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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

“Дослідження шляхів та розроблення рекомендацій щодо розслідування кіберінцидентів в корпоративній інформаційній системі із застосуванням Maltego”

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Олександра ПЄШКОВА
(підпис)

Виконала: здобувачка вищої освіти групи БСД-43

ПЄШКОВА Олександра
(прізвище, ім’я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім’я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім’я)

Київ 2024

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

Кафедра Інформаційної та кібернетичної безпеки

Ступінь вищої освіти Бакалавр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Пєшковій Олександрі Ігорівні
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: “Дослідження шляхів та розроблення рекомендацій щодо розслідування кіберінцидентів в корпоративній інформаційній системі із застосуванням Maltego”

керівник кваліфікаційної роботи Гахов Сергій, к.військ.н., доцент
(прізвище, ім’я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “27” лютого 2024 року № 36.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.06.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Maltego;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз стану та процесу розслідування кіберінцидентів.

2. Дослідження методів та засобів розслідування кіберінцидентів із застосуванням Maltego.

3. Розроблення рекомендацій із застосування Maltego при розслідуванні кіберінцидентів у корпоративній інформаційній системі.

5. Перелік графічного матеріалу

Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності питання розслідування кіберінцидентів.	15.04.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	19.04.2024 р.	
3.	Аналіз методів та засобів розслідування кіберінцидентів.	26.04.2024 р.	
4.	Дослідження технології проведення розслідування кіберінцидентів із застосуванням Maltego.	29.04.2024 р.	
5.	Розробка рекомендацій щодо застосування методів та засобів розслідування кіберінцидентів з використанням Maltego.	01.05.2024 р.	
6.	Оформлення результатів дослідження.	17.05.2024 р.	
7.	Підготовка доповіді до захисту.	31.06.2024 р.	

Здобувачка вищої освіти _____ Олександра ПЄШКОВА
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Сергій ГАХОВ
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувачки ПЄШКОВОЇ Олександри
на тему: «Дослідження шляхів та розроблення рекомендацій щодо розслідування кіберінцидентів в корпоративній інформаційній системі із застосуванням Maltego»

Актуальність: Своєчасне та швидке розслідування кіберінцидентів у корпоративній інформаційній системі є критично важливою складовою реагування на інциденти, кількість та складність яких демонструє тенденцію до зростання. Програмні рішення для розслідування кіберінцидентів спрощують та пришвидшують процес розслідування, таким чином сприяючи вчасному виявленню та нейтралізації кіберзагрози.

Складні кібератаки характеризуються високим ступенем прихованості та здатні завдати значної шкоди матеріальним ресурсам та репутації організації. Відтак тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1 На основі проведеного аналізу, в роботі окреслено зміст проблеми розслідування кіберінцидентів у корпоративній інформаційній системі, описано основні підходи до її вирішення, а також програмне рішення для проведення розслідувань Maltego, його основні компоненти.

2 Досліджено методи та засоби захисту розслідування кіберінцидентів з використанням програмного рішення Maltego.

3 Запропоновано варіант проведення розслідування кіберінциденту в корпоративній інформаційній системі з використанням Maltego на прикладі ботнету Kaiji, активність якого спостерігалася в організації, де здобувачка проходила переддипломну практику, а також запропоновано рекомендації щодо її застосування.

4 Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1 У роботі бажано було б надати компаративний аналіз рішень для розслідувань кіберінцидентів.

2 Представлення процесів функціонування рішення Maltego бажано було б розширити.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувачка **ПЄШКОВА Олександра** – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувачка ПЄШКОВА Олександра до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Дослідження шляхів та розроблення рекомендацій щодо розслідування кіберінцидентів в корпоративній інформаційній системі із застосуванням Maltego».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувачка ***ПЄШКОВА Олександра*** обрала тему роботи, метою якої було дослідити методи та засоби розслідування кіберінцидентів у корпоративній інформаційній системі та розробити рекомендації щодо проведення розслідувань. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ПЄШКОВА Олександра*** показала добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконувала сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувачки ***ПЄШКОВОЇ Олександри*** на оцінку **"добре"** та присвоїти їй кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Сергій ГАХОВ
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка **ПЄШКОВА Олександра** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 51 сторінка, 25 рисунків, 28 джерел.

Об'єкт дослідження – розслідування кіберінцидентів у корпоративній інформаційній системі.

Предмет дослідження – методи та засоби розслідування кіберінцидентів у корпоративній інформаційній системі із застосуванням Maltego.

Мета роботи – розроблення рекомендацій щодо застосування методів та засобів розслідування кіберінцидентів у корпоративній інформаційній системі, які пропонує рішення Maltego, а також рекомендацій щодо їх реалізації.

Методи дослідження – аналіз фахової та наукової літератури, експлуатаційної та технічної документації, українського законодавства та міжнародних стандартів у галузі розслідування кіберінцидентів; виконання дослідно-конструкторської роботи та експериментального розслідування кіберінциденту.

Розслідування кіберінцидентів є важливою складовою реагування на кіберінциденти – одного з процесів, що забезпечує кібербезпеку компанії. Рішення для розслідування кіберінцидентів надають можливість візуального представлення цифрових доказів та їх аналізу, спрощуючи розуміння перебігу кіберінциденту аналітиком.

В роботі проаналізовано проблему розслідування кіберінцидентів у корпоративних інформаційних системах у світі та в Україні, визначено сутність розслідування та підходи до нього, пропоновані міжнародними стандартами. Проаналізовано програмні рішення, які дозволяють виконувати розслідування кіберінцидентів. Проаналізовано методи та засоби розслідування кіберінцидентів у корпоративній інформаційній системі, що пропонуються рішенням Maltego.

Описано призначення, архітектуру й ключові компоненти Maltego, а також основні процеси його функціонування.

На основі вищеописаних досліджень та результатів розслідування реального кіберінциденту розроблено рекомендації фахівцям щодо розслідування кіберінцидентів у корпоративній інформаційній системі з використанням Maltego.

Галузь використання – кібербезпека інформаційної системи організації: реагування на інциденти.

РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ, КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, MALTEGO, МЕТОДИ ТА ЗАСОБИ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ, ПІДХОДИ ДО РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ, ВІЗУАЛЬНИЙ АНАЛІЗ ЦИФРОВИХ ДОКАЗІВ, ISO/IEC 27043, СУТНІСТЬ MALTEGO, ТРАНСФОРМ MALTEGO

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

CTAS – Commercial Transform Application Server

DFIR – Digital Forensics and Incident Response

PDCA – Plan, Do, Check, Act

SIEM – Security Information and Event Monitoring

SOC – Security Operations Center

TDS – Transform Distribution Server

ВСТУП

Актуальність дослідження. Швидкі темпи глобалізації та цифровізації, а також загострення геополітичних протиріч у сучасному світі спричинюють стійке зростання активності кіберзлочинців. Характер, стиль та методи кіберзлочинів зазнають постійної трансформації, стаючи все більш витонченими та довершеними. Розширення спектру інформаційних та мережевих послуг, розвиток кіберфізичних систем та інтернету речей, виникнення нових технологій стимулюють появу нових видів злочинів.

На жаль, кіберзлочини характеризуються досить високим ступенем прихованості – більшість з них навіть не реєструється. При цьому темпи розвитку методів та засобів цифрової криміналістики значно випереджають появу експертних теоретичних та методичних розробок, а також розвиток та вдосконалення законодавчого регулювання цієї сфери.

З урахуванням цього особливого значення набуває теоретичне та практичне дослідження методів та засобів розслідування кіберінцидентів у корпоративних інформаційних системах. У фокусі цифрової криміналістики збір, обробка та зберігання доказів вчинення кіберзлочину. Найпершим етапом розслідування є збір розрізнених даних, які необхідно обробити для одержання з них цінної інформації щодо перебігу злочину та можливих його наслідків. Від успіху цього етапу залежить подальше розслідування, тому використання наукових підходів та найкращих програмних рішень для збору та обробки даних є критичним.

Рішення для розслідування кіберінцидентів, що полегшують збір та обробку даних, дозволяють простежити логічні зв’язки між різними сутностями, а також згрупувати їх та виявити найважливіші за певними ознаками. Поєднуючи такі рішення з засобами реєстрації мережевої активності, активності користувачів на пристроях, дампу оперативної пам’яті та жорсткого диску тощо, фахівці з кібербезпеки можуть отримати цілісну картину розгортання кіберінциденту та розробити вчасні й адекватні заходи стримування загрози, відновлення

скомпрометованих інформаційних систем та подальшого запобігання аналогічним інцидентам у майбутньому.

Вищеописане визначає актуальність теми цієї кваліфікаційної роботи, основний зміст якої становлять дослідження методів та засобів розслідування кіберінцидентів у корпоративній інформаційній системі із застосуванням Maltego.

Об'єкт дослідження – розслідування кіберінцидентів у корпоративній інформаційній системі.

Предмет дослідження – методи та засоби розслідування кіберінцидентів у корпоративній інформаційній системі із застосуванням Maltego.

Метою роботи є розроблення рекомендацій щодо застосування методів та засобів розслідування кіберінцидентів у корпоративній інформаційній системі, які пропонує рішення Maltego, а також рекомендацій щодо їх реалізації.

Наукові завдання:

дослідити сутність проблеми розслідування кіберінцидентів у корпоративній інформаційній системі;

проаналізувати основні підходи до розслідування кіберінцидентів у корпоративній інформаційній системі;

проаналізувати існуючі рішення, що дозволяють виконувати збір, впорядкування та обробку даних під час проведення розслідування кіберінциденту в корпоративній інформаційній системі;

проаналізувати методи та засоби розслідування кіберінцидентів у корпоративній інформаційній системі, що пропонуються рішенням Maltego;

розробити рекомендації щодо застосування методів та засобів розслідування кіберінцидентів, що пропонуються Maltego.

Методи дослідження – аналіз фахової та наукової літератури, експлуатаційної та технічної документації, українського законодавства та міжнародних стандартів у галузі розслідування кіберінцидентів; виконання дослідно-конструкторської роботи та експериментального розслідування кіберінциденту.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів розслідування кіберінцидентів, а також рекомендації фахівцям з цифрової криміналістики та реагування на інциденти щодо реалізації цих методів та засобів.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

1.1 Дослідження стану та процесу розслідування кіберінцидентів

У сучасному світі організації, установи та підприємства дедалі частіше покладаються на інформаційно-комунікаційні системи для здійснення повсякденної діяльності та досягнення цілей. Пандемія COVID-19 та загострення геополітичних конфліктів в усьому світі сприяли тому, що люди почали працювати вдома, що прискорило впровадження рішень на основі моделі “as-a-service”, розбудову інфраструктури з використанням хмарних обчислень, віртуалізацію робочих місць тощо. Ускладнення та диверсифікація програмних та апаратних рішень призвела до збільшення поверхні атаки. Як зазначають дослідники Recorded Future та Insikt Group, у 2023 році кіберзлочинці все активніше експлуатували вразливості в програмних продуктах третіх осіб, які дозволяли скомпрометувати декілька корпоративних середовищ.

Також було відзначено зростання складності атак на ланцюг постачання та частіше використання довірених веб-сервісів та застосунків для приховування активності в інфраструктурі організації, установи чи підприємства. Окрім цього, дослідники зафіксували підвищення зловмисної активності на серверах з встановленими операційними системами Linux та MacOS, що вказує на розробку кіберзлочинцями кросплатформенного зловмисного програмного забезпечення, яке дозволить охопити більшу кількість потенційних жертв.

Спостерігається й поява нових загроз. Так, аналітики безпеки зіткнулися з новими викликами, серед яких більш інтенсивні та переконливі атаки соціальної інженерії, здійснювані з використанням штучного інтелекту [6, с. 2].

Розглянуті вище загрози транслюються у високі ризики. За даними IBM, у 2023 році середня вартість витоку даних склала 4,45 млн доларів, що на 15% вище, ніж за три попередні роки [9]. 83% організацій, що належать до критичної інфраструктури, відзначили, що зіткнулися зі спробами несанкціонованого доступу до даних протягом останніх трьох років [10]. При цьому лише 51% організацій готовий збільшувати витрати на DFIR (Digital Forensics and Incident Response, цифрова криміналістика та реагування на інциденти) та покращення організаційних і програмно-апаратних засобів захисту [9].

Аналізуючи швидку еволюцію загроз та зростання ризиків, деякі дослідники характеризують стан розслідування кіберінцидентів як невідповідний викликам сучасності. Так, аналітики IDC та Binalyze вказують, що в середньому розслідування кіберінциденту триває 26,1 дня, і додатково ще 17,1 дня витрачається на відновлення після нього. Таку повільність пов’язують з багатьма факторами, серед яких складність отримання даних з віддалених кінцевих точок, необхідність проведення віддаленого розслідування, нестача засобів автоматизації, збір доказів з різнорідних джерел, труднощі при роботі з різноманітними програмними рішеннями, організації процесу розслідування, аналізу доказів, документування тощо. 81% організацій відзначив нестачу кваліфікованих кадрів як найкритичнішу проблему при розслідуванні кіберінцидентів [11].

Гостроту проблеми розслідування кіберінцидентів в Україні демонструє звіт Державного центру кіберзахисту щодо роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: протягом 2023 року за допомогою засобів Системи було опрацьовано 18 мільярдів подій, виявлено 133 мільйони підозрілих подій інформаційної безпеки та опрацьовано 148 тисяч критичних подій інформаційної безпеки. Крім того, аналітиками безпеки було зафіксовано та оброблено 1105 кіберінцидентів, що на 62,5% більше, ніж у 2022 році (рис. 1.1) [1].

Рис. 1.1. Події та інциденти інформаційної безпеки, опрацьовані Державним центром кіберзахисту [1]

Розглянутий стан проблеми розслідування кіберінцидентів вимагає дослідження сучасних підходів до розслідування.

1.2 Дослідження підходів до розслідування кіберінцидентів

Розслідування кіберінцидентів є інтегральною складовою процесу управління інцидентами, який регламентується значною кількістю нормативних документів та стандартів: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27035, ISO/IEC 27043, ISO/IEC TR 18044, CMU/SEI-2004-TR-015, NIST SP 800-61, NIST SP 800-12, ITU-T E.409, RFC 2350 та інші.

У міжнародному стандарті ISO/IEC 27002 інцидент інформаційної безпеки або кіберінцидент визначається як одна або декілька взаємопов'язаних подій інформаційної безпеки, які є потенційно шкідливими для активів або бізнес-процесів організації [15, с. 3]. Події інформаційної безпеки в свою чергу являють собою порушення конфіденційності, цілісності та/або доступності інформації чи порушення функціонування засобів захисту. Відтак розслідування кіберінцидентів — це процес збору, аналізу, оцінки та документування доказів з метою подальшого встановлення порядку настання подій інформаційної безпеки та пояснення причин виникнення кіберінциденту [12, с. 309].

Дослідник Ю. Копитін розширює поняття розслідування кіберінцидентів, визначаючи його як сукупність дій, серед яких підтвердження факту настання інциденту (чи не є даний інцидент результатом невизначених чинників – природних умов або катастроф), збір доказів по інциденту та визначення таких його складових, як:

- причини інциденту;
- об'єкт (інформація відкрита або з обмеженим доступом) та (або) суб'єкт (співробітник фірми, клієнт і т. п.), проти якого спрямовано інцидент;
- місце та час інциденту;
- засоби та заходи для здійснення атаки;
- розмір збитків;
- порушник або група порушників, а також особи, які знали про наміри порушників й намагалися приховати сліди інциденту;
- мета порушення;
- причини, що могли послугувати для успішної реалізації атаки;
- відповідні дисциплінарні стягнення [3, с. 61].

Ці дії корелюються з підходом, пропонованим стандартом NIST SP 800-61, у якому визначаються чотири базові етапи розслідування інцидентів:

1. Збір даних. На цьому етапі визначаються, розмічуються, збираються та документуються дані з релевантних джерел з дотриманням вимог до збереження цілісності даних.

2. Дослідження даних. На цьому етапі виконується обробка зібраних даних з метою відбору інформації, необхідної для розуміння причин та перебігу кіберінциденту.

3. Аналіз даних. На цьому етапі виконується аналіз результатів попереднього етапу та визначення складових та особливостей кіберінциденту.

4. Складання звітності. На цьому етапі результати розслідування оформлюються у вигляді звіту, у якому, окрім опису дій аналітиків та застосовуваних ними методів та інструментів, надаються рекомендації щодо відновлення після кіберінциденту, запобігання подібним інцидентам у майбутньому та покращення самого процесу розслідування [23, с. 2-2].

Більш деталізований підхід до розслідування інцидентів пропонується в міжнародному стандарті ISO/IEC 27043, який прийнято в Україні як ДСТУ ISO/IEC 27043:2016. Слідуючи моделі PDCA, яка покладена в основу всіх стандартів серії ISO/IEC, що регламентують кібербезпеку, ISO/IEC 27043 декомпозує процес розслідування кіберінцидентів на окремі процеси, які утворюють п’ять класів: підготовчі процеси (Readiness processes), початкові процеси (Initialization processes), процеси збору інформації (Acquisitive processes), процеси розслідування (Investigative processes), одночасні процеси (Concurrent processes).

Підготовчі процеси виконуються до появи кіберінциденту. Їх призначення – забезпечення готовності систем захисту та персоналу до реагування на потенційний інцидент. До підготовчих процесів належать визначення сценарію атаки та потенційних джерел цифрових доказів, планування порядку збору, обробки та зберігання доказів та їх аналізу, планування виявлення інциденту, визначення та імплементація архітектури системи тощо.

До початкових процесів належать ті, які передують розслідуванню. Серед них виявлення інциденту, перше реагування (first reponse), планування та підготовка.

Процеси збору інформації стосуються виявлення та збору цифрових доказів. До цього класу відносяться процеси виявлення, збору, транспортування та зберігання потенційних доказів.

Процеси розслідування є ключовими у загальному процесі розслідування кіберінцидентів. В рамках цього класу виконуються процеси дослідження та аналізу даних, зібраних у ході виконання процесів класу збору, інтерпретації доказів, звітності, представлення звітності та закриття розслідування.

Окремим класом є клас одночасних процесів. Їх особливістю є порядок перебігу: вони виконуються одночасно з процесами інших класів, а не послідовно. При цьому вони не обов’язково мають слідувати один за одним. Серед таких процесів отримання дозволів на провадження робіт з розслідування, документування, управління інформаційним потоком, зберігання ланцюга передачі інформації (chain of custody) та цифрових доказів, взаємодія з фізичним розслідуванням (interaction with physical investigation).

Загальне співвідношення процесів представлено на рисунку 1.2 [16, с. 5-7].

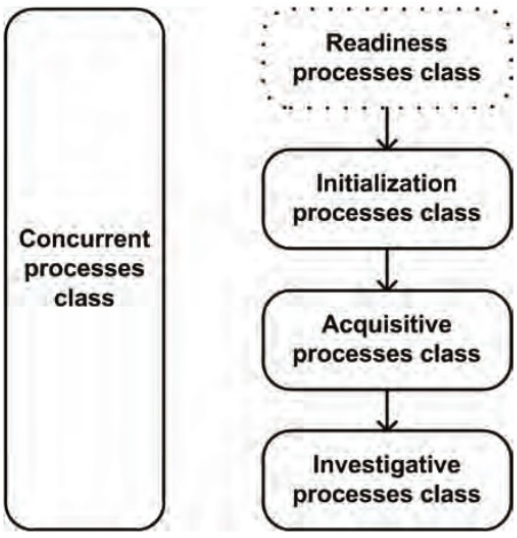

Рис. 1.2. Класи процесів розслідування кіберінцидентів згідно з міжнародним стандартом ISO/IEC 27043 [16, с. 5-7]

Як бачимо, у підходах до розслідування кіберінцидентів, пропонованих міжнародними стандартами, важливу роль відведено процесам аналізу потенційних цифрових доказів. Відтак наші подальші дослідження будуть сфокусовані саме на цих процесах, охоплюючи програмні рішення, які можуть бути застосовані для виконання аналізу.

1.3 Дослідження існуючих рішень для розслідування кіберінцидентів

На ринку пропонується ряд рішень для спрощення збору, впорядкування та аналізу цифрових доказів. Серед найбільш відомих – програмні рішення SpiderFoot, Lampyre, Palantir, i2 Analyst's Notebook, Maltego [4].

Рішення SpiderFoot є інструментом автоматизації збору та аналізу даних, яке отримує інформацію з більш ніж 100 публічних джерел та представляє дані у вигляді, зручному для виконання аналізу та пошуку зв'язків між об'єктами. Функціонал рішення може бути розширеним за рахунок модулів. SpiderFoot має комерційну версію та версію з відкритим вихідним кодом. На відміну від версії з відкритим вихідним кодом комерційна версія працює в хмарі та має розширені можливості керування збором даних та їх візуалізацією. Рішення створене з використанням мови програмування Python [7].

Рішення Lampyre є комерційним і також виконує збір даних з більш ніж 100 джерел та представляє їх у вигляді графу, карти або таблиці, з якими можна працювати одночасно. Рішення також пропонує можливість статистичного аналізу даних та аналізу на певному проміжку часу. API рішення створений з використанням мови програмування Python [18].

Компанія Palantir пропонує рішення для аналізу даних з використанням штучного інтелекту для державних органів та фінансових установ – Gotham та Metropolis. Рішення покладаються як на традиційні бази даних та інші структуровані джерела, так і на текстову, аудіо- та відеоінформацію [19, с. 157-158]. Рішення Gotham призначене для роботи з різнорідними джерелами та використовує техніку онтологій, тоді як Metropolis сфокусоване на числових даних та виявлення аномалій у них [5].

Комерційне рішення i2 Analyst's Notebook є інструментом візуального аналізу, що дозволяє збирати інформацію з різних джерел та налаштовувати способи її представлення. Рішення має функціонал аналізу соціальних мереж, який дозволяє застосовувати математичний інструментарій для виявлення ключових сутностей та їх групування. Функціонал i2 Analyst's Notebook може бути розширений за рахунок інтеграції з іншими рішеннями i2 – i2 iBase, i2 Text Chart або i2 Analyze [13].

Рішення Maltego є одним із найпопулярніших на ринку. Окрім звичної візуальної аналітики та збору даних, воно надає можливість обирати, з яких джерел будуть збиратись дані та виконувати їх покрокову обробку. Окрім цього, воно може бути інтегроване з найрізноманітнішими інструментами, від систем обробки тікетів до SIEM-систем. Компанія-постачальник пропонує три варіанти (тарифні плани) рішення: Community-версію, яка є безкоштовною, тарифний план Professional та тарифний план Enterprise, призначений для компаній. Окрім цього, рішення Maltego може бути інтегроване з іншими, які дозволяють використовувати можливості штучного інтелекту для проведення розслідувань [22]. Гнучкість, кросплатформенність, відкритий вихідний код, широкі можливості аналізу даних та активна спільнота користувачів є ключовими факторами, які сприяли вибору саме цього рішення для проведення подальшого дослідження.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ ІЗ ЗАСТОСУВАННЯМ MALTEGO

2.1 Архітектура та компоненти рішення Maltego

Інформація, яку збирає Maltego, представляється у вигляді графу, який демонструє зв’язки між зібраними даними. Відтак ключовими компонентами Maltego є сутності (Entity), трансформи (Transform) та машини (Machine). Деякі фахівці також визначають зв’язки (Links) як суттєвий компонент [2]. Сутність представляє собою деякі дані, які використовуються як вхідні для подальшого збору інформації, що виконується трансформом згідно з характеристикою зв’язку. Трансформи об’єднуються в машини, призначені для випадків, коли інформацію неможливо зібрати з використанням лише одного трансформа [8, с. 124-125].

В основі Maltego лежить клієнт-серверна архітектура: трансформи розгортаються на серверах трансформів (Transform Server, CTAS), які мають доступ до даних, які необхідно зібрати. Підключитися до таких серверів можуть лише сервери поширення трансформів (Transform Distribution Server, TDS). Клієнтські застосунки Maltego отримують доступ до трансформів лише через цей сервер. Взаємодія клієнтів із серверами схематично представлена на рисунку 2.1.

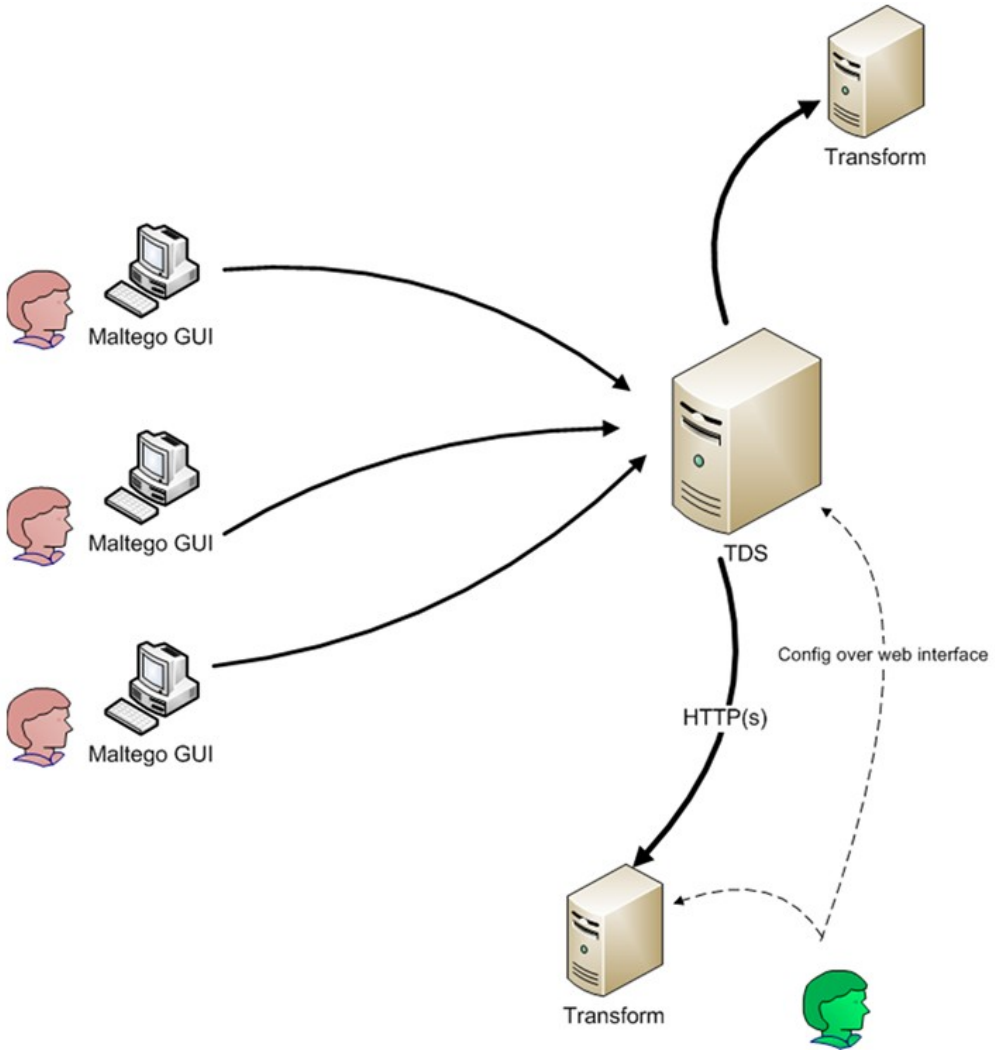

Рис. 2.1. Загальна архітектура рішення Maltego [26]

Сервер поширення трансформів TDS надає клієнтові налаштування трансформів та користувальницьких сутностей та направляє виклики трансформів до серверів, на яких ці трансформи розгорнуті. Код трансформів виконується на відповідному сервері, але налаштовуються вони на TDS.

Коли до клієнтського застосунку додається новий набір трансформів, розпочинається процес пошуку сервера, де встановлено відповідний набір. Клієнт запитує налаштування в TDS і додає новий сервер трансформів до свого списку постачальників трансформів. Таким чином користувач може встановити будь-які трансформи з репозиторію (Transform Hub), вбудованого в Maltego.

Коли користувач виконує трансформ, запит надсилається до відповідного TDS, який перенаправляє його на потрібний сервер [26].

Окрім цього, в інфраструктурі Maltego може бути наявний сервер спільної роботи (Comms Server), призначений для роботи в команді. Цей сервер забезпечує доступність одного графу для всіх аналітиків та надає можливість спілкування через вбудований месенджер [24].

Архітектура серверів Maltego представлена на рисунку 2.2.

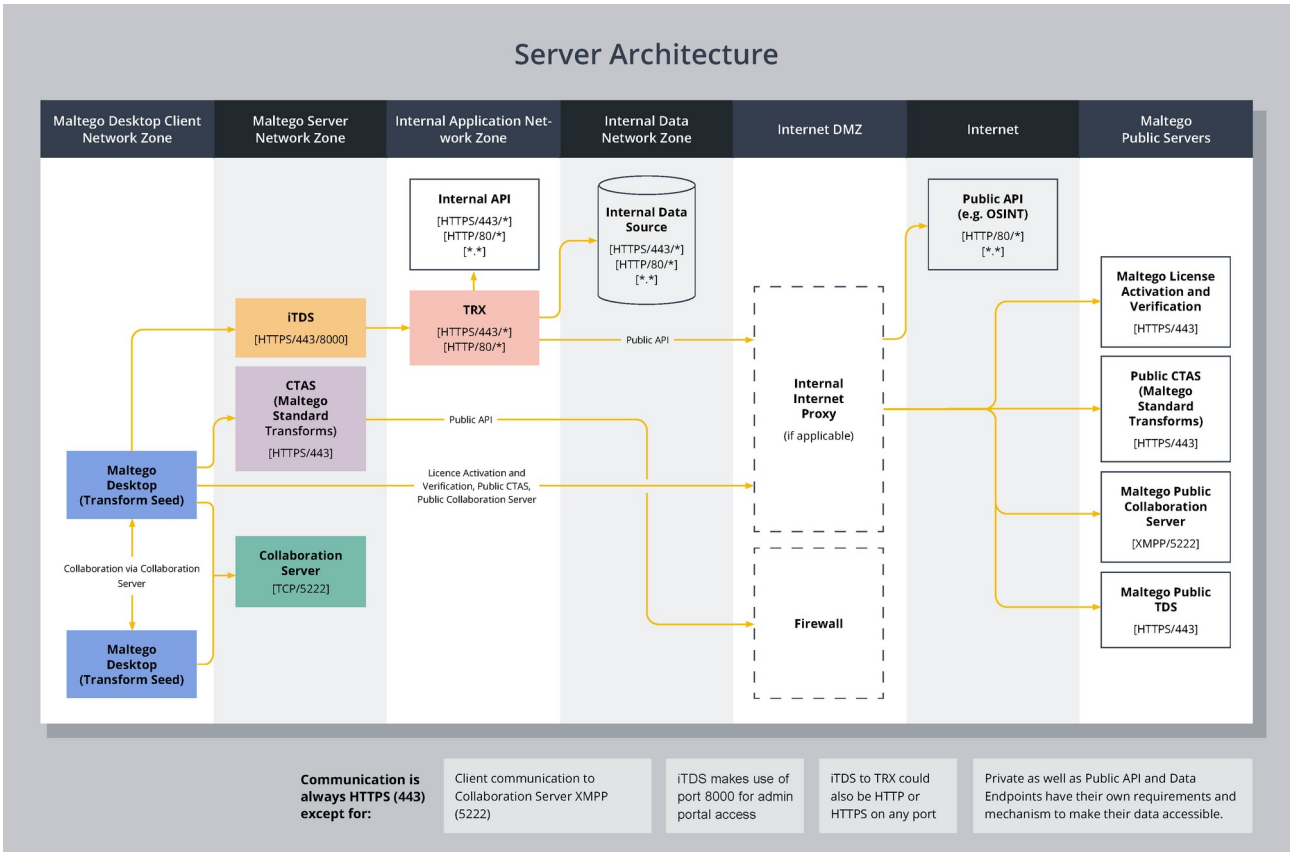

Рис. 2.2. Архітектура серверів Maltego [24]

Аналіз архітектури рішення вимагає більш детального розгляду призначення та основних функцій його компонентів.

2.2 Призначення та основні функції компонентів Maltego

Будь-які розслідування кіберінцидентів у Maltego починаються з сутностей та зв’язків між ними. Сутності представляють інформацію, яка вже є в аналітика. Maltego відображає їх у вигляді вузлів графу. У ході розслідування до сутностей застосовуються трансформи, які дозволяють отримати інші сутності, пов’язані з аналізованою. Так, наприклад, URL-адреса веб-ресурсу може бути “трансформована” в асоційовані з нею IP-адреси. Maltego також може знаходити зв’язки між наявними сутностями, як не були знайдені аналітиком.

Найпростіша сутність являє собою представлення типу ключ-значення. Всього Maltego має 39 стандартних сутностей, поділених на 8 класів. Таблиця 2.1 представляє коротку характеристику всіх доступних сутностей рішення [14].

Таблиця 2.1.

Класифікація сутностей Maltego

Клас сутності	**Тип сутності**	**Характеристика сутності**
Особисті (Personal)	Документ (Document)	Документ, що знаходиться на веб-сервері. Може мати будь-який формат, від PDF до SQL-дампу.
	Номер телефону (Phone number)	Номер телефону фізичної або юридичної особи. Через розбіжність стандартів форматування номерів телефонів у різних країнах Maltego розбиває номер на 4 частини: код країни, код міста, код району та залишок (Rest). Під час обробки номерів трансформи виконують їх пошук у різних варіантах запису.
	Адреса електронної	Адреса електронної пошти, на яку можна надсилати листи.

Клас сутності	Тип сутності	Характеристика сутності
	пошти (E-mail)	
	Зображення (Image)	Візуальне представлення об’єкту, предмету або явища.
	Вислів (Phrase)	Будь-який текст або уривок з тексту. Цей тип сутності дозволяє передавати в трансформ оператори пошукових систем з метою отримання більш релевантної інформації.
	Особа (Person)	Прізвище та ім’я людини.
	Настрій (Sentiment)	Відчуття щодо сутності.
	Псевдонім (Alias)	Нікнейм, ім’я користувача або псевдонім, використовуваний у соціальній мережі. Зазвичай ці дані унікальні для користувача в межах однієї соціальної мережі.
Пристрої (Devices)	Пристрій (Device)	Пристрій, наприклад, камера чи телефон.
Групи (Groups)	Компанія (Company)	Організація, метою якої є отримання прибутку.
	Організація (Organization)	Соціальна група, що розподіляє завдання з метою досягнення спільної мети.
IT-Інфраструктура (Infrastructure)	Банер (Banner)	Текст банера.
	Назва веб-ресурсу (Website Title)	Назва веб-ресурсу.
	Домен (Domain)	Доменне ім’я веб-ресурсу.

Клас сутності	Тип сутності	Характеристика сутності
	MX-запис (MX Record)	DNS-запис для електронного листування.
	Адреса IPv4 (IPv4 Address)	IPv4-адреса веб-ресурсу.
	Гіперпосилання (URL)	Адреса ресурсу в мережі інтернет. Maltego може не повністю відображати гіперпосилання, якщо воно занадто довге.
	FQDN (DNS Name)	Повне доменне ім’я хоста.
	AS	Автономна система в мережі інтернет.
	Код стеження (Tracking Code)	Код, що додається до веб-ресурсів сервісами веб-аналітики (Google Analytics, AdWords та інші).
	Вебсайт (Website)	Вебсайт в мережі інтернет.
	NS-запис (NS Record)	Запис, який ідентифікує авторитетний сервер імен для певного хоста.
	Блок IP-адрес (Netblock)	Блок IP-адрес, виданих для певної автономної системи.
	CVE	Ідентифікатор та оцінка вразливості в базі даних CVE.
	Адреса IPv6 (IPv6 Address)	IPv6-адреса веб-ресурсу.
	Запис WHOIS	Запис доменного імені або IP-адреси в базі

Клас сутності	Тип сутності	Характеристика сутності
	(WHOIS Record)	даних WHOIS.
	SSL-сертифікат (SSL Certificate)	Сертифікат SSL/TLS, використовуваний клієнтами та серверами.
	Блок IP-адрес у форматі CIDR (Netblock CIDR)	Представлення блоку IP-адрес, виданих для певної автономної системи, у форматі CIDR.
Локації (Locations)	GPS-координати (GPS Coordinate)	Локація на планеті Земля, визначена з використанням Всесвітньої геодезичної системи.
	Колова площа (Circular Area)	Локація на планеті Земля, окреслена колом з визначеним радіусом.
	Повна адреса локації (Nominatim Location)	Повна адреса локації.
	Локація (Location)	Локація на планеті Земля. Від повної адреси локації відрізняється більшою кількістю даних (включається місто, область та країна, а також поштовий індекс).
Шкідливе ПЗ (Malware)	Хеш (Hash)	Хеш файлу, що пов’язаний зі шкідливим програмним забезпеченням.
Тестування на проникнення (Penetration Testing)	Порт (Port)	Номер порту TCP/UDP.
	Служба (Service)	Служба (поєднання порту й банера).
	Технологія за BuiltWith	Технологія, покладена в основу веб-ресурсу та визначена за допомогою сервісу BuiltWith.com.

Клас сутності	Тип сутності	Характеристика сутності
	(BuiltWith Technology)	
	Зв’язок за BuiltWith (BuiltWith Relationship)	Зв’язок, визначений за допомогою сервісу BuiltWith.com.
Соціальна мережа (Social Network)	Обліковий запис Flickr (Affiliation – Flickr)	Наявність облікового запису в соціальній мережі Flickr.
	Хештег (Hashtag)	Хештег Twitter/X.
	Обліковий запис Twitter (Affiliation – Twitter)	Наявність облікового запису в соціальній мережі Twitter/X.
	Обліковий запис (Affiliation)	Наявність облікового запису в соціальній мережі.
	Твіт (Tweet)	Пост у соціальній мережі Twitter/X.
	Список користувачів Twitter (Twitter User List)	Список користувачів Twitter List.

Сутності обробляються за допомогою трансформів, які можуть бути написані будь-якою мовою програмування, однак зазвичай пишуться мовою Python. Трансформи створюються з дотриманням двох базових вимог:

- розширюваність (представлення інформації має бути зручним для використання в інших трансформах);
- атомарність (трансформ повинен повертати найменшу можливу частину інформації). Така вимога ставиться з метою забезпечення гнучкості аналізу зв'язків між сутностями, що з'являються в результаті роботи трансформу.

Трансформи можуть реєструватися в застосунку з використанням серверів поширення трансформів або бути розгорнутими локально. Другий варіант рекомендується, якщо є необхідність виконувати операції, що є специфічними для обладнання. Перший варіант дозволяє розпочати роботу з Maltego без додаткових витрат часу.

Під час виконання трансформу клієнт звертається із запитом до TDS, надсилаючи йому ім'я трансформу, сід та вхідну сутність. TDS виконує пошук необхідного трансформу та пересилає запит до сервера трансформів.

Сервери поширення трансформів можуть бути публічними – доступними будь-кому – та внутрішніми (Internal TDS, iTDS), доступними лише співробітникам компанії, яка їх розгорнула. Внутрішні TDS рекомендовано використовувати, якщо Maltego обробляє чутливі дані компанії, які не можуть бути передані на обробку третім особам. iTDS надає можливість управляти:

- налаштуваннями та параметрами трансформів;
- сідами – функціоналом, що пов'язує в один пакет трансформи та їх налаштування (сутності, іконки, набори трансформів та машини);
- налаштуваннями OAuth для трансформів;
- користувальницькими сутностями;
- резервним копіюванням трансформів та їх налаштувань.

Внутрішній TDS може бути розгорнутий як образ Docker або віртуальна машина на основі Ubuntu або Debian [28].

Для виконання трансформів або машин TDS звертаються до серверів трансформів (Commercial Transform Application Server, CTAS). На таких серверах розгорнуті трансформи, які виконують запити до DNS-серверів, пошукових систем, соціальних мереж, інтерфейсів програмування застосунків (API), баз даних та інших джерел. Якщо компанія використовує в ході розслідування кіберінцидентів чутливі дані, сервер CTAS може бути розгорнутий як внутрішній сервер. Сервер поставляється як образ Docker [27].

Далі дослідимо основні процеси функціонування рішення Maltego, у яких задіяні описані компоненти та які будуть використані в ході подальшого дослідження.

2.3 Процеси функціонування рішення Maltego

Оскільки Maltego покладається на мережеву інфраструктуру, для його використання необхідна реєстрація на сайті постачальника рішення, а при першому запуску – вхід до облікового запису. Початкове вікно Maltego (Home) виглядає так, як представлено на рисунку 2.3.

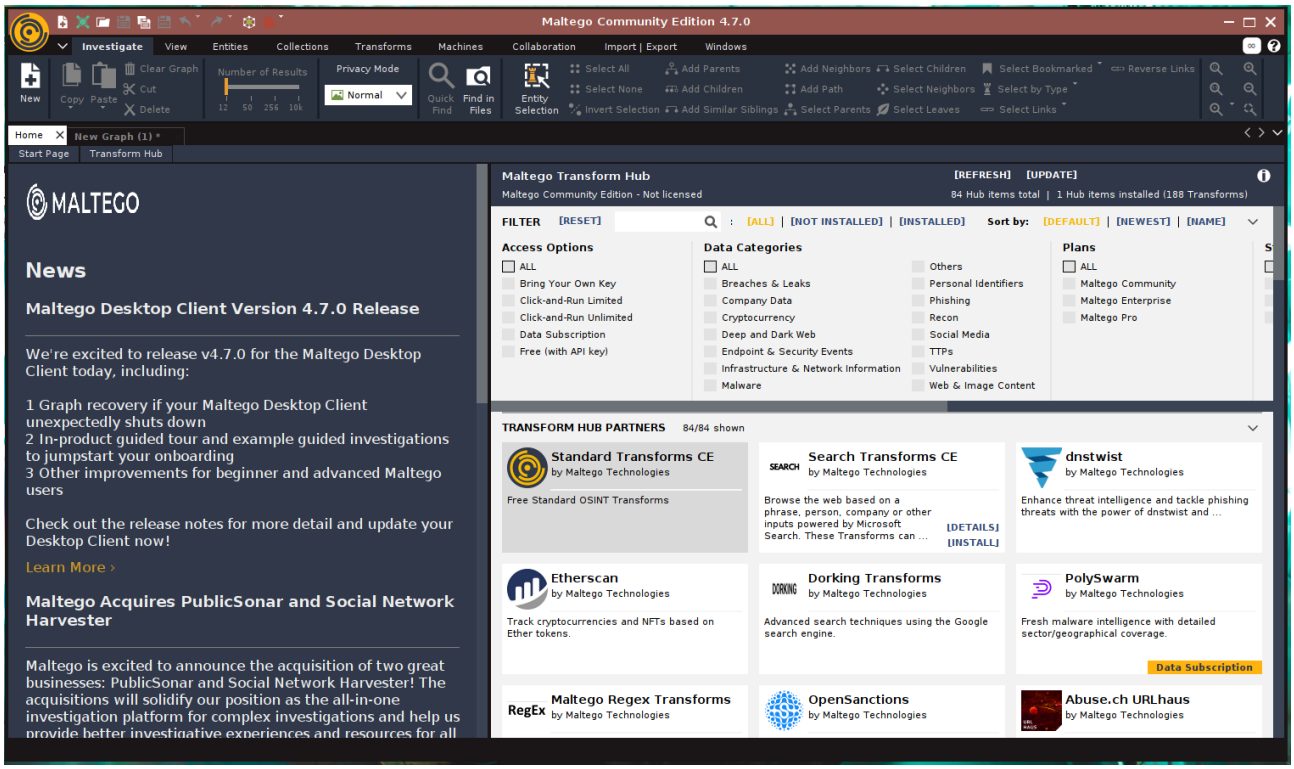

Рис. 2.3. Початкове вікно Maltego

У цьому вікні представлено новини від компанії Paterva, а також усі набори трансформів, доступні на її серверах – Transform Hub. Представлена можливість фільтрації наборів трансформів за їх особливостями та можливостями, серед яких:

- варіанти доступу (Access Options), які варіюються від безлімітних до таких, що вимагають підписки. Деякі трансформи можна використовувати лише отримавши API-ключ сервісу, для якого їх розроблено;
- категорії даних (Data Categories). Трансформи маркуються за напрямами діяльності аналітика з кібербезпеки: дослідження витоків даних, аналіз даних компанії, аналіз криптовалют, дослідження даркнету, аналіз сповіщень антивірусних рішень та SIEM-систем тощо. Відповідний фільтр дозволяє підібрати трансформи для конкретної задачі, яку необхідно вирішити аналітикові;

– тарифний план (Plans). Деякі набори трансформів недоступні при використанні Maltego Community Edition. За допомогою цього фільтру можна відібрати ті, які підходять для безкоштовного використання або певного тарифного плану;
– вибір співробітників (Staff Picks). Набори, рекомендовані командою Maltego;
– корисне для команд (Useful for Teams). Набори, підібрані для командної роботи;
– спеціальний доступ (Special Access).

Створення, відкриття та зберігання графів виконується за допомогою іконок управління на верхній (червоній) панелі Maltego. Після створення нового графу відкривається вікно робочої області, як показано на рисунку 2.4.

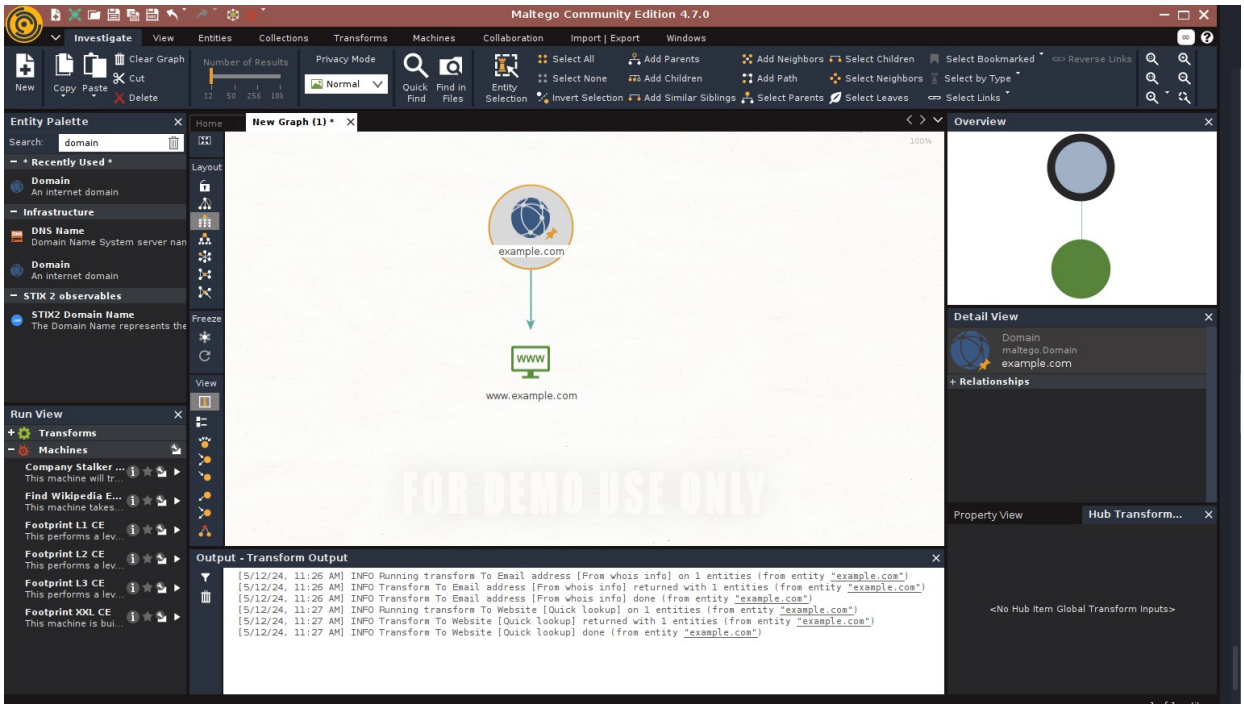

Рис. 2.4. Вікно робочої області Maltego

Крайня зліва панель містить сутності (угорі), трансформи та машини (внизу), які можуть бути виконані для певної сутності. Властивості відображення графу розміщуються справа від нього. Під ним розташоване вікно текстового виводу операцій трансформів. У разі виникнення помилки вона буде відображена в цьому вікні. Зліва розташоване вікно відображення графів (угорі) та вікно властивостей сутностей чи зв’язків (посередині та внизу).

При встановленні Maltego трансформи в рішенні відсутні. Їх необхідно встановити з Transform Hub. Для кожного набору трансформів доступний опис, у якому окрім функціоналу описано й порядок встановлення та використання. Ознайомитися з описом можна, натиснувши на напис [DETAILS] на картці трансформу (рис. 2.5).

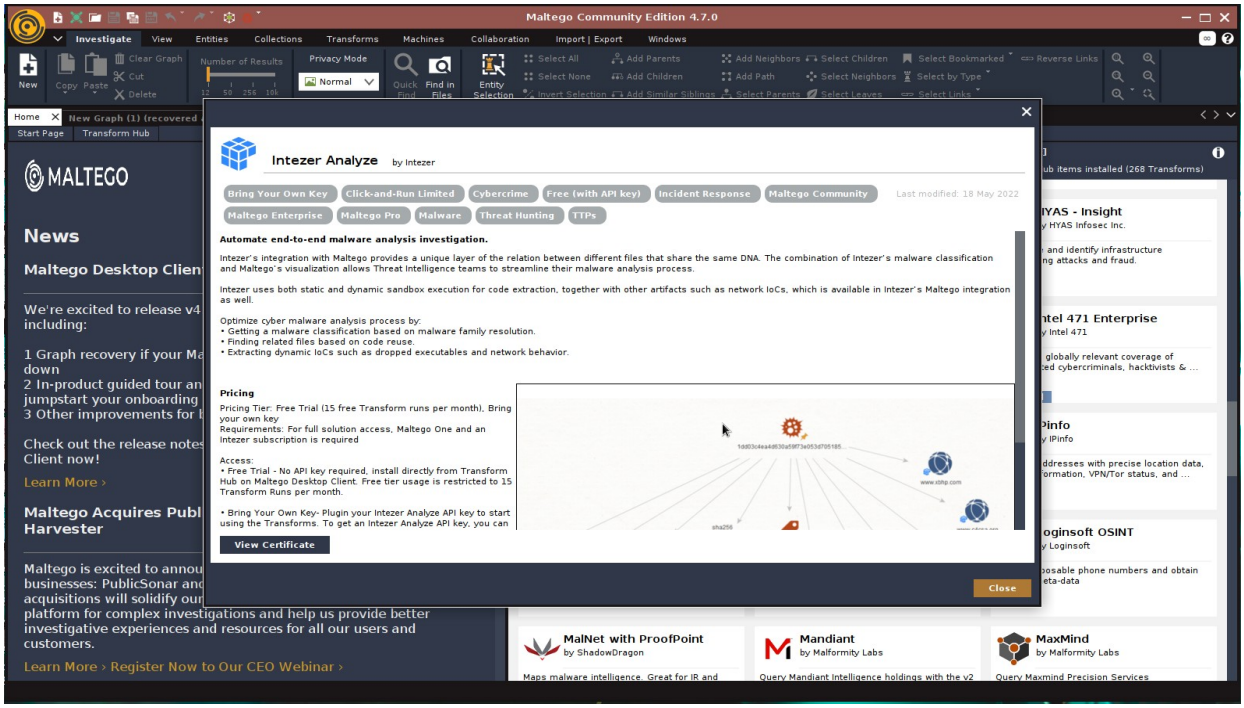

Рис. 2.5. Приклад опису набору трансформів Intezer Analyze

Під час встановлення трансформу може знадобитись API-ключ, який необхідно ввести в спеціальне поле, як показано на рисунку 2.6.

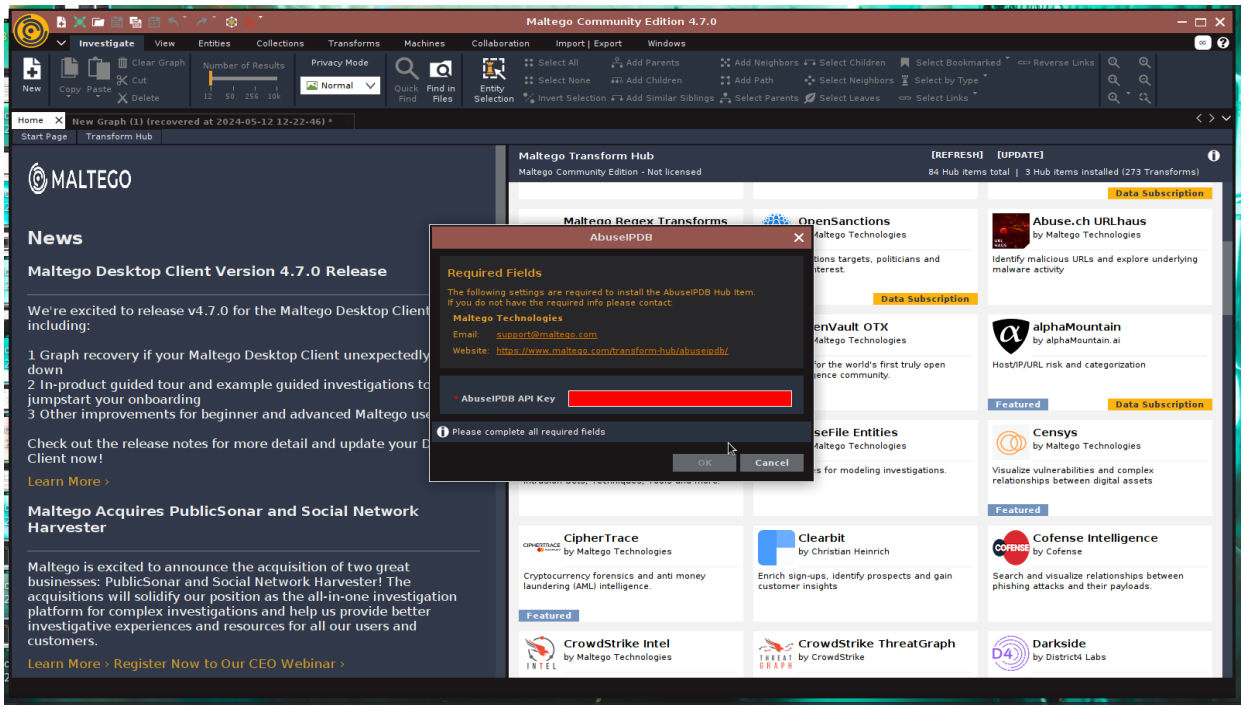

Рис. 2.6. Запит на введення API-ключа сервісу встановлюваного трансформу

Після виконання встановлення Maltego представить звіт щодо результатів виконаної роботи (рис. 2.7).

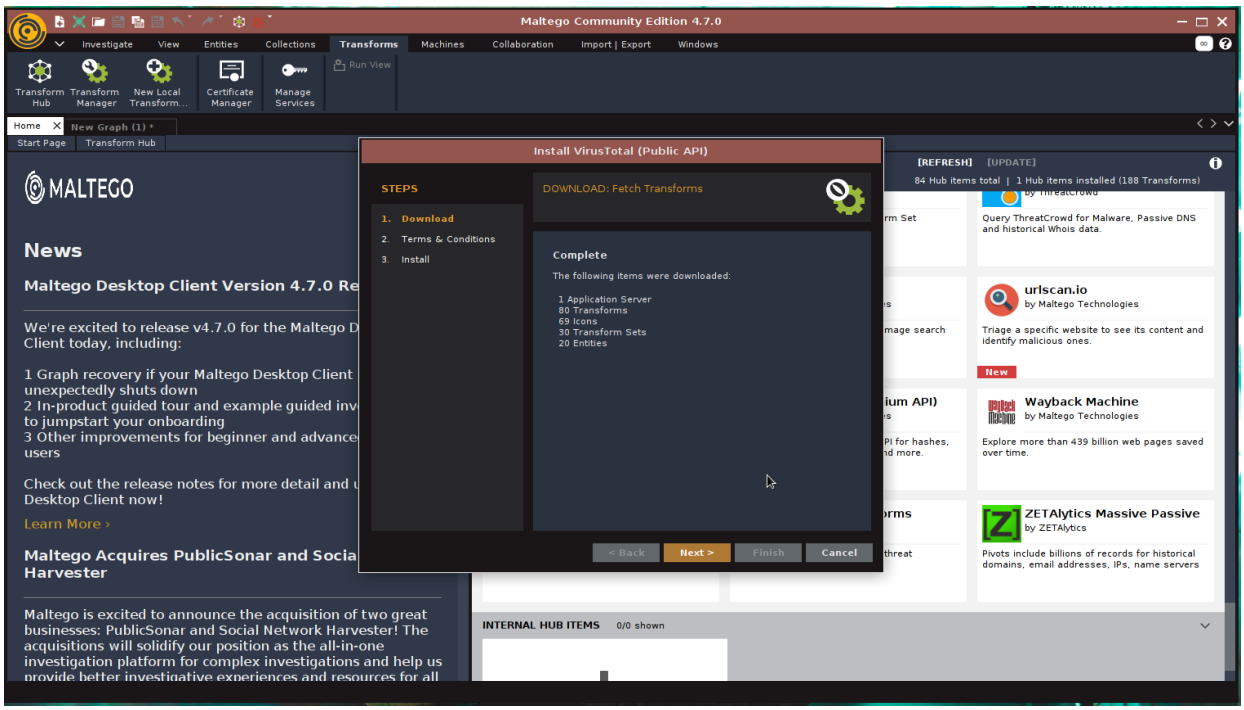

Рис. 2.7. Завершення встановлення набору трансформів

Встановлення локальних трансформів виконується в інакшому порядку. Продемонструємо його на прикладі набору трансформів для інструменту співставлення адреси електронної пошти та соціальних мереж Holehe (рис. 2.8).

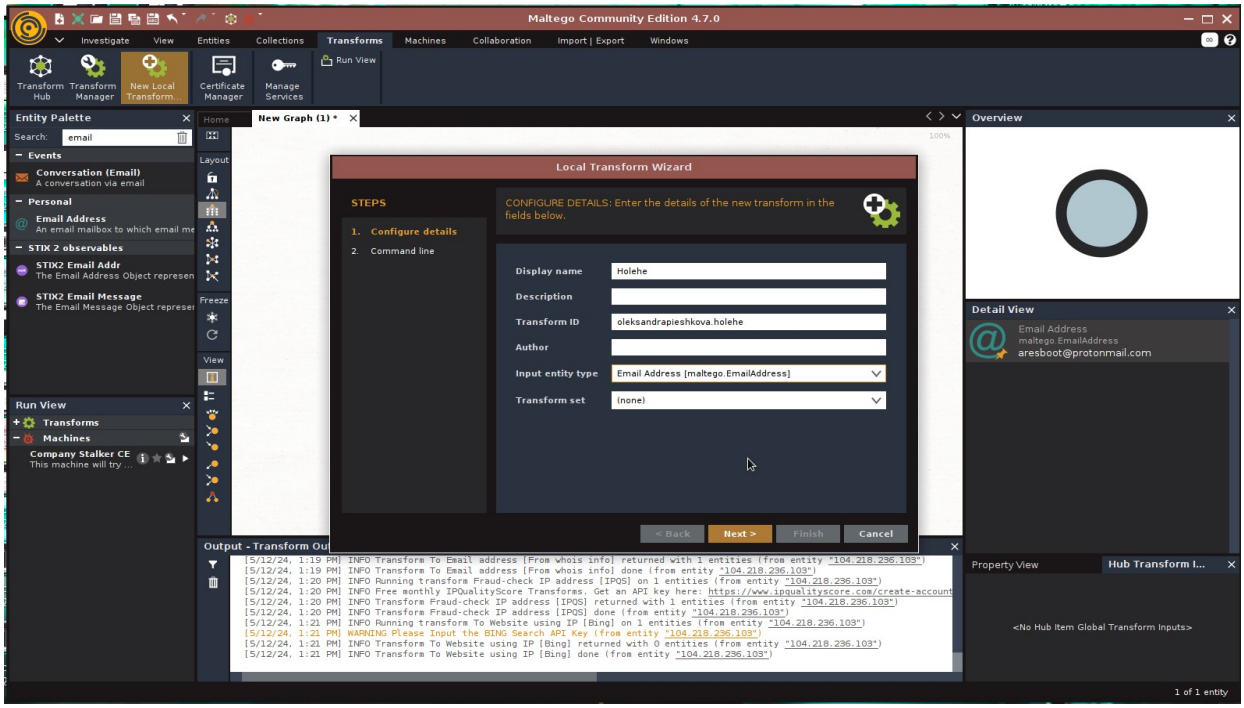

Рис. 2.8. Налаштування локального трансформу

Найперше необхідно визначити загальні налаштування трансформу – його назву, ID та базову сутність. Наступний етап – визначення аргументів командного рядка для нього (рис. 2.9).

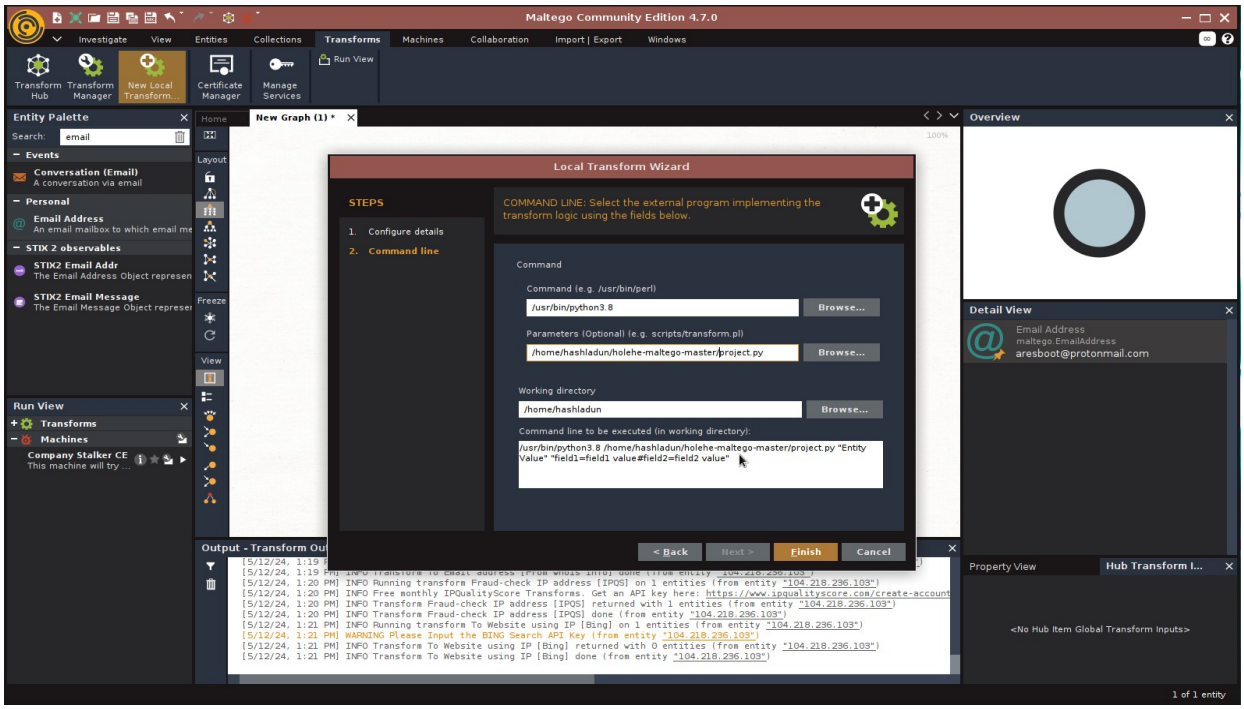

Рис. 2.9. Визначення аргументів командного рядка для локального трансформу

Трансформи для Maltego пишуться переважно мовою програмування Python, тому шлях до виконуваного файлу цієї мови необхідно визначати в полі Command. Поле Parameters відведене для повного шляху до файлів самого трансформу. У полі Working Directory визначається робоча директорія трансформу. Усі представлені налаштування командного рядка можуть бути перевірені в полі Command line to be executed (in working directory).

Якщо при налаштуванні було допущено помилку, виправити її можна в Transform Manager, який доступний на вкладці Transforms (рис. 2.10).

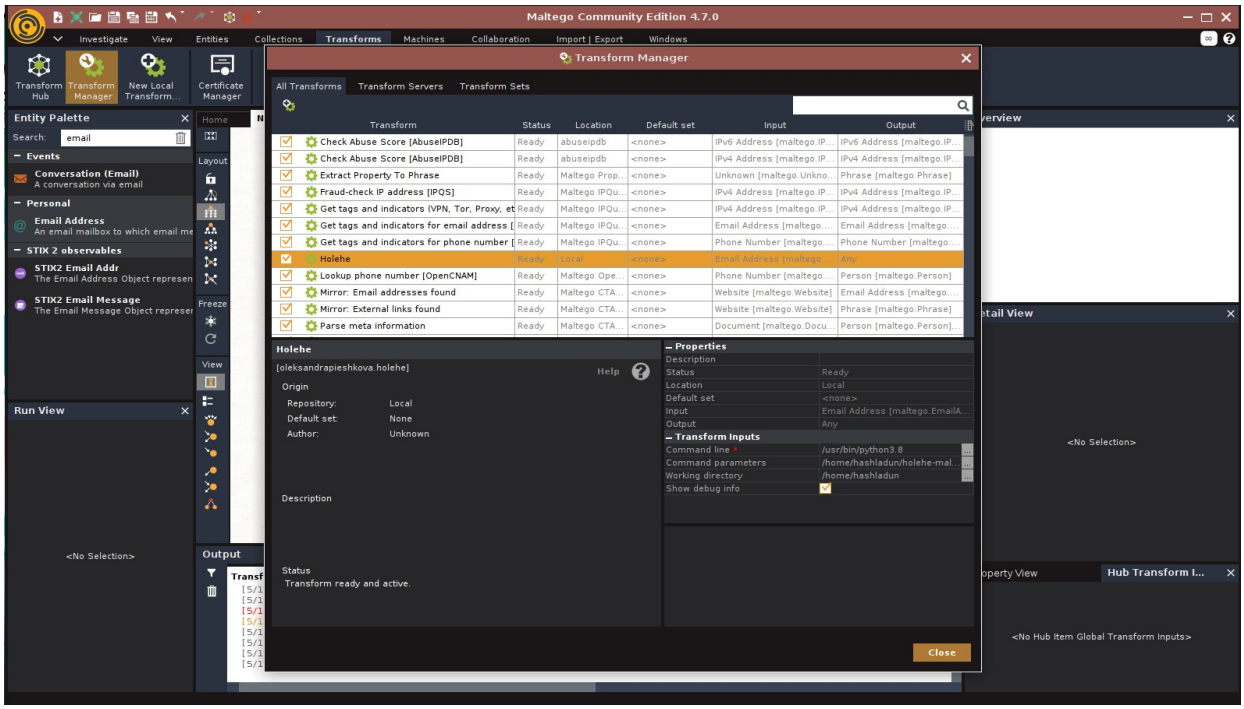

Рис. 2.10. Вікно Transform Manager, що демонструє встановлений трансформ Holehe

Для початку роботи необхідно перетягнути на вікно графу сутність з лівої панелі та замінити дані за замовченням на власні. Далі потрібно клацнути на сутності правою кнопкою миші та обрати зі списку необхідний трансформ або набір трансформів. Трансформи організовані ієрархічно, що дозволяє виконувати їх разом або окремо (рис. 2.11).

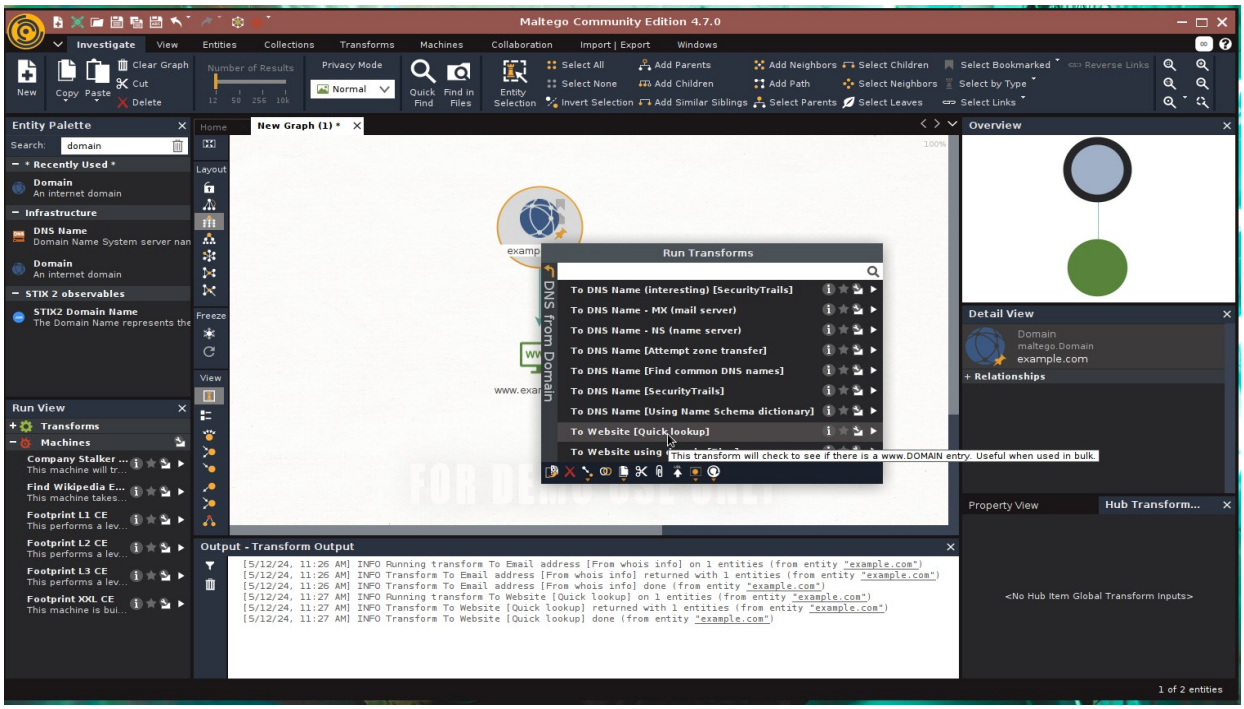

Рис. 2.11. Розміщення сутності типу Домен на графі та виконання трансформу To Website для неї

Як бачимо, Maltego значно спрощує проведення розслідувань кіберінцидентів у корпоративних інформаційних системах двома шляхами:

– широким застосуванням хмарних обчислень – основна робота виконується на серверах компанії, що значно пришвидшує освоєння рішення великими та малими підприємствами, установами й організаціями, а також окремими особами, а також знижує витрати на розбудову інфраструктури для рішення та його інтеграцію в інформаційну систему компанії;
– інтуїтивно простим інтерфейсом та мінімальною кількістю підготовчих дій для проведення розслідування.

Відтак розглянемо варіанти проведення розслідування із застосуванням Maltego та розробимо рекомендації щодо його використання.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ ІЗ ЗАСТОСУВАННЯМ MALTEGO

3.1 Варіант проведення розслідування із застосуванням Maltego на прикладі ботнету Kaiji

Перед початком розслідування кіберінциденту необхідно розробити порядок дій. Розглянемо деякі рекомендації компанії Paterva щодо використання рішення для проведення розслідувань, зокрема оцінки поверхні атаки та аналізу сповіщень SIEM-систем.

Оцінка поверхні атаки – процес, що належить до класу початкових за ISO/IEC 27043. Відомо, що зловмисники постійно збирають дані про різні компанії, шукаючи вразливі активи. Відтак окремі особи та корпоративні системи можуть зазнавати атак соціальної інженерії або спроб експлуатації вразливостей. Метою команди реагування на інциденти є виявлення потенційно скомпрометованого програмного забезпечення компанії. Припустимо, що команда має такі вхідні дані:

- назва компанії;
- діапазони IP-адрес, що належать компанії;
- домени компанії.

Paterva рекомендує такий порядок дій з використанням Maltego:

1. Додати до графу Maltego сутність типу Домен.

2. Виконати пошук усіх DNS-записів для домену з використанням відповідного стандартного трансформу.

3. Виконати пошук усіх IP-адрес, пов’язаних із попередньо знайденими DNS-записами, скориставшись відповідним стандартним трансформом.

4. Згрупувати всі знайдені IP-адреси в блоки.

5. Згрупувати блоки IP-адрес так, щоб можна було визначити номери AS.

6. Визначити номери AS, які напряму пов’язані з компанією, а потім – блоки адрес, виділені компанії.

7. Вибрати IP-адреси, пов’язані з визначеними блоками, та з використанням відповідного стандартного трансформу виявити запущені на них сервіси та служби.

8. Використовуючи ті ж IP-адреси, виконати трансформ Shodan з метою виявлення вразливостей у знайдених сервісах та службах.

9. Отримати більше інформації щодо виявлених вразливостей з використанням трансформу NIST NVD.

10. (Необов’язково) Вибрати блоки IP-адрес та виконати пошук служб, сервісів та їх вразливостей по всіх IP-адресах блоків [21, с. 9-10].

Граф, створений в ході дослідження, представлено на рисунку 3.1.

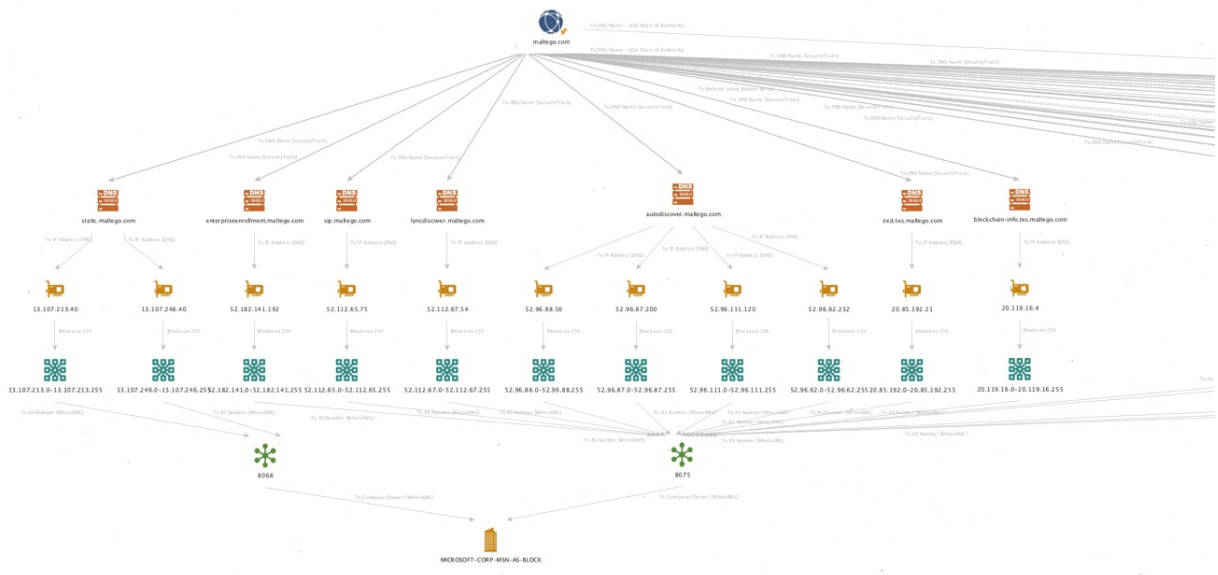

Рис. 3.1. Граф Maltego, що відображає порядок пошуку інформації при виконанні оцінки поверхні атаки [21, с. 9-10]

Аналіз подій SIEM-систем виконується в рамках класу процесів розслідування, визначеного ISO/IEC 27043. Припустимо, що аналітик SOC отримав сповіщення типу Possible Beaconing у SIEM-системі Splunk, представлене на рисунку 3.2 [25].

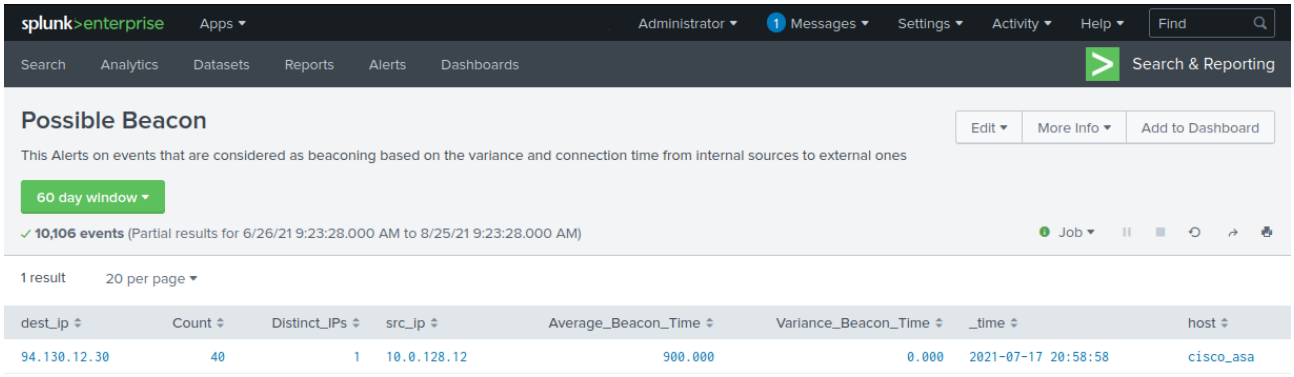

Рис. 3.2. Сповіщення Splunk [25]

Рекомендований порядок дій є таким:

1. На початку розслідування необхідно винести на граф сутність типу Вислів, до якої додати текст запиту, який викликав появу сповіщення.

2. Далі використовується трансформ Run Raw Splunk Query з набору трансформів для Splunk. Цей трансформ дозволяє вибрати проміжок часу для виконання запиту та отримати події SIEM, що сталися протягом нього.

3. З події необхідно одержати інформацію про час її виникнення, пов’язані пристрої та IP-адреси тощо за допомогою трансформу To Interesting Fields.

4. Для внутрішніх IP-адрес потрібно виконати перевірку логів DHCP за період, що відповідає часу появи сповіщення в SIEM-системі. Виконується трансформ Get Network Sessions Events.

5. До логів слід застосувати трансформ To Interesting Fields, що демонструє зв’язки між ними.

6. Далі необхідно перевірити активність зовнішніх IP-адрес, оскільки вони можуть бути включені до інфраструктури зловмисників. Для цього можна застосувати трансформи таких сервісів, як AbuseIPDB, Intezer, Shodan та VirusTotal. Пошук в базі AbuseIPDB надає місцезнаходження, ім’я хоста, назву провайдера та спосіб використання ресурсу за досліджуваною IP-адресою. Пошук у Shodan виявляє номери портів, відкритих на зовнішньому веб-ресурсі, властивості SSL-сертифікатів тощо. За допомогою VirusTotal виявляються шкідливі файли, пов’язані з IP-адресою.

7. Якщо пошук у VirusTotal повертає позитивний результат, можна робити припущення щодо потенційного зараження користувача або клієнта компанії шкідливим ПЗ. Для перевірки гіпотези може бути виконаний трансформ з набору VirusTotal, який отримує хеші для кожного виявленого файлу. Далі за допомогою трансформу Get Malware Events [Splunk] можна перевірити, чи були файли з такими хешами виявлені в логах інформаційної системи компанії.

8. Якщо результати перевірки підтверджують факт зараження, необхідно точно встановити сімейство шкідливого ПЗ, виявленого на комп’ютері користувача. Для цього підійдуть трансформи Intezer [25].

Як бачимо, описані підходи узгоджуються з рекомендаціями ISO/IEC 27043 та включають:

- визначення сценарію атаки – опис ситуації, яка виникла або може виникнути в процесі діяльності організації, установи або підприємства;
- визначення мети розслідування;
- збір вхідних даних – цифрових доказів;
- дослідження та інтерпретація даних з використанням Maltego.

Застосуємо проаналізовані підходи до виконання розслідування реального кіберінциденту із застосуванням Maltego на прикладі попередження про виявлення на віртуальному приватному сервері клієнта компанії сервера управління та контролю (C2) ботнету Kaiji – зловмисного програмного забезпечення, націленого на сервери на основі Linux. Попередження було отримане від AWS Shield через систему обробки тікетів, як представлено на рисунку нижче. Відтак, за можливий сценарій приймемо розгортання сервера C2 ботнету в інформаційній системі одного з клієнтів компанії (рис. 3.3).

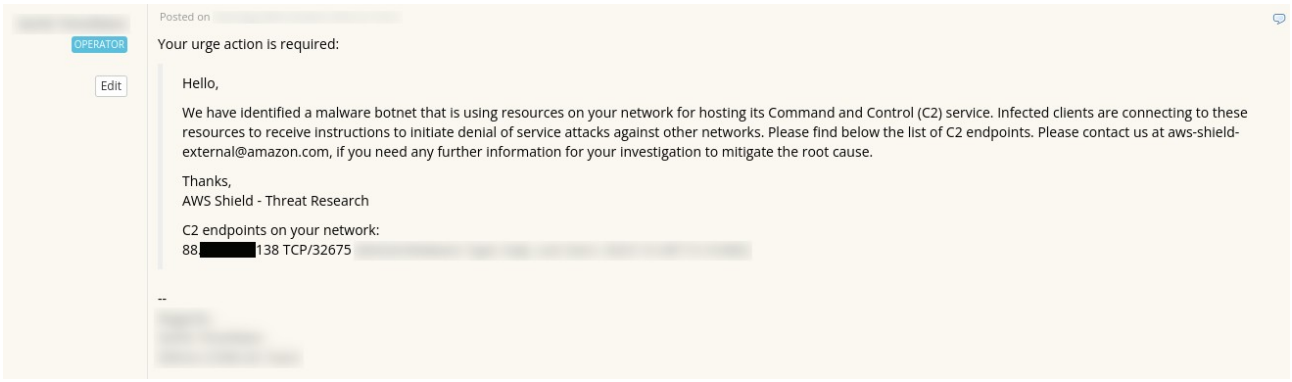

Рис. 3.3. Повідомлення від AWS Shield про виявлення активності сервера C2 ботнету Kaiji

У ході подальшого аналізу активності в інфраструктурі компанії було зібрано такі вхідні дані:

1. IP-адреса користувача, чий сервер був заражений (приховано за вказівкою керівника компанії).

2. Зовнішня IP-адреса, з якої виконувалося підключення до зараженого сервера: 104.218.236.103.

3. Адреса електронної пошти, з якої клієнт-замовник віртуального приватного сервера реєструвався на сайті компанії та робив замовлення: a******t@protonmail.com (приховано за вказівкою керівника компанії).

4. Хеш SHA-256 потенційно шкідливого файлу, знайденого на віртуальному приватному сервері клієнта: da3934f14d3f1d037214510d63a919eeb8bdd6462109aa5714d1c6b355d4c666.

Метою розслідування є верифікація кіберінциденту, виявлення масштабу атаки та визначення заходів щодо припинення зловмисної діяльності в інформаційній системі компанії.

Виконаємо розслідування в два етапи, проаналізувавши зовнішню та внутрішню (яка належить компанії) IP-адреси. Найперше додамо до графу сутність типу IPv4 Address та запишемо до неї зовнішню IP-адресу. Перевіримо її репутацію та інші дані за допомогою трансформів Reputation and Details від AbuseIDPB, як представлено на рисунку 3.4.

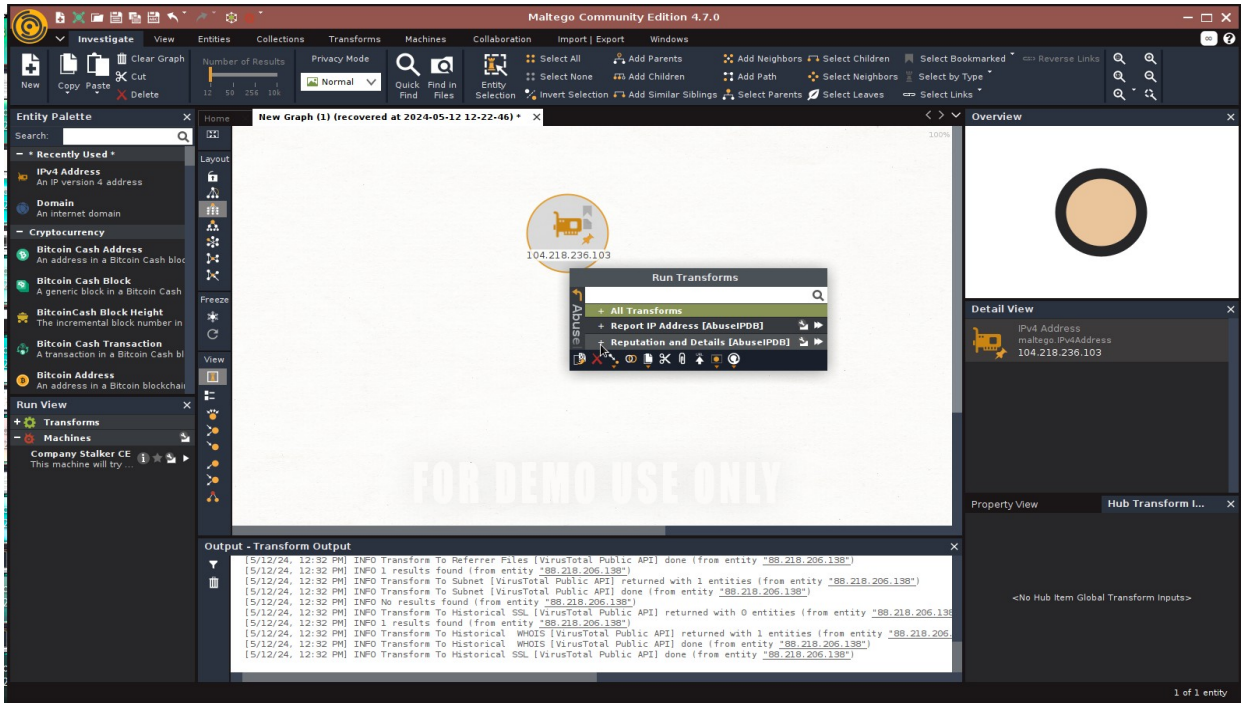

Рис. 3.4. Перевірка репутації зовнішньої IP-адреси за допомогою трансформів AbuseIDPB

Сервіс AbuseIDPB надав назву та тип компанії, якої стосується IP-адреса, а також країну, в якій вона розташована, як показано на рисунку 3.5.

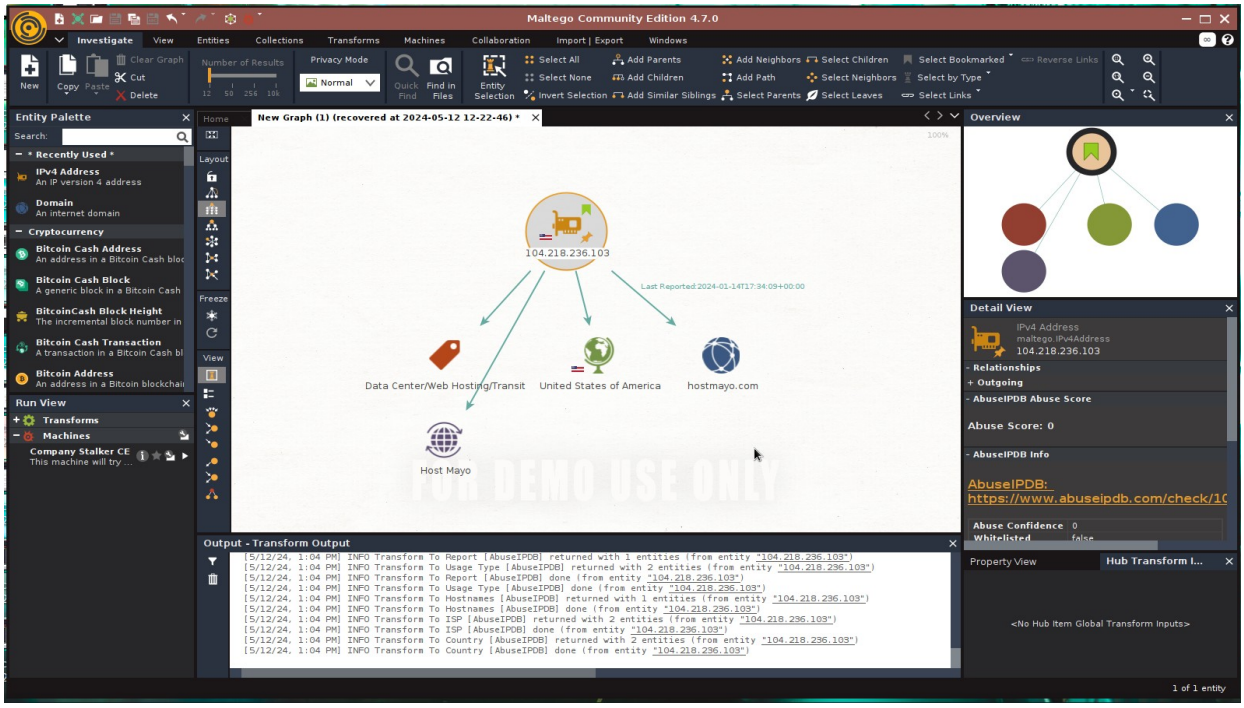

Рис. 3.5. Результати роботи трансформів AbuseIDPB

Незважаючи на нульовий рівень небезпечності (Abuse Score), IP-адреса перебуває в чорному списку (Whitelisted: false), як зазначено у вікні властивостей. Окрім цього, на графі присутня відмітка Last Reported з датою та часом подання останнього звіту про зловмисну активність, у якій було задіяно досліджувану IP-адресу. Такий стан справ вимагає її подальшого аналізу за допомогою Shodan та VirusTotal. Найперше отримаємо додаткову інформацію від Shodan з використанням трансформу To Vulnerabilities [Shodan Internet DB], який є частиною стандартного пакету трансформів Standard Transforms CE (рис. 3.6).

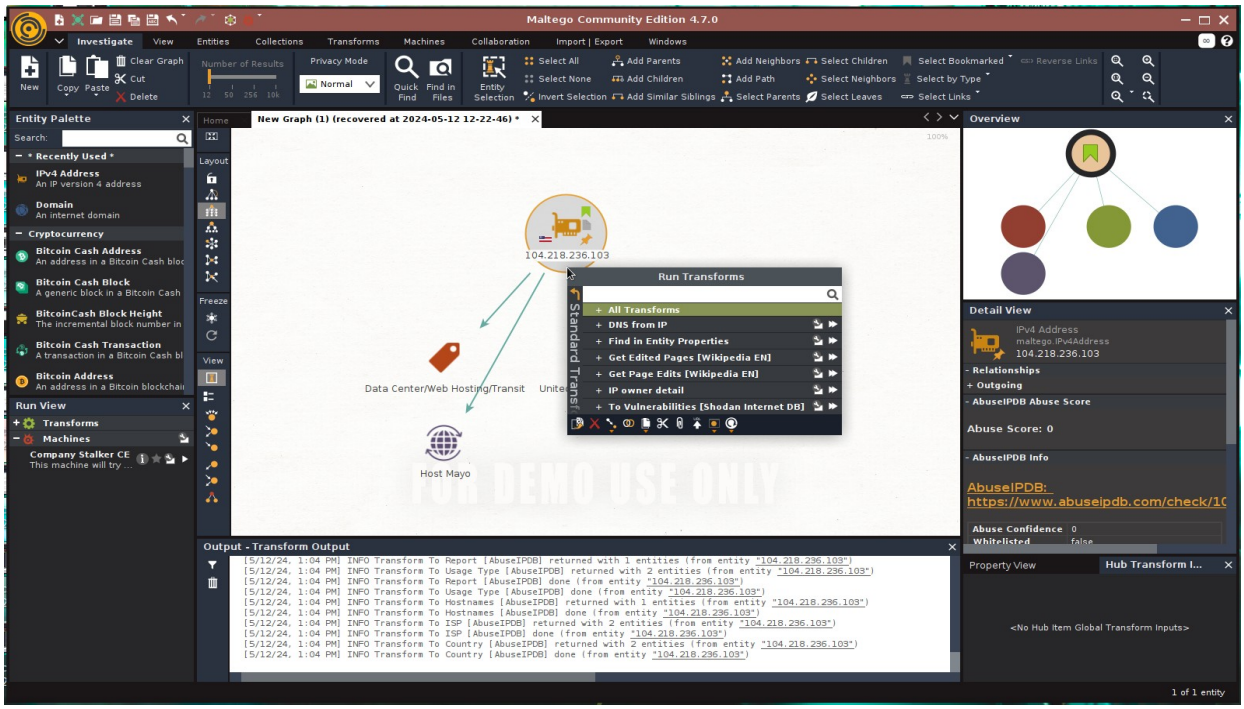

Рис. 3.6. Вибір трансформів To Vulnerabilities [Shodan Internet DB]

Серед результатів пошуку наявні порти та сервіси, запущені на веб-ресурсі, ідентифіковному за досліджуваною IP-адресою. Серед них – служба ssh (порт 22), а також порт SMTP з шифруванням SSL/TLS (порт 587) та порт HTTP (порт 80), показані на рисунку 3.7.

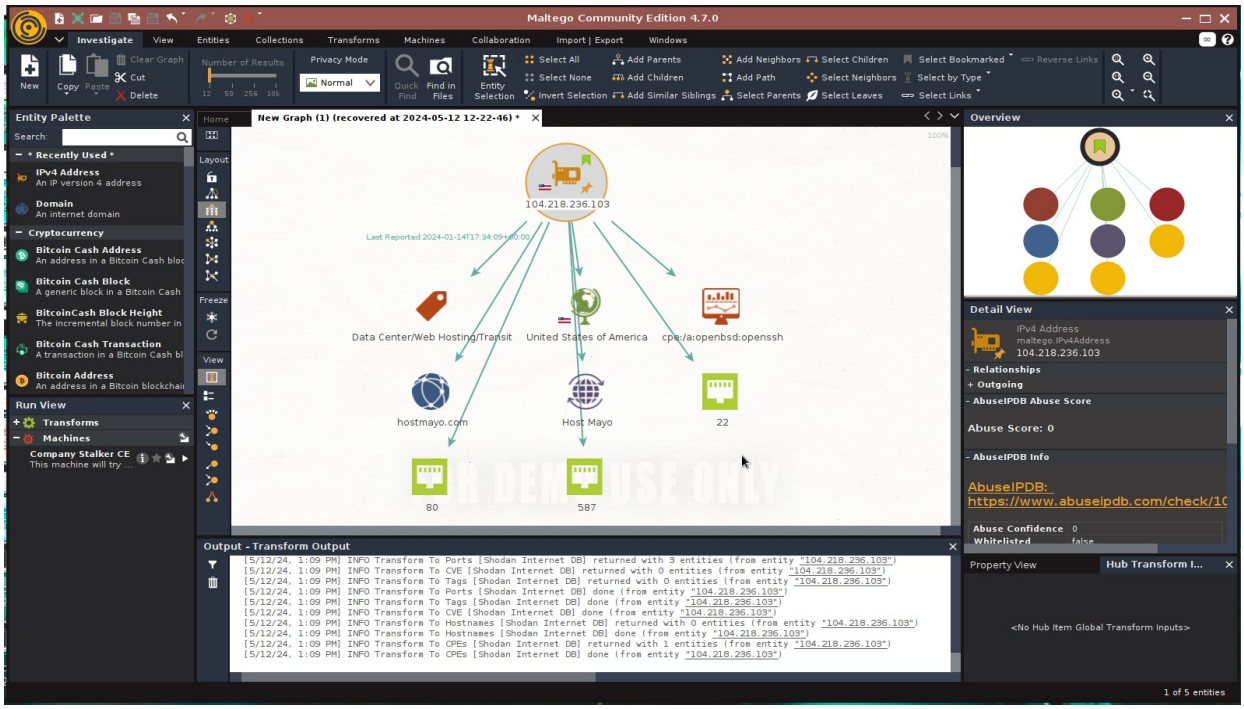

Рис. 3.7. Результати виконання трансформу To Vulnerabilities

Наступний крок – перевірка відомостей про можливу причетність IP-адреси до одного з відомих ботнетів. Виконання перевірки за допомогою VirusTotal повертає результати, представлені на рисунку 3.8.

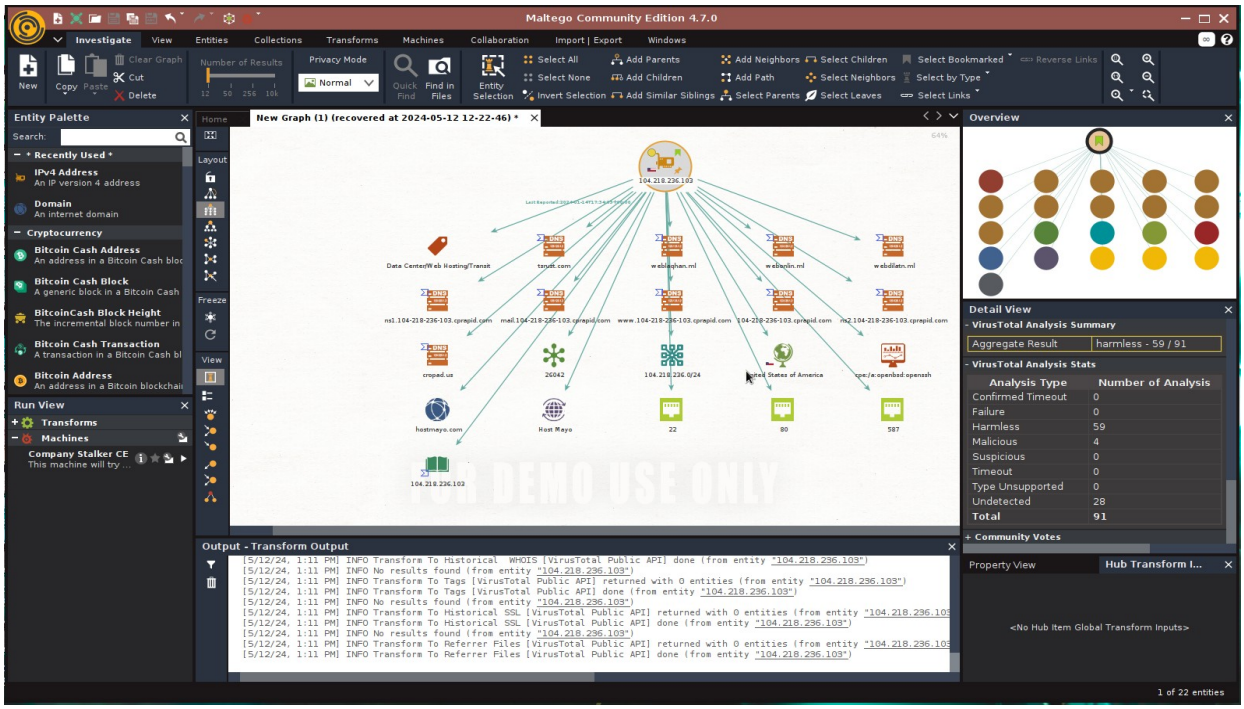

Рис. 3.8. Виконання перевірки зловмисної активності IP-адреси за допомогою трансформів VirusTotal

Як видно з інформації, представленої у вікні властивостей, 4 постачальники рішень безпеки відзначили досліджувану IP-адресу як таку, що асоційована зі злочинною активністю. Аналіз коментарів спільноти VirusTotal показує, що адреса належить до ботнету Kaiji, описаному в звіті QiAnXin Threat Intelligence Center від 27 лютого 2023 року (рис. 3.9) [17].

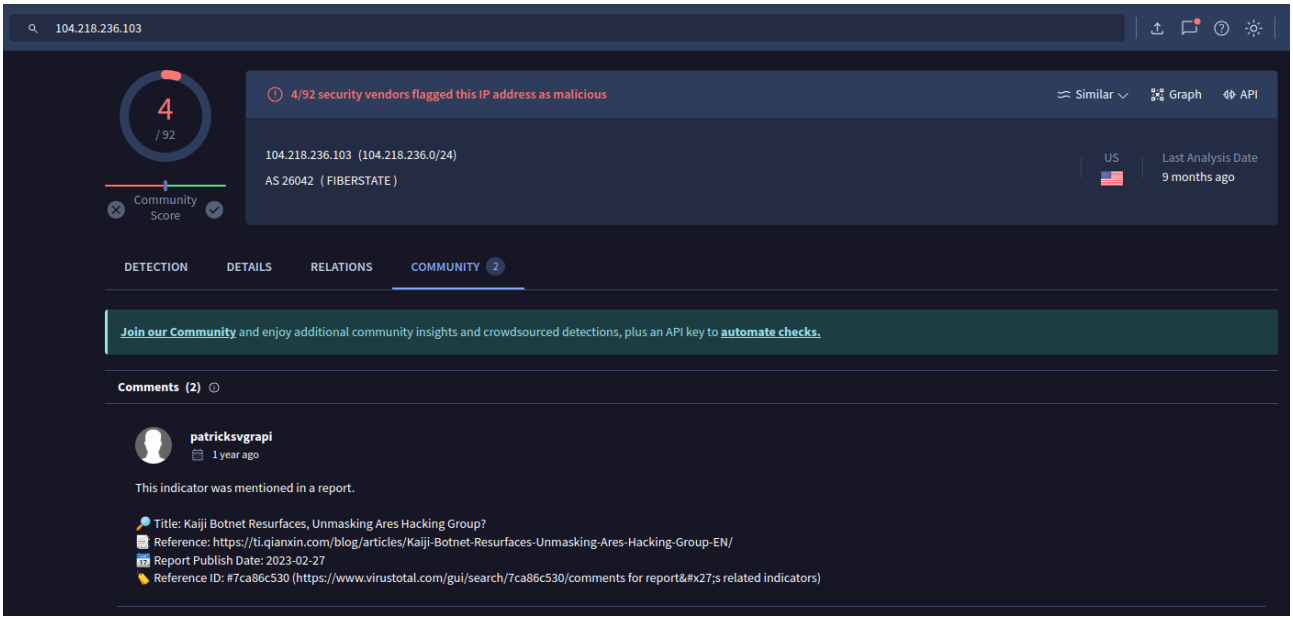

Рис. 3.9. Коментарі спільноти VirusTotal щодо приналежності досліджуваної IP-адреси до ботнету Kaiji

Звіт QiAnXin Threat Intelligence Center відзначає, що ботнет Kaiji пов’язаний з хакерським угрупованням Ares [17]. А Intezer, постачальник автоматизованих рішень для SOC, вказує www.aresboot[.]xyz як один з індикаторів компрометації, властивий більш ранній активності ботнету, виявленій у 2020 році [20]. Зазначимо, що адреса електронної пошти клієнта-замовника віртуального приватного сервера збігається з індикатором компрометації. Перевірка цієї адреси за допомогою інструменту Holehe демонструє, що вона була створена 26 серпня 2023 року – у тому ж році, в якому востаннє спостерігалася активність ботнету (рис. 3.10).

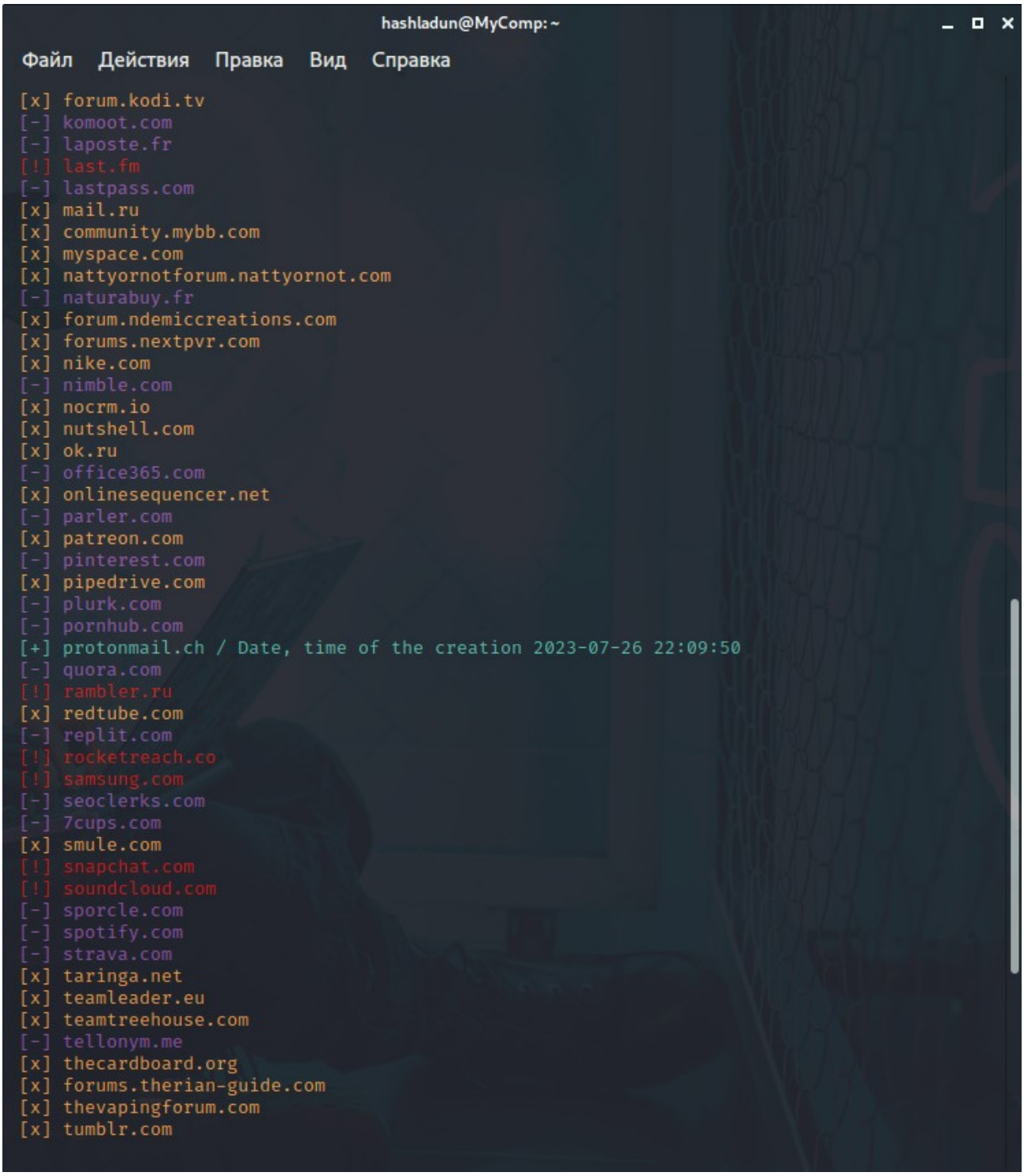

Рис. 3.10. Виявлення дати створення адреси електронної пошти клієнта з використанням Holehe

Хеш потенційно шкідливого файлу, знайдений на віртуальному приватному сервері клієнта, також позначений спільнотою VirusTotal як шкідливий, незважаючи на відсутність виявлень антивірусними рішеннями (рис. 3.11).

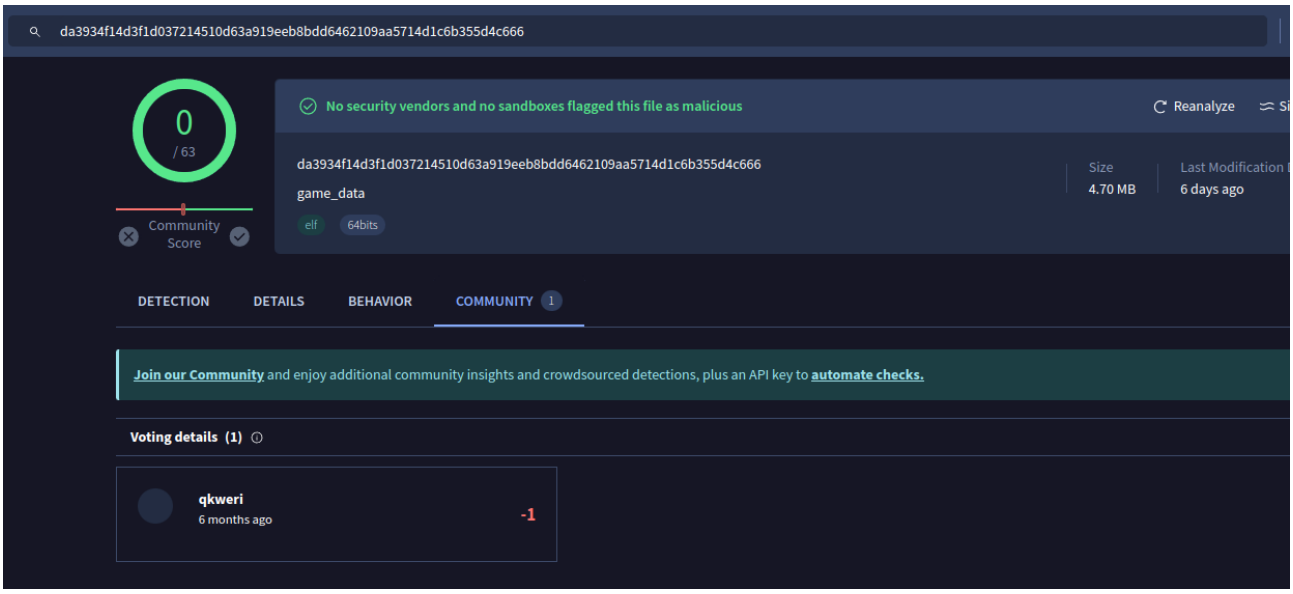

Рис. 3.11. Спільнота VirusTotal визначає файл, знайдений на віртуальному приватному сервері клієнта, як шкідливий

Виконаний аналіз дозволяє стверджувати, що клієнт причетний до злочинної діяльності, здійснюваної з використанням ботнету Kaiji, а не встановив шкідливе програмне забезпечення випадково. Відтак інцидент вважається підтвердженим, а віртуальний приватний сервер клієнта – скомпрометованим. З метою запобігання подальшій злочинній діяльності роботу сервера та подальше обслуговування клієнта було припинено.

Після виконання заходів з припинення зловмисної діяльності виконаємо перевірку репутації внутрішньої IP-адреси. Це можна зробити з використанням трансформів VirusTotal. Для цього розмістимо на графі сутність з цією IP-адресою та виконаємо відповідні трансформи (рис. 3.12).

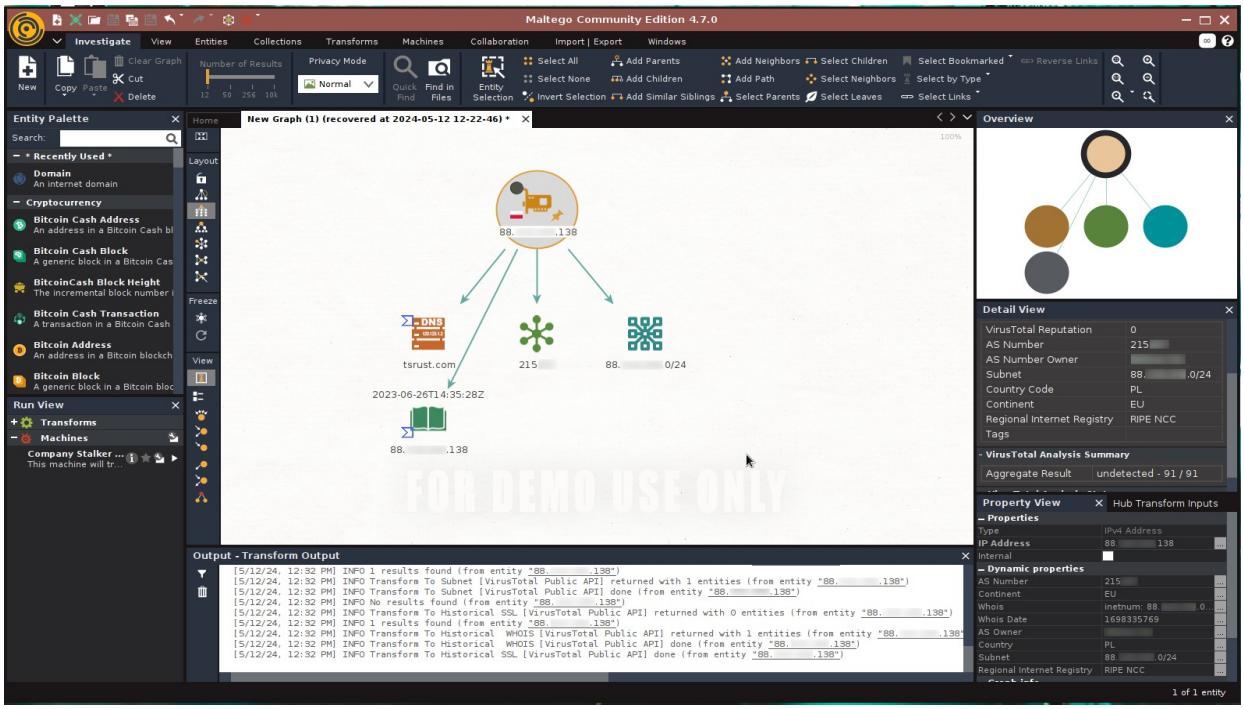

Рис. 3.12. Перевірка внутрішньої IP-адреси за допомогою трансформів VirusTotal.

Як бачимо з вікна властивостей, адреса не асоціюється зі зловмисною діяльністю жодним із постачальників антивірусних рішень. Відтак, репутаційної шкоди компанії завдано не було.

За результатами виконання розслідування дамо ряд рекомендацій щодо розслідування кіберінцидентів у корпоративній інформаційній системі із застосуванням Maltego.

3.2 Рекомендації щодо розслідування кіберінцидентів в корпоративній інформаційній системі

При проведенні розслідувань з використанням Maltego необхідно враховувати чотири аспекти – фінансовий, організаційний, безпековий та технічний. Рекомендації в рамках кожного викладено в таблиці 3.1.

Таблиця 3.1.

Рекомендації щодо застосування Maltego при проведенні розслідувань кіберінцидентів

Аспект	**Стисла характеристика аспекту**	**Складова аспекту**	**Опис складової**
Фінансовий	Можливості організації, установи або підприємства щодо придбання рішення Maltego (або іншого рішення)	Ціна	Безкоштовна версія Maltego має певні обмеження, однак ліцензія може виявитись надто дорогою, особливо для малого бізнесу. Відтак при виборі ліцензії необхідно враховувати розмір та вид діяльності організації, установи чи підприємства, а також обсяг та типи даних, які будуть оброблятися. Наприклад, для невеликої хостингової компанії, яка проводить лише прості розслідування інцидентів на нерегулярній основі, підійде версія Maltego Community Edition, тоді як великій компанії, основним напрямом діяльності якої є розслідування складних кіберінцидентів, може знадобитись тарифний план Maltego Enterprise і версія Maltego One.

Аспект	Стисла характеристика аспекту	Складова аспекту	Опис складової
Організаційний	Принципи організації та проведення розслідувань кіберінцидентів	Сценарій можливої атаки та мета розслідування	Сценарій має бути складений з рівнем деталізації, достатнім для визначення мети розслідування та порядку дій. Мета має бути сформульована так, щоб в ході розслідування можна було визначити, чи її досягнуто
		Етичні міркування	Під час проведення розслідування кіберінциденту необхідно дотримуватись етики та вимог законодавства, демонструючи повагу до конфіденційності осіб, які можуть бути так чи інакше залучені в процес, а також отримуючи дозволи на доступ до тієї чи іншої інформації
		Перевірка джерел інформації	Інформація, отримувана за допомогою Maltego, може бути застарілою, неправдивою або неточною, тому необхідно виконувати її додаткову перевірку за допомогою надійних джерел
		Крива кваліфікації	Почати використовувати Maltego для проведення розслідувань досить легко, але для повного

Аспект	Стисла характеристика аспекту	Складова аспекту	Опис складової
			опанування його можливостей потрібен час
Безпековий	Безпека цифрових доказів, здобутків розслідування та аналітиків, що з ними працюють	Чутливі цифрові докази	Якщо у процесі збору цифрових доказів було виявлено чутливі дані, необхідно вирішити, чи можуть вони оброблятися на серверах Maltego
		Спільна робота	Якщо виникає необхідність поділитися графом розслідування з іншими, необхідно перевірити, чи мають ті особи право доступу до інформації, представленої на ньому
		Безпечне виконання розслідування	У процесі розслідування можуть виникнути загрози життю та здоров’ю аналітика. У такому разі варто використовувати режим приховування активності (Stealth Mode) в Maltego. Однак необхідно пам’ятати, що навіть у цьому режимі деякі трансформи можуть отримувати дані від цілі, використовуючи публічний сервер CTAS або комп’ютер аналітика

Аспект	Стисла характеристика аспекту	Складова аспекту	Опис складової
		Створення резервних копій даних розслідування	Необхідно регулярно створювати резервні копії даних розслідування в Maltego, особливо при виконанні критично важливих або термінових розслідувань. Якщо станеться технічний збій або інше порушення функціонування інформаційної системи, здобутки не будуть втрачені
Технічний	Вибір та використання окремих компонентів Maltego, адміністрування рішення	Використання коректних сутностей	Для уникнення некоректних результатів роботи Maltego слід використовувати сутності, відповідні до типів даних, які використовуються як вхідні
		Використання коректних трансформів	Підбір та використання трансформів мають виконуватись обережно з метою уникнення появи зайвої інформації на графі
		Регулярні оновлення	Нові версії Maltego отримують більше нового функціоналу, який може пришвидшити розслідування. Окрім цього, застарілі версії рішення з часом перестають працювати

Аспект	Стисла характеристика аспекту	Складова аспекту	Опис складової
			(користувач отримує повідомлення “Access denied – request is unauthorized” при спробі виконати будь-який трансформ)

Підбиваючи підсумки, відзначимо, що гнучкість у виборі джерел інформації, що стосується цифрових доказів, її централізований збір та зберігання, а також можливість її візуального аналізу є ключовими перевагами Maltego при проведенні розслідувань кіберінцидентів у корпоративній інформаційній системі. Однак найкращих результатів можна досягнути, враховуючи рекомендації щодо фінансового, організаційного, безпекового та технічного забезпечення розслідування інцидентів.

ВИСНОВКИ

У роботі окреслено світову та вітчизняну проблематику розслідування кіберінцидентів у корпоративних інформаційних системах. При сучасних стрімких темпах еволюції кіберзагроз якість та швидкість проведення розслідувань залишається невисокою. Серед причин такого стану справ дослідники та експерти в галузі називають складність отримання даних з віддалених кінцевих точок, необхідність проведення віддаленого розслідування, нестача засобів автоматизації, збір доказів з різнорідних джерел, труднощі при роботі з різноманітними програмними рішеннями, організації процесу розслідування, аналізу доказів, документування, нестача кваліфікованих кадрів.

Показано існуючі підходи до розслідування кіберінцидентів, які можуть значно покращити ситуацію в сфері розслідування кіберінцидентів і викладені в міжнародних стандартах NIST SP 800-61 та ISO/IEC 27043.

Проаналізовано програмні рішення, що дозволяють проводити розслідування кіберінцидентів. Обрано рішення Maltego як найбільш оптимальний варіант з представлених з огляду на функціонал, кросплатформеність, відкритий вихідний код та співвідношення якість-ціна. Maltego – інструмент візуального аналізу, здатний виконувати самостійний збір інформації з відкритих джерел. Його ключові компоненти – сутності, що представляють певний тип даних (цифрових доказів), такий, як домен або IP-адреса, трансформи – код, який виконує підключення до API джерел інформації та отримує дані, машини – набір трансформів, призначений для отримання даних в тому випадку, коли одного трансформа недостатньо. Трансформи виконуються на серверах трансформів, до яких клієнтські застосунки підключаються через сервер поширення трансформів TDS, який надає налаштування трансформів і користувальницьких сутностей та направляє виклики трансформів до відповідних серверів.

Виокремлено методи та засоби розслідування кіберінцидентів у корпоративній системі із застосуванням Maltego. Загальна методика проведення розслідування за допомогою Maltego вкладається в рамки підходу, запропонованого ISO/IEC 27043 і включає визначення сценарію атаки та мети розслідування, збір вхідних даних та їх дослідження й інтерпретацію з використанням Maltego. Практично розслідування виконується шляхом послідовного застосування вибраних трансформів до кожної сутності, розширюючи уявлення аналітика про перебіг кіберінциденту.

За результатами проведеної роботи розроблено рекомендації щодо використання рішення, які враховують фінансовий, організаційний, безпековий та технічний аспекти розслідування кіберінцидентів.

Отже, розслідування кіберінцидентів займає важливе місце серед процесів, що підтримують діяльність організації, установи чи підприємства. Maltego – комплексне рішення, що дозволяє збирати дані з різних джерел та візуалізувати їх, пришвидшуючи процес розслідування. Воно допомагає компаніям дотримуватись кращих практик при проведенні розслідувань, оскільки може бути гнучко налаштоване для конкретного випадку.

Таким чином, продумані та налагоджені процеси розслідування кіберінцидентів мають сприяти ефективній протидії все більш розвиненим кіберзагрозам.

Теоретичні розробки, викладені в роботі, можуть бути використані при створенні науково-методичних матеріалів, присвячених розслідуванню кіберінцидентів у корпоративній інформаційній системі. Практичні результати можуть бути використані при проведенні розслідувань кіберінцидентів малими та середніми організаціями, установами та підприємствами, для яких розслідування кіберінцидентів не є основним напрямом діяльності. Дослідження не претендує на вичерпність.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2023. Звіт про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a (дата звернення: 18.04.2024).

2. 4 релізи Maltego. Принципи роботи та можливості. *Хабр*. URL: https://habr.com/ru/companies/tomhunter/articles/462457/ (дата звернення: 26.04.2024).

3. Копитін Ю. Розслідування інцидентів інформаційної безпеки. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник.* 2010. № 1(20). С. 58–65. URL: https://ela.kpi.ua/server/api/core/bitstreams/34223b6b-fcfa-409f-a473-b6bcb024eae0/content (дата звернення: 19.04.2024).

4. Хантер Т. ТОП безкоштовних OSINT-інструментів за версією T.Hunter в 2024-му році. *Хабр*. URL: https://habr.com/ru/companies/tomhunter/articles/809725/ (дата звернення: 21.04.2024).

5. Черняк Л. Аналитика подвійного призначення. *Відкриті системи. СУБД*. 2013. № 10. С. 48–50.

6. 2023 Annual Report. URL: https://go.recordedfuture.com/hubfs/reports/ta-2024-0321.pdf (дата звернення: 17.04.2024).

7. Attack surface documentation. *Intel471*. URL: https://intel471.com/attack-surface-documentation (дата звернення: 22.04.2024).

8. Chauhan S. Hacking web intelligence: Open source intelligence and web reconnaissance concepts and techniques. Waltham, MA : Syngress, 2015. 281 c.

9. Cost of a data breach 2023 | IBM. *IBM in Deutschland, Österreich und der Schweiz*. URL: https://www.ibm.com/reports/data-breach (дата звернення: 17.04.2024).

10. Cybersecurity risk underestimated by operational technology organizations. URL: https://www.skyboxsecurity.com/resources/report/cybersecurity-risk-underestimated-operational-technology-organizations/ (дата звернення: 18.04.2024).

11. DFIR State Report 2023 – Binalyze. *Binalyze – Modern Digital Forensics and Incident Response*. URL: https://www.binalyze.com/resources/dfir-state-report-2023 (дата звернення: 18.04.2024).

12. Emerging trends in digital forensic and cyber security – an overview / *S. Bhoopesh ma ін. 2019 Sixth HCT information technology trends (ITT)* : матеріали Міжнар. наук. конф., м. Ras Al Khaimah, 20–21 листоп. 2019 р. 2020. С. 309–313. URL: https://www.proceedings.com/54199.html (дата звернення: 19.04.2024).

13. i2 Analyst's Notebook. URL: https://i2group.com/hubfs/Products/i2-Analysts-Notebook.pdf (дата звернення: 23.04.2024).

14. Introduction to Maltego Standard Entities. URL: https://docs.maltego.com/support/solutions/articles/15000035722-introduction-to-maltego-standard-entities (date of access: 28.04.2024).

15. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. На заміну ISO/IEC 27002:2013 ; чинний від 2024-02-15. Вид. офіц. 2022. 152 с. URL: https://www.iso.org/standard/75652.html (дата звернення: 19.04.2024).

16. ISO/IEC 27043:2015. Information technology – Security techniques – Incident investigation principles and processes. Чинний від 2015-03-01. Вид. офіц. 2015. 30 с. URL: https://www.iso.org/ru/standard/44407.html (дата звернення: 19.04.2024).

17. Kaiji Botnet Resurfaces, Unmasking Ares Hacking Group?. URL: https://ti.qianxin.com/blog/articles/Kaiji-Botnet-Resurfaces-Unmasking-Ares-Hacking-Group-EN/ (дата звернення: 01.05.2024).

18. Lampyre: Data analysis & OSINT tool for everyone. URL: https://lampyre.io/ (дата звернення: 23.04.2024).

19. Lee N. Counterterrorism and Cybersecurity. Total Information Awareness. New York : Springer, 2013. 234 c.

20. Litvak P. Kaiji: New Chinese Linux malware turning to Golang. *Intezer*. URL: https://intezer.com/blog/research/kaiji-new-chinese-linux-malware-turning-to-golang/ (дата звернення: 02.05.2024).

21. Maltego Handbook for Incident Response. URL: https://static.maltego.com/cdn/Handbooks/Maltego-Handbook-for-Incident-Response.pdf (дата звернення: 29.04.2024).

22. Maltego. The World's Most Used Cyber Investigation Platform. URL: https://www.maltego.com/ (дата звернення: 23.04.2024).

23. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Вид. офіц. 2006. 121 с. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (дата звернення: 19.04.2024).

24. Overview of Maltego Servers. URL: https://docs.maltego.com/support/solutions/articles/15000031270-overview-of-maltego-servers#introduction-0-0 (date of access: 28.04.2024).

25. Siem-plify Your Investigations with Splunk and Maltego!. URL: https://www.maltego.com/blog/simplify-your-investigations-with-splunk-and-maltego/ (дата звернення: 30.04.2024).

26. System Architecture. URL: https://docs.maltego.com/support/solutions/articles/15000034017-system-architecture (дата звернення: 28.04.2024).

27. What is a Maltego Standard Transforms Add-on (CTAS) Server?. URL: https://docs.maltego.com/support/solutions/articles/15000020187-what-is-a-ctas- (дата звернення: 28.04.2024).

28. What is a Transform Distribution Server (TDS/iTDS)?. URL: https://docs.maltego.com/support/solutions/articles/15000020198-what-is-itds-#the-itds-0-1 (дата звернення: 28.04.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)