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

ТЕРЕЩЕНКО Олександр Сергійович

Алгоритми розвідки кіберзагроз на базі платформи з відкритим кодом / Cyber threat intelligence algorithms based on open source platform

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБзм -21
О.С. Терещенко

Науковий керівник
д.т.н., професор В.В.Яцків

Кваліфікаційну роботу
Допущено до захисту:

«____» _____ ___2022 р.

Завідувач кафедри
_____ **В.В.Яцків**

ТЕРНОПІЛЬ - 2022

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

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
«____» _____ 2021 року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

ТЕРЕЩЕНКО Олександру Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Алгоритми розвідки кіберзагроз на базі платформи з відкритим кодом / Cyber threat intelligence algorithms based on open source platform
керівник роботи д.т.н., професор В.В. Яцків

затверджені наказом по університету від 31 грудня 2021 року № 606

2. Строк подання студентом закінченої кваліфікаційної роботи 16 листопада 2022 р.

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

4. Основні питання, які потрібно розробити:
– визначити типи розвідки кіберзагроз;
– провести аналіз платформ розвідки кіберзагроз з відкритим кодом;
– дослідити використання правил YARA в розвідці кіберзагроз;
– розробити структуру та алгоритм розвідки кіберзагроз;
– провести аналіз подій при розвідці кіберзагроз;
– розробити алгоритм створення події на основі звіту.

5. Перелік графічного матеріалу у роботі:
– типи розвідки кіберзагроз;
– платформи розвідки кіберзагроз з відкритим кодом;
– життєвий цикл аналізу загроз;
– стандарти обміну інформацією про загрози;
– структура та алгоритм розвідки кіберзагроз;

– алгоритм розвідки кіберзагроз;
– аналіз подій при розвідці кіберзагроз;
– створення події на основі звіту.

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання 11 жовтня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз систем розвідки кіберзагроз на базі платформи з відкритим кодом	12.2021 р. – 03.2022 р.	
2	Структура та принципи організації розвідки кіберзагроз	03.2022 р. – 05.2022 р.	
3	Розробка системи розвідки кіберзагроз на базі MISP	05.2022 р. – 11.2022 р.	

Студент _____ Терещенко О.С.
(підпис)

Керівник роботи _____ д.т.н., професор В.В. Яцків
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Алгоритми розвідки кіберзагроз на базі платформи з відкритим кодом» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека» освітньо-професійної програми «Кібербезпека» написана обсягом 72 сторінки і містить 28 ілюстрації, 1 таблиця, 2 додатки та 27 джерел за переліком посилань.

Метою кваліфікаційної роботи є підвищення ефективності алгоритмів обміну інформацією про кіберзагрози на базі платформи з відкритим кодом.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи розвідки кіберзагроз, методи поширення інформації про загрози, методи проектування.

Результати дослідження: удосконалено алгоритм розвідки та поширення інформації про кіберзагрози на основі життєвого циклу аналізу загроз.

Встановлено та налаштовано систему обміну інформацією про кіберзагрози на базі MISP. Створено подію на основі звіту про кіберзагрозу з відкритих джерел.

Результати роботи можуть бути застосовані при розгортанні власної системи розвідки кіберзагроз та обміну розвідувальними даними про загрози.

Ключові слова: РОЗВІДКА КІБЕРЗАГРОЗ, MISP, ЛАНДШАФТ КІБЕРЗАГРОЗ, ПРАВИЛА YARA.

ABSTRACT

Qualification work on "Cyber threat intelligence algorithms based on open source platform" for the degree of "Master" in the specialty 125 "Cybersecurity" educational and professional program "Cybersecurity" is written in 72 pages and contains 28 illustrations, 1 table, 2 appendices and 27 source according to the list of links.

The purpose of the qualification work is to increase the efficiency of algorithms for exchanging information about cyber threats based on an open source platform.

Research methods. To solve the tasks in this qualification work, the following methods of cyber threat intelligence, methods of disseminating information about threats, and design methods were used.

The results of the study: the algorithm for reconnaissance and dissemination of information about cyber threats based on the life cycle of threat analysis has been improved.

A system for exchanging information about cyber threats based on MISP has been installed and configured. An event was created based on an open source cyber threat report.

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

Keywords: CYBER THREAT INTELLIGENCE, MISP, THREAT LANDSCAPE, YARA RULES.

ЗМІСТ

ВСТУП

Актуальність роботи. З появою Інтернету речей (IoT) відбулося значне зростання кількості кібератак, які постійно вдосконалюються та стають все більш складними. Зловмисники використовують широкий набір інструментів і тактик, щоб атакувати своїх жертв із мотивами, починаючи від збору розвідувальних даних до знищення даних.

Провідні постачальники засобів кібербезпеки повідомляють про збільшення середньої кількості атак на компанії приблизно на 31%. Згідно щорічного звіту ENISA Threat Landscape про стан ландшафту загроз кібербезпеці, новими або найчастішими джерелами інцидентів, з якими стикається організація, є: програми-вимагачі, шкідливе програмне забезпечення, загрози соціальної інженерії, загрози щодо даних, загрози доступності: відмова в обслуговуванні, дезінформація, атаки на ланцюги поставок [1].

Розвідка кіберзагроз (Cyber Threat Intelligence, CTI) – нова сфера інформаційної безпеки, у якій багато організацій інвестують у розробку належних інструментів і послуг, а також у інтеграцію інформації, пов’язаної з розвідувальними даними. Розвідка кіберзагроз дозволить краще зрозуміти мотивацію та тактику зловмисника. Крім того, CTI є важливою для запобігання атак нульового дня.

Розвідка – це інформація та знання, отримані про супротивника шляхом спостереження та аналізу; розвідувальні дані – це результат аналізу, і вони повинні бути ефективними, щоб задовольнити потреби поточних систем захисту, яким доводиться мати справу з кібератаками та реагувати на них. Розвідка про кіберзагрози (CTI) зосереджується на можливостях, мотивації, цілях супротивника та способах їх досягнення. Серед іншого, приклади CTI включають індикатори, сповіщення безпеки, звіти про інциденти та розвідку про загрози, а також будь-яку іншу відповідну інформацію про рекомендовані конфігурації інструментів безпеки [1].

Ефективний обмін розвідданими про кіберзагрози є основою виявлення та запобігання кіберзагрозам, оскільки він дозволяє створювати багаторівневі автоматизовані інструменти зі складними та ефективними захисними можливостями, які безперервно аналізують величезну кількість різнорідних даних, пов'язаних із тактикою та технікою зловмисників. Враховуючи численні архітектури, продукти та системи, які використовуються як джерела даних для механізмів обміну інформацією, необхідні стандартизовані та структуровані представлення CTI, щоб забезпечити необхідний рівень взаємодії між різними зацікавленими сторонами. Тому протягом останнього десятиліття було докладено значних зусиль для стандартизації форматів даних і протоколів обміну інформацією про розвідку загроз, включаючи CTI для Інтернет речей. Актуальною залишається задача покращення обміну даними про кіберзагрози між різними зацікавленими сторонами.

Мета і завдання дослідження. Метою роботи є підвищення ефективності алгоритмів обміну інформацією про кіберзагрози.

Досягнення визначеної мети передбачає вирішення таких завдань:

– провести аналіз платформ розвідки кіберзагроз з відкритим кодом;

– дослідити типи розвідки кіберзагроз;

– проаналізувати стандарти обміну інформацією про загрози;

– дослідити та вибрати канали обміну даними про загрози;

– дослідити виявлення загроз з використанням мови опису правил Yara;

– розробити алгоритм виявлення загроз на базі платформи з відкритим MISP.

Об'єкт дослідження – процеси збору, аналізу та обміну даними про кіберзагрози;

Предмет дослідження – алгоритми аналізу та обміну даними про кіберзагрози.

Методи досліджень. Для розв'язання поставлених задач у даній кваліфікаційній роботі використано: методи розвідки кіберзагроз, методи поширення інформації про загрози, методи проектування.

Наукова новизна одержаних результатів. Удосконалено алгоритми аналізу та обміну даними про кіберзагрози за рахунок використання правил Yara.

Практичне значення отриманих результатів. Розгорнуто систему виявлення загроз на базі платформи з відкритим кодом MISP, яка дозволяє збирати і аналізувати дані про загрози з багатьох джерел. А також дозволяє ділитися даними про виявлені загрози.

Публікації та апробація КР.

1. Терещенко О.С., Яцків В.В. Сучасні платформи розвідки кіберзагроз з відкритим кодом. Матеріали проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2022), Тернопіль, 2022. – С. 100-103.

2. Яцків В.В., Терещенко О.С. Розвідка кіберзагроз з використанням мови опису правил YARA. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2022), Тернопіль, 2022. – С. 40-42.

1 АНАЛІЗ СИСТЕМ РОЗВІДКИ КІБЕРЗАГРОЗ НА БАЗІ ПЛАТФОРМИ З ВІДКРИТИМ КОДОМ

1.1 Визначення ключових понять

Розвідка кіберзагроз (Cyber Threat Intelligence, CTI) – це концепція кібербезпеки, яка передбачає збір, обробку та аналіз даних з багатьох джерел за допомогою розширених аналітичних алгоритмів, про ризики безпеці, які загрожують активам організації [1].

Відсутність точних визначень ключових понять розвідки загроз у багатьох випадках призводить до непорозумінь і плутанини, коли фахівці використовують різні терміни для одного поняття. Тому доцільно привести набір основних визначень, які використовуються в роботі. Зокрема, визначено терміни процес аналізу загроз, джерело CTI, продукт CTI, виробник CTI, споживач CTI та система CTI наступним чином:

– процес аналізу загроз – це будь-який процес, який складається з дій, які виконує аналітик безпеки для перетворення необроблених даних у придатну для використання інформацію;

– джерело CTI – це будь-яке джерело даних, яке може сприяти ситуаційній обізнаності щодо можливостей захисту від кіберзагроз;

– продукт CTI є результатом будь-якого процесу аналізу загроз, який відповідає набору попередньо визначених характеристик якості;

– виробник CTI – це будь-яка організація, яка застосовує процес аналізу загроз для виробництва продуктів CTI;

– споживач CTI – це будь-яка організація, яка може використовувати продукти CTI для підвищення своїх оборонних можливостей або прийняття рішень щодо проблем, пов’язаних з кібербезпекою;

– система CTI – це будь-яка система кібербезпеки, інструмент або система, здатна виконувати або підтримувати частину або всі дії процесу аналізу загроз.

На рисунку 1.1 приведені зв’язки між ключовими концепціями CTI.

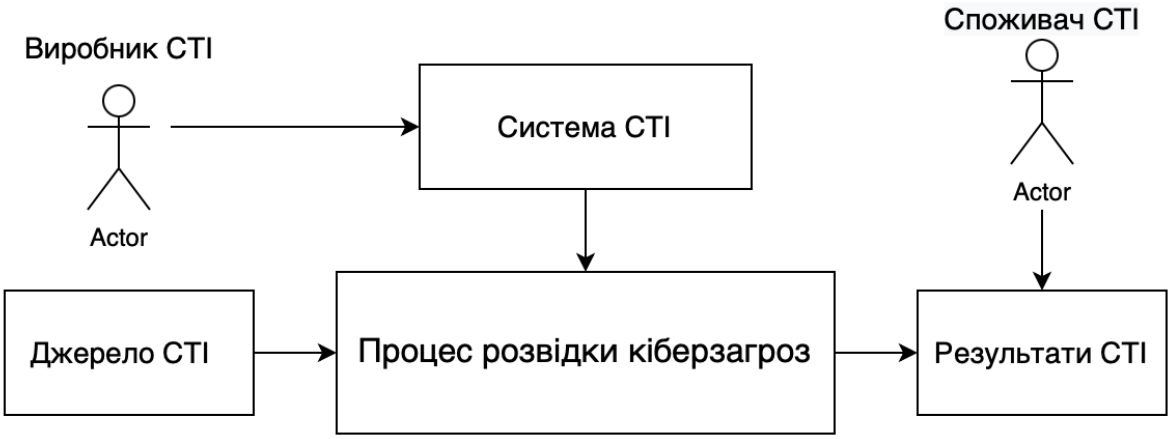

Рисунок 1.1 – Взаємозв’язки між ключовими термінами CTI

Збираючи великі обсяги даних про поточні загрози та тенденції кібербезпеки та виконуючи аналітику цих даних, постачальники аналізу загроз можуть отримувати придатні для використання дані та статистичні дані, які допомагають своїм клієнтам краще виявляти кіберзагрози та готуватися до них.

1.2 Типи розвідки кіберзагроз

У військовому, бізнес-контексті чи контексті кібербезпеки розвідка – це інформація, яка надає організації підтримку прийняття рішень і, можливо, стратегічну перевагу. Розвідка про загрози є частиною більшої стратегії розвідки безпеки. Він містить інформацію, пов’язану із захистом організації від зовнішніх і внутрішніх загроз, а також процеси, політики та інструменти, які використовуються для збору та аналізу цієї інформації.

Розвідувальні дані про загрози забезпечують краще розуміння ландшафту загроз та учасників загрози, а також їхні новітні тактики, методи та процедури. Це дозволяє організаціям діяти проактивно в налаштуванні засобів безпеки для виявлення та запобігання розширеним атакам і загрозам

нульового дня. Багато з цих налаштувань можна автоматизувати, щоб безпека залишалася узгодженою з останніми розвідувальними даними в режимі реального часу.

Переваги використання розвідки кіберзагроз [2]:

– покращує якість оповіщення;

– покращує можливості організації щодо виявлення та реагування;

– збільшує охоплення інцидентів;

– мінімізує час розслідування;

– зменшує середній час для відповіді;

– виявляє критичні загрози.

Розвідка про загрози допомагає організаціям приймати обґрунтовані рішення про те, як найкраще захистити свої IT-ресурси.

Структура розвідки про загрози складається з трьох різних типів (рисунок 1.2) [2]:

– тактична розвідка;

– оперативна розвідка;

– стратегічна розвідка.

Рисунок 1.2 – Типи розвідки про кіберзагрози

Стратегічна розвідка кіберзагроз. Розвідка про загрози враховує не лише технічні аспекти ризиків, але й мотивацію, що стоїть за ними. Стратегічний напрямок розвідки про кіберзагрози враховує, хто або яка

організація керує атаками, які їхні цілі та причина вибору цілі. Вона використовується, щоб забезпечити своєчасне попередження про загрози, що очікуються, і допомогти організаціям проактивно встановити захист на основі сучасних тенденцій атак.

Стратегічна розвідка про загрози збирає та аналізує різнорідні дані, зокрема засоби масової інформації, аналітичні документи від урядів і неурядових організацій, а також експертів у відповідній галузі. Безпекові організації збирають багато інформації в брифінги, документи, звіти та у інші форми. Ця інформація зазвичай використовується IT-менеджерами та CISO, а відповідні основні моменти передаються команді виконавців. Це допомагає організаціям визначити пріоритетність бюджетів і розподіл внутрішніх ресурсів.

Типи інформації, зібраної в рамках стратегічної розвідки про кіберзагрози, включають:

- тенденції атак;
- подробиці про відомі порушення;
- фінансовий вплив кіберзагроз;
- відомі кіберзлочинці, злочинні синдикати та актори національних держав;
- статистична інформація, пов’язана з витоками даних і зловмисним програмним забезпеченням;
- ландшафт загроз, характерний для секторів промисловості.

Тактична розвідка кіберзагроз. Тактична розвідка про кіберзагрози зосереджується на тактиці, техніках і процедурах, щоб визначити, як і де відбуваються атаки та отримати повне розуміння технічних деталей атак. Тактична розвідка про кіберзагрози надає інформацію, необхідну для розробки ефективного захисту, що дозволяє організаціям бути добре підготовленими до реагування. Крім того, це допомагає зупинити напад або пом'якшити його вплив.

Частково тактична розвідка про кіберзагрози оцінює події та розслідування в режимі реального часу для підтримки щоденних заходів безпеки, таких як розробка сигнатур та індикаторів компрометації. У деяких випадках вона включає аналіз низького рівня інтелекту. Часто дані про тактичні загрози надаються сторонніми постачальниками для використання членами IT-команд, включаючи мережеву безпеку, архітектуру та адміністрування.

Тактична розвідка про кібернетичні загрози зазвичай містить інформацію про вектори атак, інструменти та інфраструктуру, які використовують зловмисники. У ньому також детально описано уразливості, на які спрямовано напад, тактику, яку використовують зловмисники, а також стратегії та інструменти, які вони використовують, щоб уникнути або відтермінувати виявлення.

Тактична розвідка про кіберзагрози включає:

– звіти групи нападу;

– доступні патчі;

– звіти про кампанію;

– звіти про інциденти;

– інформація, отримана шляхом збору розвідувальних даних людини;

– відомі індикатори загрози;

– оновлення шкідливих програм.

Оперативна/технічна розвідка кіберзагроз. Інформація, отримана з операційної або технічної розвідки про кіберзагрози, збирається з відомих атак, зокрема активних кампаній, інформації, яка зібрана в результаті розслідувань минулих атак, і даних, наданих сторонніми дослідницькими групами. Додатковими оперативними або технічними джерелами розвідки про загрози є люди, соціальні мережі та чати.

Цей тип розвідки про загрози має менший термін зберігання, ніж тактична розвідка про загрози, і головним чином зосереджується на конкретних індикаторах компрометації (IoC), щоб пришвидшити відповідь на

атаки. Оперативна або технічна інформація про кіберзагрози представлена у звітах, які містять відомості про зловмисну діяльність, рекомендації щодо захисту та усунення, а також попередження про майбутні атаки.

Оперативна або технічна розвідка про кіберзагрози надає IT-командам і командам безпеки конкретні відомості про виявлені індикатори. Потім їх можна включити в захисні системи, такі як фільтри спаму, брандмауери, системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS), оркестровка безпеки, автоматизація та реагування (SOAR), а також інформація про безпеку та керування подіями (SIEM). Дії, вжиті на основі оперативної або технічної інформації про кіберзагрози, включають блокування атак, сортування та перевірку сповіщень, а також пошук і нейтралізацію виявлених загроз.

Приклади технічної розвідки про кіберзагрози включають:

– канали управління;

– деталі, пов’язані з конкретним впровадженням шкідливого програмного забезпечення;

– імена файлів;

– шкідливий трафік;

– підозрілі IP-адреси та домени;

– інструменти, що використовуються для атак;

– URL-адреси.

Замість того, щоб запроваджувати повний обсяг програми аналізу загроз за один раз, необхідно розпочати із зосередження на кожному окремому типі аналізу загроз. Це не тільки спростить загальний процес впровадження, але природним чином призведе до розробки найповнішої програми аналізу загроз.

1.3 Аналіз платформ розвідки кіберзагроз з відкритим кодом

Основна мета розвідки загроз – розпізнати мотиви, поведінку та цілі зловмисника, щоб допомогти фахівцям з безпеки запровадити проактивні заходи безпеки для ефективного запобігання витоку даних.

Розвідка загроз дає змогу виявляти, та боротися з атаками, надаючи відомі сигнатури зловмисного програмного забезпечення, типи даних, на які групи програм-вимагачів націлюються, і ознаки пошкодження пристрою/мережі, на які слід звернути увагу. Захистити організацію від витоку даних і програм-вимагачів неможливо без розуміння вразливостей безпеки, індикаторів загроз і креативних методів злому. Отримавши інформацію з цих даних, розробники або спеціалісти з безпеки зможуть створити надійну парадигму безпеки, точно визначити пріоритети вразливостей, провести аналіз першопричини та розробити інші процеси безпеки високого рівня.

Розглянемо найбільш поширені платформи розвідки кіберзагроз з відкритим кодом.

1. MISP. Malware Information Sharing Platform (MISP), платформа для аналізу та обміну інформацією про загрози з відкритим кодом – це безкоштовна платформа для обміну індикаторами компрометації (Indicator of Compromise, IoC) і інформацією про вразливості між підприємствами. Організації з усього світу використовують платформу для створення надійних спільнот, які обмінюються даними, щоб зіставити їх і краще зрозуміти ризики, націлені на певні галузі чи регіони. MISP пропонує інтерфейс користувача, який дозволяє створювати, шукати та ділитися подіями з іншими користувачами чи групами MISP. Таким чином, замість того, щоб надавати IoC через електронну пошту та у вигляді PDF-файлів, платформа дозволяє компаніям-учасникам ефективніше керувати обміном і централізацією інформації. Крім того, вся інформація, що зберігаються в базі даних MISP, доступна через API, що дозволяє експортувати дані в форми,

включаючи XML, JSON, OpenIOC, STIX та інші. MISP має автоматичний кореляційний механізм, який може знаходити зв'язки між характеристиками, об'єктами та ознаками механізму кореляції шкідливих програм (рисунок 1.3).

Рисунок 1.3 – Загальна структура MISP

Крім того, MISP структуровано зберігає дані, пропонує суттєву підтримку індикаторів кібербезпеки та полегшує обмін даним про загрози як для людей, так і для машин [1].

2. OpenCTI. Проект OpenCTI, також відомий як Open Cyber Threat Intelligence – це платформа, розроблена для полегшення обробки інформації та обміну цими знаннями для цілей розвідки про кіберзагрози. Це результат співпраці між (Групою реагування на комп'ютерні надзвичайні ситуації Європейського Союзу) (CERT-EU) і Національним агентством кібербезпеки

Франції (ANSSI). Для полегшення здатності учасників структурувати, зберігати, організовувати, візуалізувати та ділитися своєю інформацією, платформа тепер повністю опублікована у відкритому коді та стала доступною для всієї спільноти розвідки про кіберзагрози (рисунок 1.4) [2].

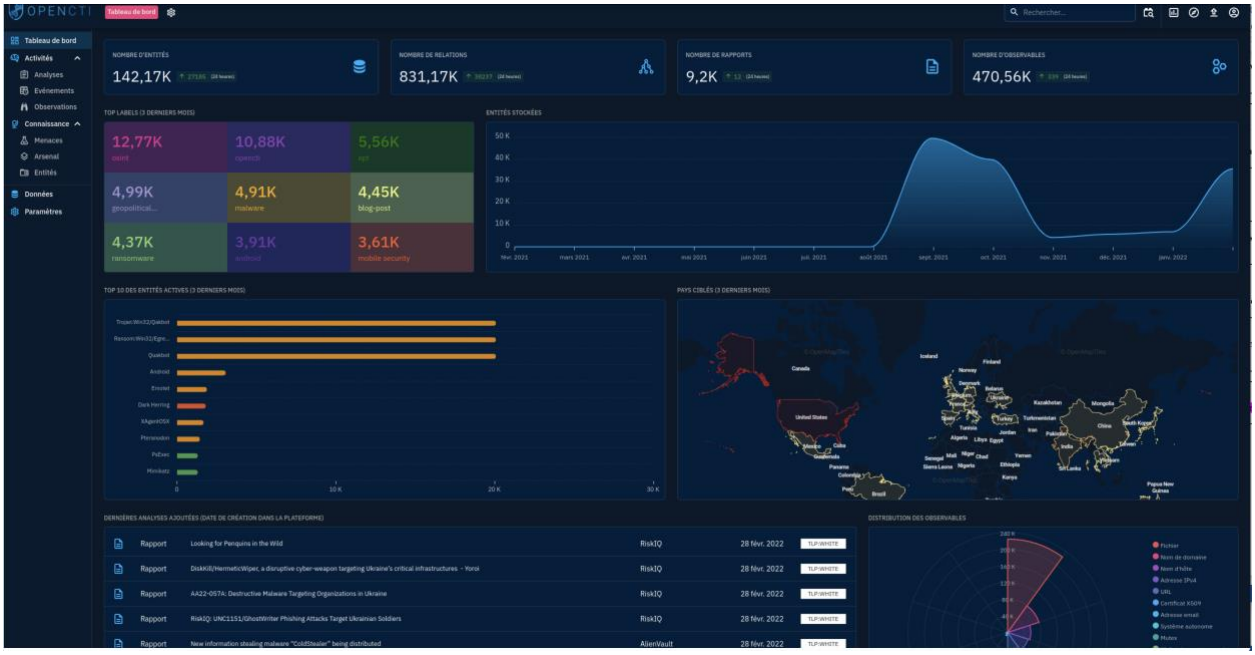

Рисунок 1.4 – Інтерфейс OpenCTI

До важливих елементів включених в дану платформу аналізу загроз необхідно віднести: уніфікована модель даних, яка базується на стандартах STIX2; автоматизовані робочі процеси; інтеграція з екосистемою інформаційних технологій; інтелектуальна візуалізація даних; інструменти для аналізу подій.

OpenCTI, на додаток до ручного введення даних про загрози, підтримує з’єднання для автоматичного отримання даних про загрози та інформації з відомих джерел розвідки про загрози, включаючи MITER ATT&CK, MISP і VirusTotal.

3. Harpoon – це програма командного рядка, яка містить колекцію плагінів Python для автоматизації розвідувальних дій із відкритим кодом. Кожен плагін пропонує команду, яку аналітики можуть використовувати для доступу до API сайтів, таких як MISP, VirusTotal, Shodan, Passive Total,

Hybrid Analysis, AlienVault OTX, Censys, RobTex, ThreatGrid, GreyNoise, TotalHash, MalShare та Have I Been Pwned. Аналітики можуть отримати інформацію про IP-адресу або домен з усіх цих платформ одночасно за допомогою команд вищого рівня. Інші сценарії також можуть здійснювати пошук у сховищах GitHub, соціальних мережах і платформах веб-кешу [3].

4. Yeti. Yeti – платформа, яка була створена у відповідь на необхідність аналітиків безпеки консолідувати різні канали даних про загрози. Yeti дозволяє аналітикам об’єднувати показники компрометації і інформацію про тактику, техніку та процедури, які використовують зловмисники, в єдине уніфіковане сховищ. Yeti пропонує інтерфейс користувача на основі Bootstrap і машинний інтерфейс веб-API (рисунок 1.5).

Рисунок 1.5 – Платформа YETI

Платформа YETI включає в себе добре організоване сховище, яке добре адаптується та розширюється, а також пропонує допомогу в автоматизації [4].

5. GOSINT – це платформа з відкритим вихідним кодом, створена Cisco CSIRT, яка зосереджена на зборі та обробці інформації. Вона збирає,

обробляє та експортує IoC, таким чином контролюючи процес включення даних платформи та збагачуючи його високоякісною інформацією. GOSINT агрегує та перевіряє показники для використання іншими інструментами, такими як MISP і CRITs3, або безпосередньо в системах керування журналами та SIEM, одночасно підтримуючи STIX, TAXII, VERIS, Incident Sharing, які використовуються в системах обміну інформацією про загрози (рисунок 1.6) [5] .

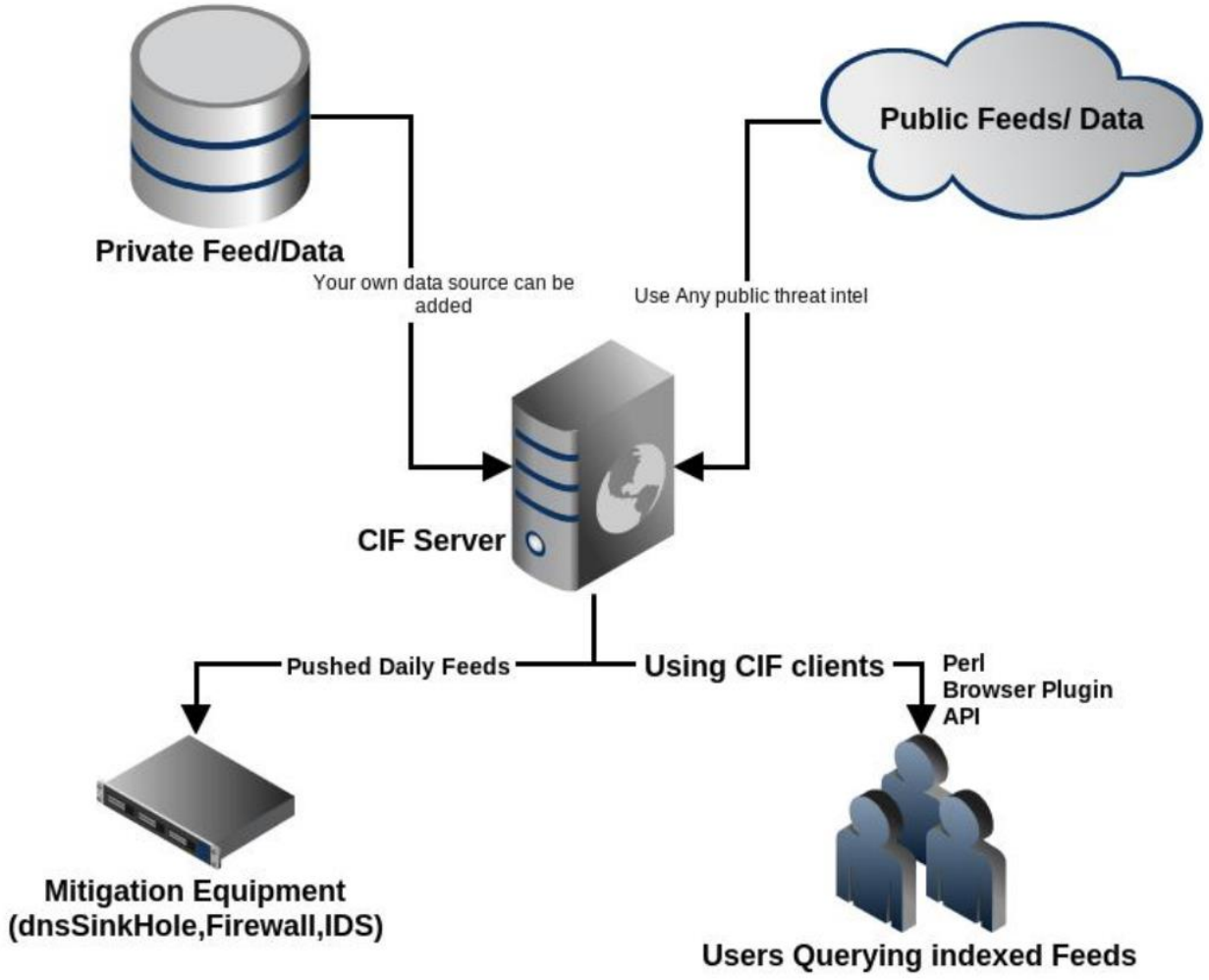

Рисунок 1.6 – Обмін даними в платформі GOSINT

GOSINT додатково підтримує формат обміну описом об’єктів інциденту (IODEF) і формат обміну повідомленнями про виявлення вторгнень (IDMEF), що дозволяє фахівцям-криміналістам збирати структуровані та неструктуровані дані про події, що стосуються третіх осіб.

Інтерфейс GOSINT розроблено на JavaScript. Основні недоліки платформи GOSINT стосуються здебільшого управління пакетами. Зокрема, менеджери пакетів GOSINT надають застарілі версії програмного забезпечення; отже, їх необхідно перевірити, щоб перевірити сумісність. GOSINT має структурований репозиторій, систему керування даними та можливості експорту даних.

6. CIF – це система керування даними про загрози та одна з платформ ENISA для обміну про загрози. CIF дозволяє користувачам аналізувати, нормалізувати, зберігати, оброблювати, запитувати, ділитися та створювати дані CTI, а також збирати інформацію про відомі шкідливі загрози з кількох джерел для ідентифікації (реагування на інциденти), виявлення та пом’якшення. Вона також дозволяє автоматизовано формувати найпоширеніші типи інформації про загрози, такі як IP-адреси та URL-адреси, пов’язані зі зловмисною поведінкою. Структура CIF збирає різноманітні дані спостережень із багатьох джерел. Коли користувач запитує дані CTI, система надає йому серію відсортованих у хронологічному порядку повідомлень; потім користувачі можуть виносити судження, оцінюючи надані результати у спосіб, подібний до аналізу загроз електронною поштою. Сервер CIF складається з багатьох модулів, таких як CIF-smrt, CIF-worker, CIF-starman, CIF-router і ElasticSearch [6].

Модуль CIF-smrt має дві основні функції: отримувати файли через HTTP(s) і аналізувати файли за допомогою вбудованих парсерів для регулярних виразів, файлів JSON, XML, RSS, HTML і простого тексту. Модуль CIF-worker допомагає CIF витягувати додаткову інформацію із зібраних даних про загрози, модуль CIF-starman забезпечує середовище HTTP API, модуль CIF-router діє як посередник між клієнтом і веб-платформою, а модуль ElasticSearch є даними сховище для зберігання даних, що стосуються вторгнень. CIF має структурований репозиторій і систему адміністрування. Вона поєднує інформацію про шкідливу загрозу для ідентифікації, виявлення і пом’якшення.

7. OpenTAXII – це вдосконалена версія платформи TAXII. Дизайн системи відповідає стандартам TAXII. Вона надає набір стандартів загроз і розширювані рівні стійкості та автентифікації через спеціалізований API. Крім того, вона пропонує необхідні послуги та можливість обміну повідомленнями. Інші функції OpenTAXII включають налаштування API, автентифікацію та різноманітне ведення журналів [7].

OpenTAXII має добре організоване сховище та структуру управління, а також може імітувати раніше визначені ситуації та ризики. Вона адаптована і розширювана, оскільки пропонує машинозчитувані дані про загрози, розширення джерела інформації та розширення API.

8. OpenTPX – це платформа сховища даних на основі JSON, яка дозволяє реєструвати та ділитися інформацією про інциденти. OpenTPX є внеском LookingGlass Cyber Solutions у спільноту відкритих кодів. Вона підтримує різноманітні, добре відомі протоколи, такі як HTTP, SMTP, FTP тощо, і була розроблена, щоб сприяти розробці високомасштабованих систем розвідки загроз, аналізу та безпеки мережі, які швидко передають великі обсяги даних. OpenTPX пропонує способи передачі інформації про топологію мережі, сегментацію мережі, метадані загроз, розвідку про загрози та заходи щодо їх пом’якшення [8].

OpenTPX має добре організований репозиторій, який є універсальним і розширюваним, а також пропонує допомогу в автоматизації. Це також покращує можливості обробки даних, дозволяючи додавати доповнення до спостережуваних описів загроз. Вона пропонує повну систему оцінки загроз, яка дає змогу аналітикам безпеки, дослідникам загроз, операторам мережевої безпеки та службам реагування на інциденти легко приймати відповідні рішення щодо пом’якшення загроз.

Тема розвідки про кіберзагрози ще молода і активно розвивається. Аналіз платформ обміну інформацією про загрози показав, що такі платформи мають схожі функції, але й ряд відмінностей. Всі платформи підтримують чотири фази процесу обміну інформацією про загрози,

забезпечуючи при цьому обмін інформацією та спільне використання інформації. Для поширення та інтеграції даних більшість платформ використовують REST API і підтримують стандарти STIX і TAXII. Загалом, гнучкість і сумісність платформ значно відрізняються, проте майже всі платформи можна розширювати та налаштувати під конкретні задачі. Впровадження систем розвідки загроз допомагає організації виявляти та зменшувати різноманітні бізнес-ризики, перетворюючи невідомі загрози на відомі, а також допомагає впроваджувати різноманітні передові стратегії захисту.

2 СТРУКТУРА ТА ПРИНЦИПИ ОРГАНІЗАЦІЇ РОЗВІДКИ КІБЕРЗАГРОЗ

2.1 Життєвий цикл аналізу загроз

Модель життєвого циклу розвідки про кіберзагрози використовується для отримання дієвої інформації з необроблених даних, щоб допомогти організаціям налаштувати захисні механізми, мінімізуючи ризик шляхом зменшення та посилення потенційних поверхонь для атак. Ефективні моделі життєвого циклу кіберзагроз використовують цілісний підхід і працюють як безперервний, циклічний набір процесів, призначених для виявлення прогалин у розвідувальній інформації та підказки щодо нових вимог до збору, які починають цикл розвідувальної інформації заново. Нижче наведено шість основних етапів життєвого циклу аналізу загроз (рисунок .2.1) [9].

Рисунок 2.1 – Основні етапи життєвого циклу аналізу загроз

1. Планування. Щоб розвинути інтелект, важливо починати з правильних запитань. Вони мають бути зосереджені на конкретному факті, події чи діяльності, а не на відкритих питаннях. Крім того, важливо враховувати аудиторію та споживачів інформації. Завчасне виділення часу на планування розвідки про кіберзагрози гарантує, що результати будуть корисними та максимально використають цінні ресурси.

2. Колекція. Збираючи необроблені дані, найкраще використовувати широкий спектр внутрішніх і зовнішніх джерел, які відповідають критеріям, встановленим на етапі планування. Джерела даних для підтримки життєвого циклу аналізу загроз включають:

- підібрана розвідка про загрози;
- дані з відкритої та темної мережі;
- сповіщення про інциденти з внутрішніх систем;
- інформація з джерел новин і соціальних мереж;
- шкідливі IP-адреси, домени та хеші файлів;
- журнали мережевих подій;
- розвідка з відкритим кодом;
- записи реагування на минулі інциденти;
- розвідка третіх сторін.

3. Обробка. Після збору необроблені дані слід відсортувати та впорядкувати. Щоб створити надійний набір даних для аналізу, обробка даних має включати:

- додавання метаданих;
- класифікація;
- очищення;
- моделювання даних;
- дедуплікація;
- збагачення;
- нормалізація.

4. Аналіз. Щоб перетворити необроблені дані на корисну інформацію, фаза аналізу має вирішальне значення. Тут виявляються проблеми безпеки шляхом виявлення підозрілої активності та шаблонів. Необхідно виконувати різні типи аналізу, щоб задовольнити потреби різноманітних аудиторій, наприклад списки загроз і рецензовані звіти. На етапі аналізу життєвого циклу загрози використовуються структуровані аналітичні методи, які перекривають упередження та невизначеності. Аналіз повинен включати:

- співвідношення показників та інцидентів;
- встановлення стосунків;
- структурування даних для індексації та пошуку;
- візуалізація даних.

5. Поширення. Звіти про результати аналізу слід поширювати якомога швидше та надавати у форматах, які відповідають уподобанням споживачів. Хто яку інформацію отримує, має бути встановлено на етапі планування та виконано на етапі розповсюдження. Як зазначалося раніше, дані про загрози повинні бути інтегровані з платформою автоматизації стану кібербезпеки, щоб забезпечити уніфіковану модель кіберризику, що працює майже в реальному часі, для визначення пріоритетів уразливостей і усунення, щоб зменшити ймовірність і вплив загроз.

6. Зворотній зв'язок. Оцінка якості та ефективності розвідки про кіберзагрози підтверджує, що інформація відповідає вимогам, встановленим на етапі планування. Збір відгуків також допомагає виявити прогалини чи помилки та висуває додаткові запитання чи проблеми, що продовжують життєвий цикл аналізу загроз.

2.2 Стандарти обміну інформацією про загрози

Аналітику безпеки доводиться мати справу з різними стандартами для підтримки збору, аналізу, опису та розповсюдження інформації. Система CTI

повинна інтегрувати ці стандарти для сумісності з рештою індустрії кібербезпеки. Стандарти регламентують конкретні процедури, пов’язані з CTI (наприклад, обмін інформацією CTI).

2.2.1 Формат STIX

Structured Threat Information Expression (STIX™) – це мова та формат серіалізації, які використовуються для обміну даними про кіберзагрози (CTI). STIX дозволяє організаціям обмінюватися CTI одна з одною в узгодженому та машиночитаному вигляді, дозволяючи спільнотам безпеки краще розуміти, які комп’ютерні атаки вони найімовірніше побачать, і передбачати та/або реагувати на ці атаки швидше та ефективніше. STIX розроблено для вдосконалення багатьох різних можливостей, таких як спільний аналіз загроз, автоматичний обмін загрозами, автоматичне виявлення та реагування.

Об’єкти та функції, додані для включення в STIX 2.1, представляють ітераційний підхід до виконання основних вимог споживачів і виробників щодо спільного використання CTI.

З STIX вносити та приймати дані розвідки стає набагато простіше. За допомогою STIX усі аспекти підозри, компромісу та приписування можна чітко представити за допомогою об’єктів і описових зв’язків. Інформація STIX може бути представлена візуально для аналітика або збережена у форматі JSON для швидкого читання машиною. Відкритість STIX дозволяє інтегрувати в існуючі інструменти та продукти або використовувати для ваших конкретних потреб аналітика чи мережі.

STIX 2.1 відрізняється від STIX 2.0 наступним чином:

1) нові об'єкти: групування, інфраструктура, мова-контент (інтернаціоналізація), розташування, аналіз шкідливих програм, примітка ;

2) об'єкти, які зазнали значних змін: шкідливі програми, усі SCO;

3) нові поняття: впевненість;

4) кіберспостережувані об’єкти STIX тепер можна безпосередньо пов’язувати за допомогою об’єктів зв’язку STIX;

5) перейменовано конфліктні властивості об’єкта каталогу, об’єкта файлу, об’єкта процесу та об’єкта ключа реєстру Windows;

6) додано зв’язок між індикатором і спостережуваними даними під назвою «на основі»;

7) додано опис до Sighting і додано назву для Location;

8) зроблено деякі зв’язки SCO зовнішніми на доменне ім’я, IPv4-адресу та IPv6-адресу.

Об'єкти STIX 2.1. Об’єкти STIX класифікують кожну частину інформації за допомогою певних атрибутів, які потрібно заповнити. Об’єднання кількох об’єктів за допомогою зв’язків дозволяє легко або складно представляти CTI.

Об’єкти STIX 2 представлені у форматі JSON. На. рисунку 2.2 наведено приклад об’єкта STIX 2.1 Campaign на основі JSON [10]:

```
{
    "type": "campaign",
    "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "spec_version": "2.1",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:23.000Z",
    "name": "Green Group Attacks Against Finance",
    "description": "Campaign by Green Group against targets in the
financial services sector."
}
```

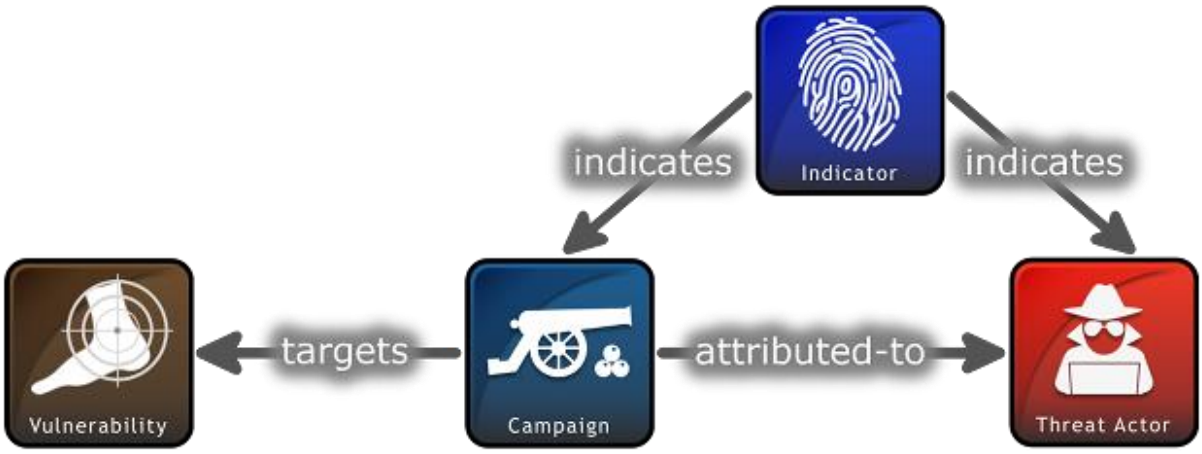

Рисунок 2.2 – Приклад зв’язку STIX 2

В таблиці 2.1 наведено список об’єктів, які можна представити за допомогою STIX. Більш детальну інформацію та візуальні представлення можна знайти в [10].

Таблиця 2.1 – STIX 2.1 визначає 18 об’єктів домену STIX (SDO):

Об’єкт	Назва	Опис
	Шаблон атаки	Тип TTP, який описує способи, якими супротивники намагаються скомпрометувати цілі.
	Операція	Групування змагальної поведінки, яка описує набір зловмисних дій або атак (іноді їх називають хвилями), які відбуваються протягом певного періоду часу проти певного набору цілей.
	Групування	Явно стверджує, що об’єкти STIX, на які посилаються, мають спільний контекст, на відміну від набору STIX (який явно не передає контексту).
	Шкідливе програмне забезпечення	Тип TTP, який представляє шкідливий код.
	Інструмент	Легітимне програмне забезпечення, яке можуть використовувати зловмисники для здійснення атак.
	Індикатор	Містить шаблон, який можна використовувати для виявлення підозрілої або зловмисної кіберактивності.
	Вразливість	Помилка в програмному забезпеченні, яка може бути безпосередньо використана хакером для отримання доступу до системи чи мережі.

Повна інформація про STIX 2 доступна на веб-сайті Технічного комітету (TC) OASIS Cyber Threat Intelligence (CTI) [10, 11].

2.2.2 TAXII

Trusted Automated Exchange of Intelligence Information (TAXII™) – це прикладний протокол для обміну розвідувальною інформацією CTI через HTTPS. TAXII визначає RESTful API (набір служб і обміну повідомленнями) і набір вимог до клієнтів і серверів TAXII. Як показано нижче, TAXII визначає дві основні служби для підтримки різноманітних загальних моделей спільного доступу [12, 13].

Колекція. Колекція – це інтерфейс до логічного сховища об’єктів CTI, наданого сервером TAXII, що дозволяє виробнику розміщувати набір даних CTI, які можуть запитувати споживачі: клієнти та сервери TAXII обмінюються інформацією за моделлю запит-відповідь (рисунок 2.3).

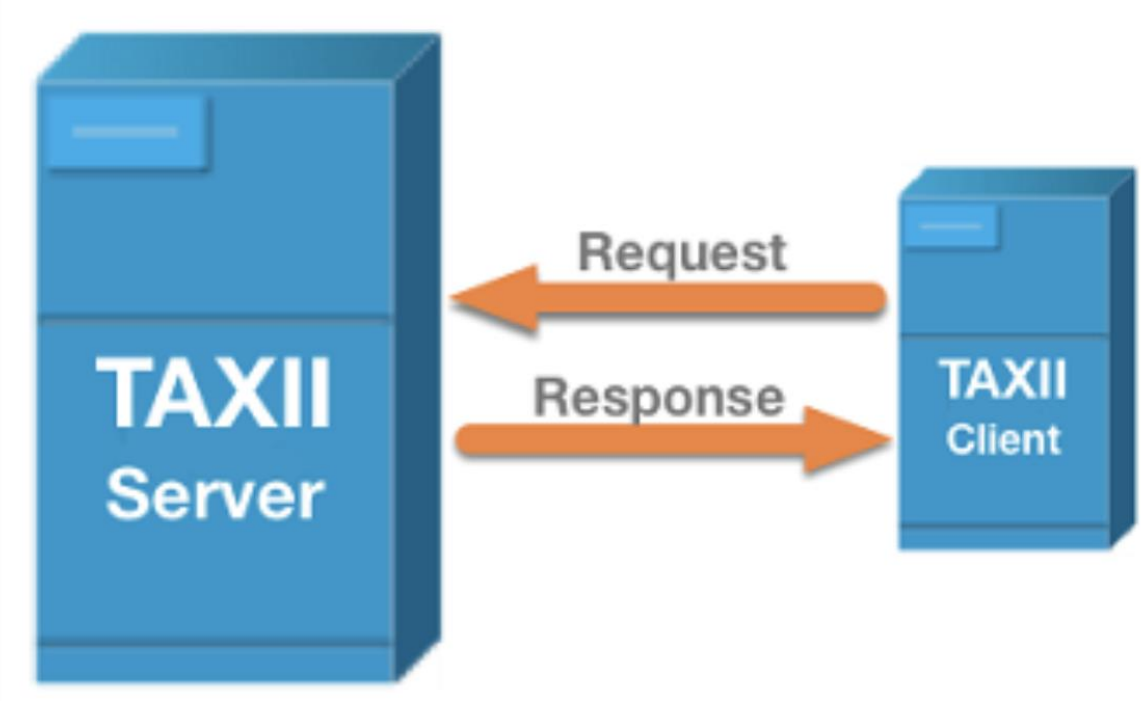

Рисунок 2.3 – Модель спільного доступу «Колекція»

Канал. Канал, який підтримується сервером TAXII, дозволяє виробникам надсилати дані багатьом споживачам, а споживачам – отримувати дані від багатьох виробників: клієнти TAXII обмінюються

інформацією з іншими клієнтами TAXII за моделлю публікації-підписки. Специфікація TAXII 2.1 резервує ключові слова, необхідні для каналів, але не визначає служби каналу. Канали та їхні послуги будуть визначені в пізнішій версії TAXII (рисунок .2.4).

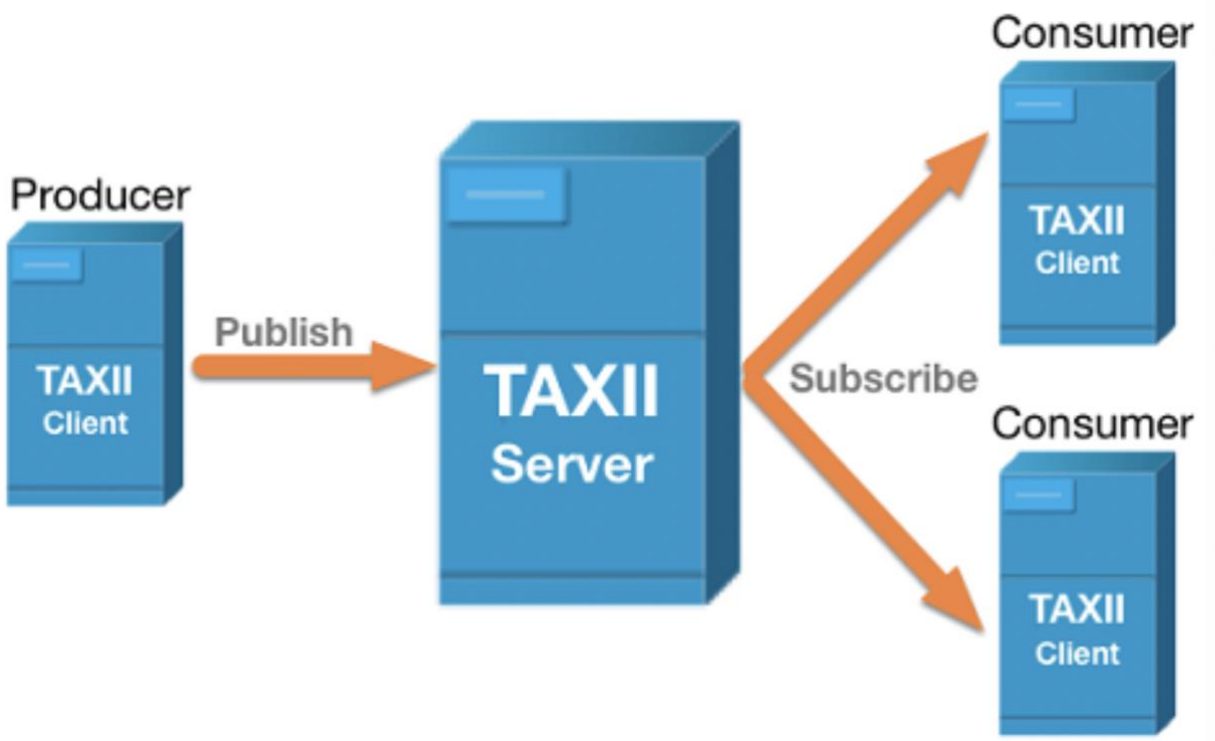

Рисунок 2.4 – Модель спільного доступу «Канал»

Колекції та канали можна організовувати різними способами. Наприклад, їх можна згрупувати для підтримки потреб певної групи довіри.

Примірник сервера TAXII може підтримувати один або кілька коренів API. Корені API — це логічні групування каналів і колекцій TAXII, і їх можна розглядати як екземпляри API TAXII, доступні за різними URL-адресами, де кожен кореневий API є «кореневою» URL-адресою конкретного екземпляра API TAXII.

TAXII покладається на існуючі протоколи, коли це можливо. Зокрема, сервери TAXII виявляються в мережі за допомогою записів служби DNS (та/або за допомогою кінцевої точки виявлення, описаної в наступному розділі). Крім того, TAXII використовує HTTPS як транспорт для всіх

комунікацій, а також використовує HTTP для узгодження вмісту та автентифікації.

TAXII був спеціально розроблений для підтримки обміну CTI, представленим у STIX, і підтримка обміну вмістом STIX 2.1 є обов'язковою для впровадження. Однак TAXII також можна використовувати для обміну даними в інших форматах. Важливо зазначити, що STIX і TAXII є незалежними стандартами: структури та серіалізація STIX не залежать від жодного конкретного транспортного механізму, і TAXII можна використовувати для транспортування даних, відмінних від STIX.

Принципи проектування TAXII включають мінімізацію операційних змін, необхідних для прийняття; легка інтеграція з існуючими угодами про спільний доступ і підтримка всіх широко використовуваних моделей обміну загрозами: хаб-і-зв'язок, одноранговий зв'язок, джерело-підписник.

2.2.3 OpenloC

OpenloC, цей стандарт є форматом XML для передачі даних IoC. Система була розроблена Mandiant/FireEye і є безкоштовною для використання. Однак цю систему складно інтегрувати в автоматизовані процеси генерації та споживання, оскільки вона створює три записи для кожного IoC – метадані, посилання та визначення [14].

Mandiant і FireEye пройшли через злиття, ребрендинг і поділ. У результаті відповідальність за OpenIoC тепер лежить на FireEye. Компанія пропонує безкоштовний редактор OpenIoC, OpenIoC Writer і IoC Finder.

2.2.4 MAEC

Перелік і характеристика атрибутів зловмисного програмного забезпечення (MAEC) – це проект із відкритим вихідним кодом, який створює низку макетів, які можна використовувати для надсилання чи отримання розвідувальних даних про зловмисне програмне забезпечення. Формати пропонують мови для кодування даних для використання

інструментами, вилучення закодованих даних у форматі, зрозумілому людині, і автоматизованої передачі між інструментамиv [15].

MAEC схожа на мову програмування, яка описує поведінку та характеристики кожного зловмисного програмного забезпечення в пакеті, який містить записи різних форматів.

2.3 Використання правил YARA в розвідці кіберзагроз

Головною ідеєю при початковій оцінці підозрілих файлів є синтаксичні підписи, які вже тривалий час використовуються у боротьбі зі шкідливим програмним забезпеченням. Ці сигнатури передусім дозволяють виявляти та ідентифікувати сімейства шкідливих програм, що допомагає пришвидшити процедуру аналізу, використовуючи попередні знання щодо цих сімейств. Одним із важливіших і популярних інструментів у цьому контексті є YARA [16, 17].

YARA – це високоефективний механізм зіставлення шаблонів, який супроводжується доступною мовою опису правил. Завдяки своїй ефективності, що YARA стала квазістандартом із широким впровадженням серед практиків і багатьма правилами, які поширюються відкрито або в приватних групах пошуку загроз. При цьому, розробка правил, які добре виявляють і водночас уникають помилкової класифікації, все ще залишається актуальною задачею. Цей процес часто виконується вручну, що вимагає від аналітика знань і досвіду. Серед поширених варіантів використання YARA можна навести наступні: ідентифікація та класифікація шкідливих програми; знаходження нових зразків на основі характерних для сімейства шаблонів; служби реагування на інциденти можуть розгортати правила YARA для ідентифікації зразків і скомпрометованих пристроїв; проактивне впровадження спеціальних правил YARA може посилити захист організації.

Під час аналізу шкідливого програмного забезпечення фахівці створюють правила YARA, які в подальшому захисники будуть використовувати для виявлення цього ШПЗ. При збиранні індикаторів компрометації (IoC) шкідливого програмного забезпечення програмного забезпечення з інших джерел, можна писати правила YARA або знаходити правила YARA з інших джерел і надавати їх захисникам для виявлення ШПЗ. Список джерел правил YARA наведений в [18].

Синтаксис правила YARA. Синтаксис вимагає, щоб кожне правило YARA починалося зі слова rule. Після слова rule потрібно буде додати ім'я або ідентифікатор, який містить будь-які буквено-цифрові символи. Синтаксис YARA також допускає підкреслення в імені/ідентифікаторі, але не дозволяє першому символу бути числом. Зазвичай правила складаються з двох розділів: визначення рядків і умови. Розділ визначення рядків можна опустити, якщо правило не буде перевіряти жодний рядок, але розділ умов завжди потрібний. Розглянемо просте правило Yara, яке завжди має значення true, тобто воно завжди відповідає будь-якому файлу:

```
rule test
{
        condition: true
}
```

Щоб проаналізувати файл за допомогою правила yara, використовується команда:

yara <yara-rule> <target-file>,

де перший аргумент – файл правила, а другий – файл, який потрібно сканувати.

Метадані. Метадані не впливають на те, що шукатиме правило YARA, натомість вони надають корисну інформацію про саме правило, зокрема: author**,** date**,** version**,** reference**,** description, hash.

Параметри YARA. Щоб зробити аналіз файлів більш ефективним використовують параметри YARA. Команда для запуску аналізу із параметрами має вигляд:

yara [OPTIONS] <rule-file> <target-file>

Розглянемо основні параметри в правилах YARA:

-m –друкує метадані правил, які були виконані під час аналізу. Метадані можуть надати хеш sha256 зразка, який згодом можна надіслати в інші механізми сканування, наприклад, Virus Total або Hybrid Analysis;

-c – виводить кількість збігів у форматі:

file path:match result (шлях до файлу: результат відповідності);

-s – друкує відповідні рядки у форматі:

hexadecimal virtual address:$string identifier:string value.

Розглянемо приклад правила для ідентифікації pdf файлу.

```
rule check_pdf
{
  meta:
    author = "magistr"
    description = "Identification PDF files."
  strings:
    $xpdf = "%PDF"     # %PDF  це стандартний заголовок для файлів
PDF
    $ypdf = "%%EOF"    # %%EOF  це стандартний маркер кінця файлу
PDF
  condition:
    $xpdf at 0 and $ypdf
}
```

Виконання правила запускаємо командою:

$ yara -m check_pdf.yar test555.pdf

Результатом виконання правила буде інформація, яка підтверджує, що виявлено файл pdf.

check_pdf [author="magistr",description="Identification PDF files."] test555.pdf

Однак, покладатися лише на захист на основі правил вже недостатньо. Зловмисники розробили контрзаходи, які вони можуть використовувати, щоб обійти цей метод. Використовуючи різноманітні служби шифрування, пакувальники та поліморфізм, вони можуть легко генерувати ШПЗ, яке є достатньо відмінним, щоб його не ввиявляли існуючі сигнатури. Відповідно, потрібен деякий час, перш ніж буде створено нові правила. Однак, ці недоліки не роблять виявлення на основі сигнатур застарілим механізмом. Фахівці з безпеки діляться новими індикаторами загроз, тому ці типи інструментів залишаться актуальними і дієвими.

Розвідка кіберзагроз поєднує численні фактори, включно з мотивацією кіберзлочинців та індикаторами компрометації, щоб допомогти командам безпеки зрозуміти виклики від очікуваної кіберзагрози та підготуватися до них. Надаючи командам безпеки актуальні дані про кіберзагрози, що насуваються, розвідка кіберзагроз заохочує проактивний підхід до кібербезпеки – найефективнішого типу кіберзахисту.

2.4 Структура та алгоритм розвідки кіберзагроз

Система розвідки про кібернетичні загрози дозволяє ефективно зменшувати ризик загроз. Основні модулі структури наступні: модуль агрегації даних; модуль аналізу загроз; модуль машинного навчання; модуль автоматизації (рис.2.5). Розглянемо призначення модулів детальніше [20, 21].

Модуль агрегації даних. Модуль агрегації даних про загрози є важливим елементом будь-якої системи розвідки про кіберзагрози. Першим кроком процесу кіберрозвідки є збір даних про загрози. Рішення для кіберрозвідки об’єднують численні канали розвідки про загрози, щоб

забезпечити послідовну категоризацію та характеристику подій кіберзагроз. Велика кількість джерел допомагає командам з кібербезпеки визначати тенденції в діяльності зловмисників. Більше даних про історію загроз означає більше важливої інформації для команд з кібербезпеки. Аналіз кіберзагроз ефективніший із великими наборами даних, особливо якщо його доповнити машинним навчанням.

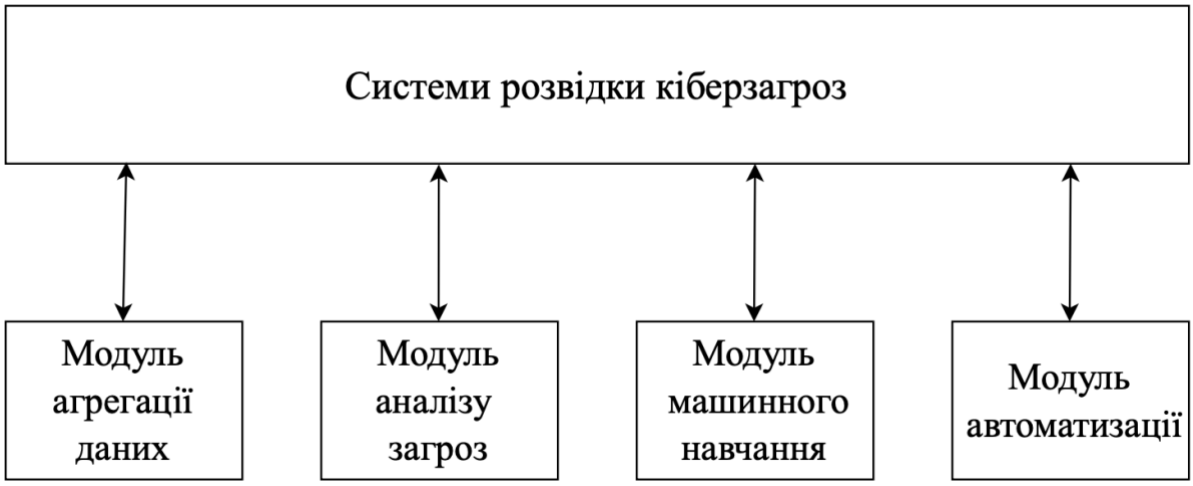

Рисунок 2.5 – Структура системи розвідки кіберзагроз

Модуль аналізу загроз. Після того, як база даних загроз готова, рішення кіберрозвідки використовують модуль аналізу загроз, щоб проаналізувати отримані дані, класифікувати їх на основі ризику та поєднати зі значущим контекстом, щоб отримати корисну інформацію про загрози, з якими стикається організація. У зв’язку з тим, що галузі, як очікується, зіткнуться зі зростаючими загрозами кібербезпеці у 2022 році та пізніше, боротьба зі складними та добре скоординованими спробами атак є критично важливою. Аналіз загроз дає змогу командам безпеки залишатися попередженими та готувати контрзаходи для конкретних, ймовірних кібератак.

Модуль машинного навчання. Поява машинного навчання (ML) значно розширила можливості рішень кіберрозвідки. Модуль ML вирішує дві великі проблеми захисту від загроз: швидку еволюцію поширених кіберзагроз і постійне зростання кількості цих загроз. Можливості розпізнавання шаблонів

і прогнозування загроз у майже реальному часі ML з використанням великих наборів даних допомагають фахівцям із кібербезпеки швидко виявляти та визначати пріоритетність кіберзагроз і реагувати на ті, які потребують втручання людини.

Модуль автоматизації. Модуль автоматизації об’єднує три інші модулі. Це дозволяє рішенням кіберрозвідки аналізувати кіберзагрози, передаючи великі набори даних про загрози через компонент машинного навчання. Автоматизація дозволяє системі проактивно виявляти та блокувати кіберзагрози та повідомляти команди безпеки, коли потрібне їхнє втручання.

Сфера аналізу кіберзагроз отримує переваги від застосування нових методів у інформатиці, зокрема, науки про дані та машинного навчання. Ці дисципліни можуть допомогти автоматизувати масштабний аналіз інформації про кіберзагрози, допомагаючи знаходити функції та виявляти шаблони, які підтримують ефективнішу класифікацію загроз.

Інформація, зібрана в циклі розвідки про кіберзагрози, служить основою для автоматизованого аналізу (обробки) даних розвідки. Робочі процеси можна застосовувати до даних, щоб зменшити шум, виявити та ідентифікувати зловмисну активність, а також сформувати точніше розуміння тактичних методів і процедур противника. Цього можна досягти шляхом об’єднання та кореляції підтверджених показників компромісу, отриманих із кількох звітів аналізу. Важливим кроком у цьому процесі є перевірка зібраних даних на їх достовірність.

Загальник алгоритм розвідки кіберзагроз приведений на рисунку 2.6.

Перший крок алгоритму «Знайти» має на меті дати відповідь на запитання: «Хто, що, коли, де, чому» та використовується для визначення кандидата на ціль.

На другому кроці «Виправити» здійснюється перевірка цілей, визначених на попередньому кроці, яка зазвичай включає кілька джерел вимірювання одного й того ж показника за допомогою не менш як трьох методів з метою незалежного підтвердження результатів. Цей крок

ефективно перетворює дані розвідки, отримані під час кроку «Знайти», у докази, які можна використовувати як основу для дій на наступному кроці.

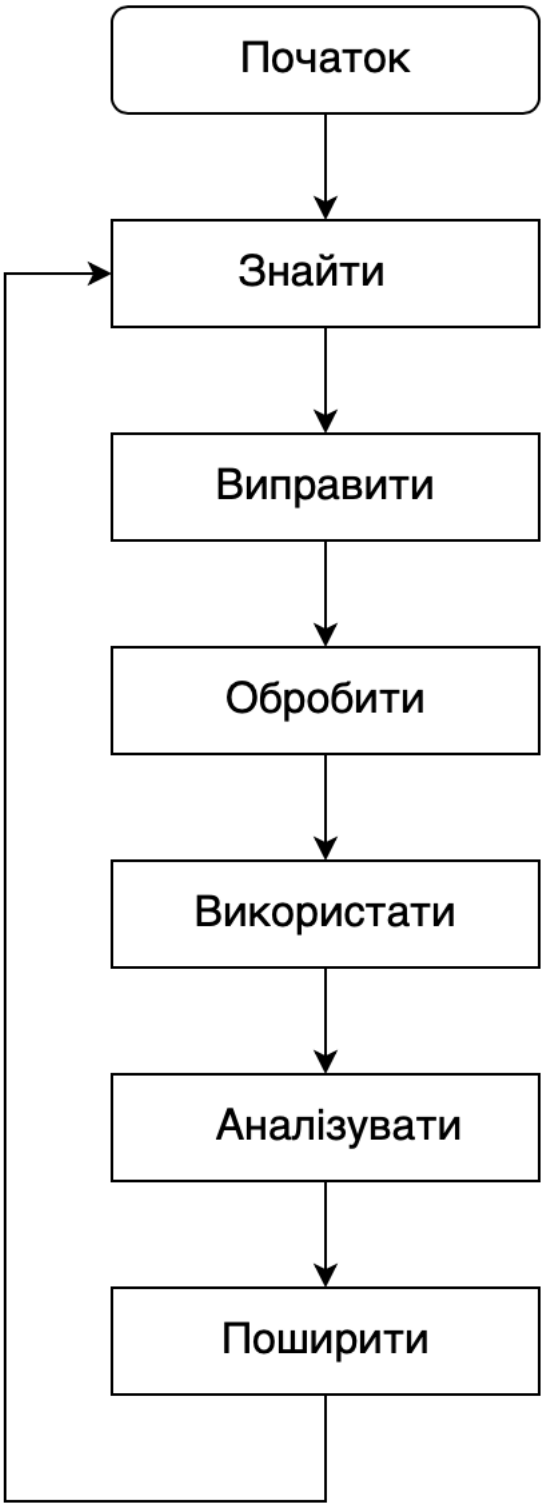

Рисунок 2.6 – Алгоритм розвідки кіберзагроз

Перевага перших трьох кроків для реагування полягає в тому, що вони дозволяють набагато більш детально оцінити ресурси, необхідні для досягнення мети вимог до розвідки. По суті, «Знайти та виправити» допомагає команді створити кінцевий ефект, будь то видалення сайту, підтвердження витоку даних або аналіз зловмисного програмного забезпечення. Оскільки ці етапи часто є нетривіальними, це може вивести цю підоперацію за рамки ширшої операції, надаючи оперативному керівнику чітке рішення, як діяти дальше.

На кроці «Використати» відбувається деконструкція доказів, отриманих на завершальній фазі. Мета цього кроку не збігається з етапом аналізу, оскільки мета полягає в тому, щоб створити нові вимоги до розвідки для наступного циклу, який додасть ширшої картини розвідці.

На основі доказів, отриманих в попередніх двох кроках, на кроці «Обробити» керівник операції нав’язує свої правила цілі.

Крок «Аналізувати» має дати відповідь на питання, який результат аналізів і на уточнити вимоги до розвідки.

Завданням останнього кроку «Поширити» є публікація результатів дослідження зацікавленим сторонам і поєднати використані докази з більш широкою картиною розвідки.

3 СИСТЕМА РОЗВІДКИ КІБЕРЗАГРОЗ НА БАЗІ ПЛАТФОРМИ MISP

3.1 Встановлення та налаштувати MISP

Метою MISP є сприяння обміну структурованою інформацією всередині співтовариства безпеки та за кордоном. MISP надає функціональні можливості для підтримки обміну інформацією, а також використання зазначеної інформації системами виявлення вторгнень у мережу (NIDS), LIDS, а також інструментами аналізу журналів, SIEM.

Основні функції MISP [22 -23]:

1. Ефективна база даних і індикаторів IOC, яка дозволяє зберігати технічну та нетехнічну інформацію про зразки зловмисного програмного забезпечення, інциденти, зловмисників і розвідку.

2. Автоматичний пошук кореляції зв’язків між атрибутами та індикаторами зловмисного програмного забезпечення, кампаній атак або аналізу. Механізм кореляції включає кореляцію між атрибутами та більш розширені кореляції, такі як кореляція нечіткого хешування (наприклад, ssdeep) або зіставлення блоків CIDR. Також можна ввімкнути кореляцію або вимкнути подію для кожного атрибута.

3. Гнучка модель даних, у якій складні об’єкти можна виражати та зв’язувати разом, щоб виражати дані про загрози, інциденти чи пов’язані елементи.

4. Вбудована функція обміну для спрощення обміну даними за допомогою різних моделей розподілу. MISP може автоматично синхронізувати події та атрибути між різними примірниками MISP. Розширені функції фільтрації можна використовувати для відповідності політиці спільного використання кожної організації, включаючи гнучку групу спільного доступу та механізми розподілу на рівні атрибутів.

5. Інтуїтивно зрозумілий інтерфейс користувача для створення, оновлення та спільної роботи над подіями та атрибутами/індикаторами. Графічний інтерфейс для легкої навігації між подіями та їхніми кореляціями.

Функція графіка подій для створення та перегляду зв’язків між об’єктами та атрибутами. Розширені функції фільтрації та списки попереджень, які допомагають аналітикам вносити події та атрибути та обмежують ризик помилкових спрацьовувань.

6. Зберігання даних у структурованому форматі (що дозволяє автоматизовано використовувати базу даних для різних цілей) із широкою підтримкою показників кібербезпеки разом із показниками шахрайства, як у фінансовому секторі.

7. Експорт: генерація IDS, OpenIOC, вихідний текст, CSV, MISP XML або JSON для інтеграції з іншими системами (ідентифікатори мережі, ідентифікатори хостів, спеціальні інструменти), формат кешу (використовується для криміналістичних інструментів), STIX (XML і JSON) 1 і 2, експорт NIDS (Suricata, Snort і Bro/Zeek) або зона RPZ. Багато інших форматів можна легко додати за допомогою модулів misp.

8. Імпорт: масовий імпорт, пакетний імпорт, імпорт із OpenIOC, пісочниці GFI, ThreatConnect CSV, стандартного формату MISP або STIX 1.1/2.0. Багато інших форматів легко додаються за допомогою модулів misp.

9. Гнучкий безкоштовний інструмент імпорту тексту для полегшення інтеграції неструктурованих звітів у MISP.

10. М’яка система для спільної роботи над подіями та атрибутами, що дозволяє користувачам MISP пропонувати зміни або оновлення атрибутів/індикаторів.

11. Обмін даними: автоматичний обмін та синхронізація з іншими сторонами та довірчими групами за допомогою MISP.

12. Делегування спільного доступу: дозволяє простий псевдоанонімний механізм делегувати публікацію події/індикаторів іншій організації.

13. Гнучкий API для інтеграції MISP із вашими власними рішеннями. MISP поєднується з PyMISP, яка є гнучкою бібліотекою Python для отримання, додавання або оновлення атрибутів подій, обробки зразків шкідливих програм або пошуку атрибутів. Повний API restSearch для легкого

пошуку індикаторів у MISP і експорту їх у всіх форматах, які підтримує MISP.

14. Регульована таксономія для класифікації та позначення подій відповідно до власних схем класифікації або існуючої класифікації. Таксономія може бути локальною для вашого MISP, але також доступною для інших примірників MISP.

15. Словники розвідки, які називаються галактикою MISP і в комплекті з існуючими загрозами, зловмисними програмами, RAT, програмами-вимагачами або MITER ATT&CK, які можна легко пов’язати з подіями та атрибутами в MISP.

16. Модулі розширення в Python для розширення MISP власними службами або активації вже доступних misp-модулів.

17. Підтримка спостереження для отримання спостережень від організацій щодо спільних показників і атрибутів. Спостереження можна надати через інтерфейс користувача MISP, API як документ MISP або документи спостереження STIX.

18. Підтримка STIX: імпорт і експорт даних у форматі STIX версії 1 і версії 2.

19. Вбудоване шифрування та підпис сповіщень через GnuPG та/або S/MIME залежно від уподобань користувача.

20. Канал публікації та підписки в режимі реального часу в MISP, щоб автоматично отримувати всі зміни (наприклад, нові події, індикатори, спостереження або теги) у ZMQ (наприклад, misp-dashboard) або публікацію Kafka.

Для проведення досліджень встановлюємо MISP на віртуальну машину (VM) у VirtualBox. Для цього завантажуємо VM MISP з офіційного сайту [25]. Запускаємо віртуальну машину (рисунок 3.1). У браузері на хост-машині відкриваємо https://localhost:8443.

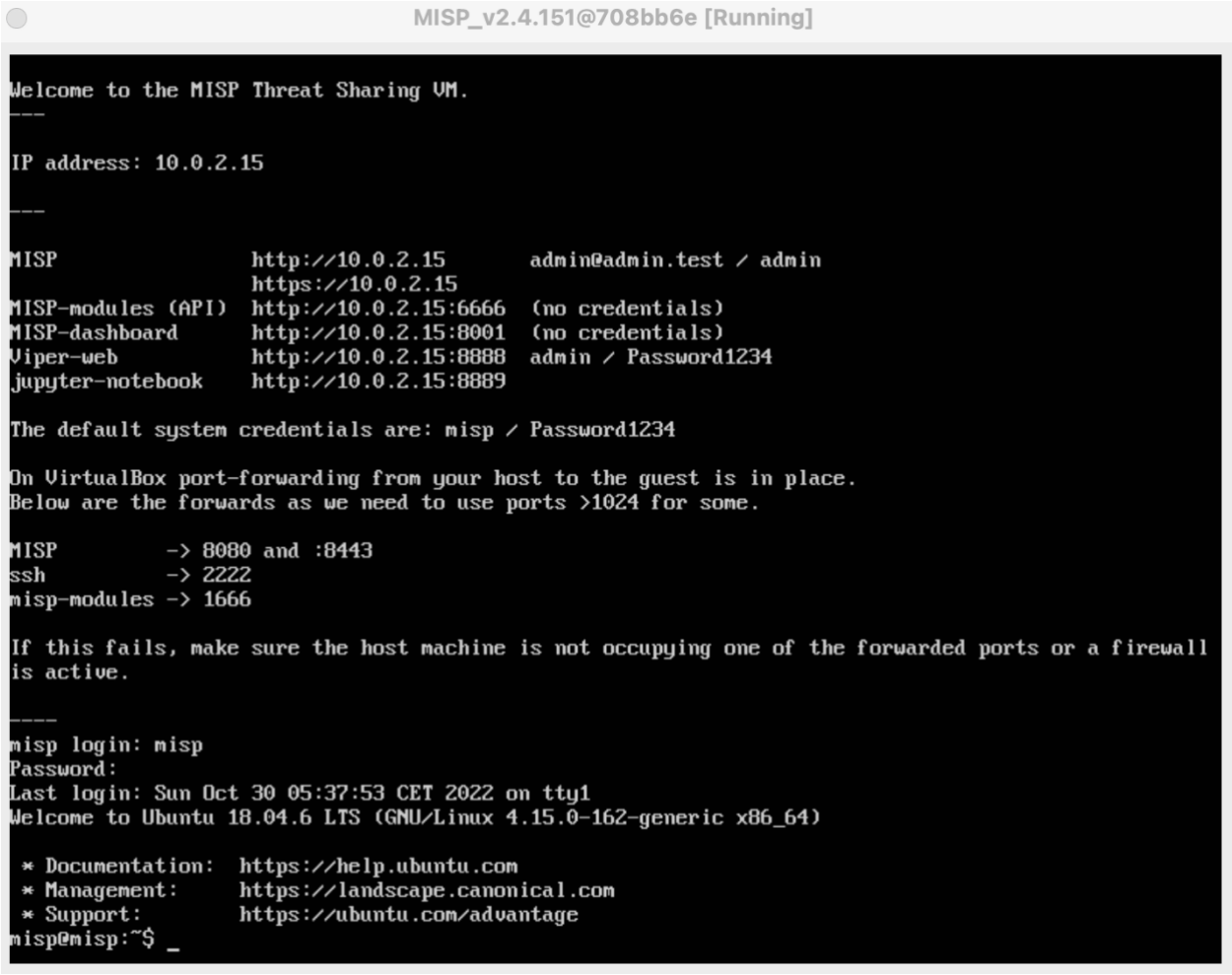

Рисунок 3.1 – Початковий екран після запуску MISP

Ігноруємо попередження про сертифікат (MISP використовує самопідписаний сертифікат).

Входимо, використовуючи ім’я користувача за замовчуванням: admin@admin.test і пароль admin (рисунок 3.2).

Коли буде запропоновано змінити пароль. Натискаємо редагувати мій профіль «Edit My Profile» і змінюємо адресу електронної пошти, якщо ви хочете отримувати електронні листи для облікового запису адміністратора за умовчанням.

Натискаємо синхронізація каналів списку дій «Sync Actions > List Feeds».

Натискаємо завантажити стандартні метадані каналу «Load default feed metadata».

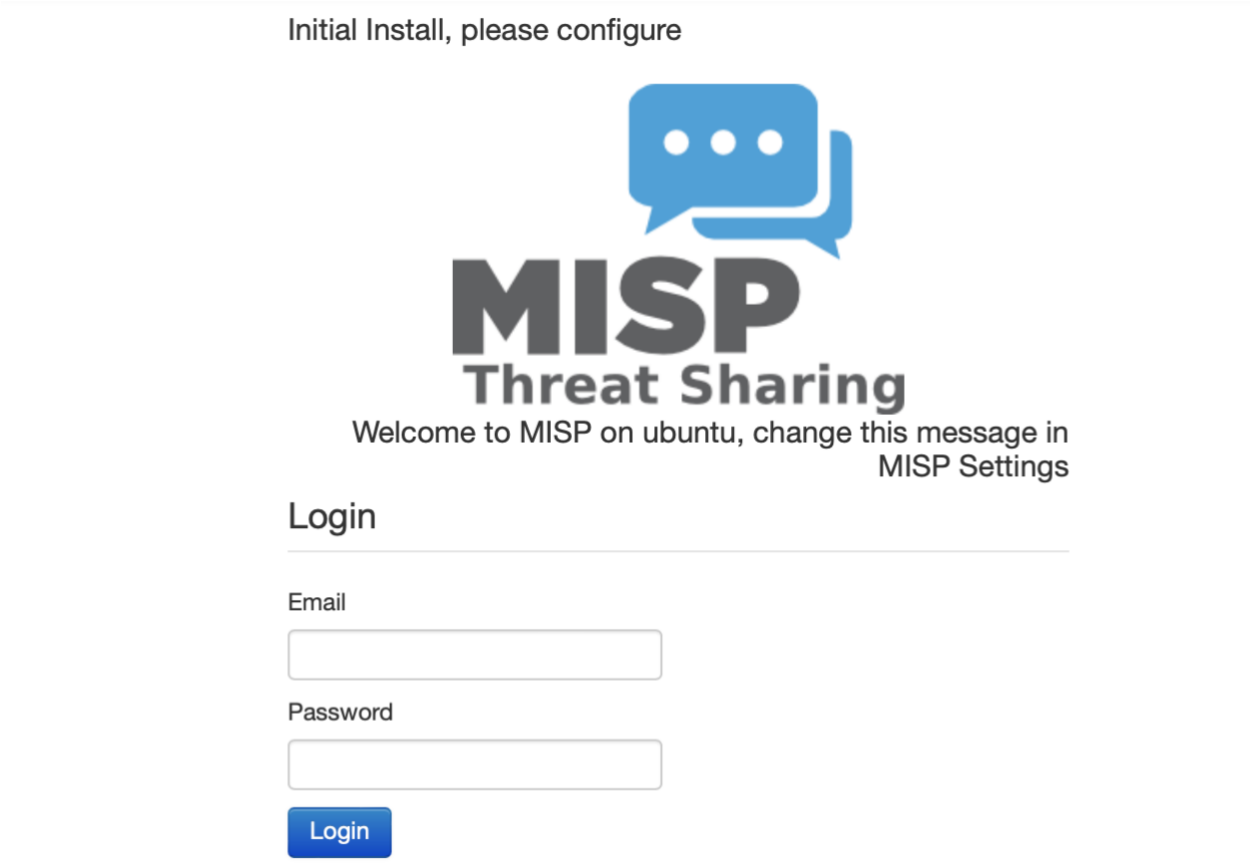

Рисунок 3.2 – Інтерфейс входу в MISP з браузера хоста

Ставимо прапорці біля каналів, які потрібно ввімкнути, а потім натисніть увімкнути вибране «Enable selected» (рисунок 3.3).

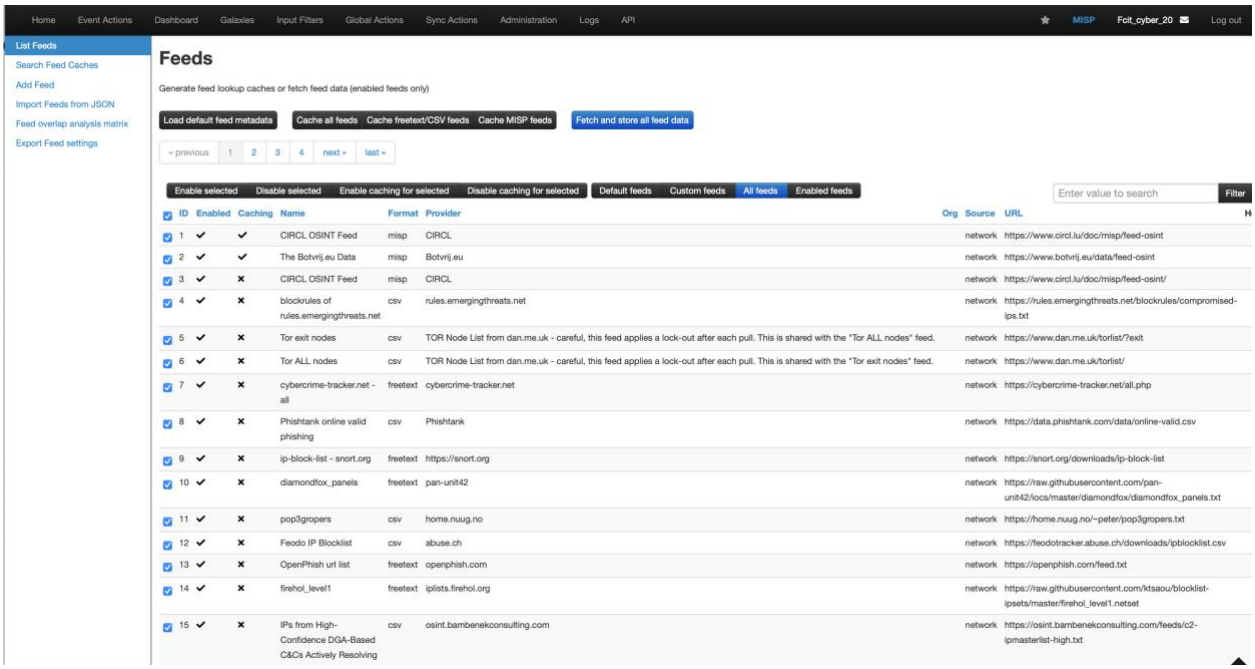

Рисунок 3.3 – Вибір та синхронізація каналів списку дій

Натискаємо отримати та зберегти всі дані каналу «Fetch and store all feed data».

Натискаємо завдання адміністрування «Administration > Jobs» та переконуємося, що завдання fetch_feed успішно виконано (рисунок 3.4). Якщо цього не сталося, перевіряємо журнал помилок за адресою /var/log/apache2/misp.local_error.log. Помилки можуть виникнути віртуальна машина втратить підключення до Інтернету.

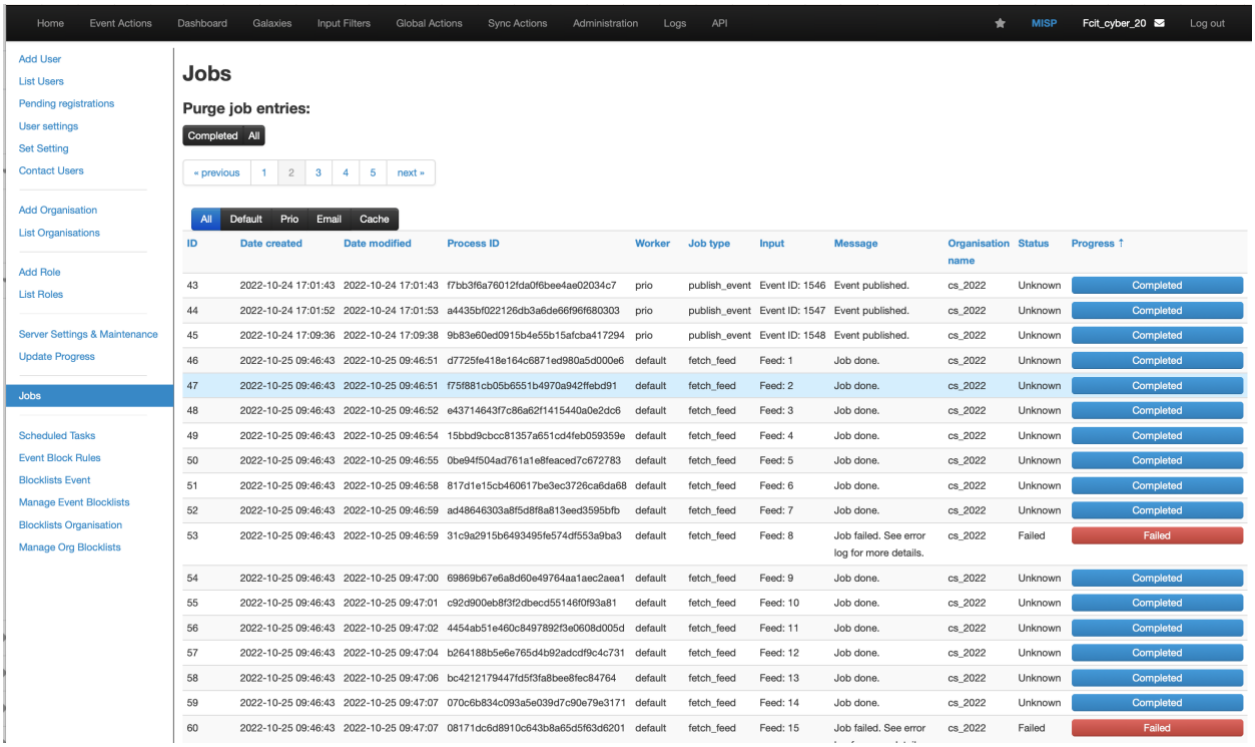

Рисунок 3.4 – Завантаження каналів подій

Як видно з рисунку 3.4 помилка виникла тільки при завантаженні даних з двох каналів, завантаження даних інших каналів відбулося успішно.

Наступним кроком необхідно додати користувача. Для цього натискаємо «адміністрування», «додати користувача» «Administration > Add User» та створюємо обліковий запис користувача для регулярного використання MISP без права адміністратора.

3.2 Аналіз подій при розвідці кіберзагроз

Удосконалення процесу аналізу може варіюватися від простого сповіщення про хибно-позитивний результат або виправлення друкарської помилки, аж до повного конкурентного або контраналізу вихідного аналізу.

Поширеною проблемою в аналізі загроз є вдосконалення існуючих аналізів і особливо те, як це зробити ефективно. Одне з головних запитань, яке варто задати [23]: «Якою буде цільова аудиторія покращеного аналізу та його мета?». При цьому можуть бути наступні три відповіді.

1. Інформування початкового аналітика/автора (наприклад, постачальника засобів безпеки або CSIRT) про конкретну помилку чи помилку, яку потрібно виправити.

2. Удосконалення існуючого аналізу шляхом виконання додаткового аналізу або перегляду, який буде наданий іншій групі (наприклад, певній складовій частині, або команді у вашій організації, або члену ISAC тощо).

3. Кінцевим споживачем буде автомат.

Для того щоб переглянути деталі події необхідно натиснути ідентифікатор даної події «event IDs» (рисунок 3.5).

MISP дозволяє додати теги до всієї події. Для більш точної специфікації теги також можна розмістити на рівні атрибутів. Це дозволяє користувачеві надати більш детальний і вибірковий перегляд кожного атрибута. Якщо тег застосовується до всіх або більшості атрибутів у події, найкраще включати певний тег лише для атрибутів, коли вони є винятком із тегу, встановленого на рівні події. На наведеному нижче знімку екрані показаний приклад найкращої практики: тег tlp:white встановлюється лише на рівні події (рисунок 3.6).

На рисунку 3.7 приведена детальна інформація про подію з ID 1559.

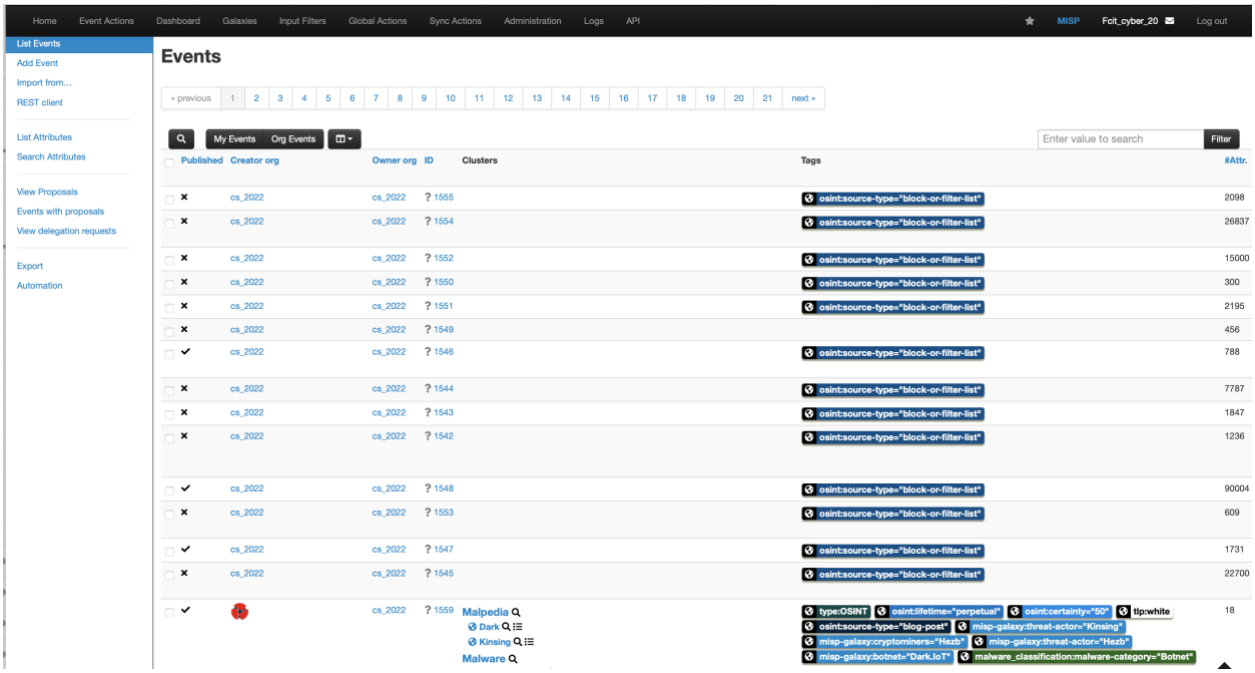

Рисунок 3.5 – Вікно подій

Рисунок 3.6 – Детальна інформація про подію з ID 1559

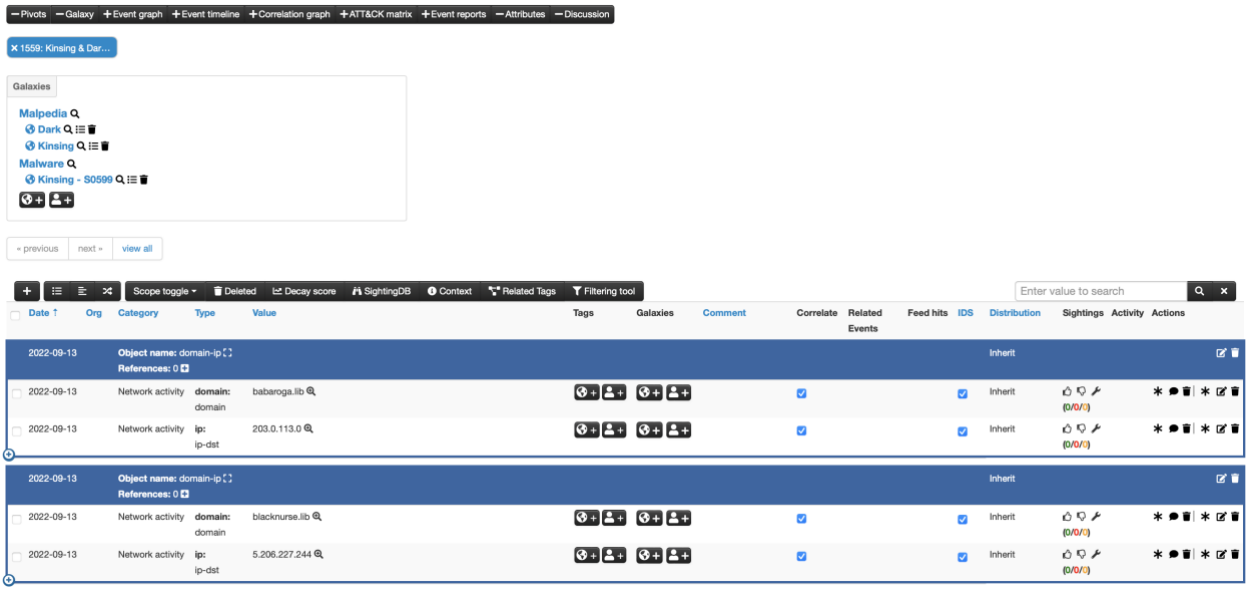

Рисунок 3.7 – Додаткова інформація про подію з ID 1559

Граф взаємозв’язків для події з ID 1559 приведений на рисунку 3.8.

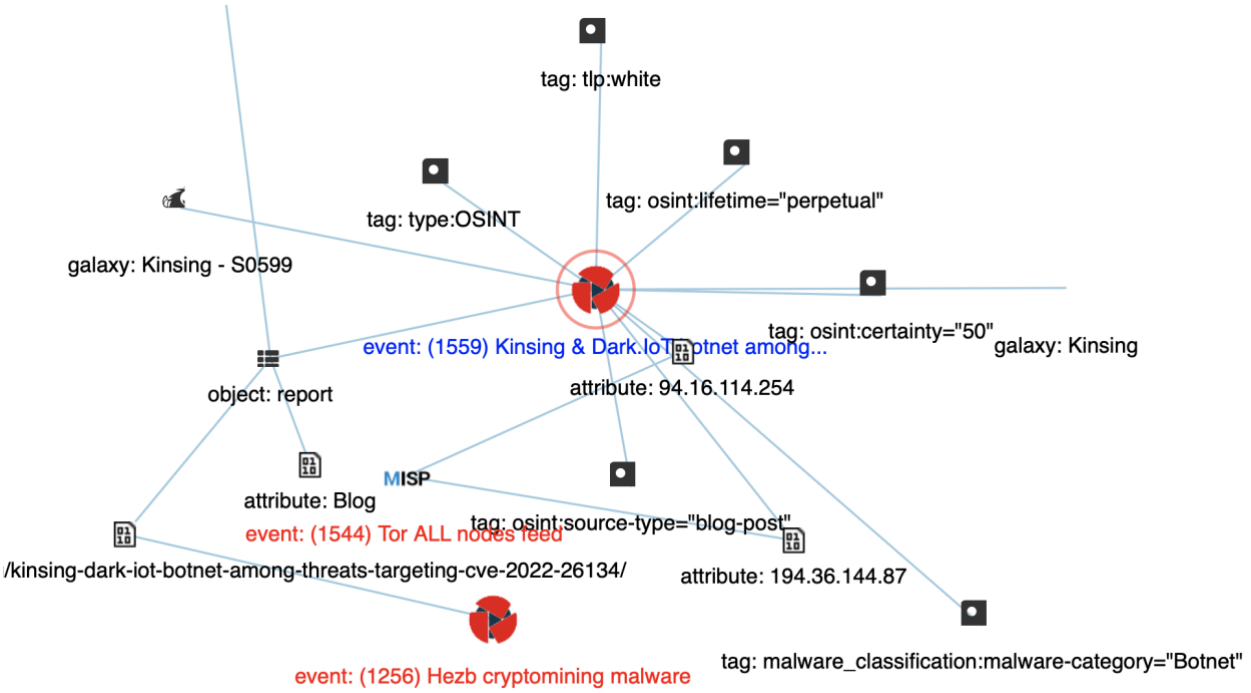

Рисунок 3.8 – Граф взаємозв’язків для події з ID 1559

Приведений кореляційний граф показує зв’язки між джерелами інформації про подію та інші атрибути та індикатори компроментації (див. рис.3.8).

3.3 Створення події на основі звіту

Процес введення події можна розділити на 3 етапи: створення самої події, заповнення її атрибутами і анотаціями та остаточна публікація (рисунок 3.9).

Алгоритм створення події на базі платформі MISP складається з наступних кроків:

Крок 1. Отримання артефактів і визначення типу артефакту.

Крок 2. Створення події.

Крок 3. Додавання початкового шаблону до події.

Крок 4: Додавання атрибуту та анотації.

Крок 5. Додавання групи.

Крок 6. Завершення події та її публікація.

Розглянемо кроки даного алгоритму.

Під час цього першого кроку створюється основна подія без будь-яких фактичних атрибутів, але зберігається загальна інформація, така як опис, час і рівень ризику інциденту. Щоб розпочати створення події, натискаємо кнопку Нова подія ліворуч і заповнюємо форму, яка відкрилася. Необхідно заповнити такі поля [24].

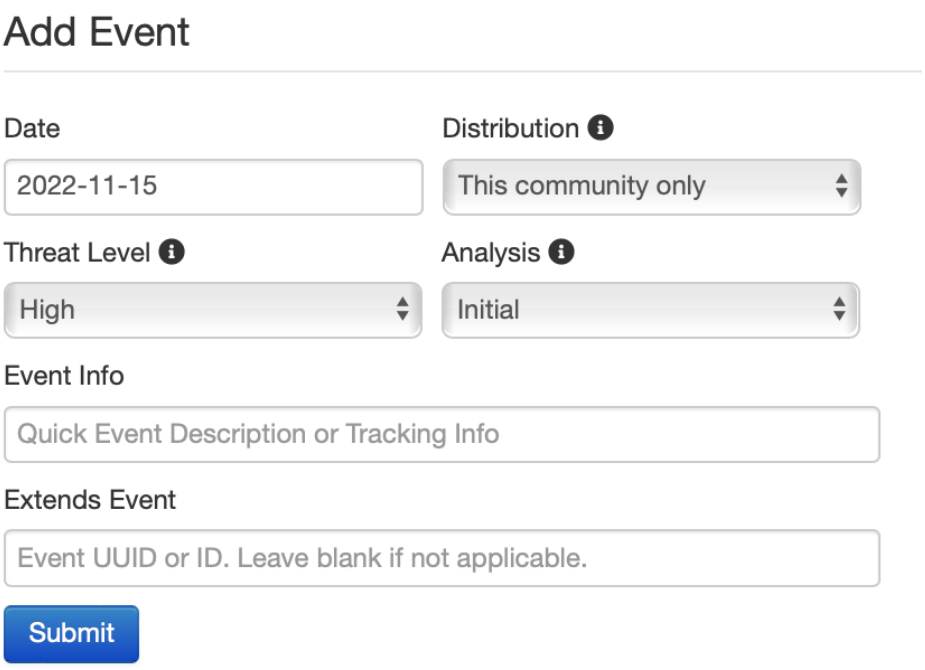

Рисунок 3.9 – Інтерфейс створення події

Date: дата, коли стався інцидент. Просто натисніть це поле, і з’явиться вікно вибору дати, де ви зможете вибрати потрібну дату.

Distribution: це налаштування визначає, хто зможе бачити цю подію після її публікації та, зрештою, коли її буде видалено. Крім можливості встановити, яким користувачам на цьому сервері дозволено переглядати подію, це також визначає, чи буде подія синхронізована з іншими серверами чи ні. Розподіл успадковується за атрибутами: виграє найбільш обмежувальне налаштування. Доступні такі варіанти:

Your organization only: це налаштування дозволить лише членам вашої організації бачити це. Його може перетягнути в інший екземпляр один із членів вашої організації, де лише ваша організація зможе його бачити. Події з цим параметром не будуть синхронізовані.

This Community-only: користувачі, які є частиною вашої спільноти MISP, зможуть побачити подію. Це включає вашу власну організацію, організації на цьому сервері MISP та організації, на яких працюють сервери MISP, які синхронізуються з цим сервером. Будь-які інші організації, підключені до таких пов’язаних серверів, не зможуть переглядати подію.

Connected communities: користувачі, які є частиною вашої спільноти MISP, зможуть побачити подію. Сюди входять усі організації на цьому сервері MISP, усі організації на серверах MISP, які синхронізуються з цим сервером, і хостингові організації серверів, які підключаються до вищезазначених серверів.

All communities: подія буде доступна для всіх спільнот MISP, що дозволить вільно передавати подію з одного сервера на інший.

Sharing group: це надасть доступ до події визначеній групі спільного доступу. Це стосується лише організацій, визначених у групі спільного доступу. Розповсюдження може бути локальним і міжінстанційним залежно від визначення групи спільного доступу.

Threat Level: у цьому полі вказується рівень ризику події. Інциденти можна класифікувати за трьома різними категоріями загрози (низька, середня, висока). Це поле також можна залишити невизначеним. Є три варіанти:

– Low: загальне масове шкідливе програмне забезпечення.

– Medium: Advanced Persistent Threats (APT).

– High: складні APT і 0-денні атаки.

Analysis: вказує на поточний етап аналізу події з такими можливими параметрами:

– Initial: аналіз тільки починається.

– Ongoing: аналіз триває.

– Completed: аналіз завершено.

Event Description: інформаційне поле, де зловмисному програмному забезпеченню/інциденту можна дати короткий опис, починаючи з внутрішнього посилання. Це поле має бути максимально коротким і лаконічним, більш детальний опис відбувається через атрибути на наступному етапі створення події. Майте на увазі, що система автоматично замінить виявлені текстові рядки, які відповідають запису регулярного виразу, встановленому адміністратором(ами) вашого сервера.

GFI Sandbox: за допомогою цього інструменту можна завантажити експортований файл .zip із GFI Sandbox. Вони будуть розібрані MISP, і список атрибутів і вкладень буде автоматично згенеровано з файлу .zip. Хоча це виконує більшу частину роботи, яку необхідно виконати на другому етапі створення події, важливо вручну переглянути всі дані, які вводяться

Для прикладу ми використаємо звіт, знайдений на Bleeping Computer, який вважається OSINT (рисунок 3.10) [25].

Рисунок 3.10 – Звіт про програму вимагач

Додавання події. Перш за все, нам потрібно створити нову подію. Для цього ми клацаємо опцію "Add Event" у списку подій. Тоді ми отримуємо форму додавання події.

Заповнюємо форму даними зі звіту, які у нас уже є:

Дата: тут ми поставимо дату звіту, тобто 2022-11-13 (рисунок 3.11).

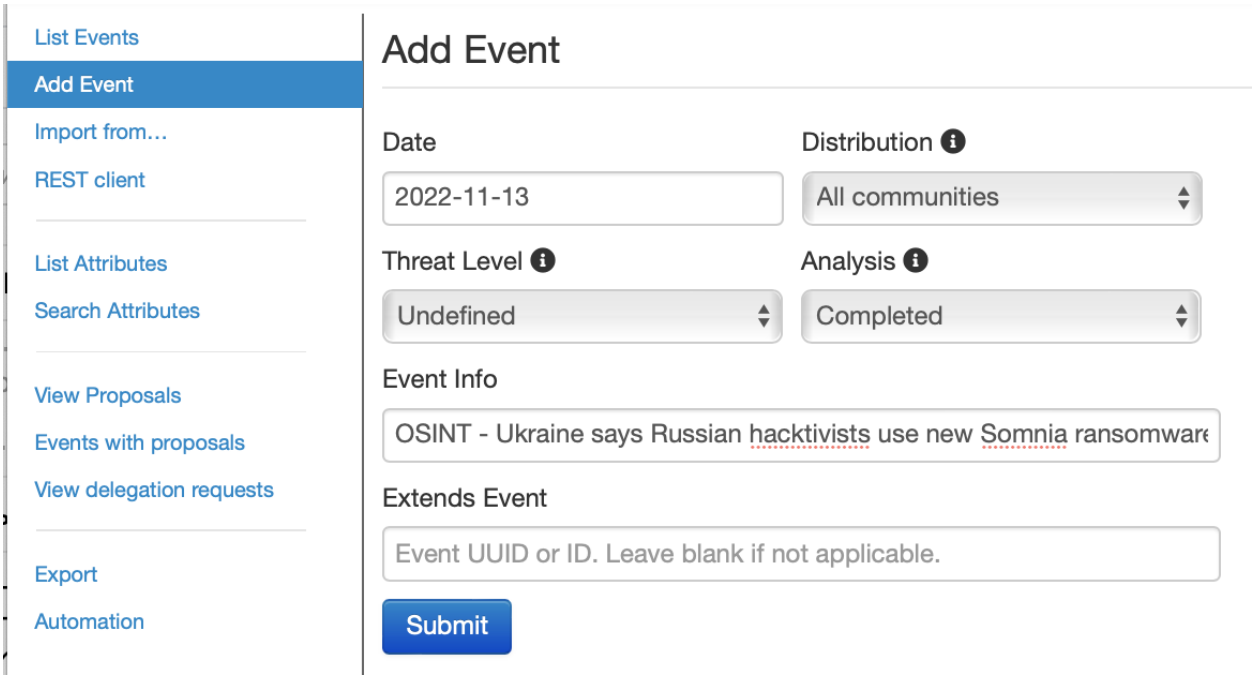

Рисунок 3.11 – Заповнена форма про нову подію

Натискаємо синю кнопку «Submit», і нова подія створена (рисунок 3.12).

Розповсюдження: Залежно від події ми можемо захотіти, щоб вона була більш-менш поширена в екземплярах MISP. Для цього, оскільки це

публічний звіт, немає причин обмежувати розповсюдження 'Усіми спільнотами'.

Рівень загрози: пояснюється сам собою. Оскільки програмне забезпечення-вимагач у звіті не використовує величезний експлойт, ми можемо використовувати низький або невизначений, оскільки ми насправді не знаємо.

Аналіз: Укажіть поточний етап аналізу. Оскільки звіт опублікований, можна вважати, що аналіз завершено.

Інформація про подію: інформація про подію насправді є назвою або заголовком події, тому здається законним розмістити тут також назву звіту. Оскільки це публічна інформація, ми також додаємо до неї префікс «OSINT».

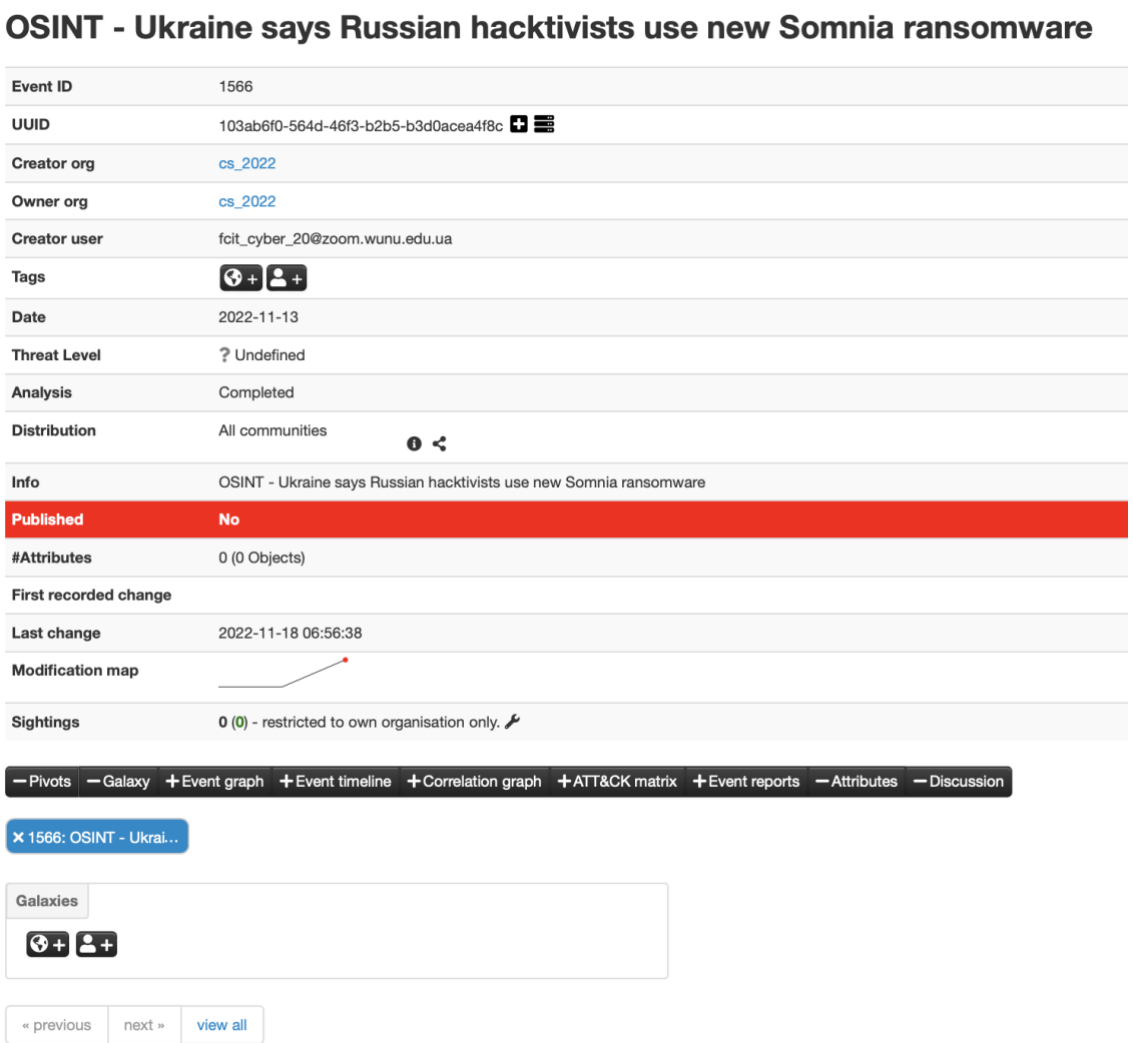

Рисунок 3.12 – Приклад створення нової події

Додавання атрибутів. Тепер треба заповнити дані про подію. Але перш ніж додавати IoC, необхідно додати глобальну інформацію про сам звіт: посилання на звіт і коротке пояснення або вступ. Для цього потрібно натиснути опцію «Додати атрибут» у бічному меню (рисунок 3.13).

Спочатку додаємо посилання на звіт. Оскільки це було написано іншим дослідником, це буде розглядатися як «Зовнішній аналіз», ми вибираємо цю категорію.

Стосовно типу, щодо типу даних, які ми додаємо, очевидно, що ми виберемо тип «посилання».

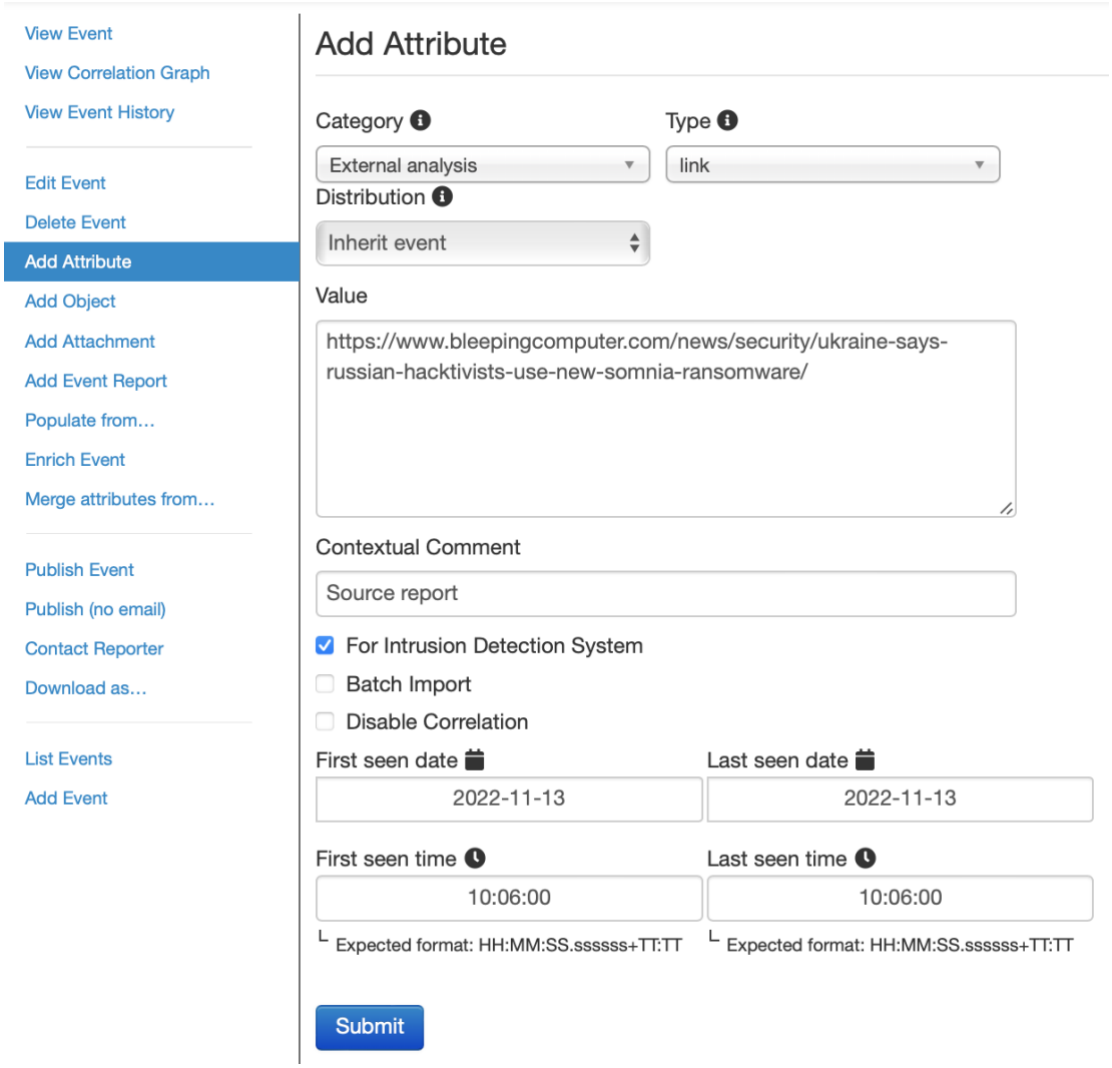

Рисунок 3.13 – Додавання атрибутів події

Перевіряємо чи правильно заповнені всі поля і тоді натиснемо кнопку «Надіслати» (рисунок 3.14).

Поле розподілу може бути дещо складним. Можна вибрати один із варіантів, які вже були доступні на рівні події, або «Успадкувати подію». Якщо вибрати останнє, буде надано спільний доступ так само, як і подія, до якої він включений (тут до «Усі спільноти»). З іншого боку, якщо вручну виберемо розподіл для атрибута, буде застосовано найбільше обмеження між розподілом подій і розподілом атрибутів. Отже, якщо розподіли подій і атрибутів однакові, змін не буде (подібно до «Наслідування події»).

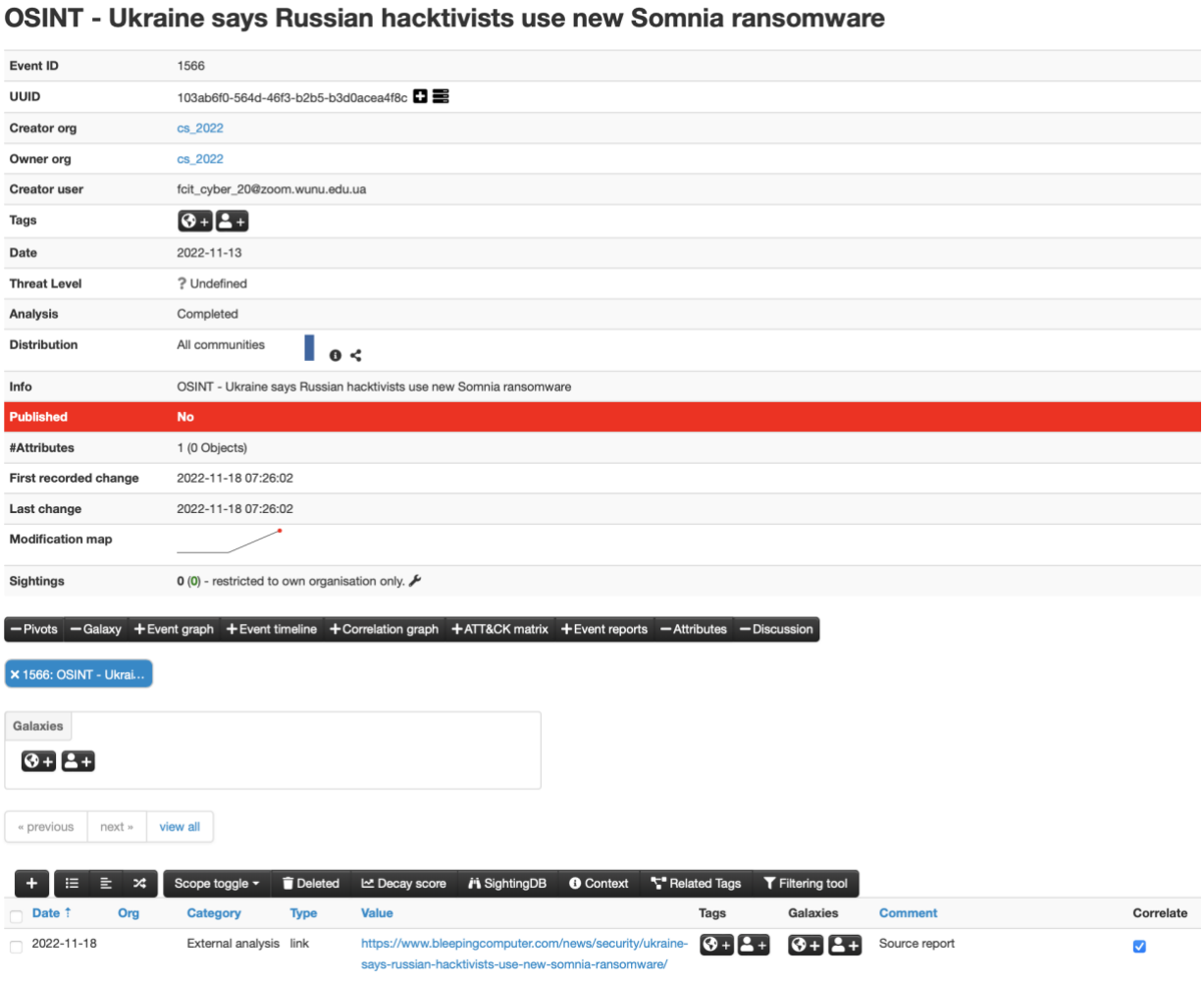

Рисунок 3.14 –Атрибути події

Наприклад, якщо подія розповсюджується як «усі спільноти», а атрибут обмежено «Лише ця спільнота», подію справді буде поширено для всіх спільнот, але без цього конкретного атрибута, який обмежуватиметься

лише цією спільнотою. Те ж саме працює навпаки, якщо атрибут можна розповсюдити для «всіх спільнот», тоді як пов'язана подія обмежена цією спільнотою, атрибут залежить від події, він буде наданий лише цій спільноті, ґрунтуючись на його розподілі подія (рисунок 3.15).

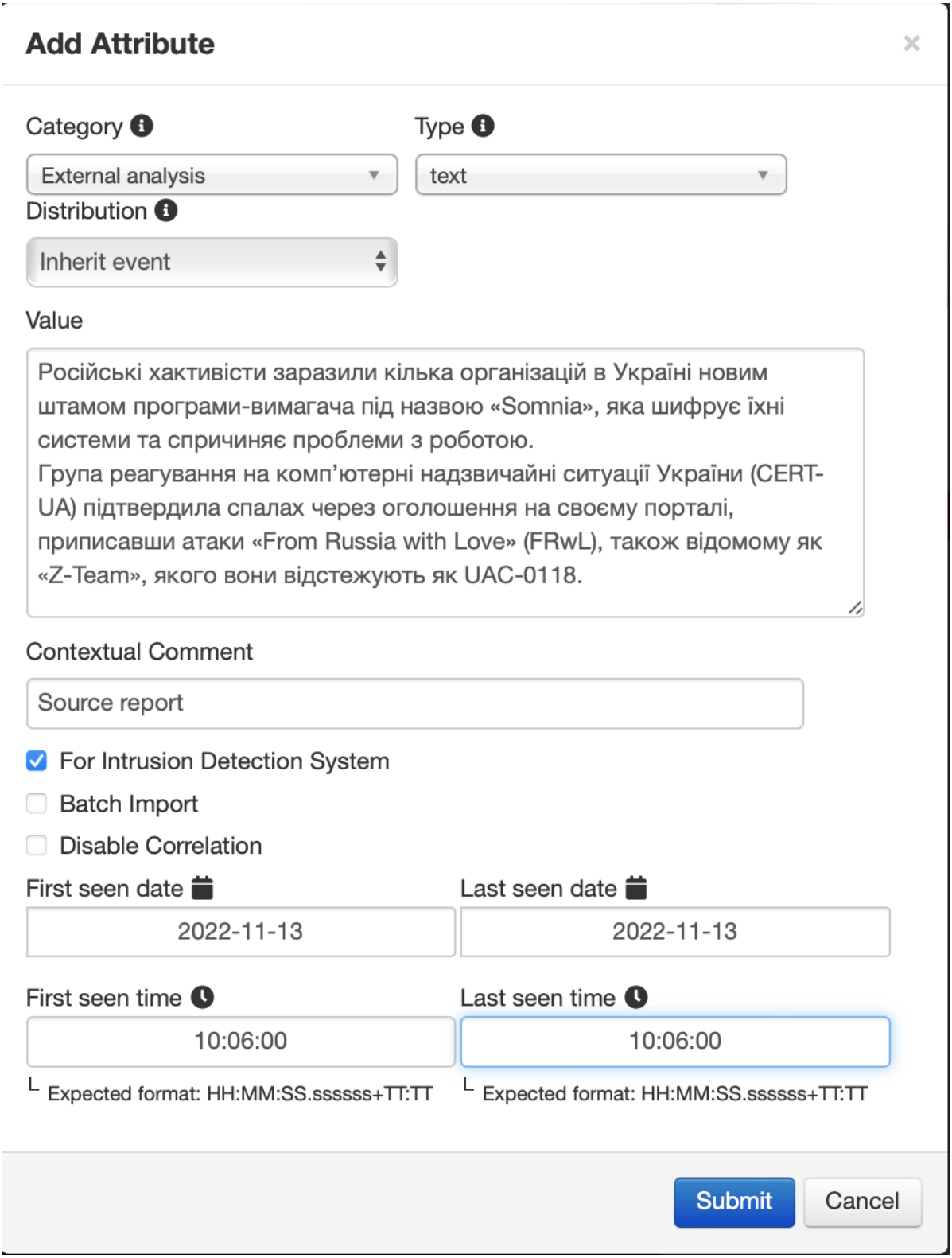

Рисунок 3.15 – Додаткова інформація про подію

Значення – це просто дані, які ми хочемо додати, тут це посилання на звіт.

Контекстний коментар – це поле, яке не використовуватиметься для кореляції, і в основному призначене для додавання деякої додаткової інформації про атрибут. Може бути портом для IP або іншою ознакою.

Тут немає окремої інформації, яку можна додати, окрім, можливо, що це джерело звіту, тому розмістимо цю інформацію «для системи виявлення вторгнень». Якщо встановлено прапор IDS, атрибут використовуватиметься як підпис IDS під час експорту даних NIDS. У цьому випадку у нас немає підстав для перевірки.

Пакетний імпорт є корисною опцією, коли потрібно додати кілька IoC однієї категорії/типу, що дозволяє додавати їх одразу, розділяючи розривом рядки між рядками в полі значення.

Тепер можна зробити аналогічну процедуру, щоб додати вступ до звіту (тобто перший абзац звіту). Потім надсилаємо дані, натиснувши на синю кнопку «Submit» (див. рис.3.15).

Змінимо тип тексту. Але цього разу ми отримаємо доступ до форми додавання атрибутів, натиснувши маленький символ + поруч із таблицею атрибутів. У спливаючому вікні з’явиться та сама форма, що й раніше. Знову заповнюємо її необхідними даними. Результат додавання інформації приведений на рисунку 3.16.

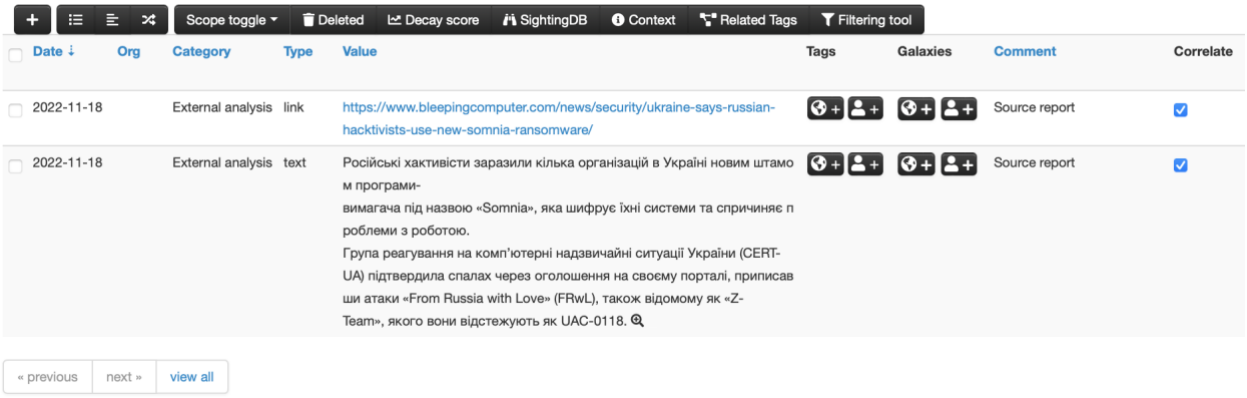

Рисунок 3.16 – Приклад додавання нової інформації про подію

Теплова карта показує активність користувачів за кожен день протягом цього місяця та 4 місяців, що передували йому (рисунок 3.16).

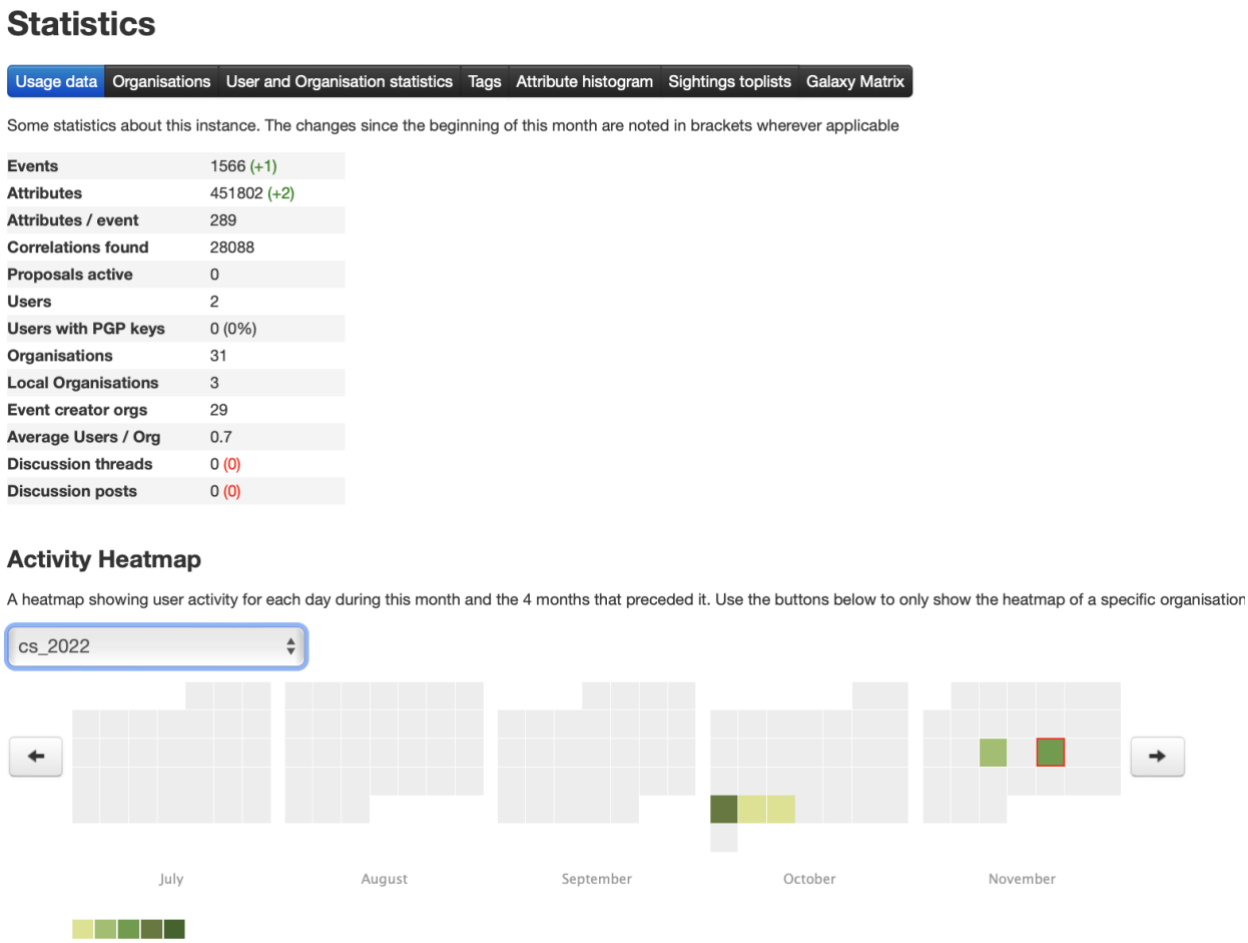

Рисунок 3.16 – Теплова карта активності користувачів

Використовуючи кнопки можна вибрати теплову карту лише певної організації, в даному прикладі показано активність організації cs_2022 (див. рис.3.16).

На даний час це вся інформація, яку ми можемо отримати зі звіту приведеного в [25]. Якщо провести детальніший пошук то ще можна знайти іншу інформація, наприклад, назва файлу, записки про викуп та інше.

Розроблений алгоритм створення події MISP на основі зібраних артефактів OSINT дозволяє спростити процес додавання та обміну про події кібербезпеки.

ВИСНОВКИ

В кваліфікаційній роботі розв’язано актуальну задачу підвищення ефективності обміну інформацією про кіберзагрози. При цьому отримано наступні результати.

1. Проведено аналіз платформ розвідки кіберзагроз з відкритим кодом. Розкрито їх функціональні можливості, переваги та недоліки. Обґрунтовано вибір платформи MISP.

2. Досліджено типи розвідки кіберзагроз, серед який виділено наступні: тактична розвідка; оперативна розвідка; стратегічна розвідка.

3. Розроблено загальну структуру та алгоритм роботи системи виявлення загроз, який складається з шести кроків та реалізований на платформі MISP.

4. Показано можливість виявлення загроз з використанням мови опису правил Yara. Розроблено правило ідентифікації pdf файлів на мові Yara.

6. Створено подію про загрозу на основі звіту з відкритих джерел на базі платформи MISP.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. MISP features and functionalities. [Електронний ресурс]. – Режим доступу: https://www.misp-project.org/

2. OpenCTI-Platform. [Електронний ресурс]. – Режим доступу: https://github.com/OpenCTI-Platform/opencti

3. Harpoon. [Електронний ресурс]. – Режим доступу: https://github.com/Te-k/harpoon#readme

4. Introducing the Yeti. [Електронний ресурс]. – Режим доступу: https://yeti-platform.github.io/introducing-yeti

5. GOSINT - Open Source Threat Intelligence Gathering and Processing Framework. [Електронний ресурс]. – Режим доступу: https://github.com/ciscocsirt/GOSINT

6. CIF v3. [Електронний ресурс]. – Режим доступу: https://github.com/csirtgadgets/bearded-avenger

7. OpenTAXII [Електронний ресурс]. – Режим доступу: https://github.com/eclecticiq/OpenTAXII

8. OpenTPX - Threat Partner eXchange. [Електронний ресурс]. – Режим доступу: https://github.com/Lookingglass/opentpx

9. Bissell, K.; Fox, J.; LaSalle, R.M.; Cin, P.D. State of Cybersecurity Report 2021. Technical Report. Accenture Security. 2021. [Електронний ресурс]. – Режим доступу: https://www.accenture.com/ acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

10. Ardagna, C.; Corbiaux, S.; Sfakianakis, A.; Douligeris, C. ENISA Threat Landscape 2021; Technical Report; European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2021

11. X Force. IBM X-Force Threat Intelligence Index|IBM. Technical Report. IBM Security. 2020. [Електронний ресурс]. – Режим доступу: https://www.ibm.com/downloads/cas/DEDOLR3W .

12. Shackleford, D. CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey; SANS Institute: Bethesda, MD, USA, 2018.

13. MITRE. CybOX–Cyber Observable Expression|CybOX Project Documentation. [Електронний ресурс]. – Режим доступу: https://cyboxproject.github.io/

14. MITRE. About MAEC|MAEC Project Documentation. [Електронний ресурс]. – Режим доступу: https://maecproject.github.io/about-maec/

15. ENISA Threat Landscape 2022. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

16. Virustotal. YARA – The Pattern Matching Swiss Knife for Malware Researchers. [Електронний ресурс]. – Режим доступу: https://virustotal.github.io/yara/

17. Welcome to YARA's documentation! [Електронний ресурс]. – Режим доступу: https://yara.readthedocs.io/en/stable/index.html

18. Awesome YARA. [Електронний ресурс]. – Режим доступу: https://github.com/InQuest/awesome-yara#rules

19. OASIS Cyber Threat Intelligence (CTI) TC. [Електронний ресурс]. – Режим доступу: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

20. Introduction to TAXII. [Електронний ресурс]. – Режим доступу: https://oasis-open.github.io/cti-documentation/taxii/intro

21. Ullah, F.; Babar, M.A. Architectural Tactics for Big Data Cybersecurity Analytics Systems: A Review. J. Syst. Softw. 2019, 151, 81–118.

22. MISP Threat Sharing [Електронний ресурс]. – Режим доступу: https://vm.misp-project.org//latest/

23. Existing MISP modules. [Електронний ресурс]. – Режим доступу: https://misp.github.io/misp-modules/

24. MISP Communities and MISP Feeds. [Електронний ресурс]. – Режим доступу: https://www.misp-project.org/communities/

25. Терещенко О.С., Яцків В.В. Сучасні платформи розвідки кіберзагроз з відкритим кодом. Матеріали проблемно-наукової міжгалузевої конференції«Автоматизація та комп’ютерно-інтегровані технології» (АКІТ - 2022), Тернопіль, 2022. – С. 100-103.

26. Яцків В.В., Терещенко О.С. Розвідка кіберзагроз з використанням мови опису правил YARA. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ - 2022), Тернопіль, 2022. – С. 40-42.

27. Ukraine says Russian hacktivists use new Somnia ransomware. [Електронний ресурс]. – Режим доступу: https://www.bleepingcomputer.com/news/security/ukraine-says-russian-hacktivists-use-new-somnia-ransomware/

ДОДАТОК А

Копії публікацій

ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
НАДВІРНЯНСЬКИЙ КОЛЕДЖ НТУ
ГАЛИЦЬКИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

Проблемно-наукова міжгалузева конференція

АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

(АКІТ – 2022)

21—23 лютого 2022 року

Тернопіль

БЕЗПЕКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 004.056.5

Терещенко О.С.[1], Яцків В.В.[1]

[1]Західноукраїнський національний університет

СУЧАСНІ ПЛАТФОРМИ РОЗВІДКИ КІБЕРЗАГРОЗ З ВІДКРИТИМ КОДОМ

Вступ. Державний сектор та критична інфраструктура України є основною мішенню для кібератак з боку кібертерористів, груп «хактивістів» та інших злочинців. Для зменшення ризиків та ефективного використання обмежених ресурсів, для галузі важливо розуміти загрози, з якими вона стикається. Обмін даними про кіберзагрози є одним із засобів досягнення цієї мети шляхом використання загальногалузевих знань для боротьби з постійними взаємними загрозами. За даними Statista світовий ринок аналізу кіберзагроз зростає швидкими темпами і досягне приблизно 982 мільйона доларів до 2023 року, при тому, що за різними оцінками в 2020 році становив до 392 мільйона доларів.

Мета: дослідження сучасних платформ розвідки кіберзагроз з відкритим кодом**.**

1. Платформи розвідки кіберзагроз з відкритим кодом

Розвідка кіберзагроз (CTI, Cyber Threat Intelligence) – це концепція кібербезпеки, яка передбачає збір, обробку та аналіз даних про ризики безпеці, які загрожують активам організації.

Основна мета розвідки загроз – розпізнати мотиви, поведінку та цілі зловмисника, щоб допомогти фахівцям з безпеки запровадити проактивні заходи безпеки для ефективного запобігання витоку даних.

Розвідка загроз дає змогу виявляти, та боротися з атаками, надаючи відомі сигнатури зловмисного програмного забезпечення, типи даних, на які групи програм-вимагачів націлюються, і ознаки пошкодження пристрою/мережі, на які слід звернути увагу. Захистити організацію від витоку даних і програм-вимагачів неможливо без розуміння вразливостей безпеки, індикаторів загроз і креативних методів злому. Отримавши інформацію з цих даних, розробники або спеціалісти з безпеки зможуть створити надійну парадигму безпеки, точно визначити пріоритети вразливостей, провести аналіз першопричини та розробити інші процеси безпеки високого рівня.

Розглянемо найбільш поширені платформи розвідки кіберзагроз з відкритим кодом.

1. MISP. Malware Information Sharing Platform (MISP), платформа для аналізу та обміну інформацією про загрози з відкритим кодом – це безкоштовна платформа для обміну індикаторами компрометації (Indicator of Compromise, IoC) і інформацією про вразливості між підприємствами. Організації з усього світу використовують платформу для створення надійних спільнот, які обмінюються даними, щоб зіставити їх і краще зрозуміти ризики, націлені на певні галузі чи регіони. MISP пропонує інтерфейс користувача, який дозволяє створювати, шукати та ділитися подіями з іншими користувачами чи групами MISP. Таким чином, замість того, щоб надавати IoC через електронну пошту та у вигляді PDF-

файлів, платформа дозволяє компаніям-учасникам ефективніше керувати обміном і централізацією інформації. Крім того, вся інформація, що зберігаються в базі даних MISP, доступна через API, що дозволяє експортувати дані в форми, включаючи XML, JSON, OpenIOC, STIX та інші. MISP має автоматичний кореляційний механізм, який може знаходити зв'язки між характеристиками, об'єктами та ознаками механізму кореляції шкідливих програм. Крім того, MISP структуровано зберігає дані, пропонує суттєву підтримку індикаторів кібербезпеки та полегшує обмін даним про загрози як для людей, так і для машин [1].

2. OpenCTI. Проект OpenCTI, також відомий як Open Cyber Threat Intelligence – це платформа, розроблена для полегшення обробки інформації та обміну цими знаннями для цілей розвідки про кіберзагрози. Це результат співпраці між (Групою реагування на комп'ютерні надзвичайні ситуації Європейського Союзу) (CERT-EU) і Національним агентством кібербезпеки Франції (ANSSI). Для полегшення здатності учасників структурувати, зберігати, організовувати, візуалізувати та ділитися своєю інформацією, платформа тепер повністю опублікована у відкритому коді та стала доступною для всієї спільноти розвідки про кіберзагрози [2]. До важливих елементі включених в дану платформу аналізу загроз необхідно віднести: уніфікована модель даних, яка базується на стандартах STIX2; автоматизовані робочі процеси; інтеграція з екосистемою інформаційних технологій; інтелектуальна візуалізація даних; інструменти для аналізу подій. OpenCTI, на додаток до ручного введення даних про загрози, підтримує з'єднання для автоматичного отримання даних про загрози та інформації з відомих джерел розвідки про загрози, включаючи MITER ATT&CK, MISP і VirusTotal.

3. Harpoon – це програма командного рядка, яка містить колекцію плагінів Python для автоматизації розвідувальних дій із відкритим кодом. Кожен плагін пропонує команду, яку аналітики можуть використовувати для доступу до API сайтів, таких як MISP, VirusTotal, Shodan, Passive Total, Hybrid Analysis, AlienVault OTX, Censys, RobTex, ThreatGrid, GreyNoise, TotalHash, MalShare та Have I Been Pwned. Аналітики можуть отримати інформацію про IP-адресу або домен з усіх цих платформ одночасно за допомогою команд вищого рівня. Інші сценарії також можуть здійснювати пошук у сховищах GitHub, соціальних мережах і платформах веб-кешу [3].

4. Yeti – платформа, яка була створена у відповідь на необхідність аналітиків безпеки консолідувати різні канали даних про загрози. Yeti дозволяє аналітикам об'єднувати показники компрометації і інформацію про тактику, техніку та процедури, які використовують зловмисники, в єдине уніфіковане сховищ. Yeti пропонує інтерфейс користувача на основі Bootstrap і машинний інтерфейс веб-API. Платформа YETI включає в себе добре організоване сховище, яке добре адаптується та розширюється, а також пропонує допомогу в автоматизації [4].

5. GOSINT – це платформа з відкритим вихідним кодом, створена Cisco CSIRT, яка зосереджена на зборі та обробці інформації. Вона збирає, обробляє та експортує IoC, таким чином контролюючи процес включення даних платформи та

збагачуючи його високоякісною інформацією. GOSINT агрегує та перевіряє показники для використання іншими інструментами, такими як MISP і CRITs3, або безпосередньо в системах керування журналами та SIEM, одночасно підтримуючи STIX, TAXII, VERIS, Incident Sharing, які використовуються в системах обміну інформацією про загрози [5].

GOSINT додатково підтримує формат обміну описом об'єктів інциденту (IODEF) і формат обміну повідомленнями про виявлення вторгнень (IDMEF), що дозволяє фахівцям-криміналістам збирати структуровані та неструктуровані дані про події, що стосуються третіх осіб. Інтерфейс GOSINT розроблено на JavaScript. Основні недоліки платформи GOSINT стосуються здебільшого управління пакетами. Зокрема, менеджери пакетів GOSINT надають застарілі версії програмного забезпечення; отже, їх необхідно перевірити, щоб перевірити сумісність. GOSINT має структурований репозиторій, систему керування даними та можливості експорту даних.

6. CIF – це система керування даними про загрози та одна з платформ ENISA для обміну про загрози. CIF дозволяє користувачам аналізувати, нормалізувати, зберігати, оброблювати, запитувати, ділитися та створювати дані CTI, а також збирати інформацію про відомі шкідливі загрози з кількох джерел для ідентифікації (реагування на інциденти), виявлення та пом'якшення. Вона також дозволяє автоматизовано формувати найпоширеніші типи інформації про загрози, такі як IP-адреси та URL-адреси, пов'язані зі зловмисною поведінкою. Структура CIF збирає різноманітні дані спостережень із багатьох джерел. Коли користувач запитує дані CTI, система надає йому серію відсортованих у хронологічному порядку повідомлень; потім користувачі можуть виносити судження, оцінюючи надані результати у спосіб, подібний до аналізу загроз електронною поштою. Сервер CIF складається з багатьох модулів, таких як CIF-smrt, CIF-worker, CIF-starman, CIF-router і ElasticSearch [6].

Модуль CIF-smrt має дві основні функції: отримувати файли через HTTP(s) і аналізувати файли за допомогою вбудованих парсерів для регулярних виразів, файлів JSON, XML, RSS, HTML і простого тексту. Модуль CIF-worker допомагає CIF витягувати додаткову інформацію із зібраних даних про загрози, модуль CIF-starman забезпечує середовище HTTP API, модуль CIF-router діє як посередник між клієнтом і веб-платформою, а модуль ElasticSearch є даними сховище для зберігання даних, що стосуються вторгнень. CIF має структурований репозиторій і систему адміністрування. Вона поєднує інформацію про шкідливу загрозу для ідентифікації, виявлення і пом'якшення.

7. OpenTAXII – це вдосконалена версія платформи TAXII. Дизайн системи відповідає стандартам TAXII. Вона надає набір стандартів загроз і розширювані рівні стійкості та автентифікації через спеціалізований API. Крім того, вона пропонує необхідні послуги та можливість обміну повідомленнями. Інші функції OpenTAXII включають налаштування API, автентифікацію та різноманітне ведення журналів [7]. OpenTAXII має добре організоване сховище та структуру управління, а також може імітувати раніше визначені ситуації та ризики. Вона адаптована і розширювана, оскільки пропонує машинозчитувані дані про загрози, розширення джерела інформації та розширення API.

8. OpenTPX – це платформа сховища даних на основі JSON, яка дозволяє реєструвати та ділитися інформацією про інциденти. OpenTPX є внеском LookingGlass Cyber Solutions у спільноту відкритих кодів. Вона підтримує різноманітні, добре відомі протоколи, такі як HTTP, SMTP, FTP тощо, і була розроблена, щоб сприяти розробці високомасштабованих систем розвідки загроз, аналізу та безпеки мережі, які швидко передають великі обсяги даних. OpenTPX пропонує способи передачі інформації про топологію мережі, сегментацію мережі, метадані загроз, розвідку про загрози та заходи щодо їх пом'якшення [8].

OpenTPX має добре організований репозиторій, який є універсальним і розширюваним, а також пропонує допомогу в автоматизації. Це також покращує можливості обробки даних, дозволяючи додавати доповнення до спостережуваних описів загроз. Вона пропонує повну систему оцінки загроз, яка дає змогу аналітикам безпеки, дослідникам загроз, операторам мережевої безпеки та службам реагування на інциденти легко приймати відповідні рішення щодо пом'якшення загроз.

Висновки. Тема розвідки про кіберзагрози ще молода і активно розвивається. Аналіз платформ обміну інформацією про загрози показав, що такі платформи мають схожі функції, але й ряд відмінностей. Всі платформи підтримують чотири фази процесу обміну інформацією про загрози, забезпечуючи при цьому обмін інформацією та спільне використання інформації. Для поширення та інтеграції даних більшість платформ використовують REST API і підтримують стандарти STIX і TAXII. Загалом, гнучкість і сумісність платформ значно відрізняються, проте майже всі платформи можна розширювати та налаштувати під конкретні задачі. Впровадження систем розвідки загроз допомагає організації виявляти та зменшувати різноманітні бізнес-ризики, перетворюючи невідомі загрози на відомі, а також допомагає впроваджувати різноманітні передові стратегії захисту.

Перелік використаних джерел.

1. MISP features and functionalities. [Електронний ресурс]. - Режим доступу: https://www.misp-project.org/

2. OpenCTI-Platform. [Електронний ресурс]. - Режим доступу: https://github.com/OpenCTI-Platform/opencti

3. Harpoon. [Електронний ресурс]. - Режим доступу: https://github.com/Te-k/harpoon#readme

4. Introducing the Yeti. [Електронний ресурс]. - Режим доступу: https://yeti-platform.github.io/introducing-yeti

5. GOSINT - Open Source Threat Intelligence Gathering and Processing Framework. [Електронний ресурс]. - Режим доступу: https://github.com/ciscocsirt/GOSINT

6. CIF v3. [Електронний ресурс]. - Режим доступу: https://github.com/csirtgadgets/bearded-avenger

7. OpenTAXII [Електронний ресурс]. - Режим доступу: https://github.com/eclecticiq/OpenTAXII

OpenTPX - Threat Partner eXchange. [Електронний ресурс]. - Режим доступу: https://github.com/Lookingglass/opentpx


КІБЕРБЕЗПЕКА ТА
КОМП'ЮТЕРНО-ІНТЕГРОВАНІ
ТЕХНОЛОГІЇ
КБКІТ-2022
науково-практична конференція
молодих вчених
аспірантів та студентів
м.Тернопіль

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2022)

науково-практична конференція
молодих вчених, аспірантів та студентів

29–31 серпня 2022
Тернопіль

ЗМІСТ

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

БЕЗПЕКА ТА ІНТЕРНЕТ РЕЧЕЙ

УДК 004.056.5

Яцків В.В.[1], Терещенко О.С.[1]

[1]Західноукраїнський національний університет

РОЗВІДКА КІБЕРЗАГРОЗ З ВИКОРИСТАННЯМ МОВИ ОПИСУ ПРАВИЛ YARA

Вступ. Провідні постачальники засобів кібербезпеки повідомляють про збільшення середньої кількості атак на компанії приблизно на 31%. Згідно щорічного звіту ENISA Threat Landscape про стан ландшафту загроз кібербезпеці, новими або найчастішими джерелами інцидентів, з якими стикається організація, є: програми-вимагачі, шкідливе програмне забезпечення, загрози соціальної інженерії, загрози щодо даних, загрози доступності: відмова в обслуговуванні, дезінформація, атаки на ланцюги поставок [1]. Розвідка кіберзагроз (Cyber Threat Intelligence, CTI) – нова сфера інформаційної безпеки, у якій багато організацій інвестують у розробку належних інструментів і послуг, а також у інтеграцію інформації, пов'язаної з розвідувальними даними. Розвідка кіберзагроз дозволить краще зрозуміти мотивацію та тактику зловмисника. Крім того, CTI є важливою для запобігання атак нульового дня.

Мета: дослідження розвідки кіберзагроз з використанням мови опису правил Yara.

1. Розвідка кіберзагроз

Розвідка кіберзагроз є важливою стратегією захисту організацій від складних організованих кібератак. CTI складається з інформації пов'язаної з кіберзагрозами та їх суб'єктами, а також містить різні джерела, які допомагають ідентифікувати та пом'якшувати шкідливі дії та потенційні атаки, що відбуваються в кіберпросторі. CTI об'єднує джерела кіберрозвідки в інформацію, яка допомагає підтримувати операції безпеки. Серед найбільш поширених джерел інформації про кіберзагрози можна виділити наступні: інтелект людини; розвідка з відкритих джерел; розвідка з використанням соціальних мереж; технічна розвідка; файли журналів пристрою; аналіз Інтернет-трафіку; дані з темної та глибинної мережі; дані, отримані криміналістичним шляхом. Дані отримані в результаті розвідки кіберзагроз використовуються: при управлінні кіберризиками для розуміння ризиків, з якими стикається організація, і прийняття відповідних засобів контролю для їх пом'якшення; в центрах безпеки (SOC) для надання аналітикам SOC додаткової інформації про суб'єктів загроз, що діють у контрольованому середовищі; при управлінні вразливими місцями для виявлення вразливих місць і визначенні їх пріоритетності відповідно до впливу на бізнес; при розслідуванні інцидентів і реагуванні на них для виявлення першопричини інцидентів безпеки та більш ефективного реагування; при визначенні відповідності організації вимогам безпеки.

2. Використання правил YARA в розвідці кіберзагроз

Головною ідеєю при початковій оцінці підозрілих файлів є синтаксичні підписи, які вже тривалий час використовуються у боротьбі зі шкідливим програмним забезпеченням. Ці сигнатури передусім дозволяють виявляти та

ідентифікувати сімейства шкідливих програм, що допомагає пришвидшити процедуру аналізу, використовуючи попередні знання щодо цих сімейств. Одним із важливіших і популярних інструментів у цьому контексті є YARA. Це високоефективний механізм зіставлення шаблонів, який супроводжується доступною мовою опису правил. Завдяки своїй ефективності, що YARA стала квазістандартом із широким впровадженням серед практиків і багатьма правилами, які поширюються відкрито або в приватних групах пошуку загроз. При цьому, розробка правил, які добре виявляють і водночас уникають помилкової класифікації, все ще залишається актуальною задачею. Цей процес часто виконується вручну, що вимагає від аналітика знань і досвіду. Серед поширених варіантів використання YARA можна навести наступні: ідентифікація та класифікація шкідливих програми; знаходження нових зразків на основі характерних для сімейства шаблонів; служби реагування на інциденти можуть розгортати правила YARA для ідентифікації зразків і скомпрометованих пристроїв; проактивне впровадження спеціальних правил YARA може посилити захист організації.

Під час аналізу шкідливого програмного забезпечення фахівці створюють правила YARA, які в подальшому захисники будуть використовувати для виявлення цього ШПЗ. При збиранні індикаторів компрометації (IoC) шкідливого програмного забезпечення програмного забезпечення з інших джерел, можна писати правила YARA або знаходити правила YARA з інших джерел і надавати їх захисникам для виявлення ШПЗ. Список джерел правил YARA наведений в [3].

Синтаксис правила YARA. Синтаксис вимагає, щоб кожне правило YARA починалося зі слова rule. Після слова rule потрібно буде додати ім'я або ідентифікатор, який містить будь-які буквено-цифрові символи. Синтаксис YARA також допускає підкреслення в імені/ідентифікаторі, але не дозволяє першому символу бути числом. Зазвичай правила складаються з двох розділів: визначення рядків і умови. Розділ визначення рядків можна опустити, якщо правило не буде перевіряти жодний рядок, але розділ умов завжди потрібний. Розглянемо просте правило Yara, яке завжди має значення true, тобто воно завжди відповідає будь-якому файлу:

```
rule test
{
        condition: true
}
```

Щоб проаналізувати файл за допомогою правила yara, використовується команда: yara <yara-rule> <target-file>, де перший аргумент – файл правила, а другий – файл, який потрібно сканувати.

Метадані. Метадані не впливають на те, що шукатиме правило YARA, натомість вони надають корисну інформацію про саме правило, зокрема: author, date, version, reference, description, hash.

Параметри YARA. Щоб зробити аналіз файлів більш ефективним використовують параметри YARA. Команда для запуску аналізу із параметрами має вигляд:

yara [OPTIONS] <rule-file> <target-file>

Розглянемо основні параметри в правилах YARA: -m –друкує метадані

правил, які були виконані під час аналізу. Метадані можуть надати хеш sha256 зразка, який згодом можна надіслати в інші механізми сканування, наприклад, Virus Total або Hybrid Analysis; -c – виводить кількість збігів у форматі: file path:match result (шлях до файлу: результат відповідності); -s – друкує відповідні рядки у форматі: hexadecimal virtual address:$string identifier:string value.

Розглянемо приклад правила для ідентифікації pdf файлу.

```
rule check_pdf
{
 meta:
  author = "magistr"
  description = "Identification PDF files."
 strings:
  $xpdf = "%PDF"    # %PDF  це стандартний заголовок для файлів
PDF
  $ypdf = "%%EOF"   # %%EOF  це стандартний маркер кінця файлу
PDF
 condition:
  $xpdf at 0 and $ypdf
}
```

Виконання правила запускаємо командою:

$ yara -m check_pdf.yar test555.pdf

Результатом виконання правила буде інформація, яка підтверджує, що виявлено файл pdf.

check_pdf [author="magistr",description="Identification PDF files."] test555.pdf

Однак, покладатися лише на захист на основі правил вже недостатньо. Зловмисники розробили контрзаходи, які вони можуть використовувати, щоб обійти цей метод. Використовуючи різноманітні служби шифрування, пакувальники та поліморфізм, вони можуть легко генерувати ШПЗ, яке є достатньо відмінним, щоб його не ввиявляли існуючі сигнатури. Відповідно, потрібен деякий час, перш ніж буде створено нові правила. Однак, ці недоліки не роблять виявлення на основі сигнатур застарілим механізмом. Фахівці з безпеки діляться новими індикаторами загроз, тому ці типи інструментів залишаться актуальними і дієвими.

Висновок. Розвідка кіберзагроз поєднує численні фактори, включно з мотивацією кіберзлочинців та індикаторами компрометації, щоб допомогти командам безпеки зрозуміти виклики від очікуваної кіберзагрози та підготуватися до них. Надаючи командам безпеки актуальні дані про кіберзагрози, що насуваються, розвідка кіберзагроз заохочує проактивний підхід до кібербезпеки – найефективнішого типу кіберзахисту.

Перелік використаних джерел.

1. ENISA Threat Landscape 2022. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

2. Welcome to YARA's documentation! [Електронний ресурс]. – Режим доступу: https://yara.readthedocs.io/en/stable/index.html

3. Awesome YARA. [Електронний ресурс]. – Режим доступу: https://github.com/InQuest/awesome-yara#rules

ТЕРНОПІЛЬСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
ТЕРНОПІЛЬСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ
ДЕПАРТАМЕНТ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ
вул. Грушевського, 8, м.Тернопіль, 46021, тел./факс (0352) 51-70-10
E-mail: digital@te.gov.ua, Web: digital.te.gov.ua Код згідно ЄДРПОУ 44253982

від_____ № _____ На № _____ від_____

Зав. кафедри кібербезпеки
д.т.н., проф. Василю ЯЦКІВУ

ДОВІДКА ПРО ВИКОРИСТАННЯ

Виконана студентом групи КБзм-21 факультету комп'ютерних інформаційних технологій Західноукраїнського національного університету Терещенком О.С. кваліфікаційна робота на тему „Алгоритми розвідки кіберзагроз на базі платформи з відкритим кодом" відповідає замовленню організації, має практичну значимість і планується до використання.

Директор департаменту **Олександр ШЛАПАК**