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: “ РЕКОМЕНДАЦІЇ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ PURPLE TEAM ”

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

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

_____ Денис ДОБРОВОЛЬСЬКИЙ

(Підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Денис ДОБРОВОЛЬСЬКИЙ

Керівник:
ст. викл. Дмитро РАБЧУН

Рецензент:
д.т.н., професор Ім’я ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедрою УІКБ

_____ Світлана ЛЕГОМІНОВА

“____”_____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Добровольському Денису Ігоровичу

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Рекомендації щодо підвищення ефективності функціонування Purple Team”

керівник кваліфікаційної роботи Дмитро РАБЧУН, ст. викл.

(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “19“ жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи “18” грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління інформаційною безпекою, нормативні документи, стандарти,*

4. Перелік питань, які потрібно розробити:

   1. Здійснити теоретичний аналіз основних сучасних досліджень у галузі Purple Team та суміжних тем.
   2. Провести аналіз досвіду впровадження методології в різних організаціях ключових принципів та підходів Purple Team.
   3. Розробити пропозиції та рекомендації які спрямовані на покращення роботи Purple Team.
   4. Перелік ілюстративного матеріалу: *презентація*

5. Дата видачі завдання “02” жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: ”02” жовтня 2023 р..

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	виконано
2.	Збір та аналіз літератури.	15.10.2023	виконано
3.	Аналіз понять та принципів функціонування Purple Team	25.10.2023	виконано
4.	Огляд сучасних досліджень у галузі Purple Team та суміжних тем	11.11.2023	виконано
5.	Розробка та впровадження рекомендацій щодо підвищення ефективності функціонування Purple Team .	15.11.2023	виконано
6.	Формулювання висновків за результатами проведеного дослідження.	28.11.2023	виконано
7.	Оформлення роботи.	04.12.2023	виконано
8.	Оформлення презентації.	14.12.2023	виконано
9.	Отримання рецензії на роботу.	18.12.2023	виконано
10.	Захист в ДЕК.	18.01.2024	виконано

Здобувач вищої освіти _____ Денис ДОБРОВОЛЬСЬКИЙ
(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 магістра

Направляється здобувач Добровольський Д.І. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: “ Рекомендації щодо підвищення ефективності функціонування Purple Team”
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи
Здобувач **ДОБРОВОЛЬСЬКИЙ Денис**

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

“_____“____2024 року

Висновок кафедри про кваліфікаційну роботу

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Добровольського Денис Ігоровича

на тему "РЕКОМЕНДАЦІЇ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ PURPLE TEAM"

Актуальність

Позитивні сторони

1.

2.

3.

Недоліки

1.

Висновок:

Рецензент: професор кафедри Інформаційної та кібернетичної безпеки, д.т.н, професор _____ *підпис* *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 71 стор., 3 рис., 6 табл., 32 джерел.

Метою роботи Метою даної науково-дослідної практики є формулювання основних цілей та завдань, спрямованих на покращення роботи Purple Team, визначення сучасних викликів та загроз, що вимагають підвищеної ефективності методології Purple Team.

Об'єктом дослідження – діяльність Purple team.

Предмет дослідження – є фактори, що впливають на ефективність роботи purple team, та рекомендації щодо підвищення цієї ефективності.

Методи дослідження. Для вирішення поставленого наукового завдання в роботі були застосовано метод системного аналізу, теорія інформаційної безпеки та метод порівняння та теоретичного узагальнення, аналізу та синтезу.

Короткий зміст роботи. У роботі проведено аналіз сучасних досліджень у галузі Purple Team, ключових принципів та підходів, висвітлено переваги та недоліки існуючих практик. Проаналізовано сучасні загрози та атаки які враховуються при використанні методології. В заключному розділі проведений аналіз використання Purple Team у реальних сценаріях, впроваджено перелік рекомендацій та перспективи розвитку методології у майбутньому.

Галузь застосування. Розглянуті методики, рекомендації щодо підвищення ефективності функціонування можуть бути застосовані в будь-якій організації, яка хоче підвищити свій рівень кібербезпеки.

КЛЮЧОВІ СЛОВА: ПІДВИЩЕНА ЕФЕКТИВНІСТЬ, ФУНКЦІОНУВАННЯ, РЕКОМЕНДАЦІЇ, МЕТОДОЛОГІЯ, ДОСЛІДЖЕННЯ, БЕЗПЕКА.

ABSTRACT

The text part of the qualifying work for the Master's degree: 76 pages, 3 figures, 6 tables, 32 sources.

The purpose of the work is to formulate the main goals and tasks aimed at improving the Purple Team's operations, identifying modern challenges and threats that require enhanced effectiveness of the Purple Team methodology.

The object of the research is the activities of the Purple team.

The subject of the study is the factors affecting the effectiveness of the purple team and recommendations for improving its effectiveness.

Research methods: To address the set scientific task, the work applies methods of systemic analysis, information security theory, comparison and theoretical generalization, as well as analysis and synthesis.

Brief summary of the work: The paper analyzes current research in the field of Purple Team, key principles and approaches, highlighting the advantages and disadvantages of existing practices. Modern threats and attacks considered in the use of Purple Team are analyzed. In the conclusion, an analysis of real-world scenarios is conducted, a list of recommendations and prospects for the development of the methodology in the future is introduced.

Field of research: The methodologies and recommendations for improving effectiveness can be applied in any organization that aims to enhance its cybersecurity level.

KEYWORDS: ENHANCED EFFECTIVENESS, FUNCTIONING, RECOMMENDATIONS, METHODOLOGY, RESEARCH, SECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ – інформаційна безпека

ІС – інформаційна система

СУІБ – система управління інформаційною безпекою

ISO – International Organization for Standardization

IEE – Institute of Electrical and Electronics Engineers

SIEM – Security Information and Event Management

DLP – Data Loss Prevention

PT – Purple Team

RT – Read Team

BT – Blue Team

DFIR - Digital Forensics and Incident Response

CTI - Cyber Threat Intelligence

SOC - Операційний центр безпеки

ВСТУП

У сучасному світі, в якому все більше і більше уваги надається кібербезпеці, організації стикаються з постійним шквалом витончених загроз від зловмисників. Для ефективного захисту від цих “еволюціонуючих” з кожним днем загроз, надійні заходи кібербезпеки мають вирішальне значення. Одним з найважливіших елементів таких заходів є “Purple Team” (фіолетова або пурпурова команда) - спільний підрозділ, що складається з червоних і синіх команд, який бере участь в імітації атак і захисних заходів для тестування і вдосконалення системи безпеки організації. Однак навіть добре сформовані фіолетові команди можуть отримати вигоду від постійного вдосконалення та оптимізації. Це дослідження зосереджується саме на цьому, маючи на меті підвищити ефективність роботи фіолетових команд за допомогою набору стратегічних рекомендацій.

Актуальність цієї теми є багатогранною. По-перше, кібератаки постійно зростають у частоті та складності, що вимагає гнучких та ефективних засобів захисту. Посилення Purple Team, яка відіграє ключову роль у виявленні вразливостей і тестуванні засобів контролю безпеки, безпосередньо відповідає цій потребі. По-друге, існуючі дослідження акцентують увагу на теоретичних основах роботи фіолетових команд. Це дослідження заглиблюється глибше, пропонуючи практичні, дієві рекомендації, засновані на всебічній оцінці реальної Пурпурової команди. Такий прагматичний підхід гарантує, що результати дослідження будуть легко застосовні та ефективні.

Ця робота переслідує дві основні мети. Перша полягає у визначенні сфер для вдосконалення в досліджуваній фіолетовій команді. Завдяки ретельному аналізу сильних і слабких сторін, можливостей і загроз, дослідження виявляє прогалини та неефективність, які перешкоджають оптимальній роботі. Друга мета - розробити чіткий план для впровадження покращень. Цей план підкреслює пріоритетні рекомендації з чіткими вказанням впровадження, забезпечуючи відчутний прогрес на шляху до збільшення ефективності Purple Team.

Очікувані результати цього дослідження мають значну практичну цінність. Очікується, що завдяки впровадженню запропонованих рекомендацій Purple Team отримає рекомендації та поради щодо підвищення ефективності:

Підвищення рівня виявлення та реагування: Оптимізація процесів Purple Team може призвести до швидшого виявлення та пом'якшення кіберзагроз.

Покращення моделювання атак та навчань: Більш реалістичні та складні симуляції краще підготують організацію до реальних атак.

Посилення співпраці та комунікації: Ефективні операції Purple Team сприяють міжфункціональній співпраці та обміну інформацією, зміцнюючи загальний стан безпеки.

Скорочення часу на усунення інцидентів: Оптимізовані процеси та вдосконалення навичок дозволяють швидше реагувати на порушення безпеки, мінімізуючи потенційні збитки.

Отже, ця робота розглядає дуже актуальну тему, яка може значно підвищити ефективність "Purple Team". Визначаючи конкретні сфери для вдосконалення і надаючи конкретний план для реалізації, надає практичні рекомендації, які можуть призвести до посилення кібербезпеки і зниження ризиків для організацій у різних сферах.

Об'єкт дослідження - функціонування Purple Team.

Предмет дослідження – ефективність функціонування Purple Team.

Мета роботи полягає у формулювання основних цілей та завдань, спрямованих на покращення роботи Purple Team..

Для досягнення цієї мети в роботі виконано наступні *завдання:*

1. Здійснено аналіз наукової літератури та публікацій, досліджень пов'язаних із функціонуванням Purple Team або Фіолетової команди.

2. Проаналізовано тенденцію сучасних загроз та атак, що враховується при використанні Purple Team.

3. Розроблено перелік рекомендацій які покращать функціонування Purple Team, методики оцінки ефективності за допомогою критеріїв та метрик.

4. Проаналізована перспектива розвитку Purple Team у майбутньому.

РОЗДІЛ 1
Огляд сучасних досліджень у галузі Purple Team та суміжних тем

1.1 Огляд сучасних досліджень у галузі Purple Team

Purple Team є відносно новим підходом до забезпечення кібербезпеки, але він швидко набирає популярності. Це пов'язано з тим, що такий підхід дозволяє більш ефективно протидіяти кіберзагрозам, які стають все більш складними та небезпечними.

Термін "Purple Team" був вперше введений у 2016 році компанією Microsoft. Він походить від поєднання двох кольорів: синього (blue team), який символізує захист, і червоного (red team), який символізує атаку.

Сучасні дослідження в галузі Purple Team зосереджені на наступних напрямках:

Розробка методів та інструментів для ефективного співробітництва між командами безпеки та операційними командами. Це включає в себе розробку спільних мов, методологій та процесів, а також створення інструментів, які допомагають командам спілкуватися та співпрацювати в реальному часі.

Вдосконалення методів для оцінки та підвищення ефективності Purple Team. Це включає в себе розробку метрик ефективності, які можна використовувати для вимірювання успіху Purple Team, а також розробку методів для проведення навчань та оцінки Purple Team.

Розширення застосування Purple Team на нові сфери, такі як кібербезпека критичної інфраструктури та кібервійна. Це включає в себе розробку методів для адаптації Purple Team до специфічних потреб цих сфер.

Одним із важливих напрямків досліджень у галузі Purple Team є розробка методів та інструментів для ефективного співробітництва між командами безпеки та операційними командами. Це важливо, оскільки успіх Purple Team залежить від того, наскільки добре ці дві команди можуть працювати разом.

Однією з проблем, з якою стикаються команди безпеки та операційні

команди, є те, що вони використовують різні мови та методи. Команди безпеки часто використовують технічну мову, яка може бути незрозумілою для операційних команд. Операційні команди, з іншого боку, часто використовують бізнес-мову, яка може бути незрозумілою для команд безпеки.

Щоб вирішити цю проблему, дослідники розробляють спільні мови та методології, які можуть використовуватися як командами безпеки, так і операційними командами. Наприклад, деякі дослідники розробляють спільні описи загроз, які можуть використовуватися командами безпеки та операційними командами для спільної оцінки загроз.

Дослідження Lares 2022 року висвітлили п’ять найпоширеніших помилок з якими зіштовхувалися працівники компанії під час роботи.

1. *Непридатне або зайве ведення журналу подій:* Багато організацій повинні приділяти більше уваги критичним подіям у журналах або збирати занадто багато зайвих подій, які заповнюють сховища та приховують важливі дані. У своєму недбалому ставленні вони можуть упустити критичні ознаки зловмисної діяльності.

2. *Відсутність знань в області атакуючої безпеки:* Моніторинг оточення організації на предмет потенційних загроз вимагає більше, ніж просте базове розуміння атакуючих тактик, технік та процедур (TTP). Важливо визначати, коли та як використовуються ці TTP для вжиття належних заходів для захисту організації. Наприклад, нагляд за безпекою може передбачати моніторинг внутрішньої комунікації для виявлення можливих індикаторів зловмисної діяльності.

3. *Співзалежні відносини в SOC :* багато керованих операційних центрів безпеки (SOC) створюють нові проблеми для команд захисту, а не вирішують їх. Затримки сповіщень виникають, коли керований SOC не вдається належним чином налаштувати інструменти та технології для виявлення інцидентів безпеки та реагування на них. Події, які можуть бути використані для запобігання атакам, відкладаються або взагалі не видно. Крім того, керовані SOC часто пригнічують критичні події через тиск з боку вищого керівництва або зовнішніх клієнтів.

4.*Надмірна залежність від інструментів:* Захисники стають занадто залежними від рішень з виявлення та реагування на кінцевих точках (EDR) та розширених рішень з виявлення та реагування (XDR), чекаючи, що вони виявлять всі зловмисників. Це може призвести до помилкових сигналів та невірної атрибуції. EDR і XDR слід розглядати як частину широкого захисного рішення, а не єдиний пункт моніторингу.

5.*Марнотратство ресурсів:* Зазвичай організації віддають свої знання щодо захисних заходів на зовнішнє замовлення. Хоча це може здаватися найпростішим рішенням, воно завдає більше шкоди, ніж користі і перешкоджає працівникам набувати важливі навички, необхідні для ефективності, що коштує компанії більше грошей у довгостроковій перспективі. Замість повного замовлення всіх знань з безпеки компанії слід інвестувати в своїх працівників і дозволяти їм вчитися та розвиватися.

Іншим напрямком досліджень у галузі Purple Team є вдосконалення методів для оцінки та підвищення ефективності Purple Team. Це важливо, оскільки дозволяє організаціям оцінити, наскільки ефективно їхні Purple Team працюють, і внести необхідні покращення.

Одним із методів для оцінки ефективності Purple Team є використання метрик ефективності. Метрики ефективності - це показники, які можна використовувати для вимірювання успіху Purple Team. Наприклад, однією з метрик ефективності може бути кількість успішних інцидентів, які були попереджені або виявлені Purple Team.

Наступним методом для оцінки ефективності Purple Team є проведення навчань, тренувань та оцінки Purple Team. Ці підходи Purple Team можуть допомогти організаціям виявити потенційні проблеми та внести необхідні покращення.

Останнім напрямком досліджень у галузі Purple Team є розширення застосування Purple Team на нові сфери. Наприклад, дослідники вивчають, як Purple Team можна використовувати для захисту критичної інфраструктури та для кібервійни.

Захист критичної інфраструктури є важливим завданням, оскільки критична інфраструктура є життєво важливою для економіки та суспільства. Purple Team можна використовувати для захисту критичної інфраструктури, шляхом оцінки загроз, виявлення інцидентів та реагування на них.

Сучасні дослідження в галузі Purple Team сприяють розвитку цього підходу до кібербезпеки. Ці дослідження допомагають організаціям ефективніше захищатися від кібератак.

Ситуація в галузі кібербезпеки являє собою постійне перетягування каната між зловмисниками і захисниками. Традиційні підходи покладалися на окремі червоні команди (що імітують нападників) і сині команди (відповідальні за захист), які працюють ізольовано. Це часто призводить до появи "сліпих зон" і неефективності виявлення загроз і реагування на них. Саме тут концепція Purple Team стає потужним переломним моментом.

Фіолетові команди, спільний підрозділ, що складається з членів наступальних (червоних) і захисних (синіх) команд, беруть участь у симуляції атак і захисту. Це безперервне середовище спарингу дає їм змогу тестувати й удосконалювати стан безпеки організації, виявляти вразливості та розробляти ефективніші стратегії реагування на інциденти. Їхня унікальна здатність долати розрив між нападом і захистом сприяє розвитку культури безперервного навчання і вдосконалення, що в кінцевому підсумку підвищує загальну готовність організації до кібербезпеки.

Однак, незважаючи на їх незаперечну цінність, навіть Пурпурні команди, які добре зарекомендували себе, можуть втрачати свою ефективність. Прогалини в процесах, недостатність навичок можуть перешкоджати їхній здатності оптимально виявляти, аналізувати та реагувати на кіберзагрози. Це підкреслює гостру необхідність постійного оцінювання та покращення діяльності.

1.2 Вивчення досвіду впровадження методології в різних організаціях

Purple Team об'єднує в собі представників різних команд, що відповідають за безпеку, таких як кібербезпека, операційна безпека, кіберрозвідка та

кіберполіція. Це дозволяє ефективно обмінюватися інформацією та співпрацювати для виявлення та протидії кіберзагрозам.

Проактивність. Purple Team не просто реагує на кібератаки, а й намагається їх передбачити та запобігти. Для цього команда використовує різні методи, такі як кіберрозвідка, аналіз загроз та моделювання безпеки.

Ефективність. Purple Team працює в єдиному командному просторі, що дозволяє їй швидко та ефективно приймати рішення.

Конкретні функції Purple Team можуть відрізнятися в різних організаціях, але в цілому вони включають в себе наступне:

• Розробка та впровадження політики та процедур безпеки.

• Виявлення та реагування на кіберзагрози.

• Проведення кібертренінгів та підвищення обізнаності про кібербезпеку.

• Розробка та впровадження нових методів і технологій безпеки.

Компанія Google використовує Purple Teams з 2018 року. У рамках програми Purple Team, яку компанія запустила в 2018 році, Google створила команду Purple Team, яка складалася з фахівців з кібербезпеки, IT-інженерів і бізнес-аналітиків.

Команда Purple Team компанії Google проводить регулярні симуляції кібератак, щоб відпрацьовувати свої навички виявлення і відбиття атак.

Симуляції кібератак проводяться за допомогою спеціального програмного забезпечення, яке називається Cyber Range. Cyber Range - це віртуальна середовище, в якому можна відтворити різні сценарії кібератак.

Симуляції кібератак проводяться за наступним сценарієм:

1. Команда Purple Team розробляє сценарій кібератаки. Сценарій може включати в себе такі елементи, як:

- Тип кібератаки
- Мета кібератаки
- Методи і інструменти, які будуть використовуватися для проведення

2. Проводиться симуляція кібератаки на цільові системи і мережі.

3. Команда, яка відповідає за захист цільових систем і мереж, намагається

виявити і відбити кібератаку.

4. Після проведення атаки Purple Team оцінює ефективність дій команди, яка відповідає за захист цільових систем і мереж, такі як:

- Вчасність виявлення кібератаки
- Ефективність відбиття кібератаки
- Методи та інстументи які були застосовані під час атаки та інш.

Симуляції кібератак повинні проводитися регулярно, щоб відпрацьовувати свої навички виявлення і відбиття атак.

Ось кілька прикладів сценаріїв кібератак, які використовувалися компанією Google:

- Вторгнення в систему
- Шахрайство
- Фішинг
- Розкрадання даних
- Порушення роботи системи

Завдяки впровадженню Purple Team, компанія Google змігла підвищити ефективність свого захисту від кібератак.

- У 2020 році команда Purple Team компанії Google виявила і відбила атаку, яка була спрямована на крадіжку конфіденційної інформації з однієї з інфраструктурних систем компанії.
- У 2021 році команда Purple Team компанії Google виявила і відбила атаку, яка була спрямована на порушення роботи однієї з критичних програмних систем компанії.

Компанія Google вважає, що Purple Teams є ефективним способом підвищення кібербезпеки. Компанія планує продовжувати впроваджувати Purple Teams в інших своїх підрозділах.

Компанія Google дає такі поради іншим компаніям, які розглядають можливість впровадження Purple Team:

- Почніть з невеликої команди. Не потрібно створювати велику команду Purple Team з самого початку. Почніть з невеликої команди, яка зможе швидко і

ефективно виявляти і відбивати кібератаки.

• Залучіть представників різних відділів. Команда Purple Team повинна складатися з представників різних відділів компанії, таких як кібербезпека, IT, операції та бізнес. Це допоможе команді краще зрозуміти потреби один одного і працювати разом над підвищенням кібербезпеки.

• Проводьте регулярні тренінги. Члени команди Purple Team повинні регулярно проходити тренінги з питань кібербезпеки. Це допоможе їм підтримувати свої навички на високому рівні.

Компанія Google вважає, що ці поради допоможуть компаніям успішно впровадити Purple Team.

1.3 Аналіз ключових принципів та підходів Purple Team

Впровадження Purple Team вимагає значних зусиль та ресурсів, але це може бути ефективним способом підвищення кібербезпеки організації.

Концепція Purple Team являє собою динамічний і спільний підхід до кібербезпеки, що усуває розрив між традиційними червоними і синіми командами. Це сприяє розвитку культури постійного вдосконалення шляхом об'єднання наступальних і оборонних можливостей в єдиний підрозділ.

Purple Team (фіолетова команда) - це спільна команда з кібербезпеки, що складається з людей, які мають як наступальний Red Team (червона команда), так і захисний Blue Team (синя команда) досвід. Для успішного впровадження Purple Team (PT) очікується, що Blue Team (BT) та Red Team (RT) встановлять відмінний робочий взаємозв'язок та максимально співпрацюватимуть, створюючи унікальний досвід навчання та покращуючи взаємопізнання одне одного.

Рис. 1.1 Класифікація purple team

Також слід враховувати бар'єри між різними зацікавленими сторонами, які можуть ускладнювати взаєморозуміння через різні типи знань і експертизи. Оскільки інформація повинна переходити між різними командами, мову слід адаптувати так, щоб всі учасники мали спільне розуміння. Сторони повинні бути відкритими та уважними, щоб створити міст для відкритого обговорення та моделювати таку кооперативну поведінку. Для сприяння такій поведінці RT повинна вести приклад, чітко пояснюючи свої тактики та цілі BT, визнаючи області сильних сторін і поступово розкриваючи розмову щодо тих аспектів, які потребують вдосконалення. Це може бути здійснено через проведення живої корекції для вдосконалення існуючих контролів або впровадження нових, наприклад.

Ключові функції фіолетової команди:

Моделювання кібератак: PT проводять реалістичне моделювання атак, щоб перевірити ефективність заходів безпеки, виявити вразливості та оцінити можливості організації реагування на інциденти.

Оцінювання вразливостей і тестування на проникнення: вони виконують комплексні оцінювання вразливостей і тести на проникнення, щоб виявити і використовувати слабкі місця в системах і мережах організації.

Розробка та вдосконалення політик і процедур безпеки. На основі своїх висновків PT допомагають організаціям розробляти й удосконалювати політики

та процедури безпеки для усунення виявлених вразливостей і поліпшення загального стану безпеки.

Проведення навчань з реагування на інциденти. Проводять реалістичні навчання з реагування на інциденти, щоб перевірити і поліпшити здатність організації виявляти, реагувати і відновлюватися після кібератак.

Навчання та розвиток навичок: фіолетова команда дозволяє синім командам вивчати наступальні прийоми червоних команд, допомагаючи фахівцям із безпеки покращити свої навички кібербезпеки та розуміння вразливостей.

Конкретний склад Purple Team варіюватиметься залежно від розміру організації, галузі та конкретних потреб. Однак зазвичай до нього входять люди, які мають досвід у таких галузях:

Червона команда: фахівці з наступальної безпеки, хакери і тестери на проникнення, що моделюють кібератаки.

Синя команда: аналітики безпеки, фахівці з реагування на інциденти і захисники мереж, які зосереджені на захисті систем і мереж організації.

Додаткові ролі: Залежно від потреб організації до "фіолетової команди" можуть також входити люди, які мають досвід у сфері криміналістики, аналізу загроз і юридичних питань.

Загалом концепція Purple Team(PT) пропонує потужний підхід до підвищення кібербезпеки організації шляхом об'єднання наступальних і оборонних перспектив у середовищі співпраці. Постійно тестуючи й удосконалюючи рівень безпеки за допомогою моделювання атак і навчань, PT допомагає організаціям випереджати кіберзагрози, що розвиваються, і створювати більш стійку інфраструктуру безпеки.

Введення в дію цих концепції PT включає підхід який здебільшого складається з цих чотирьох фаз

Фаза 1: Збір інформації про загрози. Кібер-відомості про загрози (CTI) надають фактологічні знання, контекст, індикатори та поведінку потенційних загроз, які можуть впливати на організацію. Ця фаза передбачає збір даних про

загрози та розповсюдження аналізу для Червоної та Синьої команд.

Використовуючи цю інформацію, команди отримують цінні уявлення про тактику та методи, які використовуються адверсарами, і мають можливість розробляти ефективні контрзаходи.

Фаза 2: Підготовка вправи. Підготовка має важливе значення для успішного проведення вправи PT. На цій фазі Purple Team визначає мету та об'єктиви вправи, встановлює будь-які вказівки чи обмеження для Червоної та Синьої команд. З ретельною підготовкою PT забезпечує фокус, актуальність та відповідність вправи потребам безпеки організації.

Фаза 3: Виконання вправи Purple Team. Під час виконання Червона команда, представляючи атакуючих, емулює сценарії загроз реального світу і намагається використати вразливості в системах та мережах організації.

Синя команда, яка складається з оборони організації, активно моніторить та захищається від цих симульованих атак. Вони аналізують тактики, техніки та процедури (TTPs) Червоної команди, щоб отримати уявлення про можливі слабкі місця в їхніх стратегіях оборони.

Фаза 4: Перегляд та документування вивчених уроків. Після серії симульованих атак Червона та Синя команди обговорюють застосовані методології і працюють разом для розуміння вразливостей в системі, а також способів посилення безпеки організації.

Після завершення процесу команда Purple фіксує отримані звіти. Координатори документують протоколи, нотатки, завдання та отримують зворотний зв'язок від учасників та спонсорів. З цих даних вони створюють комплексний документ "вивчених атак". Цей звіт надає roadmap (карту маршруту) для подальших поліпшень та коригувань стану безпеки організації.

Для успішного проведення процесу Purple Team організації повинні дотримуватися таких найкращих практик:

1.Кларифікувати об'єктиви вправи Purple Team, вказуючи, які аспекти інфраструктури безпеки будуть протестовані та очікувані результати.

2.Залучати кваліфікованих фахівців із Червоної та Синьої команд з

необхідними навичками для реалістичного, ефективного тестування та продуктивної співпраці.

3.Збудовувати співпрацю, включаючи відкриту комунікацію, обмін знаннями та підтримуюче середовище, де команди можуть вільно обмінюватися інформацією, уявленнями та вивченими уроками.

4.Використовувати реалістичні сценарії, що емулюють загрози реального світу та актуальні техніки атак для надання точних уявлень про безпековий стан організації.

5.Постійно вдосконалювати, переглядати та оновлювати заходи безпеки на основі висновків та рекомендацій вправ.

6.Документувати та відстежувати виявлені під час вправ висновки, вразливості та рекомендації, відстежуючи прогрес у вирішенні слабкій місць та вимірюючи ефективність підвищень у сфері безпеки.

7.Залучати стейкхолдерів, таких як вищий менеджмент та відповідні відділи, щоб створити усвідомленість кібербезпекових ризиків, отримати підтримку для ініціатив з безпеки та полегшити необхідні зміни.

8.Налаштовувати та масштабувати вправи Purple Team під конкретні потреби та розмір організації, пристосовуючи підхід до нових технологій, загроз та бізнес-вимог при еволюції організації.

1.4 Висвітлення переваг і недоліків існуючих практик

Концепція фіолетової команди швидко отримала популярність у кібербезпекових спільнотах. Вона була прийнята багатьма організаціями, включаючи урядові агентства, великі підприємства та невеликі компанії. Зокрема, роль та ефективність команд Red Team і Blue Team стали предметом суперечок та дебатів. У цьому контексті також з'явився новий підхід - Purple Team, що спрямований на інтеграцію червоної та синьої команд для досягнення синергії та покращення захисту.

Для кращого розуміння та вибору оптимального підходу, наведена нижче таблиця порівняння Red Team, Blue Team та Purple Team яка виокремлює

ключові риси та характеристики кожного з підходів яка допомагає визначити оптимальну стратегію для забезпечення високого рівня кібербезпеки в конкретному контексті.

Таблиця 1.1.

Характеристика	Червона команда	Синя команда	Фіолетова команда
Наступальна безпека	+	-	+
Оборонна безпека	-	+	+
Співпраця	Ні	Ні	Так
Загальні сертифікації	OSCP, GPEN, PenTest+, GXPN, OWASP, BSCP	Security+, GSEC, CISSP, CGIH, CSA, CTIA, CYSA+, CCSP	GDAT, CPTA, OSCP, CEH, CGIH, Security+
Допомога в покращенні безпеки	Так	Так	Так

Так як Purple Team це відносно нова концепція, яка має потенціал для підвищення кібербезпеки організацій, яка набрала популярності у більшості великих компаній, банків та звичайних організацій вона має свої переваги і недоліки з котрими потрібно працювати.

Існує багато різних практик, які часто можуть бути використані організаціями.

Деякі з найбільш поширених практик включають:

- Фахове навчання та розвиток: Команди червоних та синіх повинні мати відповідне навчання та розвиток, щоб ефективно виконувати свої ролі.
- Спільні тренування: Команди червоних та синіх повинні регулярно проводити спільні тренування, щоб практикуватися в роботі разом.
- Інтеграція інструментів: Організації повинні використовувати інструменти, які дозволяють командам червоних та синіх співпрацювати ефективно.

Організації також вільні розробляти власні практики Purple Team, які відповідають їхнім конкретним потребам. Далі наведено приклади переваг та недоліки деяких часто застосованих практик.

Підвищена безпека: моделюючи реальні атаки і виявляючи слабкі місця, Purple Team допомагають організаціям зміцнити свій захист і усунути вразливості, перш ніж вони будуть використані реальними зловмисниками.

Поліпшення співпраці та комунікації. Спільний характер команди сприяє спілкуванню та обміну знаннями між наступальними та оборонними командами, що призводить до більш уніфікованого та ефективного підходу до забезпечення безпеки.

Постійне навчання та вдосконалення. Постійна участь у модельованих атаках і навчаннях дає змогу залишатися на передньому краї розвитку кіберзагроз, даючи їм змогу згодом адаптуватися і вдосконалювати свої навички та стратегії.

Зниження ризику та збитків. Шляхом попереджувального виявлення та усунення вразливостей Purple Team допомагають організаціям мінімізувати потенційний вплив кібератак і знизити ризик витоку даних та інших інцидентів безпеки.

Не зважаючи на численні переваги фіолетової команди, вона також, може включає деякі недоліки, які важливо врахувати при розгляді практик та враховувати їх. Розглянемо деякі з важливих аспектів, котрім слід надати уваги:

Опір змінам: Перехід до підходу Purple Team може спричинити опір з боку існуючих червоних та синіх команд, звиклих працювати незалежно. Чітка комунікація та стратегії управління змінами є ключовими для подолання цього перешкоди.

Обмеження ресурсів: Інтеграція та утримання вимагає відділених ресурсів, включаючи персонал, інструменти та інфраструктуру. Тому, організації повинні ретельно оцінити свої потреби та обмеження бюджету перед впровадженням.

Відсутність навичок: Деяким командам може бракувати необхідних навичок та експертизи для ефективного проведення червоних та синіх вправ.

Інвестування в програми навчання та розвитку є важливим для заповнення будь-яких відсутностей у навичках та забезпечення успіху фіолетової команди.

Метрика та оцінка: Вимірювання ефективності може бути складним завданням. Встановлення чітких метрик та KPI, відповідних організаційним цілям забезпечення безпеки, є важливим для відстеження прогресу та демонстрації цінності ініціативи.

Висновки до першого розділу

Концепція Purple Team є відносно новим підходом до кібербезпеки, який має потенціал для підвищення ефективності захисту організацій.

Фіолетові команди об'єднують наступальні та оборонні команди в єдиний підрозділ, що сприяє більш ефективній співпраці та комунікації, а також підвищує рівень знань та навичок у галузі кібербезпеки.

Однак, впровадження Purple Team також може включати деякі виклики, такі як опір змінам, обмеження ресурсів та відсутність навичок.

Організації, які розглядають можливість впровадження Purple Team, повинні ретельно оцінити свої потреби та ресурси, а також розробити чіткі плани управління змінами та навчанням.

У розділі було проведено аналіз переваг та недоліків Purple Team, для чіткішого розуміння, було розглянуто сучасні дослідження у галузі Purple Team, проаналізовано впровадження методології до різних компаній та організацій та їх досвід.

Концепція Purple Team все ще перебуває в процесі розробки та впровадження. Очікується, що в майбутньому вона стане все більш поширеним підходом до кібербезпеки, оскільки організації шукають способи підвищити ефективність свого захисту.

РОЗДІЛ 2.
Критичний огляд сучасних тенденцій кіберзагроз

2.1. Аналіз сучасних загроз та атак, що враховується при використанні Purple Team

"Purple Team" - це методологія, яка об'єднує червоний (Red Team) та синій (Blue Team) підходи до забезпечення кібербезпеки. Вона спрямована на вдосконалення заходів безпеки та виявлення слабких місць у системах оборони. Основна ідея полягає в тому, щоб забезпечити співпрацю між атакуючим (червоний) та захисним (синій) елементами для покращення відповіді на загрози.

Сучасні технології несуть у собі безліч загроз для безпеки, і однією з найпоширеніших є соціальний інжиніринг. Це не атака на технічному рівні; це скоріше мистецтво обману та маніпуляції людьми. Зловмисники використовують соціальний інжиніринг для отримання конфіденційної інформації, враховуючи дедалі складніші кібератаки, дуже важливо, щоб організації мали комплексну систему безпеки.

MITRE ATT&CK - це база знань яка доступна для кожного та яка має дані про тактику і техніки супротивників, заснована на спостереженнях у реальному світі. База знань ATT&CK використовується як основа для розробки конкретних моделей загроз та методологій у приватних підприємствах, уряді та послуг з кібербезпеки.

Система яка допомагає вирішити безліч проблем пов’язаних з атаками, також об’єднує спільноти для розробки більш ефективних засобів для кібербезпеки. ATT&CK відкритий і доступний будь-якій особі або організації для використання безкоштовно[26].

ATT&CK включає в себе різні тактики та техніки, які використовуються зловмисниками на всіх етапах кібератаки. Ця інформація допомагає організаціям розуміти загрози та розробляти ефективні стратегії захисту.

ATT&CK Framework охоплює широкий спектр атак та технік, відзначаючи їх за тактичними етапами та докладно описуючи конкретні методи використання.

Кожна тактика включає різні техніки, які можуть бути використані для досягнення цілей цієї тактики.

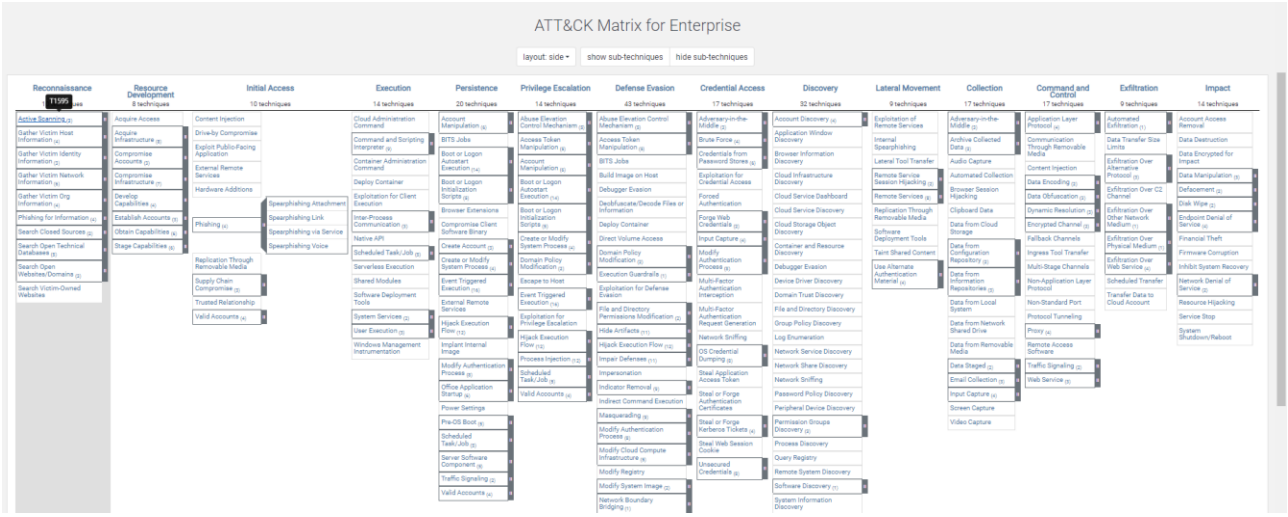

Рис. 2.1 Матриця тактик та технік ATT&CK

ATT&CK Framework використовується як інструмент для аналізу кіберзагроз та вдосконалення стратегій кіберзахисту. Організації можуть використовувати його для виявлення слабких місць у своїх захисних стратегіях та вдосконалення заходів захисту. Далі наведена таблиця для кращого розуміння основник Тактик ATT&CK .

Таблиця 2.1

Тактика	Техніки (Приклади)
Початковий доступ (Initial Access)	Спосіб отримання атакуючими початкового доступу до системи чи мережі.
Виконання (Execution)	Виконання шкідливого коду чи команд для досягнення своїх цілей.
Стійкість (Persistence)	Техніки, які дають змогу атакуючим залишатися в системі після початкового доступу.
Підняття прав (Privilege Escalation)	Техніки, спрямовані на підняття рівня прав атакуючого для отримання більш високих привілеїв.
Ухилення від захисту (Defense Evasion)	Техніки, спрямовані на ухилення від виявлення та блокування захисних механізмів.
Доступ до облікових записів та записів (Credential access)	Техніки, які використовуються для отримання доступу до облікових записів, паролів та інших автентифікаційних даних.
Виявлення (Discovery)	Техніки, що дозволяють атакуючому виявляти та збирати інформацію про цільову систему.
Горизонтальний рух (Lateral Movement)	Техніки, спрямовані на рух у мережі та розповсюдження вірусів після отримання початкового доступу.

Тактика	Техніки (Приклади)
Збір інформації (Collection)	Техніки, які атакуючі використовують для збору конкретної інформації під час атаки.
Виведення (Exfiltration)	Техніки, які атакуючі використовують для виведення зібраної інформації зі системи чи мережі.
Вплив (Impact)	Техніки, спрямовані на спричинення шкоди системі чи даним, зазвичай внаслідок атаки.

Отож, фреймворк MITRE ATT&CK ідеально компонує для Purple Team, адже вона має широкий спектр тактик, прийомів і процедур, які кожен спеціаліст може використовувати для організації свого тестування та стратегії. Це безцінний ресурс для фіолетових команд, щоб визначити пріоритетність тестування, інвестування та планування в міру розвитку стратегій для протидії новим і існуючим загрозам.

Загроза полягає в тому, що атаки, спрямовані на отримання конфіденційної інформації, не завжди використовують технічні вразливості. Замість цього вони використовують вразливості в людському факторі. Соціальні інженери вивчають поведінку користувачів та використовують цю інформацію для створення докладних схем обману, які можуть включати в себе відправлення фішингових листів, створення фальшивих веб-сайтів або навіть фізичний доступ до приміщень.

Для боротьби з цією загрозою використовується методологія Purple Team. Підходи Purple Team включають тестування ефективності заходів навчання та підвищення свідомості користувачів. Команди, відповідальні за кібербезпеку, спільно працюють для розуміння сценаріїв соціального інжинірингу, якими можуть скористатися атакуючі. Це включає в себе симуляції фішингових атак та інші техніки, які можуть використовувати зловмисники для отримання конфіденційної інформації від персоналу.

Під час таких симуляцій команди Purple Team також оцінюють ефективність захисних заходів та швидкість реакції на виявлення атаки. Цей синергетичний підхід дозволяє виявляти слабкі місця у захисті систем та забезпечувати постійне покращення стратегій та заходів безпеки, зменшуючи

ймовірність успішних соціально-інженерних атак.

Фішинг – це метод атак, в якому зловмисники використовують підроблені повідомлення та техніки маніпулювання для обману користувачів та отримання конфіденційної інформації. Ця загроза є однією з найпоширеніших та найефективніших, оскільки вона висить в реальному часі над користувачами, які щодня отримують безліч електронних повідомлень [5-6].

Суть фішингу полягає в тому, щоб видати себе за достовірний джерело або службу, якою може користуватися потенційна жертва. Зловмисники можуть використовувати електронну пошту, повідомлення в соціальних мережах або навіть короткі повідомлення, щоб вивести людину з рівноваги та намагатися витягти від неї конфіденційну інформацію, таку як паролі, фінансові дані чи інші особисті дані.

Відповідно до загрози, підходи до боротьби з фішингом розвиваються. Одним із способів боротьби є вдосконалення систем фільтрації електронної пошти. Розробники та адміністратори мереж вдосконалюють антиспамові та антифішингові фільтри, щоб визначати та блокувати підроблені повідомлення. Крім того, ключовим аспектом є освіта користувачів. Навчання персоналу та користувачів впізнавати фішингові атаки є ефективним заходом проти цієї загрози. Людей повинні навчати розрізняти легітимні повідомлення від фішингових та виявляти підозрілі сигнали, такі як неперевірені відправники, непередбачені вкладення або сумнівні посилання[6].

Однак фішинг постійно еволюціонує, і тому Purple Team також включає симуляції фішингових атак для оцінки ефективності систем та користувачів у виявленні та уникненні подібних загроз. Це співпраця між атакуючим та захисним елементами допомагає виявляти слабкі місця та постійно вдосконалювати стратегії протистояння фішинговим атакам.

Програма-вимагач, програма-здирник, програма-шантажист - це тип шкідливої програми, який злочинці встановлюють на комп'ютерах користувачів. Програми, які вимагають викуп, надають злочинцям можливість віддалено заблокувати комп'ютер. Після цього програма відображає спливаюче вікно з

повідомленням, що комп'ютер заблокований і що до нього немає доступу, доки не заплатите кошти.[7]

Програма-вимагач становить серйозну загрозу для сучасних інформаційних систем, проникаючи в їхню структуру і завдаючи значних збитків. Ця форма кіберзлочинності полягає в зараженні комп'ютерних систем шифрованим програмним забезпеченням, що блокує доступ до файлів або навіть всієї системи. Зловмисники вимагають викуп за розблокування даних або відновлення нормального функціонування системи.

Загроза програми-шантажисту особливо актуальна для підприємств, організацій та навіть індивідуальних користувачів. Атаки цього типу можуть спричинити великі фінансові втрати, втрату конфіденційної інформації та вразити репутацію.

Для захисту від програми-шантажисту ключовим є аналіз вразливостей в системах. Це включає в себе постійне оновлення та патчінг програмного забезпечення, виявлення та усунення слабких місць у конфігурації систем, а також моніторинг активності для виявлення аномальних покладань.

Однак реакція на програмну вимагання також важлива. Purple Team може використовувати симуляції атак, щоб випробувати ефективність заходів виявлення та реагування на такі загрози. Це включає в себе вивчення швидкості виявлення атаки, взаємодію між інформаційно-безпечнішими системами та здатність до швидкого відновлення після атаки.

Подібні підходи допомагають удосконалити стратегії захисту від шантажистів та готовність реагування на екстрені ситуації. Вони створюють можливість не лише запобігти зараженню, але й ефективно відновити систему у разі атаки, зменшуючи вплив і можливі збитки.

Атаки з використанням витоку інформації є серйозною загрозою для безпеки інформаційних систем. Ця форма кіберзлочинності полягає в неправомірному отриманні і розголошенні конфіденційної інформації через вразливості в системах або недоліки в їхній конфігурації. Зловмисники можуть використовувати різноманітні методи, такі як експлойти вразливостей, недоліки

у програмному забезпеченні або атаки на недостатньо захищені мережеві з'єднання, для отримання несанкціонованого доступу до конфіденційних даних.

Загроза витоку інформації може мати серйозні наслідки, включаючи фінансові втрати, порушення конфіденційності клієнтів, а також пошкодження репутації організацій та осіб. Часто такі витоки відбуваються через враження системи внаслідок атак, які вдаються в обхід існуючих захисних заходів.

Таблиця 2.1

Таблиця найбільш поширених загроз та атак

Тип загрози/ атаки	Опис	Інструменти/методи	Попередні заходи безпеки	Засоби виявлення	Засоби захисту	Засоби реагування
Phishing (фішинг)	Використання соціальної інженерії для отримання конфіденційної інформації	Спам-пошта, підроблені сайти	Ефективне навчання персоналу, двофакторна аутентифікація	Email Security Gateways, Anti-Phishing Tools	EDR (Endpoint Detection and Response)	Перевірка інциденту, ізолювання вразливостей
Ransomware (програми-вимагачі)	Вірус, який шифрує файли користувача та вимагає викуп	Відомі віруси (WannaCry, Ryuk), експлойти, вразливості	Резервне копіювання даних, патчі безпеки	Network Traffic Monitoring Behavior-based Analytics	Data Backup Solutions, Endpoint Security	Відновлення даних, аналіз вразливостей
DdoS (відмова в обслуговуванні)	Переповнення ресурсів мережі для заборони доступу користувачам	Ботнети, зламані пристрої IoT	Мережеві заходи захисту, CDN	Traffic Anomaly Detection	DDoS Mitigation Services	Відновлення мережевих ресурсів
Insider Threats (Внутрішні загрози)	Небажаний доступ або витік інформації зсередини організації	Недозволений доступ, недбалість персоналу	Сегментація доступу, Monitoring System Access	User Behavior Analytics	Data Loss Prevention Tools	Аудит та відключення доступу

Тип загрози/ атаки	Опис	Інструменти/методи	Попередні заходи безпеки	Засоби виявлення	Засоби захисту	Засоби реагування
Zero-Day Exploits (Вразливість нульового дня (ПО))	Вразливості в програмному забезпеченні, які відомі тільки зловмисникам	Нові експлойти в програмах	Застосування патчів, Intrusion Detection Systems	Threat Intelligence Platforms	Intrusion Prevention Systems	Швидке застосування патчів або відключення вразливих систем

Підходи до боротьби з цією загрозою орієнтовані на тестування вразливостей систем та постійне оновлення політик безпеки. Тестування систем на вразливості включає в себе ідентифікацію та усунення слабких місць в інфраструктурі, програмному забезпеченні та мережевих протоколах. Це може включати в себе автоматизовані інструменти для виявлення вразливостей та ручний аналіз коду та конфігурацій.

Оновлення політик безпеки означає постійне удосконалення та адаптацію стратегій захисту до нових вимог та відомостей про загрози. Включення Purple Team дозволяє команді кібербезпеки об'єднати свої зусилля для ефективного виявлення та усунення вразливостей, а також для реагування на нові та розвиваючись загрози в області витоку інформації.

Зловживання привілеїв представляє серйозну кіберзагрозу, оскільки зловмисники, які отримують доступ до піднятих привілеїв, можуть виконувати різноманітні несанкціоновані дії, включаючи знищення, крадіжку конфіденційної інформації, розголошення даних та навіть загрози інфраструктурі. Загроза полягає в зловживанні привілеїв, які надаються користувачеві або програмі з метою виконання конкретних завдань або отримання доступу до певних ресурсів. Зловмисники можуть використовувати різноманітні техніки, такі як експлойти вразливостей або соціальний інжиніринг, для отримання піднятих привілеїв і, отже, отримання контролю над системою.

Ефективні підходи до протистояння цій загрозі включають перевірку систем на можливість виявлення зловживань привілеїв. Це означає ретельний

аналіз активності користувачів, виявлення аномалій та надання важливості моніторингу піднятих привілеїв для виявлення потенційно небезпечних сценаріїв.

Обмеження зловживання привілеїв також включає в себе встановлення адекватних політик безпеки та належної конфігурації систем. Правильне встановлення принципів "найменших привілеїв" дозволяє обмежити доступ користувачів чи програм тільки до тих ресурсів та функцій, які необхідні для виконання їх завдань, зменшуючи тим самим ризик надання непотрібних привілеїв. У контексті Purple Team, ефективне виявлення та захист від зловживання привілеїв може включати симуляції атак, які допомагають командам забезпечення безпеки оцінити ефективність своїх захисних заходів та реагувати на подібні загрози.

Злам паролів є однією з найпоширеніших та ефективних атак, які використовуються кіберзлочинцями для отримання несанкціонованого доступу до систем та ресурсів. Загроза полягає в тому, що атакуючі використовують різноманітні методи для розгадування або обходу паролів користувачів з метою отримання повного контролю над системою чи конфіденційною інформацією. Атаки на слабкі паролі використовують вразливості в парольній політиці та практиці користувачів. Зловмисники можуть використовувати словники, атаки перебору та інші методи для спроби вгадати або обчислити паролі, які часто обираються людьми через їхню недостатню складність.

Ефективні підходи до захисту від атак на слабкі паролі включають перевірку та посилення парольної політики. Це означає встановлення складних вимог щодо довжини паролів, використання різних символів та вимог до регулярної зміни паролів. Також важливо вести навчання користувачів стосовно безпечної практики створення та управління паролями. Підходи Purple Team до боротьби з цією загрозою можуть включати симуляції атак, щоб перевірити ефективність захисних заходів проти атак на слабкі паролі.

Таблиця 2.3

Стратегії захисту за шаровою моделлю

Рівень захисту	Заходи захисту	Загрози, які уникати або виявляти
Фізичний	Безпека приміщень, контроль доступу до пристроїв	Несанкціонований доступ до приміщень, крадіжка обладнання
Додатковий	Антивірусне програмне забезпечення	Мальварні програми, трояни, шпигунське ПЗ, різноманітні віруси
Мережевий	Фаєрволи, ідентифікація та аутентифікація	Мережеві атаки (DDoS, MITM), незаконне використання мережі
Периметральний	IPS (системи запобігання вторгнення)	Вторгнення через вразливості мережевих пристроїв, експлойти
Корпоративний	Системи моніторингу та аналізу подій	Внутрішні загрози, небажана активність користувачів у мережі

Це дозволяє команді забезпечення безпеки оцінити свої системи, виявити слабкі місця та вжити заходів для їх усунення. Також важливо внести регулярні оновлення у політику безпеки, враховуючи останні методики та технології, щоб утримати атаки на слабкі паролі під контролем.

Атаки на додатки є серйозною загрозою для безпеки інформаційних систем, оскільки вони використовують вразливості у програмному забезпеченні для здійснення атак. Ці вразливості можуть включати помилки у коді, недоліки безпеки та інші слабкі місця, які можуть бути використані зловмисниками для незаконного доступу, розкриття конфіденційної інформації або виконання шкідливих операцій на системі.

Загроза атак на додатки може виявитися особливо великою, оскільки багато організацій використовують різноманітне програмне забезпечення для своєї діяльності, включаючи веб-додатки, мобільні додатки та корпоративне

програмне забезпечення. Зловмисники можуть використовувати різні техніки, такі як ін'єкції SQL, перехоплення сесій, атаки на кросс-сайтовий скриптінг (XSS) та інші для здійснення атак на додатки.

Ефективні підходи до захисту від атак на додатки включають проведення тестів на проникнення. Це означає систематичне та цілеспрямоване тестування систем та додатків на виявлення вразливостей. Такі тести можуть включати в себе сканування за вразливостями, аналіз коду, а також симуляцію атак для визначення, наскільки добре системи можуть витримати атаки ззовні.

Враховуючи атаки на додатки, Purple Team може використовувати сценарії атак, які моделюють реальні загрози, щоб перевірити ефективність заходів безпеки та реагування на можливі інциденти. Це допомагає виявляти та усувати вразливості, а також підвищує готовність системи до можливих атак на додатки.

Purple Team спрямований на виявлення, оцінку та вирішення цих та подібних проблем. Співпраця між Red Team та Blue Team дозволяє ефективно впроваджувати заходи безпеки та реагувати на нові загрози

Щоб захиститися від стрімко змінюючихся кіберзагроз, компаніям потрібно постійно адаптуватися та інноваційно розвиватися. Це означає, що червоні та сині команди повинні постійно співпрацювати для максимізації свого індивідуального та колективного впливу. Методологія "фіолетового" тестування дозволяє їм досягти цього ефективніше, значно покращуючи кіберзахист організацій.

"Фіолетове" тестування може відігравати ключову роль в укріпленні підходу організації до кіберзахисту. Це відбувається завдяки можливості для команд з кіберзахисту покращувати ефективність виявлення вразливостей, полювання на загрози та моніторингу мережі. Це досягається точним моделюванням типових сценаріїв загроз та сприяє створенню нових методів для запобігання та виявлення нових видів загроз.

Деякі організації виконують "фіолетове" тестування як окремі спрямовані заходи, де кіберзахист визначається чіткими цілями, графіками та ключовими результатами. Цей підхід передбачає формальний процес оцінки отриманих

уроків протягом операції, а також визначення недоліків у сфері оборони та нападу, а також визначення майбутніх потреб у тренуванні та технічних аспектах.

Червона команда – це група фахівців із офенсивного кіберзахисту, які відповідають за використання реальних технік адверсарів для виявлення та усунення вразливостей в інфраструктурі, системах та додатках, а також слабкостей у процесах та поведінці людей.

Навпаки, синя команда, яка зазвичай базується в Операційному Центрі Кібербезпеки (SOC), – це група аналітиків та інженерів, спрямованих на захист організацій від кібератак за допомогою поєднання запобігання загрозам, обману, виявлення та реагування.

У "фіолетовому" тестуванні червоні та сині команди продовжують виконувати свої відокремлені обов'язки, але співпрацюють одна з одною для обміну розвідувальними даними. Метою є подолання ефекту "колодязя", який може виникати, коли спеціалісти працюють в межах відокремлених, рішучих команд. У "фіолетовому" тестуванні експерти обох команд активно співпрацюють для максимізації впливу своєї роботи. Це забезпечує більш чітко визначений та ефективний рівень здатності виявлення та реагування компаній на загрози.

Процес "фіолетового" тестування досягає цього, обмінюючи розвідувальними даними через цей процес з метою покращеного розуміння тактик, технік та процедур загроз. Імітуючи ці типи атак через різні сценарії червоних команд, синя команда може покращити свою здатність до виявлення та реагування. Це є значним кроком вперед порівняно із тим, що раніше сині команди можливо не мали видимості на компрометації безпеки через те, що вибір методу атаки адверсарі виявлявся невиявленим.

Незалежно від розміру, галузі або ресурсів, всі організації потребують як червоних, так і синіх команд, щоб ефективно протидіяти кіберзагрозам.

Дії червоних команд, чи то оцінка вразливостей та тестування на проникнення, чи повномасштабні симуляції кібератак, спрямовані на виявлення

проблем безпеки, викликаючи виклики для синіх команд та оцінюючи методи та процеси виявлення.

Оцінки червоних команд можуть використовуватися для оцінки оборони організацій проти останніх інструментів, тактик і процедур, що використовуються кримінальними противниками, і надавати важливий зворотний зв'язок для прискорення виявлення загроз та реагування на інциденти.

Загрозовий інтелект відіграє критичну роль у цьому процесі — синій команді важко бути ефективною без найновіших відомостей про тактику атак і видатні види загроз.

Синя команда відповідає за управління та моніторинг ряду засобів виявлення, використовуючи останні відомості, для пошуку та ліквідації загроз у їхньому витоку цілодобово.

Для багатьох організацій червоні та сині команди часто працюють як повністю відокремлені та несполучені сутності. У деяких невеликих організаціях, наприклад, внутрішній персонал відділу IT часто відповідає за моніторинг, виявлення та реагування, тоді як етичні хакери наймаються зовнішніми провайдерами для виконання випадкового пошуку вразливостей та тестування на проникнення.

Це означає, що часто відсутні канали для неперервного обміну відгуками між червоними та синіми командами. Замість того, щоб співпрацювати та постійно вдосконалювати системи безпеки через "фіолетове" тестування, багато організацій вибирають краткостроковий погляд на безпеку та не використовують відомості червоних і синіх команд для формулювання та оцінки довгострокових цілей та стратегії безпеки.

Користь "фіолетового" тестування

Вправи "фіолетового" тестування відрізняються від тестів на проникнення тим, що вони не призначені для виявлення конкретних вразливостей. Замість цього вони призначені для надання ряду загальних користей у сфері безпеки, включаючи:

Покращення знань про безпеку

Можливість спостерігати та брати участь в атаках дозволяє синій команді краще розуміти, як діють атакуючі, що дозволяє їм більш ефективно використовувати технології для обману справжніх атакувальників та вивчати їх тактику, техніки та процедури (TTP).

Прискорення продуктивності без збільшення бюджету

Поєднання оборони та нападу через вправи "фіолетового" тестування дозволяє організаціям підняти стандарт функції моніторингу безпеки швидше та за менше вартості. Це дозволяє компаніям отримати найкращу вартість за свій бюджет на безпеку в умовах, коли кіберзагрози продовжують диверсифікуватися.

Оптимізація поліпшень у сфері безпеки

Інший підхід в галузі кібербезпеки - розглядати "фіолетове" тестування як концептуальну структуру, яка працює в усій організації. Це може сприяти створенню спільної культури, яка сприяє постійному вдосконаленню кібербезпеки.

Отримання критичного розуміння

"Фіолетове" тестування дозволяє внутрішній команді з безпеки критично розуміти прогалини в їхньому стані безпеки та допомагає виявити можливі напрямки, які потребують додаткової уваги.

Так само, як і з іншими видами оцінок, періодичність проведення "фіолетового" тестування повинна бути визначена конкретними потребами та пріоритетами кожної організації. Деякі організації можуть здобути вигоду від річного "фіолетового" тестування, тоді як іншим може знадобитися більш часте оцінювання. Незалежно від конкретної періодичності, важливо регулярно проводити "фіолетове" тестування для того, щоб забезпечити, що підхід організації до кібербезпеки залишається актуальним на тлі постійно змінюючогося пейзажу загроз.

Щоб ефективно скористатися "фіолетовим" тестуванням, звертайтеся до свого поточного чи потенційного постачальника кібербезпеки щодо їхнього підходу. Перевірте, як вони втілюють його на практиці для клієнтів та

переконайтеся, що ви запитуєте докладну інформацію про процеси та методології, що включаються. Хороший постачальник кібербезпеки буде використовувати "фіолетове" тестування як стандартну практику та зможе навести конкретні підходи та варіанти використання.

2.2. Визначення необхідності апгрейду методології у зв'язку із змінами у кіберландшафті. Вивчення можливостей використання інноваційних технологій та підходів

Необхідність апгрейду методології в сфері кібербезпеки виникає в зв'язку з постійними змінами у кіберландшафті, які охоплюють еволюцію загроз, нові технології та стратегії атак. Це важливий процес для забезпечення високого рівня захисту інформаційних систем у світі, де кіберзлочинці постійно адаптуються та вдосконалюють свої методи.

В сучасному кіберландшафті, сталі та швидкі зміни в технологіях ведуть до появи нових загроз та вдосконалення методів атак. Це ставить під сумнів ефективність існуючих методологій кібербезпеки, оскільки нові сценарії атак можуть бути інноваційними та несподіваними.

З'явлення нових типів загроз та атак може походити від різноманітних джерел, таких як зловмисники, які постійно адаптуються до захисних заходів, або виникнення нових технологій, що відкривають нові можливості для кіберзлочинців. Великий обсяг інформації, що обробляється в мережах, а також зростання кількості підключених пристроїв у Інтернеті речей (IoT), роблять цю проблему особливо актуальною.

Для ефективного захисту від нових загроз важливо не лише реагувати на конкретні випадки, але й активно вивчати та розуміти нові сценарії атак. Адаптація заходів безпеки відповідно до цих нових реалій є ключовою для забезпечення надійного захисту інформаційних систем.

Вивчення нових загроз включає в себе аналіз таких аспектів, як методи використання нових технологій зловмисниками, їхня тактика та техніки.

Забезпечення відповідності заходів безпеки до сучасних реалій кіберпростору дозволяє організаціям підтримувати високий рівень захисту та мінімізувати ризик виникнення нових форм кіберзагроз. Тільки шляхом активного вивчення нових загроз та адаптації кіберзахисних стратегій до змін у кіберландшафті можна забезпечити надійну безпеку інформаційних ресурсів.

Зміни в технологічному ландшафті приводять до суттєвих трансформацій у способах, якими організації взаємодіють з інформацією та ведуть свою діяльність. Введення новітніх технологій, таких як хмарні сервіси, Інтернет речей (IoT) та штучний інтелект, визначає новий стандарт у розвитку бізнесу та інформаційних систем.

Хмарні сервіси дозволяють організаціям ефективно використовувати ресурси, виключаючи потребу в обладнанні та інфраструктурі на місці. Однак це також вносить нові виклики у сфері кібербезпеки, оскільки дані переміщаються за межі традиційних корпоративних мереж, вимагаючи від організацій змінювати свої підходи до контролю та захисту інформації.

Інтернет речей, які стає все більшою частиною бізнес-екосистеми, розширює атакуальну поверхню інфраструктури. Зв'язок між мільярдами підключених пристроїв може створити нові точки вразливості, і забезпечення безпеки цього роду мереж вимагає глибокого розуміння та інтеграції відповідних заходів безпеки.

Штучний інтелект, використовуваний для автоматизації процесів та аналізу великих обсягів даних, вносить новий елемент у загальну динаміку кіберзахисту. Це включає в себе використання алгоритмів машинного навчання для виявлення аномалій та прогнозування потенційних атак. Захист від атак на штучний інтелект вимагає розробки нових методів та технік для розпізнавання та контролю атак на самому рівні алгоритмів. [17]

Оновлення методів захисту та адаптація до нового технологічного ландшафту є критичним завданням для забезпечення безпеки в умовах постійних змін. Проактивне впровадження інноваційних заходів безпеки є необхідною умовою для успішного функціонування та розвитку сучасних бізнес-систем

Поширення робочих площин атак у сучасному кіберландшафті є невід'ємним наслідком трансформацій у способах організації роботи та доступу до інформації. Віддалена робота та використання віртуальних робочих просторів роблять робочі площини більш розподіленими та глобальними, але це також призводить до появи нових викликів у сфері кібербезпеки.

З одного боку, віддалена робота розширює можливості для зручного доступу до робочого середовища, що сприяє ефективності та гнучкості працівників. З іншого боку, це також створює нові вектори атак для зловмисників, які можуть намагатися використовувати вразливості в віддалених системах або отримувати несанкціонований доступ до конфіденційної інформації.

Розподілена природа віртуальних та фізичних робочих площин створює важливу задачу для забезпечення безпеки інформації та захисту мережі. Підвищений ризик витоку інформації може виникнути через незахищені з'єднання, недостатню аутентифікацію або слабко захищені кінцеві точки, які використовуються для віддаленої роботи.

Кіберландшафт постійно змінюється, і кібератаки стають дедалі складнішими та витонченішими. Ці зміни вимагають від організацій постійно удосконалювати свої методи кібербезпеки, щоб залишатися захищеними.

Для того, щоб Purple Team була ефективною, вона повинна постійно удосконалюватись у зв'язку із змінами у кіберландшафті. Ось деякі конкретні області, в яких Purple Team може вимагати апгрейду методології:

Нові технології, такі як штучний інтелект та машинне навчання, можуть допомогти Purple Team ефективніше виявляти та реагувати на кібератаки. Нові загрози, такі як атака Zero-day, вимагають від Purple Team нових методів реагування. Комунікація та співпраця є ключовими для ефективної роботи Purple Team. Purple Team повинна постійно удосконалювати свої процеси комунікації та співпраці, щоб бути готовою до будь-яких кібератак.

Організації повинні зосередитися на розвитку сучасних засобів виявлення загроз, вдосконаленні систем інтелігентного моніторингу та використанні

аналітики для вчасного виявлення та реагування на атаки. Також важливим є розвиток культури кібербезпеки серед персоналу та реалізація проактивних заходів для захисту конфіденційної інформації на всіх рівнях. Поглиблення кібершпіонажу вимагає від організацій не лише реагувати на інциденти, а й будувати стратегічні та комплексні заходи з кібербезпеки для запобігання таким загрозам у майбутньому.

При появі нових регуляторних стандартів, організації повинні проводити оцінку своїх існуючих заходів з кібербезпеки та адаптувати їх для відповідності новим вимогам. Це може включати в себе вдосконалення політик безпеки, впровадження нових технологій, які відповідають новим вимогам, та проведення навчання персоналу.

Найефективніші підходи до управління змінами у вимогах до регулювання включають постійний моніторинг, активну участь відділу кібербезпеки в процесах прийняття рішень та розробку агільних стратегій, які дозволяють організаціям швидко реагувати на зміни в кіберзахисті. Оновлення методологій для відповідності новим регуляторним вимогам є необхідним елементом стратегії кібербезпеки будь-якої сучасної організації.

Досвіди, отримані з аналізу попередніх кіберінцидентів, визначаються як надзвичайно цінні в удосконаленні загальної стратегії кібербезпеки. Кожен кіберінцидент стає важливим етапом для вивчення причин та наслідків, виявлення вразливостей і недоліків в існуючих заходах безпеки.

Аналіз попередніх інцидентів дозволяє виявити слабкі місця в системі безпеки, які можуть бути використані зловмисниками для проведення атак. Це може бути недостатня сегментація мережі, слабка аутентифікація, відсутність систем моніторингу або інші проблеми, які сприяють успішним атакам.

Навчання на основі попередніх інцидентів передбачає ретельний аналіз того, яким чином атака відбулася, які методи використовувалися зловмисниками та які саме слабкі місця були використані для проникнення. Цей аналіз стає основою для розробки та впровадження нових стратегій та заходів безпеки.

Одним із ключових аспектів вивчення попередніх інцидентів є також

розробка та впровадження ефективних механізмів виявлення та реагування на подібні атаки у майбутньому. Системи моніторингу та реагування повинні бути покращені на основі отриманих знань.

Навчання на попередніх інцидентах стимулює створення більш адаптивних та реактивних стратегій кібербезпеки, спроможних ефективно протистояти новим загрозам. При цьому важливо створювати культуру навчання та постійного вдосконалення, щоб персонал завжди був готовий реагувати на швидко змінюючіться умови кіберзагроз. Запровадження Purple Team може також бути частиною апгрейду методології, оскільки цей підхід дозволяє поєднувати силу атаки та оборони для постійного вдосконалення заходів безпеки та реагування на загрози. Апгрейд методології кібербезпеки є необхідним елементом стратегії кіберзахисту, спрямованої на підтримку високого рівня безпеки та відповідь на зростаючі виклики у кіберпросторі.

Інноваційні технології швидко проникли в усі сфери нашого життя, викликаючи необхідність використання комп'ютерної техніки під час вивчення різних предметів шкільного курсу. Завдяки постійним змінам у світовій екології, законодавстві, природних умовах і погоді, інформація, що міститься в підручниках, швидко застаріває ще до їхнього виходу. Використання інноваційних технологій, комп'ютерної техніки та останньої інформації з Інтернету під час вивчення окремих предметів або тем - це один із методів оптимізації та рознообразження навчально-виховного процесу. Тому сьогодні використання комп'ютера в навчальному процесі вважається інновацією.

Під інноваціями в широкому розумінні розуміється впровадження нововведень у вигляді нових технологій, продуктів і послуг, організаційно-технічних та соціально-економічних рішень у виробничому, фінансовому, комерційному, адміністративному або іншому контексті. Життєвий цикл інновації - це період від зародження ідеї до її використання. Враховуючи послідовність проведення робіт, життєвий цикл інновації розглядається як інноваційний процес. Використання персонального комп'ютера в навчальному процесі є новою технологією в освіті, нововведенням в учбовому процесі.

Заради посилення демократичних тенденцій у суспільстві, освітні системи переорієнтовуються з масових педагогічних явищ на особистість учня, розглядаючи можливості та обставини його індивідуального розвитку, саморозкриття та самореалізації. Тенденція особистісної орієнтованості в освітніх системах проявляється і в педагогічній освіті. Сучасні школи потребують не лише добрих вчителів, але й вчителів-технологів, майстрів та новаторів. Створення альтернативних шкіл та визнання права кожної школи мати свій унікальний образ, працювати за власними програмами, потребують вчителів з інноваційним мисленням, які готові взяти на себе відповідальність за особистість постійно розвиваючоїся людини та школи як системи, що також перебуває в розвитку.

Останнім часом ідея впровадження інноваційних технологій у навчання стала предметом інтенсивних досліджень як у теоретичному, так і в практичному плані. Етап її реалізації характеризується розробкою та проведенням учителями інноваційних уроків різних профілів, а також теоретичним аспектом, який включає створення та вдосконалення інноваційних та інтегрованих курсів, об'єднуючи при цьому різні предмети, що вивчаються за навчальними планами. Інноваційні технології надають можливість з одного боку подати учням "світ у цілому", об'єднавши різноманіття наукових знань, та з іншого - використовувати вивчений матеріал для профільної диференціації у навчанні.

Ця вимога визначає необхідність освоєння комп'ютерних технологій вже на етапі шкільної освіти, щоб випускник зміг швидко впровадитися в сучасне суспільство. Для ефективного використання комп'ютера важливо не просто вміти програмувати, але й володіти ефективними готовими програмами для вирішення різних завдань.

Висновки до другого розділу

Аналіз сучасних загроз та атак, що враховується при використанні Purple Team, показує, що ця методологія є ефективною для виявлення та усунення кіберзагроз. Однак, у зв'язку зі змінами у кіберландшафті, існує необхідність апгрейду методології.

Однією з можливостей апгрейду Purple Team є використання інноваційних технологій та підходів. Наприклад, можна використовувати штучний інтелект та машинне навчання для автоматизації завдань, а також для кращого розуміння кіберзагроз.

Іншою можливістю апгрейду Purple Team є впровадження нових методів навчання та підготовки персоналу. Наприклад, можна використовувати симулятори кібератак для підготовки персоналу до реального реагування на атаки.

Впровадження інноваційних технологій та підходів у Purple Team може допомогти організаціям підвищити ефективність захисту від кіберзагроз.

РОЗДІЛ 3.
Проведення оцінки ефективності Purple Team

3.1. Розробка методики оцінки ефективності за допомогою критеріїв та метрик

Розробка методики оцінки ефективності в галузі кібербезпеки вимагає створення систематичного підходу, який враховує різноманітні аспекти захисту інформації та інфраструктури. Визначення критеріїв та метрик грає ключову роль у визначенні та вимірюванні рівня ефективності кіберзахисту організації. У першому етапі розробки методики оцінки ефективності в галузі кібербезпеки визначається об'єкт оцінки, що становить фундаментальний крок у процесі визначення ефективності заходів з кіберзахисту. Цей об'єкт може представляти собою різноманітні компоненти технологічного середовища, такі як системи, мережі, програмне забезпечення, процеси кібербезпеки, персонал, або ж складні комплекси інфраструктури.

Важливо визначити конкретні області чи аспекти, які піддаються оцінці, ідентифікувати їхню роль у загальній системі безпеки та забезпечити ясність щодо об'єму та масштабу оцінювання. Наприклад, це може бути визначення рівня захисту конкретної інформаційної системи, оцінка безпеки великої мережі або вивчення ефективності заходів безпеки персоналу.

Визначення об'єкта оцінки встановлює основну рамку для подальшого розроблення критеріїв та метрик, спрямованих на конкретні аспекти кібербезпеки. Цей етап дозволяє визначити обсяг і завдання оцінювання, щоб забезпечити зрозумілість та конкретність у процесі визначення ефективності системи кіберзахисту в цілому.

Другий етап розробки методики оцінки ефективності в галузі кібербезпеки включає визначення ключових критеріїв, які визначають рівень ефективності системи кіберзахисту. Це важливий крок у процесі створення об'єктивної системи вимірювання та оцінки, яка дозволяє здійснювати оцінку та порівняння різних аспектів кібербезпеки.

Ключові критерії, що визначають ефективність, охоплюють різноманітні

аспекти безпеки. Перш за все, це захищеність даних - міра успішності заходів, спрямованих на збереження конфіденційності та цілісності інформації. Доступність системи визначається її здатністю функціонувати в умовах атак або невдач.

Ефективність системи кіберзахисту також визначається швидкістю та ефективністю виявлення потенційних загроз та реагування на них. Це включає в себе системи моніторингу та аналізу, які забезпечують не тільки виявлення інцидентів, але й швидке реагування для мінімізації можливих збитків.

Регулярність та своєчасність впровадження патчів та оновлень стають також критичними метриками. Швидке та систематичне вирішення вразливостей через патчі та оновлення є важливим елементом стратегії кібербезпеки для усунення потенційних точок входу для зловмисників.

Ці критерії не лише визначають ефективність системи кіберзахисту, але й стають основою для подальшого визначення конкретних метрик та інструментів вимірювання. Забезпечуючи повний огляд різних аспектів безпеки, ці критерії допомагають створити збалансовану та комплексну систему оцінки ефективності кіберзахисту.

У третьому етапі розробки методики оцінки ефективності системи кібербезпеки здійснюється розробка конкретних метрик для кожного визначеного критерію. Це є критичним етапом, оскільки саме метрики надають конкретні вимірювання, які дозволяють кількісно оцінювати та порівнювати різні аспекти ефективності кіберзахисту. [25]

Оцінка ефективності Purple Team є важливим завданням, оскільки вона допомагає організаціям зрозуміти, наскільки ефективно їх команди з реагування на інциденти та кібербезпека можуть працювати разом, щоб захистити організацію від кібератак.

При виборі методики оцінки ефективності Purple Team важливо враховувати конкретні потреби та цілі організації. Наприклад, організація, яка зосереджена на запобіганні кібератакам, може зосередитися на оцінці результатів. Організація, яка зосереджена на швидкому реагуванні на інциденти,

може зосередитися на оцінці процесів.

Нижче розроблена таблиця яка має конкретні критерії та метрики, які можуть бути використані для оцінки ефективності Purple Team.

Таблиця 3.1

Таблиця оцінки ефективності за допомогою критеріїв та метрик

Метод оцінки	Критерії	Метрики
Оцінка результатів	Запобігання кібератакам	Кількість успішних атак, які були відбиті
Оцінка результатів	Швидке реагування на інциденти	Середній час на виявлення інциденту, середній час реагування на інцидент, кількість інцидентів, які були успішно вирішені
Оцінка процесів	Ефективна комунікація та співпраця	Кількість випадків ефективної комунікації та співпраці між членами Purple Team
Оцінка навичок	Навички членів Purple Team	Кількість членів Purple Team, які мають необхідні навички для виявлення та реагування на кібератаки, рівень компетентності членів Purple Team у виявленні та реагуванні на кібератаки

Дані критерії та метрики можуть бути використані як основа для розробки плану оцінки ефективності Purple Team, вибір критеріїв та метрик оцінки залежить від цілей оцінки та від того, які аспекти ефективності Purple Team необхідно оцінити. У роботі 3.2 наведено

Ці метрики визначають ефективність систем виявлення потенційних атак та швидкість реагування на їхні наслідки. Для своєчасності оновлень визначається метрика, яка відображає час від випуску оновлення до його впровадження в систему. Це важливий показник, який характеризує швидкість реагування на нові вразливості та актуалізацію заходів безпеки. Розробка конкретних метрик дозволяє зробити процес оцінки ефективності більш конкретним та об'єктивним, а також надає базу для подальшого збору та аналізу даних у рамках визначених параметрів.

Четвертий етап розробки методики оцінки ефективності в кібербезпеці

передбачає визначення вагомості кожної метрики, що є ключовим кроком у створенні комплексної системи вимірювань та оцінок. Вагомість метрик визначає, наскільки важливим є кожен показник великому контексті безпеки, враховуючи специфіку та стратегію організації.

Таблиця 3.2

Таблиця оцінки ефективності за допомогою критеріїв та метрик

Критерій	Метрика	Опис
Запобігання кібератакам	Кількість успішних атак, які були відбиті	Кількість атак, які були розпочаті злодійниками, але були успішно зупинені Purple Team
Запобігання кібератакам	Кількість потенційних атак, які були виявлені та нейтралізовані	Кількість атак, які були виявлені Purple Team на ранніх стадіях і не дозволили злочинцям розпочати атаку
Швидке реагування на інциденти	Середня година виявлення інциденту	Середня година, яка пройшла від моменту початку інциденту до моменту його виявлення Purple Team
Швидке реагування на інциденти	Середня година реагування на інцидент	Середня година, яка пройшла від моменту виявлення інциденту до моменту його успішного вирішення
Швидке реагування на інциденти	Кількість інцидентів, які були успішно вирішені	Кількість інцидентів, які були успішно вирішені Purple Team протягом певного періоду години
Ефективна комунікація та співпраця	Кількість випадків ефективної комунікації та співпраці між членами Purple Team	Кількість випадків, коли члени Purple Team ефективно спілкувалися та співпрацювали один з одним для виявлення та реагування на кібератаки.
Ефективна комунікація та співпраця	Кількість випадків неефективної комунікації та співпраці між членами Purple Team	Кількість випадків, коли члени Purple Team не ефективно спілкувалися та співпрацювали один з одним для виявлення та реагування на кібератаки.
Навички членів Purple Team	Кількість членів Purple Team, які мають необхідні навички для виявлення та реагування на кібератаки	Кількість членів Purple Team, які мають необхідні знання, навички та досвід для виявлення та реагування на кібератаки
Навички членів Purple Team	Рівень компетентності членів Purple Team у виявленні та реагуванні на кібератаки	Рівень знань, навичок та досвіду, якими володіють члени Purple Team для виявлення та реагування на кібератаки.

При визначенні вагомості метрик слід враховувати стратегічні цілі та пріоритети безпекової політики компанії. Наприклад, якщо для організації найважливішим є забезпечення конфіденційності даних, метрики, пов'язані з

захищеністю даних, можуть мати вищий рівень вагомості.

Для захищеності даних вагомість може визначатися на основі чутливості інформації та потенційних наслідків витоку даних.

У випадку доступності системи вагомість може бути пов'язана з важливістю неперервної роботи бізнес-процесів та уникненням значних перерв у роботі системи.

Виявлення і реагування на загрози може мати вагомість, залежну від часу реакції на критичні загрози та можливості зменшення збитків.

Вагомість метрик своєчасності патчів та оновлень може визначатися швидкістю реагування на нові вразливості та зменшенням ризиків внаслідок відкритих вразливостей.

Збалансоване визначення вагомості дозволяє приділяти увагу тим аспектам, які найбільше важливі для організації, і забезпечує об'єктивність в процесі оцінювання ефективності системи кібербезпеки. Враховуючи вагомість метрик, організація може краще адаптувати свої заходи безпеки до конкретних потреб та викликів у великому контексті кібербезпеки.

П'ятий етап методики оцінки ефективності в кібербезпеці передбачає впровадження розробленої системи вимірювань та оцінок, а також активний процес збору даних та оцінки отриманих результатів. Цей етап відіграє критичну роль у вдосконаленні безпекових стратегій та адаптації до змін у кіберландшафті.

Впровадження методики передбачає її реальне застосування у робочому середовищі, де здійснюється збір та аналіз відповідних даних, пов'язаних із визначеними метриками та критеріями ефективності. Важливо враховувати специфіку організації та її контекст, оскільки це впливає на інтерпретацію результатів та визначення пріоритетних напрямків вдосконалення.

Ретельний аналіз дозволяє виявити сильні та слабкі сторони системи кібербезпеки, а також ідентифікувати фактори, що впливають на її ефективність.

В процесі оцінки ефективності слід акцентувати увагу на виявленні можливих вразливостей, аномалій та інших аспектів, які можуть вказувати на

потенційні загрози. Оцінка повинна бути не лише кількісною, але й якісною, з урахуванням контексту організації та її специфічних потреб. [28]

На основі отриманих результатів розробляються заходи для подальшого вдосконалення системи кібербезпеки. Це може включати в себе корекцію стратегій, вдосконалення процесів, впровадження нових технологій чи оновлення політик безпеки. Контингентна адаптація до змін у кіберландшафті є ключовою у забезпеченні високого рівня захисту від сучасних кіберзагроз.

Шостий етап методики оцінки ефективності в кібербезпеці зосереджений на звітності та перегляді результатів для забезпечення прозорості та актуальності безпечних стратегій організації.

Регулярне формування звітів є важливим елементом процесу, оскільки це дозволяє чітко відображати результати оцінки ефективності системи кібербезпеки. Звіти мають бути спрямовані як на внутрішні використання, для оцінки стану безпеки власної організації, так і на зовнішні, для інформування зацікавлених сторін, таких як керівництво, акціонери, партнери та регулятори.

Періодичні перегляди методики важливі для її актуалізації та відповідності новим викликам та загрозам. Зміни в кіберландшафті, технологічний прогрес, а також внутрішні зміни в організації можуть вимагати коригування підходів до кібербезпеки. Оновлення методики є ключовим елементом для забезпечення її актуальності та ефективності у змінному середовищі.

Звітність та перегляд не тільки демонструють стан безпеки, але й служать інструментами для прийняття управлінських рішень. Ці процеси взаємодіють із зацікавленими сторонами та внутрішнім колективом для забезпечення того, що стратегії кібербезпеки відповідають потребам організації та гарантують високий рівень захисту. Такий циклічний підхід забезпечує постійну готовність до змін та ефективність заходів безпеки.

В розробці методики оцінки ефективності в кібербезпеці ключовими підходами є системність, адаптивність, інтегрованість та продовження. Ці принципи формують основу для створення комплексної та ефективної стратегії безпеки, яка враховує сучасні тенденції та змінюючийся характер кіберзагроз.

Системність передбачає оцінку системи кібербезпеки як цілісного об'єкта, враховуючи взаємодію всіх її компонентів. Такий підхід дозволяє уникнути фрагментації та забезпечує глибокий аналіз кожного елемента системи у контексті загального безпекового ландшафту.

Адаптивність є ключовим аспектом, оскільки кіберзагрози постійно змінюються. Методика повинна бути готовою до швидкого реагування на нові загрози та інновації у кіберсфері, забезпечуючи ефективний захист навіть у змінюючомуся середовищі.

Інтегрованість передбачає пов'язаність методики з іншими аспектами кібербезпеки та загальною стратегією організації. Це означає, що оцінка не повинна бути ізольованою, а має враховувати взаємодію з іншими безпековими заходами та процесами в організації.

Ці ключові підходи допомагають забезпечити, що методика оцінки ефективності в кібербезпеці є не лише ефективною в конкретний момент часу, але і готовою до викликів та змін у майбутньому.

3.2. Здійснення аналізу використання Purple Team у реальних сценаріях

Аналіз використання Purple Team у реальних сценаріях надає можливість розглянути ефективність та переваги цього підходу до кібербезпеки. Purple Team – це методологія, що поєднує Red Team і Blue Team, спрямована на покращення загальної стійкості та відповідності безпеки в організації. Об'єднуючи ці дві команди, Purple Team сприяє глибокому розумінню кожної сторони, їхніх цілей та методів діяльності.

Спільна робота Red Team і Blue Team дозволяє уникнути потенційних конфліктів між цими групами. Замість того, щоб розглядати їх як протистояння, Purple Team створює сприятливе середовище для взаємопорозуміння та спільної роботи. Це розбирає бар'єри комунікації і допомагає створити атмосферу, в якій обидві команди спрямовані на досягнення загальних цілей безпеки.

Важливий аспект — спільне усвідомлення цілей. Purple Team допомагає визначити спільні стратегічні та тактичні цілі, що сприяє покращенню взаєморозуміння в плані важливості та пріоритетності завдань. Це дозволяє створити спільний контекст для обговорення і прийняття рішень.

Ефективне тестування заходів безпеки є ключовим аспектом в сфері кібербезпеки, і Purple Team виявляється досить потужним інструментом для цього завдання. Використовуючи методи атак та вразливостей, Purple Team здійснює реалістичні сценарії атак, спрямовані на оцінку стійкості інфраструктури та захисних заходів. Purple Team допомагає ідентифікувати слабкі місця та вразливості в системі безпеки організації. Крім того, Purple Team сприяє реалістичному підходу до тестування, оскільки команди спільно працюють для виявлення потенційних загроз та вдосконалення захисних механізмів. Цей підхід відрізняється від традиційного тестування, оскільки він враховує як аспекти атак, так і заходи захисту, що робить його більш комплексним та інформативним. Таким чином, Purple Team стає ефективним інструментом для виявлення та усунення слабкі місця в системах безпеки організації, забезпечуючи при цьому більшу стійкість до потенційних кіберзагроз.

Навчання та розвиток персоналу стають ключовими аспектами, особливо в галузі кібербезпеки, де швидкі зміни у загрозах і технологіях вимагають постійного оновлення знань та навичок. Purple Team надає винятковий інструмент для навчання персоналу, пропонуючи можливість вчитися з реальних сценаріїв атак та розробляти ефективні стратегії відповіді на них.

Залучення персоналу до вправ Purple Team дозволяє йому отримувати практичний досвід у вирішенні кіберзавдань. Це робить навчання більш інтерактивним і зацікавлюючим, оскільки воно базується на реальних сценаріях та конкретних викликах, з якими організація може зіткнутися.

Структура вправ Purple Team — це сама по собі методологія, що охоплює планування, розвідку про кіберзагрози, виконання вправ і отримані уроки.

Рис. 3.1. Структура вправ «Purple Team Exercises»

Успішні навчання Purple Team вимагають активного планування та участі широкого кола зацікавлених сторін на всіх етапах навчань Purple Team: (1) Планування, (2) Розвідка про кіберзагрози, (3) Виконані вправи і (4) Набутий досвід.

Не для всіх організацій або навчань потрібні всі ці зацікавлені сторони. Purple Team Exercises може використовувати внутрішні та/або зовнішні команди. Наприклад, в організації може не бути внутрішньої команди аналізу кіберзагроз, або вона може передати SOC постачальнику керованої безпеки. Ці організації все ще можуть використовувати ефективність і переваги програми Purple Team.

У наведеній нижче таблиці наведено приклади ролей і обов’язків для

фіолетової командної вправи.

Таблиця 3.3

Ролі та обов'язки учасників Purple Team Exercise

Посада	Роль	Обов'язок
Менеджер із залучення	Координатор вправ	Провідний контактний пункт протягом усієї вправи Purple Team. Відповідає за забезпечення надання інформації про кіберзагрози. Забезпечує виконання всіх кроків планування до виконання вправ. Під час виконання вправи записує час, примітки, завдання та відгуки. Збирає звіт.
Начальник служби безпеки	Спонсор	Затвердити тренування та бюджет фіолетової команди
Розвідка кіберзагроз	Планування, глядач	Розвідка кіберзагроз
Менеджер червоної команди	Спонсор, глядач	Планування: визначення цілей, вибір учасників
Менеджер синьої команди	Спонсор, глядач	Планування: визначення цілей, вибір учасників
Менеджер DFIR	Спонсор, глядач	Планування: визначення цілей, вибір учасників
Червона команда	Учасник	Планування, виконання вправи
SOC (синя команда)	Учасник	Планування, виконання вправи
Hunt Team (Blue Team)	Учасник	Планування, виконання вправи
Цифрова криміналістика та реагування на інциденти (DFIR)	Учасник	Планування, виконання вправи

Керівництво повинно схвалити та підтримати вправу Purple Team, включаючи цілі, бюджет і обсяг перед будь-якою додатковою роботою на етапі планування чи інших етапах вправи. Менеджери відповідальні за вибір учасників вправи зі своїх команд і відмову від щоденних обов'язків цих осіб під час вправи, щоб вони могли сконцентруватися на цілях та завданнях.

Координатор(и) вправи - це головний контакт на всій етапі вправи Purple Team. Вони відповідальні за забезпечення надання інформації з кіберзагроз та проведення всіх етапів планування до виконання вправи. Під час виконання вправи вони повинні фіксувати протоколи, нотатки, завдання та відгуки. Також вони відповідальні за складання та надання документу "Навчені уроки".

Команда з розвідки кіберзагроз, чи внутрішні, чи сторонні, повинні забезпечити конкретну інформацію в ранній фазі планування вправи. Ця команда відповідає за ідентифікацію противників з можливістю, наміром та здатністю атакувати організацію, а також вивчення та витягування тактик, технік і процедур (TTPs) противників. Аналітики кіберзагроз повинні брати участь як спостерігачі в Вправі Purple Team для подальшого вивчення організації.

Red Team повинні виконати ряд обов'язків під час етапу планування і бути активними під час виконання вправи. Підготовка включатиме розуміння TTPs та забезпечення надійної та послідовної емуляції під час вправи. Red Team не обов'язково повинні використовувати ті ж інструменти і майстерність, що й при прихованій роботі, операції Red Team. Операційні менеджери повинні відмовити від інших завдань для членів Red Team для успішного виконання Вправи Purple Team.

Blue Team - загальний термін для захисників. Це може включати, але не обмежується Security Operations Center (SOC), Hunt Team, Digital Forensics and Incident Response (DFIR) та/або провайдерів управління безпекою послуг (MSSP). Конфігурація та відповідальності команд можуть відрізнятися від організації до організації і від внутрішніх до зовнішніх постачальників.

Менеджер центру операцій безпеки (SOC) повинен планувати участь та забезпечити участь аналітиків SOC в вправі. Мало очікується від SOC у фазі

планування, але обов'язкове їх участь під час виконання вправи. Менеджмент SOC повинен відповідно планувати, звільняючи вправу від обов'язків на кожен день для учасників вправи. Інші аналітики повинні бути заплановані для виконання операцій відсутності учасників. Організації, які не мають Центру операцій безпеки та користуються послугами провайдерів управління безпекою (MSSP), також можуть проводити Вправи Purple Team. Це буде вимагати планування та затвердження від MSSP для забезпечення їх участі в вправі на основі цілей та завдань[29].

Якщо в організації існує команда Hunt Team, вони також повинні брати участь. Від команди Hunt Team мало очікується у фазі планування, але очікується активна участь під час виконання вправи. Менеджер команди Hunt Team повинен поділитися своїми останніми плейбуками під час фази планування, щоб забезпечити вибір ідеальних TTP для вправи.

Аналітики в цифровій судовій експертизі та реагуванні на інциденти (DFIR) також повинні брати участь у вправі Purple Team. Від команд DFIR небагато залежить у фазі планування, але очікується активна участь під час виконання вправи. Менеджери DFIR повинні відмовитися від всіх інцидентів, що стосуються вправи, щоб щоденна робота могла продовжуватися, і участь не впливала на результати аналітика DFIR.

Покращення реакції на інциденти є критичним елементом в управлінні кібербезпекою, і Purple Team дозволяє організаціям здійснювати це на більш продуктивному та реалістичному рівні. Використовуючи Purple Team для симуляції реальних інцидентів, команди можуть перевірити ефективність своїх процедур реагування та вдосконалити їх відповідно до виявлених вразливостей.

Симуляція реальних інцидентів за допомогою Purple Team дозволяє персоналу пройти через реальний сценарій атаки, реагуючи на події, які можуть відбутися в реальному житті. Це не лише надає практичний досвід, але й визначає можливі слабкі місця в процесах реагування на інциденти. Організації можуть визначити ефективність своїх команд та процедур у реальному часі, перевіряючи їхню здатність адекватно реагувати на нові та розширені загрози.

Це дозволяє організаціям виявляти та виправляти потенційні проблеми в реакції на інциденти, а також розробляти та вдосконалювати плани невідкладних заходів. Отже, використання Purple Team для покращення реакції на інциденти допомагає організаціям готуватися до можливих кібератак, забезпечуючи швидке та ефективне реагування на інциденти в реальному часі.

Однією з ключових переваг використання Purple Team є його внесок у оптимізацію витрат на безпеку в організації. За допомогою цього підходу організації можуть більш ефективно визначити та адаптувати свої бюджети на кібербезпеку, орієнтуючись на реальні загрози та використовуючи дані з тестування для прийняття обґрунтованих рішень. Purple Team надає можливість отримувати конкретні дані про ефективність заходів безпеки. Це допомагає організаціям визначити, які заходи є найбільш важливими та ефективними в контексті їхнього конкретного середовища. За результатами тестування Purple Team можна раціонально розподілити ресурси, зосереджуючись на тих аспектах безпеки, де існує найбільший ризик. Крім того, оптимізація витрат на безпеку також полягає в попередньому виявленні слабких місць та вразливостей. Це дозволяє організаціям визначити та виправити проблеми, зменшуючи ризик виникнення інцидентів та зменшуючи необхідність у великих витратах на відновлення після атак. Таким чином, використання Purple Team стає важливим інструментом для зростання ефективності витрат на безпеку, дозволяючи організаціям більш точно визначати пріоритети та напрямки в області кібербезпеки

Моніторинг та оновлення стратегій безпеки в контексті Purple Team стає невід'ємною частиною кібербезпекового циклу. Регулярні вправи Purple Team дозволяють організаціям систематично оцінювати свою високоризикову поведінку, виявляти нові загрози та атаки, і, відповідно, адаптувати та оновлювати свої стратегії безпеки.

Спільна робота атакуючих (Red Team) і захисників (Blue Team) під час Purple Team дозволяє виявляти нові та еволюційні аспекти загроз. Це може включати в себе виявлення нових методів атак, використання нових інструментів

або розкриття раніше невідомих вразливостей у системах. Такі вправи надають організації можливість підготовитися до найактуальніших загроз та ефективно реагувати на них. Оновлення стратегій безпеки на основі результатів Purple Team стає ключовим кроком у забезпеченні того, що організація залишається високорівнево захищеною від сучасних кіберзагроз. Враховуючи нові відомості та вивчення практичних сценаріїв атак, організація може адаптувати свої стратегії для найефективнішого використання ресурсів та запобігання новим загрозам.

Проаналізуємо аналіз використання та проведення Purple Team. Організація яка хоче оцінити ефективність своєї Purple Team у запобіганні кібератакам та швидкому реагуванні на інциденти створює свої методики оцінки, які

Оцінка проводилася протягом деякого часу і включала наступні етапи:

- Аналіз документів
- Інтерв'ю з членами Purple Team
- Віртуальні атаки на організацію

На етапі аналізу документів ми вивчаємо документи, пов'язані з кібербезпекою організації, включаючи політику безпеки, процедури реагування на інциденти та звіти про інциденти.

На цьому етапі слід провести інтерв'ю з членами Purple Team, щоб дізнатися більше їх відгук про колег та, обов'язки та досвід.

Результати оцінки

Оцінка показала, що Purple Team організації має низку сильних сторін, включаючи:

- Висока кваліфікація членів Purple Team
- Добре налагоджені процеси виявлення та реагування на інциденти
- Ефективна комунікація та співпраця між членами Purple Team

Однак оцінка також виявила деякі області, в яких Purple Team може покращитися, включаючи:

- Координованість дій між різними командами кібербезпеки

- Здатність реагувати на складні атаки
- Управління знаннями

На основі результатів оцінки організація розробила низку рекомендацій для покращення ефективності своєї структурованої Purple Team, включаючи:

Впровадження нових технологій для виявлення інцидентів на ранніх стадіях

Розробка більш детальних процедур реагування на інциденти, які використовують складні техніки.

Впровадження системи управління знаннями

Вправи Purple Team можуть тривати кілька годин, днів або тижнів і включати практичну співпрацю між учасниками з інформаційної безпеки. Час планування залежить від цілей та завдань, що ініціюють вправу, настанов чи обмежень і тактик, технік та процедур (TTPs) емуляції противника.

При розробці програми Purple Team час планування буде зменшуватися, а ефективність призведе до ще більш цінних вправ.

Для успішного завершення етапу планування може бути потрібно проведення зустрічей для планування. Кількість зустрічей і підготовки буде залежати від зрілості програми Purple Team та участі зовнішніх зацікавлених сторін. Наприклад, консультанти, що пропонують вправи Purple Team, витрачатимуть більше часу на підготовку, ніж внутрішні команди, які успішно завершили кілька вправ.

Підготовка Red Team

- Створення принаймні двох систем для відображення активності атаки
- Забезпечення повної функціональності інфраструктури атаки
- Документування всіх команд, необхідних для емуляції TTP в книзі зіграної гри або плані емуляції противника
- Перевірка TTP перед вправою на різних хостах, ніж ті, що використовуються під час вправи, але які налаштовані аналогічно

Підготовка Blue Team

- Перевірка, що засоби безпеки відображають інформацію від цільових систем
- Забезпечення доступу до інфраструктури атаки через контроль проксі/вихід
- Переконатися, що інфраструктура атаки розшифровується (декрипція/перехоплення TLS)

Створення вправи відповідно до процесу DFIR

Це дозволить позначати артефакти та слідкувати за звичайними процесами без підозрілих дій (наприклад, витягування пам'яті з системи, яка не має формального випадку)

Технічна підготовка може займати більше часу на перших вправах, оскільки встановлюються внутрішні процеси. Координатор(и) вправи повинні відстежувати зацікавлених стейкхолдерів, яким були призначені завдання, щоб переконатися, що вони виконуються вчасно.

Координатори вправи повинні співпрацювати зі зацікавленими спонсорами для ідентифікації та забезпечення цільових систем на основі схвалених цілей вправи Purple Team і плану емуляції противника. Продукційні системи найточніше представлення систем у середовищі, оскільки вони повинні мати звітність від інструментів безпеки на продакшн-панелях та дозволяти випробовувати процеси з точністю. Крім того, продукційні системи - це місце, де ви маєте своїх працівників, процеси та технології.

Згідно схвалених цілей та TTPs, цільові системи можуть бути запитані за звичайними процесами, щоб забезпечити відповідність продукційним/живим системам. Якщо запитуються нові системи, вони повинні бути побудовані на тому ж зразку, як і для інших, схожих процесів.

- Операційні системи Endpoint
- Стандартні кінцеві точки - рекомендується 2 для кожної (Windows 10, Linux, macOS)

- Фізичні системи
- Віртуальна інфраструктура робочого столу
- Термінальні служби/Citrix
- Серверні операційні системи в середовищі
- Сервери Windows
- Linux Сервери
- Включаючи віртуальні та хмарні сервери
- Інструменти безпеки

Потрібно переконатися, що на цільових системах були встановлені стандартні, налаштування, інструменти та конфігурації в організації. Це може включати, але не обмежується:

- Антивірус
- Виявлення та реагування на загрози на кінцевих точках (EDR)
- Інстументи для форензиків (криміналістів)
- Потік трафіку проходить через стандартні, продукційні мережеві пристрої, такі як брандмауери та проксі

Облікові записи (також відомі як службові облікові записи, функціональні ідентифікатори) можуть бути створені для входу в системи, доступу до проксі та електронної пошти. Хоча можуть використовуватися реальні, облікові записи, потрібно переконатися, що дані для входу не будуть скомпрометовані під час вправи Purple Team відповідно до TTPs. Якщо це становить загрозу, можна вжити наступні заходи:

- Запит нового облікового запису стандартного користувача
- Запит стандартної електронної пошти
- Запит доступу до інтернету та/або проксі
- Додати новий обліковий запис як локального адміністратора цільових систем

Red Team відповідає за створення інфраструктури атаки вправи Purple Team (внутрішньої чи зовнішньої в залежності від плану емуляції противника). Це включає у себе отримання інструментів, які відворіватимуть поведінку та

методи противника.

Зовнішня інфраструктура

Використання зовнішньої чи внутрішньої інфраструктури буде залежати від організації та поставлених цілей. Одна з головних причин використання зовнішньої інфраструктури полягає в тому, що ви можете перевірити оборонні технології, людей та процеси на в мережі, крім самих хостів. Але це може вимагати більше часу на підготовку.

Вибір та закупівля зовнішнього постачальника хостингу

- Створення зовнішніх віртуальних машин
    - Дозволяти підключення лише з вихідних IP-адрес цільової організації та IP-адрес Red Team
    - Налаштування сайту крадіжки облікових даних і/або сайти доставки корисного навантаження
    - Налаштування інфраструктури C2 - на основі корисних навантажень і TTP
    - Налаштувати редиректори/ретранслятори
- Переконайтеся, що сервери SMTP дозволяють надсилати електронні листи в організацію
    - Необхідно дозволити спільну службу електронної пошти
    - Якщо використовуються нові сервери SMTP, це може потребувати більше часу для отримання репутації
- Налаштування домену або інших редиректорів (за потреби)
- Класифікування доменів або переконатися, що проксі-сервери дозволяють доступ
- Надайте IP-адреси та домени Blue Team, якщо тестування проводитиметься під час наради з планування
- Тестуйте корисні навантаження та домени разом із зацікавленими сторонами, щоб переконатися, що списки дозволених є повними та корисні навантаження/C2 працюють. Це слід робити проти тестових систем; не однакові для вправи.

Внутрішня інфраструктура

- Створення внутрішніх віртуальних машин для атаки
- Переконатися, що дозволено розміщення в рішеннях контролю доступу до мережі
- Налаштування інфраструктури C2 - на основі корисних навантажень і TTP
- Тестування корисних навантажень та доменів разом із зацікавленими сторонами, щоб переконатися, що списки дозволених є повними та корисні навантаження/C2 працюють. Це слід робити проти тестових систем; не однакові для вправи.

Для оцінки ефективності рекомендацій також можна використовувати KPI, такі як час виявлення та реакції на інциденти, кількість виявлених вразливостей, зниження кількості успішних атак та інші параметри, які відображають рівень стійкості та готовності до кіберзагроз системи.

Важливо пам'ятати, що моніторинг та оцінка ефективності мають бути регулярними та адаптованими до змін в кіберландшафті. Нові загрози, технології та вимоги можуть вимагати оновлення стратегій та заходів безпеки.

3.3. Розробка та впровадження рекомендацій

Розробка та впровадження рекомендацій у контексті кібербезпеки є ключовим етапом для забезпечення ефективності та стійкості інформаційних систем. Цей процес включає в себе аналіз поточних методів захисту, ідентифікацію слабких місць, розробку конкретних заходів безпеки та їхнє впровадження. Аналіз поточного стану у сфері кібербезпеки є критичним етапом, який надає відомостей та думок для подальших заходів з удосконалення безпекового позначення організації. Цей процес визначає фундаментальні аспекти системи безпеки та розглядає їх з точки зору захисту від потенційних кіберзагроз.

Встановлення нових програм чи засобів безпеки також може бути

частиною впровадження. Це може включати встановлення антивірусного програмного забезпечення, систем виявлення вторгнень, засобів моніторингу безпеки та інших засобів, які допоможуть у запобіганні та виявленні загроз.

Навчання персоналу - це ще один важливий елемент впровадження рекомендацій. Це може бути проведення тренінгів, презентаційних та звичайних зустрічей, щоб персонал був повністю орієнтований у нових політиках безпеки та знаходився у курсі поточних загроз.

Працюючи в рамках Purple Team, персонал отримує можливість розвивати критичне мислення та навички прийняття рішень в умовах високого тиску. Важливо також відзначити, що Purple Team сприяє розвитку експертизи в галузі кібербезпеки. Він допомагає персоналу не лише розуміти, як працюють заходи безпеки, але й навчає ефективно реагувати на реальні загрози. Це стимулює постійний розвиток та підвищення кваліфікації працівників в галузі кібербезпеки. Таким чином, навчання та розвиток персоналу в контексті Purple Team не лише роблять процес більш ефективним, але й сприяють формуванню висококваліфікованих кадрів, готових ефективно протидіяти сучасним кіберзагрозам.

Постійне удосконалення в області кібербезпеки є критично важливим елементом стратегії захисту інформації. Зважаючи на постійні зміни в кіберзагрозах та розвиток нових технологій, найбільш ефективний захист може бути забезпечений лише за умови систематичного оновлення та удосконалення заходів безпеки.

Незважаючи на те, що впровадження рекомендацій є досить унікальною та індивідуальною для кожної організації чи компанії окремо, існує декілька «загальних» рекомендацій які повинні бути впровадженні для підвищення ефективності Purple Team.

Загальний підхід до кібербезпеки передбачає циклічний процес, де аналіз, розробка рекомендацій, впровадження та оцінка ефективності становлять неперервний цикл безпеки. Такий підхід дозволяє організації підтримувати високий рівень захисту та адаптуватися до найновіших загроз та викликів у

кіберпросторі.

Створення ефективної фіолетової команди, яка підвищує рівень безпеки вашої організації та забезпечує безперебійний і позитивний досвід, вимагає наступних кроків.

1. Розробити план

Перша зустріч для планування може бути розглянута як презентація вправи Purple Team та програми Purple Team. Спонсорів та учасників може бути потрібно переконати у цінності співпраці між різними командами інформаційної безпеки. На зустрічі слід представити концепцію Purple Teaming, представити цілі та завдання, та поділитися цією методологією, яка була використана в безлічі вправ у всьому світі та в різних галузях. Може бути представлений публічний випадок використання для демонстрації миттєвої цінності, наданої вправою Purple Team. Якщо раніше вже виконувалися вправи Purple Team з різними командами, слід поділитися результатами та вдосконаленням з попередніх вправ.

Після того як спонсори та учасники погоджуються на вправу Purple Team, наступна зустріч для планування повинна охоплювати всі вимоги етапів планування та розвідки кіберзагроз. Завдання слід призначити відповідальним зацікавленим сторонам. Координатор вправи відповідає за відстеження та забезпечення виконання всіх завдань перед заключною зустріччю для планування.

Остання зустріч для планування повинна відбутися, щоб переконатися, що всі елементи етапів планування та розвідки були виконані, і все готово для початку вправи. Координатор вправи повинен провести зустріч і пройтися по кожним завданням, призначеним на попередніх зустрічах для планування, щоб перевірити, що всі етапи фази Планування були успішно завершені. Це може включати, але не обмежується:

- Перевірка того, чи відповідає фізичне розташування всім вимогам, включаючи, але не обмежуючись, електропостачання, підключення до всіх систем (інфраструктура атаки та захисту), кондиціювання повітря і т. д.

- Визначення того, чи будуть проводитися обговорення за круглим столом перед вправою чи у день вправи
- Розповсюдження порядку денного всім зацікавленим сторонам

Для почтаку комплексний план фіолетової команди, використовуючи структуру MITRE ATT&CK як керівництво. Це допоможе налаштувати вашу організацію на успіх, допомагаючи червоним і синім командам працювати разом як єдине ціле, щоб розробити потужніший захист, інформований про загрози.

2. Автоматизація

Важливо враховувати, що кіберзагрози постійно еволюціонують, тому заходи безпеки повинні бути готові відповідати новим викликам. Постійне удосконалення полягає у регулярному перегляді та оновленні стратегій, аналізі нових загроз, інтеграції останніх технологічних рішень та вдосконаленні процесів реагування на інциденти.

Інструменти автоматизації стали важливим компонентом методології фіолетової команди. Автоматизація забезпечує безперервне тестування та перевірку, а також гарантує, що прогалини в безпеці не проскочать крізь тріщини та не будуть випадково пропущені. Автоматизація також надає вашій команді безпеки дані в реальному часі та порівняльний аналіз.

3. Поставлені цілі та стратегія тестування

Без цілей команди не зможуть повністю виконати свої місії. Слід розробити своїй групі безпеки детальні цілі, щоб допомогти їм визначити проблемні області та розробити рішення. Вони можуть включати тестування раніше неперевірених тактик, прийомів і процедур (TTP), навчання захисників або тестування ланцюжків атак, щоб назвати декілька.

Стає дедалі очевиднішим, що «одноразового» тестування недостатньо для ефективної практики кібербезпеки. Визначивши найважливіші активи, які потрібно захистити, постійно перевіряйте елементи керування та використовуйте дані про продуктивність для підтвердження успіху. Поєднуючи структуру MITER ATT&CK, тестування та оптимізацію безпеки та фіолетову

команду, команди безпеки можуть «зменшити ризики» за допомогою захисту, інформованого про загрози.

4. Дотримання плану

Дотримання структурованого плану допомагає командам керувати як очікуваними, так і неочікуваними подіями безпеки, які можуть розгортатися під час тренувань фіолетової команди, щоб переконатися, що вони не відриваються від цілей і завдань.

5. Звітування результатів вправ

Після завершення вправ Purple Team слід оцінити результати, щоб отримати чітке уявлення як про успіхи, так і про порушення безпеки організації. Документування результатів допомагає краще визначити та порівняти, що потрібно вашій команді безпеки та організації зараз і в майбутньому.

3.4. Зазначення перспектив розвитку Purple Team у майбутньому

Перспективи розвитку Purple Team у майбутньому обіцяють багатоцільовий підхід до кібербезпеки, який враховує найновіші тенденції та виклики у цій галузі. Кіберзагрози постійно змінюються, і Purple Team може стати ключовим інструментом для підтримки стійкості та безпеки організацій у майбутньому.

Поки що фіолетова команда здебільшого використовується як ланка, що стосується виконання вправ, які об'єднують поєднання синьої команди, червоної команди і розвідки кіберзагроз. Вправи включають планування, узгодження обсягу і серії тестів, а також багато комунікації і прозорості протягом усього процесу. Саме завдяки комунікації та об'єднанню досвіду ці навчання мають таку високу рентабельність інвестицій. Зростаюча популярність і очікування команд безпеки по всьому світу щодо проведення фіолетових командних навчань підтверджують це.

Однією з ключових перспектив є поширення застосування Purple Team в різних галузях та типах організацій. Якщо спочатку він здебільшого

використовувався у сфері корпоративної кібербезпеки, то у майбутньому може розширитися на галузі, такі як охорона критичної інфраструктури, органи влади та навіть освітні і наукові установи.

Іншою перспективою є удосконалення інтеграції Purple Team з іншими ініціативами та технологіями в галузі кібербезпеки. Це може включати в себе поєднання Purple Team з технологіями штучного інтелекту для автоматизації аналізу загроз та вразливостей, а також зі засобами моніторингу безпеки для постійного контролю за станом безпеки систем.

Очікується, що Purple Team буде вдосконалювати свої методи та підходи відповідно до розвитку кіберзагроз та технологічного ландшафту. Можливість проведення сценаріїв атак та вразливостей, які відображають найсучасніші загрози, буде ключовим аспектом його розвитку.

Також важливою перспективою є стандартизація методологій Purple Team, що дозволить організаціям більш ефективно впроваджувати цей підхід у своїх стратегіях кібербезпеки. Створення стандартів та керівництв для використання Purple Team може сприяти поширенню його прийняття в галузі.

Усі ці напрями розвитку допоможуть Purple Team залишатися актуальним та ефективним інструментом в сфері кібербезпеки, допомагаючи організаціям бути попереду захоплюючих загроз та забезпечувати стійкий захист їх інформаційних активів.

ВИСНОВКИ

У контексті кібербезпеки, критичний огляд сучасних тенденцій кіберзагроз є необхідним етапом для визначення найбільш актуальних і серйозних викликів, які можуть впливати на безпеку інформаційних систем. Аналіз сучасних загроз та атак, який розглядається при використанні Purple Team, дозволяє зорієнтувати підхід на збалансоване врахування можливих небезпек та визначення належних заходів для їх запобігання.

Зростання кількості та складності кіберзагроз вимагає постійного апгрейду методології захисту. Інноваційні технології, такі як штучний інтелект, розширена реальність та квантові обчислення, вносять нові виклики і можливості у кіберландшафт. Визначення необхідності апгрейду методології повинно враховувати ці технологічні тенденції та розвивати стратегії захисту відповідно до сучасних вимог.

Оцінка ефективності Purple Team стає ключовим етапом в розумінні та визначенні його ролі в сучасних умовах кібербезпеки. Розробка методики оцінки, що використовує критерії та метрики, дозволяє об'єктивно вимірювати результативність та ефективність його застосування.

Аналіз використання Purple Team у реальних сценаріях вносить практичний аспект у розуміння та оцінку його впливу. Відзначення перспектив розвитку Purple Team у майбутньому визначає напрями його подальшого вдосконалення та адаптації до змін у кіберландшафті.

Розробка та впровадження рекомендацій на базі результатів оцінки дозволяє організаціям впроваджувати покращення та заходи безпеки, спрямовані на зменшення ризиків та підвищення стійкості до кіберзагроз.

Усі ці етапи тісно взаємодіють між собою, створюючи інтегрований підхід до кібербезпеки, який враховує сучасні тенденції та забезпечує ефективний захист від найбільш актуальних загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. The Operational Role of Security Information and Event Management Systems [Електронний ресурс] / Sandeep Bhatt, Pratyusa K. Manadhata, Loai Zomlot // IEEE. – 2014. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/abstract/document/6924640.

2. HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows [Електронний ресурс] / Sadegh M, Rigel Gjomemo, Birhanu Eshete, R. Sekar, V.N. Venkatakrishnan // IEEE. – 2019. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/abstract/document/8835390.

3. Evaluation of open source SIEM for situation awareness platform in the smart grid environment [Електронний ресурс] / Rafał Leszczyna; Michał R. Wróbel // IEEE. – 2015. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/abstract/document/7160577.

4. Best SIEM Tools: A Guide to Security Information and Event Management [Електронний ресурс] / Tim Keary – Режим доступу до ресурсу: https://www.comparitech.com/netadmin/siem-tools/

5. Методика порівняння ефективності сучасних SIEM-систем [Електронний ресурс] / Столова О. В. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/20810/1/13.%D0%A1%D1%82%D0%BE%D0%BB%D0%BE%D0%B2%D0%B0.163-164.pdf

6. McAfee Enterprise Security Manager Data Source Configuration [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://docs.trellix.com/bundle/enterprise-security-manager-data-sourcesconfiguration-reference-guide.

7. McAfee Enterprise Security Manager 11.5.x Product Guide [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://docs.trellix.com/bundle/enterprise-security-manager-11.5.x-product-guide.

8. Technical Aspects of Cyber Kill Chain [Електронний ресурс] / Tarun Yadav – 2015 – Режим доступу до ресурсу: https://www.researchgate.net/publication/281148852_Technical_Aspects_of_Cyber_

Kill_Chain

9. Obotu, Akor Solomon; A., Uganneya Slolomon Ph.D; та Ogezi, Ikese Christopher, «Оцінювальне дослідження системи управління цифровими записами в лікарнях Мінни. (Випадок загальної лікарні Мінна, штат Нігерія). » (2018). – 34 с.

10. «Майбутнє цифрових систем охорони здоров'я: звіт про проведення симпозіуму ВОЗ (Майбутнє цифрових систем охорони здоров'я в європейському регіоні) Копенгаген, Данія, 6–8 лютого –2019: веб-сайт. URL: https://apps.who.int (дата звернення 03.06.2021).

11. Регіональний сегмент Єдиної державної інформаційної системи у сфері охорони здоров'я Оренбурзької області – «технічне завдання»: веб-сайт. URL: https://minzdrav.orb.ru (дата звернення 02.06.2021).

12. Марченко Анна Вікторівна. Проектування інформаційних систем – 2015.

13. Авраменко В.С., Авраменко А.С. Проектування інформаційних систем – 2017.

14. ArhMax Open Server — професійний інструмент веб-розробника під Windows – 2012.

15.

16. Коннолі Т. Бази даних. Проектування, реалізація і супровід. Теорія і практика / Коннолі Т., Бегг К. – [3-е видання. : Пер. з англ.] – М. : Видавничий дім «Вильямс», 2003. — 1440 с.

17."Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in Cyberpower and National Security, FD Kramer, S. Starr, L.K. Wentz (ed.), National Defense University Press, Washington (DC) 2009.

18. THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE CISSP®-September 2011

19. ISO/IEC 27032:2012 [Текст] Information technology — Security techniques — Guidelines for cybersecurity 62

20. Department of Defense “Dictionary of Military and Associated Terms”, 12 April 2001 (As Amended Through 19 August 2009)

21. Cyber Kill Chain Analysis [Електронний ресурс] / Ioan-Cosmin Mihai – 2014 – Режим доступу до ресурсу: https://www.researchgate.net/publication/290832682_Cyber_Kill_Chain_Analysis

22. Security Automation in Information Technology [Електронний ресурс] / Sikender Mohsienuddin Mohammad – 2018 – Режим доступу до ресурсу: https://www.researchgate.net/publication/342977281_Security_Automation_in_Information_Technology

23. Understand the Roles of Red, Blue and Purple Teams [Електронний ресурс] – 2022 – URL: https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/04/19/understand-the-roles-of-red-blue-and-purple-teams (дата звернення: 25.09. 2023).

24. Strategies for Building an Effective Purple Team – 2022 – URL: https://www.iansresearch.com/resources/all-blogs/post/securityblog/2022/04/26/strategies-for-building-an-effective-purple-team

25. The Evolution of Purple Teaming – URL: https://brilliancesecuritymagazine.com/cybersecurity/the-evolution-of-purple-teaming/ (дата звернення: 01.10. 2023)

26. MIRE ATT&CK Веб-сайт URL: https://attack.mitre.org/techniques/T1606/

27. What is a purple team? – 2022 – URL: https://www.crowdstrike.com/cybersecurity-101/purple-teaming/ (дата звернення: 10.11. 2023).

28. The Pyramid of Pain: – 2014 – URL: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (дата звернення: 19.11. 2023).

29. Purple Team Exercise Framework – 2022 – URL: https://scythe.io/ptef (дата звернення: 06.11. 2023).

30.The Purple Team: Combining Red & Blue Teaming for Cybersecurity – URL: https://www.splunk.com/en_us/blog/learn/purple-team.html (дата звернення:

10.11. 2023).

31. TIBER-EU Purple Teaming Best Practices – URL: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_purple_best_practices.20220809~0b677a75c7.en.pdf (дата звернення: 10.11. 2023)

32. How purple teams can embrace hacker culture to improve security https://www.microsoft.com/en-us/security/blog/2021/06/10/how-purple-teams-can-embrace-hacker-culture-to-improve-security/ (дата звернення: 10.11. 2023)