МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “СТВОРЕННЯ ІМІТАЦІЙНИХ МОДЕЛЕЙ КІБЕРАТАК ДЛЯ ЕФЕКТИВНОГО НАВЧАННЯ ТА ТРЕНУВАННЯ СПІВРОБІТНИКІВ SOC”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Максим БОЙКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач(ка) вищої освіти гр. УБД-42

Максим БОЙКО
Ім’я, ПРІЗВИЩЕ

Керівник: Дмитро РАБЧУН
К.т.н. Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бойку Максиму Андрійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Створення імітаційних моделей кібератак для ефективного навчання та тренування співробітників SOC”,
керівник кваліфікаційної роботи РАБЧУН Дмитро, к.т.н.,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “__“ березня 2024 р. №__.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *процеси інформаційної безпеки, процеси навчання Security Operation Center, методи створення імітаційних моделей кібератак, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати сучасні кібератаки.
4.2. Дослідити основні характеристики технологій виявлення та реагування в Security Operation Center.
4.3. Вивчити інструменти та методи створення імітаційних моделей кібератак й навчання персоналу з інформаційної безпеки.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз особливостей сучасних кібератак та загроз.	08.04.2024	
4.	Дослідження основних характеристик технологій виявлення та реагування на кібератаки.	22.04.2024	
5.	Вивчення інструментів та методів створення імітаційних моделей кібератак та навчання співробітників SOC.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

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

Керівник
кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Бойко М.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Створення імітаційних моделей кібератак для ефективного навчання та тренування співробітників SOC"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач БОЙКО Максим у кваліфікаційній роботі дослідив сучасні методи створення імітаційних моделей кібератак та їх використання для ефективного навчання та тренування співробітників Центру кіберзахисту. Він проаналізував ключові аспекти і виклики, що виникають перед сучасними SOC, зосередив увагу на значенні імітаційних тренувань для підвищення рівня захищеності інформаційних систем. Здобувач розробив практичні рекомендації з оптимізації навчальних процесів та підготував матеріали, що можуть бути використані для систематичного тренування співробітників.

Здобувач продемонстрував розуміння досліджуваної проблеми, здатність застосовувати теоретичні знання та вміння вирішувати задачі в області кібербезпеки.. Результати його роботи були представлені на наукових конференції.

Враховуючи вищевикладене, кваліфікаційна робота здобувача заслуговує оцінки "відмінно" та він заслуговує на присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Бойко М.А. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти БОЙКА Максима
на тему “Створення імітаційних моделей кібератак для ефективного навчання та тренування співробітників SOC”

Актуальність. У сучасному світі, де кіберзагрози стають все більш витонченими та руйнівними, важливість імітаційних моделей кібератак для підготовки співробітників SOC (Security Operations Center) є високою. Враховуючи постійне оновлення методів атак кіберзлочинців, необхідно постійно розвивати та удосконалювати захист інформації. Такі моделі дозволяють ефективно симулювати різноманітні кібератаки, що забезпечує персоналу можливість відпрацювання реакцій на реальні загрози у безпечному середовищі.

Отже, розробка імітаційних моделей є актуальним завданням, яке відповідає сучасним вимогам кібербезпеки.

Позитивні сторони.

1. В роботі проаналізовано різні типи кібератак та методики їх імітації, що є цінним внеском у розвиток методів тренування співробітників SOC.
2. Матеріал кваліфікаційної роботи подано чітко та послідовно, з дотриманням наукового стилю і відповідно до академічних стандартів. Робота багата ілюстративними матеріалами, які допомагають краще зрозуміти суть імітаційних моделей.
3. Автор детально вивчив велику кількість наукових публікацій та джерел, що свідчить про грунтовну підготовку.
4. На основі аналізу представлені практичні рекомендації для покращення імітаційних тренувань, що можуть бути корисними для розробників тренінгових програм та керівників SOC.

Недоліки.

Хоча робота і є якісною, було б корисно розширити дослідження за допомогою експертиз, що демонструють реальне застосування розроблених імітаційних моделей у навчанні співробітників. Також можна було б детальніше розглянути використання штучного інтелекту для автоматизації симуляцій.

Висновок: Кваліфікаційна робота виконана на високому науковому і методичному рівні та заслуговує оцінки "відмінно". Здобувач заслуговує на високу оцінку за свій внесок у підготовку кадрів у галузі кібербезпеки та заслуговує на присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____

підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технологій створення імітаційних моделей кібератак для ефективного навчання та тренування співробітників SOC (Security Operations Center). Робота складається зі вступу, трьох розділів, що містять 11 рисунків, висновків і списку використаних джерел із 45 найменувань. Загальний обсяг роботи становить 74 аркушів, з яких 5 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження технологій створення імітаційних моделей кібератак для підвищення ефективності навчання та тренування співробітників SOC.

Об'єктом дослідження є процеси забезпечення інформаційної безпеки за допомогою імітаційних моделей кібератак.

Предмет дослідження – особливості застосування імітаційних моделей кібератак для навчання та тренування співробітників SOC.

Методи дослідження. Для вирішення зазначеного наукового завдання в роботі використані методи аналізу та синтезу, порівняння, моделювання, класифікації, експертної оцінки, а також системного підходу до управління інформаційною безпекою.

Як результат у роботі проаналізовано сучасні кібератаки та загрози, визначено роль SOC у забезпеченні інформаційної безпеки, розроблено методику створення імітаційних моделей кібератак та інструменти для їх проведення. Вивчено способи моніторингу, контролю безпеки та оцінки процесів SOC на основі результатів імітаційних атак.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства, а також при проведенні навчання та тренування співробітників SOC.

Ключові слова: ІМІТАЦІЙНІ МОДЕЛІ КІБЕРАТАК, НАВЧАННЯ СПІВРОБІТНИКІВ, SOC.

ABSTRACT

The qualification work is dedicated to exploring the technologies for creating simulation models of cyber attacks for effective training and practice of Security Operations Center (SOC) employees. The work consists of an introduction, three chapters containing 11 figures, conclusions, and a list of 45 references. The total volume of the thesis is 74 pages, of which 5 pages are dedicated to a list of abbreviations and the list of references.

The purpose of the study is to research the technologies for creating simulation models of cyber attacks to enhance the effectiveness of training and practice for SOC employees.

The object of study is the processes of ensuring information security through simulation models of cyber attacks.

The subject of study is the features of using simulation models of cyber attacks for the training and practice of SOC employees.

Research methods. To solve the stated scientific task, methods of analysis and synthesis, comparison, modeling, classification, expert assessment, and a systematic approach to information security management were used.

As a result, the thesis analyzes modern cyber attacks and threats, defines the role of the SOC in ensuring information security, develops a methodology for creating simulation models of cyber attacks and tools for their execution. Methods for monitoring, security control, and assessment of SOC processes based on the results of simulation attacks are studied.

Field of application. The developed approaches can be used in the planning and implementation of an enterprise's information security management system, as well as in the training and practice of SOC employees.

Keywords: SIMULATION MODELS OF CYBER ATTACKS, TRAINING EMPLOYEES, SOC.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ПЗ	Програмне забезпечення
SOC	Система управління базами даних
SIEM	Система управління інформаційною безпекою

ВСТУП

У сучасному світі, де щоденно відбуваються тисячі кібератак на державні установи, корпорації та приватних користувачів, питання забезпечення інформаційної безпеки набуває все більшої ваги. Розвиток інформаційних технологій збільшує кількість потенційних вразливостей у системах безпеки, що вимагає від організацій невпинного зміцнення своїх захисних процесів, механізмів та контролів. Особлива увага при цьому приділяється розвитку здатностей оперативно реагувати на кіберзагрози через навчання та тренування співробітників, що є критичним аспектом підтримки високого рівня інформаційної безпеки. Особливо актуальним є питання підготовки співробітників Security Operation Center (Центру кібербезпеки або SOC), які є першою лінією оборони в боротьбі з кіберзагрозами. Ефективне навчання та тренування співробітників SOC не тільки мають забезпечити здатність швидко реагувати на інциденти, але й сприяти розробці стратегій проактивного протистояння потенційним атакам. В цьому контексті, створення імітаційних моделей кібератак відіграє важливу роль у формуванні практичних навичок та глибокого розуміння загроз серед спеціалістів.

Мета роботи полягає в розробці імітаційної моделі кібератаки, яка відтворює сценарій зловмисних дій для ефективного навчання та тренування співробітників SOC.

Об’єкт дослідження – впровадження імітаційних атак в процеси інформаційної безпеки, зокрема в процеси Security Operations Centers (SOC).

Предмет дослідження - методи та техніки для забезпечення імітацій кібератак, зокрема розробка сценарію кібератаки.

Методи дослідження. У дослідженні використовуються комбіновані методи, включаючи аналіз кращих міжнародних практик в галузі кібербезпеки та семантичне моделювання.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу організаціям отримати інструмент та модель імітації кібератак для

підвищення кіберстійкості через тренування персоналу SOC. Результати дослідження дозволяють створити масштабовані та ефективні моделі атак, які можуть бути адаптовані під потреби різних організацій. Це сприяє зменшенню часу реакції на інциденти, покращенню аналітичних здібностей співробітників та зниженню ризику втрати даних або порушення роботи систем.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

РОЗДІЛ 1 КІБЕРАТАКИ ТА ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Аналіз сучасних кібератак та загроз

Перед початком дослідження необхідно розглянути атрибути інформаційної безпеки та визначення поняття загроз в інформаційній безпеці, кібератаки в свою чергу є одними з типів загроз інформаційній безпеці [1-3].

Тріада інформаційної безпеки, відома також як "CIA тріада", складається з трьох основних атрибутів (компонентів): конфіденційність (Confidentiality), цілісність (Integrity) та доступність (Availability).

Ці три принципи є фундаментальними для забезпечення безпеки інформаційних систем і даних.

Конфіденційність (Confidentiality):

Атрибут конфіденційність означає захист інформації від несанкціонованого доступу та розкриття. Це забезпечує, що лише авторизовані користувачі (процеси, активи) мають доступ до певної інформації. Методи захисту конфіденційності включають шифрування, контроль доступу, автентифікацію користувачів, а також політики та процедури, які обмежують доступ до конфіденційних даних [4].

Цілісність (Integrity):

Атрибут цілісність забезпечує, що інформація залишається точною (коректною) і не була змінена або пошкоджена будь-яким несанкціонованим способом. Це означає, що дані повинні зберігати свою точність і надійність протягом усього їхнього життєвого циклу. Методи захисту цілісності включають контроль доступу до редагування та видалення, контроль версій програми або документа, використання хеш-функцій та цифрових підписів, а також регулярні перевірки та аудит даних .

Доступність (Availability):

Атрибут доступність забезпечує, що інформація та ресурси системи доступні для авторизованих користувачів, коли вони потрібні. Це включає в себе захист системи від атак, які можуть призвести до відмови в обслуговуванні (Denial of Service, DoS), резервне копіювання даних, відновлення після збоїв, а також належне управління ресурсами і оновлення систем [5-8].

Усі три компоненти тріади мають важливе значення і повинні бути збалансовані в рамках загальних процесів забезпечення інформаційної безпеки [9-10]. Конфіденційність гарантує, що інформація захищена від несанкціонованого доступу, цілісність забезпечує, що інформація залишається точною та надійною, а доступність забезпечує, що інформація доступна тоді, коли вона потрібна [11].

Загроза – це потенційна можливість нанесення шкоди інформаційним ресурсам шляхом порушення конфіденційності, цілісності або доступності інформації. Загрози можуть бути внутрішніми або зовнішніми, випадковими або навмисними, а також техногенного, природного або соціального характеру [12].

Загрози інформаційної безпеки можна класифікувати за різними критеріями:

- За аспектом інформаційної безпеки, на який спрямовані загрози:

Загрози конфіденційності виникають, коли несанкціоновані особи отримують доступ до конфіденційної інформації. Випадки порушення конфіденційності можуть бути спричинені людським фактором (випадковим наданням прав доступу), збоями у програмному або апаратному забезпеченні та умисним зламом систем. До конфіденційної інформації належить державна таємниця, комерційна таємниця, персональні дані та інші види професійних таємниць [13].

Загрози цілісності пов'язані з можливістю модифікації інформації, що зберігається в інформаційній системі. Порушення цілісності може бути спричинене як навмисними діями персоналу або зовнішніх зловмисників, так і технічними неполадками.

Загрози доступності створюють умови за яких доступ до інформаційних ресурсів стає неможливим або затрудненим, що перешкоджає функціонуванню бізнес-процесів організації.

- За розташуванням джерела загроз:

Внутрішні загрози – джерела загроз знаходяться всередині системи.

Зовнішні загрози – джерела загроз розташовані поза системою.

- За розмірами завданого збитку:

Загальні загрози – завдають значної шкоди всій системі.

Локальні загрози – завдають шкоди окремим частинам системи.

Приватні загрози – завдають шкоди окремим властивостям елементів системи.

- За ступенем впливу на інформаційну систему:

Пасивні загрози – структура і зміст системи не змінюються

Активні загрози – структура і зміст системи піддаються змінам.

- За природою виникнення:

Природні загрози – викликані фізичними процесами або стихійними явищами, незалежними від волі людини.

Штучні загрози – спричинені діями людини. Серед них можна виділити:

Ненавмисні загрози – помилки програмного забезпечення, персоналу, збої в роботі систем, відмови техніки.

Навмисні загрози – несанкціонований доступ до інформації, розробка та використання спеціального програмного забезпечення для здійснення неправомірного доступу, створення та розповсюдження вірусних програм.

Основні проблеми інформаційної безпеки пов'язані з умисними загрозами, які є головною причиною злочинів та правопорушень.

Кібератаки є основною реалізацією умисних загроз інформаційній безпеці, використовуючи різні методи для експлуатації вразливостей та соціальної інженерії. Розуміння цих зв'язків дозволяє розробляти ефективні заходи захисту та забезпечувати конфіденційність, цілісність і доступність інформаційних ресурсів [14-15].

Кібератака – це навмисна дія, яка виконується окремими особами, групами або державно фінансованими організаціями за допомогою комп'ютерних систем, мереж або технологічно залежних підприємств з метою несанкціонованого доступу, зміни, крадіжки або знищення даних, порушення нормальної роботи комп'ютерних систем чи мереж. Атаки використовують зловмисне програмне забезпечення для зміни комп'ютерного коду, логіки роботи систем або даних. Основною метою зловмисників може бути отримання фінансової вигоди, завдання політичного або соціального впливу, шпигунство, а також просто завдання шкоди активам чи репутації цілі [16-18].

До найпоширеніших видів кібератак сьогодні можна віднести:

• Фішингові атаки. Передбачають надсилання шахрайських електронних листів або повідомлень, які нібито надходять із законного джерела та мають легітимний вміст. Мета атаки полягає в тому, щоб обманом змусити одержувача розкрити конфіденційну інформацію, таку як персональні дані, дані особистого або корпоративного облікового запису (логін, пароль, код двохфакторної аутентифікації) або фінансові дані (номер банківської картки, CVV-код). Атака є дуже поширеною завдяки своїй простоті та ефективності. Зловмисники часто використовують привабливі висловлювання, щоб спонукати до негайних дій, як-от повідомлення про компрометацію облікового запису або винагорода за виграш у лотереї. Окрім отримання конфіденційних даних, зловмисники можуть помістити в листи шкідливе програмне забезпечення, встановлення якого жертвою забезпечить негативний вплив на атаковану систему.

• Розподілена атака типу "відмова в обслуговуванні" (DDoS). DDoS-атаки перевантажують цільову систему, мережу або веб-сайт потоком інтернет-трафіку, роблячи його недоступним для користувачів. Атака може спричинити значні простої та фінансові втрати, особливо для підприємств, які покладаються на веб-ресурси та онлайн-операції. Атакуючі використовують ботнети – мережі зламаних комп'ютерів, що контролюються зловмисниками для одночасного надсилання великої кількості запитів до цільового ресурсу.

- WEB-атаки. Атака включає виконання зловмисних HTTP-запитів або SQL-запитів до веб-застосунків (веб-ресурсів) та баз даних (як частин веб-ресурсів або окремих цілей). Подібні атаки здебільшого використовують вразливості веб-серверів та баз даних, включаючи некоректну конфігурацію цільових ресурсів. До основних видів веб-атак належать SQL-ін'єкції, XSS (міжсайтові скрипти) та атаки за допомогою вразливостей в HTTP-заголовках.

- APT-атаки (Advanced Persistent Threat). Складні та тривалі кібератаки, які виконуються висококваліфікованими зловмисниками, часто з підтримкою держав. Ці атаки цілеспрямовано використовуються проти певних організацій або державних структур з метою крадіжки конфіденційної інформації, шпигунства або забезпечення тривалого впливу на цільові системи. APT-атаки можуть тривати протягом тривалого часу, залишаючись непомітними, і включати багатоступеневі методи проникнення та розповсюдження в системах жертви.

- Віруси-вимагачі (Ransomware). Ці атаки включають шифрування файлів жертви за допомогою спеціального зловмисного програмного забезпечення з подальшою вимогою викупу за відновлення доступу до даних. Зловмисники можуть погрожувати оприлюдненням або продажем конфіденційної інформації, якщо викуп не буде сплачений. Цей тип атак може бути спрямований як на окремих користувачів, так і на великі організації, включаючи лікарні, банки та урядові установи.

- Атаки на постачальників (Supply Chain Attacks). Атаки на постачальників включають компрометацію програмного забезпечення або апаратного забезпечення в ланцюгу постачання організації, що дозволяє зловмисникам отримати доступ до систем кінцевих користувачів. Ці атаки можуть бути надзвичайно складними та мати значний вплив, оскільки часто охоплюють широкий спектр організацій, які використовують зламаний продукт або послугу інших виробників (вендорів).

- Зловмисне програмне забезпечення (Malware). Зловмисне програмне забезпечення включає різні типи шкідливих програм, такі як віруси, трояни,

черви та шпигунські програми. Ці програми можуть виконувати різноманітні дії, включаючи крадіжку даних, пошкодження системи або надання зловмисникам доступу до мережі. Віруси та черви можуть самовідтворюватися і поширюватися через мережі, тоді як трояни часто маскуються під легітимні програми для проникнення в систему.

- Атаки з використанням соціальної інженерії. Цей тип атак передбачає маніпулювання людьми для отримання конфіденційної інформації або доступу до системи. Атакуючі можуть використовувати психологічні трюки, щоб змусити жертву розкрити паролі, відповісти на фішингові повідомлення або виконати дії, що порушують безпеку системи. Соціальна інженерія може бути дуже ефективною, оскільки вона експлуатує людські слабкості, такі як довірливість або бажання допомогти.

- Викрадення сесій (Session Hijacking). Ця атака передбачає перехоплення пакетів сесії користувача, що дозволяє зловмиснику отримати доступ до облікового запису жертви без її відома. Зловмисники можуть використовувати методи, такі як перехоплення трафіку або маніпулювання веб-додатками, щоб викрасти сесійні ідентифікатори і отримати контроль над обліковими записами.

- Атаки на інфраструктуру Інтернету речей (IoT). Зі збільшенням кількості підключених до Інтернету пристроїв, атаки на IoT стають все більш поширеними. Зловмисники можуть використовувати слабкі місця в безпеці IoT-пристроїв для отримання доступу до мережі, викрадення даних або навіть створення ботнетів з пристроїв IoT для здійснення DDoS-атак.

Сучасні кібератаки та кіберзагрози стають все більш складними та різноманітними, що вимагає від організацій постійного моніторингу та вдосконалення систем захисту. Актуальність питання захисту інформаційних систем не може бути переоцінена, оскільки кібератаки можуть призвести до значних фінансових втрат, компрометації конфіденційної інформації та порушення нормального функціонування організацій. Вивчення та розуміння сучасних методів атак є критичним для розробки ефективних стратегій протидії та забезпечення кіберстійкості.

Для розуміння того, як зловмисники проникають у мережі та інші комп’ютерні системи, здійснюють атаки та досягають своїх цілей, можна розглянути концептуальну модель стадій кібератаки Cyber Kill Chain від американської компанії Lockheed Martin. Ця модель включає сім основних фаз атаки (рис. 1.1) [19-20]:

1. Розвідка – атакуючий збирає інформацію про ціль, щоб виявити потенційні вразливості. Це може включати збір даних про системи, працівників, технологічні процеси тощо.

2. Озброєння – зловмисник створює шкідливе програмне забезпечення (наприклад, троянці, віруси) або підготовлює інші інструменти для атаки, об'єднуючи їх з експлойтами для використання виявлених вразливостей.

3. Доставка – шкідливе програмне забезпечення або експлойт доставляється до цілі через різні канали, такі як електронна пошта, веб-сайти, зовнішні накопичувачі, соціальна інженерія тощо.

4. Експлуатація – шкідливе ПЗ активується на цільовій системі, використовуючи знайдені вразливості для отримання доступу або контролю над системою.

5. Встановлення – шкідливе ПЗ встановлюється на цільовому обладнанні, забезпечуючи атакуючому стабільний доступ до системи.

6. Команди та контроль – шкідливе ПЗ встановлює зв'язок з зовнішнім керуючим сервером, що дозволяє атакуючому керувати зараженою системою.

7. Дії над об’єктами – на цьому кінцевому етапі атакуючий виконує свої основні завдання, які можуть включати крадіжку даних, зміну або знищення даних, перешкоджання роботі системи тощо.

Модель Cyber Kill Chain надає змогу ефективно аналізувати і покращувати розуміння методів зловмисників, ідентифікувати слабкі місця систем на різних стадіях атаки та розробляти механізми захисту, що відповідають кожному етапу. Зокрема, модель слугує орієнтиром для створення імітаційних атак та їх семантичних моделей.

Застосування Cyber Kill Chain в процесі створення імітаційних моделей кібератак дозволяє краще зрозуміти послідовність дій зловмисників, що підвищує якість відтворення реальних кібератак [21].

Завдяки розумінню кожної фази атаки, організації можуть впроваджувати проактивні заходи безпеки, такі як виявлення та блокування шкідливого програмного забезпечення на етапі доставки або встановлення.

Розробка стратегій та контролів захисту, що базуються на моделі Cyber Kill Chain, сприяє підвищенню стійкості організації до кібератак шляхом зменшення вразливостей та покращення процесів реагування на інциденти [22].

Модель Cyber Kill Chain є ефективним інструментом для аналізу та покращення кібербезпеки. Вона дозволяє організаціям систематично підходити до захисту своїх активів, ідентифікуючи та усуваючи слабкі місця на кожній стадії можливих кібератак [23].

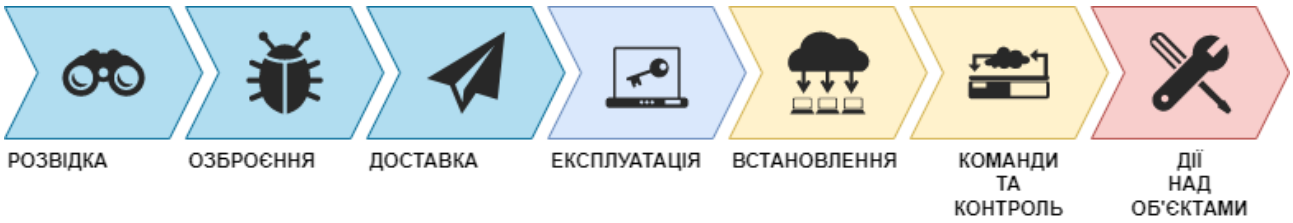

Рис. 1.1 Фази атаки згідно моделі Cyber Kill Chain

1.2 Активи в інформаційній безпеці

У сфері інформаційної безпеки «активи» (assets) стосуються будь-яких цінних інформаційних об’єктів та суб’єктів в організації, які необхідно захистити від загроз безпеці [24].

Активи можуть включати:

Апаратні засоби – ця категорія охоплює фізичні пристрої, такі як комп’ютери, сервери, мережеве обладнання та мобільні пристрої. Захист цих

активів передбачає захист від несанкціонованого доступу, крадіжки та пошкодження.

Програмне забезпечення – сюди входять операційні системи, програми та бази даних. Активи програмного забезпечення захищені регулярними оновленнями, виправленнями та керуванням дозволами користувачів для запобігання зараженню зловмисним програмним забезпеченням і несанкціонованому доступу.

Активи даних – дані є одним із найважливіших активів будь-якої організації. Сюди входить інформація про клієнтів, фінансові записи, приватні дослідження та інша конфіденційна інформація. Захист даних передбачає шифрування, контроль доступу та стратегії резервного копіювання, щоб запобігти витоку та втраті даних.

Інтелектуальна власність – патенти, товарні знаки та власні процеси є ключовими активами для багатьох організацій. Захист інтелектуальної власності передбачає юридичні заходи, а також методи безпеки IT, як-от контроль доступу та шифрування даних.

Персонал – співробітники також вважаються активами, оскільки вони володіють знаннями та навичками, які мають вирішальне значення для роботи організації. Навчання співробітників обізнаності з кібербезпекою та передовим практикам допомагає захистити від атак соціальної інженерії та внутрішніх загроз.

Захист цих активів передбачає поєднання технічних засобів контролю, політик і процедур, призначених для зменшення ризиків і реагування на потенційні загрози.

Інформаційний актив є ціллю реальних та імітаційних кібератак, тому глибокий аналіз власниками (захисниками) активів їх властивостей та вразливостей дозволяє забезпечити безпечне функціонування систем [25-26].

Грамотне управління активами включає в себе ідентифікацію (рис. 1.2) критичних активів, оцінку ризиків та впровадження адекватних заходів захисту, таких як шифрування, резервне копіювання даних, контроль доступу, а також

навчання персоналу принципам кібербезпеки. Це допомагає організаціям зменшити ймовірність успішних кібератак і мінімізувати потенційні збитки від них.

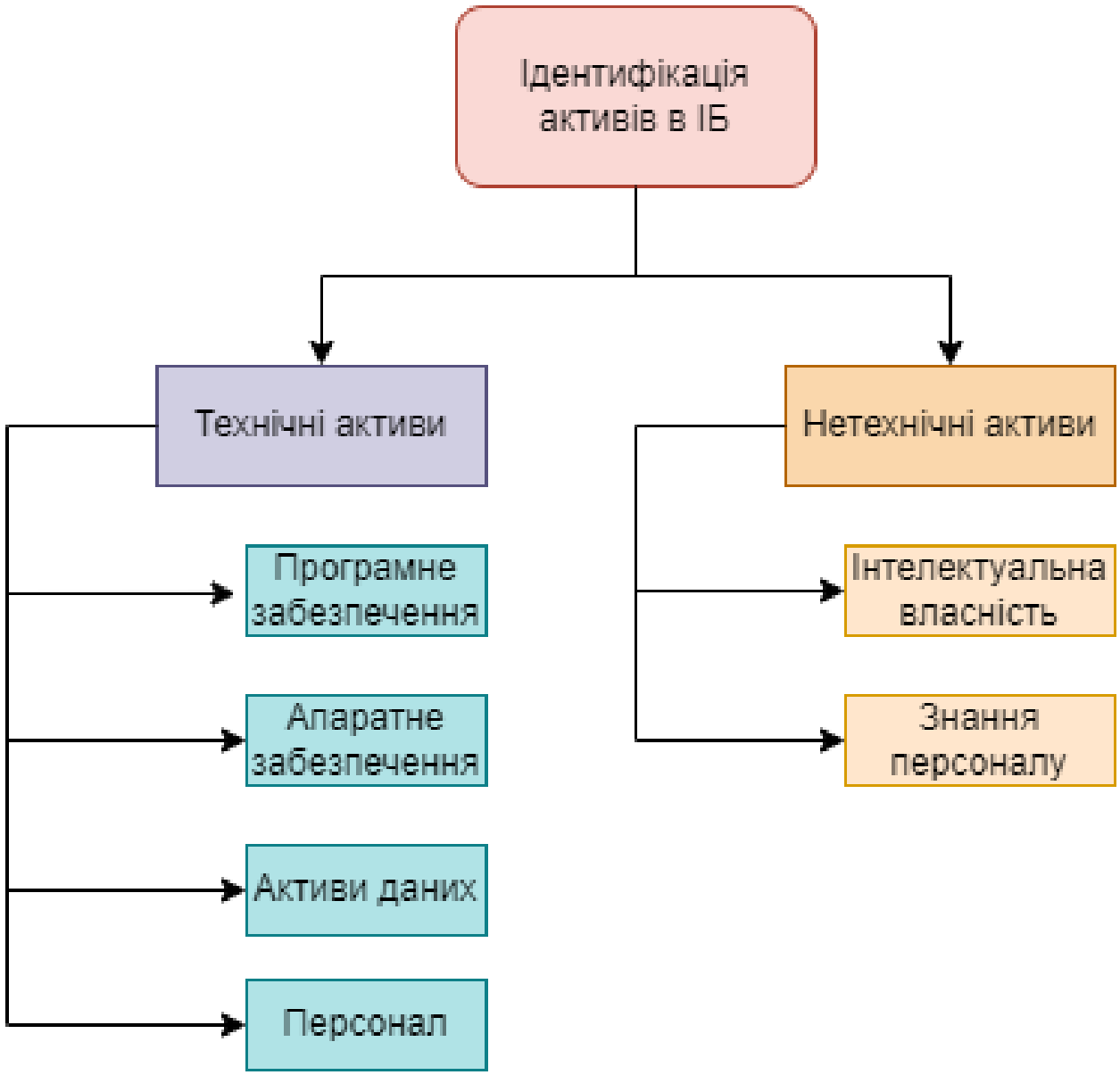

Рис. 1.2 Схема ідентифікації категорії активів

1.3 Роль SOC в забезпеченні інформаційної безпеки

Security Operation Center (SOC) або Центр кібербезпеки є ключовим елементом у структурі забезпечення інформаційної безпеки організації та є

головною частиною в організаційній структурі відділу (департаменту) ІБ організації. SOC відіграє важливу роль у виявленні, аналізі та реагуванні на кібератаки, а також у забезпеченні неперервного захисту інформаційних систем та активів від нових та вже відомих загроз ІБ [27].

Основні аспекти роботи (процеси) SOC включають:

1. Моніторинг та аналіз – SOC використовує різноманітні інструменти для постійного моніторингу мережі, систем та додатків на наявність потенційних загроз. Це дозволяє оперативно виявляти аномалії та підозрілі дії.

2. Реагування на інциденти – коли загроза або кібератака виявлена, SOC координує процес реагування, який може включати ізоляцію заражених систем, аналіз зловмисного програмного забезпечення та відновлення нормальної роботи систем.

3. Прогнозування та запобігання – SOC аналізує існуючі загрози і розробляє стратегії для запобігання майбутнім атакам, включаючи вдосконалення захисту систем та проведення навчань для співробітників.

4. Дотримання нормативних вимог – SOC допомагає організації виконувати вимоги до інформаційної безпеки, встановлені законодавством і стандартами галузі, забезпечуючи аудит та звітність.

5. Співпраця з іншими відділами – SOC тісно співпрацює з IT-відділом, керівництвом та іншими підрозділами організації для координації заходів із забезпечення безпеки.

6. Постійне вдосконалення – SOC постійно аналізує ефективність існуючих заходів безпеки та шукає шляхи для їх покращення, зокрема через впровадження нових технологій і підходів.

Роль SOC є особливо важливою в контексті швидкого розвитку кіберзагроз та постійної еволюції методів кібератак. Завдяки SOC організація може ефективно захищати свої активи та мінімізувати ризики втрати даних чи неправомірного доступу до інформаційних систем [28-29].

Структура SOC у комерційних організаціях може варіюватися в залежності від розміру та потреб організації, але основні елементи зазвичай включають:

• Керівництво – SOC Manager або керівник з кібербезпеки, який відповідає за загальне управління центром, стратегічне планування та координацію з іншими відділами.

• Аналітики безпеки (SOC аналітики) – спеціалісти, які безпосередньо працюють з моніторингом, виявленням аномалій та аналізом потенційних загроз. Вони зазвичай поділяються на аналітиків різних рівнів:

SOC Tier 1, які відповідають за початковий моніторинг і виявлення тривог;

SOC Tier 2, які займаються детальним аналізом виявлених інцидентів та координацією реагування.

• Інженери безпеки – спеціалісти підтримки та налаштування рішень інформаційної безпеки, таких як SIEM (Security Information and Event Management), NGFW (Next Generation Firewall), WAF (Web Application Firewall), EDR (Endpoint Detection and Response), AV (Antivirus), MG (Messaging Gateway) та інших систем. Вони також працюють над впровадженням змін у захист, що базується на аналізі загроз.

• Команда інцидентного реагування (Incident Response Team) – група, яка займається реагуванням на інциденти безпеки. Вони відповідають за ізоляцію заражених систем, видалення шкідливого ПЗ, відновлення даних та вживання заходів для запобігання повторному виникненню подібних інцидентів.

• Група дотримання нормативних вимог (Compliance and Audit Team) – члени цієї групи займаються перевіркою та забезпеченням дотримання організацією встановлених стандартів і нормативів безпеки. Вони також проводять регулярні аудити та підготовку звітів.

У великих організаціях відділ інформаційної безпеки, що включає SOC, можна умовно розділити на три команди в рамках процесів імітацій кібератак:

• Червона команда (Red Team): Імітує дії порушників та забезпечує здійснення імітаційних атак.

• Пурпурова команда (Purple Team): Координує дії червоної команди та аналітиків SOC, аналізує результати проведення імітаційних атак та переглядає аналітичні звіти червоної та синьої команд.

• Синя команда (Blue Team): Включає аналітиків безпеки (SOC аналітиків) та співробітників команди реагування.

Розглянемо поширену структуру Центру кібербезпеки та відділу ІБ на схемі взаємодії з іншими департаментами (відділами) організації (рис. 1.2) [30-33].

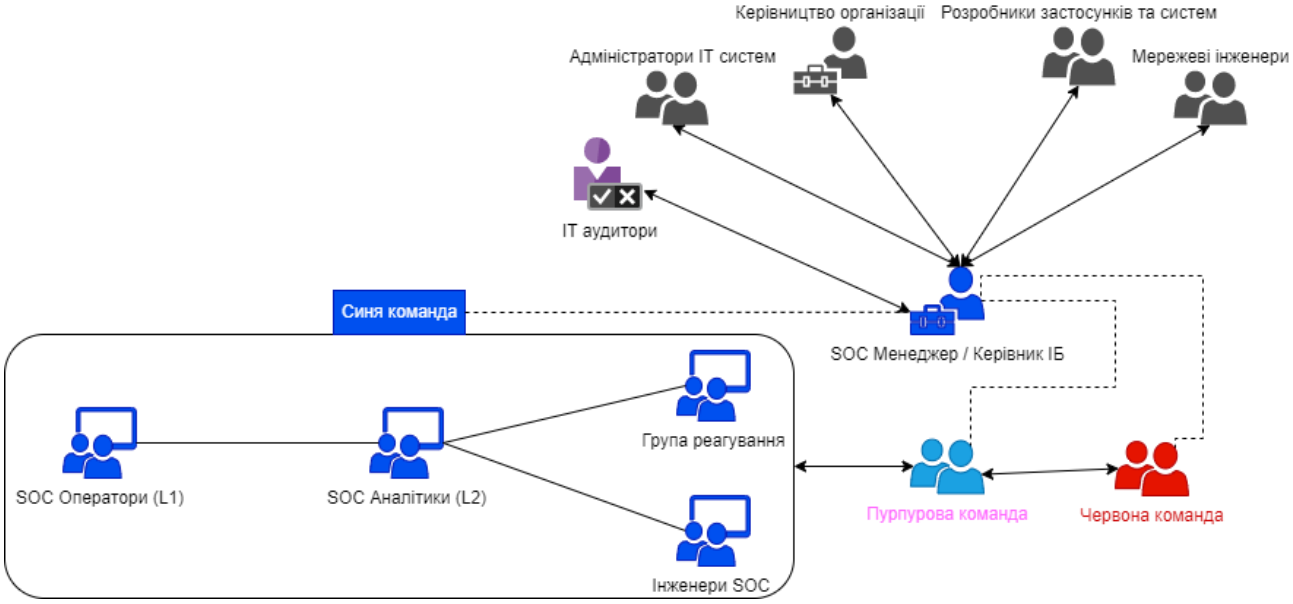

Рис. 1.3 Структура Центру кібербезпеки (SOC)

1.4 Інструменти та системи захисту інформації

SOC (відділ ІБ організації) та організація в цілому використовують різноманітні системи та інструменти для забезпечення інформаційної безпеки. Кожен тип системи має свою специфічну функцію та спрямований на захист від різних видів загроз. Розгляну основні типи систем захисту, їх функції та приклади використання.

1. Системи виявлення та запобігання вторгненням (IDS/IPS)

Системи виявлення та запобігання вторгненням включають IDS (Intrusion Detection System) та IPS (Intrusion Prevention System). IDS пасивно моніторять мережевий трафік або системні журнали для виявлення підозрілої або шкідливої активності, генеруючи сповіщення. IPS активно втручаються у потоки даних, блокуючи підозрілу активність у реальному часі. Прикладами таких систем є Snort, Suricata та Cisco IPS. Ці системи ефективно захищають від DoS/DDoS атак, сканування портів та експлойтів вразливостей.

2. Системи управління інформаційною безпекою та подіями (SIEM)

SIEM (Security Information and Event Management) системи забезпечують централізоване збирання, аналіз та кореляцію логів і подій безпеки з різних джерел. Вони поєднують функції управління інформацією про безпеку (SIM) та управління подіями безпеки (SEM). Основні функції включають збір даних, кореляцію подій, моніторинг у реальному часі, сповіщення та звітування. Прикладами SIEM систем є Splunk, IBM QRadar та ArcSight. Вони дозволяють ефективно виявляти APT (Advanced Persistent Threats), внутрішні загрози та складні багатокрокові атаки.

3. Антивірусні та антивредоносні програми

Антивірусні та антивредоносні програми забезпечують захист кінцевих точок від шкідливого програмного забезпечення. Вони сканують файли, мережевий трафік та системні процеси на предмет підозрілої активності, використовуючи сигнатурний та евристичний аналіз. Основні функції включають сканування в режимі реального часу, сканування на вимогу, видалення шкідливого ПЗ та оновлення баз даних сигнатур. Прикладами таких програм є Symantec, McAfee, Kaspersky та Windows Defender. Вони захищають від вірусів, троянських програм, шпигунського ПЗ та програм-вимагачів.

4. Фаєрволи (брандмауери)

Фаєрволи контролюють вхідний та вихідний мережевий трафік на основі встановлених правил безпеки. Вони можуть бути апаратними або програмними і використовуються для захисту мережевих сегментів від несанкціонованого доступу. Основні функції включають фільтрацію пакетів, становий аналіз та

підтримку VPN. Прикладами фаєрволів є Cisco ASA, Fortinet та pfSense. Вони ефективно захищають від несанкціонованого доступу, сканування портів та мережевих черв'яків.

5. Системи захисту кінцевих точок (EDR)

EDR (Endpoint Detection and Response) системи забезпечують детальний моніторинг кінцевих точок (комп'ютерів, мобільних пристроїв) для виявлення та реагування на підозрілу активність. Вони використовують аналітичні інструменти для виявлення аномалій і надають можливості для глибокого розслідування інцидентів. Основні функції включають моніторинг в реальному часі, виявлення аномалій, реагування на інциденти та звітування. Прикладами EDR систем є CrowdStrike, Carbon Black та Microsoft Defender ATP. Вони захищають від шкідливого ПЗ, фішингу, експлойтів на кінцевих точках та атак з привілейованими користувачами.

6. Засоби багатофакторної аутентифікації (MFA)

MFA (Multi-Factor Authentication) засоби забезпечують додатковий рівень захисту, вимагаючи від користувачів підтвердження своєї особи за допомогою двох або більше незалежних факторів (наприклад, паролю та одноразового коду, відбитка пальця). Основні функції включають підтвердження особи користувача та запобігання несанкціонованому доступу. Прикладами MFA засобів є Google Authenticator, Duo Security та Microsoft Authenticator. Вони ефективно захищають від викрадення облікових даних, фішингу та атак грубої сили.

7. Системи запобігання втрати даних (DLP)

DLP (Data Loss Prevention) системи забезпечують захист конфіденційних даних від витоку або несанкціонованого доступу. Вони моніторять та контролюють передачу даних, виявляють спроби витоку даних та блокують їх. Основні функції включають моніторинг передачі даних, виявлення та блокування витоків даних і звітування. Прикладами DLP систем є Symantec DLP, McAfee Total Protection for DLP та Forcepoint DLP. Вони ефективно запобігають витоку даних, крадіжці конфіденційної інформації та внутрішнім загрозам.

8. Інструменти управління вразливостями (Vulnerability Management)

Інструменти управління вразливостями забезпечують ідентифікацію, оцінку та усунення вразливостей в інформаційних системах. Вони здійснюють регулярне сканування систем та мереж на предмет вразливостей, надають звіти про знайдені проблеми та рекомендації щодо їх усунення. Основні функції включають сканування вразливостей, оцінку ризиків, управління патчами та звітування. Прикладами інструментів управління вразливостями є Tenable Nessus, Qualys та Rapid7 Nexpose. Вони допомагають організаціям підтримувати високий рівень безпеки, своєчасно виявляючи та усуваючи вразливості в їхніх системах [34].

Систем захисту цих типів забезпечують всебічний захист інформаційних систем, допомагаючи організаціям ефективно виявляти, реагувати та запобігати різноманітним кіберзагрозам, підвищуючи загальний рівень кібербезпеки.

На рис. 1.3 зображено схему взаємозв’язку систем захисту інформації та.

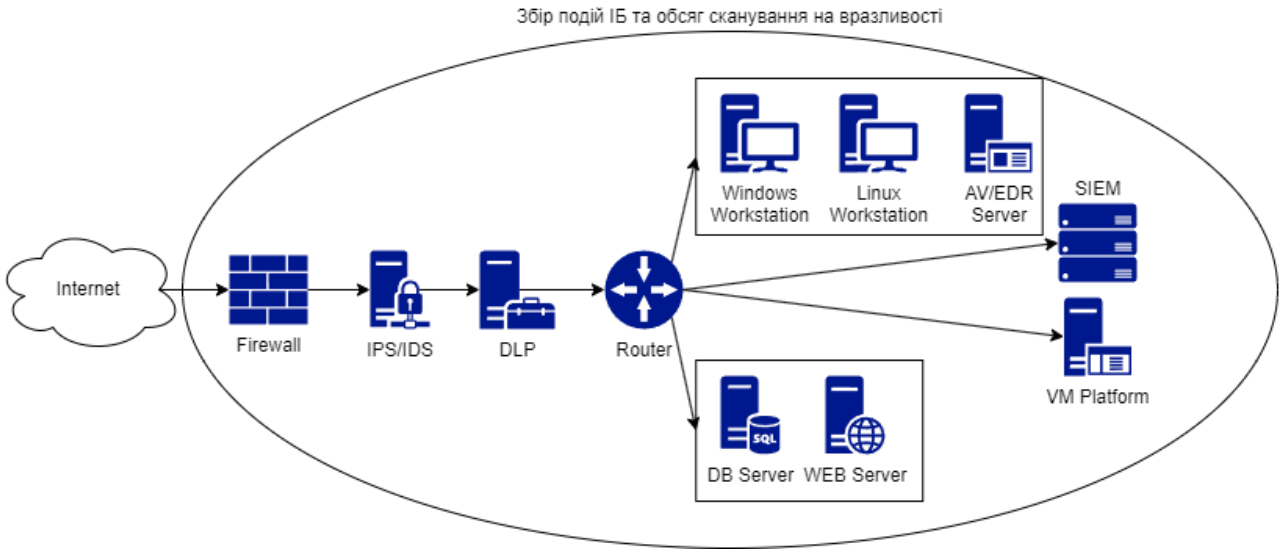

Рис. 1.4 Схема зв’язку систем захисту ІБ з інформаційними активами

Висновок до розділу 1

З огляду на широкий спектр сучасних кібератак, важливо визначити, як вони розвиваються та адаптуються до змін у механізмах (контролях), технологіях та засобах захисту. Від фішингу до складних APT-атак, атаки стають більш

витонченими та цілеспрямованими. Тому знання актуальних методик зловмисників дозволяє прогнозувати та ефективно реагувати на потенційні загрози.

Загалом, захист інформаційних активів, розуміння методик зловмисників та ефективна робота SOC є критично важливими компонентами для забезпечення інформаційної безпеки (кібербезпеки). Впровадження передових технологій, регулярний аналіз загроз та навчання персоналу дозволять забезпечити високий рівень захисту інформаційних систем та активів організації. У даному розділі детально розглянуто ключові компоненти та виклики, які стоять перед сучасною інформаційною безпекою в контексті кібератак. Аналіз сучасних кібератак і загроз підкреслив значення розуміння тріади інформаційної безпеки: конфіденційності, цілісності, та доступності. Виділено, що кожен з цих аспектів вимагає особливої уваги та захисту з урахуванням специфічних загроз, що можуть бути спрямовані проти них.

Дослідження різних видів кібератак, включаючи фішинг, DDoS, веб-атаки, APT-атаки, а також атаки з використанням соціальної інженерії, показало, що кіберзлочинці неухильно вдосконалюють свої методи та стратегії. Це створює високі вимоги до проактивного підходу в інформаційній безпеці, що включає як технічні, так і організаційні заходи.

Особливо значущим є розуміння і захист активів в інформаційній безпеці, де необхідно не лише ідентифікувати та захищати фізичні та цифрові ресурси, а й забезпечити захист даних та інтелектуальної власності. Стратегії управління активами повинні враховувати як внутрішні, так і зовнішні загрози, що вимагає комплексного підходу до безпеки.

Роль Security Operation Center (SOC) у забезпеченні інформаційної безпеки є вирішальною. SOC виконує критичні функції, від моніторингу та аналізу, до реагування на інциденти та прогнозування потенційних загроз. Ефективність SOC безпосередньо впливає на здатність організації протистояти кібератакам, забезпечуючи необхідний рівень захисту активів та мінімізацію можливих збитків.

У підсумку, розглянутий матеріал підкреслює важливість комплексного підходу до інформаційної безпеки, який включає розуміння та застосування новітніх стратегій і технологій для захисту проти все більш різноманітних і складних кіберзагроз. Зміцнення інформаційної безпеки повинно бути пріоритетом для кожної організації, з особливою увагою до захисту активів та розробки відповідних заходів реагування на інциденти.

РОЗДІЛ 2 ІМІТАЦІЙНІ МОДЕЛІ КІБЕРАТАК

2.1 Імітаційні моделі кібератак

Імітації кібератак є одним з ключових елементів в тренуванні та підготовці команд забезпечення кібербезпеки, таких як SOC. Цей процес включає створення контрольованих сценаріїв, які наслідують реальні атаки, щоб перевірити контролі (політики або інструкції), процеси та інструменти, які використовує організація для захисту своїх активів [35].

Основні аспекти імітації кібератак включають:

Забезпечення реалістичності сценаріїв атак – імітаційні сценарії повинні максимально точно відображати реальні атаки, використовуючи відомі техніки та тактики зловмисників. Це дозволяє командам краще підготуватися до можливих загроз.

Тестування систем захисту інформації: Імітації дозволяють оцінити ефективність існуючих заходів безпеки, виявити слабкі місця та запропонувати шляхи їх усунення. Це включає перевірку таких систем, як антивірусне ПЗ, міжмережеві екрани, системи виявлення вторгнень (IDS/IPS), а також політики доступу та управління обліковими записами.

Залучення до процесу імітаційних кібератак різних команд з забезпечення інформаційної безпеки: Для ефективного проведення імітацій важливо залучати різні команди, включаючи червону команду (Red Team), синю команду (Blue Team) та пурпурову команду (Purple Team). Червона команда виконує роль зловмисників, синя команда захищає системи, а пурпурова команда координує та аналізує результати атак [36-37].

Постійне вдосконалення методів та засобів імітаційних атак: Імітаційні атаки повинні бути динамічними та адаптивними до нових загроз. Постійне оновлення сценаріїв, методик та інструментів імітації забезпечує відповідність актуальним загрозам та підвищує рівень захисту.

Роль команд інформаційної безпеки в імітаційних кібератаках

У забезпеченні функціонування імітаційних моделей кібератак ключову роль відіграють команди інформаційної безпеки.

На рис. 2.1 зображено схему ролей та операційних задач команд ІБ.

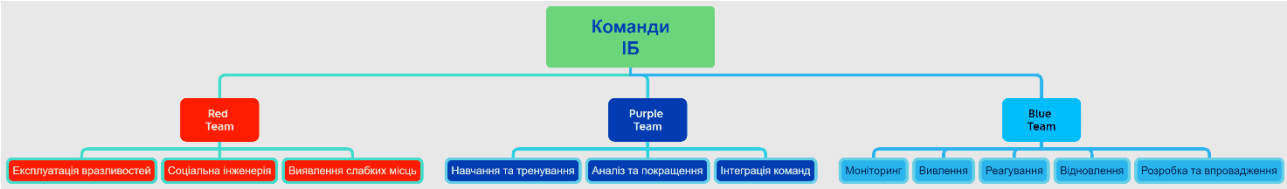

Рис. 2.1 Ролі та обов’язки команд з забезпечення інформаційної безпеки

Кожна з них має свої специфічні завдання і функції, які разом створюють ефективний процес тестування та покращення кібербезпеки організації:

Червона команда (Red Team): Займається розробкою та проведенням імітаційних атак, використовуючи реальні методи зловмисників. Мета червоної команди – виявити вразливості та продемонструвати можливі наслідки атак.

Синя команда (Blue Team): Відповідає за захист систем, моніторинг активності та реагування на інциденти під час імітаційних атак. Вони розробляють та впроваджують заходи безпеки для запобігання успішним атакам.

Пурпурова команда (Purple Team): Координує дії червоної та синьої команд, аналізує результати атак та розробляє рекомендації щодо покращення захисту. Пурпурова команда забезпечує зворотний зв'язок між командами для підвищення ефективності заходів безпеки.

Імітаційні моделі кібератак є критично важливими для тренування та підготовки команд кібербезпеки. Вони дозволяють реалістично оцінити поточний рівень захисту, виявити слабкі місця та вдосконалити стратегії захисту. Залучення різних команд до процесу імітаційних атак забезпечує комплексний підхід до кібербезпеки та підвищує готовність організації до реальних загроз [38].

2.2 Метод створення імітаційних моделей кібератак

Процес контрольованого відтворення кібератаки, який дозволяє аналізувати реакції та оборонні механізми системи безпеки в безпечному середовищі, включає створення деталізованих сценаріїв атак, що імітують поведінку зловмисників та їхні методи атаки. Це необхідно для тестування здатності організації виявляти, протидіяти та відновлюватися після кіберзагроз [39].

Імітаційна модель допомагає виявити слабкі місця в системах безпеки, підготувати персонал до реагування на інциденти та покращити загальні заходи кіберзахисту. Створення імітаційних моделей кібератак вимагає систематичного підходу та детального планування. Розглянемо загальні кроки до створення імітаційної моделі кібератаки та підготовки до здійснення атаки:

Визначення мети створення імітаційної моделі та мети здійснення атаки: Першим кроком є встановлення конкретних цілей, які потрібно досягти за допомогою імітації. Це можуть бути перевірка захисту критичних активів, оцінка ефективності заходів реагування або підвищення обізнаності персоналу.

Визначення інформаційних активів організації, які будуть цілями атаки: Необхідно визначити системи, хости, обладнання або користувачів, які є найбільш критичними для забезпечення діяльності організації та захист яких потребує вдосконалення.

Збір та аналіз інформації про активи: На цьому етапі збирається інформація про обрані активи, включаючи їх архітектуру, програмне забезпечення, вразливості та можливі шляхи доступу.

Розробка сценарію атаки: Створення сценарію, який включає детальний опис методів, інструментів та етапів атаки. Сценарій повинен бути реалістичним і відображати можливі дії зловмисників.

Розгортання інструментів та систем для здійснення атаки: Підготовка необхідного обладнання та програмного забезпечення для виконання сценарію

атаки. Це можуть бути експлойти, інструменти соціальної інженерії, шкідливе ПЗ тощо.

Безпосереднє здійснення атаки за сценарієм: Проведення атаки відповідно до розробленого сценарію. Під час цього етапу важливо фіксувати всі дії та їх результати.

Аналіз результатів та звітність: Після завершення атаки проводиться детальний аналіз отриманих результатів. Визначаються слабкі місця в системах захисту, ефективність заходів реагування та розробляються рекомендації щодо покращення.

Вдосконалення моделі: На основі отриманих результатів та рекомендацій проводяться необхідні зміни та вдосконалення імітаційної моделі, щоб підвищити її ефективність для майбутніх тестів.

Слідування крокам створення та впровадження моделі атаки, що зображені на рис. 2.2 дозволить впровадити та успішно використовувати імітаційні атаки для покращення інформаційної безпеки організації. Цей процес забезпечує постійний розвиток захисних механізмів та підвищення рівня обізнаності і готовності персоналу до потенційних кіберзагроз [40].

Рис. 2.2 Кроки для створення та впровадження імітаційної моделі кібератаки

Для кращого розуміння процесу створення імітаційної моделі, розгляну детальніше кожен крок впровадження.

2.2.1 Визначення мети

Визначення мети створення імітаційної моделі кібератаки полягає в конкретизації завдань, які мають виконуватися за допомогою цієї моделі. Нижче наведено варіанти конкретних цілей для створення різних моделей атак:

Першочерговою метою створення імітаційної моделі кібератаки є підвищення ефективності захисту інформаційних систем та підготовки співробітників SOC до реальних загроз. Конкретні цілі можуть включати наступні аспекти:

1. Тестування та валідація існуючих систем безпеки

Мета: Перевірити ефективність фаєрволів, систем виявлення вторгнень (IDS), систем запобігання вторгнень (IPS), антивірусного ПЗ та інших заходів безпеки.

Приклад: Створення моделі DDoS атаки для оцінки стійкості системи до великих обсягів трафіку та виявлення потенційних вузьких місць.

2. Навчання та тренування співробітників SOC

Мета: Підвищити кваліфікацію співробітників у виявленні, аналізі та реагуванні на кібератаки.

Приклад: Розробка сценарію фішингової атаки для тренування співробітників у розпізнаванні та реагуванні на спроби соціальної інженерії.

3. Виявлення вразливостей у системі

Мета: Виявити потенційні слабкі місця в інфраструктурі безпеки, які можуть бути використані зловмисниками.

Приклад: Модель атаки з використанням експлойту відомої вразливості програмного забезпечення для перевірки наявності патчів та оновлень.

4. Розробка та тестування нових заходів безпеки

Мета: Оцінити ефективність нових технологій та стратегій безпеки до їхнього впровадження.

Приклад: Імітація атаки типу "Man-in-the-Middle" для оцінки ефективності нових протоколів шифрування та захисту мережевих комунікацій.

5. Підвищення обізнаності про загрози

Мета: Розширити знання співробітників про сучасні загрози та методи атак, що застосовуються зловмисниками.

Приклад: Створення моделей атак типу "Advanced Persistent Threat" (APT) для демонстрації складних та тривалих загроз.

6. Оцінка реакції на інциденти

Мета: Перевірити швидкість та координацію дій співробітників під час інциденту безпеки.

Приклад: Імітація атаки типу "Ransomware" для оцінки здатності команди SOC ефективно ізолювати та відновлювати систему.

7. Відпрацювання сценаріїв відповідно до регуляторних вимог

Мета: Забезпечити відповідність вимогам регуляторних органів та стандартам безпеки.

Приклад: Модель атаки на персональні дані для перевірки дотримання вимог міжнародного стандарту щодо захисту та обробки даних.

Кожна конкретна мета створення імітаційної моделі кібератаки має бути чітко визначена та спрямована на вирішення специфічних завдань у сфері інформаційної безпеки. Відповідність цим цілям дозволяє оптимізувати підготовку співробітників, підвищити рівень захисту інформаційних систем та забезпечити більш ефективне реагування на реальні загрози.

2.2.2 Визначення активів

Для ефективного захисту активів необхідно провести оцінку їхньої критичності, що дозволяє визначити, які з них є найбільш важливими для організації та вимагають особливої уваги під час моделювання кібератак. Оцінка критичності може базуватися на таких факторах:

Вплив на бізнес-процеси, наскільки важливим є актив для безперебійного функціонування основних бізнес-процесів організації.

Цінність інформації, ступінь конфіденційності та важливості даних, що зберігаються або обробляються активом.

Залежність від активу, кількість інших систем та процесів, які залежать від цього активу.

Ймовірність загрози того, що актив ста не мішенню для кібератак, виходячи з минулого досвіду та актуальних загроз.

2.2.3 Аналіз активів

Аналіз активів є процесом, що включає визначення загроз та вразливостей активів.

Для кожного ідентифікованого активу проводиться аналіз можливих загроз і вразливостей, загрози можуть включати різні типи кібератак, такі як фішинг, DDoS атаки, використання експлойтів вразливостей програмного забезпечення, внутрішні загрози тощо. Вразливості визначаються шляхом оцінки поточного стану захисту активу та можливих слабких місць. Враховуються як безпосередні наслідки атак (втрата даних, порушення роботи систем), так і непрямі (фінансові втрати, шкода репутації).

При аналізі можливих загроз також важливо врахувати усі властивості інформаційної системи, наприклад:

- Місцезнаходження (фізичне)
- Апаратне забезпечення (характеристики процесору, пам’яті, фізичних портів, модулів (модуля шифрування); характеристики живлення)
- Операційна система
- Програмне забезпечення (програми, сервіси)
- Підключення до SIEM
- Покриття системами захисту ІБ (встановлення агентів AV, EDR), наявність контролів безпеки, що пов’язані з активом або кореляційних правил
- Тип та можливості для автентифікації користувачів в операційній системі активу або в сервісі, який розгорнутий на хості (сервері, системі) активу.

Аналіз впливу дозволяє визначити пріоритетність захисту активів та розробити відповідні заходи безпеки. На основі проведеного аналізу загроз і вразливостей активів створюються сценарії імітаційних кібератак.

2.2.4 Розробка сценарію атаки

Розробка сценарію атаки є ключовим етапом у процесі створення імітаційних моделей кібератак та оцінки ефективності заходів безпеки. Сценарій атаки має бути детально розроблений, щоб забезпечити реалістичне відтворення дій зловмисників та адекватну підготовку до реальних кіберзагроз.

Детальний план атаки повинен включати опис цілей атаки, вектори атак, етапи атаки, засоби та інструменти, а також очікувані результати. Після розробки детального плану атаки необхідно провести тестування сценарію в контрольованому середовищі, щоб переконатися у його ефективності та реалістичності. Це включає запуск сценарію, моніторинг та аналіз дій системи та співробітників SOC під час атаки, а також оцінку результатів.

Сценарій атаки, розроблений та протестований, може використовуватись для різних цілей, таких як тренування співробітників, тестування систем безпеки, розробка та вдосконалення політик безпеки.

2.2.5 Забезпечення атаки

Підготовка до атаки включає кілька важливих етапів, таких як вибір необхідних інструментів та забезпечення безперешкодного здійснення атаки.

Приклади перешкод для здійснення атаки:

- Заблоковані (закриті) мережеві потоки для мережевого доступу до цільової системи
- Недостатня кількість ресурсів апаратного забезпечення

Вибір інструментів та методів залежить від ідентифікованих активів. Наприклад, для сканування вразливостей можуть бути використані OWASP ZAP, Nessus, Burp Suite, а для експлуатації вразливостей – Metasploit Framework

та sqlmap. Важливо також враховувати актуальні загрози та тренди в кіберзлочинності.

Розгортання віртуальних машин на всередині організації та віртуальних хмарних серверів у зовнішньому хмарному середовищі є наступним важливим етапом, який дозволяє створити платформу, що імітує реальну інформаційну інфраструктуру потенційних зловмисників. Використання платформ віртуалізації, таких як VMware, VirtualBox або Hyper-V, дозволяє налаштувати віртуальні машини для атаки внутрішніх активів організації, а також конфігурувати віртуальні мережі для імітації реальної мережевої інфраструктури.

2.2.6 Здійснення атаки за сценарієм

Здійснення атаки за сценарієм є наступним етапом після підготовки. На першому етапі здійснюється збір інформації (розвідка), який включає використання пошукових систем, реєстраторів доменів та соціальних мереж для збору загальнодоступної інформації про цільовий веб-ресурс. Далі проводиться мережеве сканування з використанням Nmap для виявлення відкритих портів і активних хостів, а також сканування веб-додатків за допомогою OWASP ZAP або Burp Suite для виявлення вразливостей.

На етапі експлуатації вразливостей здійснюються автоматизовані запити з використанням OWASP ZAP та sqlmap для виявлення та експлуатації вразливостей веб-додатків і баз даних, а також ручне тестування з використанням Burp Suite для виявлення та експлуатації вразливостей, які можуть бути пропущені автоматизованими інструментами. Це включає проведення атак типу SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF). Після успішного проникнення в систему здійснюється закріплення в системі, яке включає створення бекдорів та встановлення руткітів для забезпечення довгострокового доступу.

Ексфільтрація даних передбачає витяг конфіденційних даних з бази даних веб-ресурсу з використанням sqlmap та доступ до конфігурації веб-застосунку. Виведення з експлуатації включає видалення слідів присутності зловмисника, очищення логів та видалення тимчасових файлів. На завершення проводиться аналіз результатів, що охоплює оцінку ефективності атакуючих дій, виявлених вразливостей, часу реакції систем захисту та дій співробітників SOC.

Документування всіх етапів атаки є важливим для подальшого аналізу та удосконалення заходів безпеки. Регулярне проведення тренувань допомагає підтримувати високий рівень кібербезпеки в організації та забезпечує готовність до реагування на інциденти.

2.2.7 Аналіз результатів та звітність

Необхідно виконати збір всіх даних, отриманих під час імітаційної атаки, включаючи кожне сканування та кожен успішний запит співробітників Red Team. На основі цих даних проводиться детальний аналіз ефективності атакуючих дій, оцінюється успішність досягнення цілей атаки, включаючи проникнення в систему, експлуатацію вразливостей, закріплення в системі та ексфільтрацію даних.

Ключовим елементом є виявлення вразливостей, які були експлуатовані під час атаки, та проведення ретельного аналізу цих вразливостей для розробки конкретних заходів з їх усунення. Документування всіх результатів атаки, виявлених вразливостей, дій зловмисників та ефективності заходів безпеки є важливим кроком, що включає створення звітів з детальним описом всіх етапів атаки, використаних інструментів та методів, результати експлуатації вразливостей та рекомендації щодо покращення.

На основі проведеного аналізу розробляються рекомендації щодо покращення заходів безпеки, включаючи технічні та організаційні заходи, а також детальний план дій для усунення виявлених вразливостей. Завершальним

етапом є презентація результатів атаки та рекомендацій керівництву організації та іншим зацікавленим сторонам. Результати аналізу використовуються для навчання персоналу, підвищення їхньої обізнаності та готовності до реальних загроз. Регулярні тренування та навчання допомагають підтримувати високий рівень кібербезпеки в організації.

Таким чином, аналіз результатів та звітність дозволяють не лише оцінити ефективність проведеної атаки, але й виявити слабкі місця в системі захисту, надати рекомендації для їх усунення та вдосконалення існуючих заходів безпеки, сприяючи підвищенню загального рівня кіберстійкості організації.

2.2.8 Вдосконалення моделі

Включає ретельний аналіз результатів попередніх імітаційних атак, щоб оцінити ефективність атакуючих дій, виявлених вразливостей, часу реакції системи захисту та дій співробітників SOC. На основі цього аналізу вносяться корективи у моделі атак, адаптуючи їх до нових типів загроз та сучасних технік атак. Це може включати зміну сценаріїв атак – додавання нових етапів або методів, що імітують реальні дії зловмисників. Крім того, необхідно регулярно оновлювати бази даних вразливостей та аналізувати нові методи атак, щоб забезпечити актуальність імітаційних моделей.

Наступний етап включає покращення методів та інструментів, що використовуються під час імітаційних атак, впровадження нових інструментів для збору інформації, сканування вразливостей, експлуатації слабких місць та моніторингу системи. Постійне навчання співробітників SOC щодо використання цих інструментів та новітніх методів атак є ключовим для підвищення кваліфікації персоналу.

Розробка нових сценаріїв атак на основі вдосконалених моделей та нових загроз дозволяє забезпечити різноманітність імітаційних атак та підвищити готовність співробітників SOC до різних типів загроз. Вдосконалення моделі

кібератаки є безперервним процесом, що включає регулярний перегляд та оновлення моделей атак, адаптацію до нових загроз і тенденцій у кіберпросторі, а також постійне навчання та підвищення кваліфікації співробітників, сприяючи підвищенню рівня кібербезпеки організації.

2.3 Створення сценаріїв атак

Створення сценарію імітаційної кібератаки розглянемо на прикладі WEB-атаки на зовнішній веб-ресурс організації. Поетапний сценарій здійснення імітаційної атаки [41]:

1. Збір інформації (розвідка):

- Збір інформації про ресурс з публічних джерел інформації (пошукові системи, реєстратури).
- Здійснення мережевого сканування (порти та хости) за допомогою мережевого сканеру.
- Сканування (HTTP-запитами) за допомогою сканера вразливостей веб-застосунків.

2. Експлуатація вразливостей:

- Здійснення автоматизованих запитів для виявлення та експлуатації вразливостей веб-застосунку та бази даних за допомогою інструментів OWASP ZAP та sqlmap.
- Проведення ручного тестування та експлуатації вразливостей за допомогою інструменту Burp Suite.

3. Отримання (вивантаження) даних та отримання доступу до конфігурації веб-застосунку:

- Отримання даних з бази даних та доступу до конфігурації веб-застосунку.

Частково етапи сценарію засновані на моделі Cyber Kill Chain, яка є зразком кращих практик у проведенні кібератак.

За створення сценарію атаки відповідають члени червоної команди (Red Team) та пурпурової команди (Purple Team). Кожен з етапів імітаційної атаки здійснюється червоною командою та узгоджується з керівництвом ІБ організації.

Виконання імітаційних атак – імітаційні атаки з реальними експлуатаціями вразливостей здебільшого мають здійснюватися на тестових веб-ресурсах, зупинка функціонування яких не є критичною для бізнес потреб. Це дозволяє мінімізувати ризики для основних операцій та забезпечити безперервність бізнес-процесів.

Документування кожного етапу – важливо детально документувати всі кроки, інструменти та методи, які використовуються під час створення та виконання сценаріїв атак. Це допоможе в подальшому аналізі та удосконаленні захисних заходів.

Оцінка ефективності атак – після проведення імітаційних атак необхідно оцінити їх ефективність, враховуючи час виявлення, швидкість реагування та можливі наслідки для системи. Це дозволить виявити слабкі місця та розробити рекомендації для покращення.

Навчання персоналу – залучення персоналу до процесу імітаційних атак сприяє підвищенню їхньої обізнаності та готовності до реальних загроз.

Регулярне проведення тренувань допомагає підтримувати високий рівень кібербезпеки в організації.

Створення імітаційних сценаріїв кібератак є важливою складовою процесу забезпечення кібербезпеки, що дозволяє не лише покращити захисні заходи, але й підготувати організацію до можливих загроз.

2.4 Інструменти для здійснення імітацій кібератак

Для забезпечення процесу імітаційних атак необхідні програмні інструменти [42].

Інструменти здійснення імітації майже не відрізняються від поширених інструментів зловмисників для здійснення кібератак. Основні види програмного

забезпечення, що використовуються для проведення кібератак (або одного з елементів атаки), включають:

Мережеві сканери (nmap, Nessus, OpenVAS). Мережеві сканери використовуються для виявлення вразливостей у мережевій інфраструктурі, таких як неправильно налаштовані сервіси, відкриті порти, вразливі версії програмного забезпечення тощо. nmap дозволяє виконувати сканування портів і виявлення активних хостів. Nessus та OpenVAS забезпечують глибше сканування, виявляючи специфічні вразливості та надаючи рекомендації щодо їх усунення.

WEB-сканери вразливостей (Burp Suite, OWASP ZAP). Інструменти, такі як Burp Suite та OWASP ZAP, дозволяють ідентифікувати вразливості веб-застосунків, проводячи як автоматизовані, так і ручні тести. Burp Suite пропонує комплексний набір інструментів для тестування безпеки веб-додатків, включаючи інтерсептор запитів та сканер вразливостей. OWASP ZAP є популярним інструментом для виявлення різних типів вразливостей, таких як SQL-ін'єкції та міжсайтові скрипти (XSS).

Інструменти для експлуатації вразливостей (Metasploit Framework, sqlmap, BeEF). Metasploit Framework дозволяє створювати та запускати експлойти для виявлених вразливостей, а також розробляти власні модулі. sqlmap автоматизує процес виявлення та експлуатації SQL-ін'єкцій. BeEF фокусується на експлуатації вразливостей браузера та дозволяє здійснювати складні атаки через веб-інтерфейси.

Інструменти для аналізу та маніпулювання трафіком (Ettercap, Wireshark). Інструменти, такі як Ettercap та Wireshark, дозволяють перехоплювати, аналізувати та модифікувати мережевий трафік. Wireshark є потужним аналізатором протоколів, який надає детальну інформацію про мережевий трафік та допомагає виявити аномалії. Ettercap дозволяє виконувати атаки типу "людина посередині" (MITM) для перехоплення та зміни трафіку.

Інструменти для соціальної інженерії (Social-Engineer Toolkit (SET), Maltego): SET надає засоби для створення фішингових сторінок, відправлення

шкідливих електронних листів та інших методів соціальної інженерії. Maltego використовується для збору інформації та аналізу зв'язків між різними об'єктами, що допомагає у плануванні та виконанні атак.

Використання різних інструментів для здійснення імітаційних кібератак дозволяє максимально реалістично відтворювати дії зловмисників та ефективно тестувати захисні механізми організації. Цей підхід допомагає виявляти слабкі місця, покращувати заходи безпеки та підвищувати готовність до реальних кіберзагроз.

2.5 Забезпечення постійного функціонування моделей імітаційних атак

Забезпечення постійного функціонування моделей імітаційних атак є складним і багатогранним процесом, який вимагає постійного оновлення сценаріїв атак і підтримки відповідної інфраструктури. Регулярне оновлення сценаріїв атак дозволяє відображати новітні загрози, а ефективна підтримка інфраструктури забезпечує надійне і ізольоване середовище для проведення тестувань. Використання віртуалізації, контейнеризації та інструментів автоматизації сприяє зниженню ризиків та підвищенню гнучкості й ефективності процесу, що в кінцевому підсумку підвищує рівень кібербезпеки організації [43].

Забезпечення актуальності сценаріїв атак передбачає систематичний моніторинг нових загроз. Це включає в себе регулярне відстеження джерел інформації про вразливості, таких як Common Vulnerabilities and Exposures (CVE) та National Vulnerability Database (NVD), а також спеціалізованих форумів і звітів з кібербезпеки. Оновлення сценаріїв повинно включати останні техніки та тактики, що використовуються зловмисниками, щоб тестування відображало реальні загрози.

Використання віртуальних машин та контейнерів дозволяє створювати ізольовані середовища для тестування, що знижує ризик впливу на реальну інфраструктуру та підвищує гнучкість тестування. Віртуалізація дозволяє швидко розгортати та конфігурувати середовища для тестування, а

контейнеризація забезпечує легкість у масштабуванні та оновленні цих середовищ.

Планувальники задач є ключовими компонентами автоматизації процесів, що дозволяють забезпечити безперервність виконання різноманітних завдань, включаючи регулярні оновлення сценаріїв атак, збір логів та запуск скриптів для тестування безпеки. Одним з найбільш поширених і потужних планувальників задач в Linux є cron. Використання таких інструментів дозволяє автоматизувати рутинні процеси та зосередитися на аналізі та вдосконаленні захисних заходів.

Також слід розглянути цільне BAS (Breach and Attack Simulation) рішення. BAS рішення є новітнім підходом до тестування безпеки, який дозволяє постійно і автоматично оцінювати здатність організації виявляти та реагувати на кібератаки. Використання BAS-рішень, таких як Cymulate, AttackIQ або SafeBreach, забезпечує проведення регулярних імітаційних атак на реальну інфраструктуру без ризику порушення роботи систем.

BAS-рішення забезпечують комплексний підхід до тестування безпеки, включаючи наступні ключові функції:

- Автоматизоване тестування – BAS-рішення дозволяють автоматично виконувати складні сценарії атак, що включають різні типи кібератак, такі як фішинг, експлойти, атаки на веб-додатки, атаки на кінцеві точки та мережеві атаки.

- Безперервне оцінювання – системи BAS можуть працювати постійно, надаючи організаціям можливість безперервно оцінювати свою готовність до кібератак та оперативно реагувати на виявлені вразливості.

- Реалістичні імітації – використовуючи найсучасніші методи та техніки, BAS-рішення імітують реальні атаки, що дозволяє виявляти слабкі місця в захисних механізмах організації.

- Звітування та аналітика – BAS-рішення генерують детальні звіти, які включають інформацію про виявлені вразливості, ефективність захисних заходів та рекомендації щодо покращення безпеки. Ці звіти допомагають керівництву

організації приймати обґрунтовані рішення щодо удосконалення системи кібербезпеки.

Використання BAS-рішень також надає організаціям численні переваги:

- Актуальність захисту: BAS-рішення дозволяють забезпечити актуальність заходів безпеки, відображаючи сучасні загрози та тактики атакуючих.
- Підвищення ефективності: Автоматизація тестування дозволяє значно підвищити ефективність процесів оцінки безпеки, знижуючи навантаження на фахівців з кібербезпеки.
- Зниження ризиків: Безперервне оцінювання та своєчасне виявлення вразливостей допомагають знижувати ризики компрометації інформаційних систем.
- Підвищення готовності: Реалістичні імітації атак покращують підготовку співробітників SOC та інших відповідальних за кібербезпеку, підвищуючи їхню готовність до реальних інцидентів.
- Регулярне вдосконалення: Детальні звіти та аналітика забезпечують основу для регулярного вдосконалення системи кібербезпеки організації, дозволяючи вчасно впроваджувати необхідні зміни.

На ринку існує кілька провідних BAS-рішень, кожне з яких має свої унікальні особливості та функціональні можливості. Деякі з найпопулярніших BAS-рішень включають:

Cymulate, яке забезпечує повний спектр імітаційних атак, включаючи атаки на електронну пошту, веб-додатки, кінцеві точки та мережі. Система надає детальні звіти та рекомендації щодо покращення безпеки.

AttackIQ, яке пропонує платформу для безперервного тестування безпеки, яка включає сценарії атак, створені на основі сучасних методів і технік зловмисників. Платформа інтегрується з існуючими засобами захисту для забезпечення максимальної ефективності.

SafeBreach, яке забезпечує імітацію реальних атак на інформаційні системи, допомагаючи організаціям виявляти та усувати вразливості. Платформа

пропонує автоматизоване тестування та детальні звіти з рекомендаціями щодо покращення безпеки.

Використання BAS-рішень зосереджено на симуляції широкого спектру атак, але в той самий час, процеси та дії Red Team (червоної команди) зосереджуються саме максимально реалістичному відтворенні.

Забезпечення постійного функціонування моделей імітаційних атак вимагає систематичного підходу, який включає регулярне оновлення сценаріїв, використання передових технологій віртуалізації та контейнеризації, а також впровадження автоматизації. Використання BAS-рішень додатково підвищує ефективність цього процесу, забезпечуючи актуальність та повноту тестування.

Цей комплексний підхід дозволяє організаціям ефективно реагувати на сучасні кіберзагрози та підтримувати високий рівень кібербезпеки.

Висновки до розділу 2

В цьому розділ, зосередив увагу на аналізі методології створення та використання імітаційних моделей кібератак, які є невід'ємною частиною тренувань і підготовки співробітників SOC.

Моделі кібератак дозволяють забезпечити реалістичне відтворення кіберзагроз, що значно покращує готовність команд забезпечення кібербезпеки до реагування на реальні кібератаки. Основні аспекти імітаційних моделей кібератак включають створення реалістичних сценаріїв атак, використання інтегрованого підходу у тестуванні та постійне оновлення та адаптацію. Імітаційні сценарії атак повинні точно відтворювати поведінку зловмисників і використовувати актуальні методики, що забезпечує ефективність навчання і перевірку існуючих систем безпеки. Включення різних команд (червона, синя та пурпурова команди) в процес імітації забезпечує комплексний підхід до аналізу та виявлення вразливостей, а також покращує зворотній зв'язок і взаємодію в процесі відповіді на інциденти. Імітаційні моделі мають регулярно

оновлюватися, щоб відповідати новим кіберзагрозам і тенденціям. Це забезпечує актуальність моделей і підвищує їхню ефективність у підготовці персоналу.

Методи створення імітаційних моделей кібератак включають детальне планування, вибір інструментів та постійний розвиток та удосконалення.

Важливість чіткого визначення цілей імітаційних атак та детального планування кожного етапу забезпечує глибоке розуміння потенційних ризиків і вразливостей, які можуть бути виявлені і усунені в процесі навчання.

Використання спеціалізованого програмного забезпечення та інструментів, таких як інструменти для експлойтів та сканери вразливостей, є ключовим для забезпечення реалістичного та ефективного сценарію імітації. Розробка нових стратегій та методик для вдосконалення імітаційних моделей та покращення загальної безпекової постановки організації потребує постійного перегляду та впровадження вдосконалень, заснованих на аналізі отриманих результатів і зворотного зв'язку від команд.

Імітаційні моделі кібератак є невід'ємною частиною стратегії інформаційної безпеки, що дозволяє не тільки підвищити обізнаність і навички співробітників SOC, але й значно покращити здатність організації протистояти реальним кібератакам. Комплексний підхід до створення та використання таких моделей забезпечує глибоке розуміння потенційних загроз і виявлення вразливостей, що є ключовим для підвищення рівня кібербезпеки будь-якої організації.

Комплексний підхід до створення та використання таких моделей має бути забезпеченим глибоким розумінням потенційних загроз і вразливостей.

Використання контрольованих імітаційних кібератак дозволило не лише аналізувати можливі вектори атак, але й оцінити готовність команд до реагування на інциденти. Процеси визначення цілей імітації, підготовки сценаріїв атак та їх виконання відповідно до заздалегідь встановлених параметрів забезпечили покращення заходів безпеки.

Ключовим аспектом також є постійне функціонування імітаційних моделей кібератак. Регулярне оновлення сценаріїв атак, відстеження нових загроз та оновлення інфраструктури для тестування є необхідними для адаптації захисних

систем до постійно змінюваних умов цифрового середовища. Це дозволяє підвищити здатність організацій протистояти сучасним кіберзагрозам.

РОЗДІЛ 3 РЕЗУЛЬТАТИ ВПРОВАДЖЕННЯ ІМІТАЦІЙНИХ МОДЕЛЕЙ КІБЕРАТАК

3.1 Приклад створеної імітаційної моделі кібератаки

Створена на основі сценарію модель ілюструє послідовність дій, що виконуються червоною командою (Red Team) для здійснення кібератаки, починаючи від експлуатації вразливостей до отримання конфіденційних даних та встановлення контролю над цільовою системою. Процес розробки імітаційної моделі кібератаки базувався на аналізі сучасних методів і технік, що використовуються зловмисниками.

Імітаційна модель кібератаки (рис. 3.1) складається з п'яти основних етапів, кожен з яких відображає конкретні дії, що виконуються під час атаки для досягнення кінцевої мети – отримання конфіденційних даних та встановлення контролю над цільовою системою:

Проведення сканування: На цьому етапі проводиться виявлення слабких місць у захисті програмного забезпечення, що дозволяє здійснити несанкціонований доступ або зловмисні дії. Використовуються інструменти для сканування портів, виявлення відкритих сервісів та ідентифікації вразливостей.

Експлуатація вразливостей: Після успішного сканування та розвідки, наступним етапом є експлуатація вразливостей веб-застосунку або його бази даних з використанням спеціальних інструментів. Це може включати SQL-ін'єкції, XSS-атаки або інші методи проникнення.

Виконання шкідливого коду: Після успішної експлуатації вразливостей, виконується шкідливий код (скрипт або програма), що дозволяє виконувати довільні команди на сервері (сервері бази даних). Це може бути використано для встановлення бекдору або завантаження додаткового шкідливого ПЗ.

Отримання конфіденційних даних або можливості до зміни налаштувань сервера: Кінцевий етап атаки полягає в доступі до конфіденційної інформації або

можливості змінювати налаштування сервера. Отримані дані можуть включати особисту інформацію користувачів, фінансові дані або інші критичні для організації відомості.

Встановлення контролю над системою: Завершальним етапом є закріплення контролю над системою для подальшого використання або проведення додаткових атак. Це може включати створення прихованих користувачів, встановлення постійних бекдорів та моніторинг активності системи.

Процес створення імітаційних моделей кібератак, що включає етапи від сканування до встановлення контролю над системою, дозволяє детально відпрацьовувати всі можливі вектори атак та тестувати здатність організації протистояти кіберзагрозам. Така модель допомагає ідентифікувати слабкі місця, покращити заходи захисту та підготувати персонал до реальних інцидентів, що пов’язані з виконанням зловмисниками атаки на зовнішній WEB-ресурс.

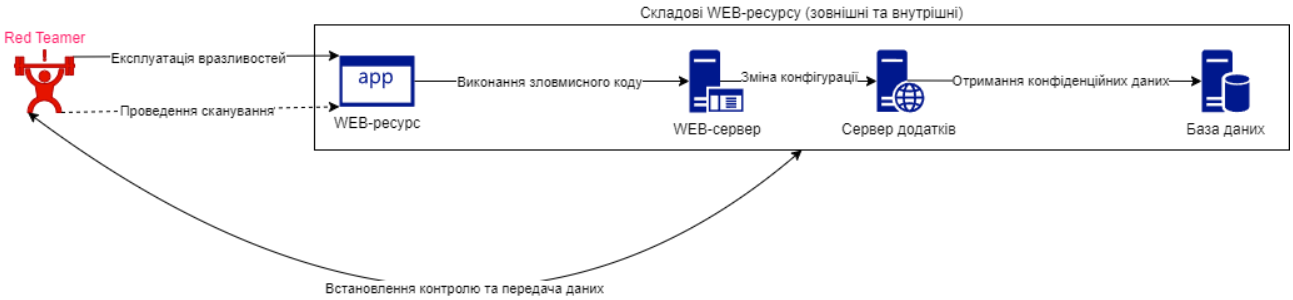

Рис. 3.1 Модель WEB-атаки на WEB-ресурс

3.2 Контролі безпеки

Для виконання свого головного завдання, а саме захисту активів організації від загроз та кібератак, SOC (відділ ІБ організаціх) використовую контролі безпеки.

Контроль безпеки – це заходи та процеси для захисту інформації (їх властивостей конфіденційності, цілісності та доступності) в системах та активах організації

Основна мета впровадження контролю безпеки: превентивна, виявлювальна, коригувальна, компенсаційна або стримуюча.

Детально розгляну типи контролів безпеки.

• Технічні контролі (Technical Control)

Технічні контролі, також відомі як логічні контролі, використовуються для нівелювання атак на апаратне та програмне забезпечення. Для захисту системи встановлюються автоматизовані програмні інструменти.

Приклади технічних контролів безпеки:

- Антивіруси та системи захисту кінцевих точок (EDR)

- Фаєрволи (NGFW, WAF)

- Системи виявлення вторгнень та запобігання вторгнень (IDS, IPS)

Технічні контролі впроваджуються за допомогою двох методів:

- Списки конролю доступів (ACL), фільтр , який контролює права доступу до об’єкту (які саме операції можуть виконуватись) з певної адреси або від певного користувача. Здебільшого застосовується на мережевому обладнанні (маршрутизатори, комутатори, фаєрволи)

- Правил конфігурації, які є набором параметрів систем, що встановлюють певні коректні налаштування, що не можуть бути змінені та зміна яких або спроба змінити свідчитиме про нелегітимну активність або помилки конфігурації систем.

• Адміністративні контролі (Administrative Control)

Адміністративні контролі безпеки включають політики, процедури та вказівки, що визначають ролі або бізнес-практики для досягнення цілей безпеки організації.

Для впровадження адміністративних контролів необхідні додаткові контролі для моніторингу та забезпечення виконання. Контролі для моніторингу та забезпечення виконання включають:

- Управлінські контролі, які зосереджуються на управлінні ризиками та управлінні інформаційною безпекою

- Операційні контролі, які є заходами безпеки, що реалізуються технічними та управлінськими засобами та виконуються відповідальними співробітниками.

• Фізичні контролі (Physical)

Фізичні контролі безпеки впроваджуються для запобігання несанкціонованому фізичному доступу до конфіденційних даних . Приклади фізичних контролів:

- Камери відеоспостереження з замкнутим контуром
- Системи датчиків руху або температури
- Охоронці та ідентифікаційні картки
- Двері на замку
- Біометричні системи

• Профілактичні контролі

Профілактичні контролі використовуються для запобігання втратам або помилкам. Приклади превентивних контролів:

- Навчання з підвищення обізнаності про безпеку: процес формальної освіти співробітників та зацікавлених сторін щодо загроз безпеки та політик і процедур організації.

- Управління змінами: заходи, що описують та впроваджують зміни як внутрішні, так і зовнішні в системі, включаючи підготовку та підтримку співробітників для виконання необхідних кроків.

- Політика відключення облікових записів: відключення облікового запису, коли співробітник залишає організацію.

• Детективні контролі

Детективні контролі використовуються для виявлення та попередження про несанкціоновані або небажані дії в організації. Це допомагає виявляти порушення безпеки та реагувати на них за допомогою інструментів. Приклади детективних контролів:

- Моніторинг пристроїв та джерел подій на предмет відключення або помилок

- Використання SIEM для кореляції подій, аналізу подій та виокремлення інцидентів із подій ІБ

- Аудит безпеки або систематична оцінка інформаційних систем, мереж і фізичної інфраструктури компанії. Аудити проводяться групою фахівців із безпеки, які використовують різні інструменти та методи для оцінки поточного стану безпеки організації.

- Коригувальні контролі

Коригувальні засоби контролю використовуються для усунення або пом'якшення наслідків інциденту ІБ та включає заходи для запобігання повторенню подібних інцидентів в майбутньому. Приклади коригувальних контролів:

- Забезпечення процесу створення та збереження резервних копій чутливих даних, втрата яких є критичною для організації

- Перенесення потенційно небажаного програмного забезпечення в антивірусний карантин

- Стримуючі контролі

Стримуючі контролі впроваджуються задля запобігання порушень інформаційної безпеки і зменшенню імовірності атаки на фізичні об'єкти. Приклади стримуючих контролів:

- Штрафи

- Камери відеоспостереження

- Освітлення

- Дверні замки

- Компенсуючі контролі

Компенсуючий контроль – це альтернативнй метод, який підтримує вимоги фактичного реалізованого контролю безпеки. Роль компенсуючого контролю полягає в тому, щоб забезпечити аналогічний рівень надійності, навіть якщо зловмисник скомпрометував фактичний контроль безпеки.

Матрична схема відповідності між типами контролів та функціями контролів безпеки відображено на рис. 3.2 .

Типи контролів безпеки	Функції контролів		
	ПРЕВЕНТИВНІ	ДЕТЕКТИВНІ	КОРИГУВАЛЬНІ
ФІЗИЧНІ КОНТРОЛІ	- Паркани - Ворота - Замки	- Камери відоспотереження	- Відновлення фізичних пошкоджень - Перевипуск кард доступу
ТЕХНІЧНІ КОНТРОЛІ	- Фаєрвол - IPS - MFA - Антивірус	- IDS - Honeypot	- Встановлення безпекових патчів - Карантин для вірусів - Перезапуск систем
АДМІНІСТРАТИВНІ КОНТРОЛІ	- Політики найму та звільнення - Розподіл обов'язків - Класифікація даних	- Перегляд прав доступу - Записи журналу аудиту та неавторизованого доступу	- Впровадження плану безперервності бізнесу - Створення плану реагування на інцидент

Рис. 3.2 Матриця відповідності типів контролів та функцій контролів безпеки

3.3 Виявлення атаки та реагування

Впровадження контролів безпеки командою SOC забезпечується здебільшого за допомогою впровадження кореляційних правил SIEM-системи організації (технічні та детективні контролі), конфігураційних правил мережевого обладнання й систем захисту (WAF, IDS, IPS, NGFW, AV, EDR) та розробки SOC Use Case (юзкейс) [42].

Контролі безпеки забезпечують загальну базу для розробки юзкейсу SOC та дозволяють SOC ефективно виявляти підозрілу активність, реагувати на інциденти та мінімізувати вплив від атак й загроз.

SOC Use Case – це сценарій організації операційної роботи для виконання контролю ІБ.

SOC Use Case Management – методолія організації управління життєвим циклом SOC Use Case.

SOC Use Case Development – процес розробки (розвитку) юзкейсу й супутніх документів, правил.

Playbook – сценарій реагування на виявлений інцидент ІБ, аномалію або невідповідність стандарту експлуатації ІТ-інфраструктури. Розробка та актуалізація – виконується за результатами аналізу та реагування.

Кореляційне правило – це конфігураційне правило в SIEM-системі, що дозволяє проводити логічний процес кореляції подій ІБ. Кореляційне правило має собі певні встановлені параметри подій, що свідчать про нелегітимну активність (атаку або інші дії зловмисників). Результатом спрацювання кореляційного правила в SIEM-системі може бути нотифікація про порушення ІБ.

На рис. 3.3 зображено схему розробки та змін в юзкейс.

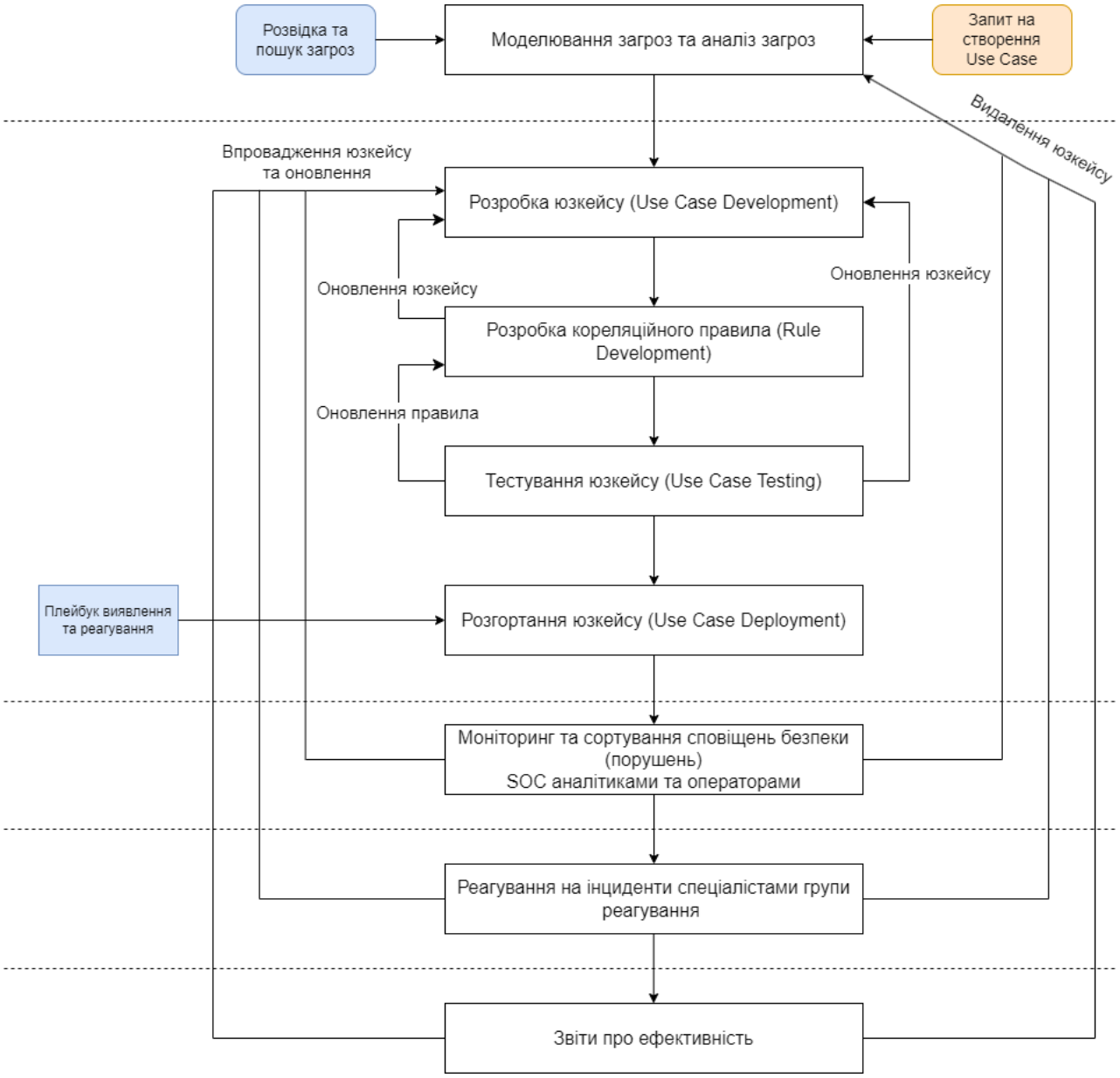

Рис. 3.3 Розробка та розвиток Use Case

Застосування юзкейсів їх та кореляційних правил є ефективним рішенням SOC для виявлення і реагування на дії зловмисників під час WEB-атаки.

Наведу приклади застосування кореляційних правил та плейбуків для нівелювання дій та наслідків кожного етапу здійснення атаки на WEB-ресурс зловмисниками. В якості порушень та інцидентів будуть розглянуті 5 етапів зі створеної імітаційної моделі:

1. Проведення сканування.

Потенційний зловмисник здійснює розвідку відкритих (доступних) портів хоста веб-ресурса за допомогою мережевого сканера або сканера вразливостей та ідентифікує сервіси, які використовують ці порти, включаючи їх назви, номерні версії та доступні дані про конфігурацію.

Ознаками, що свідчать про сканування є надсилання великої кількості пакетів до великого числа різних портів (в тому числі відомих і розповсюджених сервісів систем (SSH, Telnet, FTP, SMTP, DNS)) та події спроб підключитися до закритого або специфічного (зарезервованого, непризначеного) порта.

Процес виявлення зловмисного сканування можна забезпечити за допомогою створення кореляційного правила в SIEM-системі, джерелом подій для кореляції виступатиме мережеве обладнання зовнішнього периметру мережі (маршутизатори) та фаєрволи (WAF, NGFW).

Процес реагування на порушення включатиме аналіз подій, що пов’язані зі скануванням та блокування зовнішньої IP-адреси з якої здійснювалось сканування. Також в разі підозр на компрометацію цільового веб-ресурсу необхідно переглянути події ІБ веб-додатку та веб-серверу, які можуть свідчити про успішне отримання доступу до конфіденційної інформації та змін в кофігурації ресурсу.

2. Експлуатація вразливостей

Зловмисник за допомогою сканеру вразливостей та спеціальних інструментів (які дозволяють здійснювати зловмисні HTTP-запити та SQL-ін’єкції) виконує запити до цільового веб-ресурсу з метою отримати доступ до конфіденційної інформації або виконати зміну конфігурації.

Події зловмисних запитів матимуть в собі частини посилань, що міститимуть SQL-запити до баз даних та запити до заборонених директорій веб-ресурсу (конфігураційні файли, файли з паролями).

Процес виявлення зловмисного сканування можна забезпечити за допомогою створення кореляційного правила в SIEM-системі, джерелом подій виступатимуть фаєрволи (WAF, NGFW, які здатні перевіряти та зберігати запити до ресурсів на рівні додатку)

Процес реагування включає аналіз подій ІБ та аналіз враженого активу на наявність нелегітимних змін через перегляд подій ОС хоста. Але першочерговим є блокування зовнішньої IP-адреси з якої здійснювались запити.

3. Виконання шкідливого коду

Зловмисник отримавши можливості зміни конфігурації серверу ресурсу після здійснення успішних зловмисних запитів, завантажує та розгортає на ураженій цілі зловмисне ПЗ.

Процес виявлення застосування зловмисного ПЗ можна забезпечити за допомогою кореляційного правила, джерелом подій є операційна система ураженого хоста та події EDR рішення розгорнутого на сервері.

Процес реагування супроводжується відключенням ураженого хоста від мережі та проведенням дослідження внутрішньої мережі (інфраструктури організації) на присутність аналогічного зловмисного ПЗ абоподібних спрацювань правил (контролів).

4. Отримання конфіденційних даних

Зловмисник отримує конфіденційну інформацію з бази даних після компрометації хоста (сервера) та передає їх до власної бази для подальшого використання в інших нелегітимних діях.

Процес виявлення зчитування конфіденційної інформації можна впровадити за допомогою кореляційного правила SIEM, яке відслідковуватиме дійсність надходження подій від баз даних та виконуватиме нотифікацію SOC при аномальному збільшені трафіку від серверів баз даних.

Процес реагування передбачає відключення від мережі та очищення уражених хостів.

5. Встановлення контролю над системою

Зловмисник створює нових користувачів, залишає бекдори в існуючій системі та забезпечує за допомогою спеціального ПЗ прямий віддалений доступ до веб-серверу.

Процес виявлення впроваджуються шляхом створення кореляційних правил, які спрацьовують на події створення нових користувачів, створення

нових процесів та аномальне збільшення подій мережевих комунікацій з зовнішніми IP-адресами.

Процес реагування передбачає відключення уражених систем від мережі та перевстановлення усього програмного забезпечення та операційної системи на системі.

Схема зв’язків процесу застосування юзкейсів та їх кореляційних правил в рамках виявлення та реагування на WEB-атаку зображено на рис. 3.3 .

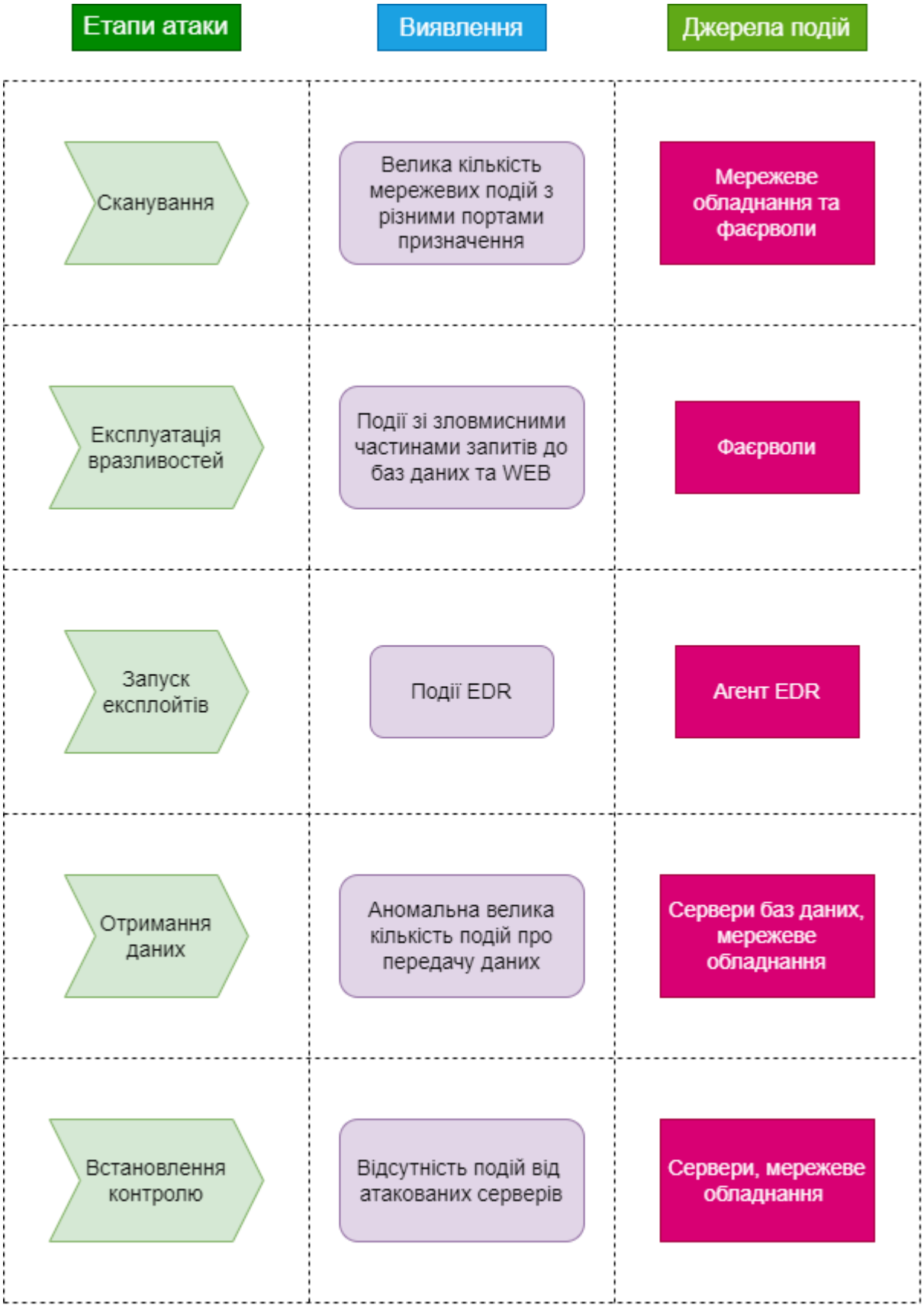

Рис. 3.4 Схема зв’язків процесу застосування юзкейсів

3.4 Збір метрик та оцінка процесів SOC

SIEM (Security Information and Event Management) в SOC, окрім кореляції подій, має інші функції, забезпечення збору, моніторингу, аналізу та звітування про події безпеки, зібрані з різних джерел у IT-інфраструктурі організації [43].

Основні технічні можливості SIEM включають:

Агрегація даних – збір усіх записів подій в одному сховищі та консолі керування.

Кореляція подій – автоматичний аналіз подій ІБ за допомогою кореляційних правил на наявність нелегітимної активності або аномалій.

Генерація звітів – створення звітів та зберігання важливих подій ІБ для відповідності вимогам стандартів.

Джерелами записів подій ІБ для SIEM є пристрої мережевого обладнання, сервери, комп'ютери, застосунки та інші системи безпеки. Архітектура WEB-ресурсу та мережева інфраструктура передбачає декілька різних хостів, які є джерелами подій для SIEM (рис. 3.2). Події ІБ цих хостів використовуються Blue Team для аналізу активності під час атак та для створення майбутніх контролів безпеки.

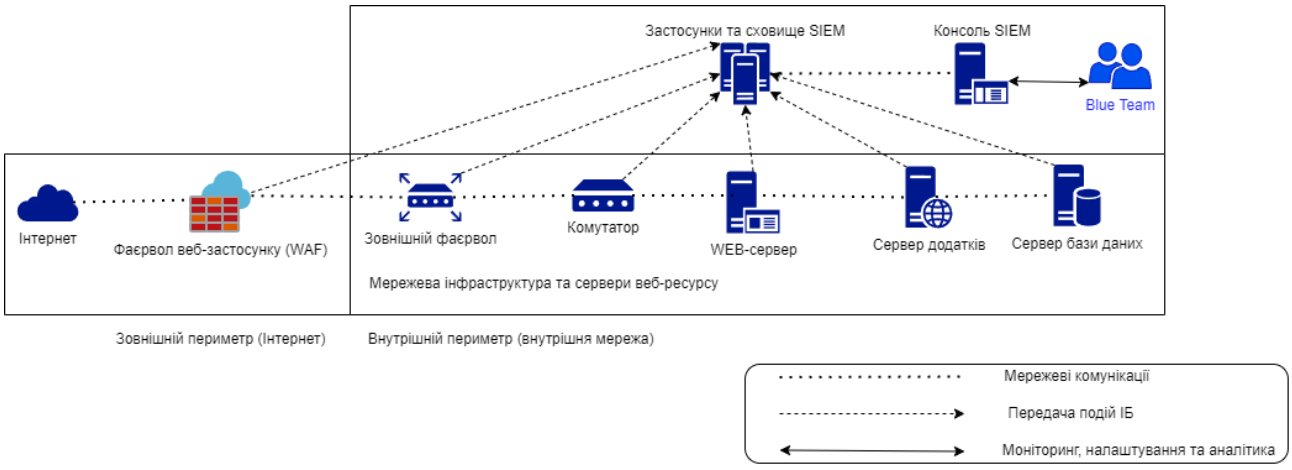

Рис. 3.5 Схема мережевої інфраструктури WEB-ресурсу та взаємодія з SIEM

Для оцінки ефективності процесів SOC використовуються різні типи метрик, включаючи [44]:

- Середній час виявлення інциденту або порушення ІБ. Час, що проходить від моменту виникнення інциденту до його виявлення.
- Середній час реагування на інцидент або порушення ІБ. Час, що проходить від моменту виявлення інциденту до початку реагування на нього.
- Середній час аналізу спрацювання кореляційного правила. Час, що витрачається на аналіз і підтвердження події безпеки після спрацювання кореляційного правила.
- Кількість сповіщень систем безпеки, порушень та інцидентів – вимірювання загальної кількості сповіщень, що генеруються системами безпеки, та кількість підтверджених порушень.
- Кількість пристроїв, що підключені до SIEM як джерела подій – загальна кількість пристроїв, які надсилають дані до SIEM для моніторингу та аналізу. Важливо також порівняти кількість джерел подій SIEM та кількість інформаційних пристроїв в організації й підключити відсутні джерела (хости) задля забезпечення контролю та моніторингу стану їх безпеки.

Використання цих метрик у комплексі дозволяє команді SOC систематично оптимізовувати робочі процеси та підготовку до майбутніх загроз. Постійний аналіз та оновлення цих метрик є невід'ємною частиною підтримання ефективності команди SOC і забезпечення безперервної відповідності до змінюваних умов інформаційного середовища. Впровадження регулярного моніторингу та звітування про ці метрики допомагає швидко ідентифікувати слабкі місця та вживати відповідних заходів для їх усунення.

3.5 Навчання співробітників SOC за результатами проведення імітаційних атак

Процес навчання співробітників SOC включає різні задачі, які виконують три основні команди: Red Team (червона команда), Purple Team (пурпурова

команда) та Blue Team (синя команда). Кожна з них відіграє свою специфічну роль у тренувальному циклі [45].

Операційні задачі команд в рамках процесу навчання SOC

- Red Team. Червона команда відповідає за підготовку та здійснення імітаційної атаки. Основні завдання команди:

1) Створення розгорнутого звіту: Докладний звіт за результатами атаки з нотацією всіх дій.

2) Консультація: Надання консультацій Purple та Blue командам.

3) Надання матеріалів: Інформація про інструменти та матеріали, використані для атаки.

4) Навчальні сесії: Проведення навчальних сесій для Blue Team.

- Purple Team. Пурпурова команда діє як посередник між червоною та синьою командами. Ця команда забезпечує:

1) Аналіз звітів: Опрацювання та аналіз звітів Red Team.

2) Координація: Координація дій Blue та Red Team.

3) Створення задач: Створення задач для Blue Team з покращення роботи контролів та систем захисту.

4) Оцінка роботи: Оцінка роботи Blue та Red команд під час та після здійснення імітаційної атаки.

- Blue Team. Синя команда відповідає за застосування набутих знань і реалізацію заходів захисту. Їх роль включає:

1) Опрацювання звітів: Робота зі звітами Red Team.

2) Виконання задач: Виконання задач від Purple Team.

3) Навчальні сесії: Участь у навчальних сесіях.

4) Аналіз подій ІБ: Перегляд усіх подій ІБ, пов’язаних з атакою.

5) Корекція контролів: Внесення коректив в існуючі контролі безпеки.

6) Виправлення конфігурацій: Виправлення конфігурації систем захисту та джерел подій.

Кожна з цих команд вносить унікальний вклад у процес навчання, що забезпечує комплексне розуміння та постійне вдосконалення інформаційної

безпеки в організації. Цей інтегрований підхід сприяє більш ефективному виявленню, реагуванню та запобіганню кіберзагрозам, підвищуючи загальний рівень кіберстійкості організації.

Комплексність навчання – залучення трьох команд забезпечує глибоке розуміння кіберзагроз.

Ефективність реагування – систематичний підхід дозволяє швидко виявляти та реагувати на інциденти.

Постійне вдосконалення – регулярне навчання та оцінка роботи команд сприяє підвищенню ефективності кібербезпеки.

Висновки до розділу 3

У третьому розділі роботи було розглянуто впровадження імітаційних моделей кібератак та оцінено їх вплив на ефективність роботи SOC. Представлено опис створеної моделі веб-атаки, що включала кроки від розвідки до отримання контролю над цільовою системою. Ця модель стала основою для збору метрик та аналізу роботи SOC, дозволяючи значно покращити процеси виявлення, реагування на інциденти та відновлення системи після атак.

Система SIEM забезпечила збір, аналіз та кореляцію подій безпеки з різних джерел, що значно сприяло підвищенню оперативності реакцій SOC на загрози. Завдяки детальному моніторингу та використанню метрик було проведено аналіз з метою оптимізації роботи команди. Основні метрики, такі як середній час виявлення інцидентів, середній час реагування та кількість сповіщень, дозволили оцінити та вдосконалити процеси SOC.

Навчання співробітників SOC за результатами проведення імітаційних атак виявилося важливим компонентом підвищення їх компетенцій. Використання імітаційних атак дозволило значно покращити здатність команди адекватно реагувати на кіберзагрози. Колаборація між Red, Purple та Blue командами забезпечила не лише обмін знаннями та досвідом, але й розробку ефективних

стратегій відповіді на інциденти, які стали основою для подальших тактик оборони від кібератак.

Загалом, впровадження імітаційних моделей кібератак, систематичний збір метрик та навчання співробітників SOC сприяло підвищенню рівня кібербезпеки організації. Комплексний підхід до аналізу та вдосконалення процесів SOC забезпечив більш ефективне виявлення, реагування та відновлення після кібератак, що значно підвищило кіберстійкість організації.

ВИСНОВКИ

Розглянувши структуру та впровадження імітаційних моделей кібератак, встановлено, що сучасні методики їх створення та застосування є ключовими для підготовки та тренування команд забезпечення кібербезпеки, зокрема SOC. Імітаційні моделі дозволяють відтворювати різноманітні сценарії атак, що сприяє реалістичному моделюванню потенційних загроз та вдосконаленню контролів безпеки. Це підходить як для виявлення уразливостей в існуючих системах, так і для оцінки ефективності заходів безпеки, що використовуються для їх усунення.

Навчання та розвиток команд SOC за допомогою імітаційних атак є невід'ємною частиною стратегічної підготовки кіберзахисту організацій. Регулярне проведення таких тренувань дозволяє не тільки виявляти слабкі сторони системи захисту, але й підвищує оперативність реагування на інциденти, забезпечуючи зміцнення захисних механізмів. Такі тренування формують у команди SOC навички, необхідні для ефективного реагування на реальні кібератаки, та сприяють розвитку професійної компетентності в умовах, максимально наближених до реальних.

Використання SIEM для моніторингу, аналізу та звітування про події безпеки підтвердило свою ефективність у забезпеченні об'єктивної оцінки роботи SOC. SIEM-системи дозволяють централізовано збирати та корелювати події з різних джерел, виявляючи складні атаки та аномалії в режимі реального часу. Впровадження комплексних метрик для вимірювання швидкості виявлення та реагування на загрози сприяє постійному вдосконаленню процесів кібербезпеки. Оцінка ефективності роботи SOC за допомогою таких метрик дозволяє своєчасно виявляти слабкі місця та підвищувати загальну ефективність захисту.

Постійне оновлення імітаційних моделей кібератак та адаптації їх до сучасних умов та загроз є важливим кроком для забезпечення заходів зі створення імітаційних моделей кібератак. Це включає систематичне оновлення

сценаріїв атак, інтеграцію новітніх технологій та методик, а також забезпечення безперервного навчання та підготовки команд SOC. Постійне вдосконалення моделей і методик імітаційних атак дозволяє організаціям бути готовими до нових викликів у сфері кібербезпеки, знижуючи ризики та підвищуючи рівень захисту.

Загалом, комплексний підхід до моделювання кібератак, регулярне оновлення методик та інструментів, а також інтеграція результатів імітаційних атак у стратегії кібербезпеки організації сприяють підвищенню загального рівня захисту інформаційних активів та кіберстійкості організації. Цей підхід забезпечує надійний захист від різноманітних загроз, підвищуючи ефективність заходів безпеки та сприяючи зниженню ризиків компрометації інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Allsopp W. Advanced penetration testing. Indianapolis, Indiana : John Wiley & Sons, Inc., 2017. URL: https://doi.org/10.1002/9781119367741 .

2. Baker K. 12 most common types of cyberattacks. www.crowdstrike.com. URL: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/.

3. Bejtlich R. Tao of network security monitoring: beyond int. Pearson Education, Limited, 2021.

4. Brown L., Stallings W. Computer security: principles and practice. Pearson, 2017. 800 p.

5. Cheng D. Cyber dragon: inside china's information warfare and cyber operations. ABC-CLIO, LLC, 2016.

6. Clark B. RTFM: red team field manual. Createspace Independent Publishing Platform, 2014. 96 p.

7. Conklin W. A., Shoemaker D. Cybersecurity: the essential body of knowledge. Delmar Cengage Learning, 2011. 528 p.

8. Conrad E. CISSP study guide. Burlington, MA : Elsevier, 2010.

9. Coursera Staff. What is the CIA triad?. www.coursera.org. URL: https://www.coursera.org/articles/cia-triad.

10. Hutchins E., Cloppert M., Amin R. Ntelligence-Driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. 2010. P. 14.

11. Kidd C. CIA triad: confidentiality, integrity & availability. www.splunk.com. URL: https://www.splunk.com/en_us/blog/learn/cia-triad-confidentiality-integrity-availability.html.

12. Kim P. The hacker playbook 3: practical guide to penetration testing. Independently published, 2018. 289 p.

13. McClure S., Shah S., Shah S. Web hacking: attacks and defense. Addison-Wesley Professional, 2002. 528 p.

14. Merkow M. S. Information security: principles and practices. Pearson IT Certification, 2014. 366 p.

15. Muniz J., AlFardan N., McIntyre G. Security operations center: building, operating, and maintaining your SOC. Cisco Press, 2015. 448 p.

16. Murdoch D. W. Blue team handbook: incident response edition : a condensed field guide for the cyber security incident responder. 2nd ed. 2014. 146 p.

17. Nathans D. Designing and building security operations center. Elsevier Science & Technology Books, 2014. 276 p.

18. Perlroth N. This is how they tell me the world ends: the cyberweapons arms race. Bloomsbury Publishing, 2022. 528 p.

19. Singer P. W., Friedman A. Cybersecurity and cyberwar: what everyone needs to know. Oxford University Press, 2014. 320 p.

20. Weidman G. Penetration testing: a hands-on introduction to hacking. No Starch Press, 2014. 528 p.

21. Allen L., Ali S., Heriyanto T. Kali linux: assuring security by penetration testing. Packt Publishing - ebooks Account, 2014. 541 p.

22. Allsopp W. Advanced penetration testing. Indianapolis, Indiana : John Wiley & Sons, Inc., 2017. URL: https://doi.org/10.1002/9781119367741.

23. Cache J., Liu V. Hacking exposed wireless (hacking exposed). McGraw-Hill Osborne Media, 2007. 386 p.

24. Cardwell K. Building virtual pentesting labs for advanced penetration testing. Packt Publishing, Limited, 2014.

25. Engebretson P. Basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier Science & Technology Books, 2013. 225 p.

26. Eperjesi A. SOC automation use cases: where to start. https://www.blinkops.com. URL: https://www.blinkops.com/blog/soc-automation-use-cases.

27. Erickson J. Hacking: the art of exploitation. 2nd ed. San Francisco, CA : No Starch Press, 2008. 472 p.

28. Harris S., Maymi F. CISSP: exam guide. McGraw-Hill Education, 2018. 1408 p.

29. Information security management principles / S. David et al. BCS Learning & Development Limited, 2020. 268 p.

30. Leary M., Andress J., Guretz D. Building a practical information security program. Elsevier Science & Technology Books, 2016. 202 p.

31. Mellen A. An actual complete list of soc metrics (and your path to DIY). www.cdotrends.com. URL: https://www.cdotrends.com/story/3905/actual-complete-list-soc-metrics-and-your-path-diy.

32. NIST Special Publication 800-53 Revision 5. Security and privacy controls for information systems and organizations. Replaces NIST Special Publication 800-53 Revision 4 ; effective from 2020-05-16. Official edition. Гейтерсберг : National Institute of Standards and Technology, 2020. 481 p.

33. Practical network security monitoring. No Starch Press,US, 2013.

34. Ramshet V. SoC SIEM Use Cases -. flexibleir.com. URL: https://playbooks.flexibleir.com/soc-siem-use-cases/.

35. Robinson M. T. V. Building virtual machine labs: a hands-on guide. Createspace Independent Publishing Platform, 2017. 600 p.

36. Stuttard D., Pinto M. Web application hacker's handbook: finding and exploiting security flaws. Wiley & Sons, Limited, John, 2011. 912 p.

37. Swartout P. Continuous delivery and devops - a quickstart guide. Packt Publishing, Limited, 2012.

38. Writer S. Implementing SOC use cases in your environment. techhyme.com. URL: https://techhyme.com/implementing-soc-use-cases-in-your-environment/.

39. Zenko M. Red team: how to succeed by thinking like the enemy. Basic Books, 2015.

40. Biniyaz J. Measuring SOC Effectiveness: Metrics & KPIs | ResilientX. resilientx.com. URL: https://resilientx.com/blog/measuring-the-effectiveness-of-security-operation-centers-metrics-and-key-performance-indicators/.

41. Coursera Staff. What is the purpose of the purple team?. www.coursera.org. URL: https://www.coursera.org/articles/purple-team.

42. Miessler D. The difference between red, blue, and purple teams. danielmiessler.com. URL: https://danielmiessler.com/p/red-blue-purple-teams/.

43. Tubberville J., Vest J. Red team development and operations: a practical guide. Independently Published, 2020. 220 p.

44. What is a purple team?. www.crowdstrike.com. URL: https://www.crowdstrike.com/cybersecurity-101/purple-teaming/.

45. Scapicchio M., Downie A., Finio M. What is a security operations center (SOC)?. *www.ibm.com*. URL: https://www.ibm.com/topics/security-operations-center.