НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО–НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2022 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Методи прискорення оцінки потенційної критичності інцидентів інформаційної безпеки

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи _ФБ-84_
(шифр групи)

Михайленко Олег Вадимович _____
(прізвище, ім'я, по батькові)

Керівник Барановський Олексій Миколайович _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

Рецензент Терещенко І.М _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2022 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«___»_____2022 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

_____ Михайленка Олега Вадимовича _____
(прізвище, ім'я, по батькові)

1. Тема роботи «Методи прискорення оцінки потенційної критичності інцидентів інформаційної безпеки», _____
_____
керівник роботи доцент кафедри інформаційної безпеки Барановський О.М., _____
_____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від « » _____ 2022 р. №

2. Термін подання здобувачем вищої освіти роботи 14 червня 2022 р.

3. Вихідні дані до роботи реалізований метод прискорення оцінки критичності _____
_____
_____

4. Зміст роботи: ознайомлення зі термінологією та теоретичними відомостями розслідування інцидентів, порівняння методів оцінки, реалізація перспективного методу, проведення повноцінного розслідування та аналізу інциденту, апробація методу.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) __
Презентація _____
_____

6. Дата видачі завдання 20 березня 2022 року

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	20.03.2022	Виконано
2	Огляд та опрацювання літературних джерел	20.03.2022 – 04.04.2022	Виконано
3	Розслідування інциденту	05.04.2022 – 19.04.2022	Виконано
4	Підведення підсумків, формування звіту за результатами розслідування	20.04.2022 – 14.05.2022	Виконано
5	Пошук методів прискорення оцінки інцидентів	15.05.2022 – 20.05.2022	Виконано
6	Тестування розробленого методу	21.05.2022 – 05.06.2022	Виконано
7	Оформлення зібраних даних у дипломну роботу.	15.05.2022 – 27.05.2022	Виконано

Здобувач вищої освіти  Олег МИХАЙЛЕНКО

(Власне ім'я, ПРІЗВИЩЕ)

Керівник роботи  Олексій БАРАНОВСЬКИЙ

(Власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Обсяг роботи 51 сторінок, 10 ілюстрацій, 8 таблиць, 1 додаток, 11 джерел посилань. В роботі розглянуто загальні теоретичні відомості про поняття інциденту, загрози та події ІБ, детально розібрано життєвий цикл інциденту інформаційної безпеки, інструменти розслідування та основні вимоги до них. Проаналізовано та проведено порівняння двох методів оцінки критичності інцидентів інформаційної безпеки, наведено перспективу використання техніки triage із матрицею ATT&CK та її переваги над «Cyber kill chain». Розроблено метод оцінки потенційної критичності інцидентів на основі практики triage та матриці ATT&CK, розроблено правила кореляції системи SIEM для прискорення та підвищення якості оцінки потенційної критичності інцидентів. Проаналізовано багатоетапну кібератаку та виявлено недоліки у поточній системі та переваги у запропонованому методі оцінки потенційної критичності інцидентів ІБ.

Метою дипломної роботи є пошук ефективного методу прискорення оцінки потенційної критичності інцидентів інформаційною безпеки.

Об’єктом дослідження дипломної роботи є необхідність скорочення часу між виникненням загрози та її реалізацією.

Предметом дослідження дипломної роботи є методи прискорення оцінки потенційної критичності інцидентів інформаційної безпеки.

Ключові слова: інцидент, методи прискорення, оцінка, критичність, подія, загроза, атака, безпека, сортування.

ABSTRACT

The volume of work is 51 pages, 10 illustrations, 8 tables, 1 appendix, 11 sources of links. The paper considers general theoretical information about the concept of incident, threats and events of IS, detailed life cycle of information security incident, investigative tools and basic requirements for them. The comparison of two methods of assessing the criticality of information security incidents is analyzed and compared, the prospect of using the triage technique with the ATT & CK matrix and its advantages over the "Cyber kill chain" are presented. A method for estimating the potential criticality of incidents based on triage practice and the ATT & CK matrix has been developed, and SIEM system correlation rules have been developed to speed up and improve the quality of potential critical criticality assessment. A multi-stage cyberattack was analyzed and shortcomings in the current system and advantages in the proposed method of assessing the potential criticality of IS incidents were identified.

The aim of the thesis is to find an effective method to accelerate the assessment of the potential criticality of information security incidents.

The object of study of the thesis is the need to reduce the time between the occurrence of the threat and its implementation.

The subject of the thesis is the methods of accelerating the assessment of the potential criticality of information security incidents.

Key words: incident, acceleration methods, evaluation, criticality, event, threat, attack, security, sorting.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Актор – у кібербезпеці, лице яке виконували деякі дії.

БД – База даних.

ІБ – інформаційна безпека.

ОС – операційна система.

ПК – персональний комп’ютер.

TI-фіди – набір індикаторів компрометації (IoC), використання яких пов'язане з підходом "Assumed Breach" ("Вважайте, що вас вже зламали"); складне шкідливе програмне забезпечення може знаходитись в інфраструктурі атакованої компанії десятки/сотні днів до моменту виявлення.

Хост – будь-який комп’ютерний пристрій у мережі.

AD – Active Directory, програмний продукт компанії Майкрософт, служба каталогів для систем Windows

API – Application Programming Interface, програмний інтерфейс додатку.

APT-угруповання – група хакерів, частіш за все працюючих на уряд, відомі голосними інцидентами у результаті аналізу яких було виділено «почерк».

Cyber Threat Intelligence (кіберрозвідка) - це пошук інформації про потенційних атакуючих, у тому числі про APT-угруповання (від Advanced Persistent Threat, ускладнена стійка загроза / цільова кібератака).

DDoS – Distributed Denial of Service, розподілена атака типу «відмова в обслуговуванні»

EDR – Endpoint Detection and Response, програмне рішення для моніторингу та управління кінцевими точками.

ICMP – мережевий протокол, що входить у стек протоколів TCP/IP. В основному ICMP використовується для передачі повідомлень про помилки та інші виняткові ситуації, що виникли при передачі даних

IoA – Indicators of Attack, індикатори що базуються на індикаторах компрометації та даних про відомі тактики зловмисників.

IoC – Indicator of Compromise, у сфері інформаційної безпеки деякий об'єкт, що спостерігається в мережі або на пристрої, що свідчить про його компрометацію.

LM – Log Management, методологія централізованого збирання та зберігання логів з усіх пристроїв мережі.

MFA – МФА, аутентифікація на основі декількох факторів підтвердження особи.

Proxy – проміжний сервер у комп'ютерних мережах, що виконує роль посередника між користувачем і цільовим сервером(jump-host), що дозволяє клієнтам виконувати непрямі запити до інших мережевих служб, та отримувати відповіді.

RDP – Remote Desktop Protocol, пропрієтарний протокол прикладного рівня призначений для віддаленого підключення до хостів, є як корисною утилітою, так і серйозною вразливістю.

SIEM – Security information and event management, сукупність програмного забезпечення та методологій для управління інформацією про безпеку та управління подіями безпеки.

SMB – Server Message Block, мережевий протокол прикладного рівня для віддаленого доступу до файлів, принтерів та інших мережевих ресурсів, а також для міжпроцесної взаємодії. Визнаний застарілим та вразливим.

SOC – Security Operation Centre, команда або відділ оперативного реагування на виявлені загрози.

SSH – Secure Shell, мережевий протокол прикладного рівня, що дозволяє встановлювати захищене віддалене керування операційною системою та тунелювання TCP-з'єднань.

URL – Uniform Resource Locator, уніфікований локатор ресурсів, адреса ресурсу.

VM – Virtual machine, емулятор апаратного забезпечення для запуску операційних систем, у вигляді програмної або апаратної реалізації.

VPN – Virtual Privat Network, технологія створення захищеного з’єднання із цільовою мережею через іншу, наприклад Інтернет.

ВСТУП

На сьогоднішній день поняття кібербезпеки можна зустріти у кожній компанії чи держустанові. Відповідно до термінології кібербезпека це – безперервний процес протидії загрозам та вдосконалення захисту цільового ресурсу. Забезпеченням належного рівня безпеки займається команда SOC, завданням якої є відстеження усіх дій у мережі та на пристроях, а також реагування на усю підозрілу активність. Причиною необхідності прийняття таких мір є бажання деяких осіб завдати збиток з політичних, соціальних або фінансових міркувань. На шляху досягнення своєї мети кожен зловмисник залишає «цифровий слід», який тягнеться від початкового до кінця атаки. Розуміння мотивів та методів зловмисників допомагає спеціалістам із забезпечення інформаційної безпеки підготуватися до неминучих атак та відреагувати на них. Але головною проблемою остається питання як на етапі підготовки атаки оцінити що буде в її кінці та взагалі ідентифікувати атаку.

Актуальність дипломної роботи полягає у тому, що вдосконалення часу реакції на кіберзагрозу є головна ціль кожного відділу інформаційної безпеки, особливо у такий непростий період.

Метою дипломної роботи є пошук ефективного методу прискорення оцінки потенційної критичності інцидентів інформаційною безпеки.

Завданням дипломної роботи є підготовка теоретичного підґрунтя, ,пошук методів прискорення оцінки, пост-аналіз інциденту, розробка свого методу оцінки потенційної критичності.

Об’єктом дослідження дипломної роботи є необхідність скорочення часу між виникненням загрози та її реалізацією.

Предметом дослідження дипломної роботи є методи прискорення оцінки потенційної критичності інцидентів інформаційної безпеки.

1 РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Перед тим як проводити детальний розбір теми інцидентів, треба чітко розібратися з чого вони складаються. Першим етапом інциденту є виникнення загрози ІБ. Складові цього процесу можна представити як абстрактне рівняння наведене на рисунку 1.1, де кожна зі змінних не дорівнює нулю.

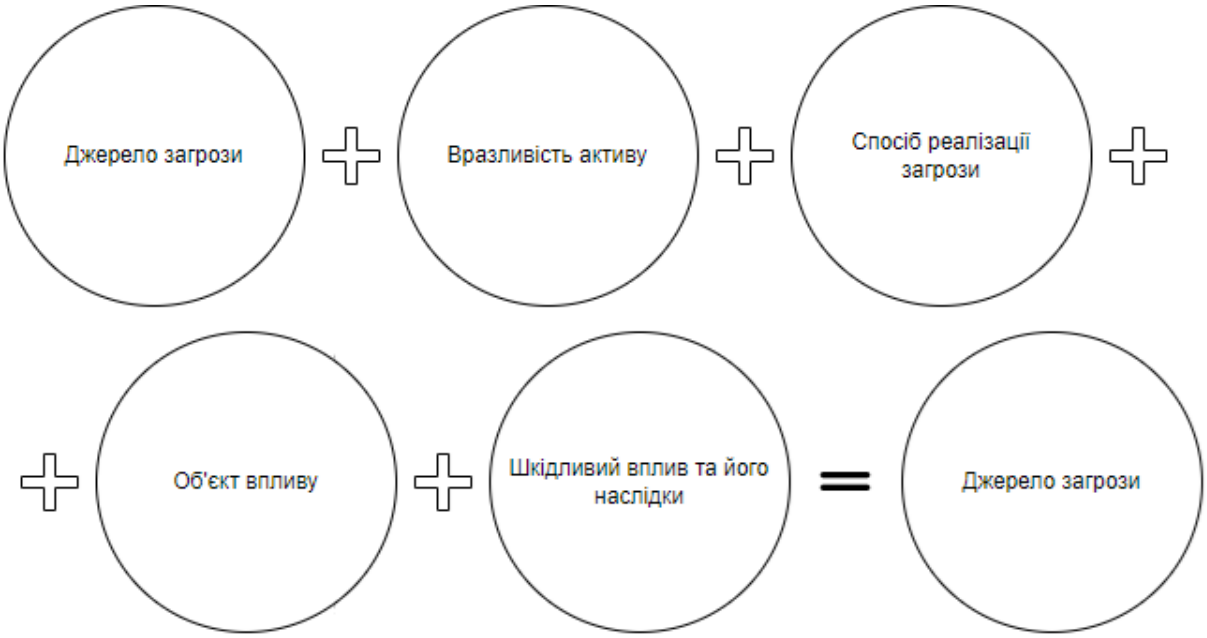


Рисунок 1.1 – Складові загрози ІБ

Джерелом загрози виступає зловмисник, APT-угруповання та інші зацікавлені особи. Вразливість активу може бути застаріле або вразливе програмне або апаратне забезпечення, можливість аутентифікації без підтвердження особи та інше. Спосіб реалізації загрози це обрана тактика, інструменти та ресурси зловмисників. Об’єктом впливу є обрана ціль: інфраструктура, окремий хост або система.

Згідно із ISO 27000:2016 загроза ІБ – це потенційна причина виникнення подій ІБ. У свою чергу подією ІБ називають певний стан системи, сервісу або мережі, що вказує на можливе порушення діючих політик ІБ, збій заходів захисту системи або деяку раніше невідому активність, що може стосуватись ІБ. Одна або декілька подій призводять до реєстрації інциденту ІБ, визначення якого є:

Це одна чи кілька небажаних чи несподіваних подій ІБ, які зі значною ймовірністю вказують на компрометацію бізнес-процесів чи реалізовану загрозу ІБ.

Загальний ланцюг причинно-наслідкового зв’язку наведено на рисунку 1.2

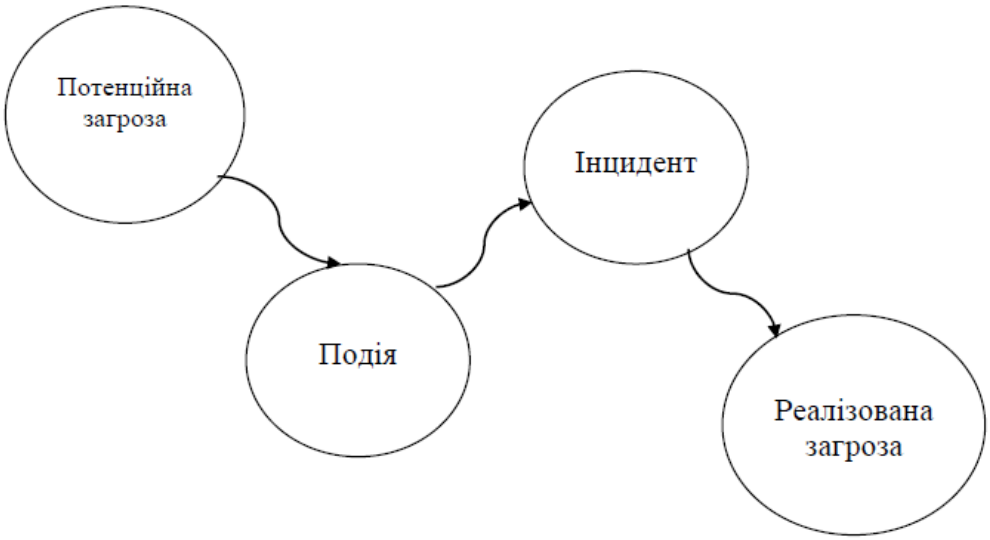


Рисунок 1.2 – Причинно-наслідковий зв’язок

Необхідність розірвати цей ланцюг або мінімізувати збитки від реалізованої загрози стає все більш актуальним питанням у зв’язку з пандемією та війною. Згідно із статистикою опублікованою ФБР та Центром розгляду скарг на інтернет-злочини за період з червня 2016 по грудень 2021 року у результаті 241000 інцидентів завдано шкоди на 43,31 мільярди доларів.

1.1 Життєвий цикл інциденту

За документом NIST SP 800-61 Computer Security Incident Handling Guide (Посібник з обробки інцидентів комп'ютерної безпеки), реагування на інциденти ІБ складається з декількох взаємопов'язаних процесів.

1. Підготовка
2. Детектування
3. Аналіз

4. Стримування/локалізація
5. Усунення
6. Відновлення
7. Пост-інциденті дії

1. Підготовка

Попередній етап, документальна підготовка: розробка та узгодження чітких, докладних та зручних політик, процедур та інструкцій з реагування. Потрібно розробити сценарії реагування(playbooks), за якими команда реагування вживатиме заздалегідь заданих дій залежно від деталей інциденту. Проводити регулярні тренування з відпрацювання кроків, визначених у написаних документах, навчання персоналу компанії та команди реагування коректним технічним та організаційним діям під час інциденту. Забезпечити команду реагування всім необхідним програмним та апаратним забезпеченням. Виконати превентивні дії щодо запобігання інцидентам (захистити мережу та пристрої компанії, встановити СЗІ, провести навчання співробітників основ ІБ).

2. Детектування

Для розуміння інциденту можна керуватися наперед визначеним списком можливих типів інцидентів ІБ та переліком ознак можливих інцидентів. Ознаки можна умовно поділити на прекурсори та індикатори інцидентів ІБ:

Прекурсор – це ознака того, що інцидент ІБ може статися в майбутньому (наприклад, сканування портів).

Індикатор - це ознака того, що інцидент вже стався або відбувається прямо зараз.

Виявлення аномалій у мережевому трафіку та поведінці користувачів може здійснюватися за допомогою модуля аналізу дій користувачів та сутностей (UEBA – User and Entity Behavior Analytics), який інтегрується із SIEM-системами.

3. Аналіз

Аналітик ІБ визначає, чи був зафіксований інцидент «бойовим», чи це було хибно-позитивна подія. Слід провести ідентифікацію та первинну обробку: визначити тип інциденту та категорувати його. Далі визначаються індикатори компрометації, аналізується можливий масштаб інциденту та порушені ним компоненти інфраструктури, проводиться обмежене форензик-обстеження для уточнення типу інциденту та можливих подальших кроків щодо реагування.

Інколи цей етап відбувається одночасно із наступними, також це і є основна проблема піднята у цій роботі, вчасна правильна класифікація інциденту дозволяє прийняти правильне рішення та мінімізувати збитки.

4. Стримування/локалізація

Оперативна мінімізація потенційної шкоди від інциденту ІБ та надання тимчасового вікна для ухвалення рішення про усунення загрози шляхом:

- увімкнення більш строгих заборонних правил на міжмережевому екрані для зараженого пристрою.
- ізоляція зараженого хоста від локальної мережі компанії.
- відключення частини сервісів та функцій
- повне вимкнення зараженого пристрою

5. Усунення

Виконуються активні дії щодо видалення загрози з мережі та запобігання повторній атаці: видаляється шкідливе ПЗ, змінюються зламані облікові записи (тимчасово заблокувати/перейменувати/змінити пароль/включити МФА), встановлюються оновлення та патчі для експлуатованих вразливостей, змінюються налаштування засобів (наприклад блокування IP-адреси зломщиків). Зазначені дії виконуються до всіх порушених інцидентом сутностей - пристроїв, облікових записів, програм.

6. Відновлення

Перевірити надійність вжитих заходів захисту, повернути системи в нормальний режим роботи, можливо, відновивши якісь системи із резервних копій або встановивши та настроїти їх заново.

7. Пост-інцидентні дії

Проаналізувати причини інциденту для того, щоб звести до мінімуму ймовірність повторного аналогічного інциденту в майбутньому, а також оцінити коректність та своєчасність дій персоналу та засобів захисту та, можливо, оптимізувати якісь процедури реагування та політики ІБ. Використовувати агреговану базу знань ведення накопиченого досвіду реагування.

1.2 Інструменти розслідування інцидентів

Для протидії атакам для відділу ІБ розгортаються засоби моніторингу та кореляції подій ІБ, LM та SIEM-системи здійснюють збір, агрегацію, запис, зберігання, пошук, таксономію, збагачення (SIEM), кореляцію (SIEM) подій ІБ від джерел. У наші дні основну перевагу надають все ж таки SIEM, тому що вона виконує наступні завдання:

1. Отримання журналів із різноманітних засобів захисту: підтримка великої кількості типів систем, пропрієтарних протоколів, API-запитів.
2. Нормалізація даних: перетворення даних у одноманітний, придатний для подальшого використання формат.
3. Таксономія нормалізованих даних: класифікація нормалізованих повідомлень для формування та подальшого аналізу послідовності типів подій з певним змістом та часом наступу.
4. Кореляція класифікованих подій: співвідношення між собою подій, які відповідають тим чи іншим умовам (правилам кореляції).

5. Створення інциденту, надання інструментів щодо розслідування.
6. Зберігання інформації про події та інциденти протягом тривалого часу (від 6 місяців) з механізмами стиснення, оптимізації.
7. Швидкий пошук за даними, що зберігаються в SIEM.

Для розуміння у якості прикладу наведено декілька правил кореляції:

- Якщо на двох і більше ПК протягом 5 хвилин спрацював антивірус з однаковою сигнатурою, це вірусна атака.
- Якщо протягом 24 годин були зафіксовані чиїсь спроби віддалено зайти на сервер, які зрештою увінчалися успіхом, а потім з цього сервера почалося копіювання даних на зовнішній файлобмінник, це може свідчити про те, що зловмисники підібрали пароль до облікового запису, зайшли на сервер та викрадають інформацію.

Характерна риса SIEM-систем – інтеграція зі сторонніми рішеннями для комплексного аналізу подій та інцидентів ІБ. Один із типів таких рішень – системи кіберрозвідки загроз (Cyber Threat Intelligence), вони передають у SIEM-систему дані, які називаються джерелами Threat Intelligence, або TI-фідами, джерелами даних кіберрозвідки. Кіберрозвідка умовно поділяється на:

- Стратегічну – пошук даних про потенційно небезпечні для компанії APT-групи, в тому числі інформації про їх підготовку до здійснення кібератаки;
- Тактичну – пошук даних про тактики, техніки та процедури атакуючих.
- Оперативну – пошук безпосередніх ознак приготування до атаки: специфічних мережевих сканувань для аналізу інфраструктури та пошуку вразливостей, шахрайських вхідних дзвінків та фішингових листів.

Індикатори компрометації (IoCs) можуть бути:

- Статичні об'єкти – хеш-суми файлів, їх імена та розташування, IP-адреси, DNS-імена серверів в мережі Інтернет або конкретні URL (посилання, наприклад на фішингові сторінки), назви гілок та ключів реєстру Windows, назви м’ютексів.
- Динамічні об'єкти – певна послідовність несанкціонованих дій на системі, що атакується (IoA), незвичайна поведінка облікових записів у системі, несанкціонована поява нових облікових записів (особливо високопривілейованих), зростання кількості підозрілих DNS-запитів, ICMP-трафіку, інших видів раніше нехарактерної мережевої активності.

Для точного виявлення атаки менш підходять статичні індикатори, найнадійнішими способами будуть методи, що використовують аналіз тактики зловмисників – послідовності кроків, що застосовуються атакуючими, які визначаються динамічними індикаторами компрометації, наприклад, послідовністю запуску певних утиліт та програм, доступом до пам'яті системних процесів, зверненням до службових мережевих ресурсів тощо.

При інтеграції системи SIEM одним із ключових завдань є виявлення подій, які матимуть найбільшу цінність з точки зору безпеки та реагування на інциденти. Захоплення занадто великої кількості подій призводить до зниження продуктивності, а якщо подій буде недостатньо, це викликає прогалини у видимості, що надається системою. Термін зберігання цих даних також є ключовим фактором. Тривале зберігання журналів полегшить розслідування як того, що відбувається зараз, так і шкідливих дій, які відбулись раніше, але не були виявлені. Вони можуть включати успішні та невдалі спроби автентифікації, доступ до певних служб, доступ до важливих файлів, модифікації ядра і т.д.

Крім журналів, що генеруються операційною системою, продукти безпеки, встановлені на кінцевих точках, такі як системи EDR або

антивірусні продукти, також можуть створювати додаткові журнали, які мають цінність. Пристрої на межах мережі, включаючи межі сегментів, можуть надавати цінну інформацію про дані потоку. Потік складається з IP-адреси пункту призначення, вихідного порту та IP-типу служби. У разі виникнення інциденту, запитавши дані потоку, можна встановити які системи у вашій мережі взаємодіяли з цією шкідливою адресою.

Висновки до розділу 1

В даному розділі було розглянуто загальні теоретичні відомості про поняття інциденту, загрози та події ІБ, детально розібрано життєвий цикл інциденту інформаційної безпеки, інструменти розслідування та основні вимоги до них.

2 КРИТЕРІЇ ТА МЕТОДИ ОЦІНКИ КРИТИЧНОСТІ ІНЦИДЕНТІВ

2.1 Загальні методи

На сьогодні, найбільш ефективним методом який використовується у ентерпрайз-рішеннях є метод базований на «Cyber kill chain» розробленій Lockheed Martin. «Cyber kill chain» — це послідовність етапів, необхідних зловмиснику для успішного проникнення в мережу та вилучення з неї даних. Кожен етап демонструє конкретну мету на шляху нападника.

Таблиця 2.1 – Cyber kill chain

Етап	Мета
Reconnaissance & Probing	• Знайти об’єкт атаки • Розробити план атаки на основі можливостей та доступних експлойтів
Delivery & Attack	• Розмістити механізм у інтернеті • Використовуючи соціальну інженерію спонукати ціль отримати доступ до шкідливого програмного забезпечення чи іншого експлойту
Exploitation & Installation	• Використати вразливості на цільовій системі задля отримання доступу • Отримати привілейований доступ та встановити корисне навантаження
System Compromise	• Ексфільтрація цінних даних не привертаючи уваги • Використання зламаної системи для створення ботнету або проведення паразитичних хмарних обчислень

Використання цієї методології включає в себе наступний принцип оцінки критичності інцидентів.

Таблиця 2.2 – Класифікація інцидентів на основі «Cyber kill chain»

Тип	Етап kill chain	Пріоритет	Рекомендація
Port Scanning Activity	Reconnaissance & Probing	Low	Ігноруйте більшість цих подій, окрім, якщо IP-адреса джерела не має відомої поганої репутації або є кілька подій з цієї самої IP-адреси за короткий проміжок часу.
Malware Infection	Delivery & Attack	Low-Medium	Усуньте будь-яке зараження шкідливим програмним забезпеченням якомога швидше, перш ніж воно прогресує. Скануйте решту вашої мережі на наявність IoC, пов’язаного з цією ШПЗ.
Distributed Denial Of Service	Exploitation & Installation	High	Налаштуйте веб-сервери для захисту від запитів HTTP та SYN flood. Координуйтеся з вашим провайдером під час атаки, щоб заблокувати вихідні IP-адреси.
Distributed Denial Of Service Diversion	Exploitation & Installation	High	Іноді DDoS використовується, щоб відвернути увагу від іншої більш серйозної спроби атаки. Збільште моніторинг і розслідуйте всю пов’язану діяльність, а також тісно співпрацюйте зі своїм провайдером або постачальником послуг.

Продовження таблиці 2.2

Тип	Етап kill chain	Пріоритет	Рекомендація
Unauthorized Access	Exploitation & Installation	Medium	Знаходьте, відстежуйте та досліджуйте спроби несанкціонованого доступу – з пріоритетом тих, які є критичними та/або містять конфіденційні дані.
Insider Breach	System Compromise	High	Визначте привілейовані облікові записи користувачів для всіх доменів, серверів, програм і критичних пристроїв. Переконайтеся, що моніторинг увімкнено для всіх систем і для всіх системних подій, а також переконайтеся, що він наповнює журнали моніторингу вашої інфраструктури.
Unauthorized Privilege Escalation	Exploitation & Installation	High	Налаштуйте свої критичні системи для запису всіх подій ескалації привілеїв та встановіть сигнали тривоги для несанкціонованих спроб підвищення привілеїв.
Destructive Attack	System Compromise	High	Зробіть резервне копіювання всіх критичних даних і систем. Перевірте, задокументуйте та оновіть процедури відновлення системи. Під час компрометації системи – ретельно збирайте докази та задокументуйте всі кроки відновлення, а також усі зібрані докази.

Кінець таблиці 2.2

Тип	Етап kill chain	Пріоритет	Рекомендація
Advanced Persistent Threat or Multistage Attack	All Stages	High	Будь-яка з перерахованих тут унікальних подій насправді може бути частиною найгіршого типу інциденту безпеки, який тільки можна уявити – APT. Важливо розглядати кожну подію в більш широкому контексті, який містить найновіші дані про загрози. (Threat Intelligence)
False Alarms	All Stages	Low	Хибно-позитивні спрацювання.
Other	All Stages	High	Реагування на інциденти – це дисципліна постійного вдосконалення. Коли ви бачите, що все більше і більше подій перетворюються на інциденти, ви відкриєте нові способи класифікації цих інцидентів, а також нові способи запобігти їх колись.

«Cyber kill chain» був «першопроходьцем» у моделюванні та класифікації поведінки зловмисників, але із еволюцією атак такий підхід вже втрачає ефективність. Кіберзлочинці, особливо ті що представляють APT-угруповання, ретельно планують кожен свій крок, і при наявності лише 9 етапів, ідентифікувати кібератаку можливо при десятій частині її успіху.

2.2 Перспективні методи оцінки інцидентів

Використання передової технології із чимось що існує вже давно, іноді дає хороший результат. Прикладом цього може стати використання матриці MITRE&ATT&CK із практикою triage. MITRE&ATT&CK – це загальнодоступна база знань про тактики та техніки кіберзлочинців на основі спостережень у реальному світі. У розумінні MITRE: тактика – це те, чого намагаються досягти зловмисники, тоді як окремі техніки – це те, як вони досягають своєї мети. Матриця ATT&CK використовується як основа для розробки конкретних моделей і методологій загроз та класифікації етапів атак у приватному секторі, в уряді, а також у спільноті продуктів і послуг кібербезпеки. Вона постійно удосконалюється та поповнюється актуальною інформацією; із повною матрицею ATT&CK можна ознайомитись по посиланням в джерелах.

Термін triage запозичений у представників воєнної медицини, дослівно це медичне сортування. Воно полягає у тому щоб класифікувати постраждалих, виходячи з терміновості надання їм медичної допомоги так, щоб у результаті вижила максимальна кількість пацієнтів. Приклад затверджений міжнародною спілкою лікарів наведену у таблиці 2.3.

Таблиця 2.3 – Медичне сортування

Ступінь	Класифікація	Критерій	Дія
I	Immediate/невідкладна допомога	Тяжко поранені, які можуть померти протягом декількох годин	Негайне надання допомоги, проведення реанімаційних заходів

Продовження таблиці 2.3

Ступінь	Класифікація	Критерій	Дія
II	Delayed/термінова допомога	Тяжко поранені, чиє життя поки не знаходиться під загрозою	Стабілізація стану здоров'я та надання другого пріоритету
III	Minor/нетермінова допомога	Легкопоранені, життю нічого не загрожує	Допомога надається третім пріоритетом
IV	Morgue/морг	Померлі або мають травми не сумісні з життям	Допомога не надається

Використання цього методу у паритеті з матрицею MITRE&ATT&CK для первинної оцінки критичності інцидентів, дає змогу досягти тієї ж мети, яку переслідують лікарі – максимальної ефективності при обмеженому часі. У якості критеріїв будуть тактики ATT&CK помічені на кінцевих точках або мережі за допомогою SIEM, класифікація буде трішки інша, оскільки якщо сервер чи система не має «ознак життя», то це відноситься до першого ступеню критичності, але з'являються інциденти інформаційного характеру. Їх можна характеризувати як ті в яких недостатньо IoC для того, щоб віднести до вищих категорій, на них не потрібно звертати увагу але у разі появи нових зловмисних дій можна буде побачити і попередню активність.

Класифікація виглядає наступним чином:

1. Critical
2. Hight
3. Medium
4. Low
5. Informational

Основні переваги використання MITRE&ATTACK у порівнянні із Cyber Kill Chain:

Таблиця 2.4 – Порівняльна характеристика

MITRE&ATT&CK	Cyber Kill Chain	Висновок
ATT&CK матриця яка містить 14 тактик, кожна з яких поділяється на техніки загальна сума яких 222	Cyber Kill Chain це чітко встановлена лінійна послідовність 9 фаз атаки	Використання MITRE дозволить виявити більш дрібний крок зловмисника, що дає більше шансів команді ІБ виконати превентивні дії
MITRE має постійно обновлювану БД із ідентифікаторами кожної техніки, доступ до неї можливо реалізувати навіть через API	Загальні положення які можливо інтегрувати лише власноруч або придбавши готовий продукт	При використанні MITRE в системі буде актуальна інформація у готовому вигляді

Висновки до розділу 2

В даному розділі було детально розглянуто наявний метод оцінки критичності інцидентів інформаційної безпеки на основі «Cyber kill chain», наведено перспективу використання техніки triage із матрицею ATT&CK та її переваги.

3 РЕАЛІЗАЦІЯ МЕТОДУ ПРИСКОРЕННЯ ОЦІНКИ КРИТИЧНОСТІ ІНЦИДЕНТІВ ІБ

3.1 Розробка методу прискорення оцінки

Класифікація

Для використання triage необхідно встановити чітку класифікацію критичності інцидентів.

1. Critical – інцидент, який потенційно призведе до порушення роботи життєво важливих бізнес-процесів компанії та свідчить про активну фазу атаки.
2. Hight – інцидент, який потенційно свідчить про наявність у зловмисника всіх умов для початку атаки.
3. Medium – інцидент, який потенційно може свідчити про пасивну присутність зловмисника.
4. Low – інцидент, який свідчить про виявлену аномалію створену у випадку людської помилки або підготовки атаки.
5. Informational – не є фактично інцидентами, одинокі підозрілі дії, які не підпадають під правила кореляції SIEM.

Критерії

Критерії це аналог «симптомів», у даній моделі використовується тактики MITRE. Також є сенс при оцінці враховувати середу у якій було помічено використання тої чи іншої техніки.

При розробці методу я спирався на розслідування інциденту у АТ «Укртелеком» яке було в рамках переддипломної практики. Усі системи розподіляються на 4 рівні важливості: Core – відповідають за роботи мережі в цілому, Mission – системи внутрішніх сервісів, Business – основні бізнес процеси, Operation – не критично важливі сервіси, якими користуються певні групи користувачів. Перші дві – групи життєво важливих серверів без яких надання послуг неможливо, тому при реєстрації інциденту із участю серверів

з цих груп, ступінь критичності збільшується на два. Відмова третьої групи робить неможливим роботу підприємства, але не несе загрози відключення користувачів та каналів спецзв'язку, при реєстрації інциденту із участю серверів з цих груп, ступінь критичності збільшується на один. Четверта, найчастіше, системи підрядників. У п'яту групу відносяться користувацькі ПК та сервери які не відносяться до попередніх груп. При реєстрації інциденту із участю серверів або ПК з останніх двох груп, ступінь критичності не збільшується.

До першого ступеню критичності відносяться усі події зареєстровані системою моніторингу які мають ознаки аномалії, наприклад підключення до заборонених веб-ресурсів.

«Reconnaissance», «Resource Development», «Discovery», «Initial Access» тактики другого ступеню, вони свідчать про інтерес з боку зловмисників до системи, через те що техніки які використовуються для них співпадають із звичайними діями систем/користувачів в мережі, генерується велика кількість подій з такою класифікацію.

«Lateral Movement», «Defense Evasion», «Credential Access», «Execution», «Persistence» відносяться до третього ступеню, при підтвердженні факту зловмисницької дії підпадаючої під одну з цих тактик, це говорить про те що зловмисник вже в системі та намагається в ній закріпитись.

«Collection», «Privilege Escalation», «Command and Control» це четвертий ступінь. Повідомлення про ці тактики несуть інформацію що у зловмисника вже є всі необхідні інструменти для проведення атаки.

«Impact» «Exfiltration» тактики п'ятого ступеню критичності, свідчать про те що атака вже відбувається або відбулась.

Ступінь критичності інциденту розраховується із двох значень: ступінь тактики по якій було зареєстровано інцидент + значення критичності активу. Якщо отримане значення більше або дорівнює 5 інцидент належить до класу «Critical»

Таблиця 3.1 – Triage-сортування інцидентів

<table>
<tr><th rowspan="2">Ступінь</th><th rowspan="2">Класифікація</th><th colspan="2">Критерій</th><th rowspan="2">Дії</th></tr>
<tr><th>Тактика</th><th>Ступінь критичності активу</th></tr>
<tr><td>V</td><td>Critical</td><td>«Impact»
«Exfiltration»</td><td rowspan="3">«CoreIT» +2
«Mission» +2
«Business» +1
«Operation» 0
Інші 0</td><td>Негайно реагування, ізоляція сегменту мережі, оповіщення відповідальних спеціалістів</td></tr>
<tr><td>IV</td><td>Hight</td><td>«Collection»
«Privilege Escalation»
«Command and Control»</td><td>Реагування згідно пріоритету, пошук інших скомпрометованих систем та облікових записів</td></tr>
<tr><td>III</td><td>Medium</td><td>«Lateral Movement»
«Defense Evasion»
«Credential Access»
«Execution»
«Persistence»</td><td>Реагування згідно з пріоритетом, ізоляція пристрою, скидання пароля потенційно скомпрометованих акаунтів.</td></tr>
</table>

Продовження таблиці 3.1

Ступінь	Класифікація	Критерій		Дії
		Тактика	Ступінь критичності активу	
II	Low	• «Reconnaissance» • «Resource Development» • «Discovery» • «Initial Access»	«CoreIT» +2 «Mission» +2 «Business» +1 «Operation» 0 Інші 0	Реагування згідно з пріоритетом, дослідження логів щодо успішності дій, оцінка ризиків
I	Information	Непрямі індикатори компроментації		Подальший моніторинг ситуації

3.2 Інтеграція методу та налаштування SIEM

Для того щоб швидко оцінювати інциденти, необхідно щоб у SIEM системі були відповідні правила кореляції подій ІБ. Важливим фактором при створенні правил є знаходження золотої середини між втратою важливих подій та отриманням хибно-позитивних результатів.

Загальна архітектура роботи SIEM наведена на рисунку 3.1

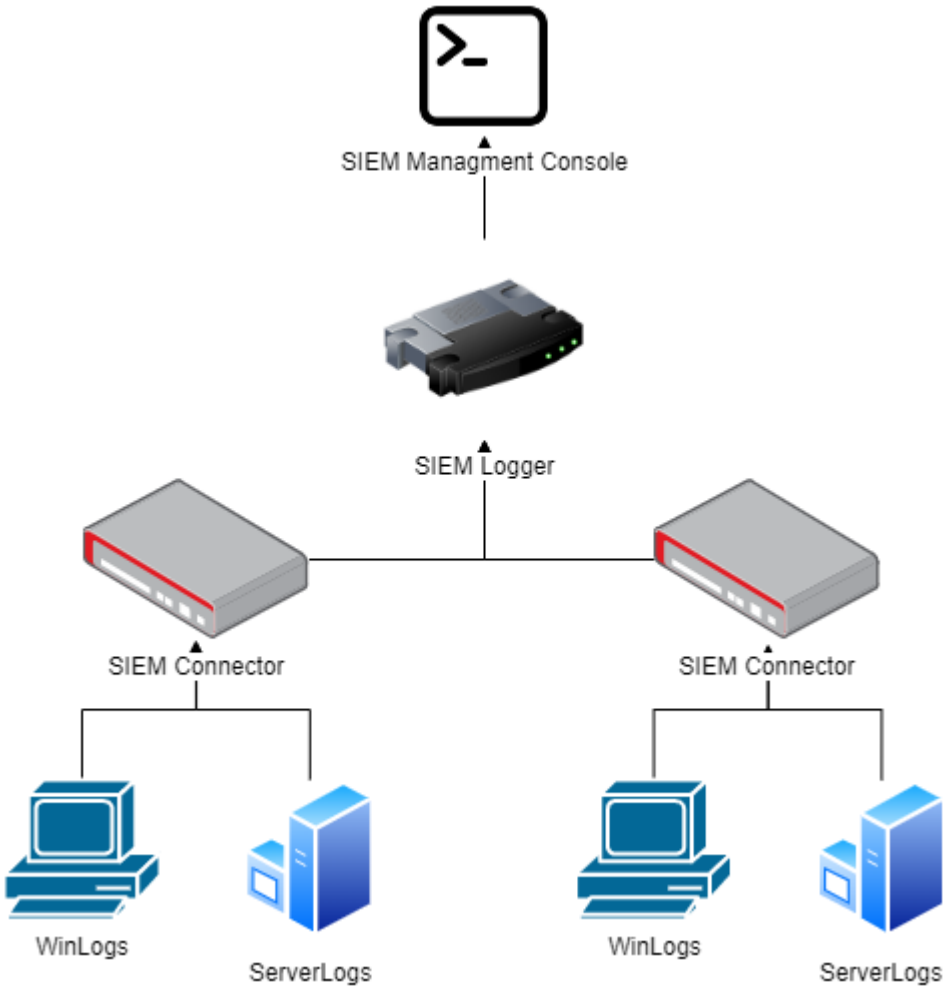


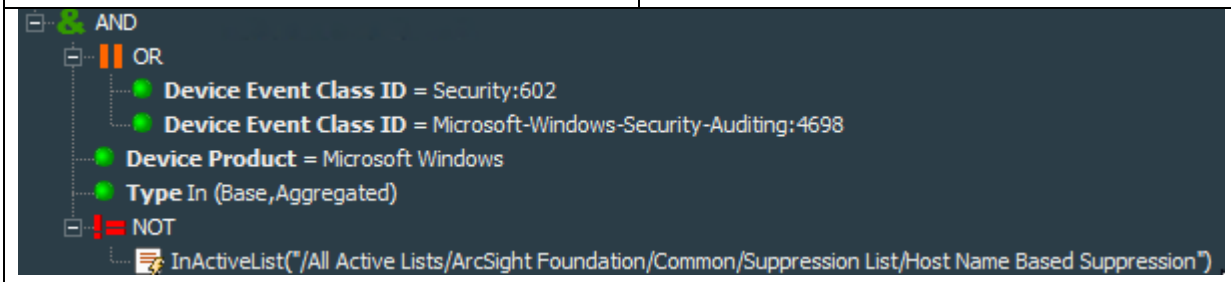
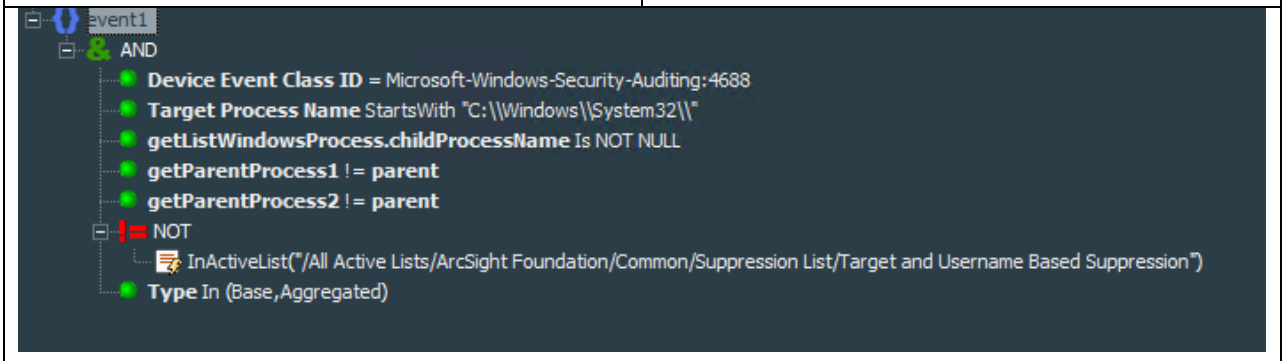
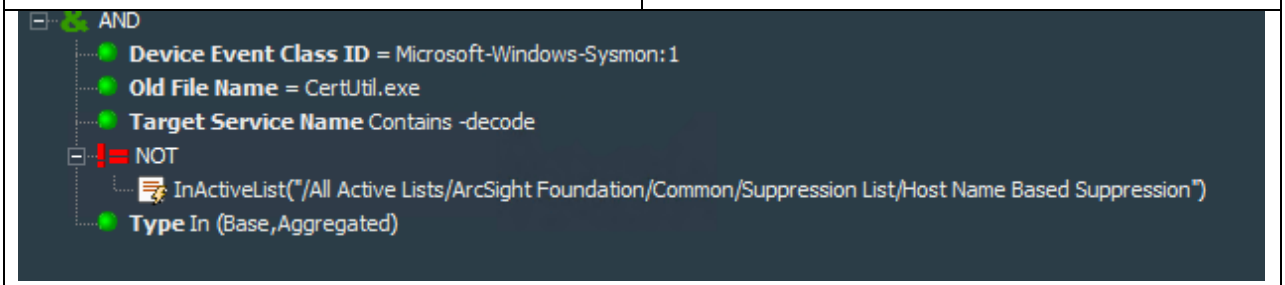
Рисунок 3.1 – Data-Flow

У якості джерел подій використовуються логи операційних систем. У кожній події в Журналі подій Windows є деякий набір параметрів: ID-події, ім’я хоста, ім’я користувача, IP-адреса і т.д. Після під’єднання пристроїв до конекторів були створені правила на основі MITRE&ATTACK. У роботі наведено більшу частину розроблених правил які більш детально демонструють логіку роботи SIEM. Правила утворюються на булевих операціях та методу станів(Conditions).

Таблиця 3.2 – Правила на основі MITRE

<table>
<tr><td>TA0001 Initial Access</td><td>T1566 Phishing</td></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td colspan="2">Як зазначалось у 1 розділі, системи SIEM мають дуже високу можливість інтеграції, у даному правилі виявляються отримані фішингові листи на основі відкритих даних кіберрозвідки(Threat Intelligence)</td></tr>
<tr><td>TA0002 Execution</td><td>T1569 System Service</td></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td colspan="2">При використанні psexec ОС створить подію у системному журналі, а SIEM інцидент з тегом Execution</td></tr>
</table>

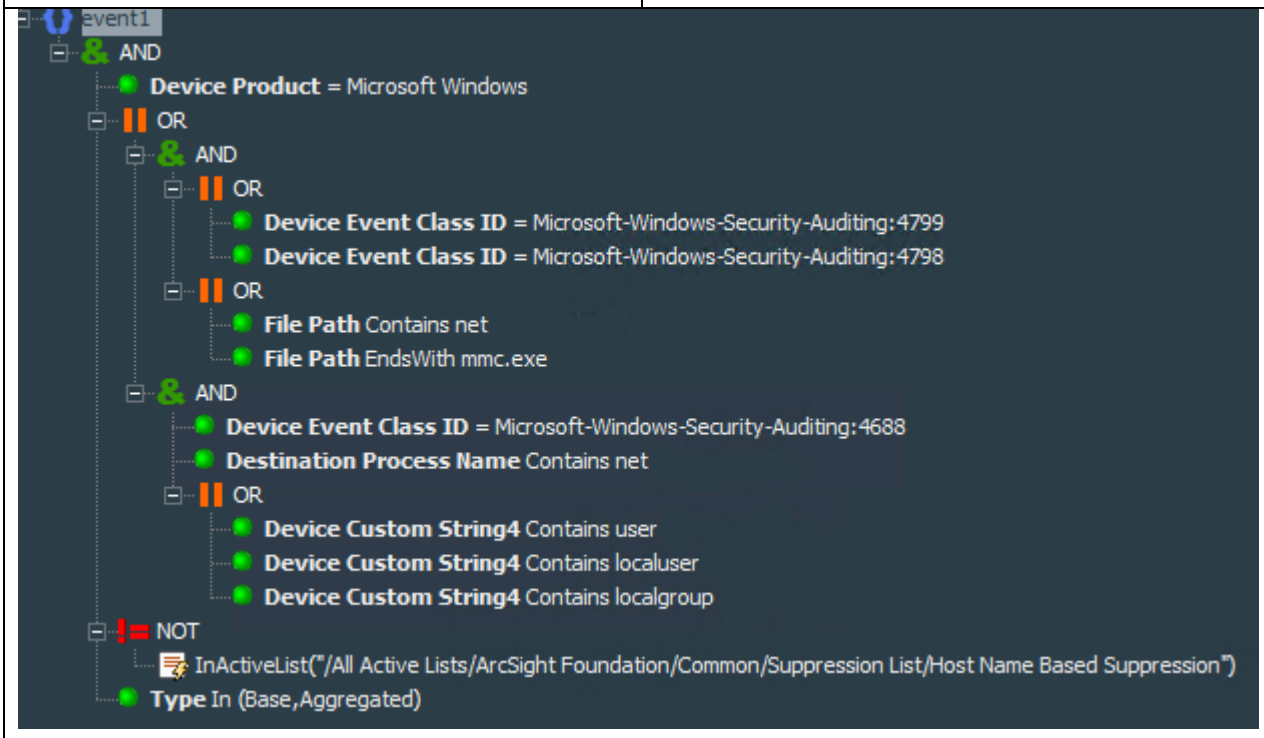
Продовження таблиці 3.2

TA0003 Persistence	T1053 Scheduled Task
	
Створення запланованого завдання відображається у системних логах. Хочу підкреслити що дане правило не є ефективним у зв'язку з частим використанням Scheduler адміністраторами.	
TA0003 Privilege Escalation	T1055 Process Injection
	
Правило перевіряє чи належить дочірній процес до батьківського для реєстрації інциденту у разі ін'єкції. Така техніка часто використовується для отримання прав адміністратора за допомогою привелійованих процесів.	
TA0005 Defence Evasion	T1140 Deobfuscate or decode files or information
	
Зловмисники часто доставляють корисне навантаження зашифрував його для уникнення детектування. Так як у цільовому середовищи може не бути інструментів, криптографічні перетворення виконуютсья системную утилітою CertUtil.	

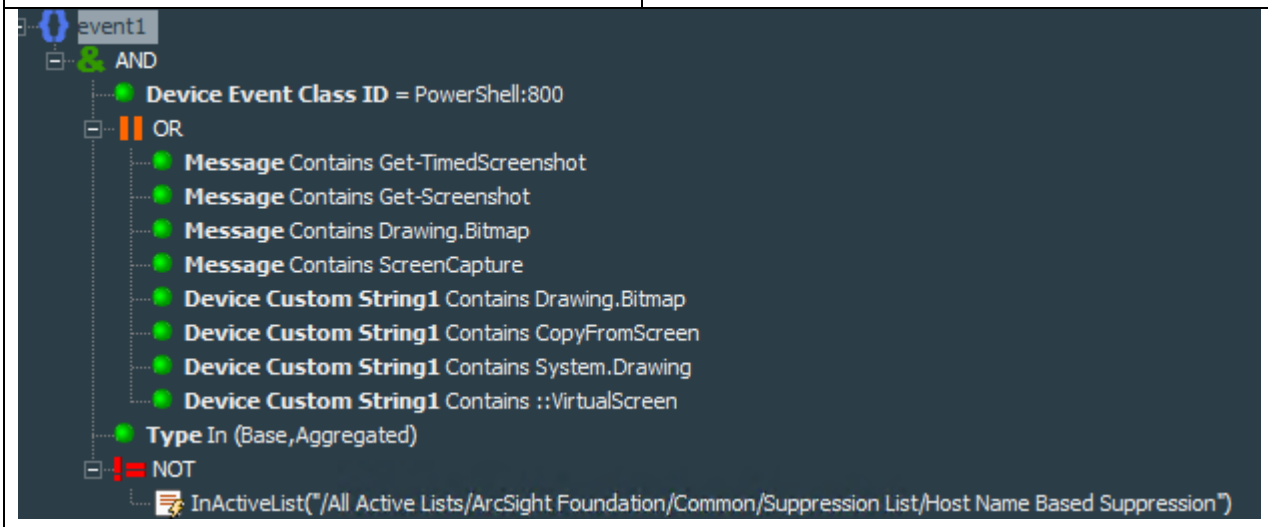
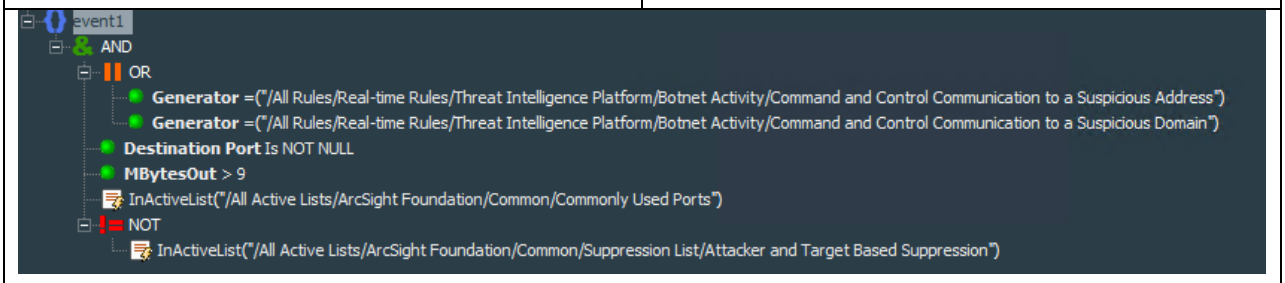
Продовження таблиці 3.2

TA0006 Credential Access	T1003 OS Credentional Dump
	
Після отримання адміністративного доступу найчастіша дія це дамп процесу lsass.exe для отримання данних обліковаих записів.	
TA0006 Credential Access	T1110 Brute Force
	
Правило спрацює якщо після довготривалого перебору паролів відбудеться аутентифікація користувача, що буде свідчити про вдалий брут-форс.	

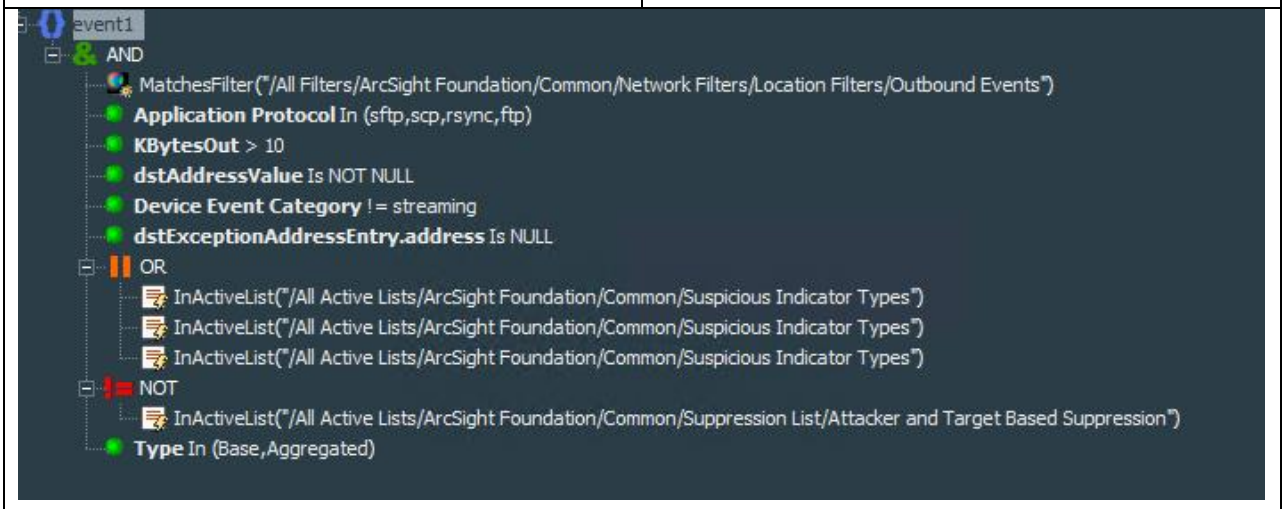
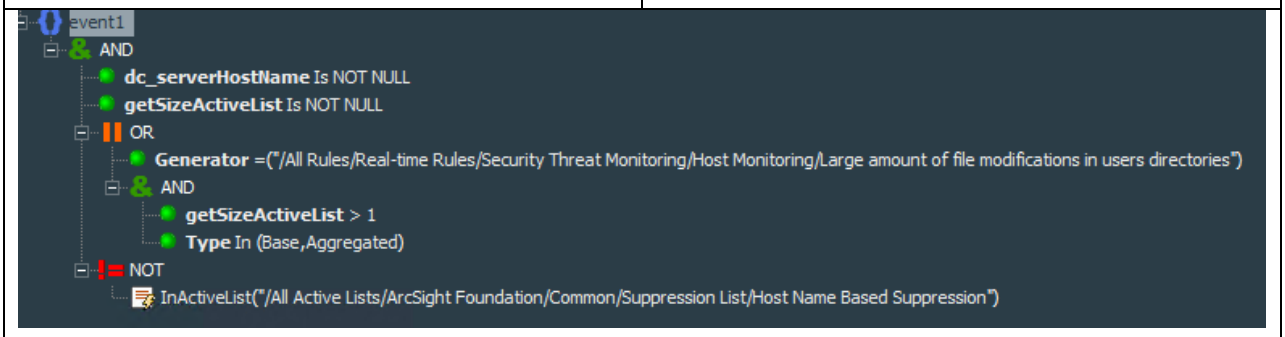
Продовження таблиці 3.2

TA0007 Discovery	T1087 Account Discovery
	
При пошуці облікових записів або груп за допомогою cmd команд зареєструється інцидент.	
TA0008 Lateral Moment	T1021 Remote service
	
RDP дуже зручний, але й самий небезпечний протокол, правило сконфігуроване на хости які апріорі не повинні підключатися до віддалених машин.	

Продовження таблиці 3.2

<table>
<tr><td>TA0009 Collection</td><td>T1131 Screen Capture</td></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td colspan="2">Правило налаштоване на детектування знімку екрану інструментами PowerShell</td></tr>
<tr><td>TA0010 Exfiltration</td><td>T1041 Exfiltration over Command and Control</td></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td colspan="2">Ще одне правило яке використовує дані кіберрозвідки, при відправці обсягу данниз більше 9 МБ на сервер відомий як шкідливий зафіксується інцидент.</td></tr>
</table>

Кінець таблиці 3.2

TA0011 Command and Control	T1105 Ingress Tool Transfer
	
При використанні вказаного стеку протколів для передачі данних	
TA0040 Impact	T1486 Data Encryption for Impact
	
Одночасна зміна великої кількості файлів на хості свідчить про імовірну роботу шифрувальника.	

Також, як було зазначено у розділі 1, головною фішкою SIEM є гнучкість та інтеграція. Для автоматизації перевірки результатів роботи вище розглянутих правил можна використовувати антивірус, DLP та EDR. Існує багато засобів для маскування ШПЗ від детектування, основна суть його полягає у проходженні статичного аналізу по базам даних відомих зразків та динамічного аналізу у вигляді відстеження системних викликів та запуск у контейнері антивірусу. На жаль захисне ПО дуже обмежено у ресурсах, тому не завжди можливо ідентифікувати файл як шкідливий. Розгорнувши сервер-пісочницю під контролем CuckooSandbox або PaloAltoNetworks можна відправляти на аналіз усі програми які з’являються на пристроях мережі без

впливу на її працездатність. Аналіз ПЗ буде займати деякий час, до моменту отримання позитивного результату від пісочниці, система EDR буде блокувати виконання програми на машинах, а SIEM наддасть змогу бачити на яких пристроях з’явилось це ПЗ, та які зміни внесло у реєстр ОС.

3.3 Апробація методики

З метою порівняння методу оцінки критичності розроблений у роботі із методом на основі «Cyber kill chain» проведено пост-інцидентний аналіз інциденту ІБ який стався у АТ «Укртелеком» 26.03.22, призвевший до обмеження використання мережі в Україні до каналів спеціального зв’язку. Для збереження конфіденційної інформації були змінені назви ресурсів та видалені IP-адреси.

У ході розслідування перше що вдалося встановити це програмне забезпечення та утиліти які використав зловмисник. Деякі з них входять у стандартний набір ОС сімейства Windows, але їх використовують частіш за все лише обмежена група користувачів. Виконання цих програм на кінцевому хості можна віднести до IoC. Повний список ПЗ наведений у таблиці 3.3.

Таблиця 3.3 – Інструменти зловмисника

Назва	Опис
WMIExec	Частина сімейства Impacket використовує інструментарій керування Windows (WMI), щоб надати вам інтерактивну оболонку/відправити команди на хост Windows через WmiPrvSE.exe

Продовження таблиці 3.3

Назва	Опис
SMBExec	Частина сімейства Impacket використовує блок повідомлень сервера (SMB), щоб надати вам інтерактивну оболонку/відправити команди на хост Windows через створення служби Windows.
cmd.exe	Усередині операційної системи Windows зловмисники використовують cmd.exe для взаємодії з хостом через командний рядок
nslookup	Всередині операційної системи Windows зловмисники використовують nslookup, щоб отримати зіставлення доменних імен та IP-адрес
icacls.exe	Усередині операційної системи Windows зловмисники використовують icacls.exe для контролю дозволів до об’єктів Windows, наприклад, файлів, папок тощо.
Meterpreter	Part of the Metasploit family and is an attack payload which is dropped to the target machine to provide an interactive shell
Scripts (.bat/.ps1)	Спеціальні скрипти для взаємодії з Active Directory, щоб увімкнути/вимкнути/видалити користувачів і змінити паролі
7-Zip	Використовується для стиснення файлів для зменшення розміру або для шифрування паролем підозрілих файлів

Продовження таблиці 3.3

Назва	Опис
Procdump.exe	Інструмент SysInternal, створений для скидання простору пам'яті процесу для даного помилкового процесу; часто використовується для дампу LSASS
SSH.exe	Клієнтський компонент, який використовується для встановлення зашифрованих з'єднань з пунктами призначення через канал SSH (22/TCP)
Goodbye.exe	Ідентифікований DELTACHERRY як стиральник, який намагався розповсюдити та виконати груповою політикою

Наступним етапом є пошук точки початкового доступу, у даному інциденті це був корпоративний ноутбук із можливістю підключення через VPN F5 до корпоративної мережі, використавши данні облікового запису власника ПК, перші дії датуються 05.03.22.

І починаючи з 26.03.22 актор використовуючи RDP та підключаючись до інших хостів підмережі почав поширювати свою присутність у системах. Так на деяких серверах було знайдено підозрілі файли які були ідентифіковані як опенсорсне ПЗ pivotnaccі виконуюче функцію proxy.

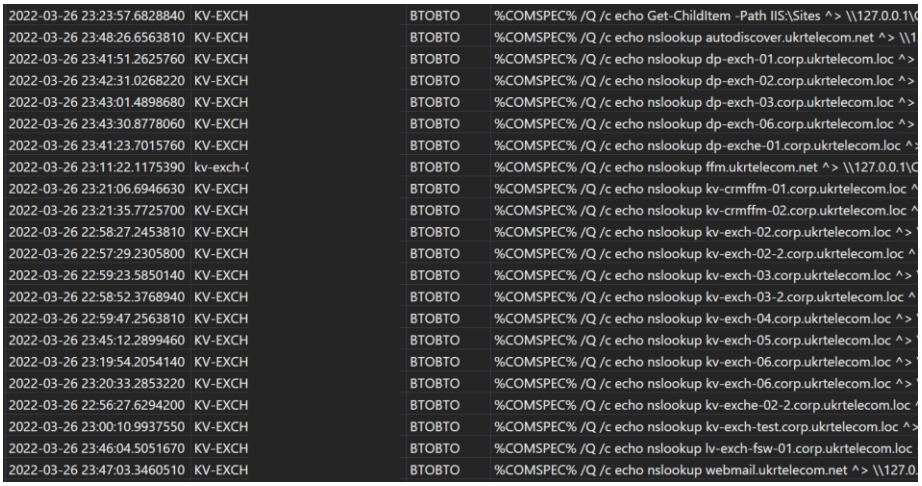
Підтвердження роботи ПЗ наведено на рисунку 3.2

DeviceDnsName	IISTimestamp	sIP	csMethod	csUriStem	sPort	cIP	csUserAgent
kv-lyncdi	2022-03-26 18:46:46.0000000	10.	GET	/dialin/error.aspx	4443	10	pivotnacci/0.0.1
kv-lyncdi	2022-03-26 18:46:46.0000000	10.	POST	/dialin/error.aspx	4443	10	pivotnacci/0.0.1
kv-lyncdi	2022-03-26 18:46:47.0000000	10.	GET	/dialin/error.aspx	4443	10	pivotnacci/0.0.1
kv-lyncdi	2022-03-26 18:58:39.0000000	10.	GET	/dialin/error.aspx	4443	10	pivotnacci/0.0.1
kv-lyncdi	2022-03-26 19:01:47.0000000	10.	GET	/dialin/error.aspx	4443	10	pivotnacci/0.0.1
kv-lyncdi	2022-03-26 19:02:08.0000000	10.	GET	/dialin/error.aspx	4443	10	pivotnacci/0.0.1
kv-lyncdi	2022-03-26 19:02:29.0000000	10.	GET	/dialin/error.aspx	4443	10	pivotnacci/0.0.1
kv-lyncdi	2022-03-26 19:02:51.0000000	10.	GET	/dialin/error.aspx	4443	10	pivotnacci/0.0.1
kv-lyncdi	2022-03-26 19:03:12.0000000	10.	GET	/dialin/error.aspx	4443	10	pivotnacci/0.0.1

Рисунок 3.2 – Слід використання proxy-агенту

За отриманням необхідного доступу слідує розвідка, звертаючись до домен контролера зловмисник робив перечислення облікових записів. За допомогою утиліти nslookup та інструменту SMBExec актор шукав вразливі

поштові сервери Exchange та їх конфігурацію з метою отримання доступу до інтерактивної оболонки. Дії зловмисника продемонстровані на рисунку 3.3



2022-03-26 23:23:57.6828840	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo Get-ChildItem -Path IIS:\Sites ^> \\127.0.0.1\C
2022-03-26 23:48:26.6563810	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup autodiscover.ukrtelecom.net ^> \\1
2022-03-26 23:41:51.2625760	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup dp-exch-01.corp.ukrtelecom.loc ^>
2022-03-26 23:42:31.0268220	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup dp-exch-02.corp.ukrtelecom.loc ^>
2022-03-26 23:43:01.4898680	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup dp-exch-03.corp.ukrtelecom.loc ^>
2022-03-26 23:43:30.8778060	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup dp-exch-06.corp.ukrtelecom.loc ^>
2022-03-26 23:41:23.7015760	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup dp-exche-01.corp.ukrtelecom.loc ^
2022-03-26 23:11:22.1175390	kv-exch-(	BTOBTO	%COMSPEC% /Q /c echo nslookup ffm.ukrtelecom.net ^> \\127.0.0.1\C
2022-03-26 23:21:06.6946630	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-crmffm-01.corp.ukrtelecom.loc ^
2022-03-26 23:21:35.7725700	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-crmffm-02.corp.ukrtelecom.loc ^
2022-03-26 22:58:27.2453810	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-exch-02.corp.ukrtelecom.loc ^>
2022-03-26 22:57:29.2305800	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-exch-02-2.corp.ukrtelecom.loc ^
2022-03-26 22:59:23.5850140	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-exch-03.corp.ukrtelecom.loc ^>
2022-03-26 22:58:52.3768940	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-exch-03-2.corp.ukrtelecom.loc ^
2022-03-26 22:59:47.2563810	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-exch-04.corp.ukrtelecom.loc ^>
2022-03-26 23:45:12.2899460	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-exch-05.corp.ukrtelecom.loc ^>
2022-03-26 23:19:54.2054140	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-exch-06.corp.ukrtelecom.loc ^>
2022-03-26 23:20:33.2853220	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-exch-06.corp.ukrtelecom.loc ^>
2022-03-26 22:56:27.6294200	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-exche-02-2.corp.ukrtelecom.loc
2022-03-26 23:00:10.9937550	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup kv-exch-test.corp.ukrtelecom.loc ^>
2022-03-26 23:46:04.5051670	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup lv-exch-fsw-01.corp.ukrtelecom.loc
2022-03-26 23:47:03.3460510	KV-EXCH	BTOBTO	%COMSPEC% /Q /c echo nslookup webmail.ukrtelecom.net ^> \\127.0.

Рисунок 3.3 – Логи SIEM

Для виконання дій що можуть нести серйозну загрозу необхідні права, на вразливому термінальному сервері зловмисник створив локальний обліковий запис «Operator» та добавив його у групу локальних адміністраторів. Дії наведені на рисунку 3.4. Це дозволило йому провести дамп пам’яті процесу LSASS у якому знаходяться дані облікових записів усіх користувачів серверу.

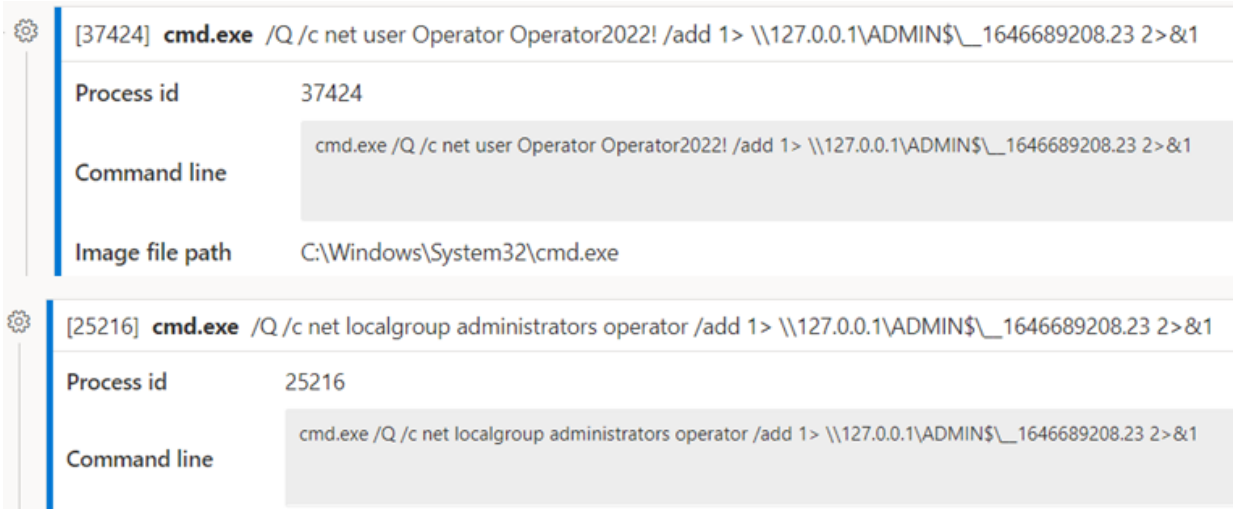


Рисунок 3.4 – Створення облікового запису Operator

Саме на цьому сервері працював адміністратор домену; після зміни паролю було піднято весь IT-персонал, почались активна протидія. Використавши привілеї адміністративного облікового запису актор

скопіював із домен-контролеру базу даних AD ntds.dit, яка містить данні усіх акаунтів каталогу, через SMB(Рисунок 3.5).

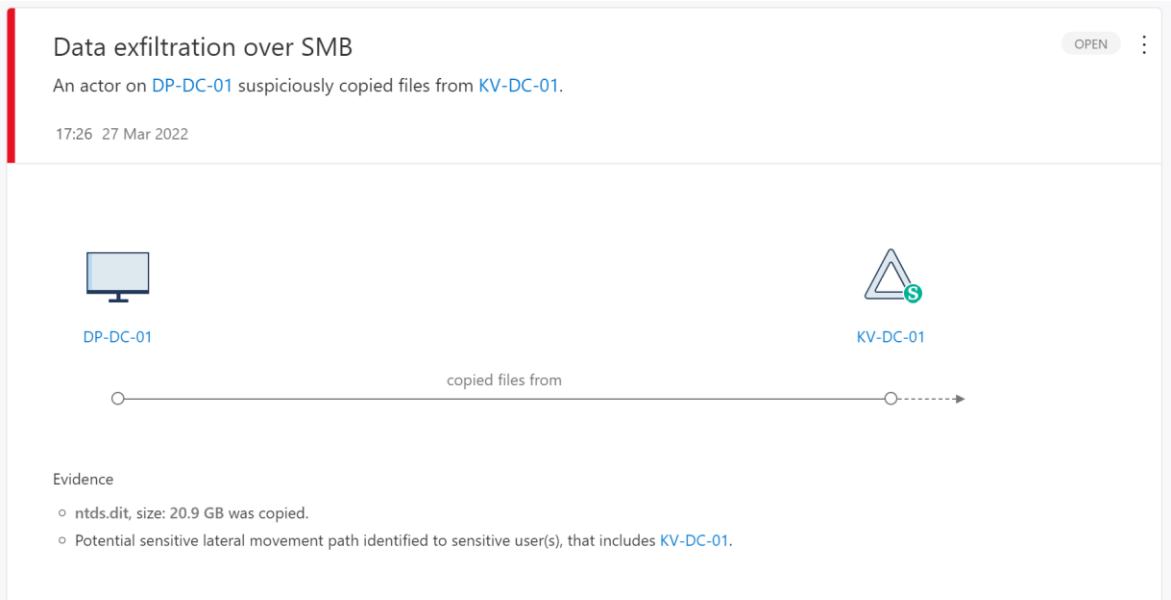


Рисунок 3.5 – Оповіщення про подію на домен-контролері

Останній удар був запуском на домен контролері PowerShell скриптів «boom.ps1» та «temp.ps1» які видалили усі паролів користувачів та згенерували нові для унеможливлювання аутентифікації працівників. Програмний код скриптів було відновлено та надано на рисунку 3.6.

boom.ps1

```
1  Import-Module activedirectory
2  Get-Content C:\ProgramData\allusers.txt | Remove-ADUser
3  Get-Content C:\ProgramData\allusers2.txt | Remove-ADUser
4  Get-Content C:\ProgramData\allusers3.txt | Remove-ADUser
5  Get-Content C:\ProgramData\allusers4.txt | Remove-ADUser
6  Get-Content C:\ProgramData\allusers5.txt | Remove-ADUser
7  Get-Content C:\ProgramData\allusers6.txt | Remove-ADUser
```

temp.ps1

```
1  Import-Module activedirectory
2  Get-Content C:\ProgramData\users.txt | Enable-AdAccount
3  Get-Content C:\ProgramData\users.txt | Set-ADAccountPassword -NewPassword (ConvertTo-SecureString -AsPlainText "LaeNd14GoxMbLz
4  Set-ADAccountPassword -Identity kv-sms-install -NewPassword (ConvertTo-SecureString -AsPlainText "BGdbwj_BWSdyz9jYi" -Force)
```

Рисунок 3.6 – Шкідливий скрипт PowerShell

Такі дії вимагали негайного вирішення проблеми докорінно. Оскільки при вже встановленій сесія користувача в домені зміна пароля не розриває з'єднання, у адміністраторі була змога відключити усе мережевого обладнання яке веде назовні.

На основі отриманої інформації можна скласти часову пряму наведу у таблиці 3.3, інтерактивний таймлайн наведено у Додатку А.

Таблиця 3.4 – Часова пряма

Час	Подія
2022-03-05 13:36:45	DESKTOP-4722KB0 назва системи, що спостерігається в журналах VPN, отримує доступ до різних внутрішніх систем
2022-03-07 01:52:37	kv-term, обліковий запис "Оператор", створений за допомогою Impacket та WMI, LSASS дампінг. WMI спостерігається по всьому навколишньому середовищу.
2022-03-07 09:04:38	kv-lyn, HackTool:Win32/DumpLsass.A спостерігається на декількох системах.
2022-03-07 13:27:41	kv-itrep, кілька пйаплайних команд, які відображають Impacket Activity, виконуються на різних системах.
2022-03-07 13:55:22	Kv-term, Impacket “cmd.exe /Q /c net user Operator delete”
2022-03-22 15:17:44	ho-le11-n188, IP Activity, пов'язана з APT-угрупованням ACTINIUM, зазначила, що в першу чергу націлена на українські суб'єкти господарювання.
2022-03-24 07:51:27	VNC спостерігається на різних системах
2022-03-26 06:46:36	kv-lyncdi, /dialin/error.aspx. Агент proxy з фреймворку Pivotnacci на різних серверах Exchange.
2022-03-26 06:49:06	kv-ic-shk2, Impacket для створення запланованого завдання для запуску update.bat, запуску "netstat -anbp

Продовження таблиці 3.4

Час	Подія
2022-03-26 18:44:33	kv-ic-shk2, активнсть Impacket, два файли, створені rsa.key & update.bat
2022-03-26 18:51:30	kv-wss-01, Impacket "cmd.exe /Q /c ping 185.82.127.2 -n"
2022-03-26 19:19:20	kv-ic-shk2, створено файл ssh.7z.
2022-03-26 20:00:33	Обліковий запис adm-mfurman rdc додав mfurmandc (Старший адміністратор інфраструктурних сервісів) до групи sensitive Domain Admins (Призначені адміністратори домену).
2022-03-26 20:58:49	KV-DC, goodbye.exe в корзині, пов'язаній з користувачем idemchukdc.
2022-03-26 21:10:18	KV-DC, Створено акаунт idemchukdc та sdudadc від імені mfurmandc. Облікові записи додаються до групи адміністраторів домену.
2022-03-26 22:09:41	DP-EXCH-1, Account adm2-mfurman зареєстрував різні завдання планувальника завдань: "\kDRmEzZe", "\mnTXHtbO" тощо на DP-EXCH-1
2022-03-26 22:28:47	DP-EXCH-1, послуга BTOBTO створюється на різних серверах Exchange.
2022-03-26 22:45:57	DP-DC, файл follow.bat в кошику системи. Також спостерігається в розділі "C:\ProgramData\usertask\".
2022-03-27 00:51:06	KV-DC, спостерігаються різні файли і скрипти: boom.ps1, temp.bat, 123.ps1, allusers[x].txt, gendir.txt, kyiv.txt і т.д. Ці файли були пов'язані з ідентифікатором користувача idemchuckdc

Кінець таблиці 3.4

Час	Подія
2022-03-27 02:31:00	desktop-lhgso0t, temp.bat і temp.ps1 запущено
2022-03-28 01:21:36	виявлено ho-shk1, Meterpreter, інструмент пост-експлуатації.
2022-03-31 09:27:47	KV-TSL, HackTool:Win32/DumpLsass.A і TrojanDownloader:Win32/Bleyr.B спостерігається на KV-TSL, DP-EXCH-1, DP-EXCH-2. Було змінено реєстр, щоб дозволити це.
2022-04-01 11:58:37	hm-ts-w002 створено новий обліковий запис користувача "admin".
2022-04-04 04:14:17	hm-ts-w002, спостерігається ескалація привілеїв за допомогою Sticky Keys. sethc.exe використовувався для створення облікового запису користувача та додавання цього облікового запису до локальної групи адміністраторів. Після цього обліковий запис використовувався для виконання різних дій на пристрої.

Висновок за результатами розслідування. Присутність зловмисника було помічено на етапі активної фази атаки – 26.03.22, у період з 05.03.22 по 25.03.22 система EDR просигналізувала лише про подію ІБ 22.03.22, про схожість ланцюгу дій на пристрої ho-le11-n188 із тактикою угруповання ACTINIUM. Після сканування пристрою антивірусом одним із працівників ІБ було прийнято рішення превстановити ОС на ПК у зв’язку із найденим ШПЗ класифікованим як троян та активатор Windows. Інші події які були висвітлені у аналізі за цей період не були помічені системами як підозрілі. Інцидент отримав статус «Критичного» на момент коли було призначено на роль «Адміністратора домену» скомпрометовані облікові записи idemchukdc та sdudadc від імені акаунту mfurmandc.

На рисунках 3.7, 3.8 продемонстрована реєстрація інцидентів ІБ з використанням MITRE&ATT&CK. У наведеному прикладі надано інформацію по емуляції одного з етапів атаки, а саме створення та видалення облікового запису локального адміністратора.

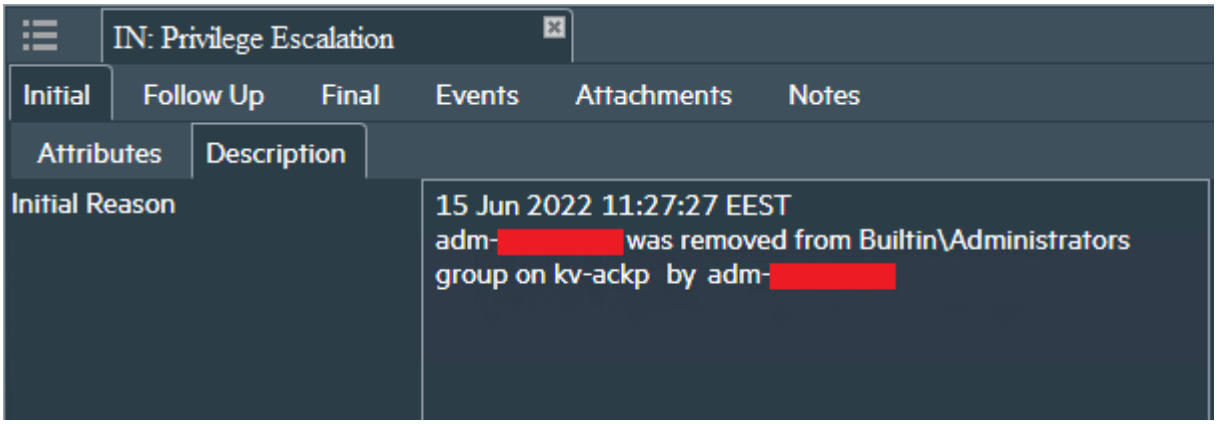


Рисунок 3.7 – Інцидент Privilege Escalation

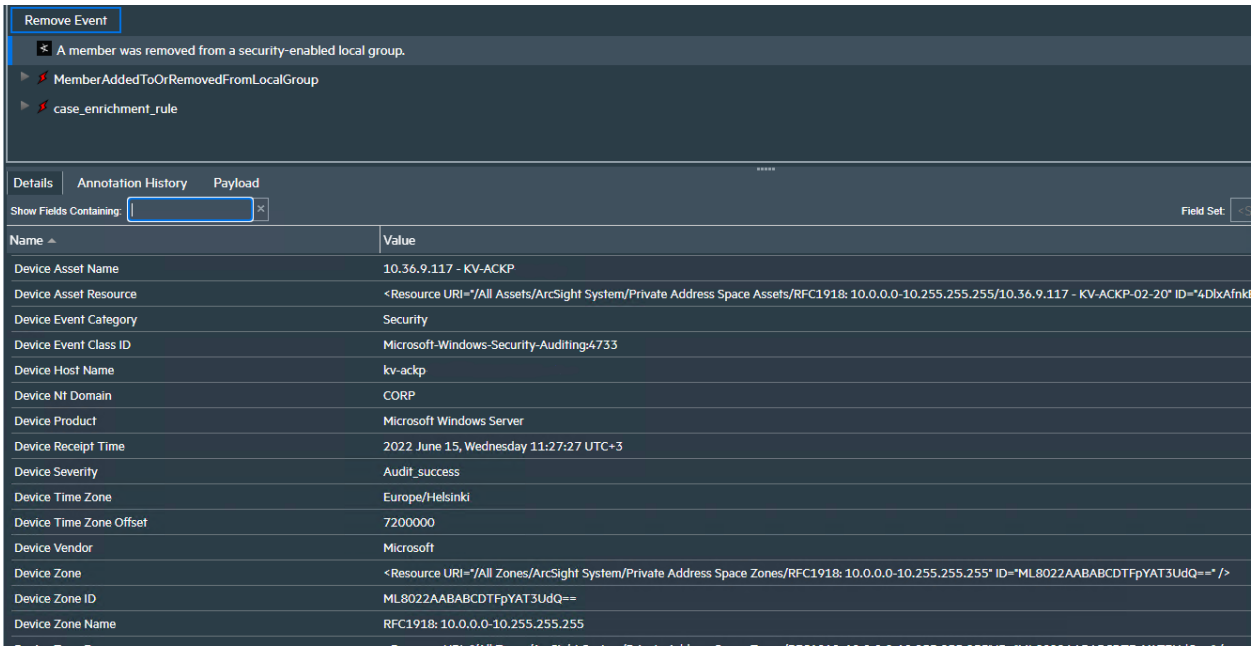


Рисунок 3.8 – Зареєстрована подія Windows 4733

При використанні запропонованого у роботі методу оцінки критичності інцидентів на основі MITRE&ATT&CK та triage, інцидент за 26.03.22 було би виявлено раніше та надано статус критичного. Отже, на підняте у роботі питання, а саме методи прискорення оцінки потенційної критичності інцидентів отримано відповідь, що за допомогою використання MITRE&ATT&CK та практики triage оцінку можна отримати хутчіш за

рахунок більш детального розбиття циклу атаки та реєстрації інцидентів на основі наявних «симптомів».

Висновки до розділу 3

У даному розділі було розроблено метод оцінки потенційної критичності інцидентів на основі практики triage та матриці MITRE&ATT&CK, було наведено правила кореляції системи SIEM для прискорення та підвищення якості оцінки потенційної критичності інцидентів. Було проаналізовано багатоетапну кібератаку та виявлено недоліки у поточній системі там переваги у запропонованому методі оцінки потенційної критичності інцидентів ІБ. Було продемонстровано роботу розроблених правил SIEM.

ВИСНОВКИ

Метою дипломної роботи був пошук методів прискорення оцінки потенційної критичності інцидентів.

В процесі роботи проведено детальне теоретичне дослідження з інформацією з чого складається інцидент, його життєвий цикл та якими інструментами користуються команди SOC дозволило більш детально зрозуміти усю проблематику оцінки критичності інцидентів.

Було проаналізовано та проведено порівняння наявного методу оцінки критичності інцидентів який базується на «Cyberkillchain» та перспективну методологію з використанням матриці MITRE&ATT&CK.

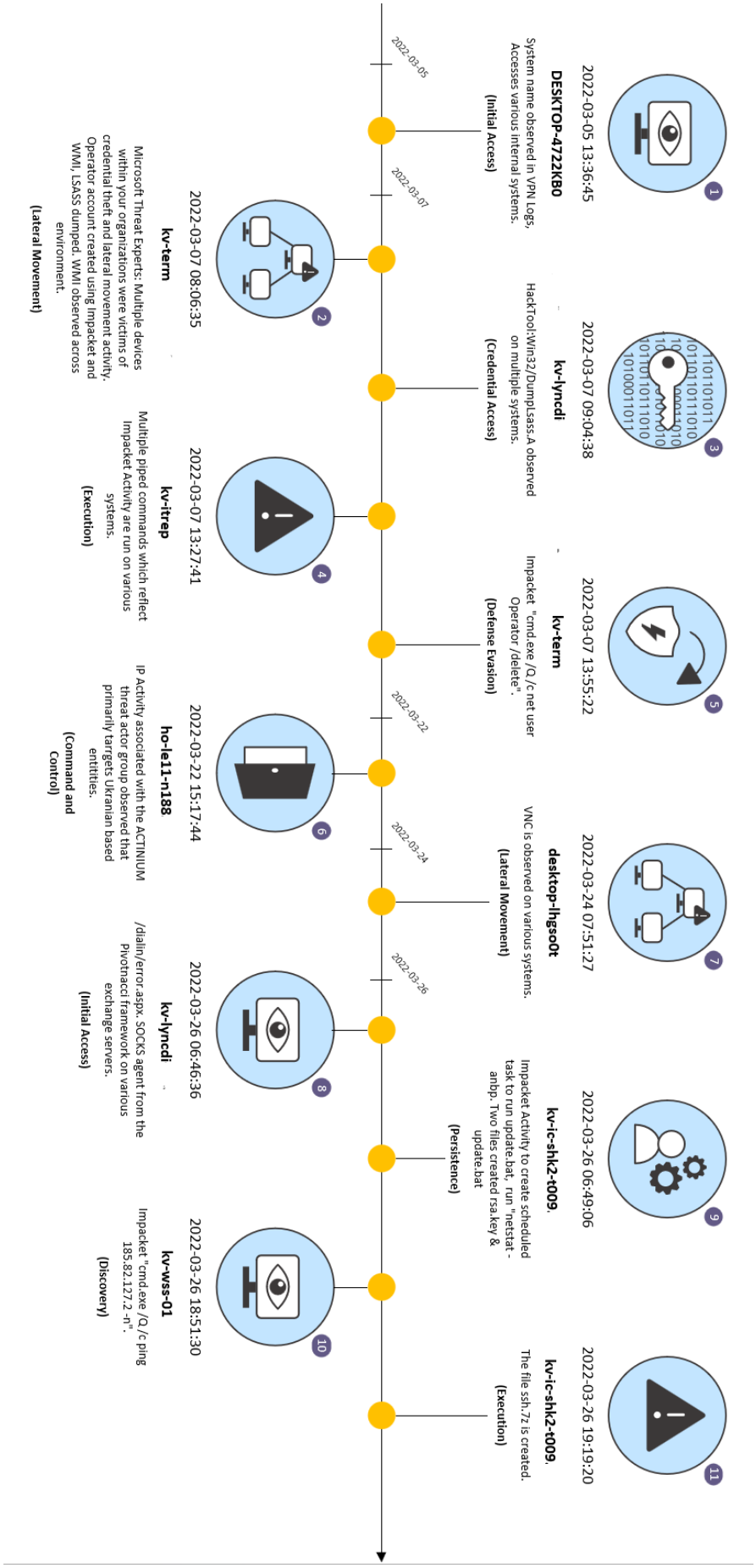
У останній частині роботи продемонстровано реалізацію методу оцінки потенційної критичності інцидентів на основі практики triage та матриці ATT&CK, наведено правила кореляції системи SIEM для прискорення та підвищення якості оцінки потенційної критичності інцидентів на основі розробленого методу. Проаналізовано багатоетапну кібератаку та виявлено недоліки у поточній системі та переваги у запропонованому методі оцінки потенційної критичності інцидентів ІБ. Було продемонстровано роботу розроблених правил SIEM.

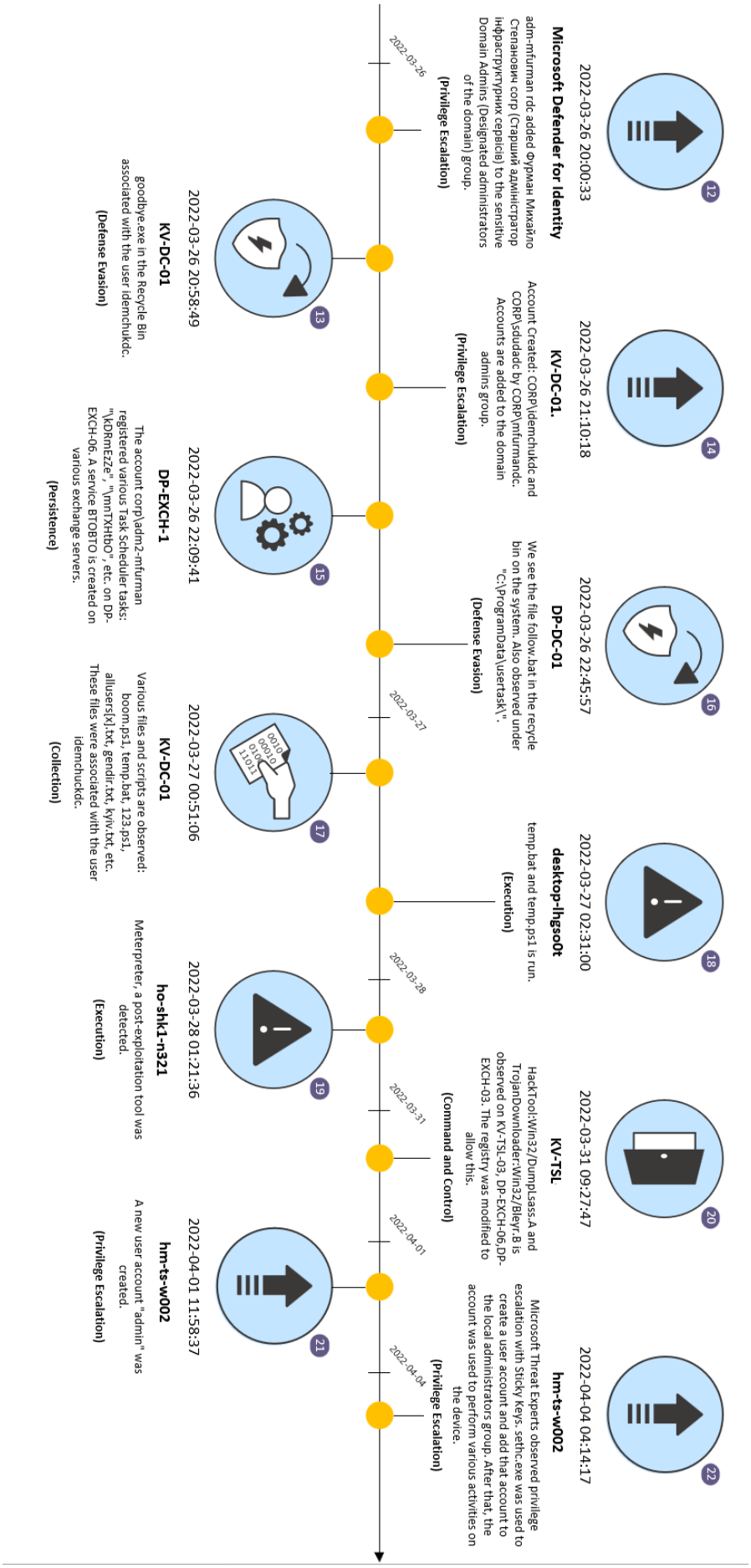
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Реагування на комп'ютерні інциденти: Прикладний курс/ Стів Енсон – 2021
2. Windows Sticky Keys Exploit [Електронний ресурс] Режим доступу до ресурсу: https://hackernoon.com/-windows-sticky-keys-exploit-the-war-veteran-that-never-dies-its-very-likely-that-youve-heard-8ei2duh
3. MITRE&ATT&CK [Електронний ресурс] Режим доступу до ресурсу: https://attack.mitre.org/
4. ISO/IEC 27035:2011[Електронний ресурс] Режим доступу до ресурсу: https://www.iso.org/standard/44379.html
5. ISO/IEC 27035-2:2016[Електронний ресурс] Режим доступу до ресурсу: https://www.iso.org/standard/62071.html
6. Reference Incident Classification Taxonomy/ European Union Agency For Network and Information Security – 2018
7. Computer Security Incident Handling Guide/ Paul Cichonski Tom Millar TimGrance Karen Scarfone – 2012 – Special Publication 800-61 Revision 2
8. Security Incidents: Types of Attacks and Triage Options [Електронний ресурс] Режим доступу до ресурсу: https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/types-of-security-incidents
9. Golden ticket attacks: How they work — and how to defend against them [Електронний ресурс] Режим доступу до ресурсу: https://blog.quest.com/golden-ticket-attacks-how-they-work-and-how-to-defend-against-them/
10. Security Incidents: Types of Attacks and Triage Options [Електронний ресурс] Режим доступу до ресурсу: https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/types-of-security-incidents
11. Управління інцидентами ІБ (конспект лекції) [Електронний ресурс] Режим доступу до ресурсу:

https://www.securityvision.ru/blog/upravlenie-intsidentami-ib-konspekt-lektsii/#

ДОДАТОК А ТАЙМЛАЙН




12
2022-03-26 20:00:33
Microsoft Defender for Identity
adm-mfurman rdc added фурман Михайло Степанович corp (Старший адміністратор інфраструктурних сервісів) to the sensitive Domain Admins (Designated administrators of the domain) group.
(Privilege Escalation)
14
2022-03-26 21:10:18
KV-DC-01.
Account Created: CORP\ademchukdc and CORP\sdudadc by CORP\mfurmandc. Accounts are added to the domain admins group.
(Privilege Escalation)
16
2022-03-26 22:45:57
DP-DC-01
We see the file follow.bat in the recycle bin on the system. Also observed under "C:\ProgramData\usertask\".
(Defense Evasion)
18
2022-03-27 02:31:00
desktop-lhgso0t
temp.bat and temp.ps1 is run.
(Execution)
20
2022-03-31 09:27:47
KV-TSL
HackTool:Win32/DumpLsass.A and TrojanDownloader:Win32/Bleyr.B is observed on KV-TSL-03, DP-EXCH-06,DP-EXCH-03. The registry was modified to allow this.
(Command and Control)
22
2022-04-04 04:14:17
hm-ts-w002
Microsoft Threat Experts observed privilege escalation with Sticky Keys. sethc.exe was used to create a user account and add that account to the local administrators group. After that, the account was used to perform various activities on the device.
(Privilege Escalation)
2022-03-26
2022-03-27
2022-03-28
2022-03-31
2022-04-01
2022-04-04
13
2022-03-26 20:58:49
KV-DC-01
goodbye.exe in the Recycle Bin associated with the user idemchukdc.
(Defense Evasion)
15
2022-03-26 22:09:41
DP-EXCH-1
The account corp\adm2-mfurman registered various Task Scheduler tasks: "\KDRmEZZe", "\mnTXHtbO", etc. on DP-EXCH-06. A service BTOBTO is created on various exchange servers.
(Persistence)
17
2022-03-27 00:51:06
KV-DC-01
Various files and scripts are observed: boom.ps1, temp.bat, 123.ps1, allusers[x].txt, gendir.txt, kyiv.txt, etc. These files were associated with the user idemchuckdc.
(Collection)
19
2022-03-28 01:21:36
ho-shk1-n321
Meterpreter, a post-exploitation tool was detected.
(Execution)
21
2022-04-01 11:58:37
hm-ts-w002
A new user account "admin" was created.
(Privilege Escalation)