МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Західноукраїнський національний університет

Факультет комп’ютерних інформаційних технологій

Кафедра кібербезпеки

МАСТАЛЯРЧУК Євгеній Володимирович

Система розвідки кіберзагроз на основі платформи MISP / Cyber threat intelligence system based on the MISP platform

спеціальність 125 Кібербезпека

освітньо-професійна програма - Кібербезпека

кваліфікаційна робота

Виконав студент групи КБм-21

Є.В. Масталярчук

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Науковий керівник:

д.т.н., професор В.В. Яцків

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кваліфікаційну роботу

допущено до захисту

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ р.

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.В. Яцків

підпис

Тернопіль – 2021

Західноукраїнський національний університет

Факультет комп'ютерних інформаційних технологій

# Кафедра кібербезпеки

Освітній ступінь «магістр»

# спеціальність: 125 "Кібербезпека"

освітньо-професійна програма - Кібербезпека

# ЗАТВЕРДЖУЮ

**Завідувач кафедри**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**В.В. Яцків

“\_\_\_\_” \_\_\_\_\_\_\_\_\_\_20\_\_\_ року

## ЗАВДАННЯ

### **НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ**

**Масталярчуку Євгенію Володимировичу**

(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи: **Система розвідки кіберзагроз на основі платформи MISP / Cyber threat intelligence system based on the MISP platform**

керівник роботи д.т.н., доцент В.В. Яцків

затверджена наказом по університету від “\_\_\_\_”\_\_\_\_\_\_\_\_\_\_20\_\_\_ року №\_\_\_\_\_

2. Строк подання студентом закінченої випускної кваліфікаційної роботи

16 листопада 2021 року.

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

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

* дослідити методологію кіберзагроз;
* вивчити групи і практики обміну розвідувальними даними;
* дослідити моделі аналізу даних по кіберзагрозах;
* розгорнути систему розвідки кіберзагроз;
* інтегрувати платформу MISP у інформаційний простір бази практики;
* автоматизувати роботу у системі;
* розглянути можливість підключення до зовнішніх екземплярів даних.

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень):

Прогнозовані наслідки кібератаки на автоматизовані системи.

Діаграма виникнення інцидентів у сфері високих технологій.

Основні методи забезпечення інформаційної безпеки.

Моделі забезпечення безпеки.

Схема інтелектуального аналізу даних.

представлення принципу обміну інформацією про загрози.

Триетапна стратегія поширення та співпраці.

Принцип роботи MISP.

Знімки екрану платформи.

6. Консультанти розділів роботи

|  |  |  |  |
| --- | --- | --- | --- |
| Розділ | Прізвище, ініціали та посада  консультанта | Підпис, дата | |
| завдання видав | завдання  прийняв |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

7. Дата видачі завдання\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

#### КАЛЕНДАРНИЙ ПЛАН

|  |  |  |  |
| --- | --- | --- | --- |
| №  з/п | Назва етапів кваліфікаційної роботи | Строк виконання  етапів кваліфікаційної роботи | Примітка |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Студент \_\_\_\_\_\_\_\_\_\_\_\_\_ Є.В. Масталярчук**

( підпис ) (прізвище та ініціали)

**Керівник кваліфікаційної роботи \_\_\_\_\_\_\_\_\_ В.В. Яцків**

( підпис ) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Система розвідки кіберзагроз на основі платформи MISP/Cyber threat intelligence system based on the MISP platform» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека» освітньо-професійної програми «Кібербезпека» написана обсягом 80 сторінок і містить 32 ілюстрації та 24 джерела за переліком посилань.

Метою кваліфікаційної роботи є інтеграція платформи розвідки кіберзагроз у інформаційний простір ВСП «РФК НУБіП України».

Методи досліджень. Для розв’язання поставлених задач у даній магістерській роботі використано: порівняння існуючих механізмів індикації ризиків; узагальнення набутою інформації; аналіз вимог до майбутньої системи, шляхом зосередження на основних задачах; експеримент над розгорнутою системою для визначення повноти реалізації поставлених завдань.

Результати дослідження: досягнуто за рахунок повного занотовування інформації про загрози у локальну базу даних та підключення середовища до зовнішніх екземплярів даних. Це в свою чергу дозволило упередити використання вразливостей інформаційної системи організації та надало можливість ознайомлювати здобувачів освіти з основними напрямками розповсюдження загроз у кіберпросторі.

Результати роботи можуть успішно застосовуватися для нагромадження вхідної інформації по інцидентах з подальшим включенням в навчальний процес для унаочнення механізму обміну захищеною інформацією по каналах зв’язку та ознайомлення з базовими принципами захисту від кіберінцидентів.

Ключові слова: БЕЗПЕКА, ПЛАТФОРМА MISP, РОЗВІДКА КІБЕРЗАГРОЗ, ОБМІН ДАНИМИ, РЕЄСТРАЦІЯ ІНЦИДЕНТІВ, ШАБЛОНУВАННЯ ПОДІЙ, РОЗПОДІЛЕНЕ НАВЧАННЯ КІБЕРЗАХИСТУ.

ANNOTATION

Qualifying work on "Cyber threat intelligence system based on the MISP platform" for the degree of "Master" in the specialty 125 "Cybersecurity" educational and professional program "Cybersecurity" is 80 pages long and contains 32 illustrations and 24 sources from the list of links.

The purpose of the qualification work is to integrate the cyber threat intelligence platform into the information space of the SSS «RPC NULES of Ukraine».

Research methods. To solve the tasks in this master's thesis used: comparison of existing mechanisms of risk indication; generalization of acquired information; analysis of requirements for the future system, by focusing on the main tasks; experiment on a deployed system to determine the completeness of the tasks.

Research results: achieved by fully recording information about threats in the local database and connecting the environment to external data instances. This, in turn, prevented the use of vulnerabilities in the organization's information system and provided an opportunity to familiarize students with the main directions of the spread of threats in cyberspace.

The results of the work can be successfully used to accumulate input information on incidents with subsequent inclusion in the educational process to illustrate the mechanism of exchange of protected information through communication channels and acquaintance with the basic principles of protection against cyber incidents.

Keywords: SECURITY, MISP PLATFORM, CYBER THREAT INTELLIGENCE, DATA EXCHANGE, INCIDENT REGISTRATION, EVENT PATTERNING, DISTRIBUTION OF STUDIES.

**ЗМІСТ**

|  |  |  |
| --- | --- | --- |
| ВСТУП | | 8 |
| 1 АНАЛІЗ МЕХАНІЗМІВ РОЗВІДКИ КІБЕРЗАГРОЗ | | 10 |
|  | 1.1 Методологія кіберзагроз | 10 |
|  | 1.2 Вивчення груп і практик обміну розвідувальними даними та інформацією в епоху злочинної діяльності в Інтернеті | 16 |
|  | 1.3 Моделі аналізу даних по кіберзагрозах | 22 |
|  | 1.4 Безпечне розподілене навчання щодо розвідки загроз | 28 |
| Висновок до першого розділу | | 32 |
| 2 РОЗГОРТАННЯ MISP THREAT SHARING ДЛЯ УПЕРЕДЖЕННЯ РОЗПОВСЮДЖЕННЮ ІНЦИДЕНТІВ | | 34 |
|  | 2.1 Використання спільної платформи для обміну інформацією про загрози | 34 |
|  | 2.2 Розгортання системи розвідки кіберзагроз MISP Threat Sharing | 41 |
|  | 2.3 Застосування платформи в межах ВСП «РФК НУБіП України» шляхом нотування виявлених інцидентів | 42 |
|  | 2.4 Автоматизація роботи у системі шляхом шаблонування | 47 |
| Висновок до другого розділу | | 51 |
| 3 РЕЗУЛЬТАТ ЗАСТОСУВАННЯ ПЛАТФОРМИ ОБМІНУ ДАНИМИ MISP THREAT SHARING | | 53 |
|  | 3.1 Результат впровадження системи розвідки кіберзагроз на прикладі ВСП «РФК НУБіП України» | 53 |
|  | 3.2 Підключення та навчання нових користувачів платформи | 57 |
|  | 3.3 Підключення до зовнішніх екземплярів даних | 61 |
| Висновок до третього розділу | | 62 |
| ВИСНОВКИ | | 64 |
| СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ | | 66 |
| ДОДАТКИ | | 69 |

**Перелік умовних позначень**

PwC - PricewaterhouseCoopers

ДПП - державно-приватне партнерство

ENISA - European Union Agency for Network and Information Security

PPP - Public Private Partnerships

KDD - Knowledge Discovery in Databases

NGFW - next generation firewall

NIDS - Network Intrusion Detection System

APT - Advanced Persistent Threats

ВСТУП

Інформаційні технології, які набули особливого розвитку за останні роки, вже глибоко інтегрувались в усі сфери суспільного життя і цілком природно, що розвиток сфери цифрових технологій не залишився поза увагою зловмисників, які застосовують різні методи втручання у роботу автоматизованих цифрових систем. Сучасні масштаби злочинної діяльності у кіберпросторі набувають ознак справжніх війн, а тому дають підстави вважати ці дії кібервійнами злочинних хакерських угруповань. В умовах гібридної агресії та необхідності протистояння сучасним кіберзагрозам, в Україні триває активна розбудова національної системи кібербезпеки.

***Актуальність теми***. Наразі досить проблематично виявити та попередити кіберзагрози, в силу їх надзвичайної латентності і складності. І тому проведення комп’ютерно-технічних і телекомунікаційних досліджень та експертиз має вкрай важливе значення для оперативного реагування на кіберінциденти та ефективного розслідування кіберзлочинів.

Важливо обмінюватися досвідом, новими напрацюваннями та досягненнями у галузі кібербезпеки. Такі дії стануть важливою платформою для комунікації вітчизняних та іноземних фахівців у сфері протидії кіберзагрозам.

Розуміння важливості цих завдань підкреслюється новою Стратегією кібербезпеки України, котра була затверджена Указом Президента від 26 серпня 2021 року за № 447.

***Мета та завдання дослідження*** – впровадження дієвої системи збору, обробки та обміну інформацією стосовно кіберінцидентів, кіберзагроз, обміну технічними даними про компрометації інформаційних систем, задля забезпечення кібербезпеки організації.

***Об’єкт дослідження*** – ітераційний процес полювання на кіберзагрозу, що виконується в автоматичному режимі спеціалізованим програмним забезпеченням.

***Предмет дослідження* –** індикація ризиків, згідно виявлених та зареєстрованих раніше інцидентів.

***Методи дослідження* –** для розв’язку поставленої задачі були визначені наступні: порівняння існуючих механізмів індикації ризиків; узагальнення набутою інформації; аналіз вимог до майбутньої системи, шляхом зосередження на основних задачах; експеримент над розгорнутою системою для визначення повноти реалізації поставлених завдань.

***Наукова новизна одержаних результатів* –** в результаті застосування обраних механізмів розвідки кіберзагроз було визначено основні напрямки розповсюдження вразливостей інформаційних систем у закладі вищої освіти, що провадить освітню діяльність, пов’язану із здобуттям ступеня бакалавра або фахового молодшого бакалавра.

***Практичне значення одержаних результатів*** досягнуто за рахунок повного занотовування інформації про загрози у локальну базу даних та підключення середовища до зовнішніх екземплярів даних. Це в свою чергу дозволило упередити використання вразливостей інформаційної системи організації та надало можливість ознайомлювати здобувачів освіти з основними напрямками розповсюдження загроз у кіберпросторі.

***Публікації та апробація КР***

1.Всеукраїнська науково-практична інтернет-конференція «Вітчизняна наука на зламі епох: проблеми та перспективи розвиту» №74 (м. Переяслав, 16.11.2021).

2. X Міжнародна науково-технічна конференція молодих учених та студентів «Актуальні задачі сучасних технологій» №202 (м. Тернопіль, 24-25.11.2021).

1 АНАЛІЗ МЕХАНІЗМІВ РОЗВІДКИ КІБЕРЗАГРОЗ

1.1 Методологія кіберзагроз

Пов’язані з кібербезпекою інциденти останнім часом почали відбуватись частіше і постійно потрапляють у заголовки новин, чим викликають все більші переживання у громадян. Незважаючи на пильну увагу до таких інцидентів, яка була акцентована за останні роки, основній масі організацій по всьому світу все ще тяжко осягнути і керувати виникаючими тут і там кіберризиками в усе більш складному інформаційному середовищі. Зважаючи на те, що кожен день цифрове середовище стає складнішим і наша залежність від даних та співпраці у мережі зростає, розвиток стійкості до кібератак – широкомасштабних подій з руйнівними інформаційними та не тільки наслідками, які розвиваються по наростаючому принципу, ще ніколи не був таким важливим.



Рисунок 1.1 - Прогнозовані наслідки кібератаки на автоматизовані системи згідно дослідження глобальних тенденцій інформаційної безпеки PwC

Вже навіть були зафіксовані поодинокі випадки кібератак, які своєю дією мали вплив на життя та здоров’я людей, а також викликали ризики екологічних катастроф. Разом з цими небезпеками, деструктивний потенціал таких кібератак стає все більш очевидним [1]. Так, у грудні 2015 року вперше в результаті кібератаки на електроенергетичну систему України були виведені з ладу системи розподілу електроенергії, залишивши без електропостачання 230 000 жителів. Дана атака також була націлена і на телефонну систему нашої країни, що не дало користувачам повідомити про перебої у постачанні електрики і в результаті значно збільшило зусилля по відновленню енергопостачання.

Але, не дивлячись на все зростаючу обізнаність та розголос на загал подій та наслідків таких кібератак, багато організацій дотепер не підготовлені до справжньої протидії загрозам [6]. З 9500 топ менеджерів у 122 країнах світу, що були опитані в рамках дослідження рівня ІТ-безпеки, 44% дали відповідь, що у них немає цілісної стратегії забезпечення кібербезпеки. Ще 48% повідомили, що у них відсутня програма навчання співробітників та підвищення їхньої обізнаності у питанні захисту інформації, а 54% взагалі заявили, що у них не передбачена політика якогось реагування на надзвичайні ситуації. «Багатьом компаніям потрібно провести переоцінку ризиків та сфокусуватись на підвищеній стійкості до неминучих загроз» - так сказав Шон Джойс, керівник практики в області кібербезпеки та конфіденційності PwC у США.

Якщо взяти до уваги дані держспецзв’язку України по кількості кібератак за період у всього лиш 7 днів, то маємо наступну статистику (рисунок 1.2).



Рисунок 1.2 - Кількість інцидентів у інформаційному просторі України протягом одного тижня

Кількість атак досягає цифри у майже 45 тисяч. Кількість підозрілих подій, про які сигналізують інформаційні монітори становить більше як пів мільйона зареєстрованих.

Які ж існують найпоширеніші типи кібератак, з якими доводиться мати справу спеціалістам із захисту.

Термін «шкідливе ПЗ» застосовується, коли йдеться про шпигунське ПЗ, або програми-вимагачі, чи віруси та інтернет-хробаки. Шкідливе програмне забезпечення потрапляє в мережу через вразливість, коли користувач переходить по сторонньому посиланню або відкриває вкладений файл в електронній пошті, що призводить до інсталювання такого програмного забезпечення. Потрапивши у середину системи, шкідливе програмне забезпечення здатне:

* блокувати доступ до ключових компонентів мережі (віруси-вимагачі);
* інсталювати шкідливі програми чи додаткове шкідливе ПЗ;
* таємно збирати дані з жорсткого диска і відправляти їх зловмиснику (шпигунське ПЗ);
* порушувати роботу певних компонентів та виводити систему з ладу.

Фішинг - це розсилка електронною поштою, шахрайських повідомлень, які мають такий вигляд, ніби надіслані надійним адресатом. Головною метою цієї діяльності є присвоєння конфіденційних даних, наприклад даних кредитної картки або облікового запису, чи встановлення шкідливого ПЗ на комп'ютері жертви. Фішинг стає все більш поширеною кіберзагрозою.

Атаки через посередника (MitM) виникають, коли хакери інтегруються у взаємодію двох сторін. Отримавши доступ до мережевого трафіку, хакери можуть фільтрувати та викрадати дані.

Два поширені способи здійснення атак через посередника:

1. У незахищеній загальнодоступній мережі Wi-Fi хакери можуть перехопити контроль на ланці між пристроєм відвідувача та мережею. Не знаючи про це, користувач передаватиме всі дані через хакера.

2. Коли шкідливе програмне забезпечення потрапляє на пристрій, хакер може інсталювати програми для аналізу усіх даних жертви.

Атака за типом "відмова в обслуговуванні" переповнює систему, сервери або мережі зловмисним трафіком, що призводить до вичерпання всіх ресурсів та пропускної спроможності. У результаті ця система втрачає здатність виконувати вхідні запити. Хакери також можуть використовувати скомпрометовані пристрої для подальшої організації атак. Цей принцип називається розподіленою атакою за типом «відмова в обслуговуванні» (DDoS-атака).

SQL ін’єкція – це передача шкідливого SQL-коду на сервер, що обробляє SQL-запити, у результаті сервер розкриває дані, які малося на меті не розкривати. Щоб інтегрувати SQL-код, іноді достатньо просто ввести шкідливий код у полі пошуку вразливого вебсайту.

Експлойт нульового дня виникає після розкриття вразливості мережі до створення виправлення або вирішення цієї проблеми. У цей час хакери атакують використовуючи розкриту вразливість. Для виявлення загроз, пов'язаних із вразливістю нульового дня, потрібний постійний моніторинг.

Тунелювання DNS — це використання протоколу DNS для передачі трафіку, що не стосується DNS, через порт 53. Ця атака дозволяє відправляти через DNS трафік HTTP та інших протоколів. Тунелювання DNS може використовуватись у різних правомірних цілях. Проте існує можливість використовувати служби VPN для тунелювання DNS із злим наміром. За допомогою їх під виглядом трафіку DNS можна передавати дані, які зазвичай передаються по інтернет-каналу. За допомогою DNS-запитів зловмисник може витягти дані зі скомпрометованої системи та перенести їх у своє середовище. Їх також можна використовувати для направлення зворотних викликів з інфраструктури хакера в скомпрометовану систему.

Знаючи ці основні типи кібервтручань, можна виділити сім головних груп, які описують передусім способи, що їх застосовують зловмисники для здійснення нападу, а саме: перехоплення паролів користувачів; «соціальна інженерія»; використання помилок ПЗ і програмних закладок, а також помилок механізмів ідентифікації користувачів і недосконалості протоколів передавання даних; отримання інформації про користувачів штатними засобами операційних систем; блокування сервісних функцій системи, що зазнає атаки.

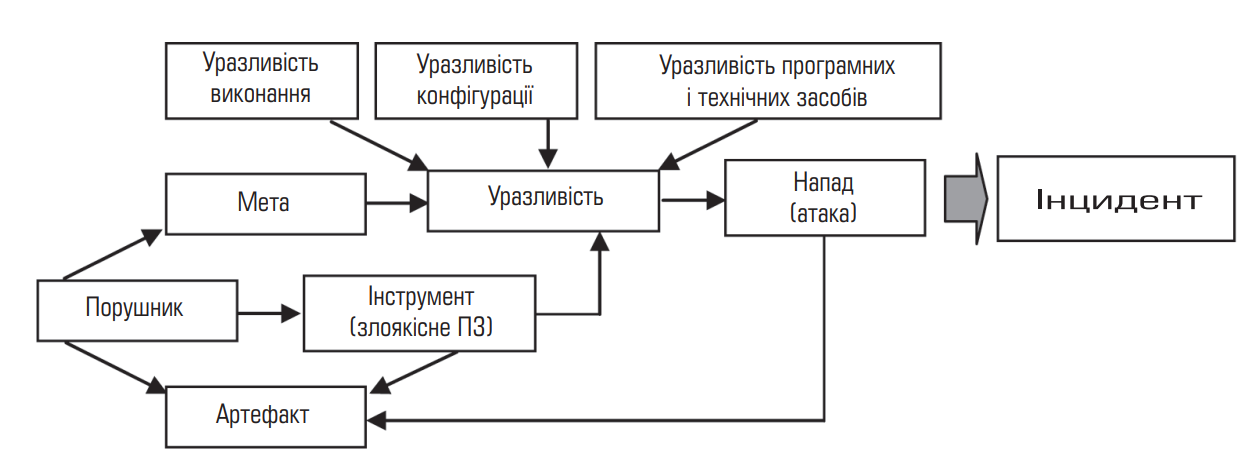


Рисунок 1.3 - Діаграма виникнення інцидентів у сфері високих технологій

Тут варто зауважити, що інтерес у плані класифікації кібернетичних втручань і загроз становить схема, запропонована Конвенцією Ради Європи 2001 року й спрямована на боротьбу з кіберзлочинністю. 1 липня 2006 року вона набула чинності для України [4].

Згідно з положеннями даної Конвенції, сторони надають одна іншій взаємну допомогу з метою розслідування або переслідування кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів у електронній формі. Відповідно до Закону України від 21.09.2010 № 2532-VI "Про внесення зміни до Закону України "Про ратифікацію Конвенції про кіберзлочинність" в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України.

Методи ж, завдяки яким можна запобігти вищеописаним кіберзагрозам, забезпечивши відповідний рівень ІБ, доцільно класифікувати так, як описано на рисунку 1.4.

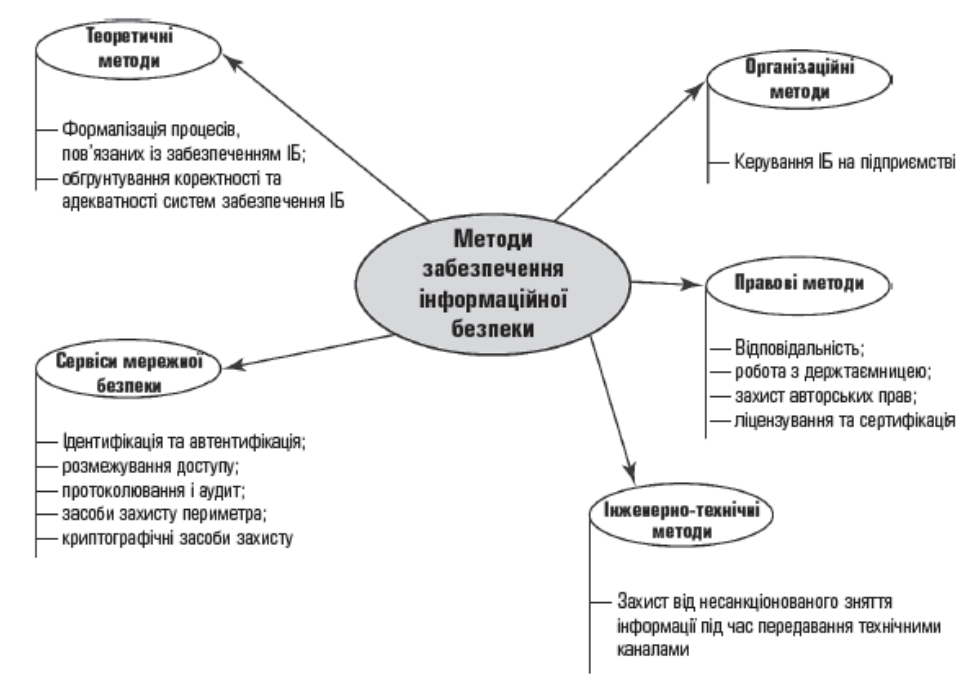


Рисунок 1.4 - Основні методи забезпечення інформаційної безпеки

Існує п’ять основних методів [8]:

* сервіси мережної безпеки (механізми захисту інформації, оброблюваної в розподілених обчислювальних системах і мережах);
* інженерно-технічні методи (мають на меті забезпечення захисту інформації від витоку по технічних каналах);
* правові та організаційні методи (створюють нормативну базу для організації різного роду діяльності, пов’язаної із забезпеченням ІБ);
* теоретичні методи забезпечення (розв’язують завдання формалізації різного роду процесів, пов’язаних із забезпеченням ІБ).

Та важливим є не тільки забезпечення цих п’яти вимог. Адже будь-яка організація повинна не вчитись на своїх помилках та аналізі проникнень у власні системи. Ключовим має стати принцип навчання, при якому отримуються актуальні розвідувальні дані про загрози.

1.2 Дослідження груп та практик розвідки та обміну інформацією в епоху злочинної діяльності в Інтернеті

У сфері кібербезпеки є кілька унікальних проблем, які ще погано досліджені та не мають стандартних рішень (більше того, їх може не бути). Американська дослідниця Медлін Карр зазначає, що навіть у США, де ДПП (державно-приватне партнерство) майже 15 років визначалося наріжним каменем національної системи кібербезпеки, сторони, на жаль, не визначили критерії, характер та сферу такого співробітництва (більше того, звіт Рахункової палати США «Доповідь про захист критичної інфраструктури: Поточний підхід до планування в секторі кібербезпеки потребує переоцінки» (Current Cyber Sector Specific Planning Approach Needs Reassessment) за 2009 р. описав досить велику кількість проблем у тих зусиллях, які були направлені американським урядом для створення ДПП у сфері кібербезпеки).

Ефективність КДПП значною мірою пов’язана з тим, як визначається кібербезпека та ступенем кореляції між кібербезпекою держави та її громадян в цілому. У багатьох випадках принцип «те, що добре для державної безпеки, має бути добре для безпеки особистості» не працює, і дуже часто – це в кібербезпеці. Більше того, майже завжди в цьому плані бракує координації, що впливає на саму основу ДПП. У зв’язку з цим Ларрі Клінтон влучно зазначає, що «партнерські відносини між громадянами, бізнесом чи урядом можуть бути набагато складнішими, ніж очікувалося. Нескоординованість ролей партнерів, їхніх обов’язків та очікувань може призвести до проблем, навіть якщо здається, що партнери мають спільні цілі. Повідомлення про потенційні відмінності також може бути проблематичним, навіть якщо партнери щиро хочуть бути успішними». Таким чином, на його думку, для ефективного ДПП раціональне та розумне управління цими відносинами може бути навіть важливішим за суть цих відносин (або їх залучення до багатьох сфер кібербезпеки).

С. Ліндер пропонує визначати суть усіх проектів кібербезпеки у сфері ДПП за двома основними напрямами:

⎯ співпраця як реформа управління;

⎯ кооперація як поділ (розподіл) влади.

Перший описаний підхід враховує, що керівники у сфері державного управління (також у сфері кібербезпеки) повинні взяти на себе навички, вміння та підхід інших колег із приватного сектору, переймаючи найкращі бізнес-практики в управлінні своїми сферами. . Цей підхід ґрунтується на тому факті, що ринок за своєю суттю більш ефективний, ніж державний, тому керівники приватного сектору є більш кваліфікованими, ніж фахівці державного сектору. Однак це припущення веде до ширших узагальнень, які логічно приводять нас до висновку, що захищати приватні мережі має приватний сектор, а не держава (такий підхід відображений в українському профільному регулюванні). Але якщо розглядати критичну інфраструктуру, то це прямо суперечить концепції загального блага, яка менше піклується про приватний сектор (який використовує власну бізнес-модель) і те, що цікавить державу та громадян. Така ситуація (у ширшому контексті) дозволила Т. Муру у своєму дослідженні виявити феномен «неузгоджених стимулів», які виникають у разі компромісу між ефективністю та безпекою. Під цим ми маємо на увазі більш звичну та інтуїтивно зрозумілу проблему, де підвищення рівня секретності (безпеки) негативно впливає на ефективність організації. Т. Мур показує такий приклад з банками: якщо банки перестануть надавати послуги онлайн-банкінгу, вони фактично стануть менш вразливими до кібератак. Проте їхні клієнти також мали б обмежений доступ до власних коштів, а витрати на обслуговування відділень цих банків (з метою забезпечення належного рівня обслуговування) були б для них непомірно високими. Та ж логіка працює в протилежному напрямку.

Другий підхід - співпраця як поділ влади базується на ідеї співпраці, при якій довіра у відносинах між партнерами замінює ідею твердої командної системи (цей підхід багато в чому підтверджує концепцію неієрархічних відносин як основа реального ДПП). Однак ця ідея «обміну інформацією» часто є найбільш суперечливою. З одного боку, і приватний сектор, і державні структури розуміють, що це одна з ключових сфер. З іншого боку, обидві сторони мають постійні застереження щодо цієї сфери співпраці. Перш за все, приватні компанії можуть злити дані про атаку. А головне, що небезпека розливу як публічно, так і виключно на своїх конкурентів. Для держави ця проблема пов’язана насамперед з тим, що більшість інформації, яка може бути цікавою для приватного сектора (і важливою для його кібербезпеки), можна охарактеризувати як обмежувальну. Також не слід ігнорувати загальну тенденцію структур держбезпеки зберігати інформацію в таємниці та збирати її, а не поширювати її іншим.

Такі дискусії вплинули на підходи до КДПП, які за своєю природою мають значний вплив на позиції основних акторів у цій сфері, зокрема Агентства Європейського Союзу з мережевої та інформаційної безпеки (ENISA). У 2010 році експерти ENISA у своєму дослідженні «Набір найкращих практик для кооперативної моделі ефективного ДПП» (де ДПП визначають як «структуровані відносини між державними та приватними організаціями, створені для суспільних інтересів та перспектив (розвитку). Досягаються через розподіл функцій (ролей) та визначення методів організації праці) запропоновано конкретну матрицю ДПП, яка дає відповіді на ключові запитання:

⎯для чого потрібен ДПП;

⎯ хто бере участь у процесі та хто є іншими учасниками;

⎯ хто про все це подбає ;

⎯ які послуги чи стимули з'являться в результаті такого впровадження;

⎯ як і коли має розвиватися така співпраця (рис. 1.5).

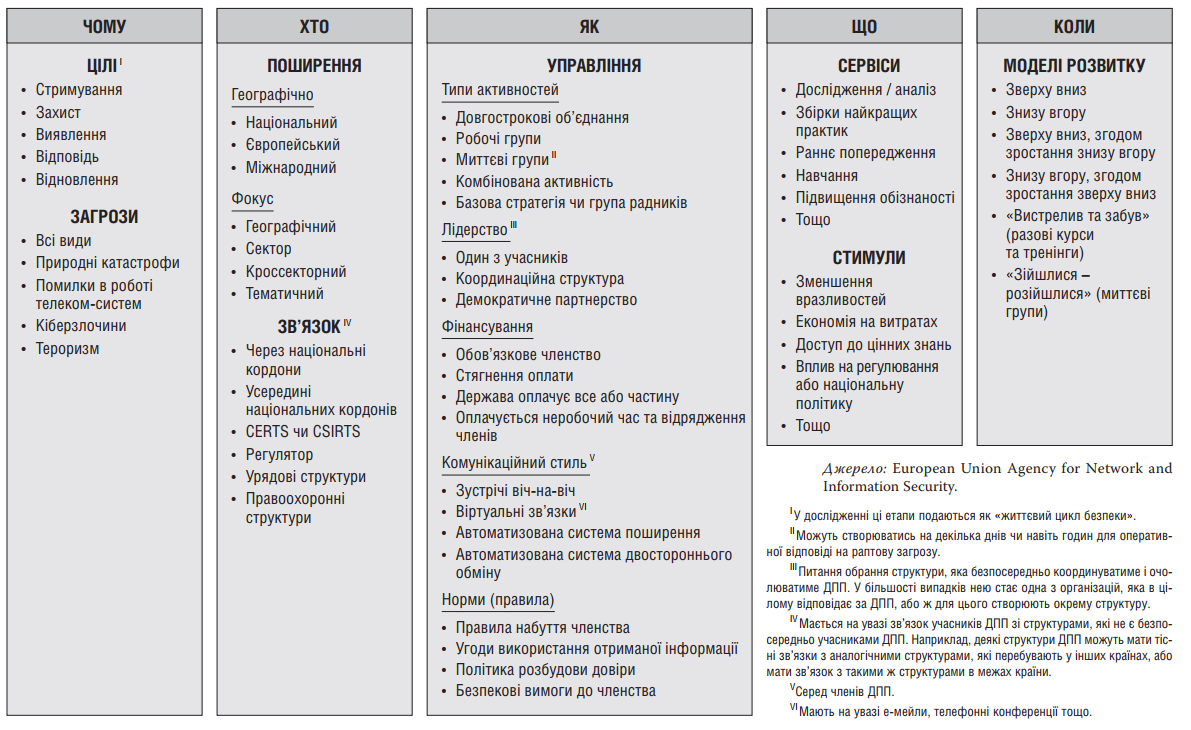


Рисунок 1.5 – матриця PPP за ENISA

 У своєму новому дослідженні державно-приватне партнерство (ДПП) «Моделі державно-приватних кооперативів», який відбувся у 2018 році, ENISA пропонує замінити цю градацію іншою, яка базується на чотирьох базових моделях КДПП:

1) інституційне ДПП. Отже, ДПП та всі інститути діють у рамках загальних принципів. Як правило, цей тип ДПП є основним джерелом для багатьох послуг, включаючи аналіз, дослідження, розробку передового досвіду, розробку рекомендацій, аудит безпеки тощо. Цей вид ДПП найчастіше пов’язують із захистом критичної інфраструктури держави. Співпраця між учасниками ДПП на основі такої моделі організовується в робочих групах, групах швидкого реагування та довгострокових асоціаціях. Основна мета — захист критичної інфраструктури в цілому, але з акцентом на захист від кібератак;

2) Цілеспрямоване ДПП. Цей тип ДПП спрямований на розвиток культури кібербезпеки в країнах-членах ЄС. Як правило, це платформа чи рада для об’єднання державного та приватного секторів для обміну знаннями та передовим досвідом.

3) послуги аутсорсингу кібербезпеки (сервіс аутсорсингу ДПП). Створення такого типу ДПП ініціюється урядом або приватним сектором, коли вони визнають недоліки в конкретній сфері, але обидві сторони не мають ресурсів чи можливостей для їх усунення. Тому головним завданням новостворених структур є підвищення рівня кібербезпеки та кіберобізнаності всіх зацікавлених сторін. З одного боку, ці структури ДПП відповідають потребам сектору у сфері рішень кібербезпеки, з іншого боку, вони можуть навіть допомагати уряду у впровадженні конкретних стандартів кібербезпеки чи підготовці національних стратегій кібербезпеки. Яскравим прикладом такого підходу є UP KRITIS в Німеччині.

4) гібридний ДПП. Загалом це означає поєднання аутсорсингу та інституційного ДПП. Такий підхід має місце, коли уряду не вистачає ресурсів, необхідних для надання певних рішень на національному рівні, і тому виникає потреба у тісній співпраці з приватною структурою, що має відповідний досвід і ресурси. Найчастіше така діяльність пов’язана з функціонуванням CSIRT.

Зрозуміло, що цей підхід (як і матриця ДПП, запропонована у 2010 р.) не є єдино можливим, але на даному етапі він дає практичне та вичерпне пояснення створення та впровадження ДПП з кібербезпеки.

У липні 2016 року Європейська комісія після низки громадських консультацій з усіма зацікавленими сторонами підписала угоду в галузі кібербезпеки, таким чином активізуючи зусилля щодо боротьби з кіберзагрозами у формі КДПП.

План дій, ініційований Європейською комісією, визначив структуру КДПП, яка надалі регулюватиме цю сферу, її економічні та правові відносини. На цю стратегію було виділено приблизно 450 мільйонів євро, основним джерелом фінансування яких є програма досліджень та інновацій в рамках Horizon 2020. Учасники ринку кібербезпеки в особі Європейської організації з кібербезпеки (ECSO) підтвердили намір інвестувати в цю ініціативу.

Партнерство має на меті забезпечити платформу для різних секторів (наприклад, охорони здоров’я, енергетики, транспорту та фінансів, а також залучення урядів, дослідницьких центрів та інших зацікавлених сторін) для розвитку інноваційного та дослідницького потенціалу сектору. Ця співпраця спрямована на зменшення негативних наслідків фрагментації ринку кібербезпеки ЄС, про що свідчать відмінності в процедурах сертифікації, щоб будь-який постачальник послуг міг працювати в будь-якій державі-члені ЄС, легко уникаючи протекціоністської політики.

Ця структура співпраці підкреслює особливу важливість інновацій - від нішевих ринків, таких як криптографія, з одного боку, до добре розроблених нових бізнес-моделей (наприклад, ринок антивірусів). Завдяки цій ініціативі Європейська комісія спробувала полегшити доступ до нових висот для малих і середніх компаній, які займаються кібербезпекою.

Загальний план дій базується на Стратегії єдиного цифрового ринку 2015 року, Європейській кіберстратегії 2013 року та Директиві ЄС щодо мережевої та інформаційної безпеки.

Європейська стратегія кібербезпеки, прийнята в 2013 році, окреслила спільне бачення Європейської комісії та Верховного представника Союзу з питань закордонних справ та політики безпеки щодо відкритого та безпечного кіберпростору.

Ця стратегія визначає основні пріоритети проблем як у національному законодавстві, так і в інших європейських країнах, пріоритетами цієї ініціативи є підвищення рівня захисту, сталий розвиток європейських мереж та розвиток технологічних і промислових ресурсів.

Хоча КДПП є вигідним для двох секторів, деякі приватні компанії неохоче дотримуються правил у цьому відношенні. Однією з головних перешкод є контроль, довіра та розкриття корпоративної інформації.

Оскільки деяка інформація може вважатися конфіденційною, багато компаній вважають, що поширення такої інформації може призвести до потенційних втрат їхньої позиції на ринку. Крім того, деякі приватні компанії можуть вважати, що поширення конфіденційної інформації може зашкодити їхній репутації, тобто публічна інформація більше не буде конфіденційною в ході державного розслідування.

Додатковим викликом є ​​складний нормативно-правовий ландшафт, за якого приватні компанії можуть бути змушені робити більше, ніж просто виконувати свої звичайні зобов’язання щодо розкриття інформації, наприклад, піддавати потенційні ризики уряду, Міністерству юстиції та навіть жертвам кіберзлочинності.

Щоб зміцнити довіру між учасниками цього процесу, Нідерланди розробили захищену інформаційну мережу, до якої уряд може отримати прямий доступ лише після того, як організація дасть свою згоду. У цій моделі суб’єкти державного та приватного секторів працюють на спільній платформі, вибудовуючи довіру, розвиваючи співпрацю та діалог, враховуючи інтереси всіх учасників процесу. Така співпраця відкриває шлях до створення нових сервісів та розвиває індустрію програмного забезпечення, покращує взаємодію суспільства та держави, підвищує прозорість і, зокрема, довіру до влади. Європейська комісія, враховуючи цілі, поставлені в Угоді, розглянула сценарії, пов’язані зі зміцненням зони кібербезпеки в Європі. Ці варіанти, після аналізу доказів з різних джерел, були ретельно відібрані, включаючи дослідження ринку кібербезпеки, опитування громадської думки та громадські консультації з понад 250 різними організаціями, що представляють як попит, так і пропозицію в галузі кібербезпеки.

1.3 Моделі аналізу даних по кіберзагрозах

Більшість систем захисту націлені на моніторинг мережі або кінцевих пристроїв й блокування шкідливого програмного забезпечення в точці входу. Ці інструменти одразу ж сканують файли або мережевий трафік на наявність загроз, як правило, використовуючи сигнатурний метод. Якщо ж шкідливе програмне забезпечення доставляється до місця призначення частинами, або воно модифікується, стаючи шкідливим після потрапляння до пристрою, то дані технології виявлення вже не зможуть помітити наступні дії з розгортання атаки [11].

При цьому нові атаки не можна назвати одномоментними: вони тривають довго і вимагають постійної уваги. Тобто традиційні методи захисту, що використовуються в підрозділах забезпечення кіберзахисту, метою яких є лише виявлення і блокування атак в точці входу, більше не ефективні.

Які ж існують моделі аналізу кіберзагроз? Це такі, як: діамантова модель аналізу вторгнень, модель Cyber Kill-Chain, адаптивна модель безпеки з компетенціями та можливостями та інші [14].

Діамантова модель представляє нову концепцію аналізу вторгнень, побудовану аналітиками кібербезпеки. Модель встановлює, що основний «атомний елемент» будь-якої діяльності зі вторгнення чи кіберінцидент, складається з чотирьох основних функцій: зловмисника, інфраструктури, спроможності та жертви (рисунок 1.6). При виявлені події автоматизовано або за допомогою аналітиків заповнюються вершини моделі. Вершини пов'язані ребрами й виділяють природні зв’язки між функціями. Проходячи по ребрах та вершинах, аналітики виявляють більше інформації про операції зловмисника та виявляють нові спроможності, інфраструктуру та жертв.

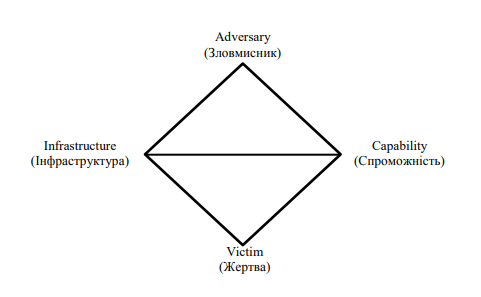


Рисунок 1.6 - Діамантова модель аналізу вторгнень

Моделлю, яку зазвичай використовують для виокремлення етапів проведення кібератак, є запропонована корпорацією Lockheed Martin, як частина моделі Intelligence Driven Defense, модель Cyber Kill-Chain. Ця модель визначає типовий порядок дій зловмисника для досягнення поставлених цілей. Так, для досягнення успіху зловмисник повинен пройти усі вісім етапів (рисунок 1.7).



Рисунок 1.7 - Модель Cyber Kill-Chain

Зрозуміло, що зловмисник не обов’язково повинен дотримуватися проходження усіх наведених кроків, але ефективність його діяльності при цьому може знизитись. Доречно припустити, що чим раніше системи захисту виявлять спрямовані зловмисні дії, тим більш ефективно працює вся система захисту. Блокування зловмисника на будь-якому етапі розриває весь ланцюжок атаки.

В той же час в аналітиками компанії Gartner було запропоновано архітектуру Адаптивної системи безпеки для захисту від просунутих атак. Представлена архітектура зміщує точку зору на захист від «реакції на інцидент» до «безперервного контролю». Вона складається з чотирьох категорій компетенцій високого рівня та з 12 категорій можливостей (рисунок 1.8). Названі компоненти архітектури повинні працювати інтелектуально разом як інтегрована, адаптивна система, яка безпосередньо втілює повноцінний процес захисту від сучасних загроз. Постійний моніторинг та аналітика є основою архітектури адаптивного захисту.

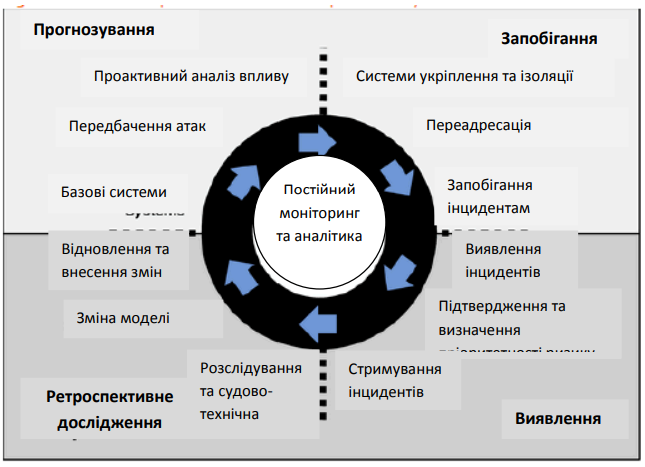


Рисунок 1.8 - Адаптивна модель безпеки з компетенціями та можливостями

Виокремимо два типи задач, розв’язуваних із різною ефективністю різними методами KDD (Knowledge Discovery in Databases).

Задачі першого типу полягають у побудові на підставі наявних даних різних моделей, якими можна скористатися з метою прогнозування та ухвалення рішення в майбутньому, за схожої ситуації.

Задачі другого типу характерні тим, що наголос у них робиться на з’ясуванні сутності залежностей у множині даних, а також взаємовпливу, тобто на побудові емпіричних моделей різних систем, які легко може сприймати людина. При цьому не так уже й важливо, щоб система добре передбачала і працювала в майбутньому, а важливо зрозуміти взаємні впливи досліджуваних закономірностей (що і чим визначається в наявному масиві даних). І навіть якщо встановлені закономірності належатимуть до специфічних особливостей саме конкретних досліджуваних даних і більше ніде не траплятимуться, але нам усе одно потрібно їх з’ясувати.

Розглянемо головні етапи (кроки), характерні для будь-якого дослідження даних за допомогою методів KDD і становлять основний цикл пошуку нового знання та його оцінювання (рисунок 1.9). Залежно від задачі кількість етапів, а також обсяг виконуваних на кожному з них дій можуть змінюватися, але загалом усі вони необхідні і так чи інакше мають належати процесу інтелектуального аналізу даних.

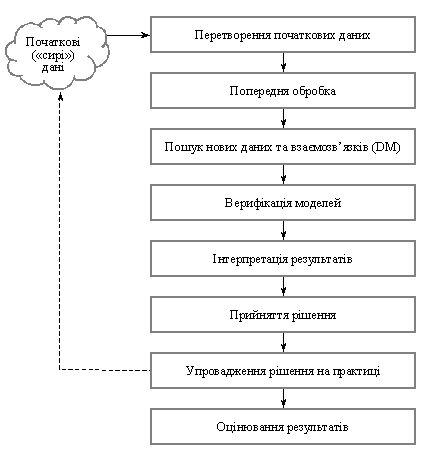


Рисунок 1.9 - Схема інтелектуального аналізу даних і оцінювання виявленого нового знання

Перший етап полягає у зведенні даних до форми, придатної для застосування конкретних реалізацій систем KDD. Нехай, скажімо, інформацію подано у вигляді текстів і потрібно побудувати автоматичний каталогізатор, класифікатор якихось анотацій, описів тощо. Вхідна інформація являє собою тексти в електронному вигляді, але практично жодна з наявних систем KDD не здатна працювати безпосередньо з текстами. Щоб працювати з певним текстом, ми маємо з вихідної текстової інформації заздалегідь дістати деякі похідні параметри (наприклад, частоту появи ключових слів, середню довжину речень, параметри, що характеризують сполучуваність тих чи інших слів у реченні тощо), тобто побудувати чіткий набір кількісних або якісних параметрів даного тексту. Ця задача найменш автоматизована в тому сенсі, що систему шуканих параметрів формує людина, хоча значення параметрів можуть обчислюватися автоматично в рамках відповідної технології первинної обробки даних. Вибравши параметри, дані можна подати у вигляді прямокутної таблиці, де кожний рядок характеризує окрему ознаку (стан, властивість) досліджуваного об’єкта, а кожний стовпець — ознаки (стани, властивості) всіх досліджуваних об’єктів. Рядки такої таблиці в теорії KDD, як і в теорії баз даних, називають записами, а стовпці — полями.

Практично всі наявні системи KDD працюють тільки зі щойно описаними прямокутними таблицями.

Здобута прямокутна таблиця — це лише «сировинний» матеріал для застосування методів KDD, і дані, що входять до неї, необхідно передусім обробити. По-перше, таблиця може містити параметри (ознаки об’єктів), що мають однакові значення в якомусь зі стовпців. Коли б досліджувані об’єкти мали тільки такі ознаки, усі вони були б абсолютно ідентичними. Звідси випливає, що відповідні ознаки жодним чином не характеризували б досліджуваних об’єктів, а отже, їх потрібно вилучити з аналізу. Можлива й така ситуація, що деяка категоріальна ознака в усіх її записах має різні значення, через що відповідне поле не придатне для аналізу даних і його також доведеться вилучити. Нарешті може статися так, що полів буде дуже багато, і якщо ми всі їх намагатимемося досліджувати, то надто відчутно збільшиться час розрахунків, оскільки практично для всіх методів KDD характерна сильна (не менш ніж квадратична, а нерідко й експоненціальна) залежність часу розрахунків від кількості параметрів, тоді як залежність часу розрахунків від кількості записів лінійна або близька до неї.

Тому у процесі попередньої обробки даних необхідно, по-перше, розглянути множину всіх ознак, що стосуються шуканої залежності, вилучити з неї ті, які явно не придатні для подальшого дослідження, та виокремити ті, що найімовірніше ввійдуть у шукану залежність. Для цього, як правило, застосовують статистичні методи, що ґрунтуються на застосуванні кореляційного аналізу, лінійних регресій, тобто методи, що дають змогу швидко, хоча й наближено оцінити вплив одного параметра на інші.

Третій етап — безпосереднє застосування методів KDD за різними сценаріями, що містять складні комбінації тих методів, які допомагають аналізувати дані з різних поглядів. Власне, цей етап дослідження і називають Data Mining (добування даних).

Четвертий етап — верифікація та перевірка результатів, найчастіше здійснювані в такий спосіб. Усі наявні дані, що мають бути проаналізовані, розбивають на дві (як правило, не однакові за розміром) групи. У більшій групі даних за допомогою тих чи інших методів KDD дістають моделі й залежності, а в меншій виконують їх перевірку. Далі за різницею в точності між результатами, здобутими для обох груп, доходять висновку щодо адекватності й статистичної значущості побудованої моделі. Існує багато інших, складніших способів верифікації (перехресна перевірка, бутстреп-аналіз тощо), які дають змогу оцінити значущість побудованих моделей без розбиття даних на дві групи.

Нарешті, на п’ятому етапі знання, що їх здобула людина, автоматично інтерпретуються з метою їх використання для прийняття рішень та внесення сформульованих правил і залежностей до баз знань тощо. Цей етап часто передбачає застосування методів, що є проміжними між технологією KDD і технологією експертних систем. Від того, наскільки ефективним він буде, значною мірою залежить успіх розв’язання поставленої задачі.

Цим етапом і закінчується цикл KDD. Остаточне оцінювання вагомості здобутого нового знання виходить за рамки аналізу, автоматизованого чи традиційного, і стає можливим тільки після впровадження на практиці рішення, прийнятого на основі такого знання. Дослідженням практичних результатів, досягнутих за допомогою здобутого засобами KDD нового знання, завершується його оцінювання (рисунок 1.9).

Таким чином будь-яке підприємство здатне йти цим шляхом аналізу та опрацювання інцидентів або ж здатне використовувати готові результати описаного дата майнінгу [12]. Зрозуміло, що обрання другого підходу має ряд беззаперечних переваг, однак для повноцінного розуміння цього можна зобразити два шляхи графічно (рисунок 1.10).

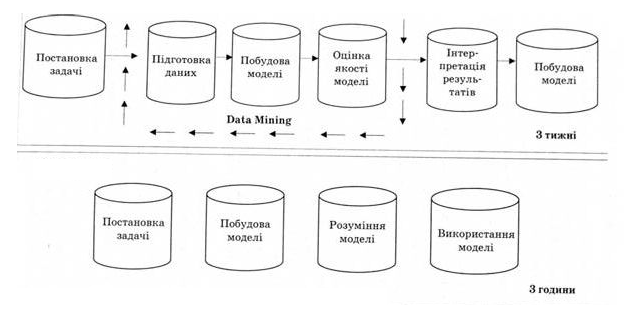


Рисунок 1.10 - Відмінність традиційного процесу збору інформації та використання середовища обміну інформацією

Найважливішим ресурсом сучасного підприємства, здатним значно вплинути на підвищення його конкурентоспроможності, є знання. Їхня значимість стає більш пріоритетною, ніж інші ресурси, капітал, праця, тощо. Можливість почерпнути сформовані знання, готові рішення, здатна вивести підприємство на значно вищий конкуренто-спроможний рівень.

1.4 Безпечне розподілене навчання щодо розвідки загроз

У сучасному взаємопов’язаному світі кількість нових загроз та індикаторів інцидентів постійно збільшується, до такої міри, що неможливо адаптувати системи виявлення та пом’якшення без оновленої та всеосяжної бази знань, яку можна використовувати для розшифрування моделей інцидентів. і тренувати передові моделі, які можуть їх передбачати та виявляти.

Поточні зусилля щодо обміну даними розвідки загроз (наприклад, платформа обміну інформацією про шкідливі програми, MISP), працюють над централізованою базою даних, куди всі організації-учасники мають завантажувати свої дані про загрози.

Інформація про кібербезпеку часто є надзвичайно чутливою та конфіденційною, вона створює компроміс між перевагами покращених можливостей реагування на загрози та недоліками розкриття інформації, пов’язаної з національною безпекою, іноземним агентствам чи установам. Це призводить до збереження цінної інформації (так само як проблема фрірайдера), що значно обмежує ефективність обміну даними [17]. Тому метою таких проектів є вирішення проблеми обміну інформацією щодо кібербезпеки шляхом надання точнішого аналізу більших обсягів більш релевантних колективних даних розвідки загроз.

Перевага проекту обміну розвідувальними даними дозволить установам створювати кращі моделі шляхом безпечної співпраці з цінними конфіденційними даними, які зазвичай не передаються. Це розширить діапазон доступних розвідувальних даних, що призведе до нових і кращих аналізів і прогнозів загроз.

Це стало можливим завдяки тому, що пропонуються доказові технологічні гарантії, коли авторизовані користувачі платформи можуть отримати доступ лише до глобальної статистики (моделі кіберзагроз), побудованої на даних усієї мережі, тоді як доступ або передача не надається до локальних даних, які залишаються під контролем його джерело. Дана мета досягається шляхом розробки MISP-сумісної розподіленої архітектури без централізованої бази даних (кожна установа зберігає повний контроль над своїми записами даних, які ніколи не залишають периметр безпеки), і шляхом інтеграції передових криптографічних методів, заснованих на парадигмі багатостороннього гомоморфного шифрування, що дає можливість ефективно та масштабовано обчислювати моделі машинного навчання на зашифрованих розподілених даних, а також забезпечити безпечний випуск або моделі, або лише передбачень, створених модель (model-as-a-service), відповідно до моделі системи [15]. Як це виглядає, можна побачити на рисунку 1.11.

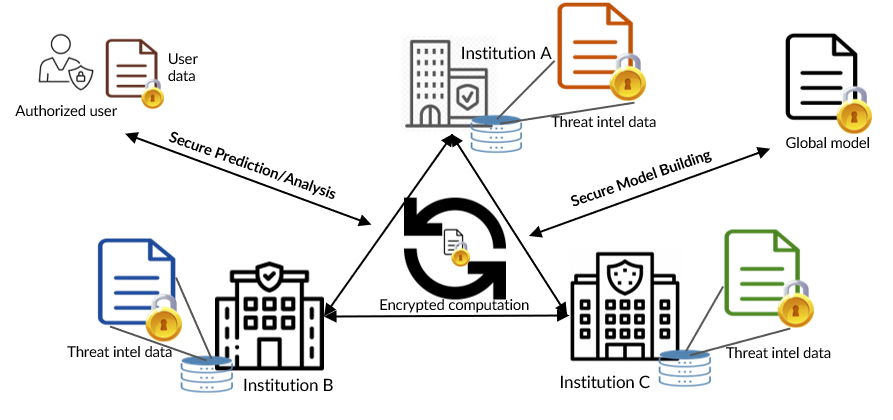


Рисунок 1.11 - Схематичне представлення принципу обміну інформацією про загрози

Модель машинного навчання (machine-learning, ML) зазвичай вимагає великих і різноманітних наборів даних (рисунок 1.12). У багатьох сферах, таких як медицина та фінанси, збирання достатньо великих наборів даних виявляється складним і часто вимагає обміну даними між кількома постачальниками даних. Це особливо вірно в медицині, де дані пацієнтів розподіляються між кількома організаціями: наприклад, щодо рідкісних захворювань, в одній лікарні може бути лише кілька пацієнтів, тоді як медичне дослідження вимагає сотень пацієнтів, щоб отримати значні результати. Обмін даними серед багатьох організацій, які можуть бути розташованими в кількох країнах, є, таким чином, необхідним. Однак, якщо дані є конфіденційними або особистими, ними особливо важко поділитися. Обмін даними сильно обмежений правовими нормами, такими як GDPR в Європі. Фінансові та репутаційні наслідки порушення даних часто роблять ризик обміну даними вищим, ніж його потенційні вигоди. Тому часто неможливо отримати достатньо даних для навчання моделей ML, які є ключовими факторами в дослідженнях, аналізі.

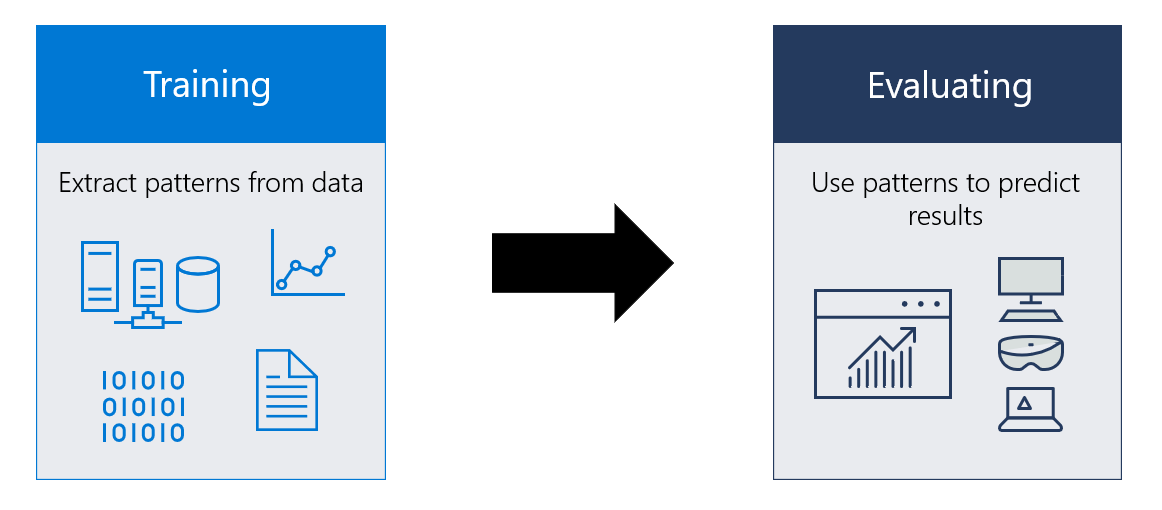


Рисунок 1.12 - Модель машинного навчання

Для вирішення цієї проблеми все більший інтерес набувають рішення для збереження конфіденційності, оскільки вони можуть бути ключами для ML із конфіденційними даними. Багато було запропоновано рішень для безпечних прогнозів, які використовують попередньо навчені моделі. Однак, безпечне навчання моделей ML, яке є набагато більш вимогливим до обчислень, було менш вивченим. Було запропоновано деякі централізовані рішення, які спираються на гомоморфне шифрування (homomorphic encryption, HE). Вони мають перевагу за рахунок того, що прості у застосуванні, але вимагають передачі окремих записів з-під контролю їх власників, що часто неможливо, наприклад, через законодавство про захист даних. Також дані переміщуються в центральне сховище, яке може стати єдиною точкою невдачі. Захищені багатосторонні обчислювальні рішення (SMC), запропоновані для цього сценарію, часто припускають, що обмежена кількість комп’ютерних сторін є чесними, але допитливими і не вступають у змову. Ці припущення можуть не виконуватися, коли дані є чутливі та/або коли у сторін є конкуруючі інтереси. Зазвичай, гомоморфне шифрування (HE) або гібридне (HE та SMC) рішення, які припускають модель шкідливої ​​загрози (наприклад, модель Anytrust), зосереджені на обмежених операціях ML (наприклад, навчання регулярній лінійній моделі з малою кількістю функцій) і не є квантово безпечними. Останні досягнення квантових обчислень зробили цю технологію потенційною загрозою в недалекому майбутньому для існуючих криптографічних рішень.

Google нещодавно оголосили про те, що вони досягли «квантової переваги». Незважаючи на те, що квантові комп’ютери ще далекі від того, щоб зламати сучасні криптосхеми, ми зазначаємо, що певні дані (наприклад, геноміка) залишаються чутливими протягом тривалого періоду та будуть під загрозою в майбутньому.

Нарешті, федеративне навчання, некриптографічний підхід до навчання моделей машинного навчання, що зберігає конфіденційність, нещодавно викликало інтерес. Дані залишаються під контролем їх власників, а сервер координує навчання, надсилаючи модель безпосередньо власникам даних, які потім оновлюють модель своїми даними. Оновлені моделі від кількох учасників усереднюють для отримання глобальної моделі.

Останні роботи показали, що обмін проміжними моделями з координуючим сервером або між учасниками може призвести до різних атак на конфіденційність, наприклад, вилучення даних учасників або висновку про членство. Щоб вирішити ці проблеми, кілька робіт покладаються на диференційовано приватний механізм для обфускації проміжних значень. Однак ця заплутаність зменшує корисність даних і моделі, тоді як навчання точних моделей вимагає великих бюджетів конфіденційності та досягнутого рівня конфіденційності залишається неясною.

Висновок до першого розділу

Під час ознайомлення з механізмами розвідки кіберзагроз було досліджено юридичне та програмне підґрунтя даної галузі. Зроблені наступні висновки.

1. Виявлено, що інтерес у плані класифікації кібернетичних втручань і загроз становить схема, запропонована Конвенцією Ради Європи 2001 року й спрямована на боротьбу з кіберзлочинністю. 1 липня 2006 року вона набула чинності для України.

2. Дослідивши статистичні дані виявлено, що не дивлячись на зростаючу обізнаність та публічний розголос подій та наслідків кібератак, багато компаній дотепер не підготовлені до реальної протидії загрозам. З 9500 топ менеджерів у 122 країнах світу, які були опитані в рамках дослідження рівня ІТ-безпеки, 44% відповіли, що у них відсутня цілісна стратегія забезпечення кібербезпеки. Ще 48% повідомили, що не мають програми навчання співробітників та підвищення їх обізнаності у питаннях захисту інформації, а 54% заявили, що у них не передбачена політика реагування на надзвичайні ситуації.

Разом з тим кібербезпекова сфера має певні унікальні проблеми, які все ще слабко досліджені та не мають універсальних «рецептів» рішень (більше того, можливо, вони взагалі їх не мають).

3. Виявлено, що основою загального плану дій захисту слугують Стратегія єдиного цифрового ринку 2015 р. (Digital Single Market Strategy for Europe), Кіберстратегія Європейського Союзу 2013 р. (Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace) та Директива ЄС щодо мережевої та інформаційної безпеки (NIS Directive on security of network and information systems).

4. Виявлено, що поточні зусилля щодо обміну даними розвідки загроз (наприклад, платформа обміну інформацією про шкідливі програми, MISP), працюють над централізованою базою даних, куди всі організації-учасники мають завантажувати свої дані про загрози.

Інформація про кібербезпеку часто є надзвичайно чутливою та конфіденційною, вона створює компроміс між перевагами покращених можливостей реагування на загрози та недоліками розкриття інформації, пов’язаної з національною безпекою, іноземним агентствам чи установам. Це призводить до збереження цінної інформації (так само як проблема фрірайдера), що значно обмежує ефективність обміну даними. Тому метою таких проектів є вирішення проблеми обміну інформацією щодо кібербезпеки шляхом надання точнішого аналізу більших обсягів більш релевантних колективних даних розвідки загроз.

2 РОЗГОРТАННЯ MISP THREAT SHARING ДЛЯ УПЕРЕДЖЕННЯ РОЗПОВСЮДЖЕННЮ ІНЦИДЕНТІВ

2.1 Використання спільної платформи для обміну інформацією про загрози

Існує два типи обміну інформацією, кожен з яких визначається тим, хто ділиться інформацією (рисунок 2.1):

1. Односпрямований обмін розвідувальними даними про загрози – один суб’єкт виробляє та ділиться розвідувальними даними про загрози, які споживають інші, а ті, хто споживає розвідку, не вносять у відповідь. Приклади односпрямованого обміну розвідувальними даними про загрози включають:

* Розвідка з відкритим кодом, яка може включати в себе використання каналу розвідки про загрози з відкритим кодом або завантаження загальнодоступного звіту про нещодавню атаку, що містить індикатори та використані методи.
* Звіти та канали із закритими джерелами

1. Двонаправлений обмін розвідувальними даними про загрози – розвідувальні дані надсилаються для споживання, але також можуть бути отримані від організацій-членів. Хоча обмін дозволений і заохочується в цих програмах, немає гарантії, що кожна організація поділиться чим-небудь.

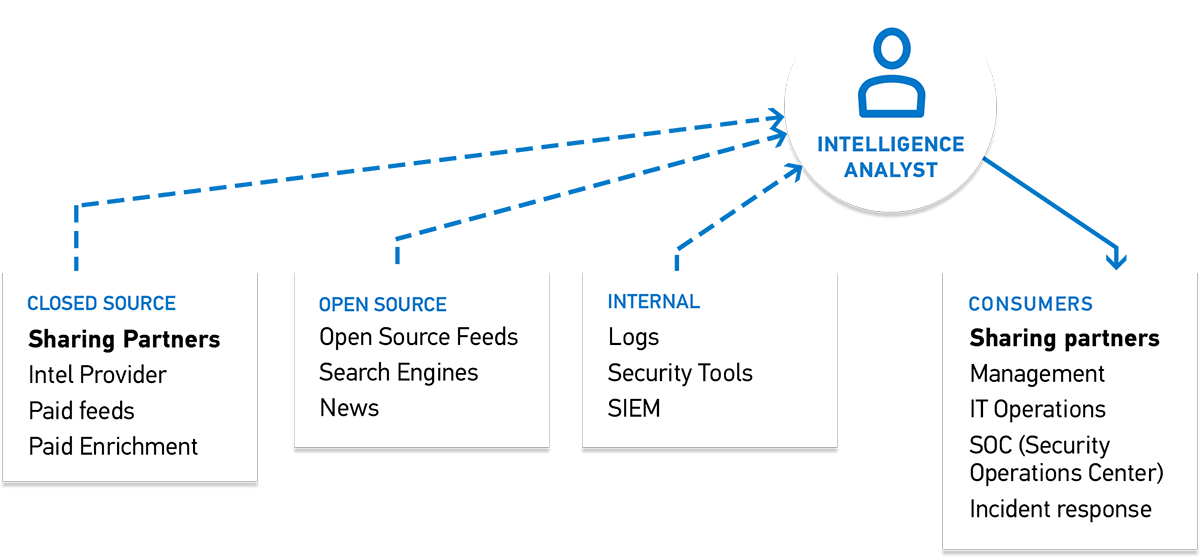


Рисунок 2.1 - Обмін розвідувальними даними про загрози

Основні функції найпопулярніших платформ розвідки загроз включають консолідацію каналів інформації про загрози з кількох джерел, автоматичне виявлення та стримування нових атак, аналітику безпеки та інтеграцію з іншими інструментами безпеки, такими як SIEM, брандмауери наступного покоління (NGFW) та EDR [18].

Найяскравішими представниками таких платформ є наступні [20].

*IBM X-Force Exchange* — це хмарна платформа для спільного аналізу загроз, яка допомагає аналітикам безпеки досліджувати показники загроз, щоб прискорити час до дій. Цей TIP поєднує створені людиною розвідувальні дані з глобальною мережею безпеки, пропонуючи унікальний погляд на потенційні загрози. Панель інструментів X-Force Exchange налаштовується, дозволяючи користувачам розставляти пріоритети відповідних розвідувальних даних відповідно до своїх потреб, таких як поради та вразливості.

*Anomali ThreatStream* об’єднує мільйони індикаторів загроз, щоб виявляти нові атаки, виявляти існуючі порушення та давати можливість командам безпеки швидко розуміти та стримувати загрози. Ключовою відмінністю Anomali є його високоточний алгоритм машинного навчання, який призначає оцінки індикаторам компромісу (IOC), щоб команди безпеки могли визначити пріоритети завдань з пом’якшення. ThreatStream також дозволяє інтегруватися з багатьма популярними SIEM та платформами оркестрування.

*SolarWinds (SEM)* — це потужний інструмент, який поєднує відстеження подій із каналом розвідки загроз. Він не тільки здатний ідентифікувати потенційні та активні загрози, але також може використовувати відповідні заходи для їх усунення. SolarWinds SEM був розроблений з чіткою централізованою панеллю інструментів і командним інтерфейсом, що дозволяє легко відстежувати виявлені загрози та швидко вживати заходів для вирішення проблем безпеки. Цю інформаційну панель також можна використовувати для створення аналітичних звітів.

*Palo Alto Networks AutoFocus* робить аналітику загроз з повним контекстом доступною для організацій будь-якого розміру. Ця розміщена служба надає командам з безпеки аналітичних даних, кореляції, контексту та автоматизованих робочих процесів запобігання, які їм необхідні для виявлення та реагування на події в режимі реального часу. AutoFocus також включає доступ до сховища оперативної розвідки Unit 42, внутрішньої групи дослідження загроз Palo Alto Networks.

*LogRhythm Threat Lifecycle Management (TLM)* забезпечує скоординовану колекцію аналізу даних та можливостей реагування на інциденти, щоб дозволити організаціям по всьому світу швидко виявляти, нейтралізувати та відновлюватися після інцидентів безпеки. Він може обробляти 26 мільярдів повідомлень на день. Платформа також може автоматизувати виявлення загроз і визначення пріоритетів за допомогою зіставлення шаблонів і розширеної кореляції з машинним навчанням і статистичним аналізом.

*FireEye Mandiant Advantage* додає контекст і пріоритет глобальним загрозам до, під час і після атаки. Що відрізняє FireEye від конкурентів, так це те, як його платформа адаптує стратегічний інтелект до корпоративного управління ризиками та бізнес-цілей організації, надаючи високо контекстуальні дані, щоб користувачі могли узгоджувати стратегії безпеки, щоб реагувати на найбільш ймовірні загрози, спрямовані на організацію.

*LookingGlass Cyber ​​Solutions* — це платформа розвідки загроз з відкритим вихідним кодом, яка забезпечує уніфікований захист від складних кібератак глобальним підприємствам і державним установам шляхом оперативної розвідки загроз. Він надає найбільш релевантні дані для бізнесу, класифікуючи елементи мережі в сховище під назвою Колекції. Його інструмент оцінки довіри індикаторів загроз потім використовує цю інформацію для визначення найбільш пріоритетних ризиків, з якими стикається організація.

*AlienVault Unified Security Management (USM)*, продукт AT&T CyberSecurity, отримує дані про загрози від AlienVault Labs та його масової Open Threat Exchange (OTX), найбільшої у світі спільної біржі загроз із натовпу. Він забезпечує централізоване виявлення загроз, реагування на інциденти та керування відповідністю для хмарних і локальних середовищ. Завдяки розвідці загроз від AT&T Alien Labs, USM автоматично оновлюється кожні 30 хвилин.

Розібравшись, які переваги має кожна з платформ, можна зробити висновок, що розвідки загроз (Threat Intelligence Platforms, TIP) є ​​критичними інструментами безпеки, які використовують глобальні дані безпеки, щоб допомогти професійно виявляти, пом’якшувати та усувати загрози безпеці. Нові загрози, які постійно розвиваються, з’являються щодня. Хоча аналітики з безпеки знають, що ключ до випередження цих загроз полягає в аналізі даних про них, проблема, яка виникає, полягає в тому, як ефективно збирати великі обсяги даних і, як наслідок, отримати корисну інформацію, щоб запобігти майбутнім атакам.

Платформи розвідки загроз працюють наступним чином: підказки об’єднують інформацію про безпеку від постачальників, аналітиків та інших авторитетних джерел про загрози та підозрілу активність, виявлені по всьому світу, за допомогою інструменту, який називається каналами розвідки загроз. Ці дані можуть надходити у вигляді шкідливих IP-адрес, доменів, хеші файлів тощо. Платформи розвідки загроз потім перетворюють ці розширені аналітичні дані в ефективні інтелектуальні дані для виявлення зловмисної активності у власній мережі. Все це складає триетапну стратегію (рисунок 2.2). Ці канали часто інтегруються в інші продукти безпеки, як-от EDR, SIEM та брандмауери наступного покоління.

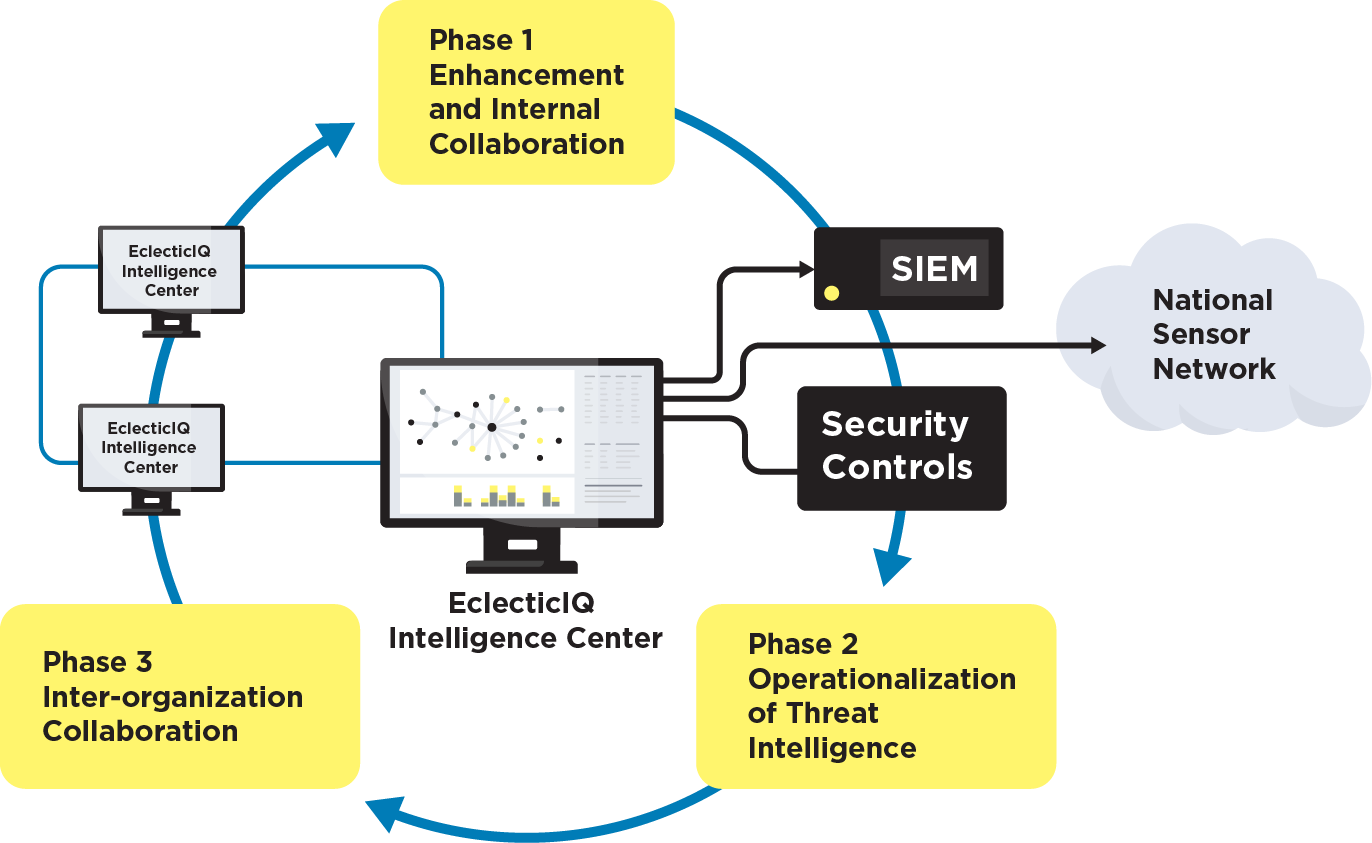


Рисунок 2.2 - Триетапна стратегія поширення та співпраці

Основною ключовою особливістю будь-якої платформи розвідки загроз є здатність аналізувати та обмінюватися даними про загрози. Ці інструменти можуть ідентифікувати сигнатури загроз у мережі та передавати цю інформацію іншим установкам, а також отримувати інформацію про нові загрози з каналів загроз. Це робить платформи розвідки загроз невід’ємною частиною зупинки загроз нульового дня.

Іншою ключовою особливістю є можливість сортування даних і сповіщень при виявленні загроз. Вони надсилатимуть сповіщення лише тоді, коли виникають законні загрози, щоб уникнути непотрібного потоку сповіщень, які можуть замутити воду для виправлення, хоча платформи можуть потребувати деякого тонкого налаштування. Щоб допомогти у виправленні, вони також можуть призначити оцінку ризику, щоб групи безпеки могли визначити пріоритети, які проблеми слід діяти першими.

Управління вразливістю доповнює функції платформ аналізу загроз. Ці рішення можуть містити загрози, коли вони виявлені, заощаджуючи команді безпеки дорогоцінний час на вирішення проблем. Вони також можуть запропонувати інструкції щодо усунення поширених та нових загроз, щоб ще більше прискорити процес.

Серед списку вищеописаних платформ є ще одна, яка і була обрана базою для проведення дослідження – MISP. Метою MISP - платформи розвідки та обміну загрозами з відкритим вихідним кодом є:

* Полегшення зберігання технічної та нетехнічної інформації про побачене зловмисне програмне забезпечення та атаки.
* Автоматичне створення зв’язків між шкідливими програмами та їх атрибутами.
* Зберігання даних в структурованому форматі (що дозволяє автоматично використовувати базу даних для подачі систем виявлення або криміналістичних інструментів).
* Створення правил для системи виявлення вторгнень в мережу (NIDS), які можна імпортувати в системи IDS (наприклад, IP-адреси, доменні імена, хеші шкідливих файлів, шаблони в пам'яті).
* Розшарювання атрибутів шкідливого програмного забезпечення та загроз з іншими сторонами та групами довіри.
* Покращення виявлення зловмисного програмного забезпечення та скасування його, щоб сприяти обміну інформацією між організаціями (наприклад, уникнення повторюваних робіт).
* Створення платформу довіри - довірена інформація від надійних партнерів.
* Зберігання локально всієї інформації з інших екземплярів (забезпечуючи конфіденційність запитів).

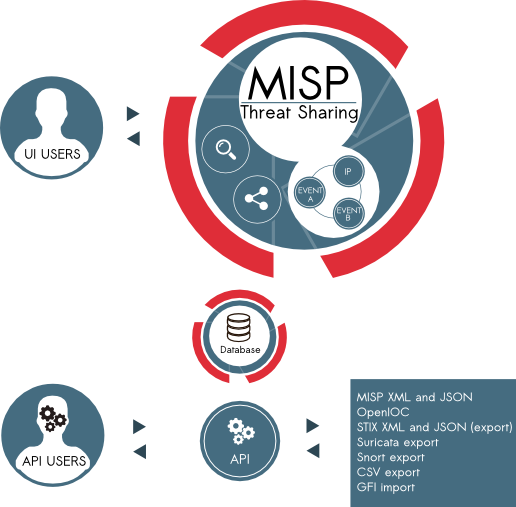


Рисунок 2.3 - Принцип роботи MISP

Платформа обміну інформацією про зловмисне програмне забезпечення доступна з різних інтерфейсів (рисунок 2.3), як-от веб-інтерфейс (для аналітиків або обробників інцидентів) або через ReST API (для систем, які надсилають і витягують IOC). Невід'ємною метою MISP є бути надійною платформою, яка забезпечує безперебійну роботу від виявлення, опрацювання та використання інформації про загрози.

Те, як інформація поширюється між інстанціями MISP у всьому світі зображено на рисунку 2.4.

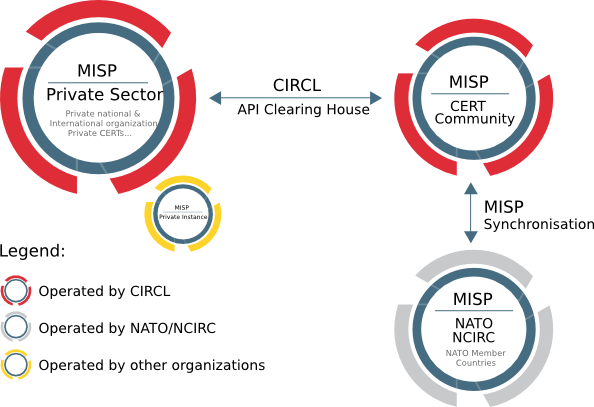


Рисунок 2.4 - Спосіб поширення інформації між інстанціями MISP

У MISP є 4 варіанти розподілу подій та їх відповідних атрибутів:

* Лише власна організація.
* Тільки поточна спільнота.
* Підключені спільноти.
* Усі громади.

Існує також набір груп спільного використання, доступних для різних членів у кожному секторі (наприклад, фінансовий сектор).

На рисунку 2.4 можна побачити огляд екземплярів якими керує MISP. Оскільки розподіл є притаманним з’єднанню між екземплярами MISP, учасники повинні пам’ятати про загальну зв’язність, щоб вибрати відповідну категорію розповсюдження.

2.2 Розгортання системи розвідки кіберзагроз MISP Threat Sharing

Для того, щоб розгорнути платформу MISP необхідна наявність встановленого дистрибутиву Ubuntu 18.04. Далі працюючи з командним рядком, починається процес інсталяції та налаштування [21].

Перш за все, необхідно додати нового користувача:

checkUsrLocalSrc () {

echo ""

if [[ -e /usr/local/src ]]; then

WRITEABLE=$(sudo -H -u $MISP\_USER touch /usr/local/src 2> /dev/null ; echo $?)

if [[ "$WRITEABLE" == "0" ]]; then

echo "Good, /usr/local/src exists and is writeable as $MISP\_USER"

else

# TODO: The below might be shorter, more elegant and more modern

#[[ -n $KALI ]] || [[ -n $UNATTENDED ]] && echo "Just do it"

sudo chmod 2775 /usr/local/src

sudo chown root:staff /usr/local/src

fi

else

echo "/usr/local/src does not exist, creating."

mkdir -p /usr/local/src

sudo chmod 2775 /usr/local/src

# TODO: Better handling /usr/local/src permissions

if [[ "$(cat /etc/group |grep staff > /dev/null 2>&1)" == "0" ]]; then

sudo chown root:staff /usr/local/src

fi

fi

}

Далі для налаштування змінних конфігурації MISP необхідно виконати наступну команду:

eval "$(curl –fsSL https://raw.githubusercontent.com/MISP/MISP/2.4/docs/

generic/globalVariables.md | awk '/^# <snippet-begin/,0' | grep -v \`\`\`)"

MISPvars

Після вищеописаних дій необхідно виконати наступні завдання:

1. запуск скрипту, для налаштування конфігурації;
2. запуск скрипту для встановлення LAMP і залежностей;
3. інтеграція коду MISP;
4. налаштування відповідних дозволів;
5. створення бази даних та користувача для неї (на даному етапі важливо не забути після створення імпортувати пусті записи);
6. конфігурація Apache-серверу;
7. конфігурація MISP.

Враховуючи те, що код цих семи завдань є доволі об’ємним, ознайомитись з ним можна у додатку А.

2.3 Застосування платформи в межах ВСП «РФК НУБіП України» шляхом нотування виявлених інцидентів

Процес введення події можна розділити на 3 фази: створення самої події, заповнення її атрибутами та вкладеннями та, нарешті, опублікування [22].

Під час першого кроку створюється основна подія без будь-яких фактичних атрибутів, але в цей момент зберігається загальна інформацію, така як опис, час і рівень ризику інциденту. Щоб розпочати створення події, натискається кнопка «Нова подія» ліворуч і заповнюється форма, що відкривається. Необхідно заповнити такі поля, як представлено на рисунку 2.5..

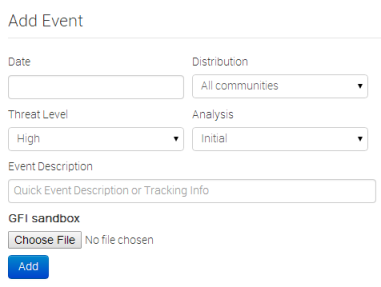


Рисунок 2.5 - Створення нової події

* *Дата*: дата, коли стався інцидент. Необхідно просто клацнути це поле, і з’явиться засіб вибору дати, де можна вибрати потрібну дату.
* *Розповсюдження*: це налаштування контролює, хто зможе побачити цю подію, як тільки вона буде опублікована, і врешті-решт, коли вона буде вилучена. Окрім можливості встановити, яким користувачам на цьому сервері дозволено бачити подію, цей пункт також контролює, чи буде подія синхронізована з іншими серверами чи ні. Розповсюдження успадковується за атрибутами: головним є найбільш обмежувальний параметр. Доступні такі варіанти:
* Лише ваша організація: це налаштування дозволить бачити це лише користувачам поточної організації. Один із користувачів поточної організації може перетягнути його в інший екземпляр, де його зможе бачити лише поточна організація. Події з цим налаштуванням не будуть синхронізовані.
* Лише для цієї спільноти: користувачі, які є частиною поточної спільноти MISP, зможуть побачити подію. Це включає власну організацію, організації на цьому сервері MISP та організації, що працюють із серверами MISP, які синхронізуються з цим сервером. Будь-які інші організації, підключені до таких зв’язаних серверів, не зможуть бачити подію.
* Підключені спільноти: користувачі, які є частиною поточної спільноти MISP , зможуть побачити подію. Сюди входять усі організації на цьому сервері MISP, усі організації на серверах MISP, які синхронізуються з цим сервером, і організації хостингу серверів, які підключаються до цих вищезгаданих серверів. Будь-які інші організації, підключені до пов’язаних серверів, які знаходяться за 2 кроки від цього власного, не зможуть бачити подію.
* Усі спільноти. Це дозволить поділитися подією з усіма спільнотами MISP, що дозволить вільно передавати подію від одного сервера до іншого.
* Група спільного доступу: ця подія надає доступ до визначеної групи спільного доступу. Це включає лише організації, визначені в групі спільного використання. Залежно від визначення групи спільного доступу розподіл може бути локальним і між примірником.
* *Рівень загрози*: це поле вказує рівень ризику події. Інциденти можна розділити на три різні категорії загроз (низька, середня, висока). Альтернативно, це поле можна залишити невизначеним. Є 3 варіанти:
* Низький: загальне масове шкідливе програмне забезпечення.
* Середній: розширені постійні загрози (APT).
* Високий: складні APT та атаки 0 днів.
* *Аналіз*: вказує на поточний етап аналізу події з такими можливими варіантами:
* Початок: аналіз тільки починається.
* Триває : аналіз триває.
* Завершено: Аналіз завершено.
* *Опис події*: інформаційне поле, де зловмисне програмне забезпечення/інцидент може отримати 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. Варто пам’ятати, що система автоматично замінить виявлені текстові рядки, які відповідають запису регулярного виразу, налаштованого адміністратором(-ами) сервера.
* *GFI Sandbox*: можна завантажити експортований файл .zip із пісочниці GFI за допомогою цього інструмента. Вони будуть опрацьовані MISP, а список атрибутів і вкладень буде автоматично створено з файлу .zip. Хоча це виконує більшу частину роботи, необхідної для виконання на другому етапі створення події, важливо вручну переглянути всі дані, які вводяться.

Другим кроком створення події є заповнення її атрибутами та вкладеннями. Це можна зробити, додавши їх вручну або імпортуючи атрибути із зовнішнього формату (OpenIOC, ThreatConnect). Щоб імпортувати із зовнішнього формату або завантажити вкладення, треба скористатися відповідними параметрами в меню (рисунок 2.6).



Рисунок 2.6 - Додавання атрибутів події

За допомогою кнопок, показаних вище, можна заповнити подію за допомогою різних інструментів.

Додавання атрибуту. Система шукає регулярні вирази в полі значень усіх атрибутів під час введення, замінюючи в ньому знайдені рядки, встановлені адміністратором сервера (наприклад, щоб застосувати стандартизоване використання великих літер у шляхах для кореляції подій або надати точні шляхи до стандартизований формат). Необхідно заповнити наступні поля.

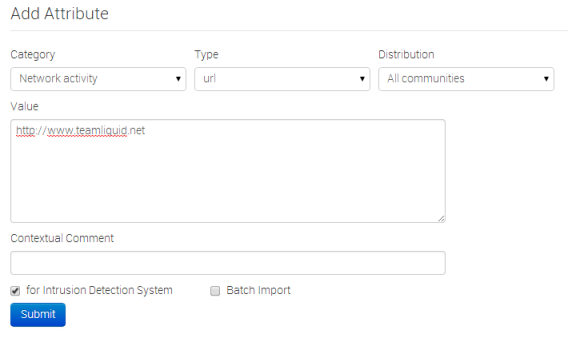


Рисунок 2.7 - Додавання атрибуту події

* *Категорія*: це спадне меню пояснює категорію атрибута, тобто який аспект зловмисного програмного забезпечення описує цей атрибут. Це може означати механізми збереження зловмисного програмного забезпечення або мережевої активності, тощо.
* *Тип*: у той час як категорії визначають, який аспект події вони описують, тип пояснює, за допомогою чого цей аспект описується. Наприклад, IP-адреса джерела атаки, вихідна адреса електронної пошти або файл, надісланий через вкладений файл, можуть описувати доставку корисного навантаження зловмисного програмного забезпечення. Це будуть типи атрибутів із категорією доставки корисного навантаження.
* *Розповсюдження*: цей спадний список дозволяє контролювати, хто зможе бачити цей атрибут. Розповсюдження успадковується за атрибутами: вверху найбільш обмежувальний параметр.
* *Значення*: вводяться дані про значення на основі того, що є дійсним для вибраного типу атрибута. Наприклад, для атрибута типу ip-src (IP-адреса джерела) 11.11.11.11 буде дійсним значенням.
* *Контекстуальний коментар*: можна додати деякі коментарі до атрибута, які не використовуватимуться для кореляції, а натомість служать виключно інформаційним полем.
* *Для системи виявлення вторгнень*: цей параметр дозволяє використовувати атрибут як підпис IDS під час експорту даних NIDS , якщо він не відхиляється списком дозволених. Щоб дізнатися більше про дозволений список, треба перейти до розділу адміністрування. Якщо прапорець IDS не встановлено, атрибут розглядається як контекстна інформація і не використовується для автоматичного виявлення.
* *Пакетний імпорт*: якщо є кілька атрибутів одного типу для введення (наприклад, список IP-адрес, можна ввести їх усі в одне поле значення, розділене розривом рядка між кожним.

Опублікування події. Після того, як усі атрибути та вкладення, які необхідно включити в подію, завантажено/встановлено, настав час завершити її створення, опублікувавши подію (кнопка «Опублікувати подію» у перегляді подій, рисунок 2.8).

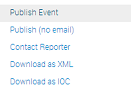


Рисунок 2.8 - Публікація події

Дана дія попередить відповідних користувачів про інцидент (на основі приватного контролю події та її атрибутів/вкладень, а також від того, чи увімкнено автоматичне сповіщення), перемістить подію до екземплярів, до яких поточний екземпляр підключається, і поширить його далі на основі правила розподілу. Він також готує атрибути, пов’язані з мережею, для створення підпису NIDS (за допомогою функції експорту підпису NIDS). Існує альтернативний спосіб публікації події без сповіщення інших користувачів за допомогою кнопки «опублікувати (без електронної пошти)». Це слід використовувати лише для незначних змін (наприклад, для виправлення друкарської помилки).

Якщо у поточному екземплярі ввімкнено фонові завдання, подія може бути опублікована не відразу. Про це варто пам’ятати.

2.4 Автоматизація роботи у системі шляхом шаблонування

Нові користувачі можуть бути легко перевантажені новою інформацією, якщо їм доведеться вручну заповнювати події атрибутами без будь-яких вказівок. Яка інформація повинна бути підкріплена до конспектування інциденту? Якою має бути категорія та тип IP-адреси C2? Шаблони дозволяють користувачам використовувати прості форми для заповнення подій. Незважаючи на те, що MISP постачається з кількома шаблонами за замовчуванням, користувачі (з відповідними правами на створення шаблонів ) можуть створювати нові шаблони для своїх користувачів або для всіх користувачів екземпляра [23]. Для того, щоб створити шаблон, необхідно спочатку перейти до Дії події - Додати шаблон, щоб перейти до перегляду створення події (рисунок 2.9).

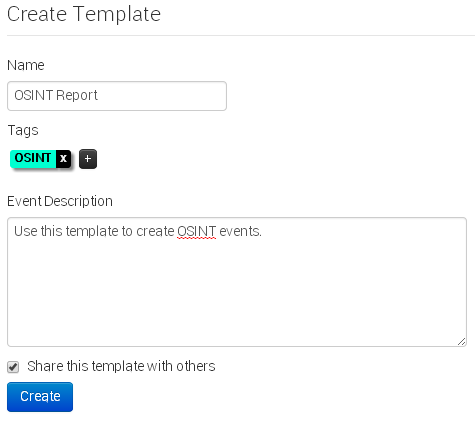


Рисунок 2.9 - Створення шаблону події MISP

Необхідно заповнити такі поля:

* *Ім’я*: ім’я шаблону має описувати, який тип події він має використовуватися для створення атрибутів.
* *Теги*: можна прикріпити теги до шаблону - подія, заповнена за допомогою шаблону, автоматично отримає тег(и). Додаються нові теги за допомогою кнопки «+». Якщо після додавання тегу користувач передумав, можна видалити його, натиснувши на хрестик біля імені тегу.
* *Опис події*: короткий опис подій, для яких слід використовувати цей шаблон.
* *Поділіться цим шаблоном з іншими*: шаблон можна налаштувати на використання будь-якою організацією в екземплярі або лише тією, яка його створила.

Після створення скелета шаблону можна почати заповнювати шаблон даними. Є 3 типи елементів, які можна використовувати під час створення шаблону: атрибут, файл і текстові елементи. Текстові елементи поділяють шаблон на розділи з інформаційним полем, за яким слідують усі поля атрибутів/файлів, доки не буде прочитано нове текстове поле. Не варто турбуватися про порядок елементів під час створення, їх можна змінити за допомогою перетягування.

Першим елементом шаблону є атрибут. Його додавання представлено на рисунку 2.10.

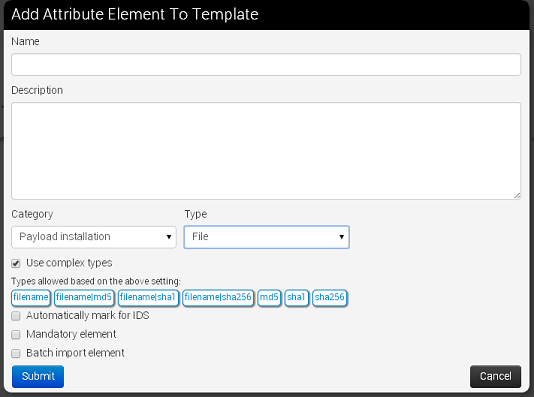


Рисунок 2.10 - Додавання атрибуту до шаблону інциденту

На цьому етапі необхідно заповнити такі поля:

* *Ім'я*: ім'я поля, яке буде представлено користувачеві.
* *Опис*: короткий опис елемента. Варто лаконічно і точно донести до користувача інформацію.
* *Категорія*: категорія, яка використовується для будь-яких атрибутів, створених за допомогою цього елемента шаблону.
* *Тип*: тип або складний тип, який використовується для будь-яких атрибутів, створених за допомогою цього елемента шаблону. Складні типи дозволяють використовувати декілька споріднених типів для введення даних. Наприклад, елемент складного типу "файл" дозволяє використовувати імена файлів і хеші.
* *Використовувати складні типи*: якщо категорія дозволяє це, можна перейти до складного типу за допомогою цього прапорця.
* *Автоматично позначати для IDS*: якщо позначено, будь-які атрибути, згенеровані за допомогою цього елемента, будуть позначені для експорту IDS.
* *Обов’язковий елемент*: якщо елемент позначено як обов’язковий, то шаблонну форму можуть надіслати лише певні користувачі.
* *Елемент пакетного імпорту*: дозволяє вводити кілька значень (розділених розривами рядків).

Наступним, другим, елементом шаблону є файл. Вікно додавання файлу до екземпляру представлене на рисунку 2.11.

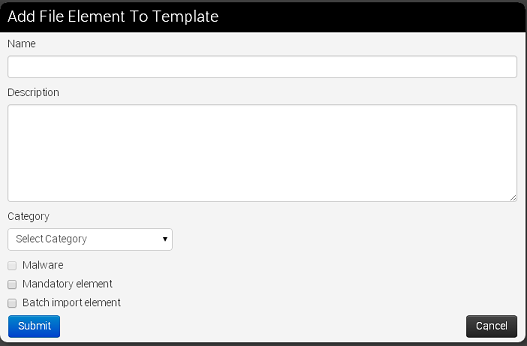


Рисунок 2.11 - Додавання файлу до події шаблону

У вказаному вікні необхідно заповнити такі поля, як: ім'я, опис, категорія, шкідливе програмне забезпечення, обов’язковий елемент, елемент пакетного імпорту.

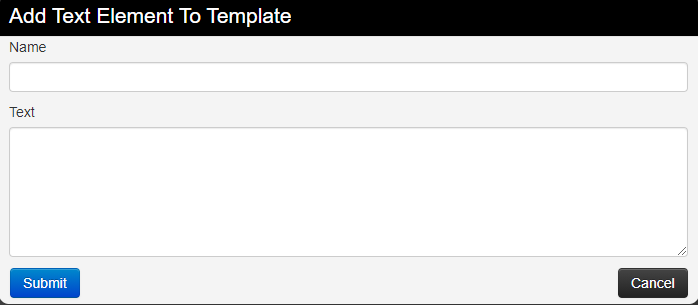


Рисунок 2.12 - Додавання текстового елементу до шаблону

Останнім, третім, елементом шаблону є файл (рисунок 2.12). У даному розділі варто коротко пояснити користувачеві, з чим будуть мати справу наступні елементи атрибута/файлу. Існує кілька способів розділити шаблон на розділи, варто намагатися мати на увазі простоту використання під час його створення.

Висновок до другого розділу

Під час розгортання та перших застосувань системи розвідки кіберзагроз було проведено аналіз даної платформи в контексті інформаційного простору ВСП «РФК НУБіП України» визначено наступні твердження.

1. Зроблено висновок, що існує два типи обміну інформацією, кожен з яких визначається тим, хто ділиться інформацією: односпрямований обмін розвідувальними даними про загрози – один суб’єкт виробляє та ділиться розвідувальними даними про загрози, які споживають інші; двонаправлений обмін розвідувальними даними про загрози – розвідувальні дані надсилаються для споживання, але також можуть бути отримані від організацій-членів.

2. Проведено аналіз основних ключових особливостей будь-якої платформи розвідки загроз, таких як здатність аналізувати та обмінюватися даними про загрози. Ці інструменти можуть ідентифікувати сигнатури загроз у мережі та передавати цю інформацію іншим установкам, а також отримувати інформацію про нові загрози з каналів загроз. Це робить платформи розвідки загроз невід’ємною частиною зупинки загроз нульового дня.

3. Зроблено висновок, що однією з передових платформ, серед тих, які є у сучасному інформаційному просторі, є MISP. Платформа обміну інформацією про зловмисне програмне забезпечення доступна з різних інтерфейсів, як-от веб-інтерфейс або через ReST API. Невід'ємною метою MISP є бути надійною платформою, яка забезпечує безперебійну роботу від виявлення, опрацювання та використання інформації про загрози.

Для того, щоб розгорнути платформу MISP необхідна наявність встановленого дистрибутиву Ubuntu 18.04.

4. Проведено аналіз процесу введення події, котрий можна розділити на 3 фази: створення самої події, заповнення її атрибутами та вкладеннями та, нарешті, опублікування. Також дана платформа має функцію шаблонування. Шаблони дозволяють користувачам використовувати прості форми для заповнення подій. Незважаючи на те, що MISP постачається з кількома шаблонами за замовчуванням, користувачі (з відповідними правами на створення шаблонів ) можуть створювати нові шаблони для своїх користувачів або для всіх користувачів екземпляра.

3 РЕЗУЛЬТАТ ЗАСТОСУВАННЯ ПЛАТФОРМИ ОБМІНУ ДАНИМИ MISP THREAT SHARING

3.1 Результат впровадження системи розвідки кіберзагроз на прикладі ВСП «РФК НУБіП України»

Для впровадження в інформаційний простір системи розвідки кіберзагроз було виділено окремий комп’ютер у локальній мережі. Він працює під керівництвом операційної системи Windows 10 (рисунок 3.1). Так як розгортання такого осередку є по суті пілотним проектом, було вирішено на початках встановити MISP у віртуальному середовищі. Для його встановлення апаратних потужностей згідно специфікації повинно бути достатньо.

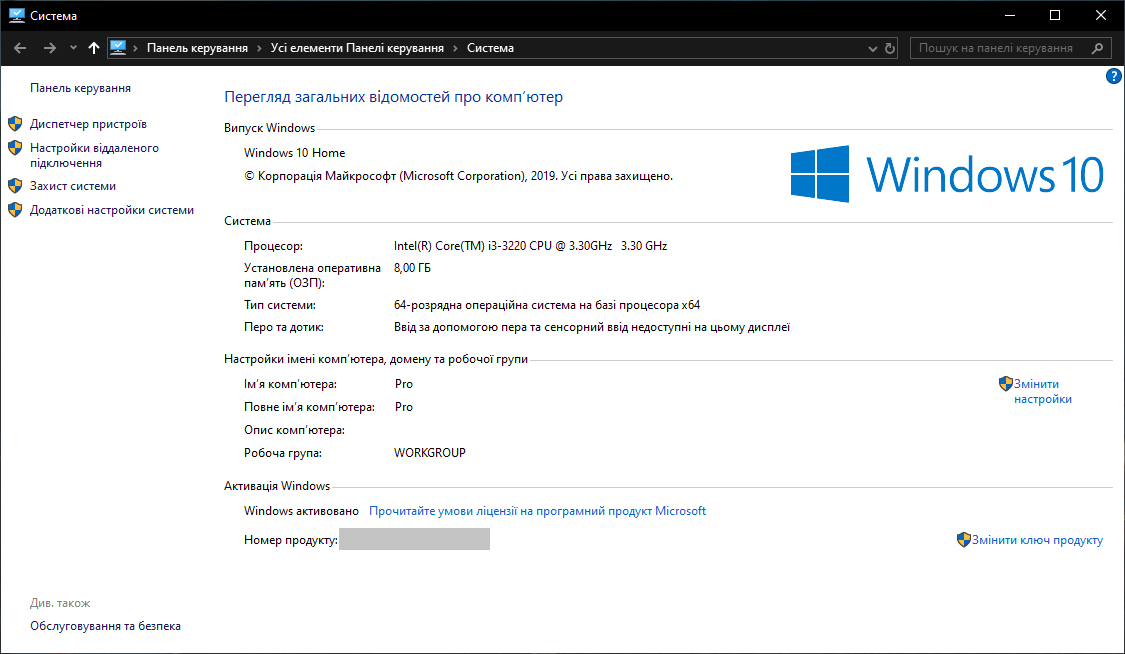


Рисунок 3.1 - Параметри серверу для розгортання платформи розвідки кіберзагроз

Існує дві типові програми, які зазвичай використовуються користувачами, котрим необхідна технологія віртуалізації. Цими програмами є: VirtualBox та VMware Workstation. Вибір пав на останню, так як вона позиціонує себе, як потужна та максимально надійна. Тож в якості віртуального осередку було обрано програму та версію VMware Workstation 15 Pro trial. Її 30-ти денного пробного періоду достатньо для ознайомлення, тестування, попереднього налаштування та подальшого створення експортних файлів платформи.

У VMware Workstation є наступні системні вимоги:

* Сумісний 64-розрядний процесор x86 або AMD64, випущений в 2011 році або пізніше.
* Тактова частота 1,3 ГГц або вище.
* Мінімум 2 Гбайт ОЗП; рекомендовано 4 Гбайт або більше.

Загальні вимоги да ОС вузла:

* Windows 10
* Windows Server 2019
* Windows Server 2016
* Windows Server 2012
* Windows 8
* Ubuntu
* Red Hat Enterprise Linux
* CentOS
* Oracle Linux

Після встановлення віртуальної машини було здійснено перше налаштування для видимості та зв’язку її з локальною мережею коледжу.

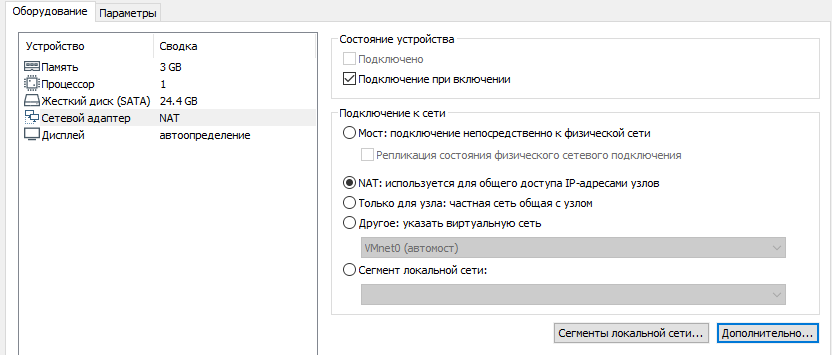


Рисунок 3.2 - Системні налаштування віртуальної машини

Процес розгортання системи розвідки кіберзагроз MISP Threat Sharing докладно описаний у пункті 2.2 даної роботи, тож повторно на ньому зупинятися не варто.

Після встановлення Ubuntu та MISP Threat Sharing, вікно віртуальної машини набуває наступного вигляду:

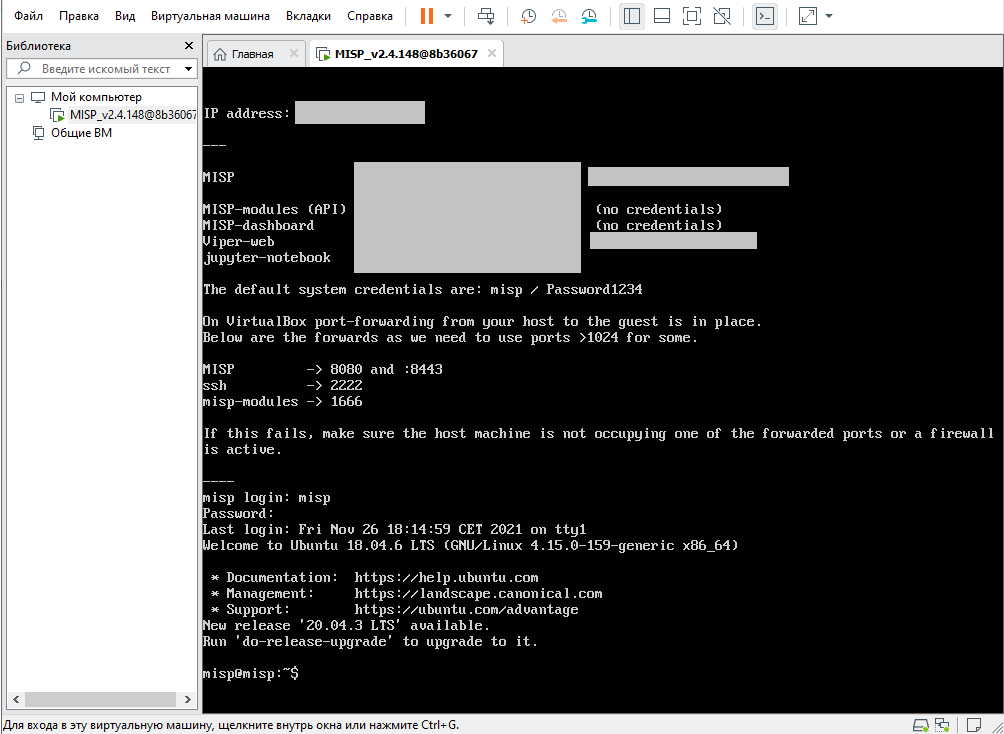


Рисунок 3.3 - Запущений віртуальний сервер Ubuntu 18.04

Коли платформа MISP налаштована, у адміністратора з’являється можливість потрапити до вебінтерфейсу з локальної мережі організації. Доступ здійснюється за допомогою ІР-адреси через будь-який, з наявних, браузер.

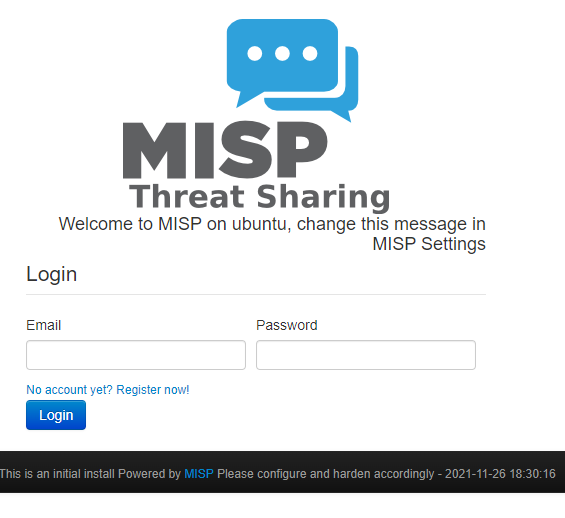


Рисунок 3.4 - Вікно авторизації у вебінтерфейс платформи розвідки кіберзагроз

Після успішного встановлення MISP є ціла низка шляхів для подальшого розвитку платформи в межах навчального закладу. По-перше планується включити ознайомлення з даною програмою в навчальний процес для унаочнення механізму обміну захищеною інформацією по каналах зв’язку та ознайомлення з базовими принципами захисту від кіберінцидентів.

По-друге, враховуючи впровадження MISP-UA Службою безпеки України ще у 2018 році для забезпечення державно-приватної взаємодії по спільному захисту інформаційного та кіберпростору, є можливість долучитися до обміну інформацією. Адже на платформі MISP-UA вже зареєстровані понад 300 користувачів, серед яких державні і приватні підприємства (в тому числі навчальні заклади).

По-третє, є можливість запускати тематичні хакатони з використанням платформи розвідки кіберзагроз, де б команди зі студентів мали можливість розвиваючи загальне поняття про основні правила з кіберзахисту, вирішувати спільні завдання з підтримки захищеності інформаційного простору.

На даний же момент іде робота по підготовці підключення платформи до зовнішніх серверів для спільного обміну інформацією.

3.2 Підключення та навчання нових користувачів платформи

Користувач з правами адміністратора, може створювати нові облікові записи для користувачів, редагувати профілі користувачів, видаляти їх або просто переглядати профілі всіх користувачів. Адміністратори організації ( Org Admin ) можуть виконувати ці дії виключно в межах користувачів своєї організації.

Щоб додати нового користувача, необхідно натиснути кнопку «Додати користувача» в меню адміністрування зліва та заповнити всі поля, доступні для завантаженого перегляду:

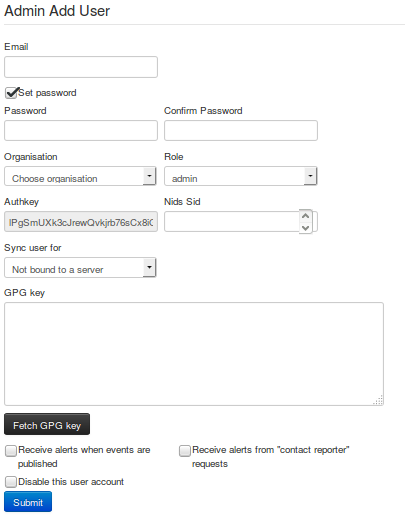


Рисунок 3.5 - Додавання нового користувача MISP

Адміністратор заповнює такі поля:

* *Електронна пошта*: адреса електронної пошти користувача, вона використовуватиметься як його/її ім’я для входу та як адреса для надсилання всіх автоматизованих електронних листів, а також електронних листів, надісланих шляхом звернення до користувача як доповідача події.
* *Установити пароль*: встановлюється прапорець, якщо необхідно визначити тимчасовий пароль для користувача. Якщо ви цього не зробите, скористайтеся кнопкою дії «скинути пароль» у вікні «Список користувачів», щоб створити його та надіслати користувачеві електронною поштою.
* *Пароль*: це текстове поле відображається лише тоді, коли встановлено прапорець «Встановити пароль». Тимчасовий пароль для користувача, який він/вона має змінити після першого входу. Необхідно переконатися, що пароль відповідає політиці паролів MISP .
* *Підтвердити пароль*: це текстове поле відображається лише тоді, коли встановлено прапорець «Встановити пароль». Це має бути точна копія поля Пароль.
* *Організація*: випадаючий список дозволяє вибрати організацію для користувача.
* *Ролі*: випадаючий список дозволяє вибрати групу ролей, до якої має належати користувач. Ролі визначають привілеї користувача, які йому приписуються.
* *Ключ автентифікації*: він призначається автоматично і є унікальним ключем автентифікації зазначеного користувача (він/вона зможе скинути його та отримати новий ключ). Він використовується для експорту та для підключення одного сервера до іншого, але він вимагає, щоб користувач був призначений ролі з дозволом авторизації.
* *NIDS SID*: система виявлення вторгнення в мережу (NIDS) ідентифікатор підпису (SID). Правила Snort, експортовані створеним користувачем, матимуть зміщення, визначене в профілі користувача, і кожне правило, згенероване під час експорту, отримуватиме зростаючий SID, починаючи зі зміщення користувача. Якщо за замовчуванням не вказано зміщення SID, буде встановлено рандомізоване значення.
* *Синхронізувати користувача для*: необхідно використовувати цей параметр, щоб надати користувачеві право синхронізувати подію між сервером MISP. Цей параметр доступний для ролі адміністратора, адміністратора організації та користувача синхронізації .
* *Gpgkey*: ключ, який використовується для шифрування електронних листів, надісланих через систему.
* *Отримати ключ GnuPG*: отримати відкритий ключ GnuPG.
* *Отримувати сповіщення, коли події публікуються*. Ця опція підписує нового користувача на автоматично створені електронні листи щоразу, коли публікується подія.
* *Отримувати сповіщення від запитів «зв’язатися з репортером»*. Ця опція підписує нового користувача на електронні листи, які генеруються, коли інший користувач намагається зв’язатися з організацією, яка повідомляє про подію, яка збігається з організацією нового користувача.
* *Вимкнути цей обліковий запис користувача*: встановлюється галочка, якщо Ви хочете вимкнути цей обліковий запис користувача.

Щоб перерахувати всіх поточних користувачів системи, необхідно просто клацнути «Список користувачів» у меню адміністрування зліва. Буде завантажено представлення даних, що містить список усіх користувачів та інші стовпці інформації:

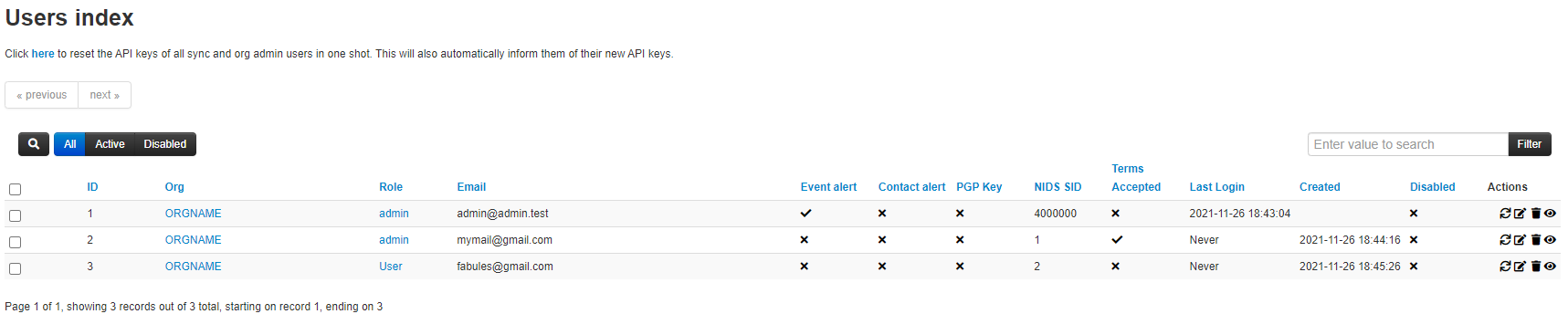


Рисунок 3.6 - Перелік усіх користувачів

Існує, звичайно ж, і можливість редагування даних користувача (рисунок 3.7). В даному вікні відображаються ті самі параметри, що й на етапі створення. Різниця полягає тільки у декількох пунктах:

* *Умови прийняті*: вказує, чи прийняв користувач уже умови використання чи ні.
* *Змінити пароль*: встановлення цього прапора вимагатиме від користувача зміни пароля після наступного входу.
* *Скинути ключ авторизації*: дане посилання використовується, щоб створити новий ключ авторизації.

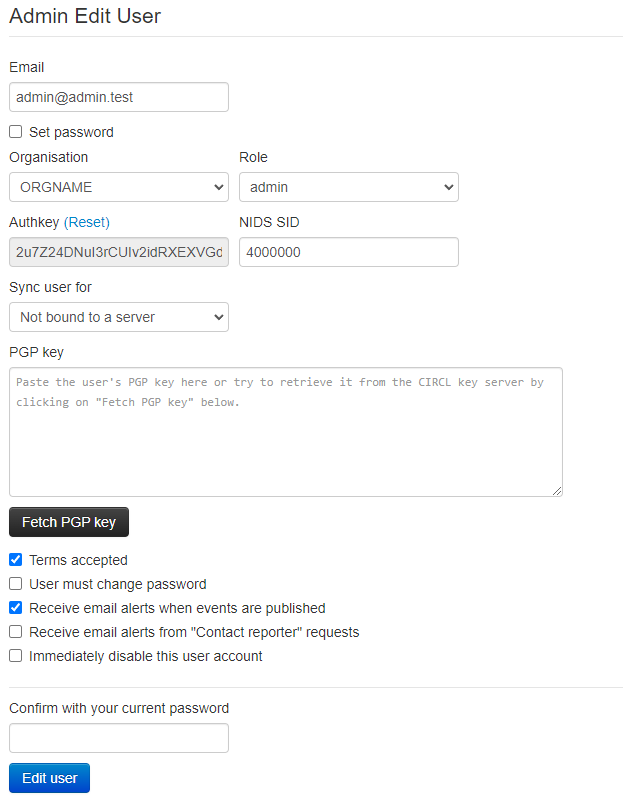


Рисунок 3.7 - Редагування профілю користувача

Адміністратори сайту можуть використовувати функцію «Зв'язатися з користувачами», щоб надіслати всім або окремим користувачам електронний лист. Користувачі, які мають набір ключів GnuPG, отримають свою електронну пошту в зашифрованому вигляді. Натиснувши кнопку ліворуч у меню, буде представлена ​​форма, яка дозволить вказати тип електронного листа, кому воно має надходити та який вміст, за допомогою вказаних параметрів.

Під час впровадження платформи у коледжі, було створено ще профілі двох користувачів (крім основного профілю адміністратора). Це дозволило розподілити обов’язки та роботу між кількома працівниками. Варто зауважити, що доцільніше створити додаткового користувача, ніж повідомляти свої авторизаційні дані стороннім особам.

3.3 Підключення до зовнішніх екземплярів даних

Окрім автономного сховища атак/зловмисного програмного забезпечення, однією з головних особливостей MISP є його здатність підключатися до інших екземплярів і ділитися (частинами) його інформацією. За допомогою використання наступних параметрів з’являється можливість налаштувати та підтримувати з’єднання з зовнішніми серверами, для отримання сторонніх екземплярів даних.

Щоб обмінюватися даними з віддаленим сервером за допомогою відправки та отримування даних, потрібно отримати дійсний ключ автентифікації в організації, яка розміщує віддалений екземпляр.

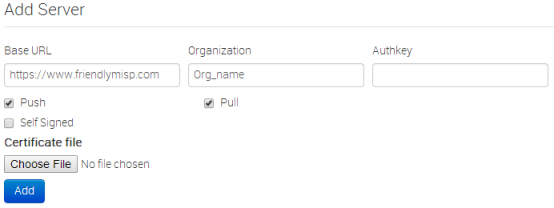


Рисунок 3.8 - Додавання підключення до зовнішнього екземпляру даних

Якщо натиснути «Список серверів», а потім «Новий сервер», з’явиться форма, яку потрібно заповнити, щоб поточний екземпляр підключився до нього. Необхідно заповнити такі поля:

*Базовий URL*: URL-адреса віддаленого сервера.

*Організація*: організація, яка керує віддаленим сервером. Дуже важливо, щоб це налаштування було заповнено точно так само, як назва організації, задана у файлі завантаження віддаленого екземпляра.

*Authkey*: ключ автентифікації, який було отримано від хостингової організації віддаленого екземпляра.

*Push*: цей прапорець визначає, чи дозволено поточному серверу надсилати запити до віддаленого екземпляра.

*Pull*: цей прапорець визначає, чи може ваш сервер запитувати вилучення всіх даних із віддаленого екземпляра.

*Самопідписаний*: установка цього прапорця дозволить синхронізувати з екземплярами, що використовують самопідписані сертифікати.

*Файл сертифіката*: якщо екземпляр, до якого необхідно підключитися, має власний ланцюжок сертифікатів, є можливість використати його для імпорту файлу .pem з ним і замінити стандартний кореневий файл CA CakePHP.

В разі налаштування, як адміністратор установи, дозволу іншому екземпляру підключатися до власного, дуже важливо дотримуватися двох правил під час налаштування облікового запису синхронізації:

1. Користувач синхронізації повинен мати дозвіл на синхронізацію та повні права читання/запису/публікування.
2. І користувач синхронізації, і налаштування організації у файлі Config/bootstrap.php поточного екземпляра повинні відповідати ідентифікатору хостингової організації.

Висновок до третього розділу

Для впровадження в інформаційний простір системи розвідки кіберзагроз було виділено окремий комп’ютер у локальній мережі. Він працює під керівництвом операційної системи Windows 10. Так як розгортання такого осередку є по суті пілотним проектом, було вирішено на початках встановити MISP у віртуальному середовищі. Для його встановлення апаратних потужностей згідно специфікації повинно бути достатньо.

Існує дві типові програми, які зазвичай використовуються користувачами, котрим необхідна технологія віртуалізації. Цими програмами є: VirtualBox та VMware Workstation. Вибір пав на останню, так як вона позиціонує себе, як потужна та максимально надійна.

По завершенні впровадження системи розвідки кіберзагроз MISP у інформаційний простір ВСП «РФК НУБіП України» було розроблено план подальших дій, що включав у себе: підключення нових користувачів, делегування їм розділених повноважень, підключення платформи до зовнішніх екземплярів даних.

Після проведеного аналізу платформи MISP було виявлено, що є ціла низка шляхів для подальшого розвитку додатку в межах навчального закладу.

По-перше планується включити ознайомлення з даною програмою в навчальний процес для унаочнення механізму обміну захищеною інформацією по каналах зв’язку та ознайомлення з базовими принципами захисту від кіберінцидентів.

По-друге, враховуючи впровадження MISP-UA Службою безпеки України ще у 2018 році для забезпечення державно-приватної взаємодії по спільному захисту інформаційного та кіберпростору, є можливість долучитися до обміну інформацією. Адже на платформі MISP-UA вже зареєстровані понад 300 користувачів, серед яких державні і приватні підприємства (в тому числі навчальні заклади).

По-третє, є можливість запускати тематичні хакатони з використанням платформи розвідки кіберзагроз, де б команди зі студентів мали можливість розвиваючи загальне поняття про основні правила з кіберзахисту, вирішувати спільні завдання з підтримки захищеності інформаційного простору.

Використання платформи є доволі зручним. Адже користувач з правами адміністратора, може створювати нові облікові записи для інших користувачів, редагувати профілі користувачів, видаляти їх або просто переглядати профілі всіх користувачів. Це зручно для делегування частини повноважень іншим працівникам. Однак варто пам’ятати, що адміністратори організації (Org Admin) можуть виконувати ці дії виключно в межах користувачів своєї організації.

ВИСНОВКИ

Під час написання самостійної, науково-дослідної роботи було синтезовано підсумок теоретичної та практичної підготовки у рамках нормативної й варіативної складових освітньо-професійної програми підготовки фахівців за спеціальністю «Кібербезпека».

Під час ознайомлення з механізмами розвідки кіберзагроз було досліджено юридичне та програмне підґрунтя даної галузі. Зроблені наступні висновки.

1. Виявлено, що інтерес у плані класифікації кібернетичних втручань і загроз становить схема, запропонована Конвенцією Ради Європи 2001 року й спрямована на боротьбу з кіберзлочинністю.

2. Дослідивши статистичні дані виявлено, що не дивлячись на зростаючу обізнаність та публічний розголос подій та наслідків кібератак, багато компаній дотепер не підготовлені до реальної протидії загрозам.

3. Виявлено, що основою загального плану дій захисту слугують Стратегія єдиного цифрового ринку 2015 р., Кіберстратегія Європейського Союзу 2013 р. та Директива ЄС щодо мережевої та інформаційної безпеки.

4. Виявлено, що поточні зусилля щодо обміну даними розвідки загроз, працюють над централізованою базою даних, куди всі організації-учасники мають завантажувати свої дані про загрози.

Під час розгортання та перших застосувань системи розвідки кіберзагроз було проведено аналіз даної платформи в контексті інформаційного простору ВСП «РФК НУБіП України» визначено наступні твердження.

1. Зроблено висновок, що існує два типи обміну інформацією, кожен з яких визначається тим, хто ділиться інформацією: односпрямований обмін розвідувальними даними про загрози; двонаправлений обмін розвідувальними даними про загрози.

2. Проведено аналіз основних ключових особливостей будь-якої платформи розвідки загроз, таких як здатність аналізувати та обмінюватися даними про загрози.

3. Зроблено висновок, що однією з передових платформ, серед тих, які є у сучасному інформаційному просторі, є MISP. Платформа обміну інформацією про зловмисне програмне забезпечення доступна з різних інтерфейсів, як-от веб-інтерфейс або через ReST API.

4. Проведено аналіз процесу введення події, котрий можна розділити на 3 фази: створення самої події, заповнення її атрибутами та вкладеннями та, нарешті, опублікування.

Для впровадження в інформаційний простір системи розвідки кіберзагроз було виділено окремий комп’ютер у локальній мережі. Він працює під керівництвом операційної системи Windows 10. Так як розгортання такого осередку є по суті пілотним проектом, було вирішено на початках встановити MISP у віртуальному середовищі.

По завершенні впровадження системи розвідки кіберзагроз MISP у інформаційний простір ВСП «РФК НУБіП України» було розроблено план подальших дій, що включав у себе: підключення нових користувачів, делегування їм розділених повноважень, підключення платформи до зовнішніх екземплярів даних.

Після проведеного аналізу платформи MISP було виявлено, що є ціла низка шляхів для подальшого розвитку додатку в межах навчального закладу.

По-перше планується включити ознайомлення з даною програмою в навчальний процес для унаочнення механізму обміну захищеною інформацією по каналах зв’язку та ознайомлення з базовими принципами захисту від кіберінцидентів.

По-друге, є можливість долучитися до обміну інформацією. Адже на платформі MISP-UA вже зареєстровані понад 300 користувачів, серед яких державні і приватні підприємства (в тому числі навчальні заклади).

По-третє, є можливість запускати тематичні хакатони з використанням платформи розвідки кіберзагроз, де б команди зі студентів мали можливість розвиваючи загальне поняття про основні правила з кіберзахисту, вирішувати спільні завдання з підтримки захищеності інформаційного простору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 90% кібератак в Україні пов’язані з РФ і хакерськими групами, які фінансує російська влада – голова Держспецзв’язку [Електронний ресурс]. — Режим доступу: <https://armyinform.com.ua/2021/06/90-kiberatak-v-ukrayini-povyazani-z-rf-i-hakerskymy-grupamy-yaki-finansuye-rosijska-vlada-golova-derzhspeczzvyazku/>
2. Стратегія національної безпеки України : Указ Президента України №287/2015 від 26.05.2015 р. : Режим доступу:  <http://zakon4.rada.gov.ua/laws/show/287/2015>.
3. Дорожня карта Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО ; Режим доступу : http://mfa.gov.ua/mediafiles/sites/nato/files/Roadmap\_Ukr.pdf.
4. 1 ЛИПНЯ - ВОСЬМА РІЧНИЦЯ НАБУТТЯ ЧИННОСТІ ДЛЯ УКРАЇНИ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ [Електронний ресурс]. — Режим доступу: <https://minjust.gov.ua/news/ministry/1-lipnya---vosma-richnitsya-nabuttya-chinnosti-dlya-ukraini-konventsii-pro-kiberzlochinnist-20026>
5. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312-320.
6. pwc, Посилення цифрового середовища проти кібер-загроз, Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік: основні висновки. – 2018. – 22с.
7. Сопілко І. В. Інформаційні загрози та безпека сучасного українського суспільства [Електронний ресурс]. — Режим доступу : http://jrnl.nau.edu.ua/index.php/UV/article/viewFile/8181/9770.
8. Дубов Д. В., Бойко В. О., Гнатюк С. Л., Ісакова Т. О., Ожеван М. А., Покровська А. В., Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України, Аналітична доповідь. – 2018. – 84с.
9. Баровська А. В. Функціональний аналіз сфери стратегічних комунікацій / А. В. Баровська, Д. В. Дубов // Стратегічні пріоритети. — № 4 (41). — 2016. — С. 105—112.
10. Ліпкан В. А. Інкорпорація інформаційного законодавства України : [монографія] /  В. А. Ліпкан, К. П. Череповський ; за заг. ред. В. А. Ліпкана. — К. : О. С. Ліпкан, 2014. — 408 с
11. Методи інтелектуального аналізу даних [Електронний ресурс]. — Режим доступу: <https://buklib.net/books/24506/>
12. Дата майніг [Електронний ресурс]. — Режим доступу: <https://pidru4niki.com/1942111747789/informatika/statistichni_metodi_data_mining>
13. Рудник Л. І. Право на доступ до інформації : дис… канд. юрид. наук : 12.00.07 / Національний університет біоресурсів і природокористування України / Людмила Іванівна Рудник. — К., 2015. — 247 с.
14. Артем Жилін, Микола Худинцев, Максим Літвінов, Функціональна модель ситуаційного центру кіберзахисту, Інформаційні технології та безпека, стаття. – 2018.
15. SECURE DISTRIBUTED-LEARNING ON THREAT INTELLIGENCE, [Електронний ресурс]. — Режим доступу: <https://lds.epfl.ch/secure-distributed-learning-on-threat-intelligence/>
16. Куцаєв В. В., Живило Є. О., Срібний С. П., Черниш Ю.О. Розширення термінології сучасного кіберпростору / Куцаєв В. В., Живило Є. О., Срібний С. П., Черниш Ю. О. [Електронний ресурс]. — Режим доступу:  mino.esrae.ru/pdf/2014/3Sm/1387.doc.
17. David Froelicher, Juan R. Troncoso-Pastoriza, Apostolos Pyrgelis, Sinem Sav, Joao Sa Sousa, Jean-Philippe Bossuat and Jean-Pierre Hubaux, Scalable Privacy-Preserving Distributed Learning, Jul 2021
18. Sharing threat intelligence [Електронний ресурс]. — Режим доступу: <https://www.anomali.com/resources/sharing-threat-intelligence>
19. Сучасні тренди кібербезпекової політики: висновки для України [Електронний ресурс]. — Режим доступу : http://www.niss.gov.ua/articles/294.
20. Top Threat Intelligence Platforms for 2021 [Електронний ресурс]. — Режим доступу: <https://www.esecurityplanet.com/products/threat-intelligence-platforms/>
21. Installation instructions for Ubuntu 18.04.5-server [Електронний ресурс]. — Режим доступу: <https://misp.github.io/MISP/INSTALL.ubuntu1804/>
22. The MISP user guide [Електронний ресурс]. — Режим доступу: <https://www.circl.lu/doc/misp/using-the-system/#templating>
23. Для протидії кіберзагрозам СБУ вводить в дію оновлену версію платформи MISP-UA [Електронний ресурс]. — Режим доступу: <https://ssu.gov.ua/novyny/7800>
24. The MISP user guide [Електронний ресурс]. — Режим доступу: <https://www.circl.lu/doc/misp/using-the-system/#setting-up-a-connection-to-another-server>

Додаток А

MISPvars () {

debug "Setting generic ${LBLUE}MISP${NC} variables shared by all flavours" 2> /dev/null

# Some distros have no openssl installed by default, catch that exception.

$(openssl help 2> /dev/null) || (echo "No openssl, please install to continue"; exit -1)

# Local non-root MISP user

MISP\_USER="${MISP\_USER:-misp}"

MISP\_PASSWORD="${MISP\_PASSWORD:-$(openssl rand -hex 32)}"

# Cheap distribution detector

FLAVOUR="$(. /etc/os-release && echo "$ID"| tr '[:upper:]' '[:lower:]')"

STREAM="$(. /etc/os-release && echo "$NAME"| grep -o -i stream |tr '[:upper:]' '[:lower:]')"

DIST\_VER="$(. /etc/os-release && echo "$VERSION\_ID")"

DISTRI=${FLAVOUR}${DIST\_VER}${STREAM}

# The web server user

# RHEL/CentOS

if [[ -f "/etc/redhat-release" ]]; then

SE\_LINUX=$(sestatus -v -b |grep "^SELinux status"| grep enabled ; echo $?)

WWW\_USER="apache"

SUDO\_WWW="sudo -H -u ${WWW\_USER} "

# Debian flavoured

elif [[ -f "/etc/debian\_version" ]]; then

WWW\_USER="www-data"

SUDO\_WWW="sudo -H -u ${WWW\_USER} "

# OpenBSD

elif [[ "$(uname -s)" == "OpenBSD" ]]; then

WWW\_USER="www"

PATH\_TO\_MISP="${PATH\_TO\_MISP:-/var/www/htdocs/MISP}"

SUDO\_WWW="doas -u www "

SUDO\_CMD="doas "

# NetBSD

elif [[ "$(uname -s)" == "NetBSD" ]]; then

WWW\_USER="www"

PATH\_TO\_MISP="$PATH\_TO\_MISP:-/usr/pkg/share/httpd/htdocs/MISP}"

SUDO\_WWW="sudo -H -u ${WWW\_USER} "

else

# I am feeling lucky

WWW\_USER="www-data"

SUDO\_WWW="sudo -H -u ${WWW\_USER} "

fi

# MISP configuration variables

PATH\_TO\_MISP="${PATH\_TO\_MISP:-/var/www/MISP}"

PATH\_TO\_MISP\_SCRIPTS="${PATH\_TO\_MISP}/app/files/scripts"

## For future use

# TMPDIR="${TMPDIR:-$PATH\_TO\_MISP/app/tmp}"

FQDN="${FQDN:-misp.local}"

MISP\_BASEURL="${MISP\_BASEURL:-""}"

MISP\_LIVE="1"

# Database configuration

DBHOST="${DBHOST:-localhost}"

DBNAME="${DBNAME:-misp}"

DBUSER\_ADMIN="${DBUSER\_ADMIN:-root}"

DBPASSWORD\_ADMIN="${DBPASSWORD\_ADMIN:-$(openssl rand -hex 32)}"

DBUSER\_MISP="${DBUSER\_MISP:-misp}"

DBPASSWORD\_MISP="${DBPASSWORD\_MISP:-$(openssl rand -hex 32)}"

# OpenSSL configuration

OPENSSL\_CN=${FQDN}

OPENSSL\_C="LU"

OPENSSL\_ST="State"

OPENSSL\_L="Location"

OPENSSL\_O="Organization"

OPENSSL\_OU="Organizational Unit"

OPENSSL\_EMAILADDRESS="info@${FQDN}"

# GPG configuration

GPG\_REAL\_NAME="Autogenerated Key"

# On a REAL install, please do not set a comment, see here for why: https://www.debian-administration.org/users/dkg/weblog/97

GPG\_COMMENT="WARNING: MISP AutoGenerated Key consider this Key VOID!"

GPG\_EMAIL\_ADDRESS="admin@admin.test"

# 3072 bits used as per suggestions here: https://riseup.net/en/security/message-security/openpgp/best-practices

GPG\_KEY\_LENGTH="3072"

GPG\_PASSPHRASE="$(openssl rand -hex 32)"

# debug alias to make sure people are not confused when blindly copy pasting blobs of code

alias debug="echo -e"

# checkAptLock alias to make sure people are not confused when blindly copy pasting blobs of code

alias checkAptLock="echo 'Function used in Installer to make sure apt is not locked'"

# php.ini configuration

upload\_max\_filesize="50M"

post\_max\_size="50M"

max\_execution\_time="300"

memory\_limit="2048M"

session0sid\_length="32"

session0use\_strict\_mode="1"

CAKE="${PATH\_TO\_MISP}/app/Console/cake"

# sudo config to run $LUSER commands

if [[ "$(groups ${MISP\_USER} |grep -o 'staff')" == "staff" ]]; then

SUDO\_CMD="sudo -H -u ${MISP\_USER} -g staff"

else

SUDO\_CMD="sudo -H -u ${MISP\_USER}"

fi

echo "The following DB Passwords were generated..."

echo "Admin (${DBUSER\_ADMIN}) DB Password: ${DBPASSWORD\_ADMIN}"

echo "User (${DBUSER\_MISP}) DB Password: ${DBPASSWORD\_MISP}"

}

Запуск скрипта для встановлення LAMP і залежностей:

installCoreDeps () {

debug "Installing core dependencies"

# Install the dependencies: (some might already be installed)

sudo apt-get install curl gcc git gpg-agent make python python3 openssl redis-server sudo vim zip unzip virtualenv libfuzzy-dev sqlite3 moreutils -qy

# Install MariaDB (a MySQL fork/alternative)

sudo apt-get install mariadb-client mariadb-server -qy

# Install Apache2

sudo apt-get install apache2 apache2-doc apache2-utils -qy

# install Mitre's STIX and its dependencies by running the following commands:

sudo apt-get install python3-dev python3-pip libxml2-dev libxslt1-dev zlib1g-dev python-setuptools -qy

}

# <snippet-end 0\_installCoreDeps.sh>

# <snippet-begin 0\_upgradePhp74.sh>

upgradeToPHP74 () {

sudo apt install software-properties-common -qy

sudo add-apt-repository ppa:ondrej/php -y

sudo apt update

sudo apt dist-upgrade -y

}

# <snippet-end 0\_upgradePhp74.sh>

# <snippet-begin 0\_installDepsPhp74.sh>

# Install Php 7.4 dependencies

installDepsPhp74 () {

debug "Installing PHP 7.4 dependencies"

PHP\_ETC\_BASE=/etc/php/7.4

PHP\_INI=${PHP\_ETC\_BASE}/apache2/php.ini

checkAptLock

sudo apt install -qy \

libapache2-mod-php7.4 \

php7.4 php7.4-cli \

php7.4-dev \

php7.4-json php7.4-xml php7.4-mysql php7.4-opcache php7.4-readline php7.4-mbstring php7.4-zip \

php7.4-redis php7.4-gnupg \

php7.4-intl php7.4-bcmath \

php7.4-gd

for key in upload\_max\_filesize post\_max\_size max\_execution\_time max\_input\_time memory\_limit

do

sudo sed -i "s/^\($key\).\*/\1 = $(eval echo \${$key})/" $PHP\_INI

done

sudo sed -i "s/^\(session.sid\_length\).\*/\1 = $(eval echo \${session0sid\_length})/" $PHP\_INI

sudo sed -i "s/^\(session.use\_strict\_mode\).\*/\1 = $(eval echo \${session0use\_strict\_mode})/" $PHP\_INI

}

Інтеграція коду MISP:

installCore () {

debug "Installing ${LBLUE}MISP${NC} core"

# Download MISP using git in the /var/www/ directory.

if [[ ! -d ${PATH\_TO\_MISP} ]]; then

sudo mkdir ${PATH\_TO\_MISP}

sudo chown ${WWW\_USER}:${WWW\_USER} ${PATH\_TO\_MISP}

false; while [[ $? -ne 0 ]]; do checkAptLock; ${SUDO\_WWW} git clone https://github.com/MISP/MISP.git ${PATH\_TO\_MISP}; done

false; while [[ $? -ne 0 ]]; do checkAptLock; ${SUDO\_WWW} git -C ${PATH\_TO\_MISP} submodule update --progress --init --recursive; done

# Make git ignore filesystem permission differences for submodules

${SUDO\_WWW} git -C ${PATH\_TO\_MISP} submodule foreach --recursive git config core.filemode false

# Make git ignore filesystem permission differences

${SUDO\_WWW} git -C ${PATH\_TO\_MISP} config core.filemode false

# Create a python3 virtualenv

${SUDO\_WWW} virtualenv -p python3 ${PATH\_TO\_MISP}/venv

# make pip happy

sudo mkdir /var/www/.cache/

sudo chown ${WWW\_USER}:${WWW\_USER} /var/www/.cache

# install python-stix dependencies

${SUDO\_WWW} ${PATH\_TO\_MISP}/venv/bin/pip install ordered-set python-dateutil six weakrefmethod

debug "Install misp-stix"

${SUDO\_WWW} ${PATH\_TO\_MISP}/venv/bin/pip install ${PATH\_TO\_MISP}/app/files/scripts/misp-stix

debug "Install PyMISP"

${SUDO\_WWW} ${PATH\_TO\_MISP}/venv/bin/pip install ${PATH\_TO\_MISP}/PyMISP

# FIXME: Remove libfaup etc once the egg has the library baked-in

sudo apt-get install cmake libcaca-dev liblua5.3-dev -y

cd /tmp

false; while [[ $? -ne 0 ]]; do [[ ! -d "faup" ]] && ${SUDO\_CMD} git clone https://github.com/stricaud/faup.git faup; done

false; while [[ $? -ne 0 ]]; do [[ ! -d "gtcaca" ]] && ${SUDO\_CMD} git clone https://github.com/stricaud/gtcaca.git gtcaca; done

sudo chown -R ${MISP\_USER}:${MISP\_USER} faup gtcaca

cd gtcaca

${SUDO\_CMD} mkdir -p build

cd build

${SUDO\_CMD} cmake .. && ${SUDO\_CMD} make

sudo make install

cd ../../faup

${SUDO\_CMD} mkdir -p build

cd build

${SUDO\_CMD} cmake .. && ${SUDO\_CMD} make

sudo make install

sudo ldconfig

# install pydeep

false; while [[ $? -ne 0 ]]; do checkAptLock; ${SUDO\_WWW} ${PATH\_TO\_MISP}/venv/bin/pip install git+https://github.com/kbandla/pydeep.git; done

# install lief

${SUDO\_WWW} ${PATH\_TO\_MISP}/venv/bin/pip install lief

# install zmq needed by mispzmq

${SUDO\_WWW} ${PATH\_TO\_MISP}/venv/bin/pip install zmq redis

# install python-magic

${SUDO\_WWW} ${PATH\_TO\_MISP}/venv/bin/pip install python-magic

# install plyara

${SUDO\_WWW} ${PATH\_TO\_MISP}/venv/bin/pip install plyara

else

debug "Trying to git pull existing install"

${SUDO\_WWW} git pull -C ${PATH\_TO\_MISP}

false; while [[ $? -ne 0 ]]; do ${SUDO\_WWW} git -C ${PATH\_TO\_MISP} submodule update --progress --init --recursive; done

${SUDO\_WWW} ${PATH\_TO\_MISP}/venv/bin/pip install -U setuptools pip lief zmq redis python-magic plyara

${SUDO\_WWW} ${PATH\_TO\_MISP}/venv/bin/pip install -U ${PATH\_TO\_MISP}/PyMISP

false; while [[ $? -ne 0 ]]; do checkAptLock; ${SUDO\_WWW} ${PATH\_TO\_MISP}/venv/bin/pip install -U git+https://github.com/kbandla/pydeep.git; done

fi

}

Налаштування відповідних дозволів:

permissions () {

debug "Setting permissions"

sudo chown -R ${WWW\_USER}:${WWW\_USER} ${PATH\_TO\_MISP}

sudo chmod -R 750 ${PATH\_TO\_MISP}

sudo chmod -R g+ws ${PATH\_TO\_MISP}/app/tmp

sudo chmod -R g+ws ${PATH\_TO\_MISP}/app/files

sudo chmod -R g+ws ${PATH\_TO\_MISP}/app/files/scripts/tmp

}

Створення бази даних та користувача для неї. На даному етапі важливо не забути після створення імпортувати пусті записи.

prepareDB () {

if sudo test ! -e "/var/lib/mysql/mysql/"; then

#Make sure initial tables are created in MySQL

debug "Install mysql tables"

sudo mysql\_install\_db --user=mysql --basedir=/usr --datadir=/var/lib/mysql

sudo service mysql start

fi

if sudo test ! -e "/var/lib/mysql/misp/"; then

debug "Start mysql"

sudo service mysql start

debug "Setting up database"

# Kill the anonymous users

sudo mysql -h $DBHOST -e "DROP USER IF EXISTS ''@'localhost'"

# Because our hostname varies we'll use some Bash magic here.

sudo mysql -h $DBHOST -e "DROP USER IF EXISTS ''@'$(hostname)'"

# Kill off the demo database

sudo mysql -h $DBHOST -e "DROP DATABASE IF EXISTS test"

# No root remote logins

sudo mysql -h $DBHOST -e "DELETE FROM mysql.user WHERE User='root' AND Host NOT IN ('localhost', '127.0.0.1', '::1')"

# Make sure that NOBODY can access the server without a password

sudo mysqladmin -h $DBHOST -u "${DBUSER\_ADMIN}" password "${DBPASSWORD\_ADMIN}"

# Make our changes take effect

sudo mysql -h $DBHOST -e "FLUSH PRIVILEGES"

sudo mysql -h $DBHOST -u "${DBUSER\_ADMIN}" -p"${DBPASSWORD\_ADMIN}" -e "CREATE DATABASE ${DBNAME};"

sudo mysql -h $DBHOST -u "${DBUSER\_ADMIN}" -p"${DBPASSWORD\_ADMIN}" -e "CREATE USER '${DBUSER\_MISP}'@'localhost' IDENTIFIED BY '${DBPASSWORD\_MISP}';"

sudo mysql -h $DBHOST -u "${DBUSER\_ADMIN}" -p"${DBPASSWORD\_ADMIN}" -e "GRANT USAGE ON \*.\* to '${DBUSER\_MISP}'@'localhost';"

sudo mysql -h $DBHOST -u "${DBUSER\_ADMIN}" -p"${DBPASSWORD\_ADMIN}" -e "GRANT ALL PRIVILEGES on ${DBNAME}.\* to '${DBUSER\_MISP}'@'localhost';"

sudo mysql -h $DBHOST -u "${DBUSER\_ADMIN}" -p"${DBPASSWORD\_ADMIN}" -e "FLUSH PRIVILEGES;"

# Import the empty MISP database from MYSQL.sql

${SUDO\_WWW} cat ${PATH\_TO\_MISP}/INSTALL/MYSQL.sql | mysql -h $DBHOST -u "${DBUSER\_MISP}" -p"${DBPASSWORD\_MISP}" ${DBNAME}

fi

}

Передостаннім етапом є конфігурація Apache-серверу:

apacheConfig () {

debug "Generating Apache config, if this hangs, make sure you have enough entropy (install: haveged or wait)"

sudo cp ${PATH\_TO\_MISP}/INSTALL/apache.24.misp.ssl /etc/apache2/sites-available/misp-ssl.conf

if [[ ! -z ${MISP\_BASEURL} ]] && [[ "$(echo $MISP\_BASEURL|cut -f 1 -d :)" == "http" || "$(echo $MISP\_BASEURL|cut -f 1 -d :)" == "https" ]]; then

echo "Potentially replacing misp.local with $MISP\_BASEURL in misp-ssl.conf"

fi

# If a valid SSL certificate is not already created for the server,

# create a self-signed certificate:

sudo openssl req -newkey rsa:4096 -days 365 -nodes -x509 \

-subj "/C=${OPENSSL\_C}/ST=${OPENSSL\_ST}/L=${OPENSSL\_L}/O=${OPENSSL\_O}/OU=${OPENSSL\_OU}/CN=${OPENSSL\_CN}/emailAddress=${OPENSSL\_EMAILADDRESS}" \

-keyout /etc/ssl/private/misp.local.key -out /etc/ssl/private/misp.local.crt

# Enable modules, settings, and default of SSL in Apache

sudo a2dismod status

sudo a2enmod ssl

sudo a2enmod rewrite

sudo a2enmod headers

sudo a2dissite 000-default

sudo a2ensite default-ssl

# Apply all changes

sudo systemctl restart apache2

# activate new vhost

sudo a2dissite default-ssl

sudo a2ensite misp-ssl

# Restart apache

sudo systemctl restart apache2

}

Та нарешті останнім етапом є безпосередньо конфігурація MISP:

configMISP () {

debug "Generating ${LBLUE}MISP${NC} config files"

# There are 4 sample configuration files in ${PATH\_TO\_MISP}/app/Config that need to be copied

${SUDO\_WWW} cp -a ${PATH\_TO\_MISP}/app/Config/bootstrap.default.php ${PATH\_TO\_MISP}/app/Config/bootstrap.php

${SUDO\_WWW} cp -a ${PATH\_TO\_MISP}/app/Config/database.default.php ${PATH\_TO\_MISP}/app/Config/database.php

${SUDO\_WWW} cp -a ${PATH\_TO\_MISP}/app/Config/core.default.php ${PATH\_TO\_MISP}/app/Config/core.php

${SUDO\_WWW} cp -a ${PATH\_TO\_MISP}/app/Config/config.default.php ${PATH\_TO\_MISP}/app/Config/config.php

echo "<?php

class DATABASE\_CONFIG {

public \$default = array(

'datasource' => 'Database/Mysql',

//'datasource' => 'Database/Postgres',

'persistent' => false,

'host' => '$DBHOST',

'login' => '$DBUSER\_MISP',

'port' => 3306, // MySQL & MariaDB

//'port' => 5432, // PostgreSQL

'password' => '$DBPASSWORD\_MISP',

'database' => '$DBNAME',

'prefix' => '',

'encoding' => 'utf8',

);

}" | ${SUDO\_WWW} tee ${PATH\_TO\_MISP}/app/Config/database.php

# Important! Change the salt key in ${PATH\_TO\_MISP}/app/Config/config.php

# The salt key must be a string at least 32 bytes long.

# The admin user account will be generated on the first login, make sure that the salt is changed before you create that user

# If you forget to do this step, and you are still dealing with a fresh installation, just alter the salt,

# delete the user from mysql and log in again using the default admin credentials (admin@admin.test / admin)

# and make sure the file permissions are still OK

sudo chown -R ${WWW\_USER}:${WWW\_USER} ${PATH\_TO\_MISP}/app/Config

sudo chmod -R 750 ${PATH\_TO\_MISP}/app/Config

Додаток Б



