступні: часове співвідношення, співвідношення на основі топології та контексту, статистичне та порогове співвідношення, кореляція на основі правил, поведінкове співвідношення.

Розробка правила співвідношення потребує збору інформації, що здатна представити система SIEM [5] та подальшої фільтрації.

Щоб цілеспрямовано збирати та аналізувати лише відповідні дані, система SIEM має орієнтуватися на результати, визначені вашими бізнес-цілями та пріоритетами безпеки.

Система має бути налаштована на виявлення конкретних, відомих загроз, які є найбільш актуальними для вашої організації.

SIEM має збирати та зберігати дані, які необхідні для проходження аудиту та підтвердження відповідності галузевим стандартам (GDPR, PCI DSS, HIPAA, ISO 27001).

Якщо SIEM збирає «все підряд», це призведе до великих витрат на зберігання та аналітичного «паралічу». Тому збір інформації має бути цілеспрямованим і залежати від того, які індикатори компрометації або аномалії ви прагнете виявити, та які бізнес-ризики зменшити.

Після запуску системи SIEM та інфраструктури SOC, підтримка активності та тестування працездатності є важливими заключними етапами впровадження. Вони забезпечують, що SOC не лише функціонує, але й ефективно справляється з реальними загрозами.

Тестування працездатності є формальним процесом, що підтверджує, що SOC здатний виявляти та реагувати на атаки.

Тестування ефективності виявлення це перевірка того, чи спрацьовують правила кореляції та чи коректно вони виявляють загрози.

Емуляція атак здійснюється шляхом імітація реальних технік зловмисників. Тестування показує, чи здатні SOC виявити ці дії.

Тестування ефективності реагування – це перевірка не технологій, а людських процесів і процедур.

Перевірка Playbooks та процедур – тестування, наскільки швидко та правильно аналітики дотримуються інструкцій (Playbooks) для ізоляції уражених систем, збору доказів та ескалації інциденту.

Регулярна підтримка та тестування гарантують, що інвестиції в SIEM та SOC приносять реальну безпекову цінність, а не просто збирають великі обсяги даних.

Можливий варіант реалізації SOC на підприємстві та процеси подано на рисунку 2.1-2.2)

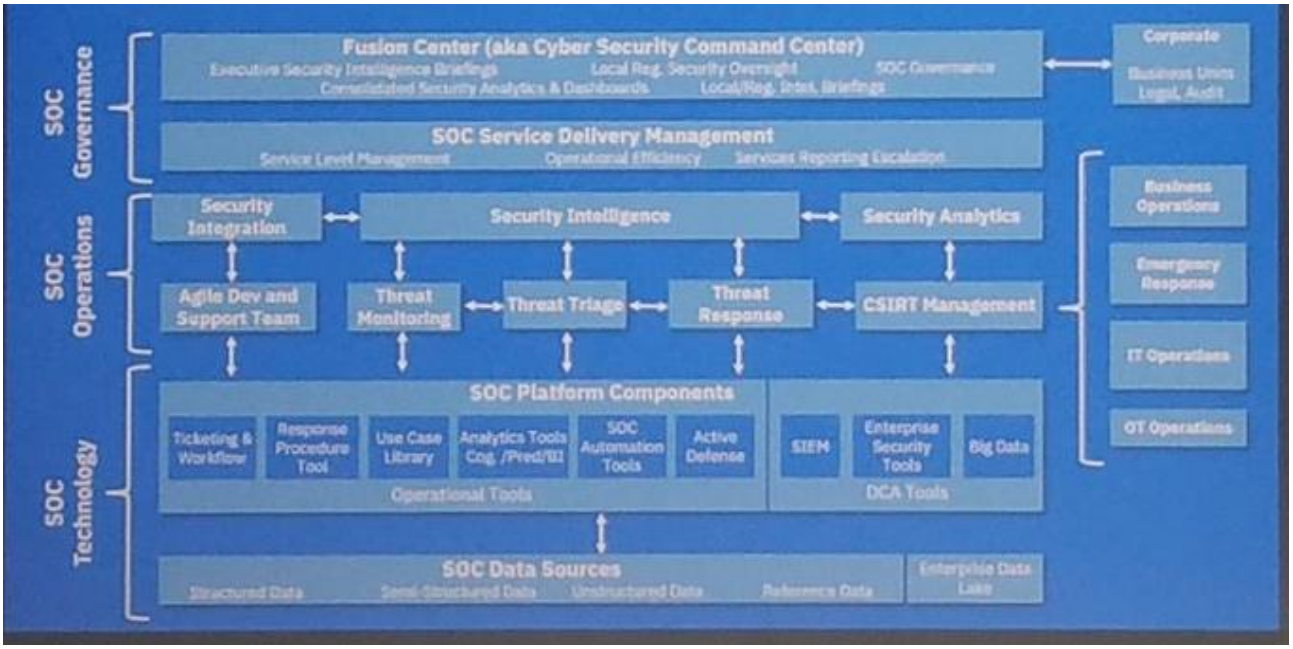

Рисунок 2.1 – Можливий варіант реалізації SOC

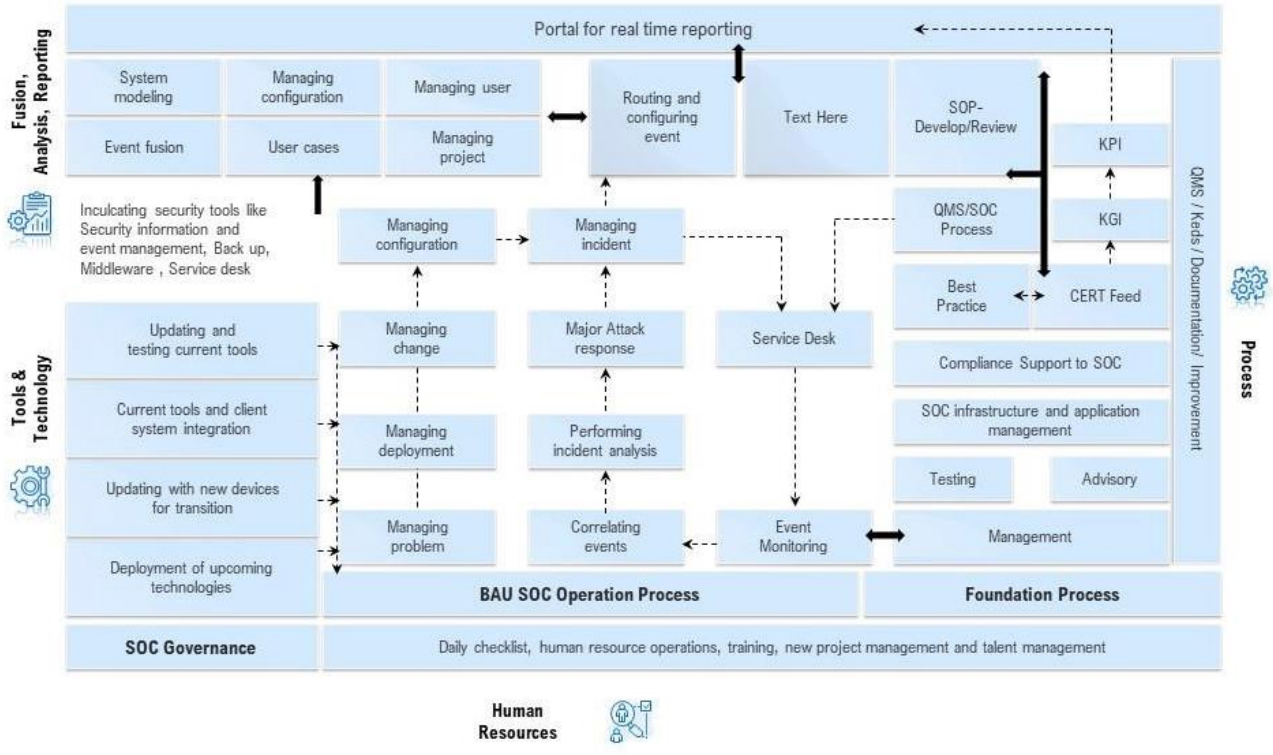

Рисунок 2.2 – Взаємодія процесів SOC

Проведений аналіз наявних моделей реалізації SOC та наведені основні чинники, які потрібно враховувати при виборі оптимальної моделі SOC, дозволив отримати необхідні рекомендації, що висвітлені у п. 2.2 даного розділу. Керуючись цими рекомендаціями можна обрати архітектуру, яка підійде для бізнесу різних типів. Порядок реалізації SOC на підприємстві висвітлено у п. 2.3.

2.4 Порівняння SIEM-систем

Розширене порівняння систем, зазначених у п. 2.3 даної роботи, варто проводити, орієнтуючись не лише на бренд, а й на їхню роль та спеціалізацію в екосистемі кібербезпеки, оскільки HPE ArcSight Marketplace та IBM Security App Exchange є не повноцінними SIEM-системами, а допоміжними каталогами контенту для своїх материнських платформ (ArcSight та QRadar відповідно).

Ми маємо чітко розділити чотири зазначені назви на дві категорії:

– повноцінні аналітичні платформи (SIEM/XSIAM) – це системи, які виконують збір, зберігання, аналіз та кореляцію подій безпеки: Palo Alto Networks (через платформу Cortex XSIAM), Splunk (через рішення Enterprise Security);

– каталоги контенту та розширень (маркетплейси) – онлайн-ресурси, що надають додаткові правила, інтеграції та застосунки для своїх материнських SIEM-систем: HPE ArcSight Marketplace (для ArcSight SIEM, тепер OpenText) та IBM Security App Exchange (для QRadar SIEM).

Palo Alto Networks позиціонує своє рішення Cortex XSIAM як еволюційний крок після SIEM (Extended Security Intelligence & Automation Management). Це сучасна платформа, створена з акцентом на штучний інтелект (AI), машинне навчання та автоматизацію (SOAR).

Ключова перевага Palo Alto Netwoks полягає у консолідації даних безпеки та автоматизації операцій. XSIAM глибоко інтегрований з іншими продуктами Palo Alto Networks (Firewalls, Prisma Cloud), що забезпечує цілісний захист від кінцевої точки до хмари. Система намагається замінити традиційні SIEM,

інтегруючи UEBA (аналіз поведінки), XDR (розширене виявлення та реагування) і SOAR в єдиному рішенні.

Palo Alto Netwoks спеціалізує фокусування на запобіганні та AI-драйвованому виявленні, мінімізуючи необхідність ручного налаштування правил кореляції (табл. 3.1).

Splunk є піонером у сфері аналізу машинних даних, і його рішення Enterprise Security (ES) – це одна з найпопулярніших SIEM-систем на ринку.

Сила Splunk полягає у його гнучкості, здатності індексувати будь-які дані з будь-якого джерела завдяки потужній мові запитів SPL (Search Processing Language). Це дає аналітикам безпрецедентну свободу для пошуку та розслідування інцидентів.

Перевага Splunk – це його Splunkbase, маркетплейс із тисячами готових застосунків та інтеграцій, розроблених спільнотою та вендорами. Це робить його надзвичайно адаптивним для інтеграції з унікальними інфраструктурами.

Спеціалізація Splunk полягає в універсальності, масштабованості та глибокому пошуку (forensics). Це ідеальний підходить для організацій, які мають команду досвідчених аналітиків, здатних писати складні запити на SPL.

IBM Security App Exchange та HPE ArcSight Marketplace не є SIEM-системами; вони є критичними розширювальними хабами для своїх материнських SIEM-платформ: IBM QRadar та OpenText ArcSight відповідно.

IBM Security App Exchange (для QRadar) служить каталогом для додатків, розширень та контенту, які додають нові можливості до IBM QRadar. Це включає нові візуалізації, інтеграції з новими джерелами даних (наприклад, хмарними API), а також пакети правил кореляції та звітів. Вона спрямована на використання технології IBM (наприклад, Watson AI) у контексті безпеки та на стандартизацію інтеграцій через чіткий API, що підтримує його велику корпоративну клієнтську базу.

HPE ArcSight Marketplace (для ArcSight) аналогічно, це репозиторій для контенту – Use Cases, правила кореляції та пакети звітів – для платформи ArcSight. Це дозволяє клієнтам швидко адаптуватися до нових загроз та вимог

комплаєнсу, завантажуючи готовий контент, створений компанією та її партнерами.

Таблиця 3.1 – Порівняння SIEM-систем

Платформа	Роль	Основна перевага
Palo Alto (XSIAM)	AI-драйвована операційна платформа (Пост-SIEM)	Глибока консолідація, AI-автоматизація та запобігання.
Splunk (ES)	Гнучка, універсальна SIEM	Неперевершена гнучкість, потужність SPL та найбільший маркетплейс (Splunkbase).
IBM App Exchange	Каталог розширень	Розширення можливостей QRadar, використання технологій IBM.
HPE ArcSight Marketplace	Каталог контенту	Готові пакети правил та звітів для ArcSight.

ArcSight історично відомий своєю надійністю та відповідністю вимогам великих регульованих організацій (фінанси, державний сектор). Marketplace підтримує цю лінійку, забезпечуючи постійне оновлення контенту без необхідності суттєвої зміни ядра системи.

Таким чином, Palo Alto та Splunk – це змагаючі аналітичні двигуни, де Palo Alto робить ставку на радикальну автоматизацію та інтеграцію, а Splunk – на універсальність даних та гнучкість. IBM та HPE пропонують свої каталоги контенту як стратегічний механізм оновлення для підтримки довговічності та актуальності їхніх власних, вже існуючих SIEM-рішень (QRadar та ArcSight).

На основі проведеного аналізу чотирьох основних компаній SIEM, які переважно беруть до уваги під час вибору чіткої моделі SOC, можна здійснити вибір оптимальної системи для впровадження на підприємстві. Кращим рішенням для підприємства є SIEM QRadar від IBM Security App Exchange [11].

РОЗДІЛ 3 РОЗРОБКА ПРОЦЕСІВ РОЗСЛІДУВАНЬ РІЗНИХ ТИПІВ ІНЦИДЕНТІВ

3.1 Інциденти фішингу

Інциденти фішингу – це одне з найпоширеніших і, на жаль, найбільш успішних кібершахрайств, яке використовує не технічні вразливості, а головним чином людську психологію. Це спосіб маскування, коли зловмисник видає себе за довірену особу чи організацію з метою викрасти конфіденційну інформацію, таку як паролі, дані кредитних карток або корпоративні облікові записи.

Фішинг можна порівняти із риболовлею: шахраї «закидають приманку» у вигляді електронного листа, повідомлення у месенджері чи SMS, сподіваючись, що хтось її «ковтне». Сценарій атаки завжди побудований на соціальній інженерії та маніпуляціях.

Атака починається зі створення повідомлення, яке імітує легітимне джерело – це може бути банк, велика компанія, державна установа, або навіть керівник компанії. Зловмисники використовують відчуття терміновості, страху, цікавості чи жадібності, щоб змусити жертву діяти необдумано. Наприклад, лист може попереджати про «несанкціоновану транзакцію, яку потрібно негайно скасувати», або про «блокування облікового запису, для відновлення якого потрібна верифікація2.

Ключовий елемент фішингу – шкідливе посилання. Натискаючи на нього, жертва переходить на шахрайську вебсторінку, яка є ідеальною копією справжнього сайту (банківського порталу, сторінки входу в корпоративну пошту, чи платіжної системи). Ввівши свої справжні дані на цій підробленій сторінці, користувач фактично добровільно передає їх зловмисникам.

Фішинг інцеденти можна вирішувати за допомогою наступних рішень:

– Office 365 Advanced Threat Protection (ATP), є комплексом хмарних онлайн-рішень, який захищає організації від просунутих загроз, що поширюються електронною поштою та через інші інструменти Microsoft 365. Він

застосовується для захисту від фішингу та спаму, здійснює сканування в реальному часі URL-адреси і, за потреби, блокує їх;

– CheckPhish – популярний онлайн-сканер посилань, який допомагає користувачам та аналітикам безпеки визначати, чи є URL-адреса фішинговою, шкідливою або підозрілою. Він є незалежним, хмарним інструментом, який використовується для проактивної перевірки потенційно небезпечних посилань, отриманих у електронних листах, повідомленнях чи на веб-сайтах;

– VirusTotal – безкоштовний, хмарний сервіс, який спеціалізується на аналізі файлів і URL-адрес на предмет виявлення шкідливого програмного забезпечення, вірусів та інших загроз;

– Cisco Talos Intelligence Group (або просто Talos) – один із найбільших і найавторитетніших у світі підрозділів з дослідження та аналізу кіберзагроз. Він належить компанії Cisco, яка займається безперервною перевіркою даних у всьому глобальному кіберпросторі;

– URLscan.io – потужний, публічний онлайн-сервіс, який спеціалізується на автоматизованому скануванні та аналізі веб-сторінок за наданими URL-адресами;

– Hybrid Analysis – багатоцільовий хмарний сервіс, який є платформою для автоматизованого та інтерактивного аналізу шкідливого програмного забезпечення. Він поєднує методи статичного та динамічного аналізу для забезпечення глибокого розуміння природи загрози;

– IBM X-Force Exchange – хмарна платформа та сервіс Threat Intelligence, який надає фахівцям з кібербезпеки актуальну інформацію та інструменти для перевірки елементів, пов’язаних із загрозами.

Електронний потік даних усіх співробітників характеризується високим обсягом щоденних вхідних повідомлень. Більшість цих повідомлень автоматично класифікується поштовим клієнтом як небажана кореспонденція (SPAM). Листи, які уникли автоматичного виявлення підозрілості, вимагають ручного втручання співробітника для подальшого інформування про них системи безпеки.

Після реєстрації запиту необхідно провести його первинну обробку для подальшого глибокого розслідування. Для цього інженер безпеки уповноважений розпочати обробку запиту та здійснити перевірку (валідацію) підозрілої URL-адреси.

Зареєстрований інцидент на обслужування інженер безпеки розглядає за допомогою спеціальних інструментів.

Наприклад, інженер завантажує Hybrid Analysis і вводить підозрілу електронну адресу у вікно для подальшого аналізу (рис. 3.1).

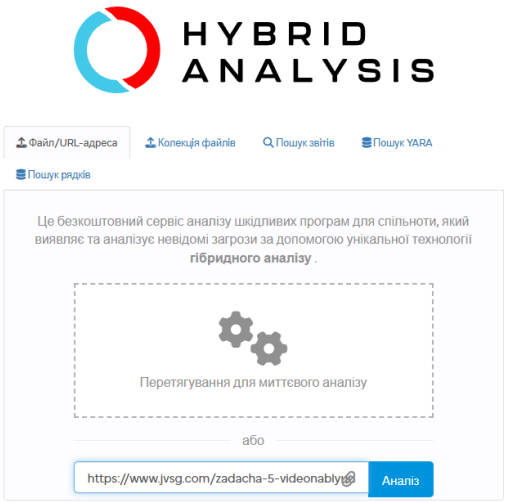

Рисунок 3.1 – Початок перевірки підозрілу електронної адреси у Hybrid Analysis

Після цього у вікні «Аналітичні середовища» фахівець задає необхідні параметри середовища аналізу (рис. 3.2) та запускає перевірку.

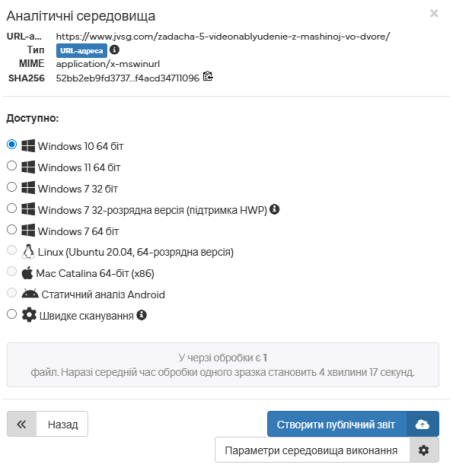

Рисунок 3.2 – Вікно «Аналітичні середовища» Hybrid Analysis

За результатами перевірки фахівець безпеки може переглянути наступні результати детального аналізу антивірусної перевірки: сканування URL-адреси, оцінку шахрайства з доменами, оцінку домена тощо (рис. 3.3).

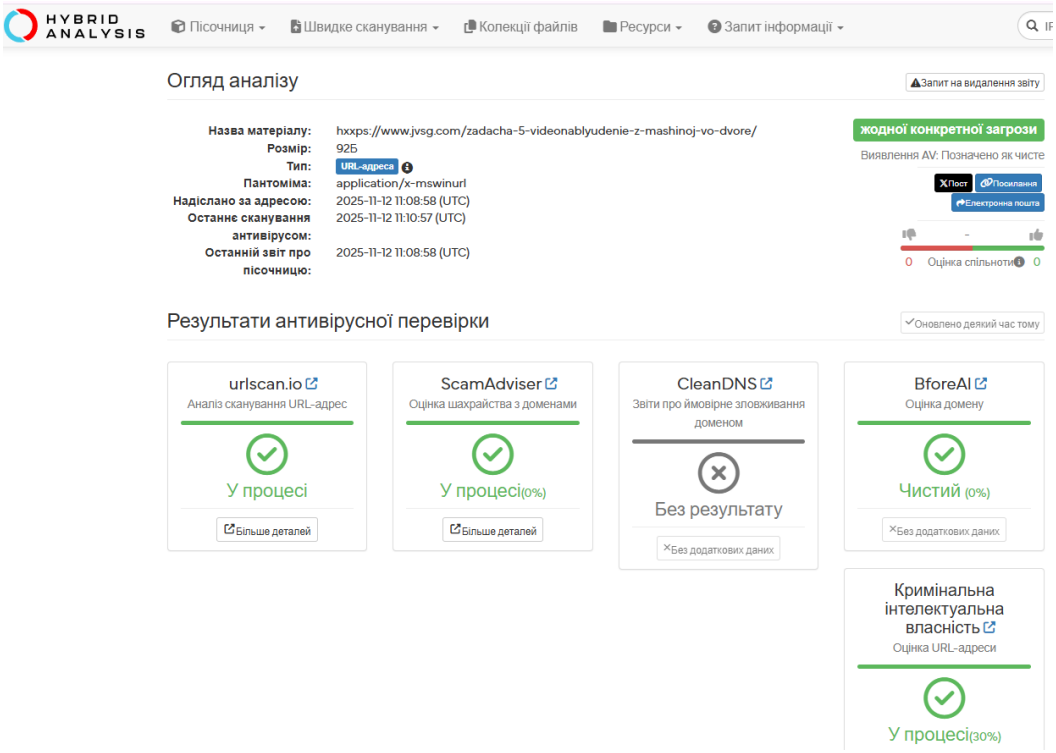

Рисунок 3.3 – Вікно результатів детального аналізу антивірусної перевірки

Зведений звіт перевірки представлений на рисунку 3.4.

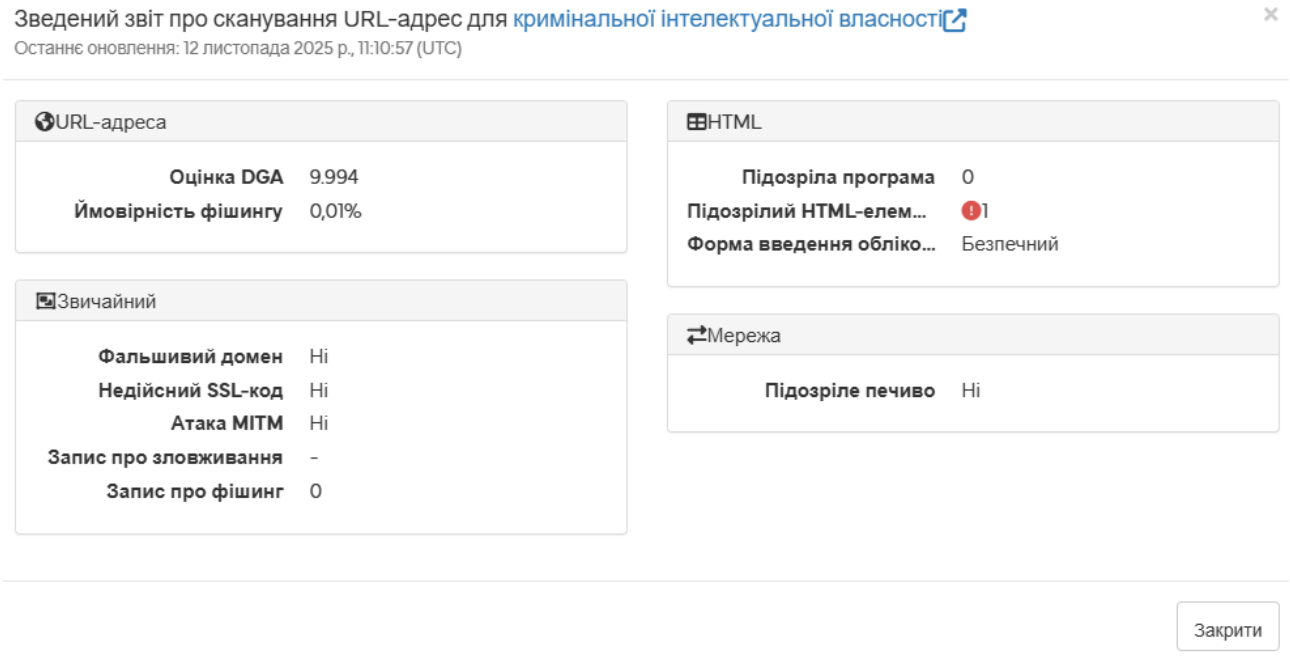

Рисунок 3.4 – Зведений звіт перевірки

У подальшому інженер безпеки здійснює перевірку на Phishing Check з метою визначення того, чи є певний цифровий об’єкт (електронний лист, посилання, веб-сайт) шахрайським і чи не є він частиною фішингової атаки. Для цього він активізує веб-сайт, який перевіряє URL-адреси, і вставляє у відповідне вікно електронну адресу (рис. 3.5).

Рисунок 3.5 – Вікно Office 365 Advanced Thread Protection

Для успішної та повної перевірки електронного листа на предмет фішингу чи шахрайства недостатньо лише аналізувати посилання. Необхідно обов’язково використовувати заголовок електронної пошти, оскільки саме він містить технічні докази, які підтверджують або спростовують легітимність відправника.

Для цього фахівець безпеки копіює код поля заголовка і, використовуючи спеціальний інструмент, аналізує його (рис. 3.6).

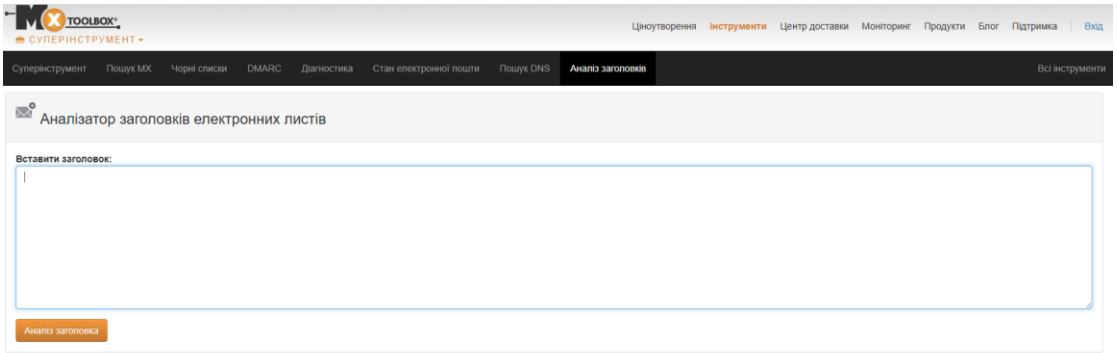

Рисунок 3.6 – Вікно аналізатора MXToolBox

За результатом проведеного аналізу аналізатор видає комплексну, структуровану інформацію, яка перетворює складний, технічний текст заголовка на зрозумілий звіт.

Для захисту листування електронною поштою застосовують протоколи SPF (Sender Policy Framework), DomainKeys (або його розвиток DKIM) та DKIM (DomainKeys Identified Mail), які використовуються для автентифікації електронної пошти і є основною лінією захисту від фішингу та спаму.

SPF дозволяє власнику домену опублікувати в DNS-записі спеціальний TXT-запис, у якому чітко перелічуються всі IP-адреси серверів, які мають право відправляти пошту від імені цього домену.

Коли поштовий сервер отримувача (наприклад, Gmail або корпоративний шлюз) отримує лист, він перевіряє IP-адресу відправника. Якщо IP-адреса не входить до списку, дозволеного SPF-записом, лист позначається як потенційно шахрайський.

У свою чергу, DKIM додає до заголовка кожного вихідного листа унікальний цифровий підпис, створений за допомогою приватного ключа домену. Відповідний публічний ключ публікується у DNS-записі домену.

Сервер отримувача використовує публічний ключ, щоб розшифрувати та перевірити підпис. Якщо підпис співпадає, це підтверджує, що лист був надісланий власником домену. Якщо підпис не співпадає, це означає, що лист був змінений під час транспортування або є підробкою.

Перевірки домену на фішинг можна здійснити низкою потужних онлайн-інструментів та ресурсів, які використовують як фахівці з кібербезпеки, так і звичайні користувачі.

Це може бути VirusTotal, Google Safe Browsing, URLscan.io, Cisco Talos Intelligence тощо.

Представимо перевірку домену на фішинг на основі Cisco Talos Intelligence.

Робоче вікно Cisco Talos Intelligence подано на рисунку 3.7.

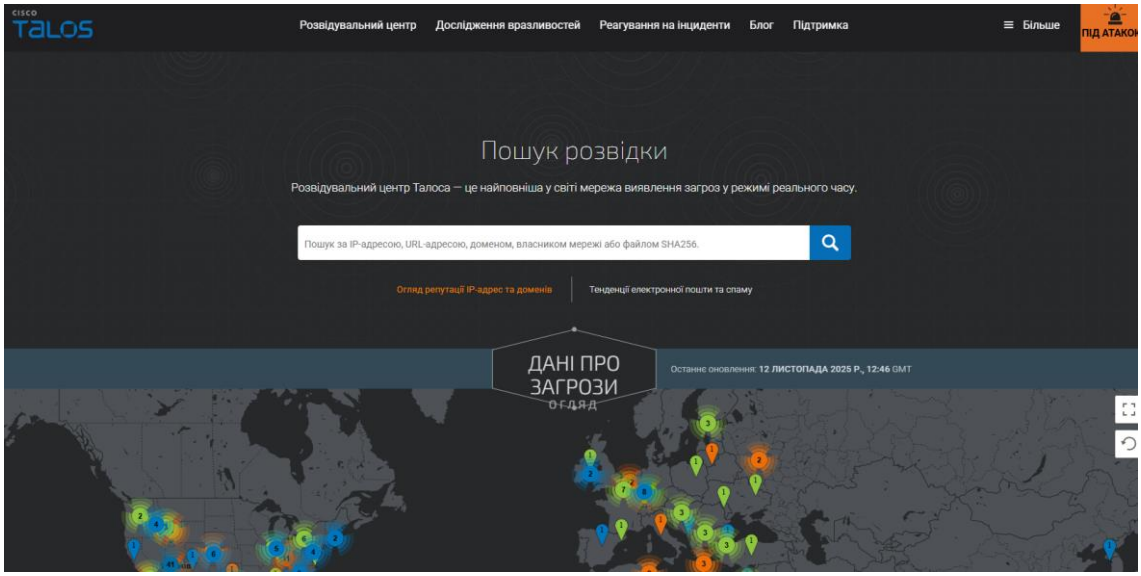

Рисунок 3.7 – Робоче вікно Cisco Talos Intelligence

У відповідну область потрібно ввести адресу домену і підтвердити свій вибір.

За результатами перевірки можна встановити приналежність домену та його репутацію.

Щоб провести аналіз посилань (Uniform Resource Locators) з метою визначення їхньої безпеки та виявлення прихованих загроз, таких як фішинг, шкідливе програмне забезпечення або шахрайство доцільно застосувати сервіс urlscan.io.

Для цього у відповідне поле вставляють електронну адресу та активізувати перевірку.

За результатами перевірки отримаємо повну інформацію про домен: кількість IP-адрес, доменів та HTTP-транзакцій, країну IP-реєстрації та реєстрації доменів і поточний висновок (рис. 3.8).

Щоб переглянути хеш для продовження аналізу за допомогою Vicheck, потрібно використати вкладку IoC. Там можна переглянути хеш-код в останньому рядку.

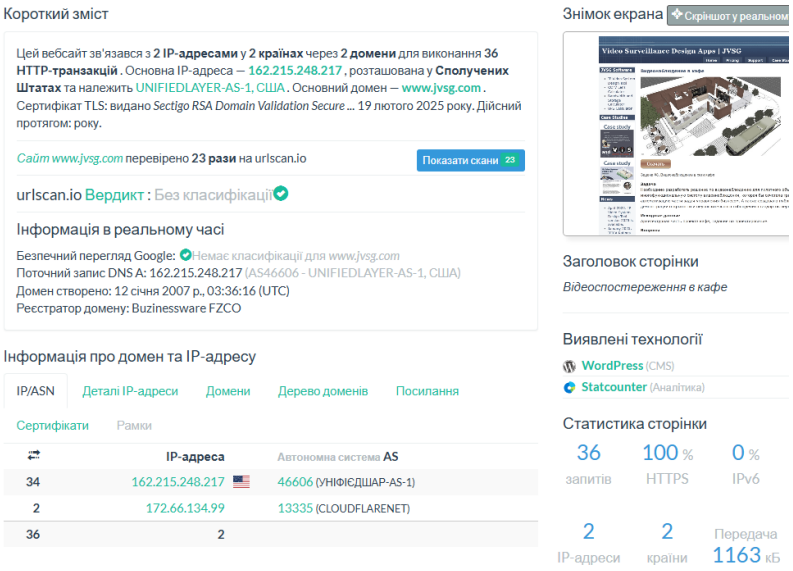

Рисунок 3.8 – Результат перевірки домена в urlscan.io

3.2 Інформація про загрози

Застосування Threat Intelligence є ресурсом знань, який дозволяє фахівцям безпеки перейти від реагування на минулі атаки до прогнозування та запобігання майбутнім.

Загрози в кібербезпеці, які часто є надзвичайно різноманітними, класифікують за окремими групами відповідно до їхнього призначення, джерелом, впливом, або характером дії.

Класифікація за призначенням допомагає фахівцям з безпеки (особливо в SOC) не лише ідентифікувати загрозу, але й передбачити наступні кроки зловмисника та вибрати відповідний сценарій реагування (Playbook).

Типовими загрозами є:

– APT-групи (Advanced Persistent Threats), які використовують цільовий фішинг (Spear Phishing), приховані бекдори, та шпигунське програмне забезпечення (Spyware) для тривалого, непомітного перебування в мережі;

– програми-вимагачі (Ransomware);

– фішинг (Phishing);

– криптоджекінг (Cryptojacking);

– масштабні віруси-вайпери (Wipers);

– DDoS-атаки.

Trusted Feed Sources являє собою надійні джерела потоків даних про загрози, які регулярно публікують або надають структуровані дані для автоматичного завантаження в системи безпеки організації.

Приклади надійних джерел подано в таблиці 3.1.

Таблиця 3.1 – Типи джерел

Тип джерела	Приклади	Принцип довіри
Комерційні	Cisco Talos Intelligence, IBM X-Force Exchange, CrowdStrike Intelligence	Довіра до експертизи та масштабу збору даних від мільйонів кінцевих точок по всьому світу
Державні/Галузеві	CERT-UA (в Україні), CISA (у США), ISACs (Information Sharing and Analysis Centers) для фінансового чи енергетичного сектору	Довіра до офіційних та конфіденційних даних про цільові атаки на критичну інфраструктуру
Відкриті (Open Source)	MalwareBazaar, Abuse.ch, AlienVault OTX	Довіра до спільноти та незалежних дослідників, які активно діляться даними

Інженери безпеки інтегрують ці потоки даних безпосередньо у свої системи SIEM, SOAR та фаєрволи для автоматичного оновлення правил блокування та виявлення.

3.3 Перевірка безпеки програмного забезпечення

Software security check (перевірка безпеки програмного забезпечення) являє собою комплексний набір практик, методологій та інструментів, які використовуються для ідентифікації, аналізу та усунення вразливостей безпеки в програмних додатках та їхньому вихідному коді.

Головна мета цього процесу – гарантувати, що програмне забезпечення не містить лазівок, які зловмисники могли б використати для компрометації системи, крадіжки даних або порушення її функціонування.

Перш ніж додавати програмне забезпечення до схваленого списку, його необхідно перевірити на наявність вразливостей.

Для цього необхідно використати сканери вразливостей, які є на підприємстві.

Щоб перевірити безпеку програмного забезпечення, потрібно переглянути все програмне забезпечення, встановлене на хості, і всі його відповідні вразливості. Для цього необхідно відфільтрувати інформацію за хостом.

Якщо сервіс Qualys не виявляє вразливості, додаткова перевірка іншими рішеннями не потрібна (рис. 3.9).

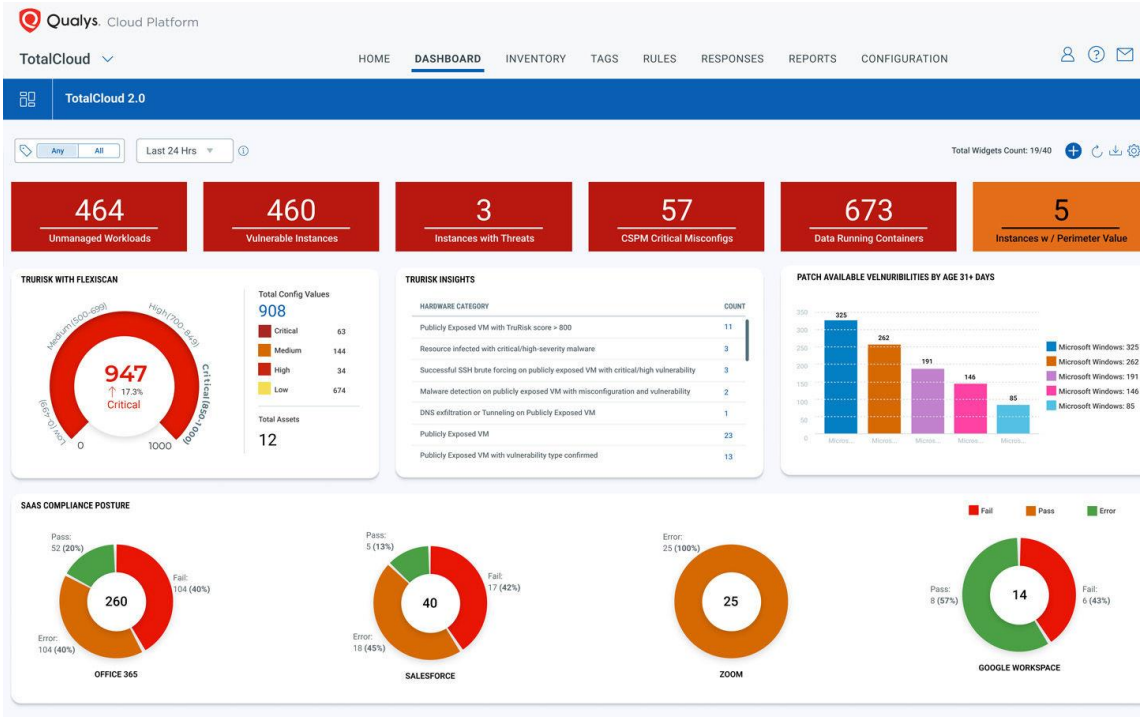

Рисунок 3.9 – Сервіс Qualys

Щоб проаналізувати шкідливі індикатори для файлу можна скористатися сервісом Hybrid Analysis.

Служба Hybrid Analysis – це багатоцільова хмарна платформа, призначена для глибокого та автоматизованого аналізу шкідливого програмного забезпечення та підозрілих файлів. Вона є незамінним інструментом для фахівців із кібербезпеки, які потребують детального розуміння природи та поведінки загрози.

Гібридний аналіз дозволяє ідентифікувати різні шкідливі індикатори, такі як записи реєстру, ін’єкції процесів тощо. Повний список показників див. у підрозділі показників.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

У ході дослідження було здійснено глибокий аналіз різних моделей та типів архітектури Security Operation Center (SOC). Визначено та обґрунтовано фактори, що впливають на вибір конкретної моделі SOC, що стало підґрунтям для розробки рекомендацій щодо оптимальної архітектури Центру безпеки підприємства.

Для формування обґрунтованого вибору SIEM-системи, яка є ключовим елементом SOC, було проаналізовано пропозиції трьох провідних компаній-постачальників. На основі отриманих даних було зроблено висновок, що SIEM-система QRadar від IBM [11] є найбільш ефективним та привабливим рішенням для впровадження на підприємстві.

Впровадження повноцінного Центру безпеки дозволяє суттєво мінімізувати ймовірність реалізації загроз та охоплює критичні аспекти інформаційної та кібербезпеки:

– контроль та моніторинг (постійний моніторинг стану інформаційної безпеки та подій безпеки);

– управління загрозами (аудит дій користувачів, моніторинг та управління вразливими місцями);

– реагування (ефективне управління інцидентами інформаційної безпеки);

– комплаєнс (контроль дотримання вимог міжнародних, промислових та внутрішніх стандартів, а також законодавства).

У практичній частині роботи було розроблено деталізовані алгоритми (плейбуки) реагування на різноманітні види інцидентів. Ці алгоритми значно прискорюють процес розслідування та нейтралізації інцидентів у Центрі безпеки підприємства.

Отримані результати є актуальними та готові до практичного використання підприємствами для побудови центрів оперативного управління кібербезпекою, підвищуючи їхню здатність до ефективного розслідування та протидії загрозам.

ПЕРЕЛІК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. What is a SOC (Security Operations Center). URL: http://securityaffairs.co/wordpress/47631/breaking-news/socsecurity-operations-center.html.

2. Security Information and Event Management. URL: https://www.gartner.com/en/informationtechnology/glossary/security-information-and-event-management-siem.

3. S. David. A Practical Application of SIM/SEM/SIEM / Automating Threat Identification. SANS Institute, 2006. p.3. URL: https://www.sans.org/reading-room/whitepapers/logging/practical-%20applicationsim-sem-siem-automating-threat-identification-1781.pdf .

4. Types of Log Collection Methods. URL: URL: https://support.symantec.com/en_US/article.INFO4456.html.

5. SIEM – Security Information and Event Management. URL: https://amica.ua/siem-security-information-and-eventmanagement/.

6. CERT-UA. URL: https://cert.gov.ua/.

7. Міжнародний стандарт ISO/IEC 27001:2013 «Система управління інформаційною безпекою. Вимоги». URL: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742.

8. Міжнародний стандарт ISO/IEC 27037:2012 «Інформаційні технології. Методи забезпечення безпеки. Настанови щодо ідентифікації, збору, придбання і збереження цифрових даних». URL: http://www.iso.org/iso/catalogue_detail?csnumber=4438.

9. Кореляція SIEM. URL: https://www.securitylab.ru/analytics/431459.php.

10. HPE ArcSight Marketplace. URL: https://marketplace.microfocus.com/arcsight.

11. IBM Security App Exchange Marketplace. URL: https://exchange.xforce.ibmcloud.com/hub.

12. Міжнародний стандарт ISO/IEC 27005:2011 «Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки». URL: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742.

13. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення. URL: http://online.budstandart.com/ru/catalog/doc-page?id_doc=61937.

14. Configuring SNMP and using the NetFlow. URL: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/netflow/configuration/12-4t/nf-12-4t-book/cfg-snmp-mib-mon-nf.html.

15. Kearney, K.T.; Torelli, F. (2011). "The SLA Model". / Wieder, P.; Butler, J.M.; Theilmann, W.; Yahyapour, R. Service Level Agreements for Cloud Computing. Springer Science+Business Media, 2011. – pp. 43–68.

16. COBIT - Цілі контролю за інформаційними та суміжними технологіями, 2012 р..