МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

Хотинський Віталій Адамович

Алгоритми виявлення загрози на основі фреймворка MITRE ATT&CK / Threat Detection Algorithms Based on the MITRE ATT&CK Framework

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБм -21
В.І. Хотинський

Науковий керівник
к.т.н., доцент Н.Г. Яцків

Кваліфікаційну роботу
допущено до захисту:

«____» _____ ___2023 р.

Завідувач кафедри
_____ **В.В.Яцків**

ТЕРНОПІЛЬ - 2023

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
«____» _____ 2022 року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

ХОТИНСЬКИЙ Віталій Адамович
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Алгоритми виявлення загрози на основі фреймворка MITRE ATT&CK / Threat Detection Algorithms Based on the MITRE ATT&CK Framework
керівник роботи к.т.н., доцент Н.Г. Яцків

затверджені наказом по університету від 1 грудня 2022 року №

2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– провести аналіз підходів до виявлення кіберзагроз;
– проаналізувати життєвий цикл кібератаки;
– проаналізувати структуру фреймворку MITRE ATT&CK;
– дослідити використання навігатора MITER ATT&CK для візуалізації та покращення можливостей виявлення загроз;
– розробити алгоритм використання MITRE ATT&CK у центрі операцій безпеки.

5. Перелік графічного матеріалу у роботі:
– структура MITER ATT&CK;
– навігатор MITRE ATT&CK – вибір TTP противника;
– додавання різних шарів в MITRE ATT&CK;
– карта виявлення загроз;

– взаємодія IOC, IOA та TTP;
– робочий процес кібероперацій;
– опис впливу вразливості методами ATT&CK.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз підходів виявлення загроз	12.2022 р. – 03.2023 р.	
2	Структура фреймворку MITRE ATT&CK	03.2023 р. – 05.2023 р.	
3	Розробка та дослідження механізму виявлення загроз	05.2023 р. – 11.2023 р.	

Студент _____ Хотинський В.А.
(підпис

Керівник роботи _____ к.т.н., доцент Н.Г. Яцків

(підпис)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Алгоритми виявлення загрози на основі фреймворка MITRE ATT&CK» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека та захист інформації» освітньо-професійної програми «Кібербезпека» написана обсягом 83 сторінки і містить 25 ілюстрації, 1 таблиця, 1 додаток та 34 джерела за переліком посилань.

Метою роботи є підвищення ефективності алгоритмів виявлення загроз на основі фреймворка MITRE ATT&CK.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи виявлення кіберзагроз, методи виявлення кібератак на основі фреймворка MITRE ATT&CK..

Результати дослідження: Удосконалено алгоритми використання MITRE ATT&CK у центрі операцій безпеки.

Показано можливість та переваги використання навігатора MITER ATT&CK для візуалізації та покращення можливостей виявлення загроз.

Результати роботи можуть бути застосовані при розгортанні власної системи розвідки кіберзагроз та центру безпеки операцій.

Ключові слова: РОЗВІДКА КІБЕРЗАГРОЗ, ВИЯВЛЕННЯ ЗАГРОЗИ, ЖИТТЄВИЙ ЦИКЛ КІБЕРАТАКИ, ФРЕЙМВОРК MITRE ATT&CK.

ABSTRACT

Qualification work on "Threat Detection Algorithms Based on the MITRE ATT&CK Framework" for the degree of "Master" in the specialty 125 "Cybersecurity" educational and professional program "Cybersecurity" is written in 83 pages and contains 25 illustrations, 1 table, 1 appendice and 34 source according to the list of links.

The purpose of the work is to improve the effectiveness of threat detection algorithms based on the MITER ATT&CK framework.

Research methods. In order to solve the tasks in this qualification work, the following methods were used: cyber threat detection methods, cyber-attack detection methods based on the MITER ATT&CK framework.

Research results: Improved algorithms for using MITER ATT&CK in the security operations centre.

The possibility and advantages of using the MITER ATT&CK navigator for visualization and improvement of threat detection capabilities are shown.

The results of the work can be applied when deploying your own cyber threat intelligence system and operations security centre.

Keywords: CYBER THREAT INTELLIGENCE, THREAT DETECTION, CYBER ATTACK LIFE CYCLE, MITER ATT&CK FRAMEWORK.

ЗМІСТ

ВСТУП

Актуальність роботи. Зважаючи на постійну зміну ландшафту кіберзагроз, організації постійно відстежують внутрішню мережу та зовнішні точки доступу для захисту від атак. Порушення безпеки призвело б до компрометації даних клієнта, шкоди репутації компанії та ризику втрати даних співробітників, інтелектуальної власності та фізичних даних. Забезпечити гарантію від кібератак складно через доступність інформації через глобальне підключення організації, доступність інформації для зовнішніх користувачів і нові технології. Зростання кількості цілеспрямованих атак продовжує становити серйозну загрозу для організації, оскільки вони продовжують розвиватися та вдосконалювати свої інструменти та тактику. Ці цілеспрямовані атаки, ймовірно, виконуються національною державою або спонсорованими державою групами, які зазвичай називають групою передових загроз (APT). APT націлений на державні, оборонні, фінансові, юридичні, промислові, виробничі, охорону здоров'я, банківську справу та багато іншого, щоб викрасти, шпигувати, руйнувати та завдавати фінансової шкоди. APT-атаки отримують початкову точку опори за допомогою кількох векторів атак, таких як фішинг, соціальна інженерія та використання вразливостей додатків, що виходять в Інтернет. Щойно зловмисник закріплюється, зловмисне програмне забезпечення поширюється внутрішньою мережею, повільно переміщується від однієї системи до іншої, щоб уникнути виявлення та, нарешті, досягти мети зловмисника – викрасти, шпигувати, порушити роботу та приховати свої сліди. APT-атаки часто підпадають під багатоетапну атаку. Враховуючи сказане розробка алгоритмів та рекомендацій виявлення загрози на основі фреймворка MITRE ATT&CK є актуальною науково-прикладною задачею.

Мета і завдання дослідження. Метою роботи є підвищення ефективності алгоритмів виявлення загроз на основі фреймворка MITRE ATT&CK.

Досягнення визначеної мети передбачає вирішення таких завдань:

– провести аналіз підходів до виявлення кіберзагроз;

– проаналізувати життєвий цикл кібератаки;

– проаналізувати структуру фреймворку MITRE ATT&CK;

– дослідити використання навігатора MITER ATT&CK для візуалізації та покращення можливостей виявлення загроз;

– розробити алгоритм використання MITRE ATT&CK у центрі операцій безпеки.

Об'єкт дослідження – процеси виявлення загроз на основі фреймворка MITRE ATT&CK.

Предмет дослідження – алгоритми та механізми виявлення загроз на основі фреймворка MITRE ATT&CK.

Методи досліджень. Для розв'язання поставлених задач у даній кваліфікаційній роботі використано: методи виявлення кіберзагроз, методи виявлення кібератак на основі фреймворка MITRE ATT&CK.

Наукова новизна одержаних результатів. Удосконалено алгоритми використання MITRE ATT&CK у центрі операцій безпеки.

Практичне значення отриманих результатів. Показано можливість та переваги використання навігатора MITER ATT&CK для візуалізації та покращення можливостей виявлення загроз.

Публікації та апробація КР.

1. Яцків Н.Г., Кметик В.В., Хотинський В.А. Візуалізація виявлення загроз з використанням MITRE ATT&CK NAVIGATOR. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2023), Тернопіль, 2023. – С. 21-23.

1. Яцків Н.Г., Смірнов Д.С., Хотинський В.А. Алгоритм використання MITRE ATT&CK у центрі безпеки операцій. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2023. – С. 193-194.

1 АНАЛІЗ ПІДХОДІВ ДО ВИЯВЛЕННЯ ЗАГРОЗ

1.1 Вартість витоку даних

За даними IBM, у 2022 році середня вартість витоку даних становила 4,35 мільйона доларів США, досягнувши найвищого рівня за весь час (рисунок 1.1). Ця цифра на 2,6% більше, ніж минулого року, коли середня вартість витоку становила 4,24 мільйона доларів. Середня вартість зросла на 12,7% з $3,86 млн. [1].

Рисунок 1.1 – Середня вартість витоку даних досягла рекордного рівня у 2022 році

Середня загальна вартість витоку даних& Організації критичної інфраструктури включали організації фінансових послуг, промисловості, технологій, енергетики, транспорту, зв'язку, охорони здоров'я, освіти та державного сектора. 29% зазнали деструктивної атаки або атаки програм-вимагачів, тоді як 17% зазнали злому через скомпрометацію ділового

партнера. 5,2% різниці в середніх витратах на порушення – між 3,15 мільйонами доларів США для повністю розгорнутого та 6,20 мільйона доларів США для нерозгорнутого – це найбільша економія коштів у дослідженні (рисунок 1.2) [2].

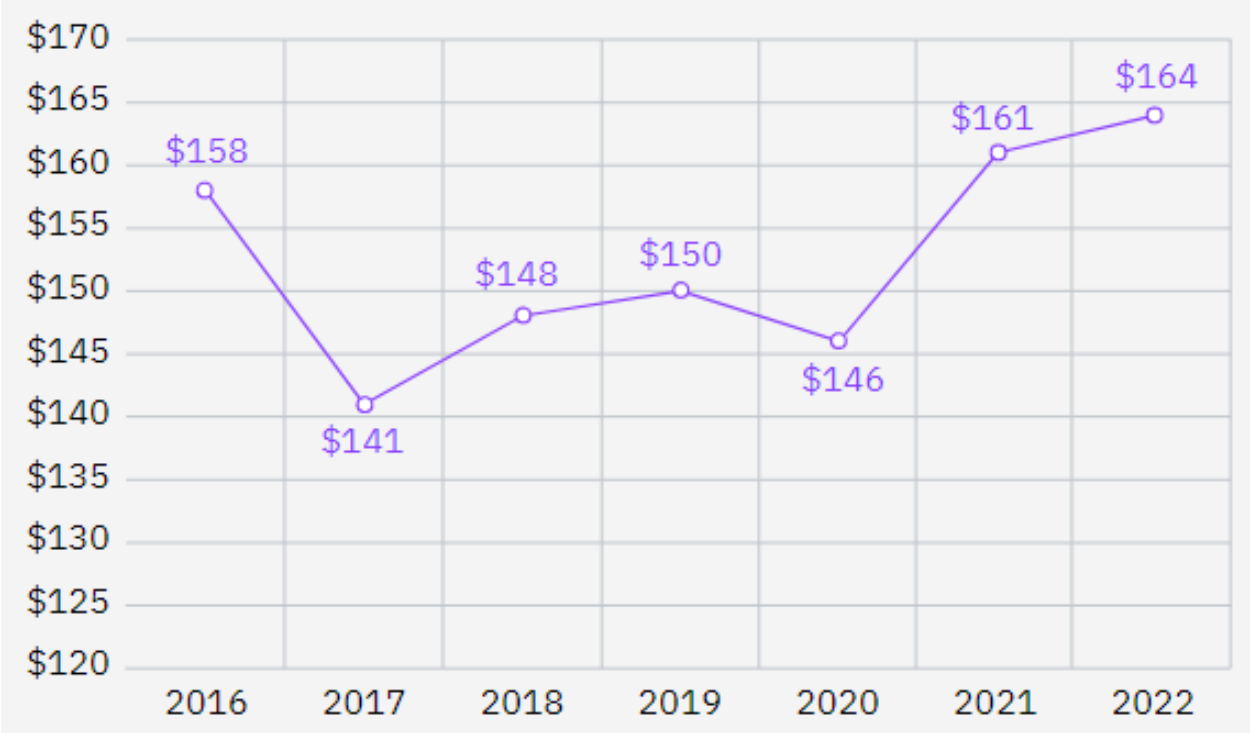


Рисунок 1.2 – Вартість витоку даних за запис досягла семирічного максимуму

Компанії з повністю розгорнутим штучним інтелектом безпеки та автоматизацією також відчули в середньому на 74 дні менший час для виявлення та локалізації порушення, відомий як життєвий цикл порушення, ніж компанії без штучного інтелекту безпеки та автоматизації – 249 днів проти 323 днів. Використання штучного інтелекту безпеки та автоматизації підскочило майже на одну п’яту за два роки, з 59% у 2020 році до 70% у 2022 році [2].

Середня вартість витоку даних за галузями. Середня загальна вартість порушення системи охорони здоров’я зросла з 9,23 млн доларів США у звіті

за 2021 рік до 10,10 млн доларів США у 2022 році, збільшившись на 0,87 млн доларів США, або на 9,4%.

Охорона здоров'я є однією з найбільш регульованих галузей і вважається критичною інфраструктурою урядом США.

Перші п'ятірки галузей за вартістю не змінилися в порядку ранжування зі звіту за 2021 рік. Слідом за охороною здоров'я були фінансова, фармацевтична, технологічна та енергетична галузі (рисунок 1.3).

Фінансовий сектор збільшився з 5,72 млн доларів США у 2021 році до 5,97 млн доларів США у 2022 році, тобто на 0,25 млн доларів США або на 4,4% [2].

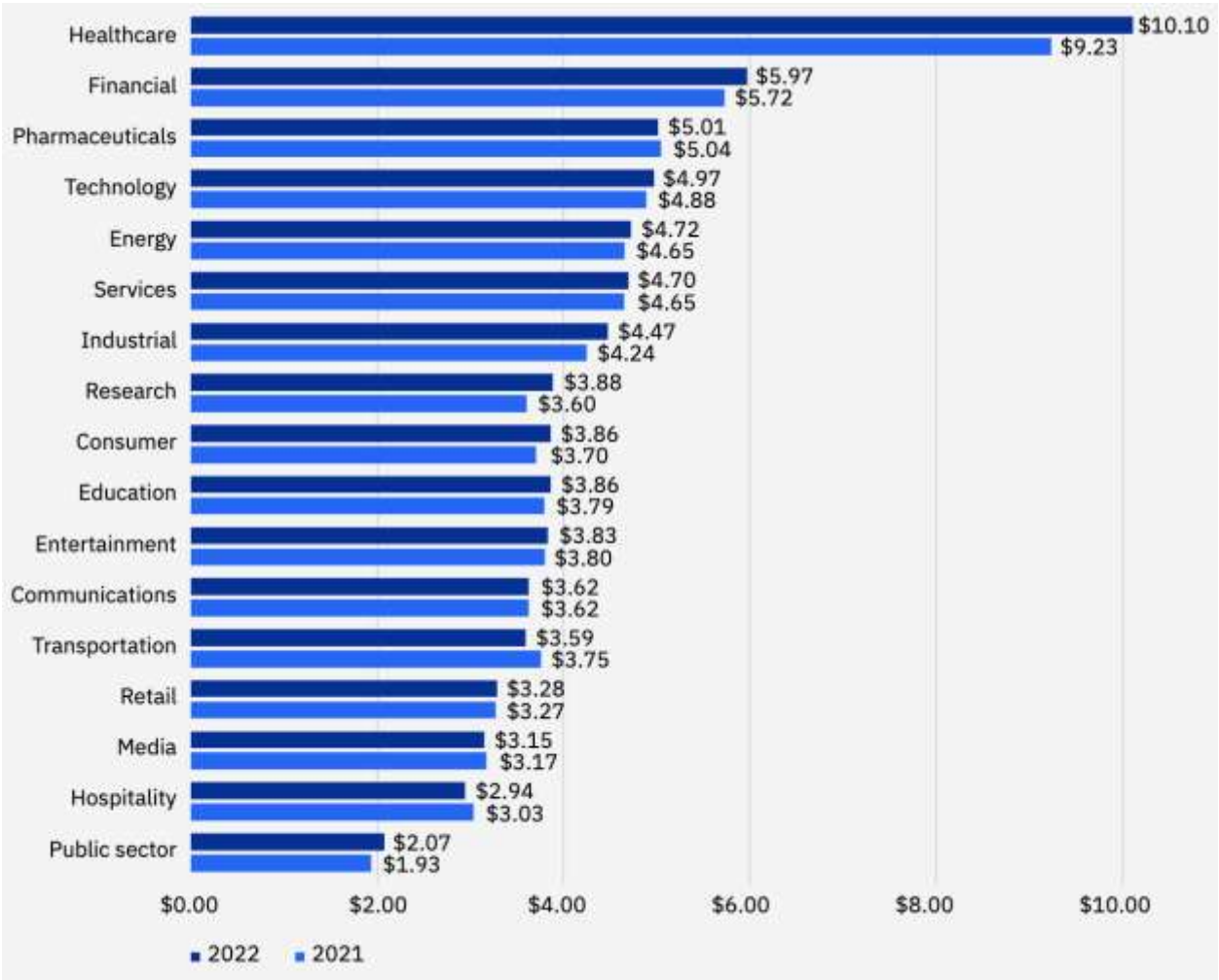


Рисунок 1.3 – Охорона здоров'я була найдорожчою галуззю 12-й рік поспіль

Промислова галузь, що складається з хімічних, машинобудівних і виробничих організацій, збільшилася з 4,24 млн доларів США до 4,47 млн доларів США в 2022 році, збільшившись на 0,23 млн доларів США або на 5,4%. Середня загальна вартість дещо знизилася в чотирьох галузях – фармацевтиці, транспорті, медіа та готельному бізнесі.

У ТОП-5 країн і регіонів із найвищою середньою вартістю витоку даних увійшли США – 9,44 млн доларів, Близький Схід – 7,46 млн доларів, Канада – 5,64 млн доларів, Велика Британія – 5,05 млн доларів і Німеччина – 4,85 млн доларів.

Сполучені Штати очолювали список 12 років поспіль. У той же час країною з найшвидшими темпами зростання в минулому році стала Бразилія, зростання на 27,8% з $1,08 млн до $1,38 млн.

Як показує звіт IBM, раннє виявлення кібератаки є ключовим для обмеження її вартості. Чим довше зловмисник залишається непоміченим і має доступ до технологічних систем цілі, тим більша у нього можливість встановити контроль і таким чином досягти своїх цілей.

Швидкість виявлення кібератак. Захисники виявляють кібератаки швидше, але вони також стикаються з коротшими життєвими циклами атак. Відповідно до «Звіту про розслідування витоків даних», опублікованого у 2022 році Verizon, американською бездротовою мережею, близько 70% порушень, не виявлених зловмисниками, виявляються протягом дня або менше, тоді як 20% потребують «місяців або більше» (рисунок 1.4).

Швидкість виявлення помітно покращилася за останні п’ять років: у 2017 році для виявлення майже 50% порушень, розкритих сторонніми особами, знадобилися «місяці або більше» [3].

Дані Verizon також продемонстрували ступінь, до якого захисники втягнуті в гонку озброєнь, причому швидше виявлення компенсується скороченням життєвого циклу атаки, зокрема через зростання поширеності атак програм-вимагачів [4].

За даними Verizon, у 2016 році близько 6% зломів характеризувалися тим, що зловмисник повідомляв ціль про свою присутність (відоме як розкриття актора).

До 2022 року ця цифра зросла до 58%, що свідчить про те, що більшість кіберзломів залишаються непоміченими, доки зловмисники не знайдуть те, що їм потрібно, і не надішлють повідомлення про викуп [5].

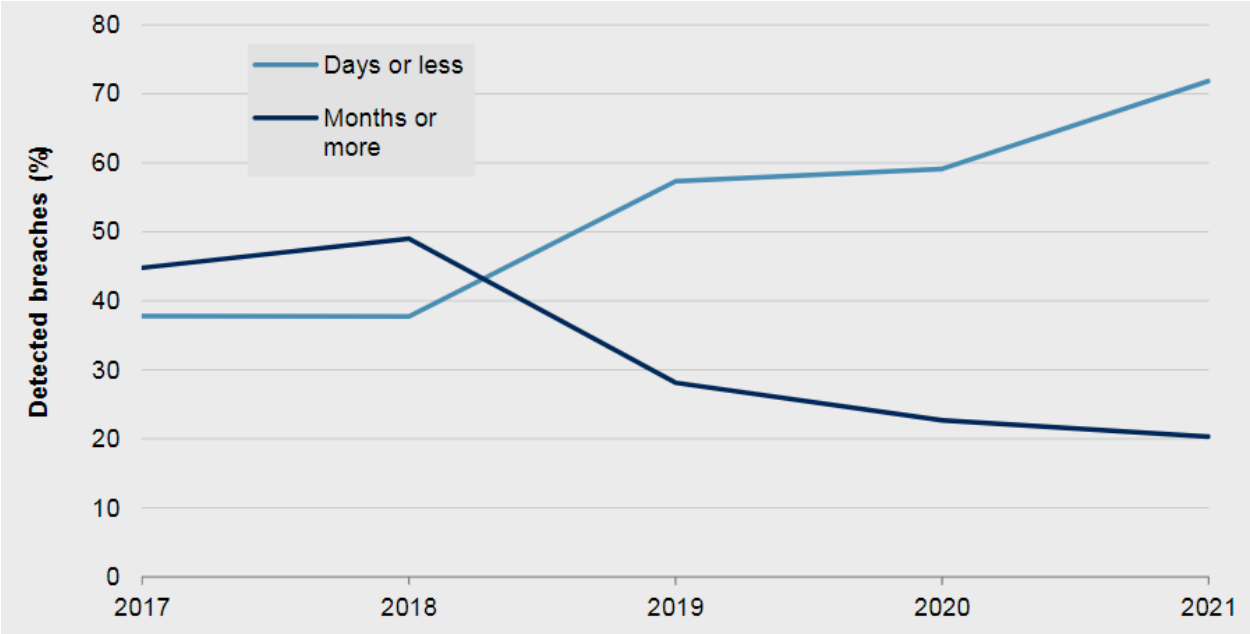


Рисунок 1.4 – Виявлення кібератак прискорюється

Урядові організації відіграють все більшу роль у виявленні інцидентів. Агентство кібербезпеки та безпеки інфраструктури США (CISA), Національний центр кібербезпеки Великобританії (NCSC) і Австралійський центр кібербезпеки (ACSC) розробляють можливості для підтримки організацій державного та приватного секторів у виявленні інцидентів, технічній підтримці, комунікація та охоплення.

Раннє виявлення є ключем до порушення життєвого циклу атаки. Емітенти, які швидко виявляють атаку, дають собі шанс порушити життєвий цикл атаки на ранній стадії та таким чином обмежити фінансовий збиток і потенційний вплив на кредитну якість. Зловмисник не отримує доступ до

цільових систем до третього з п’яти кроків (експлуатація) життєвого циклу атаки.

Таким чином, виявлення зловмисної активності на першому або другому етапі (підготовка та доставка) може звести атаку нанівець.

Наприклад, співробітник може отримати фішинговий електронний лист на етапі доставки атаки. Якщо цей співробітник навчений попереджати про фішинг і має механізм повідомлення про зловмисну електронну пошту, цільовий суб’єкт може відповісти до того, як атака отримає доступ до IT-системи та зможе доставити зловмисне програмне забезпечення.

Навіть якщо це зловмисне програмне забезпечення доставляється, що призводить до порушення системи, швидке виявлення залишається вирішальним для обмеження шкоди.

Відповідь і відновлення зазвичай стають важчими та дорожчими в міру того, як атака прогресує протягом свого життєвого циклу.

Відразу після входу зловмисник може мати доступ лише до невеликого сегменту систем і мереж організації. На цьому етапі захисники можуть ізолювати заражені системи та/або відсікати несанкціонований доступ за допомогою цілеспрямованих дій.

Після того, як зловмисник отримає наполегливість і контроль (четверта фаза життєвого циклу), їх видалення, ймовірно, буде значно дорожчим і трудомістким, вимагаючи узгоджених зусиль для виявлення всіх уражених систем і відновлення їх цілісності.

Якщо зловмисник виконує бажані дії (п’ятий етап), цільовий суб’єкт може нести додаткові витрати, включаючи перерву в бізнесі, репутаційну шкоду та регулятивні штрафи.

Величезна кількість витрат і збитків упродовж життєвого циклу кібератаки робить раннє виявлення (та ефективний план реагування) ключовим у програмі кібербезпеки організації.

Запис логів. Це практика запису активності в системах і мережах організації. Ведення журналів є базовою можливістю програми кібербезпеки у невеликій організації [6 - 8].

У разі кібератаки ефективні журнали забезпечать запис про те, як було зламано захист компанії, що було скомпрометовано, і таким чином дозволить організації (та її зовнішній допомозі) оцінити, як найкраще реагувати та відновлюватися. Це робить журналювання необхідним для скоординованої та успішної відповіді на кібератаку.

Більшим організаціям або організаціям із вищим ризиком можуть знадобитися складні й автоматизовані операції реєстрації, здатні агрегувати дані реєстрації та впорядковувати їх у форматі, зручному для швидкого й точного прийняття рішень. Програмне забезпечення, яке виконує ці функції, широко доступне. Тим не менш, створення інтегрованої системи журналювання, яка охоплює всю організацію та створює цілісне уявлення про діяльність системи для полегшення комплексного аналізу інцидентів, залишається проблемою.

Моніторинг. Моніторинг це ретельний аналіз даних журналів та інших датчиків на наявність індикаторів несанкціонованої діяльності в системах або мережах організації. Це має бути процес у режимі реального часу, який забезпечує можливість виявлення атак за першої нагоди [9-11].

Це особливо важливо для організацій з інтернет-інтерфейсом, включаючи системи електронної пошти, матимуть можливість моніторингу.

Для невеликих організацій із низьким рівнем ризику може складатися з низки автоматичних сповіщень, які попереджають про підозрілу активність.

Організаціям із більшим або вищим ризиком може знадобитися спеціальна операція, відома як центр безпеки (SOC), яка відповідає за обмеження шкоди шляхом виявлення та реагування на кібератаки, які обходять превентивну безпеку.

Такі організації також можуть керувати платформою безпеки інформації та керування подіями (SIEM), яка охоплює всі їхні системи та

мережі та поєднує програмне забезпечення для керування журналами з моніторингом подій безпеки в реальному часі.

Не всі платформи SIEM однакові, і інвестиції в більш просунуті системи можуть мати істотний вплив на зниження ризику.

Дійсно, штучний інтелект безпеки та автоматизація, які сприяють швидкому виявленню та реагування на кібератаки, були більш ефективними для зменшення витрат на кіберзлом, ніж будь-які інші інвестиції, проаналізовані IBM [2].

1.2 Найпоширеніші типи кібератак

Фішинг. Фішинг – це атака соціальної інженерії, під час якої зловмисник надсилає повідомлення особі в організації, намагаючись обманом змусити її відкрити електронний лист або вкладений файл, у результаті чого в систему потрапить зловмисне програмне забезпечення чи програма-вимагач, або розкрити облікові дані, які дозволять зловмиснику доступу до мережі та даних організації. Фішинг зростає, і, згідно з даними Microsoft, зловмисники перемістили свою увагу від атак зловмисного програмного забезпечення до використання фішингу для отримання облікових даних людей [12-14].

Шкідливе програмне забезпечення. Зловмисне програмне забезпечення – це зловмисне програмне забезпечення, яке часто вставляється в комп’ютери, коли відкриваються вкладення у фішингових електронних листах або клацаються посилання. Воно зламує інформаційні системи, використовуючи вразливі місця мережі. Зловмисне програмне забезпечення може включати віруси, клавіатурні шпигуни, програми-шпигуни, черв’яки або програми-вимагачі.

Програми-вимагачі. Програми-вимагачі – це форма зловмисного програмного забезпечення, яке блокує користувача з його інформаційних

систем, якщо зловмиснику не буде сплачено викуп. Деякі зловмисники, які не отримають викуп, у відповідь опублікують конфіденційні дані компанії в Інтернеті.

Розподілена атака на відмову в обслуговуванні (DDoS). Розподілена атака типу «відмова в обслуговуванні» бомбардує центральний сервер організації одночасними запитами даних, спричиняючи його зависання, утримуючи компанію в заручниках, доки не буде виконано вимоги зловмисника.

Інші кібератаки включають атаки грубої сили, впровадження SQL та інші атаки соціальної інженерії.

1.3 Життєвий цикл кібератаки

Сама кібератака має життєвий цикл (рисунок 1.5). Це важливо, оскільки реагування на інцидент повинно бути активовано якомога швидше, перш ніж атака перейде в наступну фазу. Чим глибша фаза, тим більше буде втрата організації [15-17].

Рисунок 1.5 – Життєвий цикл кібербезпеки

1. Розвідка: будь-який зловмисник виконуватиме розвідку або збиратиме інформацію про цільову систему, щоб отримати будь-яку поверхню для атаки. Це може бути у формі сканування портів, IP-сканування, архітектури мережі, людей (персонал/вище керівництво).

Певною мірою розвідка також може зібрати інформацію про особистість людей, щоб допомогти зловмиснику вибрати підхід соціальної інженерії (ось чому ми не публікуємо в Інтернеті багато деталей, що стосуються наших особистих інтересів).

2. Озброєння: після того, як зловмисник зрозуміє поверхню атаки (це може бути вразливість технологій або людей), зловмисник підготує «зброю» / експлойт. Зловмисник може провести дослідження експлойтів, звичайну атаку проти вразливості, створити фішинговий веб-сайт і електронну пошту тощо.

3. Доставка та використання: на цьому етапі запускається атака та намагається використати вразливість. Якщо вразливість, виявлена в системі, є SQL-ін'єкцією, тоді зловмисник здійснить атаку, надіславши запит із забороненим символом для використання вразливості. Він також може бути доставлений через спам/фішингову електронну пошту, яка використовує необізнаність людини.

4. Встановлення: на цьому етапі зловмисник тимчасово зламав систему, якщо організація помітить злом і негайно відреагує (закриє порт, вимкне вразливі служби, оновить пароль), зловмисник негайно втратить доступ. Через це зловмисник повинен підтримувати свою присутність, знаходячи спосіб встановити будь-який бекдор (таким чином зловмисник будує підземний тунель у внутрішній організації), щоб полегшити майбутню активність експлойту.

5. Командування та контроль: на цьому етапі зловмисник має постійний доступ до системи та намагатиметься використовувати більше для досягнення своєї мети (номер кредитної картки, фінансова інформація, ідентифікаційна інформація клієнта тощо). Підвищення привілеїв для отримання більшого контролю над машиною. Виконайте іншу розвідку, щоб отримати більше цілей і поверхонь для атаки. Спробуйте отримати доступ до іншої системи. У разі успіху збережіть присутність і підвищте привілей.

Всією діяльністю зловмисник керує віддалено через бекдор, встановлений заздалегідь.

6. Дії щодо цілей: це місце, де пошкодження є серйозним. Зловмисник отримав потрібний йому доступ і може запустити свої зловмисні засоби залежно від початкової мети (порушити конфіденційність, цілісність або доступність).

Отже, процес досягнення мети зловмисника – це довгий шлях. Його атаку можна зупинити відключивши певну фазу. Чим швидше буде виявлено та прийняті адекватні міри, тим легше впоратися з нападом. З точки зору реагування на інцидент, це не обов'язково має бути великий інцидент, щоб процедура реагування на інцидент була виконана. Знання цього життєвого циклу допомагає організації зробити реагування на інцидент більш зрілим і мінімізувати будь-які потенційні втрати, спричинені інцидентом.

Знаючи життєвий цикл кібератаки, ми бачимо, що інцидент не завжди має бути серйозним, коли відбувається значна втрата, а скоріше його можна врегулювати від початку фази, щоб мінімізувати або навіть «запобігти» збитку.

1.4 Полювання на кіберзагрози

Полювання за кіберзагрозами – це проактивний пошук зловмисників і вмісту у вашій системі [18-20].

Полювання на загрози є обов'язковою частиною оборонної стратегії, яка спрямована на виявлення та швидке реагування на невідомі, невиявлені та невирішені загрози. Це означає, що команда безпеки навмисно шукає зловмисні дії, які відбуваються на рівні кінцевої точки або мережі. Мисливці за загрозами аналізують дані безпеки, шукаючи приховане шкідливе програмне забезпечення або зловмисників. Пошук шаблонів підозрілої діяльності також є в їх списку.

Замість того, щоб чекати, поки відбудеться атака, мисливець за загрозами активно шукає всі події, які можуть вплинути на систему.

Зловмисникам часто вдається залишатися та діяти непоміченими протягом місяців у мережі, яку їм вдалося зламати. Їм часто вдається шукати та збирати дані, отримати облікові дані для входу, отримати несанкціонований доступ і виконувати бічні рухи в середовищі абсолютно безтурботно.

Згідно з дослідженням Джозефа Очієнга «Полювання на кіберзагрози», кіберзлочинці витрачають у середньому близько 192 днів, перш ніж їх виявляють у системі.

Оскільки жодна система не захищена на 100% ефективно, компаніям слід зосередитися не лише на класичних продуктах кібербезпеки, а й на вдосконаленні своїх методів пошуку загроз. Елементарна кібергігієна, правильне впровадження брандмауерів, правильно налаштована фільтрація DNS та інші інструменти безпеки можуть зупинити кібератаки ще до їх початку. Не менш важливо, вони можуть запобігти втраті грошей та інших ресурсів.

Якщо загрозливому суб’єкту вдалося уникнути виявлення та проникнути в систему, ви захочете, щоб із вашої мережі вийшли потенційні постійні загрози.

Полювання на загрози є критично важливим елементом стратегії безпеки. Це дозволяє бути на крок попереду зловмисників і вчасно реагувати на їхні атаки.

Процес пошуку кіберзагроз. Пошук кіберзагроз – це багатоетапний процес, який відбувається циклічно. Оскільки саме полювання є активним, мисливець насправді не знає, що саме шукати. Процес починається з визначення мети полювання на загрозу. Наступний крок – аналіз. Останнім кроком є виправлення та реакція на видалення загрози з системи. Нижче наведено опис різних етапів [21, 22]:

1. Визначення цілі пошуку кіберзагроз.

Перший етап полювання полягає в тому, щоб визначити основні причини, чому ви проводите полювання, і поставити чіткі цілі.

Які активи є найціннішими та потрібно захистити? Які з них могли б призвести до подальших, більш вражаючих збитків, якщо на них напали? Які недоліки чи вразливості може знайти та використовувати загрозливий суб'єкт?

Оскільки існує широкий спектр потенційних загроз і даних, які потрібно отримати, проведення полювання без попереднього встановлення цілей, швидше за все, не вдасться. Серія маленьких ділянок направленого полювання завжди краще, ніж велика нережисована.

2. Збір даних. Хороший пошук кіберзагроз відображає якість зібраних даних. Неповні дані часто призводять до напіввдалого полювання та помилкового відчуття безпеки. Використовуйте рішення для управління інформацією та подіями безпеки (SIEM), щоб отримати статистичні дані та записи про діяльність в IT-середовищі вашого підприємства.

Чи більше даних призводить до кращого результату? Не завжди з наступних причин:

Обсяг – збір більшої кількості даних означає, що команда витратить більше часу на їх обробку. Залежно від обставин полювання більший обсяг даних може лише призвести до збільшення часу.

Класифікація – деякі методи найкраще працюють з меншими наборами даних, ніж з великими наборами даних, наприклад групування та підрахунок стеків.

Щоб відповісти на основне запитання під час пошуку загроз, важливо зосередитися на необхідній інформації. Полювання на кіберзагрози також має бути безперервним процесом, коли минулі пошуки становлять основу та мотивацію для майбутніх.

3. Аналіз даних. Цей етап може бути справді складним, оскільки ви маєте справу з великою кількістю даних. Шифрування та кодування часто використовуються в журналах даних, щоб залишатися нерозкритими навіть

після збору. Мисливці за загрозами повинні видалити журнали, які розбивають корисне навантаження атаки на невеликі пакети, щоб повністю перевірити кожну унцію інформації, активів або даних.

Після завершення аналізу можна очікувати два результати [23, 24]:

Правильна гіпотеза – вказує на відсутність доказів присутності агента атаки в системі.

Неправильна гіпотеза – якщо висунута гіпотеза підтверджується, мисливець повинен якнайшвидше перевірити характер, ступінь і вплив атаки на систему. Більше того, мисливець за загрозами повинен розробити ефективну відповідь на атаку.

4. Відповідь. Після аналізу даних мисливець за загрозами повинен створити найкращу відповідь на загрозу, визначивши як короткострокові, так і довгострокові рішення для протидії атаці. Мета тут полягає в тому, щоб якнайшвидше припинити поточну атаку.

Група безпеки також повинна [25, 26]:

– захистити постраждалу організацію;

– запобігти пошкодженню системи;

– виключити можливість майбутнього нападу.

5. Отримані висновки. Дізнавшись про атаку, мисливець за загрозами повинен використовувати цю інформацію, щоб запобігти подібним подіям у майбутньому.

Основною метою етапу отримання висновків має бути покращення процесу безпеки, враховуючи кожен елемент. Люди за своєю природою є істотами, які схильні до помилок, тому людський фактор є значною загрозою та може бути вразливим місцем.

Наприклад, якщо не вчасно виправити системи, це може призвести до порушень безпеки. Звільнення відповідної особи не усуне загрозу чи не вирішить вирішення. Натомість кращою реакцією було б впровадження автоматизованих виправлень у всій організації.

Типи полювання на загрозу. Структуроване полювання. Відправними точками для цього типу пошуку загроз можуть бути індикатори атаки (IoA) і TTP зловмисника. Структуроване полювання на загрози використовує платформу MITER Adversary Tactics Techniques and Common Knowledge (ATT&CK) [27].

Неструктуроване полювання. У цьому випадку індикатори компромісу (IoC) працюють як тригер для процесу пошуку загроз. IoC – це криміналістичні дані, які допомагають дослідникам виявляти зловмисну активність у мережах і на пристроях. Серед виявлених загроз можуть бути витоки даних, зловмисне програмне забезпечення та трояни.

Керується ситуацією. Конкретні пов’язані з бізнесом ризики, тенденції та аналіз вразливостей, які є унікальними для системи компанії, також можуть бути відправною точкою пошуку загроз.

Ключові елементи пошуку кіберзагроз. Основна робота пошуку кіберзагроз полягає в моніторингу повсякденної діяльності та трафіку в мережі. Під час цього проактивного процесу ви досліджуватимете можливі аномалії, щоб знайти будь-які невиявлені шкідливі дії, які можуть призвести до витоку даних.

У зв’язку з цим пошук загроз складається з чотирьох ключових елементів [28, 29].

Методологія. Для успішного процесу полювання на кіберзагрози організації повинні застосовувати проактивний, постійний підхід, який постійно розвивається. Спеціальна, імпровізована перспектива буде контрпродуктивною та дасть лише мінімальні результати.

Технології. Більшість організацій уже мають комплексні рішення безпеки кінцевих точок із автоматизованим виявленням. Полювання на загрози працює на додаток до них і додає передові технології для пошуку аномалій, незвичайних шаблонів та інших слідів зловмисників, яких не повинно бути в системах і файлах.

Кваліфікований персонал. Мисливці за загрозами – це експерти з кібербезпеки, які не лише знають, як використовувати згадані технології безпеки. Вони також поєднують наполегливе прагнення йти в наступ з інстинктивними здібностями до вирішення проблем, щоб виявити та пом’якшити приховані загрози.

Інтелект загроз. Наявність доступу до глобальної розвідувальної інформації, заснованої на фактичних даних, збільшує й полегшує пошук уже існуючих індикаторів компромісу (IOC). Така інформація, як класифікація атак для зловмисного програмного забезпечення та ідентифікація групи загроз, а також розширені індикатори загрози, можуть допомогти визначити IOC.

2 СТРУКТУРА ФРЕЙМВОРКУ MITRE ATT&CK

2.1 Фреймворк MITRE ATT&CK

Сьогодні загрози кібербезпеці не просто розвиваються, а й поширюються. У зв'язку зі швидким зростанням і прогресом суб'єктів загрози реактивних механізмів захисту вже недостатньо. У минулому кібератаки складалися з простих і зрозумілих методів, оскільки складних і великих цифрових систем не існувало. Однак з часом цифрові системи розрослися та стали складнішими цифровими структурами, що ускладнює розуміння кібератак за допомогою більш просунутих методів. Це також ускладнює виявлення кібератак. Сьогодні, щоб повністю зрозуміти кібератаку, необхідно змоделювати етапи та деталі кібератак у спосіб, який підходить для конкретних груп. Одним із важливих фреймворків, які відповідають цим потребам моделювання, є фреймворк MITRE ATT&CK.

Заснована в Сполучених Штатах у 1958 році, MITER є організацією, яка створює інноваційні рішення для просування національної безпеки по-новому та служить незалежними радниками в суспільних інтересах. Сфери роботи MITRE включають кібербезпеку, авіацію, штучний інтелект і машинне навчання, авіацію та транспорт, оборону та розвідку, державні інновації, охорону здоров'я, національну безпеку та телекомунікації [30].

Фреймворк MITER ATT&CK – це структура бази даних знань, відома під акронімом Adversary Tactics, Techniques, and Common Knowledge. Це структура, представлена MITRE у 2013 році та постійно вдосконалювана за допомогою технологій. Завдяки фреймворку MITER ATT&CK кібератаки можна систематично аналізувати. Кібератаки можна розділити на певні етапи, а методи, які використовуються на кожному етапі, можна глибоко проаналізувати та використати в дослідженнях кібербезпеки. MITRE ATT&CK Framework є важливим ресурсом для кожного працівника індустрії кібербезпеки.

Структура MITER ATT&CK є важливою для аналітиків SOC. Оскільки MITER ATT&CK Framework детально охоплює кожен етап кібератак, аналітики SOC можуть чітко бачити, які кроки необхідно виконати на кожному етапі кібератаки, і використовувати їх як орієнтир. Таким чином можна більш ефективно використовувати методи виявлення та пом'якшення атак, розроблені проти кібератак, кібератаки можна відобразити, написати докладний звіт і заархівувати деталі атаки для подальшого використання. Оскільки ця структура містить чітку дорожню карту кібератак, можна проводити дослідження щодо інших можливих атак, які, можливо, ще не відбулися, таким чином розробляючи способи їх виявлення або запобігання.

2.1.1 Матриця MITRE ATT&CK

Структура MITER ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – це глобально доступна база знань про тактику та прийоми ворогів, заснована на реальних спостереженнях. Вона надає детальну матрицю стратегій, які кіберзловмисники використовують на різних етапах життєвого циклу атаки, від початкового доступу до системи до викрадання даних, допомагаючи фахівцям з кібербезпеки зрозуміти, виявити та захиститися від кіберзагроз.

MITRE ATT&CK Matrix – це метод, який використовується для класифікації та візуалізації методів атак зловмисників. Матриці можна налаштувати та перетворити на корисні візуальні елементи майже для будь-якої теми. MITER створив матриці MITER ATT&CK для візуалізації деталей поведінки зловмисників.

Типи матриць. У рамках MITER ATT&CK Framework було створено 3 різні матриці відповідно до типів платформ [31]:

1. Матриця підприємства.

2. Мобільна матриця.

3. Матриця ICS (Industrial Control Systems, Промислові системи управління).

1. Матриця підприємства – це перша матриця, створена MITEP. Ця матриця включає більше цифрових систем і ширше використовується, ніж ті, що включені в інші матриці, тому в цій матриці більше інформації, ніж в інших матрицях. Матриця підприємства часто використовується для розуміння кібератак у великій організації. На рисунку 2.1 детально показана корпоративна матриця:

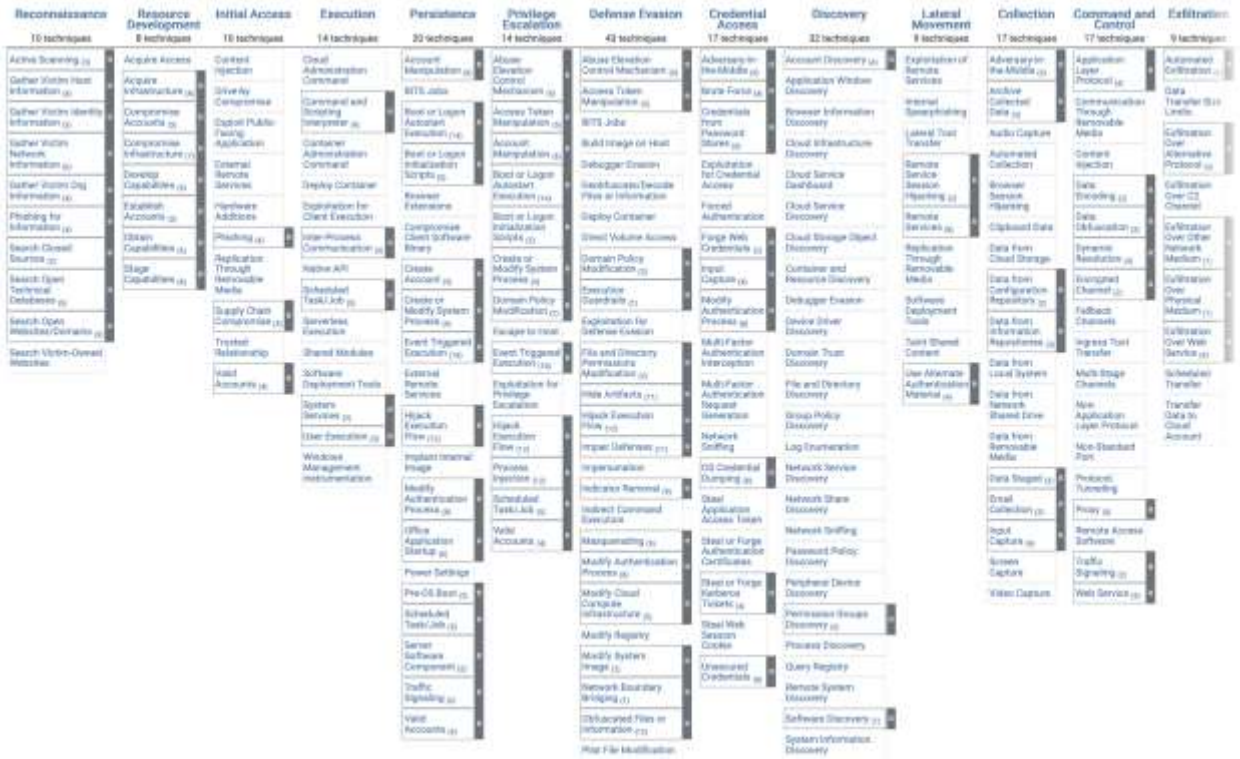


Рисунок 2.1 – Матриця підприємства

На даний час існує 7 підматриць від матриці підприємства (рисунок 2.2):

1. PRE: Ця підматриця зосереджена на фазі планування та розвідки кібератак. Вона включає методи й тактики, які атакуючі використовують для збору інформації та підготовки до нападу.

2. Windows. Підматриця Windows спеціально стосується методів і тактик атак на операційні системи Windows. Вона охоплює різні аспекти атак на основі Windows і надає інформацію про вразливості, привілеї, стійкість тощо.

3. macOS. Підматриця macOS стосується методів і тактик атак проти операційних систем macOS. Вона охоплює різні аспекти атак на основі macOS і надає інформацію про вразливості, привілеї, стійкість тощо.

4. Linux. Підматриця Linux охоплює техніку та тактику атак проти операційних систем Linux. Він охоплює різні аспекти атак на основі Linux і надає інформацію про вразливості, привілеї, стійкість тощо.

5. Хмара. Підматриця чмари розглядає техніку та тактику атак на хмарні системи. Вона охоплює різні аспекти хмарних атак і надає інформацію про вразливості, автентифікацію, витік даних тощо.

6. Мережа. Підматриця мережі обговорює методи атак і тактику проти мереж. Вона охоплює різні аспекти мережевих атак і містить інформацію про безпеку мережі, моніторинг трафіку, фішинг тощо.

7. Контейнери. Підматриця «Контейнери» стосується методів і тактик атак проти систем, заснованих на контейнерах. Він охоплює різні аспекти атак на основі контейнерів і надає інформацію про безпеку контейнерів, привілеї, поверхню атаки тощо.

Рисунок 2.2 – Підматриця матриці підприємства

2.1.2 Мобільна матриця

Мобільна матриця – це матриця, підготовлена для мобільних пристроїв і містить інформацію про кібербезпеку мобільних пристроїв. Матриці охоплюють методи, що включають доступ до пристрою та мережеві ефекти, які можуть використовувати зловмисники без доступу до пристрою. Цю матрицю можна використовувати для захисту індивідуальних і корпоративних мобільних пристроїв. У порівнянні з корпоративною матрицею вона містить менше інформації. Матриця містить інформацію для таких платформ: Android та iOS.

Mobile Matrix включає дві підматриці:

Android: підматриця Android охоплює техніку та тактику атак на операційну систему Android. Вона охоплює різні аспекти атак на пристрої на базі Android і надає інформацію про вразливості, зловмисне програмне забезпечення, дозволи користувачів тощо.

iOS: підматриця iOS стосується методів і тактик атак на операційну систему iOS. Вона охоплює різні аспекти атак на пристрої на базі iOS і надає інформацію про вразливості, зловмисне програмне забезпечення, дозволи користувачів тощо.

2.1.3 Матриця ICS

ICS Matrix – це матриця, що містить інформацію, зібрану для кібербезпеки пристроїв у промислових системах управління. Цю матрицю можна використовувати для забезпечення та аналізу кібербезпеки у промислових системах управління (рисунок 2.3).

Тактика. Тактика стосується мети кібер-зловмисника та причини його дій. Тактика є одним із найважливіших компонентів MITER ATT&CK Framework, який використовується для групування поведінки кібер-зловмисників і визначення етапів атаки. Тактика знаходиться у верхньому рядку матриці.

Рисунок 2.3 – Матриця ICS

Види тактики. Тактика зазвичай складається із загальних тверджень, оскільки вони виражають мету та причину нападу. Тому тактика для кожної матриці багато в чому схожа. Наприклад, на на рисунку 2.4 показано детальну інформацію про тактику початкового доступу матриці підприємства.

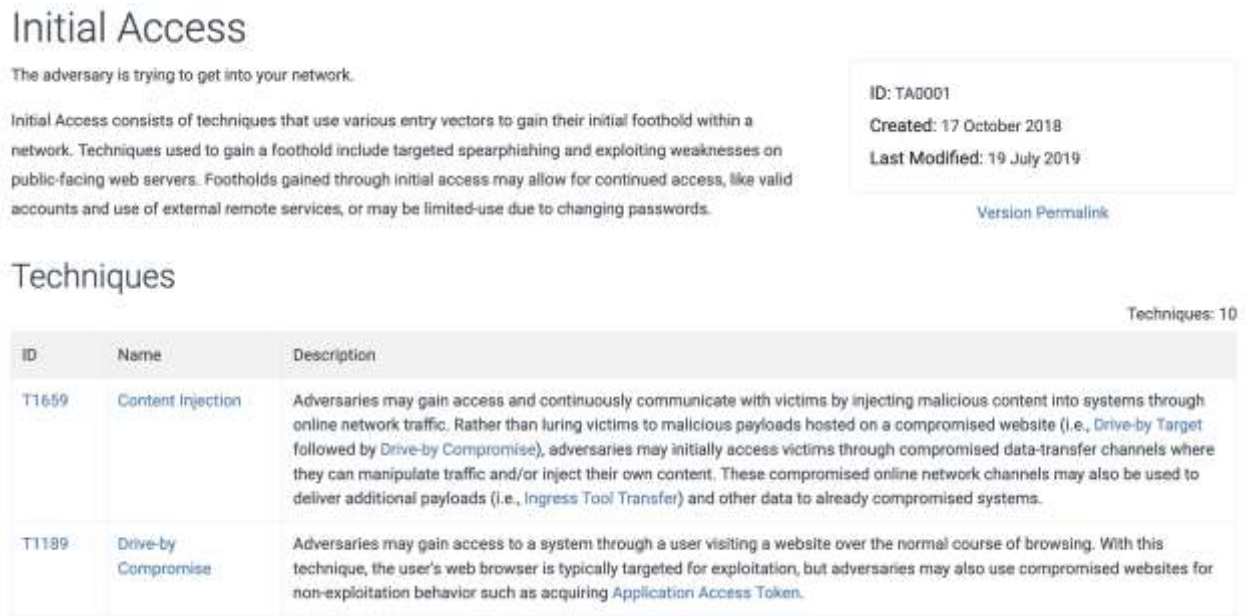


Рисунок 2.4 – Тактика в корпоративній матриці

Тактика підприємства. Тактика представляє техніки ATT&CK або підтехніки. Тактична мета зловмисника виконати дію: це причина виконання дії (рисунок 2.5). Наприклад, зловмисник може захотіти отримати доступ до облікових даних. У списку нижче наведено 14 різних тактик (рисунок 2.6).

Enterprise tactics

Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.

Enterprise Tactics: 14

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Рисунок 2.5 – Детальний опис тактики підприємства

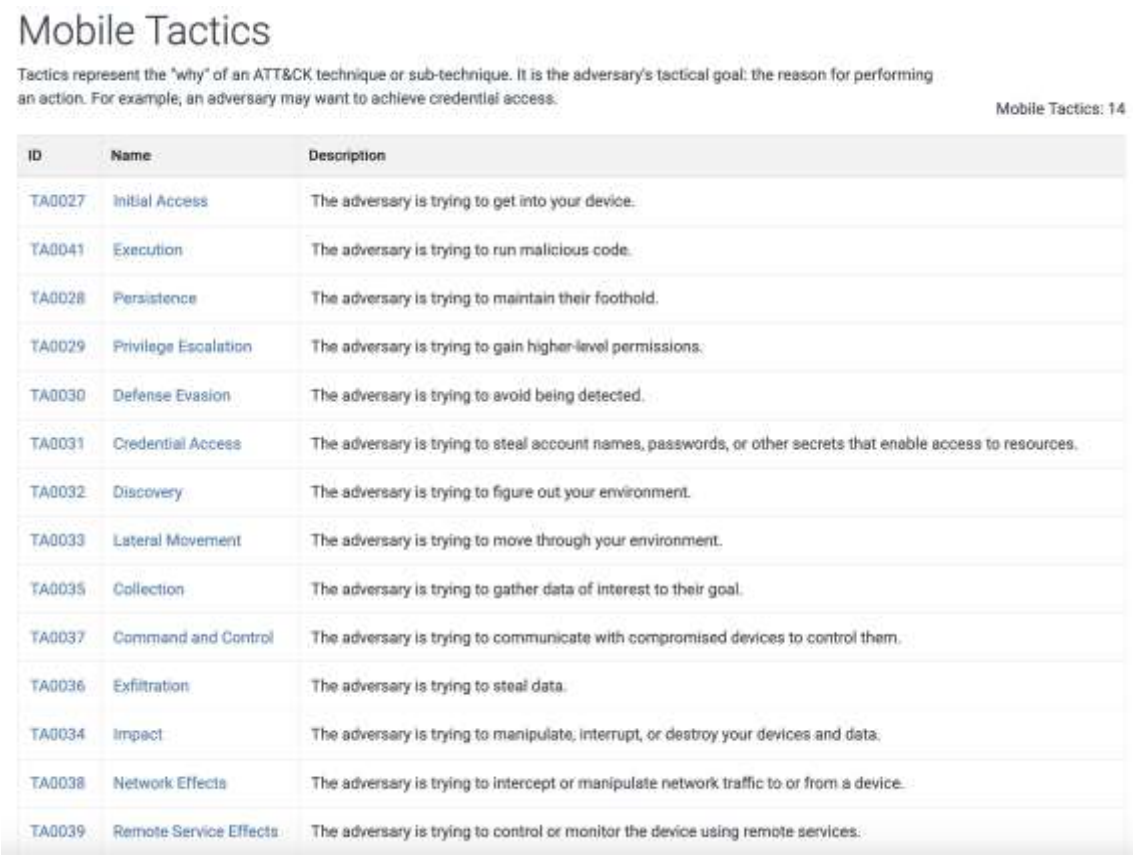
TACTICS

- Enterprise
  - Reconnaissance
  - Resource Development
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control
  - Exfiltration
  - Impact
- Mobile
- ICS

Рисунок 2.6 – Перелік тактик рівня підприємства

2.1.4 Мобільна тактика

Це тактична мета супротивника: мотив виконання дії. Наприклад, зловмисник може захотіти отримати обліковий доступ (рисунок 2.7). У списку на рисунку 2.8 наведено 14 різних тактик.



Mobile Tactics

Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.

Mobile Tactics: 14

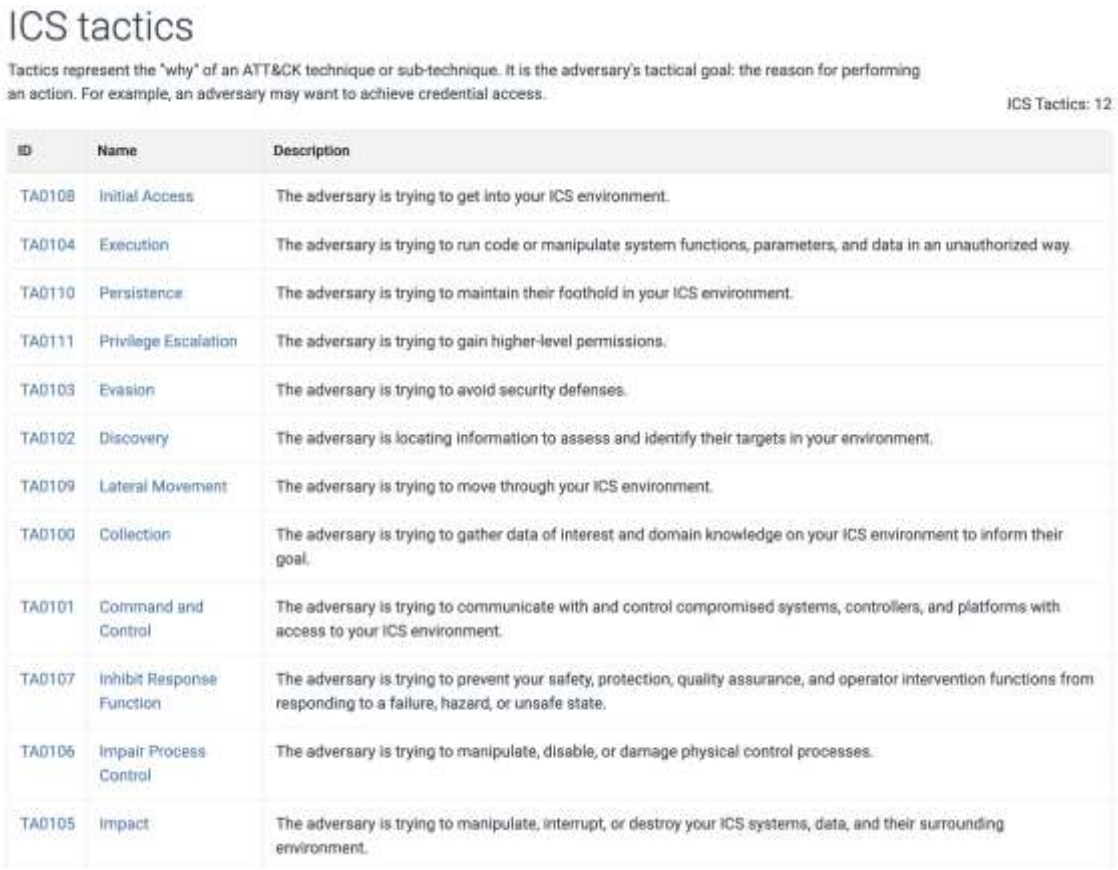
ID	Name	Description
TA0027	Initial Access	The adversary is trying to get into your device.
TA0041	Execution	The adversary is trying to run malicious code.
TA0028	Persistence	The adversary is trying to maintain their foothold.
TA0029	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0030	Defense Evasion	The adversary is trying to avoid being detected.
TA0031	Credential Access	The adversary is trying to steal account names, passwords, or other secrets that enable access to resources.
TA0032	Discovery	The adversary is trying to figure out your environment.
TA0033	Lateral Movement	The adversary is trying to move through your environment.
TA0035	Collection	The adversary is trying to gather data of interest to their goal.
TA0037	Command and Control	The adversary is trying to communicate with compromised devices to control them.
TA0036	Exfiltration	The adversary is trying to steal data.
TA0034	Impact	The adversary is trying to manipulate, interrupt, or destroy your devices and data.
TA0038	Network Effects	The adversary is trying to intercept or manipulate network traffic to or from a device.
TA0039	Remote Service Effects	The adversary is trying to control or monitor the device using remote services.

Рисунок 2.7 – Мобільні тактики

Рисунок 2.8 – Перелік мобільних тактик

2.1.5 Тактика ICS.

Тактика відображає ATT&CK техніки або підтехніки. Це тактична мета супротивника: мотив виконання дії (рисунок 2.9). Наприклад, зловмисник може захотіти отримати обліковий доступ. У списку нижче наведено 12 різних тактик (рисунок 2.10).



ICS tactics

Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.

ICS Tactics: 12

ID	Name	Description
TA0108	Initial Access	The adversary is trying to get into your ICS environment.
TA0104	Execution	The adversary is trying to run code or manipulate system functions, parameters, and data in an unauthorized way.
TA0110	Persistence	The adversary is trying to maintain their foothold in your ICS environment.
TA0111	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0103	Evasion	The adversary is trying to avoid security defenses.
TA0102	Discovery	The adversary is locating information to assess and identify their targets in your environment.
TA0109	Lateral Movement	The adversary is trying to move through your ICS environment.
TA0100	Collection	The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal.
TA0101	Command and Control	The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment.
TA0107	Inhibit Response Function	The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
TA0106	Impair Process Control	The adversary is trying to manipulate, disable, or damage physical control processes.
TA0105	Impact	The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment.

Рисунок 2.9 – ICS тактики

2.1.5 Техніки та підтехніки

Тактика в матриці показує цілі зловмисників, але не містить детальної інформації про метод атаки зловмисника. Однак техніки та підтехніки вказують на методи, які атакуючий використовує для досягнення своєї мети, і на те, як він здійснює атаку. Кожна техніка/підтехніка включена в матрицю на основі певної тактики. Наприклад, деякі методи в матриці підприємства показані на рисунку 2.10.

Більшість полів у зображеній матриці є методами. Деякі техніки мають підтехніки, а деякі ні. Як показано на рисунку 2.10, якщо в матриці поруч із полями з назвами технік є сірі зони, це означає, що ці техніки мають підтехніки. Для прикладу розглянемо підтехніки перших 5 прийомів тактики «Розвідка»:

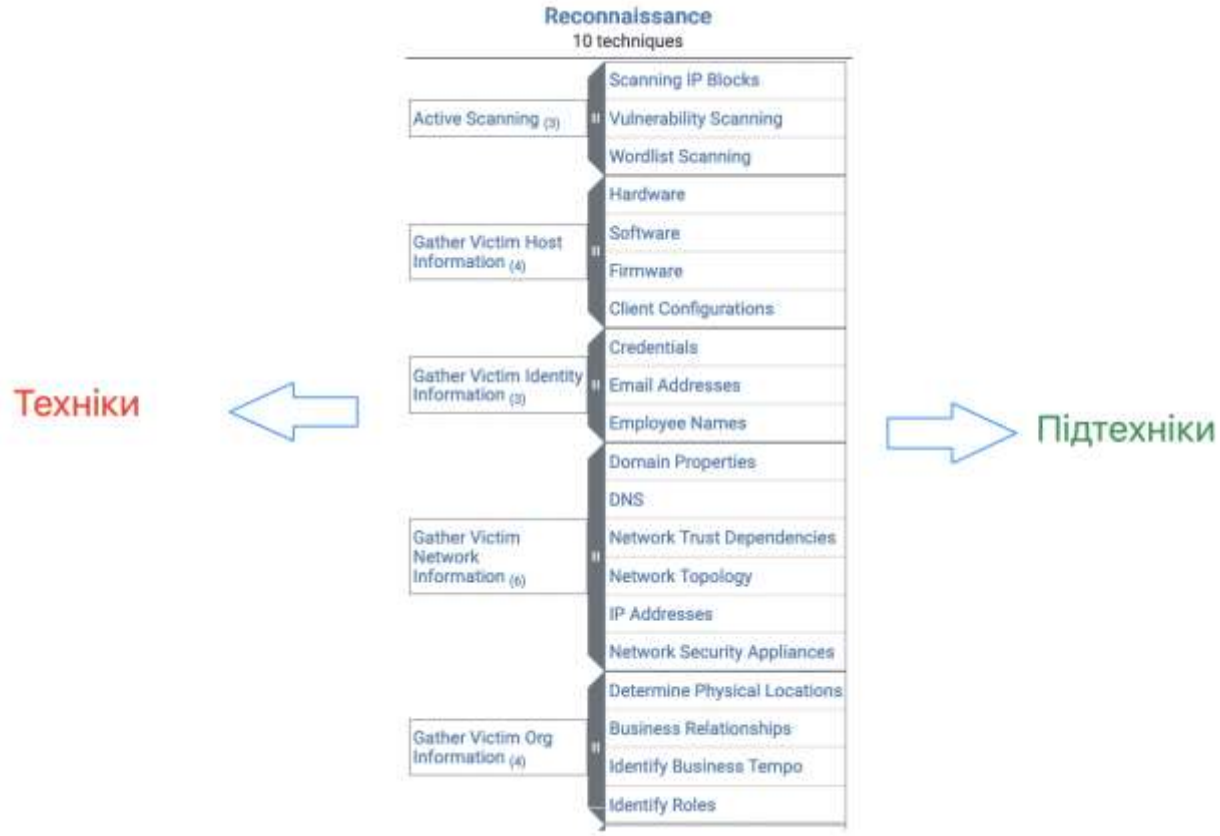


Рисунок 2.10 – Техніки та підтехніки

Типи технік і підтехніки. Техніки поділяються на 3 групи за матрицями:

– Методи підприємства.

– Мобільна техніка.

– Методи ICS.

Методи підприємства. Кількість методик Enterprise досить велика і постійно оновлюється. Поточні цифри (17.11.2023) такі:

Техніки: 201.

Підтехніки: 424.

Ви можете перевірити поточні проблеми за наступним посиланням: https://attack.mitre.org/techniques/enterprise/

Мобільна техніка. Загальна кількість мобільних технологій менша, ніж корпоративних, і з часом оновлюється. Нижче наведено кількість доступних мобільних технік і підтехнік:

Техніки: 72.

Підтехніки: 42.

Ви можете переглянути поточні проблеми за наступним посиланням: https://attack.mitre.org/techniques/mobile/

Методи ICS. Як і методи інших матриць, методи ICS оновлюються з часом. Нижче наведено кількість доступних методів і підметодів ICS:

Техніки: 81.

Підтехніки: 0.

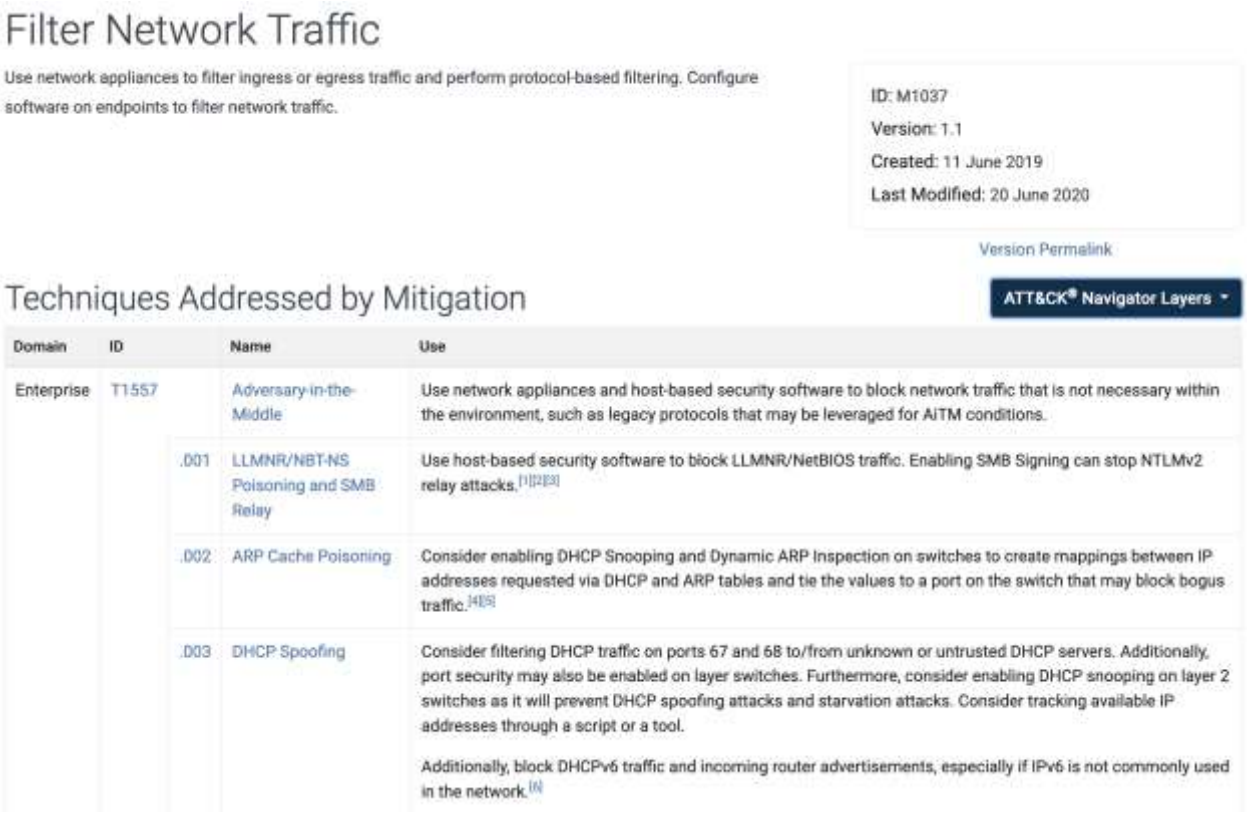
Процедура. Процедура включає приклади використання технік і підміток. Вона просто вказує, який інструмент/програмне забезпечення було використано під час виконання технік. Іншими словами, вона дає інформацію про практичне використання технік. Приклад процедури для техніки «Дампінгу облікових даних ОС» показано на зображенні нижче. Доступ до процедур також можна отримати на сторінці техніки (рисунок 2.11).

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims.[1][2][3]
G0050	APT32	APT32 used GetPassword_x64 to harvest credentials.[4][5]
G0087	APT39	APT39 has used different versions of Mimikatz to obtain credentials.[6]
G0001	Axiom	Axiom has been known to dump credentials.[7]
S0030	Carbanak	Carbanak obtains Windows logon password details.[8]

Рисунок 2.11 – Приклад процедури

Пом'якшення. Пом'якшення стосуються запобіжних заходів і дій, які можна вжити проти методів у матриці MITRE ATT&CK. Кожне пом’якшення має унікальний ідентифікатор, назву та опис, що робить їх зрозумілими. Наприклад, на рисунку 2.12 показано один із прикладів пом’якшення підприємства.



Filter Network Traffic

Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.

ID: M1037
Version: 1.1
Created: 11 June 2019
Last Modified: 20 June 2020

Version Permalink

Techniques Addressed by Mitigation

ATT&CK® Navigator Layers

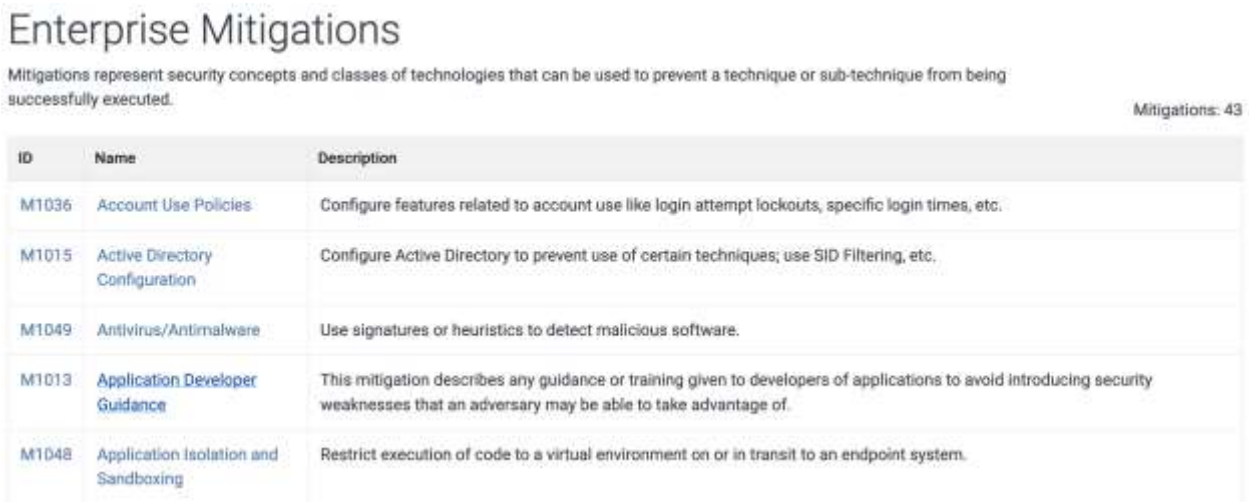
Domain	ID	Name	Use
Enterprise	T1557	Adversary-in-the-Middle	Use network appliances and host-based security software to block network traffic that is not necessary within the environment, such as legacy protocols that may be leveraged for AiTM conditions.
	.001	LLMNR/NBT-NS Poisoning and SMB Relay	Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks.[1][2][3]
	.002	ARP Cache Poisoning	Consider enabling DHCP Snooping and Dynamic ARP Inspection on switches to create mappings between IP addresses requested via DHCP and ARP tables and tie the values to a port on the switch that may block bogus traffic.[4][5]
	.003	DHCP Spoofing	Consider filtering DHCP traffic on ports 67 and 68 to/from unknown or untrusted DHCP servers. Additionally, port security may also be enabled on layer switches. Furthermore, consider enabling DHCP snooping on layer 2 switches as it will prevent DHCP spoofing attacks and starvation attacks. Consider tracking available IP addresses through a script or a tool. Additionally, block DHCPv6 traffic and incoming router advertisements, especially if IPv6 is not commonly used in the network.[6]

Рисунок 2.12 – Техніки пом’якшення

Типи пом'якшення.

- Корпоративні пом'якшення.
- Мобільні пом'якшення.
- Пом'якшення ICS.

Пом’якшувальні заходи рівня підприємства (рисунок 2.13).



Enterprise Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

Mitigations: 43

ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software.
M1013	Application Developer Guidance	This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.
M1048	Application Isolation and Sandboxing	Restrict execution of code to a virtual environment on or in transit to an endpoint system.

Рисунок 2.13 – Корпоративні пом'якшення

Розуміння та впровадження інфраструктури MITER ATT&CK є життєво важливим для сучасних зусиль у сфері кібербезпеки, оскільки вона пропонує єдину мову та структуру для опису поведінки кіберсупротивника. Це дозволяє організаціям більш повно оцінювати стан безпеки, забезпечуючи цілеспрямований пошук загроз і більш ефективне реагування на інциденти. Інфраструктура не тільки покращує здатність організації виявляти та пом’якшувати кіберзагрози, але також допомагає в ефективному розподілі ресурсів і стратегічному плануванні, тим самим сприяючи загальній безпеці та фінансовому здоров’ю організації.

2.2 Переваги використання MITER ATT&CK

Тактика та техніка в MITER ATT&CK – це сучасний метод, який використовується для розуміння учасників загроз у атаках на кібербезпеку. Тактика обговорює, які методи або методи зловмисник використовуватиме для здійснення атаки, тоді як техніка обговорює, як виконується тактика, тоді як загальні відомості - це колекція інформації та документація про використання тактики та прийомів певними супротивниками.

Фреймворк MITER ATT&CK можна використовувати для багатьох випадків, зокрема:

а) удосконалити існуючу технологію виявлення в організації;

б) провести оцінку видимості організації атак, які відбуваються;

в) використання MITRE ATT&CK для вдосконалення поточних можливостей і можливостей організації з аналізу загроз;

г) проведення симуляції суперництва між червоною командою та синьою командою, щоб побачити слабкі сторони одна одної;

д) допомагає підвищити зрілість програми пошуку загроз в організації.

Структура MITER ATT&CK – це добре задокументована база знань про тактику, техніку та процедури (TTP). ТТП – це модель поведінки справжніх злочинців. Прикладом цього є відомий звіт, опублікований FireEye про шпигунську групу Mandiant APT1. У звіті FireEye задокументувала моделі поведінки, методи, тактику, програмне забезпечення, індикатори компрометації, викрадені дані та час атаки. Фреймворк MITER ATT&CK спрощує ці результати, включаючи список розширених постійних загроз (APT) із методами та інструментами, які можна знайти в реальному житті.

У контексті структури MITER ATT&CK різниця між TTP (тактикою, технікою та процедурами), IOC (індикаторами компрометації) та IOA (індикаторами атаки) має вирішальне значення для максимізації її ефективності в пошуках загроз, аналізі загроз і техніки виявлення.

Отже, чим вони відрізняються.

TTPs: тактика, техніка та процедурами описують атаку, пропонуючи розуміння поведінки та методології, які використовують супротивники.

Тактика: це загальна мета або стратегія, якої намагається досягти супротивник. Наприклад, тактикою може бути «Первинний доступ» до мережі або системи.

Техніка: це специфічний спосіб, яким супротивник намагається досягти своєї тактичної мети. Дотримуючись тактики «Початкового доступу», технікою може бути «Фішингове вкладення».

Процедура: це точний покроковий метод, який противник використовує для виконання техніки. У контексті техніки «Spear-Phishing Attachment» процедура може бути такою: «Створення електронного листа під виглядом IT-відділу компанії та надсилання його цільовим співробітникам із вкладеним шкідливим PDF-файлом, який використовує відому вразливість в Adobe Reader».

Ця деталізація допомагає переходити від широкого розуміння цілей супротивників (тактики) до методів, які вони обирають (техніки), аж до дрібних деталей їхньої конкретної діяльності (процедури). Розуміючи TTP на цьому детальному рівні, ми можемо створити більш цілеспрямований захист.

IOCs: Індикаторами компромісу є докази, залишені після нападу. Це можуть бути IP-адреси, шкідливі файли або URL-адреси.

IOA: індикатори атаки підкреслюють намір і дії, спрямовані на компрометацію системи. Метою IOA є виявлення атаки, що триває, на відміну від IOC, які є постфактум. Це може включати неправильну передачу даних або спроби несанкціонованого доступу.

2.3 Використання навігатора MITER ATT&CK для візуалізації та покращення можливостей виявлення загроз

Інженери з виявлення або будь-хто інший, відповідальний за створення правил виявлення, іноді може страждати від того, що виявляти, і пріоритетів виявлень. У середовищі, яке швидко змінюється, як-от кібербезпека, важливо визначити пріоритетність виявлень. Враховуючи, нові кампанії атак, нові версії фреймворків, як-от MITER ATT&CK, нові нульові дні, які поширюються дуже швидко, при цьому, важливо правильно розставляти пріоритети для виявлення можливих загроз.

Розвідка про кіберзагрози (Cyber threat intelligence, CTI) є хорошим інструментом у даному арсеналі, який допомагає визначити, що виявляти

загрози. CTI дає нам змогу побачити поточний ландшафт загроз, визначити можливих супротивників і визначити пріоритети для загроз. Щоб створити варіанти використання для виявлення зловмисників, інколи для операцій SOC потрібна допомога команд CTI, які збирають інформацію з преміум-ресурсів, досліджують темну сторону мережі для збору інформації, спостерігають за звітами, щоб побачити поточні атаки, а іноді й не роблять цього. Особливо в незрілому середовищі або в середовищах, які є реактивними, а не проактивними, прості кроки чи інструменти можуть мати великий вплив на розуміння поточного ландшафту загроз організації.

MITER ATT&CK Navigator – це інструмент, який ми можемо використовувати для простої візуалізації та визначення пріоритетів нашої поточної можливої загрози, а результати можуть керувати інженерами з виявлення під час створення нових правил. Розглянемо, як використовувати навігатор для створення карти можливих загроз. Отже, інженери з виявлення можуть використовувати цю карту, щоб вирішити, що включити та/або визначити пріоритет у своїх програмах виявлення. Найкраще те, що не потрібно знати жодних подробиць про життєвий цикл CTI або мати найсучасніші канали CTI для створення карти. Базові знання фреймворку MITER ATT&CK допоможуть створити теплову карту [2].

По-перше, людина, яка відповідає за створення логіки виявлення, має визначити поточні загрози для організації. Цей процес ідентифікації може включати багато речей (політичних, географічних, фінансових тощо). Окрім деталей, для відправної точки інженер може просто переглянути APT, які націлені на галузь організації, країну та технології, які активно використовуються. Припустімо, що інженер визначає, що APT28, APT32 і FIN7 націлені на країну, в якій працює ця організація. Також інженер ідентифікує групи Magic Hound і Wizard Spiders, націлені на сектор, у якому працює ця організація. І нарешті, інженер визначив п’ять можливих APT, що становить загалом п’ять основних, які потрібно враховувати.

Вибір навігатора MITRE ATT&CK. На сторінці Navigator інженеру з виявлення потрібно створити п’ять різних рівнів для кожної групи загроз. Ці рівні складаються з TTP, який використовується кожною групою загроз. Якщо інженеру пощастить, навігатор вже має в базі даних пару Threat Group – TTP. Якщо інженер не може знайти пару Threat Group – TTP, тоді TTP потрібно дослідити. Групу загроз можна знайти, просто натиснувши кнопку «пошук і багаторазовий вибір» (1), потім потрібно знайти назву групи загроз (2). Сподіваємось, на вкладці Групи загроз інженер зможе знайти групу загроз і натиснути кнопку Вибрати (3) (рисунок 2.14) [32, 33].

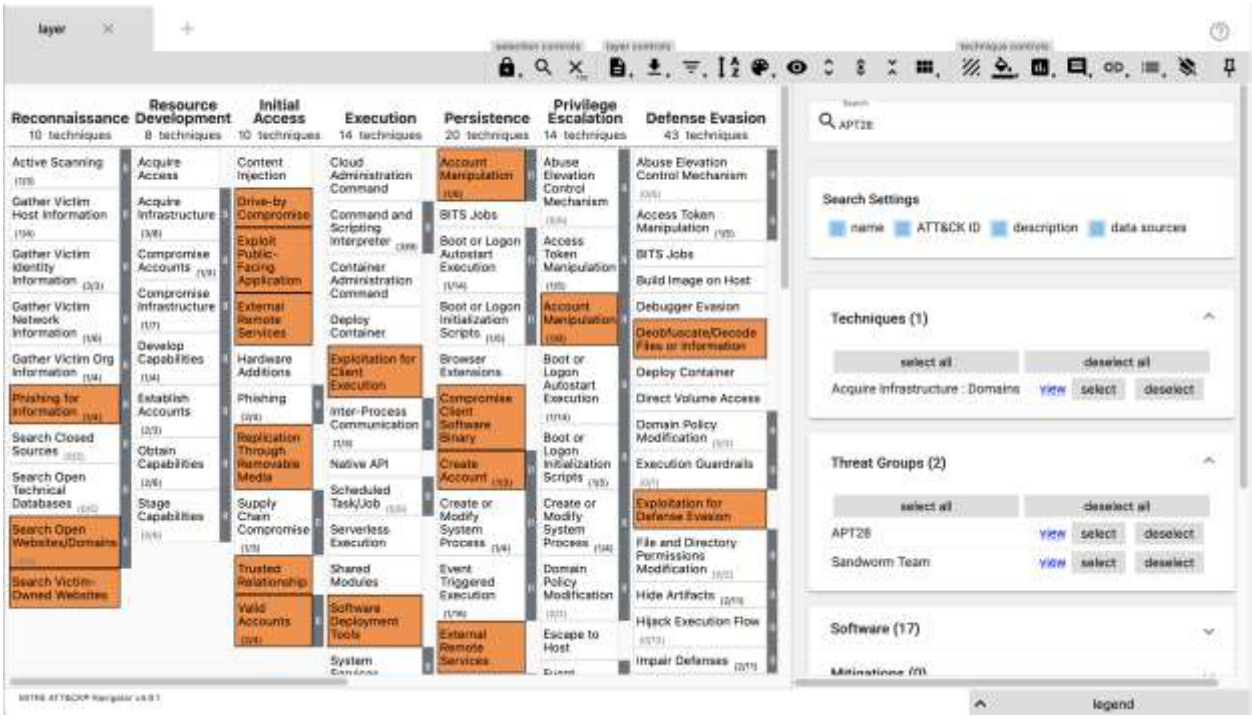


Рисунок 2.14 – Навігатор MITRE ATT&CK – вибір TTP противника

Далі інженер повинен призначити бали виділеним методам, які використовує група загроз. Це можна зробити, натиснувши кнопку «Підрахунок» і вибравши оцінку (4). Оцінку потрібно встановити на 1. Інженер повинен виконати ці чотири кроки для кожної групи загроз.

Останнім етапом буде додавання 5 пар Threat Group – TTP на одному рівні. Для цього інженеру з виявлення потрібно відкрити новий шар, але цього разу потрібно вибрати «Створити шар з інших шарів» замість

натискання «Створити новий шар». Важливим параметром у цьому меню є «вираз оцінки», який також пояснюється праворуч.

Давайте введемо «a+b» як вираз, щоб наказати ATT&CK Navigator обчислити суму всіх оцінок, призначених TTP у наших шарах «a» та «b» – подивіться, як він автоматично призначає ці змінні шарам у верхній лівій частині екрана. Можна залишити всі параметри без змін і натиснути «створити» (рисунок 2.15).

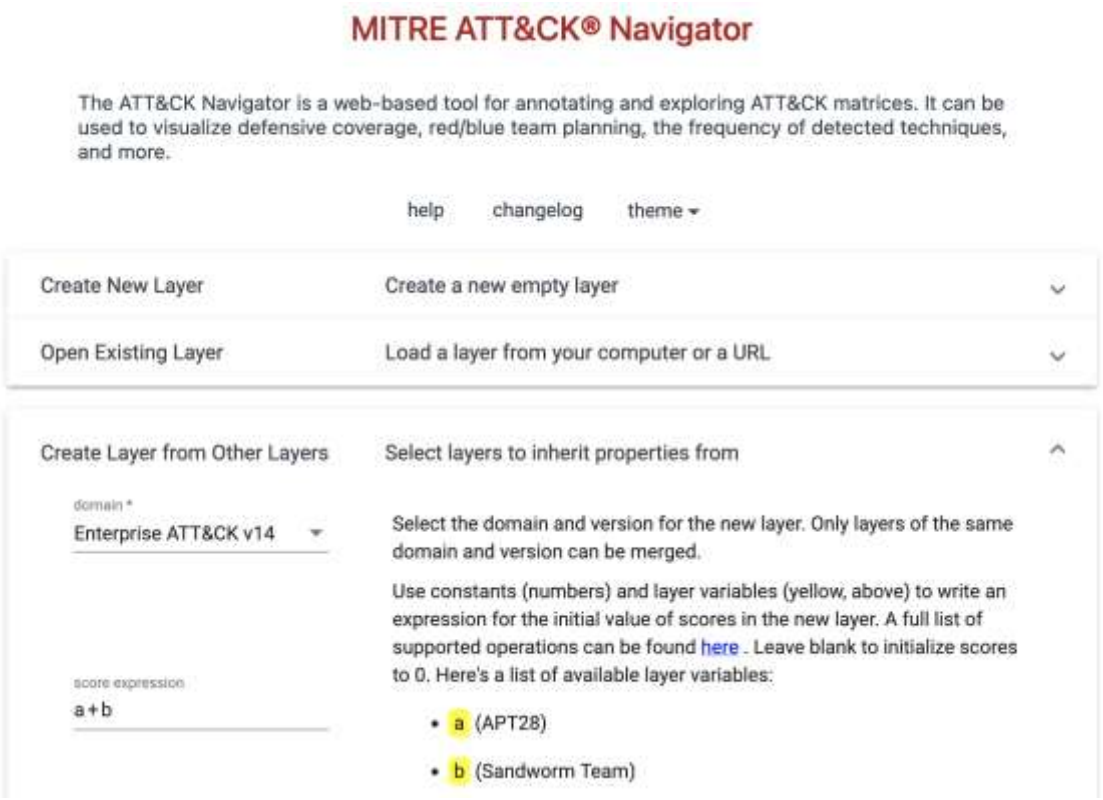


Рисунок 2.15 – Додавання різних шарів в один шар

В результаті повинні очікувати побачити карту, яка складається з різних кольорів для різних технік, як можна побачити нижче. Більш інтенсивні/темніші техніки вказують на те, що їх використовує більше APT. Наприклад, зелений колір означає, що лише один APT використовує цю техніку, а червоний означає, що всі п’ять APT використовують цю техніку.

При цьому, потрібно приділяти більше значення кольору технік, оскільки він стає інтенсивнішим/темнішим.

Палітру кольорів можна налаштувати на свій смак і використовувати, щоб уникнути будь-якої плутанини у випадку переважно «червоного» або «зеленого» TTP.

У наведеному на рисунку 2.16 прикладі бал -1 (зелений колір) свідчить про те, що TTP є досить унікальним, не дуже поширеним між цими трьома групами APT, а бал -2 (жовтий колір) зустрічається принаймні у двох із цих Групи APT, які ми щойно нанесли на карту, і оцінка-3 (червоного кольору) є загальними для всіх трьох груп APT. Тепер можна експортувати теплову карту у форматі Json, Excel або SVG (рисунок 2.17) [34].

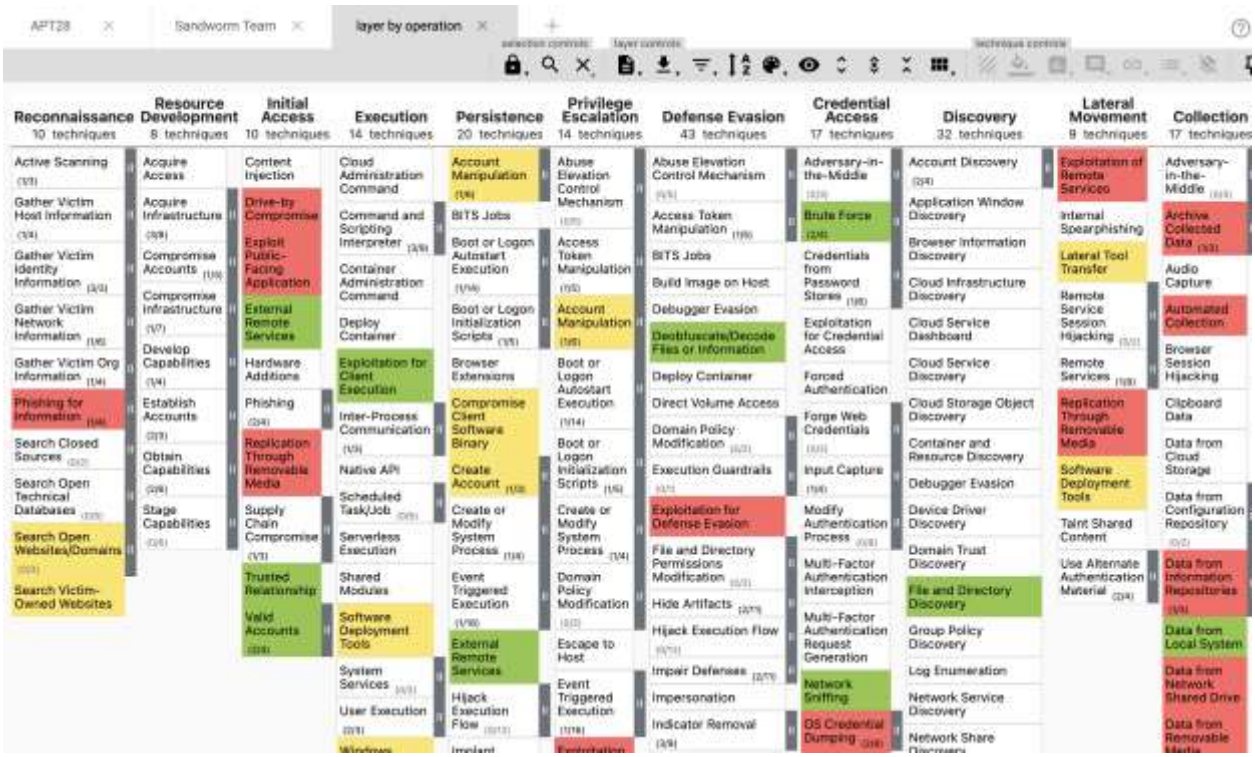


Рисунок 2.16 – Теплова карта виявлення загроз

Теплову карту можна використовувати для вирішення таких задач:

– Які TTP вже достатньо охоплені джерелами даних, які ви вже використовуєте та відстежуєте?

– Які TTP недостатньо охоплені та які джерела даних потрібні для вирішення цієї проблеми?

– Яким джерелам даних слід віддати пріоритет для підключення до середовища моніторингу безпеки?

– Чи можу я охопити той самий TTP меншою кількістю джерел даних, щоб зменшити зусилля з обслуговування, обсяги журналів, а також показники хибно-позитивних результатів?

Однак, необхідно пам’ятати про наступні обмеження будь-якого підходу на основі MITRE ATT&CK.

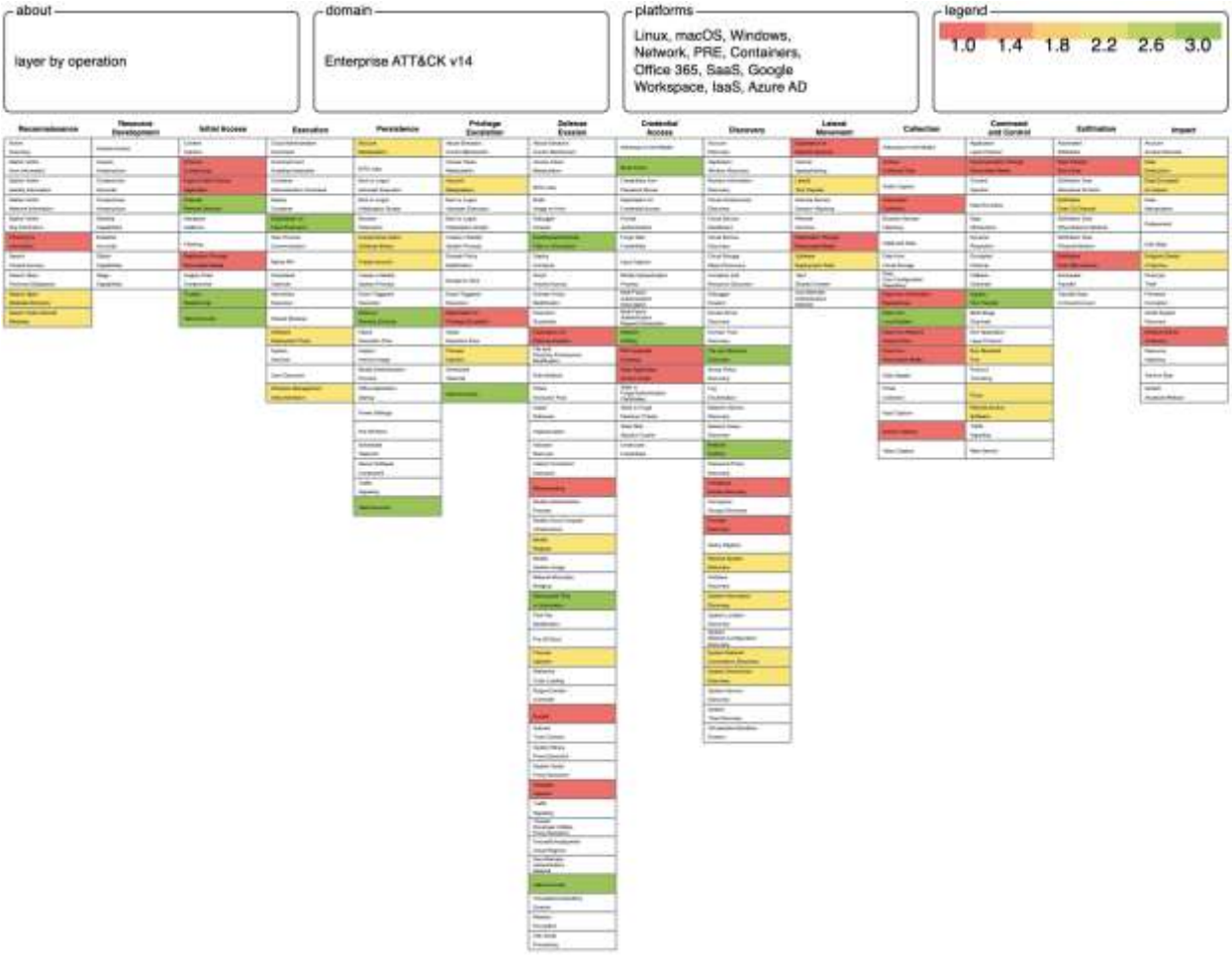


Рисунок 2.17 – Теплова карта виявлення загроз у форматі SVG

Фреймворк є чудовим ресурсом, але він може відобразити лише те, що було спостережено або виявлено.

Фахівці мають думати про всі потенційні загрози, з якими стикається організація, і про всі джерела даних, які зараз використовуються для їх виявлення, для того щоб мати повну картину. Це не одноразова вправа її доведеться робити в ітераціях і періодично.

3 РОЗРОБКА ТА ДОСЛІДЖЕННЯ МЕХАНІЗМУ ВИЯВЛЕННЯ ЗАГРОЗ

3.1 Алгоритм використання MITRE ATT&CK у центрі безпеки операцій

Використання MITRE ATT&CK у Центрі операцій безпеки (Security Operations Center, SOC) може значно розширити можливості виявлення загроз і реагування на них. Алгоритм ефективного використання фреймворку MITER ATT&CK у SOC складається з наступних кроків.

1. Ознайомлення з MITRE ATT&CK.

– Зрозумійте призначення та структуру MITER ATT&CK.

– Ознайомтеся з веб-сайтом ATT&CK (https://attack.mitre.org/) і перегляньте матрицю, техніку, тактику та підтехніки ATT&CK.

2. Зіставлення ATT&CK із вашим середовищем.

– Визначте відповідні методи й тактики MITER ATT&CK, які відповідають інфраструктурі, програмам і даним вашої організації.

– Зіставлення методів MITRE ATT&CK із наявними засобами безпеки, такими як брандмауери, системи виявлення вторгнень і рішення для захисту кінцевих точок.

3. Створення правил виявлення.

– Розробіть правила виявлення та випадки використання на основі конкретних методів і тактик MITRE ATT&CK.

– Використання системи управління інформацією про безпеку та подіями (SIEM) або платформи аналізу загроз, щоб створити правила, які запускатимуть сповіщення, коли виявлено підозрілу діяльність, пов’язану з певними методами ATT&CK.

4. Впровадження полювання на загрози.

– Використовуйте MITRE ATT&CK як керівництво для про активних навчань з пошуку загроз.

– Шукайте індикатори компрометації (IOC), пов’язані з відомими методами ATT&CK, і використовуйте їх для визначення потенційних загроз у вашому середовищі.

5. Покращення реагування на інциденти.

– Включіть MITRE ATT&CK у свої процедури реагування на інциденти.

– Розробіть посібники та плани реагування, які відповідають конкретним технікам і тактикам ATT&CK, щоб ефективно справлятися з загрозами та пом’якшувати їх.

6. Співпрацюйте з Threat Intelligence.

– Використовуйте зовнішні джерела розвідки про загрози, які відповідають MITER ATT&CK.

– Будьте в курсі останніх звітів про загрози, у яких згадуються методи й тактики ATT&CK.

Алгоритм використання MITRE ATT&CK складається з наступних кроків.

Крок 1: Пошук.

Знайдіть тактику, техніку, підтехніку або ID.

Приклад: заплановане завдання/робота: заплановане завдання.

ID: T1053.005.

Допоміжна техніка: T1053.

Тактика: виконання, наполегливість, підвищення привілеїв.

Крок 2: Вивчення знайденого.

Зрозумійте ATT&CK.

Ознайомтеся із загальною структурою ATT&CK.

Знайдіть спосіб поведінки зловмисника.

Знайдіть параметри та інструменти, які зловмисник повинен використовувати для впровадження ATT&CK.

Вивчіть поведінку / інструменти.

Шукайте техніку або підтехніку на інших ресурсах.

Дізнайтеся, як групи використовують техніку або підтехніку.

Крок 3. Виявлення зловмисника.

Знайдіть пом'якшення.

Крок 4. Перетворення TTP на правило використання SIEM.

Знайдіть правило виявлення в проекті MITER CAR.

Приклад: заплановане створення завдання, що містить підозрілі сценарії.

Джерела даних. Визначити техніку або підтехніку можна на основі наявного джерела даних, наприклад реєстру Windows або мережевого трафіку.

Приклади.

Моніторинг процесів і командного рядка процесів.

Sysmon часто збирає журнали подій Windows.

Команда, джерело даних DS0017 | MITRE ATT&CK®.

Моніторинг реєстру. Ієрархічна база даних ОС Windows, яка зберігає велику частину інформації та параметрів програмного забезпечення.

Реєстр Windows, джерело даних DS0024 | MITRE ATT&CK®.

Мережевий трафік. Наприклад отримання інформації про сокет із IP-адресою джерела/одержувача та портом(ами) (наприклад, Windows EID 5156, Sysmon EID 3 або Zeek conn.log).

Навігатор ATT&CK. Навігатор ATT&CK це веб-інструмент для дослідження матриць ATT&CK. Його можна використовувати для візуалізації захисного покриття, планування червоно-синіх команд, частоти виявлених прийомів тощо.

3.2 Механізм захисту на основі інформації про загрози

Глибоке розуміння та використання структури MITER ATT&CK дозволяє перетворити стратегію кібербезпеки з реактивної на проактивну.

На рисунку 3.1 показано взаємозв’язок IOC, IOA та TTP. IOC допомагають у розслідуванні інцидентів, IOA допомагають у виявленні загроз у режимі реального часу, а TTP допомагають у проактивному розумінні підходу супротивника до покращення захисту.

Рисунок 3.1 – Взаємодія IOC, IOA та TTP

Розуміння цих відмінностей має вирішальне значення для визначення пріоритетів ресурсів у SOC. Чітко розмежувавши ролі TTP, IOC та IOA у структурі MITER ATT&CK, команди з кібербезпеки можуть оптимізувати свої операції з пошуку загроз, розвідки та виявлення (рисунок 3.2).

Полювання на загрози: визначте пріоритетність TTP. Глибоке розуміння поведінки супротивника дозволяє проактивно ідентифікувати потенційні загрози до того, як вони проявляться як IOC або IOA.

Інтелектуальні дані про загрози: IOC є цінними тут. Збір і аналіз IOC може призвести до більш ефективних контрзаходів і оборонної тактики.

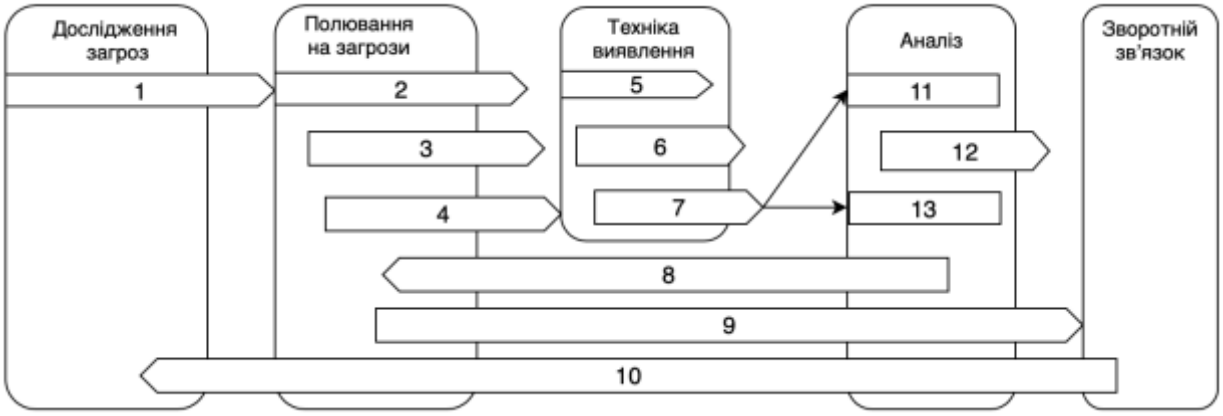


Рисунок 3.2 – Робочий процес кібероперацій:

1 – Дослідження ідентифікують новий TTP;

2 – Hunter оцінює релевантність TTP для клієнтської бази;

3 – Hunter визначає чи є TTP прийнятним правилом полювання;

4 – Знайдена інформація повідомляє про змінні правила та рівень специфічності;

5 – Генерується правило;

6 – Правило генерується та розгорнуто;

7 – Правило виявлення загроз;

8 – Hunter досліджує сповіщення та полює на активність, щоб визначити зараження;

9 – Інформація аналізується та повідомляється клієнту;

10 – Вся додаткова інформація та відгуки про вдосконалення правил повертаються в робочий процес для покращення можливостей виявлення та процесу пошуку;

11 – Помилкові спрацювання;

12 – Як удосконалити правило, щоб зменшити помилкові спрацювання?

13 – Правильні спрацювання.

Техніка виявлення: фокус на IOA. Системи виявлення в реальному часі повинні бути спрямовані на відловлювання атак у міру їх виникнення, вимагаючи акценту на IOA.

Використання комплексної матриці інфраструктури в поєднанні з цими ключовими індикаторами дозволяє створити більш цілеспрямовану та ефективну стратегію безпеки. Це не тільки оптимізує розподіл ресурсів, але й посилює заходи безпеки організації, безпосередньо узгоджуючи з фінансовими гарантіями.

Інвентаризація активів. Перш ніж занурюватися в конкретні тактики та прийоми, важливо провести ретельний опис усіх активів. Це має охоплювати як цифрові, так і фізичні активи, починаючи від локальних мереж і хмарних систем до мережевих засобів контролю фізичного доступу, таких як зчитувачі карток-ключів. Централізувавши ці різноманітні точки даних у системі безпеки та керування подіями (SIEM), команда з кібербезпеки отримує більш повне уявлення для посилення захисту.

Моделювання загроз. Адаптація матриці ATT&CK для відображення унікального ландшафту організації є ключовим кроком у оптимізації пошуку загроз. Отримавши повне розуміння ландшафту своїх активів, можна визначити, які елементи матриці ATT&CK є найбільш актуальними для вашої організації. Такий підхід дозволяє ефективно зосередити ваші ресурси, сприяючи точнішому виявленню загроз і швидшому реагуванню на інциденти. Як ми побачимо в наведених нижче прикладах, правильне налаштування може значно покращити захисну позицію вашої організації.

Приклад 1. Внутрішні загрози. Внутрішні загрози можуть бути як відкритими, так і непомітними. Розглянемо сценарій, коли журнали доступу до картки-ключа інтегровані в систему управління інформацією про безпеку та подіями (SIEM) компанії, наприклад Splunk ES.

Джерела даних: журнали доступу до ключових карток у SIEM, можливо, пов’язані з іншими даними, наприклад журналами мережевої активності.

Запити індикаторів: відхилення від звичайних шаблонів доступу, наприклад доступ до зон обмеженого доступу або використання поза стандартними годинами.

Аналіз. Необхідно порівнювати ці відхилення з іншими аномальними діями. Наприклад, використання картки-ключа у неробочий час із раптовим сплеском передачі даних може свідчити про інцидент безпеки.

Покрокове керівництво сценарієм: під час пошуку потенційних інсайдерських загроз можливим першим кроком є ретельна перевірка журналів автентифікації користувачів і даних фізичного доступу. Це, звичайно, припускає, що платформа SIEM вашої організації налаштована на прийом журналів доступу до картки-ключа на додаток до стандартних подій входу. Ці джерела даних забезпечують багатовимірне уявлення про поведінку користувачів, збагачуючи тим самим аналітичний контекст для виявлення потенційних загроз.

У Splunk ES можна почати з пошуку в таблиці активності входу та виходу користувача, а також результатів цих спроб, незалежно від того, були вони успішними чи невдалими. Кілька невдалих спроб доступу є сигналом, який вимагає подальшого дослідження.

```
index="keycard_logs" sourcetype="keycard_access"
| table user, time_in, time_out, result
| sort 0 time_in
```

Налаштуємо базові критерії пошуку відповідно до організаційної схеми, вказавши відповідний індекс і параметри типу джерела. Метою є виявити аномалії в моделях доступу користувачів. Незважаючи на те, що більшість персоналу демонструє передбачувану поведінку, яка характеризується постійними часовими мітками та місцями прибуття та виходу, відхилення від цих норм слід досліджувати додатково.

Для більш розширеного рівня перевірки необхідно використовувати функцій eventstats і eval у SPL, щоб ізолювати події, які виходять за межі діапазону двох стандартних відхилень від середнього значення, таким чином потенційно вказуючи на аномальну діяльність.

```
| eventstats avg(src_count) as avg stdev(src_count) as
stdev by user
| eval upperBound=avg+stdev*2
| where src_count>upperBound
```

Переглянемо наступні журнали доступу на прикладі компанії.

```
Mon Sep 4 12:15:44 EmployeeID=237 CardReaderID=101
Access=GRANTED
Mon Sep 4 08:11:02 EmployeeID=919 CardReaderID=203
Access=GRANTED
Mon Sep 4 12:20:33 EmployeeID=919 CardReaderID=203
Access=GRANTED
Mon Sep 4 08:20:55 EmployeeID=415 CardReaderID=305
Access=GRANTED
Mon Sep 4 12:38:41 EmployeeID=415 CardReaderID=305
Access=GRANTED
Mon Sep 4 21:02:26 EmployeeID=415 CardReaderID=101
Access=DENIED
Tue Sep 5 08:03:26 EmployeeID=237 CardReaderID=101
Access=GRANTED
Tue Sep 5 12:18:52 EmployeeID=237 CardReaderID=101
Access=GRANTED
Tue Sep 5 08:05:37 EmployeeID=919 CardReaderID=203
Access=GRANTED
```

Несанкціонована спроба співробітника 415 отримати доступ до пристрою зчитування карток 101 у неробочий час викликає відмову в доступі. Це вимагає негайної перевірки з кількох причин. По-перше, типова схема взаємодії співробітника переважно з пристроєм зчитування карток 305, що вказує на незвичайну поведінку доступу. По-друге, ми бачимо позначку часу спроби доступу о 21:02, а інші журнали вказують на типову активність близько 8:00 ранку та знову близько 12:00 вечора. Діяльність співробітника 415 значно виходить за межі стандартного оперативного вікна, що є аномалією, яка вимагає додаткової уваги. Нарешті, журнали подій «доступ заборонено» підтверджують твердження, що це була спроба несанкціонованого доступу.

На цьому етапі називати Співробітника 415 інсайдерською загрозою було б передчасно. Аномальна подія також може означати скомпрометовану картку-ключ. Мисливцю за загрозами, наступним логічним кроком буде співвіднести ці дані із мережевими журналами та подіями аналізу поведінки користувачів (UBA) для більш повної оцінки загроз.

Техніка MITRE ATT&CK. T1200: Додаткове обладнання.

Зловмисники можуть вводити комп'ютерні аксесуари, мережеве обладнання чи інші комп'ютерні пристрої в систему чи мережу, які можна використовувати як вектор для отримання доступу. Замість того, щоб просто підключати та розподіляти корисні дані через знімне сховище (тобто реплікацію через знімний носій), можна використовувати більш надійні апаратні додатки для введення нових функціональних можливостей та/або функцій у систему, якими потім можна зловживати.

T1091: Реплікація через знімний носій. Зловмисники можуть проникати в системи, можливо, у відключених або бездротових мережах, копіюючи зловмисне програмне забезпечення на знімний носій і користуючись перевагами функцій автозапуску, коли носій вставляється в систему та виконується. У випадку бічного переміщення це може статися через модифікацію виконуваних файлів, що зберігаються на знімному носії, або шляхом копіювання зловмисного програмного забезпечення та перейменування його так, щоб воно виглядало як законний файл, щоб обманом змусити користувачів виконати його в окремій системі. У випадку початкового доступу це може статися через ручну маніпуляцію носієм, модифікацію систем, які використовуються для початкового форматування носія, або зміну мікропрограми самого носія.

T1199: Довірені стосунки. Зловмисники можуть зламати або іншим чином використовувати організації, які мають доступ до передбачуваних жертв. Доступ через стосунки довіреної третьої сторони зловживає існуючим з'єднанням, яке може бути незахищеним або піддається меншій перевірці, ніж стандартні механізми отримання доступу до мережі.

T1078: Дійсні облікові записи. Зловмисники можуть отримати облікові дані наявних облікових записів і зловживати ними як засіб отримання початкового доступу, постійності, ескалації привілеїв або ухилення від захисту. Зламані облікові дані можуть використовуватися для обходу контролю доступу, розміщеного на різних ресурсах систем у мережі, і навіть можуть використовуватися для постійного доступу до віддалених систем і зовнішніх доступних служб, таких як VPN, Outlook Web Access, мережеві пристрої та віддалений робочий стіл. Скомпрометовані облікові дані також можуть надати зловмиснику підвищені привілеї до певних систем або отримати доступ до обмежених зон мережі. Зловмисники можуть не використовувати зловмисне програмне забезпечення чи інструменти разом із законним доступом, який надають ці облікові дані, щоб ускладнити виявлення їх присутності.

Враховуючи незвичайну поведінку співробітника 415, комплексний аналіз загроз повинен не лише враховувати мережеві журнали та журнали UBA, але й зіставляти ці події з відомими тактиками та техніками атак, як зазначено в матриці MITRE ATT&CK. Це забезпечить більш надійну структуру для розуміння потенційних ризиків, пов’язаних із цим, і спрямує розробку наступних стратегій полювання на загрози.

Приклад 2: Тактика виявлення та перерахування. Відкриття та підрахунок є додатковими векторами, які потребують пильного моніторингу. Це трапляється, коли зловмисник уже зламав початковий захист і активно досліджує мережу на наявність нових вразливостей і конфіденційних даних.

Джерела даних: системний журнал, журнали подій Windows і журнали NetFlow.

Запити індикаторів: незвичайне використання власних утиліт ОС, таких як ipconfig і systeminfo, або команд, які запитують системні або мережеві ресурси, особливо якщо вони виконуються у швидкій послідовності або в непарні години.

Аналіз: Контекстуалізуйте кожну підозрілу діяльність, щоб визначити, чи є вона доброякісною дією чи вимагає подальшої ескалації.

Покрокове керівництво сценарієм: у корпоративних умовах для стандартних користувачів дуже незвично перераховувати адміністративні спільні ресурси на робочих станціях або серверах. Таким чином, пошук будь-якого екземпляра, який Sysmon генерує ідентифікатор події 1 (узгоджено з подією безпеки Windows 4688), який позначає net.exe для зіставлення спільних ресурсів адміністратора з робочої станції на рівні користувача, буде добрим місцем для початку.

```
index=sysmon sourcetype="WinEventLog:Microsoft-Windows-
Sysmon/Operational" EventCode=1 Image="*\\net.exe"
```

Звідси можна визначити будь-які потенційні червоні прапорці в мережі.

```
2023-09-03T08:00:01Z Hostname=WKSTN01 EventID=1
Image=C:\Windows\System32\notepad.exe User=Bob
2023-09-03T09:30:44Z Hostname=WKSTN02 EventID=1
Image=C:\Program Files\Outlook\Outlook.exe User=Alice
2023-09-03T09:45:11Z Hostname=WKSTN01 EventID=1
Image=C:\Windows\System32\winword.exe User=Bob
2023-09-04T04:15:33Z Hostname=WKSTN03 EventID=1
Image=C:\Windows\System32\net.exe User=Yan
CommandLine="net use z: \server\adminshare"
2023-09-04T10:15:22Z Hostname=WKSTN01 EventID=1
Image=C:\Program
Files\Google\Chrome\Application\chrome.exe User=Bob
2023-09-04T10:45:01Z Hostname=WKSTN02 EventID=1
Image=C:\Windows\System32\excel.exe User= Alice
2023-09-04T15:30:11Z Hostname=WKSTN03 EventID=1
Image=C:\Program Files\Adobe\Acrobat Reader
DC\Reader\AcroRd32.exe User=Yan
```

У даному прикладі журналу користувач Yan використовує команду net.exe з робочої станції WKSTN03, щоб зіставити адміністративний спільний ресурс (\\server\\adminshare). Як правило, адміністративне відображення спільних ресурсів – це діяльність, обмежена користувачами

рівня адміністратора; стандартним користувачам, таким як Yan, незвично ініціювати такі дії.

Крім того, ці спільні ресурси часто містять конфіденційні дані, наприклад файли конфігурації, які мають бути недоступні для звичайних користувачів. Початкова точка, яка є робочою станцією, а не сервером, додає ще один рівень підозри. Схоже, що ця діяльність порушує принцип найменших привілеїв і може свідчити про розвідку, неавторизований доступ або компрометацію облікового запису.

Іншим важливим журналом для моніторингу є ідентифікатор події 4648, який генерується, коли зловмисник використовує явні облікові дані для відображення спільного доступу до мережі. Ця подія дає безцінне уявлення не лише про IP-адресу призначення та ім’я хоста, але й про оригінальні та переключені дані облікового запису. Розвідувальні дані, зібрані під час цієї події, служать для підтвердження висновків, отриманих під час попередніх подій.

```
EventID: 4648
Time: 2023-09-04 08:45:00
Host: Workstation001
Destination_IP: 192.168.1.5
Original_Account: JaneDoe
Switched_Account: ServiceAccount

EventID: 4648
Time: 2023-09-04 09:05:00
Host: Workstation001
Destination_IP: 192.168.1.10
Original_Account: JohnDoe
Switched_Account: ServiceAccount
```

```
EventID: 4648
Time: 2023-09-04 03:25:00
Host: Workstation001
Destination_IP: 192.168.2.20
Original_Account: JimBob
Switched_Account: AdminAccount
```

У цьому випадку журнали виявляють, що діяльність облікового запису Джимбоба відбувається в ненормальний час – зокрема, о 3:25 ранку. З огляду на те, що JimBob призначено як стандартний користувач із обмеженим доступом до мережі, використання облікового запису AdminAccount для цих дій значно підвищує рівень підозри.

Діяльність Jima може вказувати на потенційну розвідку, несанкціоноване проникнення або зламаний обліковий запис. Деякі техніки MITRE ATT&CK, на які варто звернути увагу:

Техніка MITRE ATT&CK. T1087: виявлення облікового запису.

Зловмисники можуть спробувати отримати список дійсних облікових записів, імен користувачів або адрес електронної пошти в системі або в скомпрометованому середовищі. Ця інформація може допомогти зловмисникам визначити, які облікові записи існують, що може допомогти в подальшій поведінці, як-от підбір, фішингові атаки або захоплення облікових записів (наприклад, дійсні облікові записи).

T1083: Виявлення файлів і каталогів. Зловмисники можуть перераховувати файли та каталоги або шукати певну інформацію у файловій системі в певних місцях на хості чи мережевому ресурсі. Зловмисники можуть використовувати інформацію з виявлення файлів і каталогів під час автоматичного виявлення, щоб формувати подальшу поведінку, включно з тим, чи зловмисник повністю заражає ціль і/або намагається виконати певні дії.

T1135: виявлення спільного доступу до мережі. Зловмисники можуть шукати спільні папки та диски на віддалених системах як засіб ідентифікації джерел інформації для збору в якості попередника для збору та визначення

потенційних систем, що представляють інтерес для бокового руху. Мережі часто містять спільні мережеві диски та папки, які дають користувачам доступ до файлових каталогів у різних системах мережі.

T1069: Виявлення груп дозволів. Зловмисники можуть спробувати виявити параметри груп і дозволів. Ця інформація може допомогти зловмисникам визначити, які облікові записи користувачів і групи доступні, членство користувачів у певних групах і які користувачі та групи мають підвищені дозволи.

Роль як мисливців за загрозами полягає у виявленні відхилень, які порушують принцип найменших привілеїв, особливо коли вони збігаються з додатковими ознаками компрометації, такими як нетипові часові рамки та зловживання привілеями облікового запису. Негайні наступні кроки мають включати співвіднесення цих висновків із додатковими даними журналу, глибоке занурення в аналітику поведінки користувачів (UBA) Боба та розгляд питання про початок комплексної судово-медичної експертизи.

Приклад 3: Виявлення та пом’якшення викрадання DNS.

Оскільки DNS-запити є плідними та нормальними, ця форма викрадання даних може залишитися непоміченою неправильно налаштованими рішеннями DLP. Це техніка, яка може бути дуже небезпечною для організації, яка хоче захистити свої конфіденційні дані.

Джерела даних: журнали DNS-сервера, дані захоплення пакетів і журнали брандмауера.

Запити-індикатори: висока частота DNS-запитів, надзвичайно великі текстові записи DNS або запити до доменів, які, як відомо, містять фішингові сайти.

Аналіз: шукайте закономірності чи кореляції в запитах DNS, які можуть вказувати на те, що дані перекачуються. Звертайте пильну увагу на «субдомени», які запитуються, оскільки це часто може бути ключовим показником.

Покрокове керівництво сценарієм: мета – завчасно виявляти потенційне викрадання даних через DNS-запити, вектор атаки, яким часто не помічають. Ви захочете ретельно перевірити журнали DNS на наявність аномалій, які можуть свідчити про неавторизовану передачу даних. Метою є раннє виявлення та пом'якшення потенційних інцидентів безпеки.

Для цього вам потрібно буде перевірити журнали DNS і виявити аномальну активність, обчисливши ентропію пакетів DNS і знайшовши викиди. Перш ніж це станеться, вам потрібно знати, що є «нормальним». Обчислення «нормальної» ентропії в контексті DNS-запитів може бути складним, оскільки те, що вважається нормальним, може відрізнятися в різних організаціях та їх мережевому трафіку. Тому першим кроком буде обчислення «нормального» діапазону ентропії за допомогою функцій eval і stats. Нижче наведено приклад того, як це можна зробити, припускаючи, що «нормальний» знаходиться в межах 2 стандартних відхилень.

```
| eval baseline_entropy=entropy(query)
| stats avg(baseline_entropy) as avg_baseline_entropy,
stdev(baseline_entropy) as stdev_baseline_entropy
| eval upper_threshold=avg_baseline_entropy + (2 *
stdev_baseline_entropy)
| eval lower_threshold=avg_baseline_entropy – (2 *
stdev_baseline_entropy)
```

Встановлюючи чисту базову лінію, важливо, щоб часові рамки введених даних припали на період, коли є висока впевненість, що зловмисна діяльність не відбувалася.

Після встановлення базового рівня можна почати шукати аномальну активність, шукаючи журнали DNS із ентропією, більшою за верхній поріг базового рівня.

Розмір пакета та ентропія є основними індикаторами компрометації під час ретельного вивчення потенційної фільтрації DNS.

Хоча максимальний розмір пакета DNS, надісланого через UDP, становить 512 байт, у більшості випадків DNS-запити зазвичай значно нижчі за це число. Розміри пакетів, які перевищують середні для вашої організації,

можуть свідчити про те, що ці пакети насправді можуть приховувати дані, які вивозяться порціями, а не прості запити DNS.

Високі значення ентропії, з іншого боку, вказують на рандомізовані або закодовані дані, поширений метод, який використовується для маскування конфіденційної інформації під час ексфільтрації. Обидва показники виходять за межі звичайного трафіку DNS і, якщо спостерігати разом, підвищують ймовірність того, що відбувається викрадання даних. Таким чином, моніторинг цих показників має бути важливим компонентом будь-якої ініціативи по пошуку загроз, спрямованої на витоки даних на основі DNS.

У разі виявлення незвичних розмірів пакетів DNS і високого рівня ентропії в запитах DNS, особливо щодо підозрілої URL-адреси, необхідно негайно вжити заходів для подальшого дослідження аномалій. Це можуть бути показники складної техніки атаки, як-от вилучення даних через DNS, узгоджене з протоколами TTP MITRE ATT&CK, такими як Exfiltration Over Alternative Protocol (T1048) і Data Encoding (T1132).

Наступні кроки мають включати такі дії. Аналіз кореляції: перехресне посилання на аномальну активність DNS з іншими журналами (наприклад, брандмауер, проксі, системний журнал, мережевий потік), щоб визначити будь-які шаблони або корельовані дії для вихідних користувачів і хостів.

Аналітика поведінки користувачів (UBA): необхідно уважно вивчити аналітику поведінки, щоб зрозуміти, чи залучений обліковий запис має інші ознаки підозрілої поведінки, наприклад невдалі спроби входу або незвичні шаблони доступу до даних.

Аналіз кінцевих точок: перевірте задіяні кінцеві точки на наявність ознак зловмисного або неавторизованого встановлення програмного забезпечення, яке може сприяти викраденню.

Канали аналізу загроз: перехресно перевірте підозрілі домени на канали аналізу загроз, щоб визначити, чи є вони відомими шкідливими доменами.

Було б доцільно також запустити процес реагування на інциденти (IR) вашої організації, а також ізолювати уражені системи від мережі, щоб запобігти подальшій втраті даних. Завжди ретельно документуйте всі висновки, вжиті дії та внесені зміни для перевірки керівниками та вдосконалення майбутніх операцій пошуку загроз.

Важливість комунікації: переклад мовою зацікавлених сторін. Здатність ефективно спілкуватися особливо важлива для команд з кібербезпеки під час спілкування із зацікавленими сторонами, оскільки ці команди відіграють ключову роль у захисті організації від значних фінансових втрат.

Нещодавнє дослідження показало, що середня вартість витоку даних зараз становить близько 4,45 мільйона доларів США, що підкреслює фінансовий вплив інцидентів безпеки.

Рамкова програма MITER ATT&CK представляє структурований підхід, який може бути неоціненним у сприянні змістовному діалогу із зацікавленими сторонами. Команди з кібербезпеки можуть надати відчутні докази відомої поведінки зловмисників, посилаючись на структуру та визначаючи потенційні вразливості, характерні для організації. Це дає їм змогу зображати сценарії загроз у чіткій, дієвій формі, дозволяючи зацікавленим сторонам зрозуміти важливість запроваджених заходів безпеки та необхідних інвестицій.

Чітке формулювання того, як ініціативи з кібербезпеки можуть запобігти або пом’якшити ці дорогі інциденти, приверне більше уваги тих, хто контролює бюджети та ресурси.

Зрозуміло, що MITER ATT&CK є важливим ресурсом, який має унікальну можливість пропонувати стратегічну інформацію для полювання на загрози. Досліджено тонкі відмінності між TTP, IOC та IOA, підкреслюючи при цьому важливу роль, яку кожен відіграє в посиленні ініціатив у сфері кібербезпеки.

Ключовий висновок у майбутньому полягає не лише в застосуванні MITER ATT&CK Framework, а й у визначенні пріоритетів для унікального ландшафту загроз організації. Правильно реалізована структура не тільки підвищить безпеку, але й сприятиме загальному фінансовому здоров'ю та стійкості організації.

3.3 Визначення пріоритетності вразливостей з урахуванням загроз

Враховуючи складність сучасних IT-середовищ, а також кількість і різноманітність базових систем, виправити кожну вразливість неможливо. Замість цього захисники повинні визначити та визначити пріоритети найбільш критичних вразливостей для своїх організацій.

Що стосується керування вразливостями та встановлення пріоритетів, загальну систему оцінки вразливостей (CVSS) FIRST і систему оцінки прогнозування експлойтів (EPSS) можна поєднати, щоб зробити пріоритетність уразливостей значно легшою.

Оцінка показників за допомогою CVSS. Підходячи до завдань, таких як визначення пріоритетів уразливості та керування нею, захисники знайомі з CVSS, який вперше був опублікований як міжнародний стандарт у 2005 році. Його мета полягає в тому, щоб охопити основні характеристики вразливості та отримати оцінку для відображення потенційної серйозності вразливості. шкода організації, якщо вона буде використана.

Оцінка CVSS складається з трьох компонентів:

1. Базовий бал, який представляє статичні характеристики вразливості. Часовий аспект, який включає фактори, що залежать від часу, такі як статус експлуатації та доступність виправлень.

Екологічний компонент, який відображає специфічні для організації властивості мережі.

Метрики базової оцінки стали найпоширенішим компонентом CVSS. Це призвело до помилкового уявлення про те, що базові бали охоплюють всю оцінку ризику, незважаючи на те, що базові показники стосуються лише деяких аспектів ризику, таких як можливість використання вразливості та її серйозність.

На жаль, якщо ви подивитеся лише на базові показники CVSS як на орієнтир, які вразливості потрібно усунути, ви знайдете справді величезну кількість «критичних» вразливостей. З 2213 опублікованих за останні 30 днів 1167 або трохи більше половини отримали оцінку 7 або вище з 9 згідно з CVE Details. Це залишає захисників питання: «Як я можу впоратися з такою кількістю критичних вразливостей?»

Прогнозування експлойту. Коли захисники визначають пріоритетність вразливостей, використовуючи лише базову оцінку, вони можуть нехтувати іншими значущими факторами, оскільки це не обов'язково є точним прогнозом реальних загроз. Визначаючи, які вразливості є найбільш актуальними, необхідно враховувати й інші фактори, наприклад, ймовірність використання загрози «в дикій природі», тому FIRST розробила EPSS.

EPSS – це система оцінки вразливостей, спеціально розроблена для оцінки ймовірності використання вразливості. Щоб досягти цього, EPSS збирає опубліковані дані про експлойти з різних джерел, включаючи системи IDS/IPS, агенти на базі хостів і опублікований код експлойтів зі сховищ (наприклад, Exploit-DB і Metasploit). Вона включає інформацію, як-от характеристики вразливості з цих даних. Результати структуровані у вигляді таблиці: рядки = уразливості; стовпці = відповідні атрибути, такі як історія експлуатації.

Методи статистичного аналізу, регресії або машинного навчання можуть використовувати цю інформацію для розрахунку ймовірності використання вразливості протягом наступних 30 днів. Поєднуючи результати CVSS і EPSS, захисники можуть звузити свою увагу до вразливостей високого ступеня серйозності, які, з високою ймовірністю,

будуть використані протягом наступних 30 днів. З 2217 CVE, опублікованих за останні 30 днів, лише 32 мають показник EPSS понад 1%.

Розуміння впливу. Після того, як захисник скоротить список із потенційно тисяч вразливостей, визначивши пріоритети за допомогою CVSS, а потім ще більше скоротить його, визначивши пріоритети за оцінкою EPSS, результат стане набагато керованішим. Наступним кроком є встановлення потенційних наслідків використаної вразливості.

Підхід до оцінки впливу на основі інформації про загрози надає захисникам інформацію, яку вони можуть використати для відповіді на запитання: «Що може зробити супротивник, скориставшись цією вразливістю?» MITER ATT&CK®, база знань про відомі тактики та прийоми супротивника, засновані на розвідці загроз, широко використовується як загальний словник для опису поведінки супротивника та забезпечення скоординованих оборонних стратегій на основі цих конкретних поведінок. Якщо вразливість використовується, ATT&CK може допомогти захисникам зрозуміти конкретну поведінку супротивника (описується як «техніки ATT&CK»), які супротивник може використати далі. Вона не тільки пропонує глибоке розуміння методів, але й пов’язує ці методи з пом’якшенням, яке може допомогти підходу до глибокого захисту.

Подолання розриву між CVE та ATT&CK. Проект зіставлення ATT&CK з CVE визначає методологію використання ATT&CK для характеристики потенційного впливу вразливостей, що дозволяє захисникам пов’язувати методи та властивості, змодельовані в ATT&CK, із уразливими місцями, переліченими в CVE. Це відображення дає змогу фахівцям із безпеки краще зрозуміти потенційну загрозу, пов’язану з конкретними вразливими місцями, і допомагає розробити стратегії пом’якшення. Завдяки систематичному та стандартизованому підходу проект покращує загальне розуміння того, як уразливості пов’язані з тактикою та технікою противника, задокументованими в ATT&CK (рисунок 3.3).

Рисунок 3.3 –Опис впливу вразливості методами ATT&CK

Однак застосування цієї методології для розуміння впливу вразливості потребує дорогоцінного часу аналітика, тому найкраще зосередитися на вразливостях вищого ступеня серйозності, які, найімовірніше, будуть використані на основі балів CVSS і EPSS.

Відображення вразливості на ATT&CK показує, що вразливість у разі її використання може дозволити зловмиснику створити дійсний обліковий запис (T1136) у системі.

Перевірка T1136 показує кілька можливих пом’якшень, які можуть обмежити здатність зловмисника успішно створити обліковий запис і забезпечити надійний моніторинг нових облікових записів.

T1136 також посилається на підходи до виявлення потенційно зловмисної діяльності. Озброївшись цією інформацією, захисники можуть вжити обґрунтованих заходів у відповідь на вразливість або просто перейти до наступного, оскільки вони вже мають засоби пом’якшення, які будуть усунути вразливість, доки не буде доступне виправлення.

Не кожен захист заснований на виявленні, він також може бути профілактикою, налаштувавши мережу відповідно до стандартів.

ID техніки MITRE: T1190. Посилання: відкритий додаток Exploit, техніка T1190 – Enterprise | MITRE ATT&CK®

Наступним у черзі є спроба зловмисників скористатися слабкістю комп’ютера або програми, що виходить в Інтернет, за допомогою програмного забезпечення, даних або команд, щоб спричинити ненавмисну або непередбачену поведінку.

Недоліком у системі може бути збій, помилка або недолік конструкції. Ці програми, які часто приймають форму веб-сайтів, також можуть мати форму баз даних (наприклад, SQL), стандартних служб (наприклад, SMB або SSH), протоколів адміністрування та керування мережевими пристроями (наприклад, SNMP і Smart Install) і будь-яких інших програм. з відкритими сокетами, які можуть підключатися до Інтернету, як-от веб-сервери та пов’язані служби.

Якщо додаток розміщено в хмарній інфраструктурі та/або контейнеризовано, його використання може призвести до компрометації базового екземпляра або контейнера.

Ізоляція програми обмежить доступ цільового експлойта до інших процесів і компонентів системи.

Щоб запобігти потраплянню експлойт-трафіку до програми, можна використовувати брандмауери веб-програм, щоб обмежити доступ до програми.

Використовуйте DMZ або іншу архітектуру хостингу, щоб розділити сервери та служби, доступні із зовнішнього світу, від решти мережі.

Використовуючи найменші привілеї для облікових записів служби, можна обмежити доступ, який має експлуатований процес, до інших частин системи.

Регулярне керування виправленнями та підтримка актуального програмного забезпечення.

Планове сканування зовнішніх систем на наявність уразливостей і встановлення методів швидкого виправлення систем у разі виявлення серйозних уразливостей.

Пропоноване виявлення на основі MITRE приведено в таблиці 3.1

Таблиця 3.1 – Пропоноване виявлення на основі MITRE

Джерело даних	Виявлення
Журнал додатків (Application Log)	Виявлення використання програмного забезпечення може бути складним залежно від доступних інструментів. Програмні експлойти можуть не завжди бути успішними або можуть спричинити нестабільність або збій у зловживаному процесі. Брандмауери веб-додатків можуть виявляти неправильні вхідні дані під час спроби використання.
Мережевий трафік (Network Traffic)	Використовуйте глибоку перевірку пакетів, щоб шукати артефакти загального трафіку експлойтів, наприклад рядки впровадження SQL або відомі корисні навантаження.

Правила можливого виявлення загрози:

1. Назва: Кілька підозрілих кодів відповіді, спричинених одним клієнтом

Опис: Виявляє можливу активність або помилки у веб-програмі

```
Author: 'NoName'
Date: 11/15/2023
Tags:
Logsource: Web logs, IIS logs
Detection psuedo:
    HTTP Status codes: '400', '401', '403', '500'
    Timeframe: 10m
Condition: count() by client_ip > 10
Level: Medium
```

2. Назва: Викрадені дані простого HTTP POST

Опис: виявлення можливого викрадання даних методом простого HTTP POST.

```
Author: 'NoName'
Date: 11/15/2023
Tags:    Logsource: Web logs, IIS logs
Detection psuedo:
    HTTP Method: POST
Arguments/Commands(contains any): 'wermgr.exe',
```

```
'svchost.exe', 'name=\"proclist\"', 'ipconfig',
'name=\"sysinfo\"', 'et view'
    Condition: HTTP Method and Arguments
    Level: High
```

3. Назва: Підозрілий командний рядок за допомогою інструментів стиснення

Опис: Виявляє підозрілі аргументи командного рядка загальних даних compression tools.

```
    Author: NoName'
    Date: 11/15/2023
    Tags:
    Logsource: EDR process creation logs, Windows
Security process creation logs.
    Detection psuedo:
        OriginalFileName(contains any): '7z*.exe',
'*rar.exe', '*Command*Line*RAR*'
        CommandLine(contains any): '* -p*', '* -ta*',
'* -tb*', '* -sdel*', '* -dw*', '* -hp*'
    Condition: OriginalFileName and CommandLine
    BenignPositives: Any ParentImage that contains
'C:\Program*'
    Level: High
```

ВИСНОВКИ

В кваліфікаційній роботі розв’язано актуальну задачу підвищення ефективності виявлення загроз на основі фреймворка MITRE ATT&CK. При цьому отримано наступні результати.

1. Проведено аналіз вартості витоку даних спричинених кібератаками. Проаналізовано поширені типів атак та їх життєвий цикл.

2. Проведено аналіз існуючих підходів до виявлення кібератак та визначено основні етапи даного процесу, серед який виділено наступні: визначення мети полювання на загрозу, аналіз даних та виправлення і реакція на видалення загрози з системи.

3. Досліджено структуру фреймворку MITRE ATT&CK. Визначено переваги використання MITER ATT&CK для виявлення загроз.

4. Показано можливість та переваги використання навігатора MITER ATT&CK для візуалізації та покращення виявлення загроз.

5. Розроблено алгоритм використання MITRE ATT&CK у центрі операцій безпеки.

6. Розроблено підхід до визначення пріоритетності вразливостей з урахуванням загроз, який враховує систему оцінки вразливостей (CVSS) FIRST і систему оцінки прогнозування експлойтів (EPSS), що значно спрощує визначення пріоритетності вразливостей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cost of a Data Breach Report 2022. [Електронний ресурс]. - Режим доступу: https://www.ibm.com/downloads/cas/3R8N1DZJ

2. Microsoft Digital Defense Report 2022. [Електронний ресурс]. - Режим доступу:https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

3. Getting Started with ATT&CK: Threat Intelligence. [Електронний ресурс]. - Режим доступу: https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f

4. A. Georgiadou, S. Mouzakitis, and D. Askounis. Assessing MITRE ATT&CK risk using a cyber-security culture framework. Sensors, 2021, vol. 21, no. 9, p. 3267.

5. R. Al-Shaer, J. M. Spring, and E. Christou. Learning the associations of MITRE ATT&CK adversarial techniques. In 2020 IEEE Conference on Communications and Network Security (CNS). IEEE, 2020, pp. 1–9.

6. M. Parmar and A. Domingo. On the use of cyber threat intelligence (cti) in support of developing the commander's understanding of the adversary. In MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM). IEEE, 2019, pp. 1–6.

7. T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah. Cyber threat intelligence sharing: Survey and research directions, Computers & Security, 2019, vol. 87, p. 101589,.

8. D. Schlette, M. Caselli, and G. Pernul. A comparative study on cyber threat intelligence: The security incident response perspective. IEEE Communications Surveys & Tutorials, 2021, vol. 23, no. 4, pp. 2525–2556.

9. G. Cascavilla, D. A. Tamburri, and W.-J. Van Den Heuvel. Cyber- crime threat intelligence: A systematic multi-vocal literature review. Computers & Security, 2021, vol. 105, p. 102258.

10. A. Dutta and S. Kant. An overview of cyber threat intelligence platform and role of artificial intelligence and machine learning. In International Conference on Information Systems Security. Springer, 2020, pp. 81–86.

11. M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof. Cyber threat intelligence–issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 2018, vol. 10, no. 1, pp. 371–379.

12. V. Mavroeidis and S. Bromander. Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In 2017 European Intelligence and Security Informatics Conference (EISIC). IEEE, 2017, pp. 91–98.

13. Цаволик Т., Яцків В., Яцків Н., Івасьєв С. Виявлення недоліків у механізмах аутентифікації користувачів в SaaS-сервісах на основі MITRE ATT&CK. Вимірювальна та обчислювальна техніка в технологічних процесах. Технічні науки. – 2023. – С.16 – 22.

14. M. K. Ahn and J. R. Lee. Research on system architecture and methodology based on MITRE ATT&CK for experiment analysis on cyber warfare simulation. Journal of the Korea Society of Computer and Information, 2020, vol. 25, no. 8, pp. 31–37.

15. S. Hong, K. Kim, and T. Kim. The design and implementation of simulated threat generator based on MITRE ATT&CK for cyber warfare training. Journal of the Korea Institute of Military Science and Technology, 2019, vol. 22, no. 6, pp. 797–805.

16. A. Kuppa, L. Aouad, and N.-A. Le-Khac. Linking CVE's to MITRE ATT&CK techniques. in The 16th International Conference on Avail- ability, Reliability and Security, 2021, pp. 1–12.

17. N. Munaiah, A. Rahman, J. Pelletier, L. Williams, and A. Meneely. Characterizing attacker behavior in a cybersecurity penetration testing competition. In 2019 ACM/IEEE International Symposium on Empir- ical Software Engineering and Measurement (ESEM). IEEE, 2019, pp. 1–6.

18. W.Xiong, E.Legrand, O.Aberg, and R.Lagerstro, “Cybersecurity threat modeling based on the MITRE enterprise ATT&CK matrix,” Software and Systems Modeling, 2021, pp. 1–21.

19. K. Kim, F. A. Alfouzan, and H. Kim, “Cyber-attack scoring model based on the offensive cybersecurity framework,” Applied Sciences, 2021, vol. 11, no. 16, p. 7738.

20. S. Choi, J.-H. Yun, and B.-G. Min, “Probabilistic attack sequence generation and execution based on MITRE ATT&CK for ics datasets,” in Cyber Security Experimentation and Test Workshop, 2021, pp. 41– 48.

21. S. Arshad, M. Alam, S. Al-Kuwari, and M. H. A. Khan, “Attack specification language: Domain specific language for dynamic training in cyber range,” in 2021 IEEE Global Engineering Education Conference (EDUCON). IEEE, 2021, pp. 873–879.

22. S. Kriaa and Y. Chaabane, “SecKG: Leveraging attack detection and prediction using knowledge graphs,” in 2021 12th International Con- ference on Information and Communication Systems (ICICS). IEEE, 2021, pp. 112–119.

23. R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. G. Gourisetti, “Cyber threat dictionary using MITRE ATT&CK matrix and NIST cybersecurity framework mapping,” in 2020 Resilience Week (RWS). IEEE, 2020, pp. 106–112.

24. S. Bromander, M. Swimmer, M. Eian, G. Skjotskift, and F. Borg, “Modeling cyber threat intelligence.” in ICISSP, 2020, pp. 273–280.

25. V. Legoy, M. Caselli, C. Seifert, and A. Peter, “Automated retrieval of ATT&CK tactics and techniques for cyber threat reports,” arXiv preprint arXiv:2004.14322, 2020.

26. Y. Lakhdhar and S. Rekhis, “Machine learning based approach for the automated mapping of discovered vulnerabilities to adversial tactics,” in 2021 IEEE Security and Privacy Workshops (SPW). IEEE, 2021, pp. 309–317.

27. G. Lee, S. Shim, B. Cho, T. Kim, and K. Kim, “Fileless cyberattacks: Analysis and classification,” ETRI Journal, 2021, vol. 43, no. 2, pp. 332–343.

28. A. Oruc, A. Amro, and V. Gkioulos, “Assessing cyber risks of an INS using the MITRE ATT&CK framework,” Sensors, 2022, vol. 22, no. 22, p. 8745.

29. M. Mundt and H. Baier, “Towards mitigation of data exfiltration techniques using the MITRE ATT&CK framework,” in International Conference on Digital Forensics and Cyber Crime. Springer, 2022, pp. 139–158

30. O. Grigorescu, A. Nica, M. Dascalu, and R. Rughinis, “CVE2ATT&CK: BERT-based mapping of CVEs to MITRE ATT&CK techniques,” Algorithms, 2022, vol. 15, no. 9, p. 314.

31. MITRE ATT&CK® Navigator. [Електронний ресурс]. - Режим доступу: https://mitre-attack.github.io/attack-navigator/

32. ATT&CK Matrix for Enterprise. [Електронний ресурс]. - Режим доступу: https://attack.mitre.org/

33. Яцків Н.Г., Кметик В.В., Хотинський В.А. Візуалізація виявлення загроз з використанням MITRE ATT&CK NAVIGATOR. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ - 2023), Тернопіль, 2023. – С. 21-23.

34. Яцків Н.Г., Смірнов Д.С., Хотинський В.А. Алгоритм використання MITRE ATT&CK у центрі безпеки операцій. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2023. – С. 193-194.

ДОДАТОК А

Копії публікацій