Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)
Кафедра Безпеки інформаційних технологій
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Організація оперативного управління кібербезпекою на підприємстві
(тема)

Виконав: Демидов О. Д.
(прізвище, ініціали)
студент 2 курсу, групи БДІРм-18-1
Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва освітньої програми)

Керівник Зав. кафедри Халімов Г.З.
(посада. прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові Демидову Олексію Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Організація оперативного управління кібербезпекою на підприємстві
затверджена наказом по університету від 04 листопада 2019 р. № 1648Ст
2. Термін подання студентом роботи до екзаменаційної комісії ____ _____ 20__ р.
3. Вихідні дані до роботи Теоретичні дані про системи SIEM для SOC центрів для підприємств
4. Перелік питань, що потрібно опрацювати в роботі аналіз архітектури і функцій SOC, аналіз факторів які впливають на вибір рішення, реагування на інциденти на підприємстві; збір доказів.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5. включається до завдання за рішенням випускової кафедри)
Презентаційний матеріал у вигляді слайдів

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	09.09.18	
2	Пошук літератури	10.09.18-07.02.19	
3	Аналіз зібраних даних	08.02.19-19.04.19	
4	Аналіз факторів які впливають на вибір рішення	20.04.19-15.05.19	
5	Розробка процесів розслідування інцидентів SOC	16.05.19-18.08.19	
6	Оформлення пояснювальної записки	19.08.19-31.10.19	

Дата видачі завдання _____ _____20__ р.

Студент ___
(підпис)

Керівник роботи _____ Зав. каф. Халімов Г.З.__
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 79 с., 4 табл., 56 рис., 16 джерел.

Об'єктом дослідження дипломної роботи є: розслідування інцидентів кібербезпеки на підприємстві.

Мета дипломної роботи: аналіз моделей та методів побудови розслідування інцидентів кібербезпеки на підприємстві, та розробка процесу розслідувань різного типу інцидентів у Security Operation Center на підприємстві.

В основній частині аналізується фактори, що сприяють вибору моделей та характеристик Security Operation Center. Були розроблені рекомендації щодо вибору моделі центру для підприємства.

Також проаналізовані різні компанії, які надають SIEM [5] - продукти для корпоративного використання та їх порівняльні характеристики.

Практична цінність полягає у розробці процусів розслідувань різного типу інцидентів. Результати дослідження можуть бути застосовані на українських підприємствах.

Наукова новизна полягає в альтернативній моделі та архітектурі Security Operation Center для різних типів підприємств та новітніх технологіях для забезпечення кібербезпеки.

Ключові слова: *Security Operation Center, SOC, SIEM.*

РЕФЕРАТ

Пояснительная записка 79 с., 4 табл., 56 рис., 16 источников.

Объектом исследования дипломной работы являются: расследование инцидентов кибербезопасности на предприятии.

Цель дипломной работы: анализ моделей и методов построения расследования инцидентов кибербезопасности на предприятии, и разработка процессов расследований разного типа инцидентов в Security Operation Center на предприятии.

В основной части анализируются факторы, способствующие выбору моделей и характеристик Security Operation Center. Были разработаны рекомендации по выбору модели центра для предприятия.

Также проанализированы различные компании, которые предоставляют SIEM [5] - продукты для корпоративного использования и их сравнительные характеристики.

Практическая ценность заключается в разработке процессов расследований разного типа инцидентов. Результаты исследования могут быть применены на украинских предприятиях.

Научная новизна заключается в альтернативной модели и архитектуре Security Operation Center для различных типов предприятий и новейших технологиях для обеспечения кибербезопасности.

Ключевые слова: *Security Operation Center, SOC, SIEM.*

ABSTRACT

Explanatory note: 79 p., 4 tables, 56 figures, 16 sources.

The object of research of the thesis is: investigation of cyber security incidents at the enterprise.

The purpose of the diploma work: analysis of models and methods of construction of investigation of cyber security incidents in the enterprise, and development of structure of investigations of different types of incidents in the Security Operation Center in the enterprise.

The main part analyzes the factors that contribute to the selection of models and characteristics of the Security Operation Center. Recommendations have been developed to select the center model for the enterprise.

Various companies providing SIEM [5] corporate products and their comparative characteristics are also analyzed.

The practical value lies in developing a process of investigations into different types of incidents. The results of the study can be applied at Ukrainian enterprises. The scientific novelty lies in the alternative model and architecture of the Security Operation Center for various types of businesses and the latest cyber security technologies.

Keywords: *Security Operation Center, SOC, SIEM.*

ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ

SIEM – Security information and event management [5];

SOC – Security operations center;

CERT – computer emergency response team [6];

DLP – Data loss prevention;

OAS – On-Access Scan;

ODS – On-Demand Scan;

MAV – Mail Anti-Virus;

WAV – Web Anti-Virus;

IDS – Intrusion Detection Scan;

VUL – Vulnerability Scan;

KAS – Kaspersky Anti-Spam;

BAD – Botnet Activity Detection;

IDS – Intrusion detection system;

NOC – Network operations center;

НСД – несанкціонований доступ;

ПЗ – програмне забезпечення;

АС – автоматизована система [13];

ІБ – інформаційна безпека;

ІС – інформаційна система;

ІТ – інформаційні технології;

КС – комп’ютерна система;

НД – нормативний документ.

ЗМІСТ

ВСТУП

В Україні за останні роки збільшилася кількість кібер-атак в корпоративному секторі так і державному, а самі хакери вже не працюють поодинці, як 20 років тому, а працюють у великих або не великих групах добре організованих як технічним оснащенням так і величезними багатомільйонними вкладеннями коштів з боку держав або коштів які були отримані незаконним шляхом [17].

Висока інтенсивність кібератак по всій Україні статистика приведена за 2019 рік (рисунок 1).

Рисунок 1 - Статистика кібер-атак на Україну за 2019 рік

OAS (On-Access Scan) - автоматична перевірка. Показує потік даних в шкідливих програмах, виявлених під час відкриття, копіювання, запуску або збереження файлів.

ODS (On Demand Scan) - Перевірка на вимогу показує потік даних в шкідливих програмах, що виникає, коли користувач вручну вибирає "Просканувати комп'ютер" в меню.

MAV (Mail Anti-Virus) - Поштовий антивірус показує потік даних в шкідливих програмах, виявлених серед нових об'єктів в поштових додатках. Поштовий антивірус перевіряє вхідні повідомлення і запускає автоматичну перевірку при збереженні завантажених файлів на диск.

WAV (Web Anti-Virus) - Веб-антивірус показує потік даних в шкідливих програмах, виявлених при відкритті HTML-сторінок веб-сайтів, а також при завантаженні файлів. Веб-антивірус перевіряє порти, зазначені в його налаштуваннях.

IDS (Intrusion Detection Scan) - Система виявлення вторгнень показує потік даних в виявлених мережевих атак.

VUL (Vulnerability Scan) - Пошук вразливостей показує потік даних по виявленим вразливостям.

KAS (Kaspersky Anti-Spam) - Касперський Анти-Спам показує підозрілий і небажаний поштовий трафік, виявлений за допомогою технологій репутаційної фільтрації «Лабораторії Касперського».

BAD (Botnet Activity Detection) - Моніторинг активності ботнетів показує статистику по виявленим IP-адресами жертв DDoS-атак і IP-адресами командних серверів ботнетів. Статистика збирається за допомогою системи DDoS Intelligence, що входить до складу рішення Kaspersky DDoS Prevention.

При цьому в корпоративному секторі працюють фахівці з кібербезпеки, а в державному секторі працює кіберполіція, СБУ ДКІБ, які мають в своєму арсеналі програмно-технічні комплекси в області захисту інформації (DLP, SIEM, IDS / IPS, WAF / FW, EDR). При всій організації захисту інформації в Україні, все одно відбуваються кібер-атаки з великим збитком державі.

Фахівці в сфері кібербезпеки давно усвідомили, то що необхідно створити єдиний централізованого комплексного вирішення в сфері реагування на кібератак і інших інцидентів які пов'язані з інформацією та можливістю розслідування інцидентів. Основним рішенням є створення центру моніторингу та оперативного реагування кібератак, який допоможе уникнути кібератак, але і протистояти атакам в режимі реального часу, а так же розслідувати їх після. Для забезпечення цілісного і комплексного підходу моніторингу і реагування на кібератаки, згідно з усіма стандартами що регулює кібербезпеку, наприклад ISO IEC 27035, ISO IEC 27001 [7]. SOC об'єднує всі дані технології, а так само процеси і професійні навички співробітників в сфері кібербезпеки, формуючи комплексну систему захисту. Що дозволяє отримати високий ступінь готовності і реагування на інциденти в сфері кібербезпеки, що дозволить уникнути критичних надалі від потенційних кібер-атак, націлених на різні сектори в державі.

Мета роботи: аналіз моделей та методів побудови розслідування інцидентів кібербезпеки на підприємстві, та розробка процесів розслідувань різного типу інцидентів у Security Operation Center на підприємстві.

Для забезпечення кібербезпеки на підприємстві на основі Оперативного центру безпеки (Security Operation Cente) необхідно вирішити наступні частні задачі:

- аналіз архітектури і функцій SOC;
- аналіз факторів які впливають на вибір рішення
- реагування на інциденти на підприємстві;
- збір доказів.

1 АРХІТЕКТУРА І ФУНКЦІЙ SOC

1.1 Реалізації SOC.

SOC [1] (Security Operations Center) - центр, основним завданням якого є консолідація всіх подій з різних систем, проведення конкретних аналізів для попередження інженерів кібербезпеки о подіях на підприємстві. Виходячи з отриманої інформації, інженери з кібербезпеки проводять кібер-розслідування, щоб виключити можливість повторення цієї події, що мінімізує втрати в бізнесі. SOC [1] - це еволюція CERT [6] (Computer Emergency Response Team) – це команди інженерів для реагування на різні та нестандартні ситуації, пов'язані з комп'ютерними технологіями. Ключовою відмінностю від CERT [6] є використання новітніх технологій аналітики для оперативного розуміння поточної ситуації на підприємстві з кібербезпеки.

Security Operation Center (SOC) [1] означає систему, розроблену та побудовану на основі SIEM [5] (Security Information and Event Management), яка призначена для збору та зберігання журналів із пристроїв та додатків для глибокого аналізу та кібер-розслідування інцидентів.

В даний час SOC [1], які створені на базі SIEM, допомагають компаніям вирішувати ключові завдання:

– збирати та зберігати лог-файли в єдиному сховищі;

– визначити активність в мережі підприємства, коли вона перевищує активність, яку вона дозволяє вказати на кібератаку на підприємство;

– виконувати співвідношення [9] подій між джерелами інформації.

Ключовий компонент SOC є SIEM.

SIEM [5] відповідає за виконання наступних завдань:

– зберігання журналів подій з джерел [2];

– аналізу подій та інцидентів;

– розбір подій та інцидентів;

– співвідношення [9] подій за правилами, встановленими інженерами;

– автоматичне повідомлення про інцидент.

Як працює SIEM:

Система збирає, аналізує інформацію, потім додає її до бази даних, потім аналізує поведінку на основі попередніх спостережень. На підприємстві реалізується за допомогою:

– агентів;

– серверів-збирання;

– серверів-баз даних;

– серверів-співвідношення [9].

SIEM [5] використовують основні джерела інформації:

- журнали контролю доступу, та аутентифікації;
- DLP;
- IDS/IPS;
- антивірусні програми;
- журнали подій;
- брандмауери;
- сканери вразливостей;
- Asset-management;
- системи веб-фільтрації;

Протоколи та інтерфейси для збору подій:

- Socket Unix;
- Plain log;
- SSH;
- Rsync;

– Samba;
– FTP, SFTP;
– NFS;
– SDEE, RDEP;
– OPSEC, CPMI;
– Syslog and Syslog-ng;
– SNMPv2 and SNMPv3[14];
– Opsec;
– HTTP, HTTPS;
– SQL, ODBC.

Після отримання інформації SIEM [5] може проаналізувати її. Для аналізу застосовується математичні та статистичні алгоритми обробки інформації. В SIEM [5] правила в форматі RBR (Rule Based Reasoning) які містять набір тригерів, лічильники, та сценаріїв всіх виконаних дій.

Основні етапи впровадження SIEM:

– аналіз інфраструктури та вибір впровадження;
– створення та підтвердження технічного завдання;
– створення керівництва адміністраторів;
– встановлення та налаштування серверу SIEM;
– налаштування агентів та встановлення;
– розробка правил реагування на різні події;
– проведення тестової експлуатації;
– налагодити та записати нові правила для належного функціонування системи;
– завершення тестового періоду та впровадження.

Впровадження SIEM [5] від 4 місяців після проведення тестового періоду.

Основних представників SIEM [5] – рішень:

– HP (ArcSight) [10];

– IBM [11] (Qradar);
– Splunk.

1.2 Задачі SOC.

Основні вимоги до корпоративного захисту інформації:

– зниження ризиків;
– запобігання загрозам;
– захист від перевантаження;
– відповідальність за процес;
– ескалація проблем;
– аудит;
– реагування на інциденти;
– збір доказів.

Ситуаційний центр – це складне організаційно-технічне рішення, яке дозволяє:

– автоматичне виявляння подій;
– забезпечити тривале зберігання всього зібраного обсягу подій;
– впровадити процес вирішення виявлених інцидентів.

Основні процеси Security Operations Center (рисунок 1.1)

Рисунок. 1.1 - Основні процеси SOC.

Все залежить від параметрів технічних установок та кваліфікованих інженерів які обслуговують підприємство.

Впроваджуючи SOC, на підприємстві впроваджуються процеси управління системою відповідно до стандартів ISO 27001, та ISO 27037 [8].

Таким чином, SOC [1] - це сукупність пов'язаних процесів управління, які автоматизують [13] їх технічні системи:

- моніторинг подій захисту інформації;
- контролювати стан інформаційної безпеки;
- аудит користувачів;
- управління вразливостями;
- управління інцидентами інформаційної безпеки;
- контроль за дотриманням законодавчих вимог;
- інвентаризація;
- консолідація інформації про випадки інформаційної безпеки;
- координація та автоматизація [13] реагування на інциденти;
- інтеграція та отримання даних із зовнішніх джерел.

Моніторинг інформаційної безпеки - це елемент управління ризиками [12] інформаційної безпеки який змінює інформаційне середовище підприємства.

Завданнями моніторингу інформаційної безпеки є швидкий та постійний моніторинг, збір, аналіз та обробка даних, а також надання повної, своєчасної, достовірної інформації для прийняття обґрунтованих рішень у сфері інформаційної безпеки.

Процеси моніторингу інформаційної безпеки в процесі управління такі:

- досліджувати, слідкувати, спостерігати, накопичувати, організувати, оцінювати інформацію;
- прогнозувати стан та якість усіх бізнес-об'єктів та процесів.

Система аудиту дій користувача записує та аналізує всі дій користувача в режимі реального часу.

Система аудиту дій користувачів вирішує завдання:

- моніторинг шкідливих дій;
- контролювати витік конфіденційної інформації;
- підготовка звітів.

Рішення Symantec DLP, яке легко інтегрується з іншими продуктами Symantec, можна використовувати для контролю дій користувачів.

Система управління вразливостями дозволяє отримувати дані за наявними вразливостями в режимі реального часу по всьому підприємстві, та відстежувати динаміку їх усунення, дозволяючи стежити за змінами.

Уразливості критичних ресурсів постійно шукаються різними способами:

- мережеве сканування;
- пен-тест на проникнення;
- перевірки системи;
- аналіз безпеки СУБД;
- аналіз безпеки веб-додатків.

Рішення Qualys Scanner, яке може бути легко інтегровано з іншими продуктами та інтеграторами, може бути використане для виявлення вразливості критичних ресурсів користувачів.

Інвентаризація та контроль інфраструктури:

На основі центрів SOC [1] завдання управління інформаційними активами, такі як:

- моніторинг інфраструктури;
- переліку критичних активів та їх оцінка;
- контроль користувачів;
- управління вразливостями.

Рішення HP Asset Manager легко використовується для інвентаризації та моніторингу інфраструктури користувачів, яка легко інтегрується з іншими продуктами та інтеграторами систем.

В інфраструктурі підприємства контролюється встановлення нових програм, які не мають дозволу на використання, та фіксація підключення нового обладнання. Візуалізація даних представлена у вигляді графіків, діаграм, які дозволяють ефективно аналізувати інфраструктуру.

Якщо в підприємстві відсутній моніторинг, інформація про інциденти не систематизується, що ускладнює процес швидкого реагування на інцидент та швидкого, якісного розслідування. Для цього потрібна єдина база даних для збору інформації про всі інциденти, що сталися в бізнесі.

Робота з управління інцидентами відбувається:

- виявлення випадків;
- реагування на інциденти;
- розслідування інциденту;
- аналіз і статистика інцидентів;
- звіт про виконану роботу.

Інформація про випадки є централізованій базі даних. Параметри інциденту реєструються: рівні критичності, рівні пошкоджень, джерело інциденту, ступінь навмисності, статус досягнення, ймовірність повторення, пріоритетність тощо.

Автоматизація [13] реакції на інцидент:

Важливо автоматизувати [13] процеси реагування на інциденти, щоб інженерам не довелося починати все с початку. У SOC, існують конструктори, за допомогою яких, можна визначити та задати правила збору інформації про інциденти відповідно до конкретних критеріїв, які роблять їх доступними, автоматично призначаються особи які відповідальні за розслідування інциденту.

Команда реагування на інциденти організована в SOC, обов'язки всіх інженерів визначені в процедурах та документах SOC, формуються звіти про реагування на інциденти та розслідування.

Інтеграція із зовнішніми продуктами, та обмін інформацією, що стосується інцидентів SOC. Це можуть бути повідомлення від - SIEM, DLP, антивіруси, сканери вразливості тощо. Автоматизація [13] реакції на інциденти (рисунок 1.2).

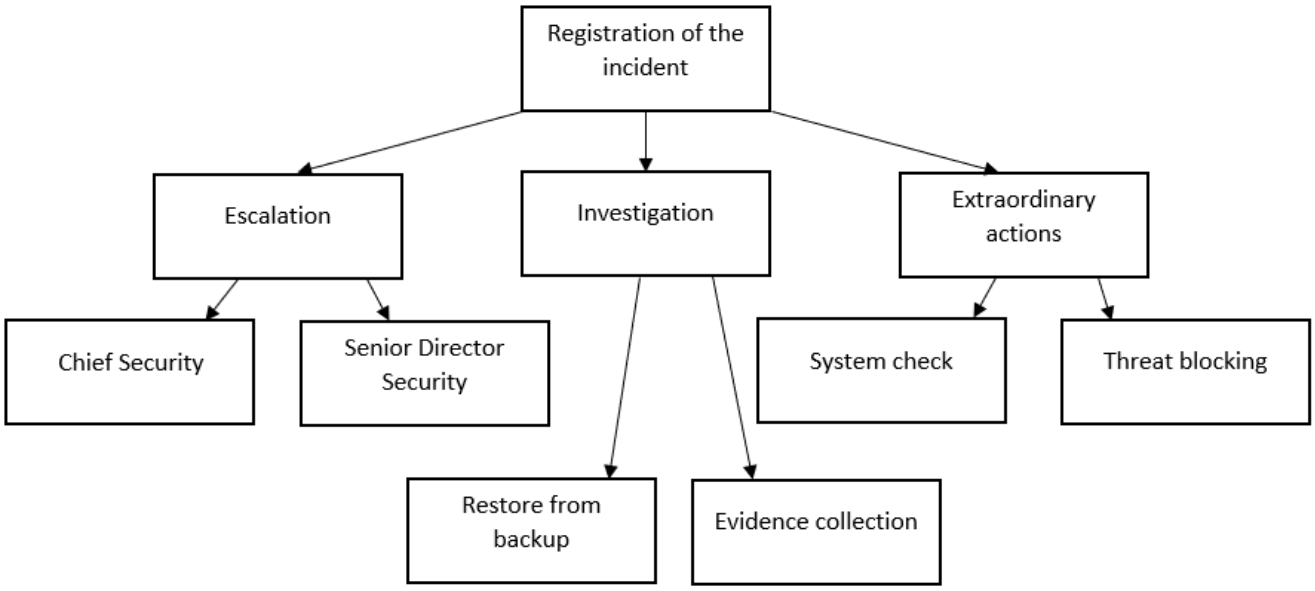


Рисунок. 1.2 - Автоматизація реакції на інцидент.

Повідомлення також надходять із зовнішніх джерел через API або сповіщення електронною поштою. Головне, щоб вони працювали за певними правилами, заснованими, наприклад, на регулярних виразах або тегах.

1.3 Аналіз моделей SOC.

Основні моделі SOC:

- Enterprise SOC;
- SOC-as-a-service;
- Hybrid SOC.

Порівнюється за такими показниками:

– технічне обладнання;
– розміщення технічного обладнання;
– структура витрат.
– розміщення персоналу;
– рівень зрілості.

У (див. табл. 1.1) порівнюється місце розміщення технічного оснащення.

Таблиця 1.1 - Порівняння місця розміщення технічного оснащення

	Enterprise SOC	**SOC-as-a-service**	**Hybrid SOC**
Equipment SIEM	E	I	E
Technical support	E	I	I
Servers to collect data	E	E	E
Servers storage data	E	I	I
Backup servers	E	I	I
SIEM, Service Desk	E	I	E

E - на підприємстві I - у інтегратора

Персонал SOC:

– Security Systems Engineer, обслуговує SIEM;
  Мінімальна кількість: 4
– SOC-Team реагування на інциденти і їх ескалацію;
  Мінімальна кількість 24x7: 7
– Digital forensic expert та Security analytic які проводить розслідування.
  Мінімальна кількість: 2

– Chief SOC

Мінімальна кількість: 1

У (див. табл. 1.2) надведене порівнюється місце розміщення пернсоналу.

Таблиця 1.2 - Порівняння розміщення персоналу

	Enterprise SOC	**SOC-as-a-service**	**Hybrid SOC**
Chief SOC	E	I	E/I
Security Systems Engineer	E	E	E
SOC-Team	E	E	O
Digital forensic expert, Security analytic	E	E/I	E/I

E - на підприємстві I - у інтегратора

Стандарт Cobit [16] розрізняє рівні зрілості IT просеців :

5 - оптимізований рівень

– характеризує рівень управління інформаційною безпекою на рівні кращих практик;

– заходи безпеки застосовуються на підприємстві;

– підприємство здатна до швидко адаптуватися до змін навколишнього середовища.

4 - керований рівень

– моніторинг та оцінка відповідності процесів, що використовуються на підприємстві;

– оптимізація забезпечується при виявленні низької ефективності впроваджених процесів управління;

– процеси управління постійно вдосконалюються і базуються на передовій практиці;

– частково використовуються засоби автоматизації [13] та управління в обмеженій мірі.

3 - певний рівень

– процеси стандартизовані, документовані та передаються персоналу через навчання;

– однак порядок використання цих процесів залишається на розсуд самих працівників;

– це визначає ймовірність відхилень від стандартних процедур;

– використовувані процедури не є оптимальними та недостатньо сучасними, але відображають практику, яку використовує підприємство.

2 - повторюваний рівень

– характеризує рівень розвитку процесів управління ІБ на рівні, коли їх виконання забезпечують різні люди, які вирішують одне і те ж завдання;

– однак немає регулярних занять та тренувань за стандартними процедурами, і відповідальність покладається на підрядника;

– керівництво підприємства багато в чому покладається на знання перекладачів.

1 - початковий рівень

– обов'язково документально зафіксовані доповіді, що повідомляють підприємству, які існують;

– використовуйте будь-які суб'єкти менеджменту, не стандартизовані, використовуючи без системно;

– загальний підхід до менеджменту не вироблений.

0 - рівень

– повна відсутність будь-яких процесів менеджменту в діяльності підприємства;

– підприємство не усвідомлює існування проблем.

Ви повинні мати 5-й рівень зрілості, щоб створити свій SOC. SOC [1] – це окремий бізнес-процес, який потім може бути проданий іншій компанії.

Для того щоб використовувати SOC [1] as a service та Hybrid достатньо 3 рівня зрілості, на інтеграторі покладають повну або часткову організацію процесу побудови та обладнання.

Щоб мати власний SOC [1] потрібно мати багато грошей, купувати обладнання, програмне забезпечення, щоб впровадити та підтримувати власну систему, ви повинні тримати штат високооплачуваних інженерів. І витрачати гроші на електроенергію та амортизацію обладнання.

Щоб мати SOC [1] as a service потрібно просто сплатити за підписку на послугу, значно нижчу за повне розгортання власного центру.

Hybrid SOC [1] вимагає витрат на апаратне та програмне забезпечення, але менше, ніж для розгортання центру, а також плата за підписку, але менше, оскільки частина функціональних можливостей та апаратних засобів розмішується на підприємстві.

Переваги та недоліки систем, представлені в порівняльній (див. табл. 1.3).

Таблиця 1.3 - Недоліки та переваги SOC

	Enterprise SOC	**SOC-as-a-Service**	**Hybrid SOC**
Переваги	Власний процес який контролюється самим підприємством	Готовий процес як послуга Порівняно невелика вартість	Порівняно невелика вартість Готовий процес як послуга Можливість розгорнути власний SOC

Недоліки	Висока вартість і складність підприємства, побудови та підтримки	Вихід інформації за рамки підприємства	Вихід інформації за рамки підприємства

У цьому розділі проаналізовано основні типи архітектур SOC, які можуть впливати на вибір конкретної моделі SOC, спираючись на ці данні, можливо розуміти основі складові SOC [1] що може допомогти вам обрати архітектуру, необхідну для різних видів бізнесу. Далі подані рекомендації для підприємства при побудові SOC [1] на підприємстві.

2 РЕКОМЕНДАЦІЇ ДЛЯ ПІДПРИЄМСТВА ПРИ ПОБУДОВІ SOC

2.1 Аналіз факторів які впливають на вибір рішення.

Основні фактори що впливають на вибір архітектури SOC:

1) Складність архітектури системи.

Масштаб системи є основою для планування, тестування, розгортання впровадження та вдосконалення SOC.

Багато залежить від кількості користувачів. Чим більше користувачів, тим більше операцій виконуються однаково і щодня трапляється більше інцидентів.

2) Кваліфікація персоналу.

SOC [1] може працює лише в під керівництвом Chief Security, бувши розмістившись у великому підприємстві, може сформувати команду з 8 працівників, які мають освіту з кібербезпеки. SOC [1] - це інструментом, який вимагає кваліфікованих фахівців, для досягнення результатів.

Вам потрібно бути впевненим, та переконатися чи потрібен вам підприємству SOC. Чи є ресурси та працівники? Чи можливо найняти та навчити нових працівників.

3) Наслідки порушення кібербезпеки на підприємстві.

Основні критерії, що використовуються, для оцінки наслідків, які виникають зі втрати спостережливості, автентичності або надійності активів:

- порушення закону;
- погіршення продуктивності бізнесу;
- втрата репутації;
- порушення особистої інформації;

– порушення конфіденційності;
– фінансова втрата;
– простій бізнесу;
– переривання обслуговування:
– втрата довіри клієнта;
– порушенні умов контракту;
– фінансові втрати;
– обладнання;
– переслідування та санкції;
– матеріальна шкода.

4) Важливим елементом підприємства є бюджет, та скільки коштів підприємство готове витратити на кібербезпеку.

2.2 Рекомендації щодо вибору архітектури та типу SOC.

1) Коли необхідно створити SOC:

– підприємству потрібно збільшити бізнес-процеси та інфраструктуру. Власники бізнес-процесів та інфраструктури, мають бути обізнані про ризики [12], які пов'язані з ризиками кібербезпеки, та їх загрозами бізнесу. Якщо керівництво підприємства звертає особливу увагу в потребі в бізнес-процесів і інфраструктурі, то слід розглянути питання про створення SOC [1] у відповідь на існуючі ризики кібербезпеки.

– підприємство має службу кібербезпеки. Витрати на кібербезпеку призводять до виправдання інвестицій та підвищення ефективності як самих підсистем.

– Процеси кібербезпеки, які потрібно оптимізувати, потребують впровадження нових процесів. Збільшення витрат також може означати, що компаніям потрібно створити SOC.

2) Створення Enterprise SOC.

Створення Enterprise SOC дуже актуальне. Особливо коли підприємство з великою кількістю співробітників яких перевищує п’ятсот осіб. Ці підприємства з офісами в різних містах та країнах.

Висока цінність захищеної інформації, велика кількість різних способів її захисту, територіальна структура, велика кількість працівників, якщо це відноситься до компанії, - це перший крок для створення власного SOC.

Основою будь-якого SOC складають компоненти:

– персонал - інженери, аналітики, директор;

– база - набори співвідношень [9], норми інцидентів, моделі оповіщення, бази знань по різні загрози та векторах атак;

– процеси - процедури аналізу інцидентів, реагування, звітності, ескалації та протидії інцидентів;

– забезпечення - розміщення SOC [1], SIEM, інструментів моніторингу продуктивності, сховищ подій, інцидентів, ліцензії на систему SIEM [5] та додаткових модулів.

В Україні дуже мало професіоналів та інженерів з кібербезпеки. Пошук інженере займає від місяця до року. Потім ще пів року, в залежно від працівника, для повного підключення його в роботу. Якщо підприємству потрібно організувати моніторинг 24x7, то все більше ускладнюється.

Заповнення бази даних SIEM [5] є найважливішим завданням, оскільки базовий набір правил не в змозі закрити всі вектори нападу на підприємство. Інженери зобов’язані підключати джерела та записувати конектори до додатків.

Окрім персоналу та бази, важливо мати чітко встановлені процеси виявлення, аналізу інцидентів, оповіщення відповідальних осіб та встановлення моделей взаємодії між підрозрюваними. Слід передбачити порядок звітування та розслідування кожного виду інциденту, SLA [15], та ескалацію. Інцидентів високої критичності повинні заздалегідь передбачити можливість загрози на

бізнес-процеси, оцінивши ризики [12] наслідків інциденту та порівнявши їх з втратами від тимчасового простою окремих підрозділів.

3) Використання SOC-as-a-service.

Для великого підприємства, яка хочу побудувати Enterprise SOC зі старту, спроба впровадження може зайняти роки, але нічого не вийде. Проблеми в будь-якому з елементів (персонал, база, процеси, забезпечення), може знищити SOC.

Головна суть в тому щоб було бажання бізнесу виділяти гроші на кібербезпеку. Але сам бізнес в цілому не готовий чекати 1 до 3 років, поки його SOC [1] розпочне працювати.

Використовуючи SOC-as-a-service це допоможе знизити ризики [12], дозволяючи запустити моніторинг, надаючи експертизу, команду та базу.

При використанні SOC as a service, ви негайно вирішуєте кадрову проблему, заповнення контентом SIEM, розробки процесів взаємодії при виявленні, аналізі та протидію на інцидентів - всі завдання переходять аутсорсиру. Постачальник послуг враховує специфіку підприємства і внутрішні вимоги.

Підприємство налаштоване на створення Enterprise SOC, в рамках довгого періоду найбільш цікавим варіантом для розгляду є використання Hybrid Security Operations Center, що передбачає використання підприємством SIEM, яку постачальник послуг забирає на адміністрування і опирається на неї контент, оптимізуючи під замовника. Hybrid варіант також вирішує завдання швидкого пошуку команди моніторингу, що дає компанії більше часу на пошук власної команди.

4) Використання Hybrid SOC.

У разі Hybrid SIEM [5] купується за кошти підприємства і розміщується в її інфраструктурі. Вибір правильного рішення є складним питанням, і при вирішенні використовувати Hybrid SOC необхідно враховувати тенденції ринку та думку компанії, яка надає аутсорсингові послуги.

Початкова установка та налаштування рішення можуть бути реалізовані інтегратором доставки та постачальником послуг моніторингу. Другий варіант кращий, адже підключаючи компанію до сервісу з виявлення інцидентів підрядник найчастіше використовує свої конектори, парсери, налаштування SIEM, і при його залученні дозволить виключити подвійну роботу.

Під час періоду надання послуг збором подій та адмініструванням серверів конекторів, як правило, керує аутсорсир, а клієнт має обмежений доступ до консолі SIEM. Цей підхід пов'язаний як з політикою конфіденційності так і з захисту авторського контенту, так і з розподілом обов’язків – SOC [1] компанії, яка відповідає за продуктивність системи, включаючи гроші, тому намагається мінімізувати ризики [12], пов'язані з людськими факторами та нештатним втручанням в роботу ПЗ.

З технічними роботами на SIEM [5] відбувається дослідження інфраструктури, спілкування з власниками підприємства, службою кібербезпеки, та розробка процедури взаємодії всіх при розборі інцидентів. Документи, що розробляється в процесі дослідження, представляють визначений регламент підприємства, який потім може бути використаний клієнтом при старті Enterprise SOC.

Окрім запису та оповіщення про інциденти кібербезпеки, основним процесом є процедура взаємодії з підрозділами для розслідування та протидії інцидентам. Під час надання послуги це дозволяє зрозуміти, як взаємодіяти зі всіма підрозділами підприємства перед запуском Enterprise SOC.

Використанні Hybrid SOC вирішуються деякі проблеми пов’язані з використанням хмарного SOC:

– усі події пов’язані з інформаційною безпекою з систем підприємства залишаються в інфраструктурі;

– коли послуга постачальника SOC відключена, в компанії залишається система збору подій, яку можна використовувати пізніше;

– Hybrid SOC значно нижче навантажує інтернет-канал, чим при хмарному варіанті підключення.

При відключенні від постачальника SOC правила та процедури, можуть використовуватися у внутрішньому SOC, найнявши команду аналітиків та інженерів.

Цей метод знижує ризики [12] поганого початку, та забезпечує моніторинг та розслідування інцидентів тут і зараз, дозволяючи найняти команду та інтегрувати їх у процес, не порушуючи процесів кібербезпеки підприємства.

2.3 Порядок розміщення SOC на підприємстві.

Основі етапи впровадження SOC:

1) Обстеження підприємства.

На цьому етапі досліджується вся інформаційна система підприємства, проводиться аналіз архітектури, визначаються основні функції цієї системи, бізнес-процеси, масштаби системи, які активи для компанії потребують моніторингу і захисту.

Системна шкала є основою для планування розгортання та дозрівання SOC. Це впливає на вибір рішень, архітектурні вимоги, потреби у персоналі та процеси та процедури.

Ви повинні бути готові, що впровадження SOC [1] дуже довгим процесом. На створення бібліотеки перевірених сценаріїв та навичок знадобиться близько року, що дозволить вам ефективно реалізувати та розширювати свій SOC. Рекомендується скористатися багато етапним підходом, який охоплює не тільки початкове розгортання, але й наступні кроки, які охоплюють додаткові сценарії та приєжанти нові джерела даних для їх підтримки. Після цього кроку ми маємо всю системну інформацію, необхідну для вибору програмних продуктів, кількість працівників, які нам потрібні для обладнання, тому наступним кроком є проєктування SIEM.

2) Проєктування системи SIEM.

У цей момент необхідно:

– сформувати проєктну команду, основні обов'язки якої включатимуть визначення цілей, сфери та етапів проєкту, а також визначення кінцевих споживачів;

– визначте цілі для моніторингу подій безпеки та початкову зону розгортання проєкту;

– визначити основні сценарії використання, охоплені SIEM;

– визначити вимоги до збору, зберігання, звітності і моніторингу подій безпеки;

– оцініть кількість джерел даних, необхідні для вибраних сценаріїв (щодо кількості подій в секунду, внутрішнього сховища чи обчислювальної потужності), а потім перевірте, чи доступні ці джерела даних.

Потім зібрана інформація використовується для:

– оцінки середовища і ресурсів;

– оцінки вимог архітектури та методи збору даних, щоб відповісти на наступні запитання: які зусилля будуть потрібні для інтеграції джерел даних та чи підтримують ці джерела журнали безпеки без погіршення продуктивності;

– визначити потенціал джерел даних для генерування очікуваних подій. Деякі джерела журналу можуть бути обмежені через продуктивність, версії програмного забезпечення тощо;

– Розробити моніторинг подій та реагування на інциденти. Зверніть особливу увагу на деталі в (playbooks), після того як ваш SIEM [5] почне створювати інциденти;

– Встановити відповідні процеси та політику з метою оцінки необхідних ресурсів для SIEM.

Після зібраної інформації вибирається необхідне технічне обладнання та програмне забезпечення.

Ми можемо виділити основні джерела даних:

– контроль доступу, аутентифікація користувачів;

– журнали подій серверів і робочих станцій;

– активне мережеве обладнання;

– IDS \ IPS;

– антивірусний захист;

– аналізатори вразливостей;

– інші системи захисту та управління політикою інформаційної безпеки: DLP, управління пристроїв;

– asset-management;

– системи обліку трафіку.

3) Купівля технічного обладнання та ліцензії на програмне забезпечення.

Згідно з проєктом SIEM [5] закуповується необхідне технічне обладнання, та ліцензії на програмне забезпечення, яке необхідне для працездатності системи.

Технічне обладнання - це комп'ютери для спостереження, сервери-зберігання інформації, призначені для попереднього накопичення подій з декількох джерел, сервер-співвідношення [9], відповідальний за збір інформації від колекторів і агентів та обробку за алгоритмами співвідношення [9] та правилами, сервер баз даних та сховища, відповідальним за зберігання журналів подій, та мережевих пристроїв.

4) Знайдіть і наймайте фахівців.

Наразі в Україні немає висококваліфікованих спеціалістів з досвідом роботи у центрах SOC, тому необхідно залучати фахівців за кордону чи провести перекваліфікацію наявний персонал у відділі кібербезпеки.

Мінімальний персонал необхідний для команди SOC такий:

– Chief SOC - 1 фахівець;

– Analytic SOC - 1 фахівець;

– Technical expert -1 фахівець;

– Engineer SIEM -1 фахівець;

– SOC Team - 4 фахівці.

5) Розгортання, підключення джерел подій до SIEM.

Встановлено всі технічні пристрої, програмне забезпечення, та джерела подій.

6) Впровадження SIEM [3], реалізація сценаріїв подій, розробка правил співвідношення [9], звітування.

Ми налаштовуємо фільтри для введення даних SIEM, обладнання, панелі візуалізації тощо.

У сценаріях подій ми розглядаємо конкретний набір правил, сценаріїв та/або механізмів візуалізації. Наприклад, для виявлення сканування портів, звірки IP адреси з зовнішньої репутаційної бази тощо. Ви можете писати сценарії подій самостійно або замовляти у підрядників.

Наразі лише 3 виробники організували власні сайти для публікації сценаріїв подій. Більшість виробників внутрішній форум для обміну інформацією та пошуку рішень проблем що трапляються.

– HPE ArcSight Marketplace [10] – платний та безкоштовний. Якщо ви не застосовуєте додаткову фільтрацію, то на сайті розміщено 170 сценаріїв подій;

– IBM [11] Security App Exchange - завантаження безкоштовне. Існує 73 сценарії подій, розроблені IBM, та його партнерами;

– Splunk - підрозділ "Security, Fraud and Compliance" містить 487 програм. Але якщо ви фільтруєте лише додатки (не аддони, хоча вони також важливі) та вказати версію продукту 6.0 і вище - то загальна сума зменшується до 236 сценаріїв подій.

Для розробки правил співвідношення [9] ми збираємо всю інформацію яку може дати нам система SIEM, і починаємо фільтрувати. Основними методами співвідношення можна виділити:

– на основі правил (rule based) - взаємозв'язок між подіями визначається аналітиками в заздалегідь визначених правилах;

– на основі графіку (graph based) - пошук залежності між компонентами системи у вигляді графа.

Інструменти SIEM [5] повинні бути адаптовані до ваших індивідуальних потреб щоб визначити конкретні події для вас.

Щоб цілеспрямовано збирати та аналізувати лише відповідні дані, SIEM [5] має орієнтуватися на результати. Це означає, що дані події слід збирати, лише в тому випадку, якщо це необхідно для кінцевого результату. Джерела журналів та подій слід приймати лише для конкретних сценаріїв, правил співвідношення [9], звітів та інформаційних панелей. Наприклад, у типовому сценарії моніторингу підозрілих вихідних з'єднань та передачі даних потрібні лише журнали брандмауера, проксі-сервери та дані мережевого потоку. Підключення журналів DHCP або доступу до веб-додатків буде зайвим.

7) Тестування в системі

Дані тесту оцінюють доцільність та зручність подій обробки на основі процесів та технологій, розроблених у проєкті. Виконуючи ці кроки, ви можете реалізувати SOC. Після запуску проводиться підтримка SOC активності та тестування працездатності. Оптимізуйте процеси що існують, найміть нових фахівців та приєднайте нові джерела подій під час роботи.

Альтернативний варінт побудови SOC на підприємстві та процесів (рисунок 2.1-2.2)

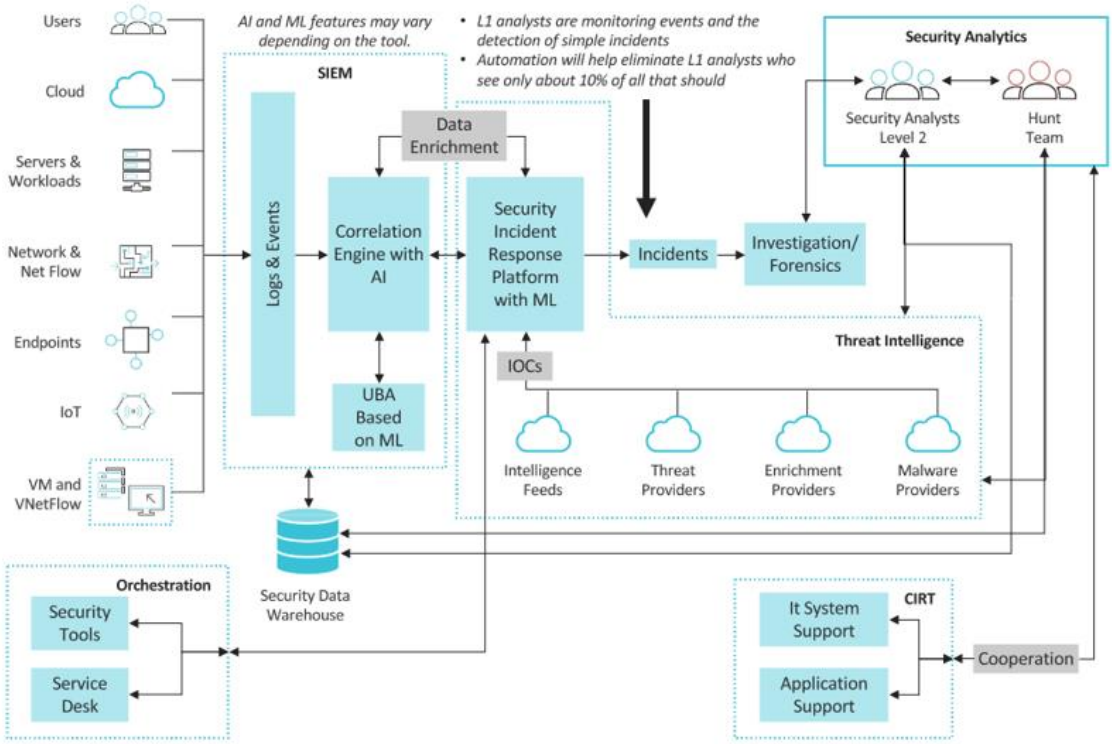


Рисунок 2.1 – Варіант побудови SOC

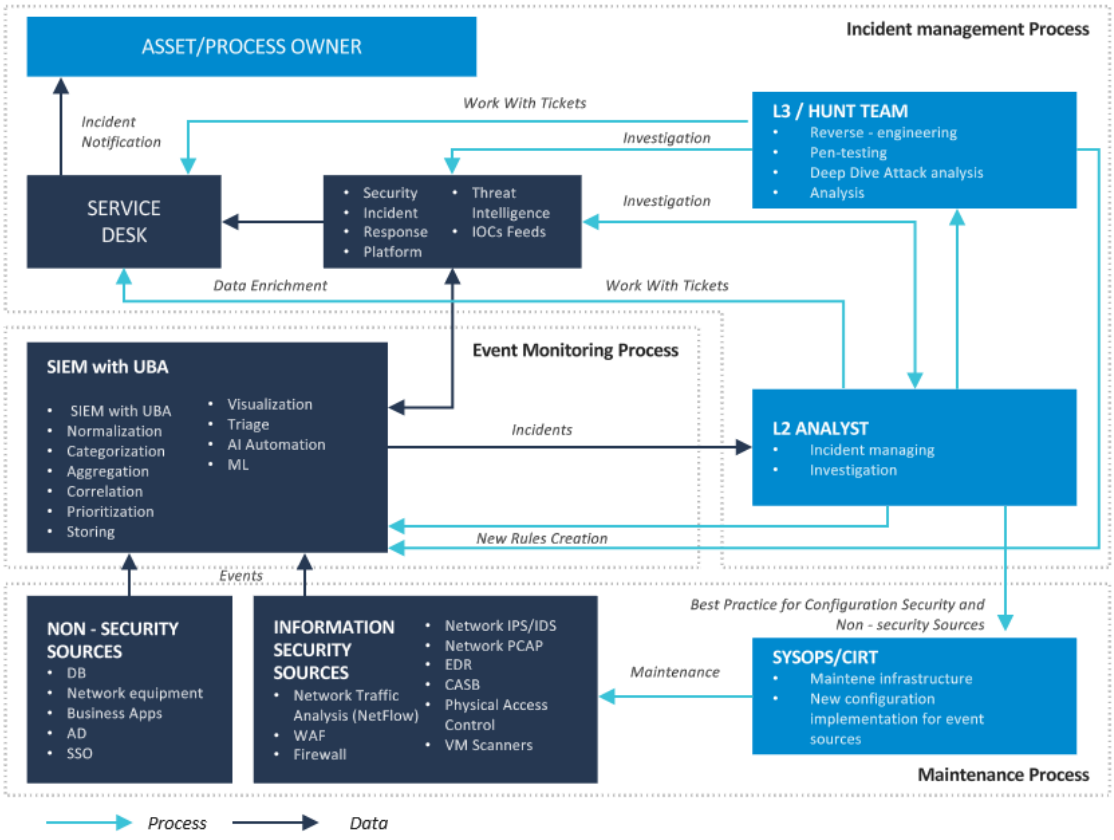


Рисунок 2.2 – Варіант побудови процесів SOC

У цьому розділі проаналізовано основні фактори, які можуть впливати на вибір конкретної моделі SOC, та подано рекомендації, які можуть допомогти вам вибрати архітектуру, необхідну для різних видів бізнесу. Представлено порядок розміщення SOC на підприємстві.

3 ПОРІВНЯННЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ПОДІЯМИ

3.1 Порівняння SIEM-систем.

Загальна інформація порівняння SIEM-систем (див. табл. 3.1):

Таблиця 3.1 - Загальна інформація порівняння SIEM-систем

Критерії оцінки / Вендор	Micro Focus (HP) ArcSight	IBM Qradar	Splunk
Назва компанії	Micro Focus International PLC	IBM (International Business Machines)	Splunk Inc
Веб-сайт	microfocus.com	ibm.com	splunk.com
Цільовий сегмент	Всі сектори. Великий і середній бізнес	Банківський, державний сектори, великий і середній бізнес	Всі сегменти у всіх галузях, від безкоштовних версій до найбільших інсталяцій
Терміни впровадження із заданими характеристиками (на одному об'єкті з підключенням понад 300 джерел і налаштуванням 15 базових правил співвідношення [9], коригування вбудованих)	Від 1 місяця (залежить від ТЗ, команди виконавця, залучення замовника)	Від 1 місяця (залежить від ТЗ, команди виконавця, залучення замовника)	Від 2 тижнів (при своєчасної залученості замовника, зафіксованих рамках проєкту)
Порівняння версії	7.0	7.3.1	Splunk Enterprise 7.0.1 + Splunk App for Enterprise Security 5.1.0
Мови інтерфейсу	Російська англійська	Російська англійська	Російська англійська
Країни в яких виконані впровадження	Північна і Південна Америка, Європа, Азія, Австралія, Африка, СНД	СНД, Європа, Америка, Азія, Африка, Австралія	СНД, Європа, Азія, Америка

Картка інциденту	55 полів, що настроюються	25 полів	0-236 штатних полів
Шляхи ескалації інциденту	побудова рівнів і шляхів ескалації інциденту	ескалація вручну	Автоматичнао настроюється ескалація на SOAR і інші засоби реагування через механізм модульних сповіщень Alerts. Ручна ескалація через Workflow Actions в картці інциденту
Оповіщення про інцидент (пошта, месенджери, SMS, інтеграції)	SMTP, SMS, API	SMTP, скрипти	Пошта, месенджери, скрипти, інтеграція зі сторонніми сервісами
Прийняття рішень в рамках процесу обробки інцидентів	Ручне і автоматичне	Ручне і автоматичне	Ручне
Інтеграція з системами Service Desk	Так (API, email)	Так (API, email, SNMP [14])	Так (API, email, SNMP [14])
Автореєстрація вразливостей (інтеграція зі сканерами)	Інтеграція з усіма популярними сканерами великих вендорів, можливості по інтеграції через API і звіти різних форматів	Інтеграція з понад 20 сканерами, підтримка формату AXIS	Інтеграція зі сканерами по відкритих протоколах. Для популярних сканерів є модулі розбору подій (Qualys, Netxpose Rapid7 і ін.)
Налаштування власної моделі визначення критичності уразливості	Так	Ні	Так
Сортування вразливостей за різними критеріями - в т. Ч. Критичності	Так	Так	Так
Можливість виділення помилкових спрацьовувань	В ручному режимі	В ручному режимі	Категоризація в ручному режимі або їх зниження з до настройку правил співвідношення
Ризик-співвідношення, облік ризик-співвідношення в правилах	Ризик-співвідношення на рівні логіки співвідношення і активів. Доп. вбудована в UBA	Ризик-співвідношення з урахуванням складових показника Magnitude (Relevance, Credibility і Severity)	Скорингова модель, що враховує дані про активи й облікові записи користувачів

Наявність встановлених правил співвідношення	Близько 350 сценаріїв співвідношення в 20 категоріях на 3 рівнях контенту доступні в ArcSight Content Brain	Більше 140, а також Content Extention Pack з IBM X-Force App Exchange	181 в Splunk ES штатно. +343 в безкоштовному додатку Splunk Security Essentials
Наявність встановлених графічних панелей (Dashboards)	28	7. Додатково з AppExchange може бути встановлено додаток візуалізації IBM QRadar Pulse	57
Наявність встановлених звітів	більше 80	Більше 110, а також Content Extention Pack з IBM X-Force App Exchange	більше 50
Перед настроєні панелі візуалізації і звіти щодо відповідності стандартам (Compliance)	PCI DSS, HIPAA, SOX, NERC, FISMA, IT GOV	COBIT [16], FISMA, GLBA, GSX-Memo22, HIPAA, NERC, PCI DSS, SOX	GDPR, HIPAA, FISMA, PCI DSS (платні і безкоштовні додатки до платформи SPLUNK ENTERPRISE и SPLUNK ES)
Робота з фільтрами (принцип - запити, поле)	Фільтри по полях, повнотекстовий пошук	Фільтри по полях, regex, мова AQL	Фільтри по полях, мова SPL
Побудова графів мережевої взаємодії	Взаємозв'язок між 3 хостами. Можлива інтеграція з продуктом мережевого моніторингу Micro Focus Network Node Manager (NNM)	Є близький аналог класичного графа, а також окремий модуль QRM	Є велика кількість графічних уявлень, реалізованих в додатках
Створення / зміна панелей	Так	Так	Так
Можливість формування звітів у вигляді документів, формати експорту звітів у вигляді документів	PDF, XLS, RTF, CSV, HTML	PDF, HTML, RTF, XML, XLS	Raw, PDF, CSV, XML, JSON
Операційна система в основі рішення	Red Hat Enterprise Linux\CentOS\SuSE Enterprise Linux	Red Hat Enterprise Linux	Linux с ядром 2.6+, Windows Server 2008 R2 та вище

СУБД	CORR-Engine	PostgreSQL, Ariel DB	Своя система зберігання даних
Наявність сформованих образів для платформ віртуалізації	VmWare	VMware, AWS	VMWare, AZURE, AWS, Docker Hub
Можливість зберігання даних на зовнішніх носіях (NAS / SAN)	Так	Так	Так
Можливість збільшення потужності компонентів системи	Розширенням доступних апаратних ресурсів	Розширенням доступних апаратних ресурсів, відповідно до рекомендацій виробника	Розширення стека ліцензій. Апаратне збільшення пам'яті і кол-ва ядер CPU збільшує кількість одночасно виконуваних запитів
Можливість розвитку системи за рахунок додавання додаткових компонентів (паралельне масштабування)	Так	Так	Так
Мінімальна кількість серверів для розгортання системи	1	1	1
Тип консолі адміністратора	Веб-консоль (ArcSight Command Center) і товстий клієнт (ArcSight Console)	Веб-консоль	Веб-консоль, CLI
Резервування конфігурації системи, можливість автоматичного відновлення	Резервне копіювання конфігурації	Так (в разі фізичного виходу з ладу - відновлення в ручному режимі)	Автоматичне відновлення при збоях, можливо збереження конфігурації на зовнішні носії
Можливість відновлення бази даних після збоїв	Так (DR сценарії або рішення по відмовостійкості)	Автоматичне резервування. Можливість відновлення (вибір варіантів) в ручному режимі	Створення резервних копій та відновлення даних за методикою вендора у відкритій документації

Рольова модель	RBAC	RBAC	RBAC
Аутентифікація (інтеграція з LDAP, Radius)	Локальна, Radius, LDAP, Active Directory	Локальна, Radius, Tacacs, Active Directory, LDAP	Active Directory, LDAP, SAML, RADIUS
Безпечні протоколи передачі даних між компонентами системи	Передача подій від ArcSight connector до ArcSight[10] ESM шифрується	TLS	TLS / SSL
Управління правилами співвідношення	об'єктний конструктор	Велика кількість вбудованих категорій, можливість використання обмеженого числа призначених для користувача категорій	Створення, зміна, видалення за допомогою Common Information Models (CIM), заснованому на моделях даних (DataModels)
Можливість використання зовнішніх динамічних листів, масивів даних	репутаційні листи	Вбудована підписка на IBM XForce, також є додаток для інтеграції з зовнішніми джерелами (STIX / TAXII і ін.)	Репутаційні бази (41 вбудована). Збагачення подій: бази даних, geoip, API, scripts
Тактичні листи (масив Даних), наповнючіх з полів подій інформаційної безпеки в системі вручну або при спрацьовуванні критерію	Необмежена кількість стовпців. Active list може заповнюватися вручну і при спрацьовуванні правил. Можна імпортувати події в Active list з CSV-файлу (наприклад, імпортувати назву вендора пристрою по MAC-адресу)	Reference List, динамічно формуються об'єкти. Наповнюються з API, CSV, правила співвідношення	Вручну - призначене для користувача контекстне правило (Action) в картці інциденту. Автоматично - призначене для користувача спрацьовування модуля оповіщення за результатами відпрацювання правила співвідношення або запиту за планувальником. Сховище підсумків - індекси, довідники (CSV, KV-store MongoDB, зовнішня СУБД чи інша система з API)
Можливість збору даних про трафік мережі	Netflow / J-flow / IPFIX	SPAN, Netflow, sFlow, jFlow і ін.	NetFlow, jFlow, sFlow, IPFIX, HTTP, MySQL, IMAP, POP3, XMPP, додаток Splunk App For Steam

Автовизначення джерел подій (Автоматичне заклад джерел подій при отриманні логів по syslog)	Так	Так	Так
Вбудована або підключається поведінкова аналітика (UBA & UEBA)	ArcSight UBA	User Behavior Analytics for QRadar	Вбудована на базі Splunk Extreme Search, Splunk UBA
Використання технологій штучного інтелекту, автоматизації [13] аналітики верхнього рівня	У ESM немає, є виділене рішення для аналітики - Investigate	QRadar Advisor With Watson	Вбудований в Splunk ES 5.0. + Функціональність Workbench Investigator
Використання алгоритмів машинного навчання	ArcSight UBA	QRadar Advisor With Watson	Splunk UBA, Splunk ML Toolkit, Splunk Extreme Search
Інтеграція з ITSM / CMDB	Так	Так (REST API)	Так
Необхідні ліцензії на стороннє ПО	Ні	Ні	Ні

У цьому розділі проаналізовано 3 основні компанії що надають SIEM, які можуть впливати на вибір конкретної моделі SOC. На основі цих даних можливо зробити вибір найкращої системи для підприємства. Найбільш привабливим рішенням для підприємства є SIEM Qradar від компанії IBM [11]. Далі були розроблена методика розслідувань різних типів інцидентів для SOC на підприємстві.

4 РОЗРОБКА ПРОЦЕСІВ РОЗСЛІДУВАНЬ РІЗНИХ ТИПІВ ІНЦИДЕНТІВ

4.1 Phishing інциденти.

Ця інформація необхідна для швидкого та детального вирішення різних phishing атак на всіх етапах.

Справа зі спамом та випадками риболовлі досягається за допомогою використання таких онлайн-рішень:

– Office 365 Advanced Thread Protection - веб-сайт, який перевіряє URL-адреси та визначає можливість потоку. Він показує фактичне посилання з декодованої URL-адреси.

– PhishCheck - веб-сайт, який фокусується на Phishing-check вставленої URL-адреси.

– CheckPhish - онлайн-сканер посилань, який ідентифікує фішинг.

– Tallos Intelligence - перевірка даних у режимі реального часу, яка визнає загрози, такі як спам, зловмисне програмне забезпечення чи законність електронної пошти.

– Virus Total - хмарний сервіс, що перевіряє підозрілі файли та URL-адреси.

– Hybrid Analysis - багатоцільовий сервіс, який перевіряє файли, посилання та колекції файлів.

– Vicheck - онлайн-перевірка хеш-запитів на зловмисне програмне забезпечення, що показує детальні результати та пошкоджені ділянки.

– URLscan.io - посилання та сканер URL-адрес, який визначає, використовується він для фішингу чи ні.

– MxToolBox - це онлайн-рішення, що надає ряд послуг для точної діагностики та пошуку мережі.

– XForce - онлайн-сервіс для перевірки домену та перевірки потоків глобальної безпеки.

Усі працівники компанії щодня отримують численні електронні листи. Більшість з них сортується як SPAM поштовим клієнтом автоматично. Ті, листи які не визнаються підозрілими системою, про яку повідомляє працівник вручну.

У Microsoft Outlook працівник відкриває потенційно шкідливу електронну пошту та натискає опцію Report Message (рисунок 4.1).

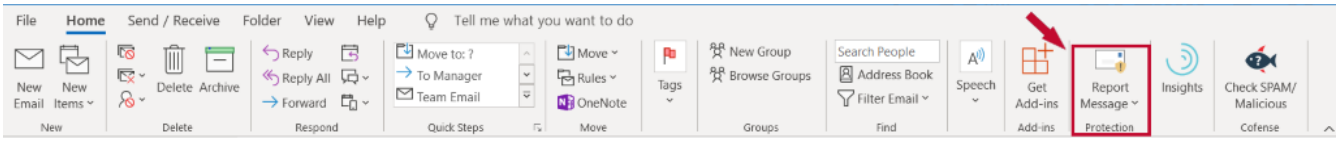


Рисунок 4.1 - Опція Report Message

Далі з'являється підменю, і користувач натискає параметр "Phishing". Він надсилає запит на перевірку повідомлення та домену (рисунок 4.2).

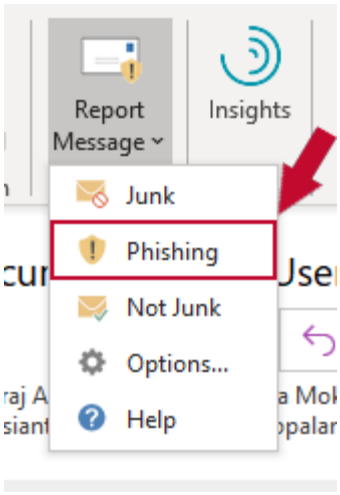


Рисунок 4.2 - Кнопка Phishing

Після надходження запиту він повинен бути оброблений для подальшого розслідування.

1) Аналіз електронної пошти.

Після того, як особа надсилає звіт про потенційний фішинг, вона стає доступною в сервісі асистенті, і інженер безпеки може розпочати обробку запиту та перевірку URL-адреси. Відкрийте один із призначених випадків та перегляньте його деталі (рисунок 4.3).

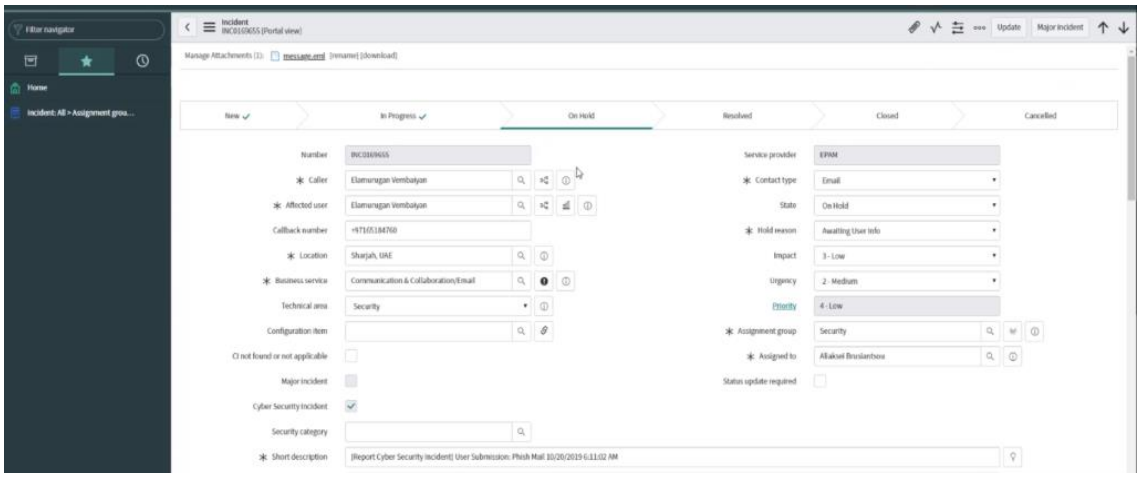


Рисунок 4.3 - Інцидент на обслуговування.

Завантажте електронну пошту, щоб побачити її компоненти (рисунок 4.4).

Рисунок 4.4 - Збереження повідомлення

Відкрийте файл і проаналізуйте його, щоб побачити, чи містить він додатки. Скопіюйте посилання, включене в електронну пошту (рисунок 4.5).

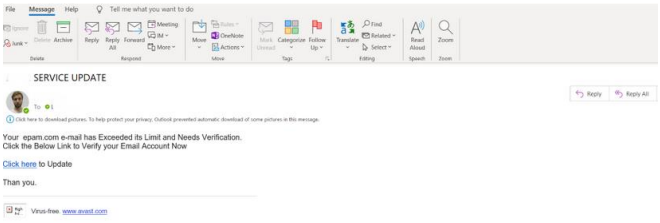


Рисунок 4.5 - Приклад фішинг-повідомлення

Проаналізуйте зв'язок з Hybrid Analysis. Відкрийте https://www.hybrid-analysis.com/ у своєму браузері. Вставте URL у поле та натисніть на параметр Analyze (рисунок 4.6).

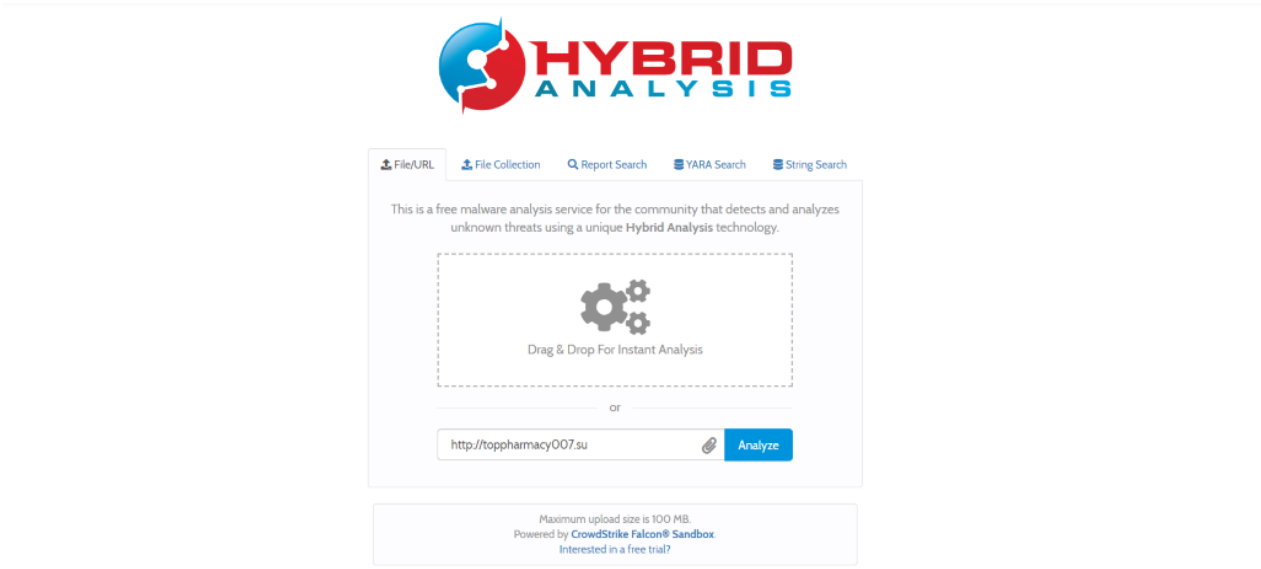


Рисунок 4.6 - Початкова сторінка Hybrid Analysis

У спливаючому вікні вкажіть додаткові параметри, включаючи прийняття політики конфіденційності, вказавши деталі середовища аналізу. Клацніть на опції Створити звіт (рисунок 4.7).

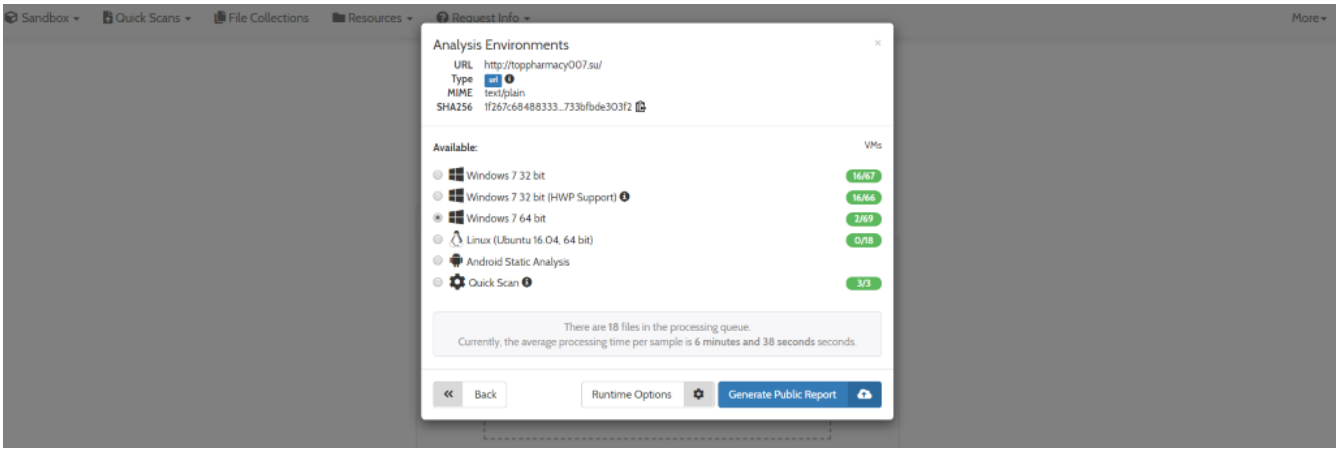


Рисунок 4.7 - Налаштування середовища Hybrid Analysis

Рішення завершить операцію детальними результатами. Спочатку відображається огляд аналізу. Він показує загальні результати для ідентифікації перевіреної веб-адреси (рисунок 4.8).

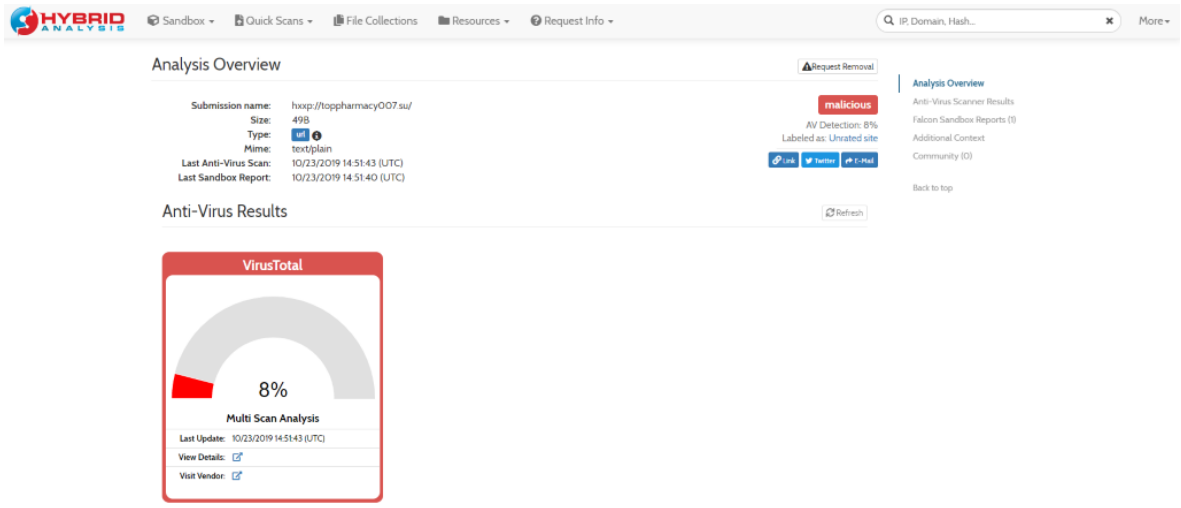


Рисунок 4.8 - Огляд Hybrid Analysis

Праве навігаційне меню допомагає побачити всі результати розслідування. Один з найкорисніших з них - Falcon Sandbox Reports (рисунок 4.9).

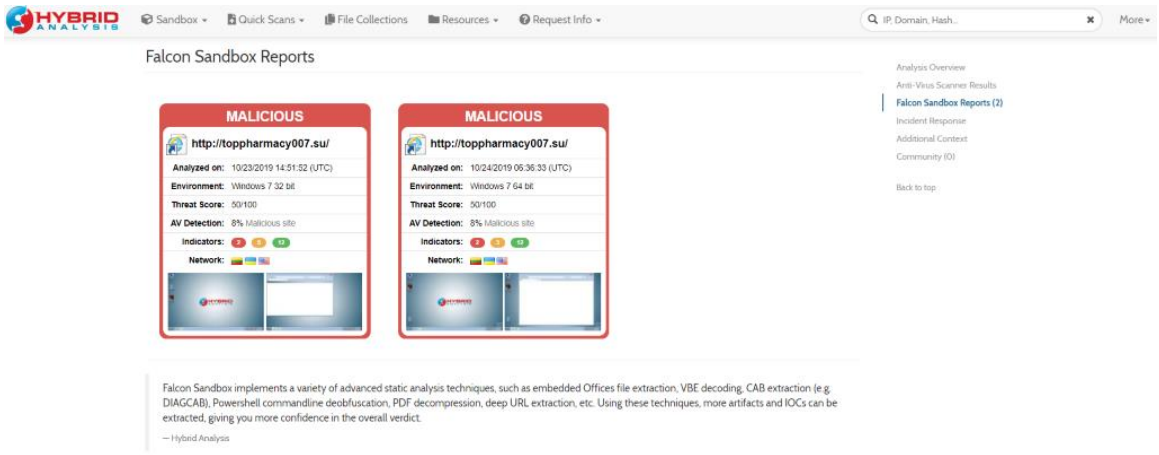


Рисунок 4.9 - Результати Hybrid Analysis Falcon Sandbox

2) Phishing check

Цей розділ містить кількість рішень для обробки інцидентів з потенційно шкідливим вмістом.

Перетворення безпечного посилання на фактичний URL.

Скопіюйте URL-адресу та перейдіть на сторінку http://www.o365atp.com/. Вставте посилання у поле і натисніть Enter (рисунок 4.10).

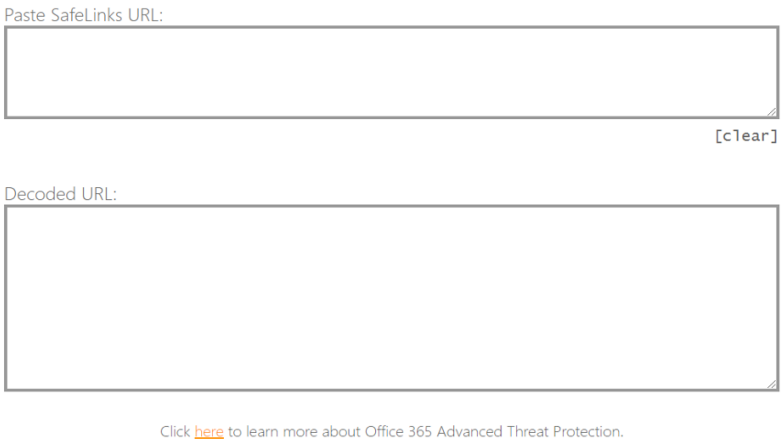


Рисунок 4.10 Веб-сайт Office 365 Advanced Thread Protection

Далі буде розшифрована URL-адреса, і ви можете продовжити перевірку.

Для успішної перевірки електронної пошти необхідно використовувати не тільки посилання, яке містить електронний лист, але й заголовок електронної пошти.

Відкрийте електронну пошту свого поштового клієнта. Клацніть на пунктирне меню, щоб переглянути джерело повідомлення (рисунок 4.11).

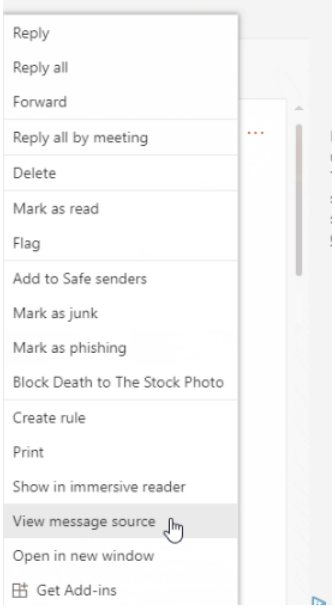


Рисунок 4.11 - Джерело повідомлення в Outlook

Далі ви побачите спливаюче меню, що містить всю інформацію про повідомлення. Заголовок доступний у вікні Інтернет-заголовки. Для завершення діагностики скопіюйте код з поля (рисунок 4.12).

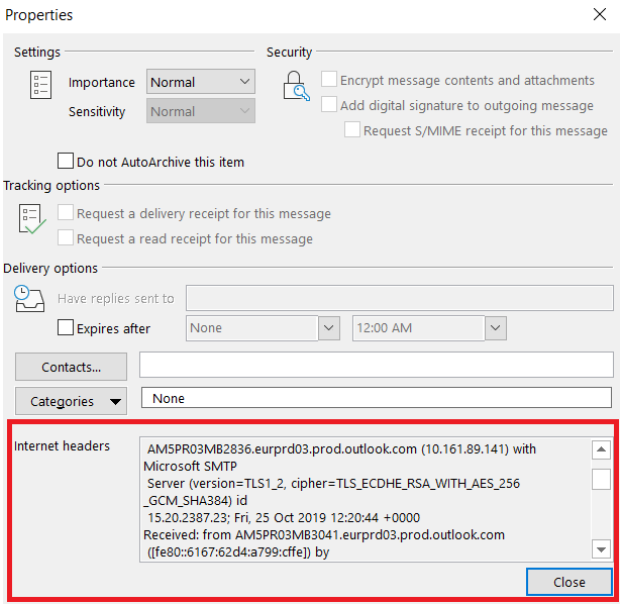


Рисунок 4.12 - Заголовок електронної пошти

Відкрийте MXToolBox за цим посиланням: https://mxtoolbox.com/EmailHeaders.aspx.

Вставте код у поле введення та натисніть кнопку Аналіз заголовка (рисунок 4.13).

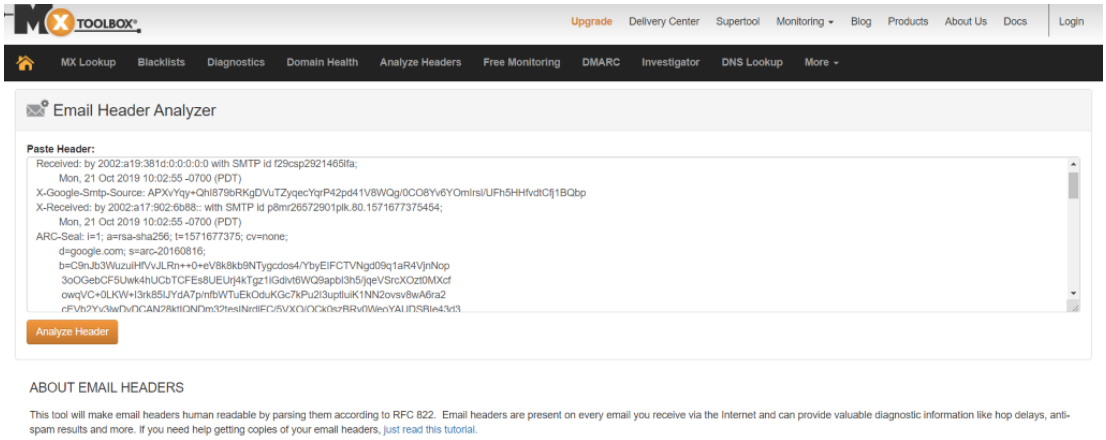


Рисунок 4.13 - Аналізатор заголовків MXToolBox

Результати з’являться далі. По-перше, інформація про доставку доступна (рисунок 4.14).

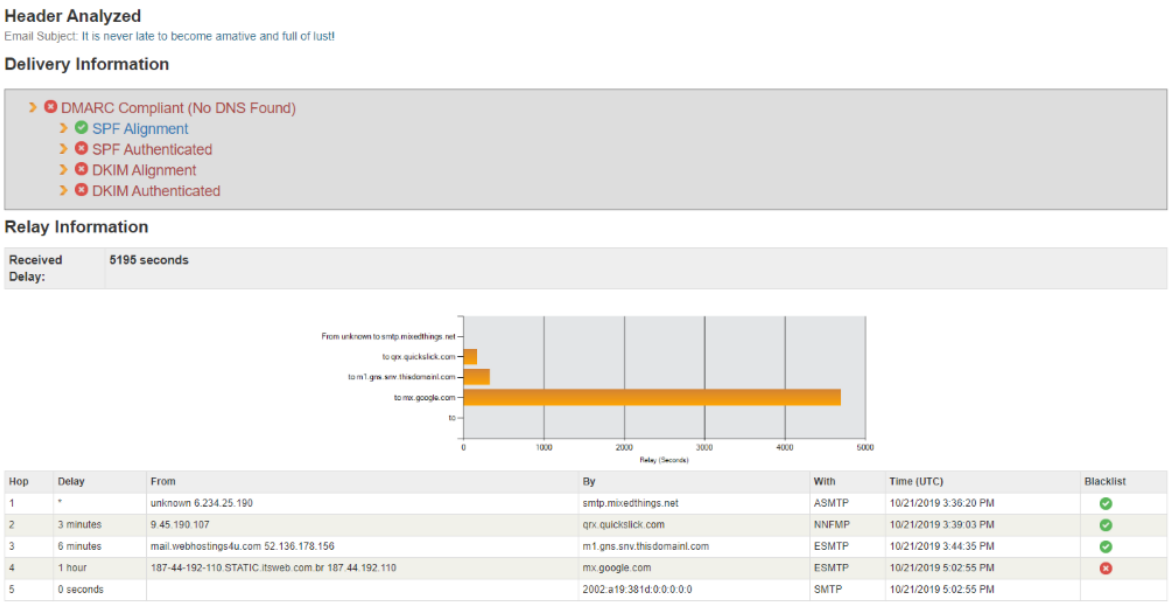


Рисунок 4.14 - Інформація про доставку MXToolBox

Прокрутіть до середини сторінки, і ви побачите опис процесів SPF та DKIM (рисунок 4.15).

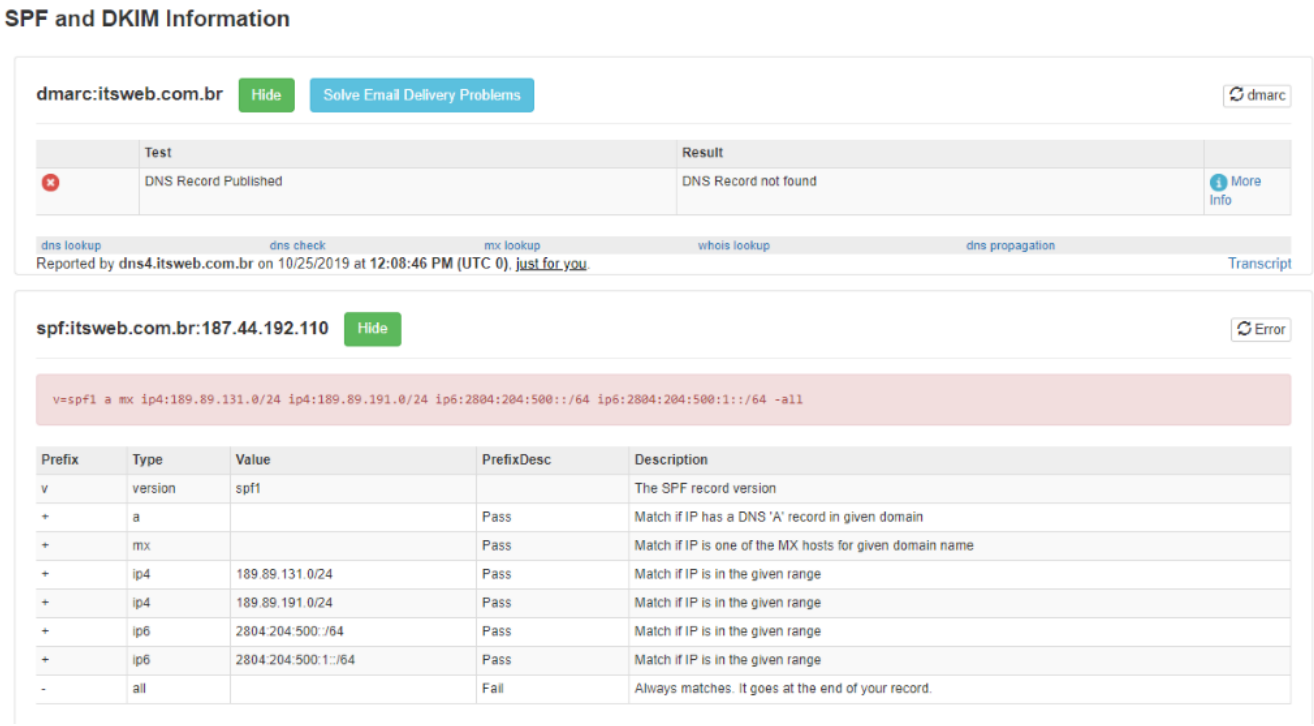


Рисунок 4.15 - Деталі MFToolBox SPF та DKIM

Внизу сторінки ви побачите всі заголовки з їх іменами та значеннями (рисунок 4.16).

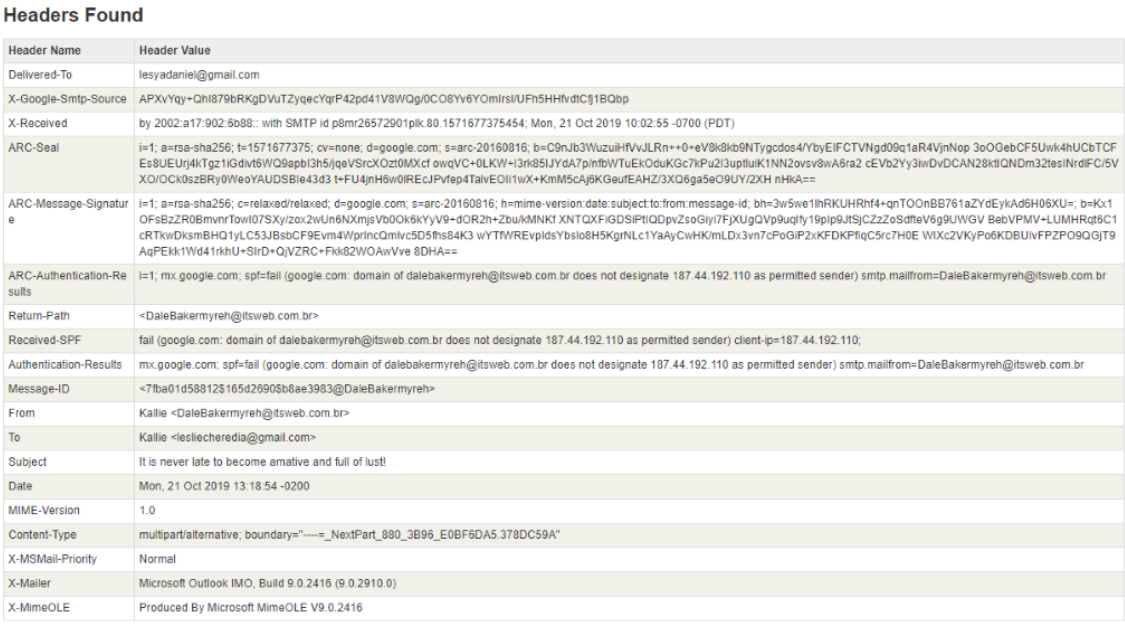
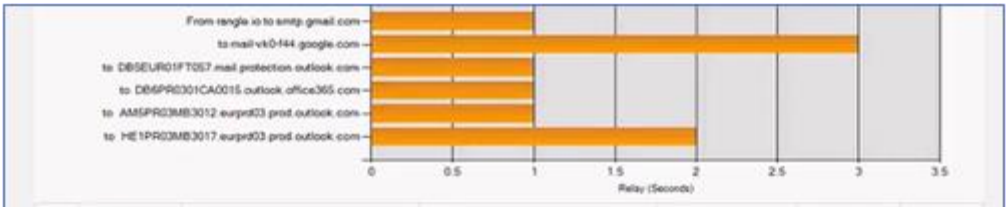


Рисунок 4.16 - Опис заголовків MXToolBox

Як результат, панель інструментів Mx відображає вичерпну інформацію про відправника повідомлення електронної пошти, таку як IP-адреса,

результати аутентифікації, отриманий SPF, шлях повернення, вихід діагностики спаму тощо.

Mx Toolbox повідомляє вас, чи є проміжний сервер, через який проходить повідомлення, у чорному списку, як показано на (рисунок 4.17).



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	rangle.io 34.192.159.190	smtp.gmail.com	ESMTPSA	12/5/2017 3:10:43 PM	
2	2 seconds		mail-vk0-f44.google.com	SMTP	12/5/2017 3:10:45 PM	
3	0 seconds	mail-vk0-f44.google.com 209.85.213.44	DB5EUR01FT057.mail.protection.outlook.com 10.152.5.104	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384)	12/5/2017 3:10:45 PM	
4	0 seconds	DB5EUR01FT057.eop-EUR01.prod.protection.outlook.com	DB6PR0301CA0015.outlook.office365.com	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_EC	12/5/2017 3:10:45 PM	

Рисунок 4.17 - Mx Toolbox повідомляє про чорний список

Найціннішу інформацію для аналізу спам-повідомлень можна знайти в заголовках Authentication-Results та Received-SPF.

3) SPF, DomainKeys та DKIM

Для додаткового захисту листування електронною поштою використовуються SPF (Sender Policy Framework), Domain Keys та DKIM (Domain Keys Identified Mail).

Оцінка запису SPF може повернути такі результати:

– Neutral - запис SPF прямо вказує, що нічого не можна сказати про дійсність;

– None - домен не має SPF-запису, або запис SPF не оцінює результат;

– Pass - запис SPF позначає хоста, якому можна дозволити відправлення;

– Fail - запис SPF визначає хоста як НЕ дозволяється надсилати;

– SoftFail - запис SPF визначає хост як НЕ дозволяється надсилати, але перебуває в переході.

4) Перевірка домену.

Для перевірки домену на фішинг ви можете скористатися кількома службами. Перший з них - Talos Intelligence. Це рішення перевіряє IP, домен або власнику мережі кількома простими клацаннями.

Перший крок - відвідати веб-сайт Talos Intelligence. Використовуйте посилання https://talosintelligence.com/ (рисунок 4.18).

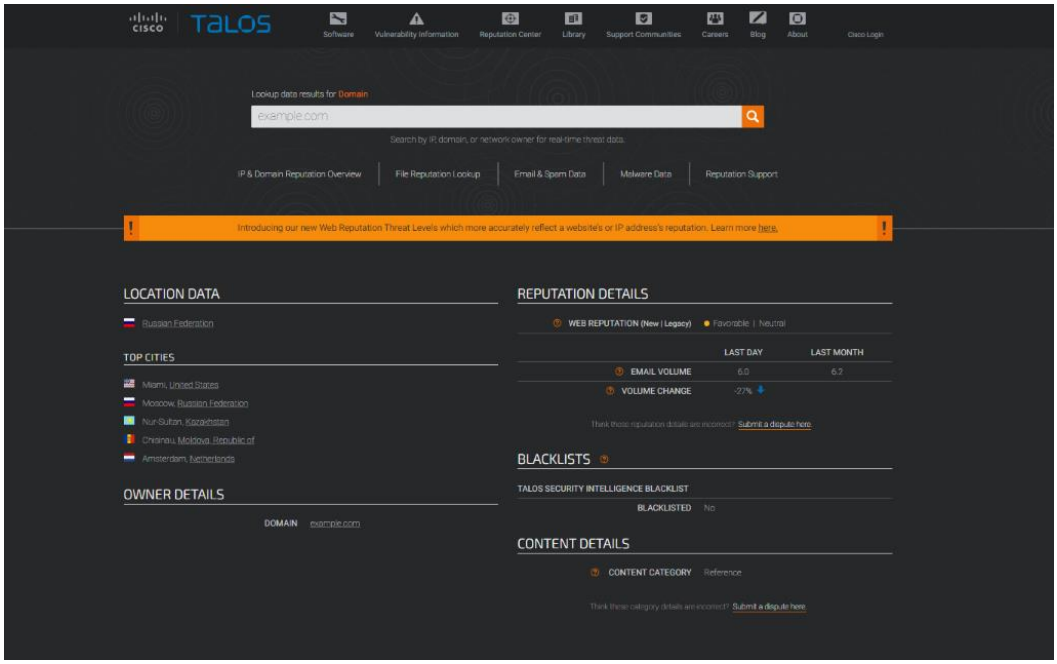


Рисунок 4.18 - Головна сторінка Talos Intelligence

Вставте або введіть адресу домену у полі введення та натисніть Enter (рисунок 4.19).

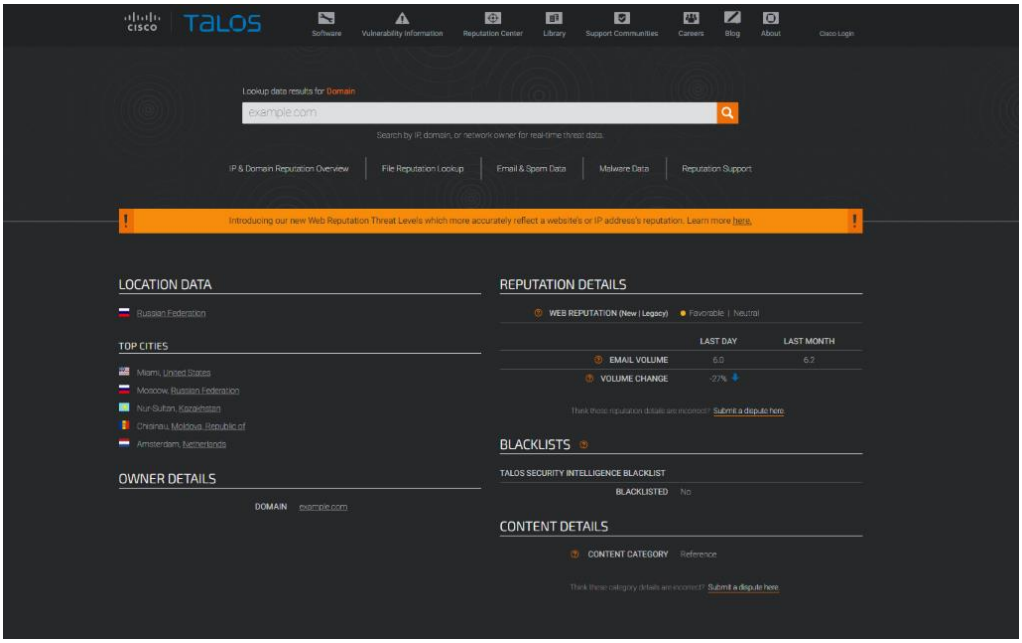


Рисунок 4.19 - Результати перевірки домену Talos Intelligence

Прокрутити униз, щоб переглянути додаткову інформацію про домен (рисунок 4.20).

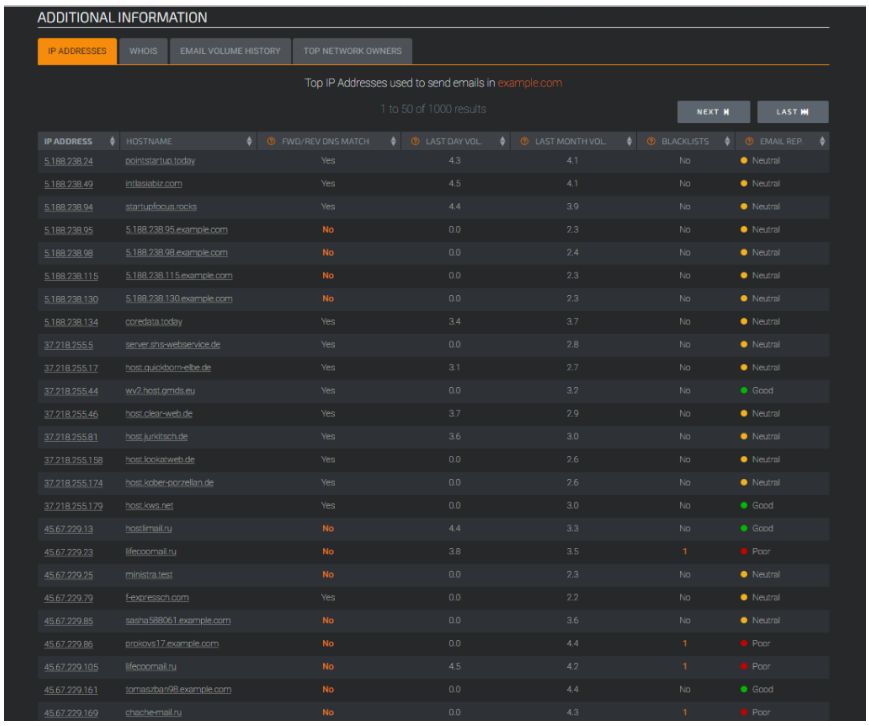


Рисунок 4.20 - Домен Talos Intelligence перевірити додаткові деталі

Використовуючи результати перевірки, ви побачите, чи домен перебуває у чорному списку, його репутацію та інформацію про вміст.

Щоб завершити дослідження домену для отримання останніх глобальних загроз безпеці, відвідайте веб-сервіс IBM [11] X-Force Exchange. Він доступний за цим посиланням https://exchange.xforce.ibmcloud.com/. Введіть доменну адресу та введіть її та скануйте, натиснувши клавішу Enter (рисунок 4.21).

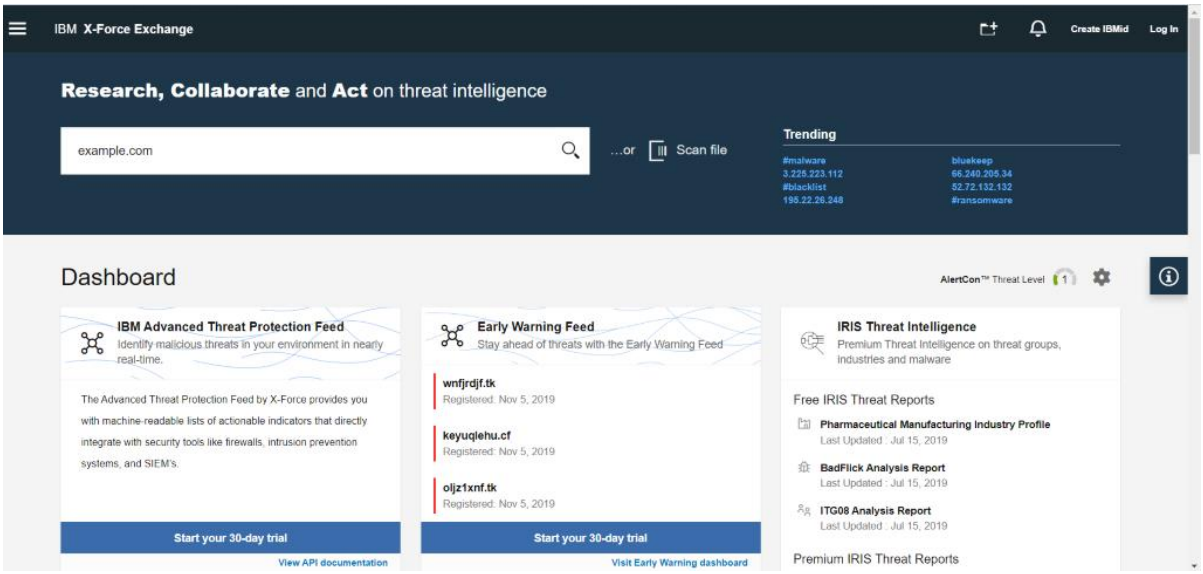


Рисунок 4.21 - Перевірка домену IBM X-Force

Після детального обстеження будуть показані всі результати. Перша частина містить загальні деталі (рисунок 4.22).

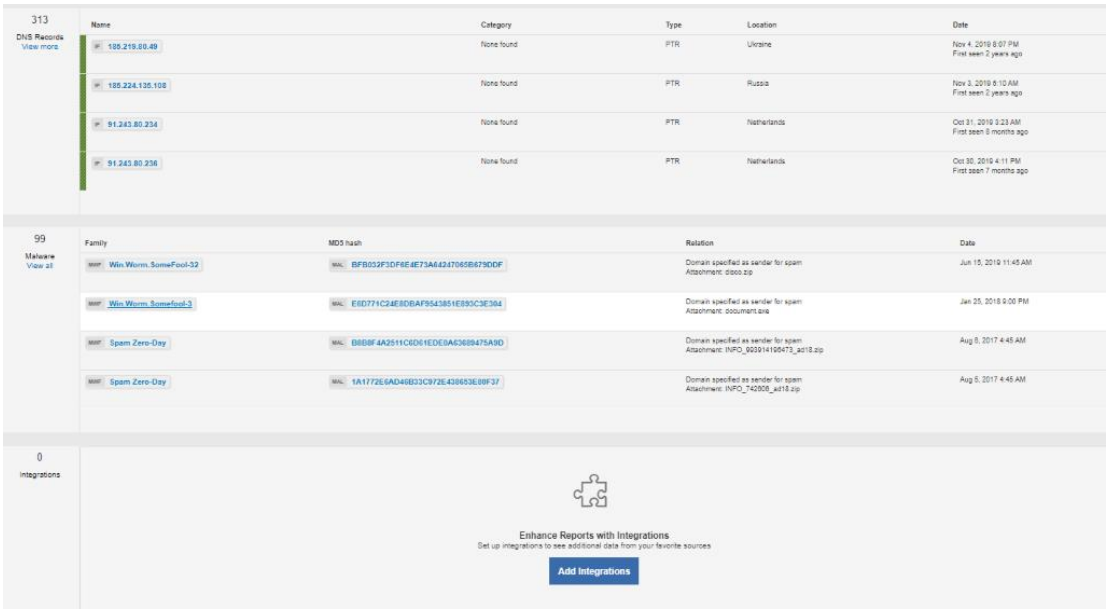


Рисунок 4.22 - Загальні деталі IBM X-Force

Прокрутіть униз, щоб переглянути повний звіт із додатковою інформацією про перевірений домен (рисунок 4.23).

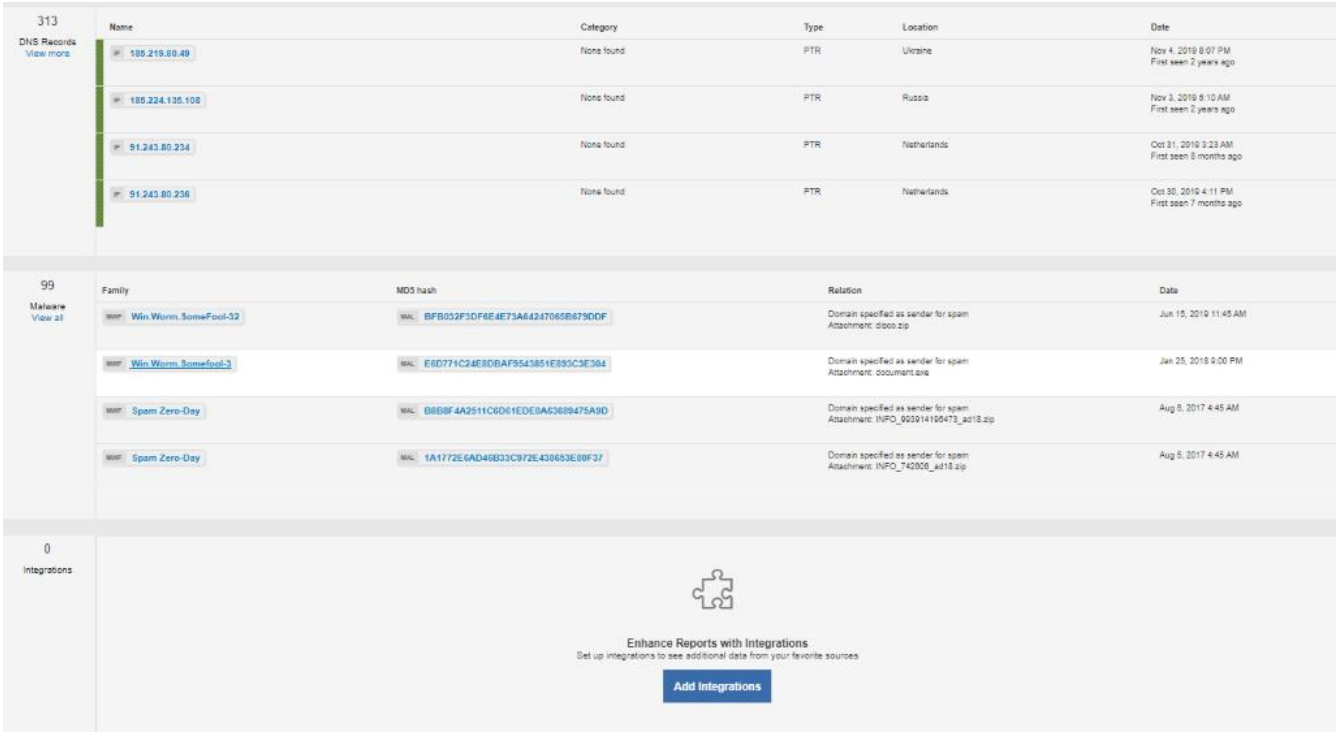


Рисунок 4.23 - Детальний звіт про домен IBM X-Force.

Ще одним інструментом для перевірки домену є VirusTotal. Відкрийте його за адресою https://www.virustotal.com/gui/home/url. Використовуйте область введення, щоб додати доменну адресу. Вставте адресу та натисніть Enter (рисунок 4.24).

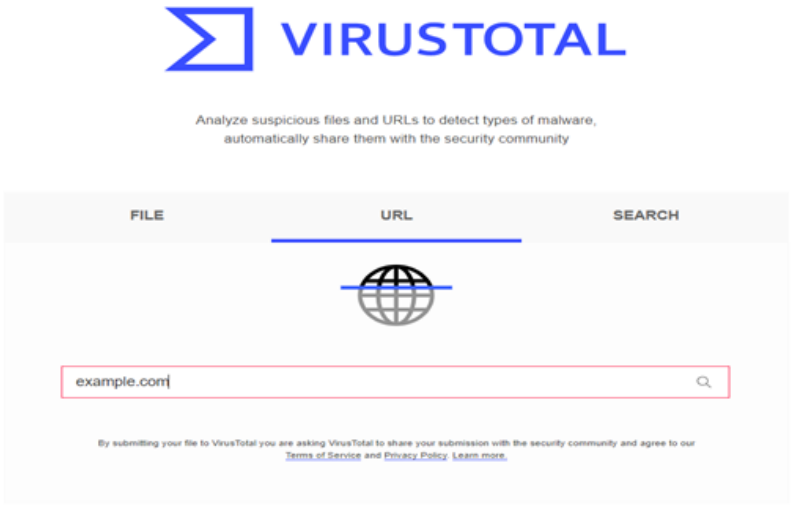


Рисунок 4.24 - Перевірка VirusTotal

Результати будуть такими (рисунок 4.25):

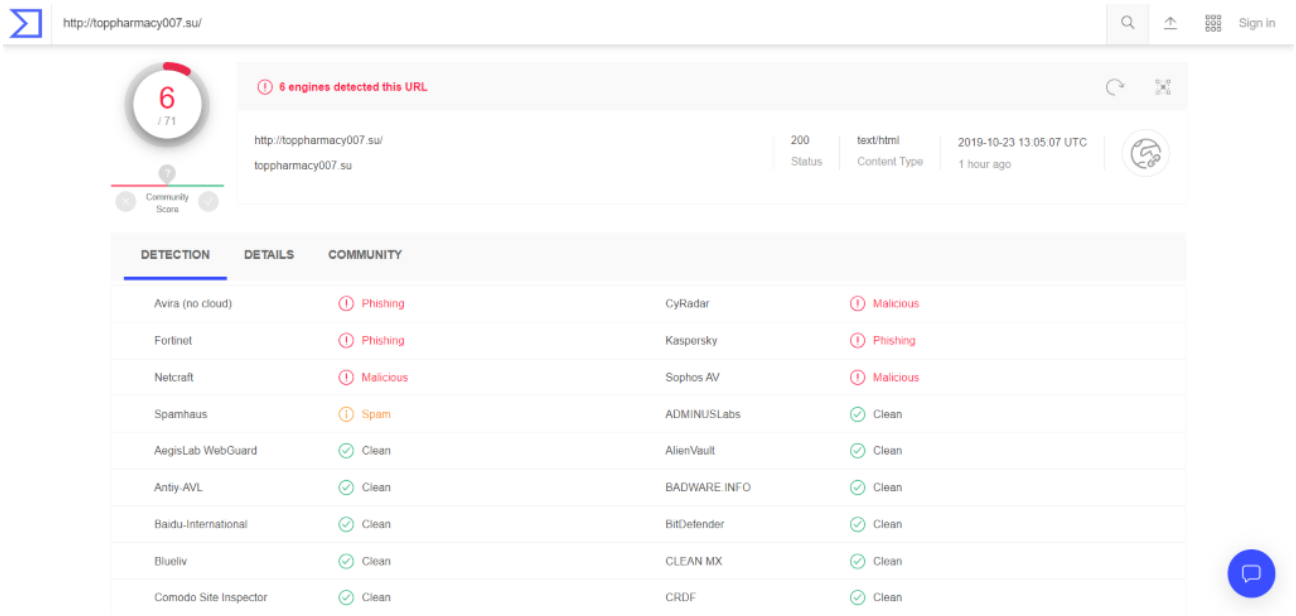


Рисунок 4.25 - Результати VirusTotal

Адреса домену легко перевіряється сервісом Urlscan.io. Щоб завершити перевірку, відвідайте веб-сторінку https://urlscan.io/. Вставте адресу домену та натисніть на опцію сканування (рисунок 4.26).

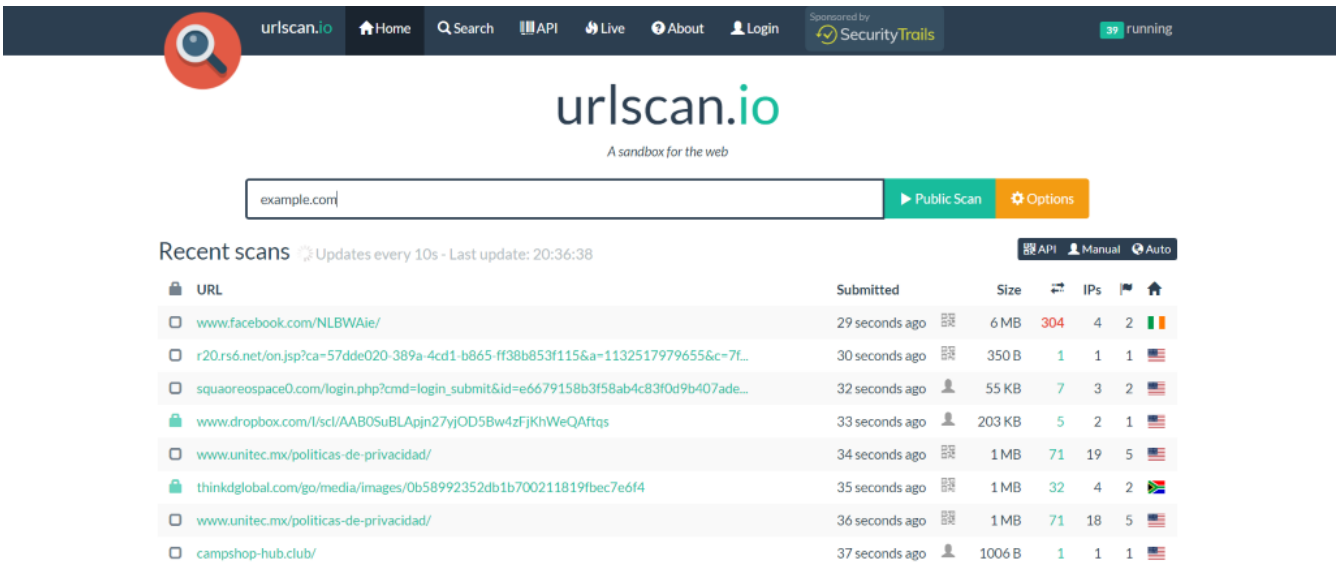


Рисунок 4.26 - Головна сторінка Urlscan

Зачекайте, поки процес конкурує (рисунок 4.27).

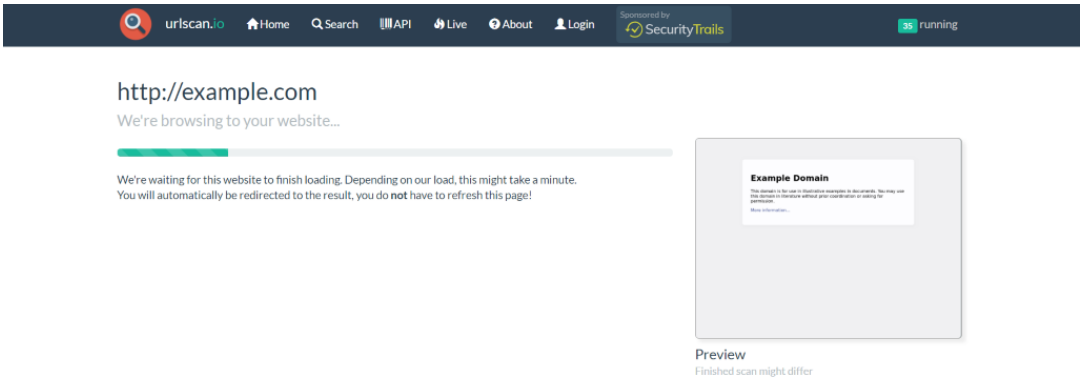


Рисунок 4.27 - Процес перегляду Urlscan

Верхівка відобразить такі результати (рисунок 4.28):

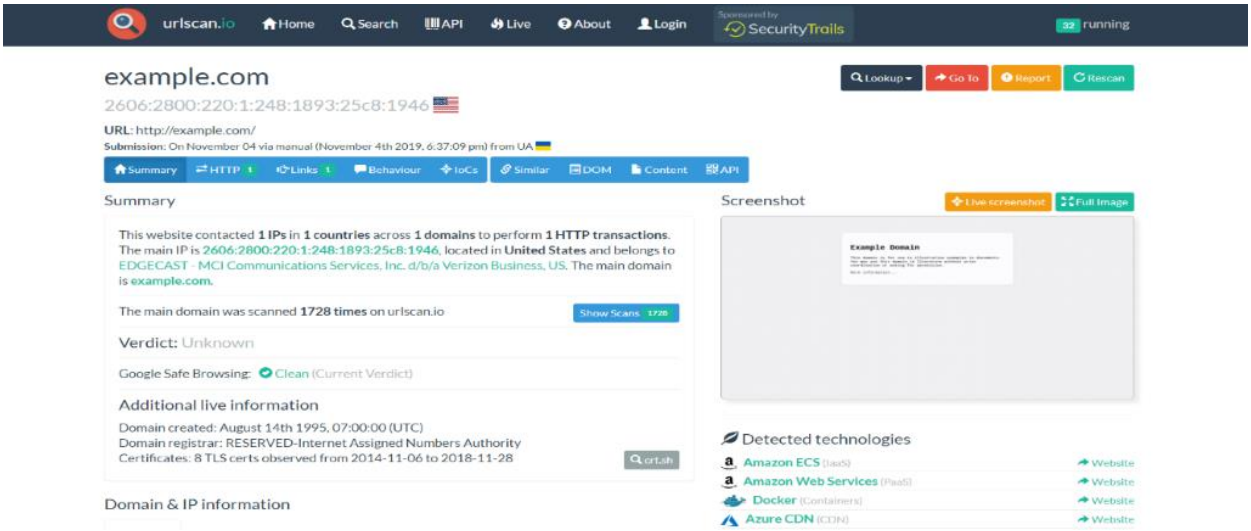


Рисунок 4.28 - Результати Urlscan

Щоб перевірити повну безпеку та безпеку домену, а також його проблеми та наявність чорного списку, використовуйте сервіс MXToolBox.

Відкрийте https://mxtoolbox.com/ у своєму браузері. Додайте доменну адресу до області введення та натисніть клавішу Enter (рисунок 4.29).

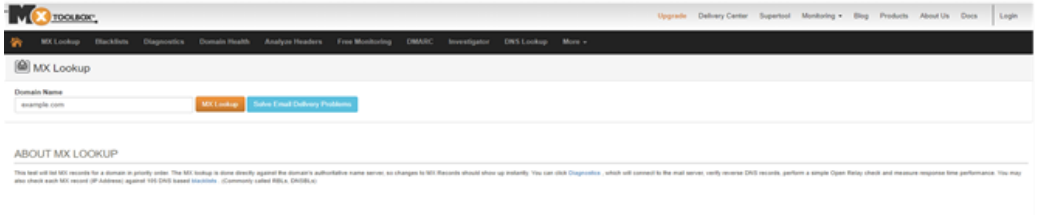


Рисунок 4.29 - Перевірка домену MXToolBox

Результати перевірки будуть відображені докладно (рисунок 4.30).

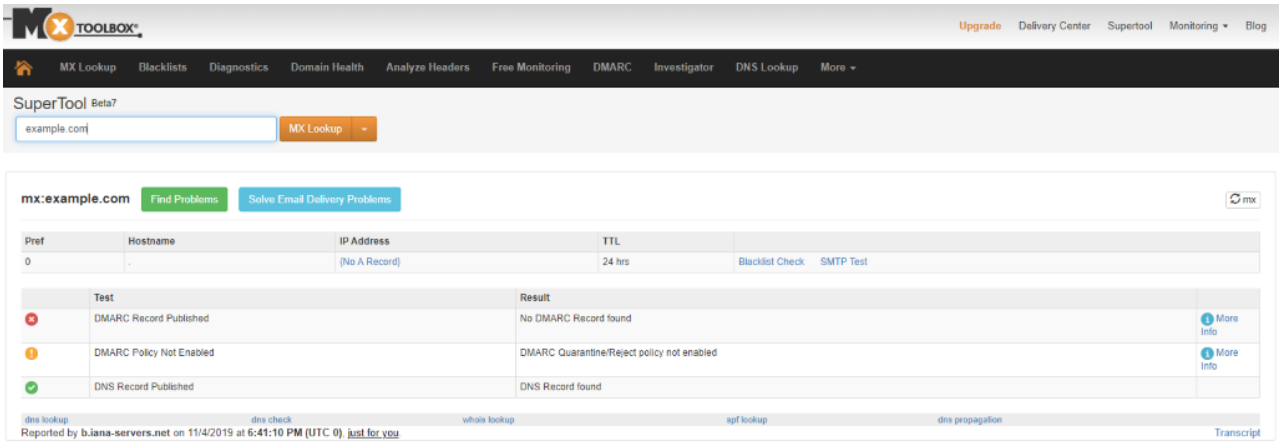


Рисунок 4.30 - Результати MXToolBox

Щоб дізнатися більше про перевірений домен, натисніть кнопку Знайти проблему. Сервіс відобразить усю додаткову інформацію про домен (рисунок 4.31).

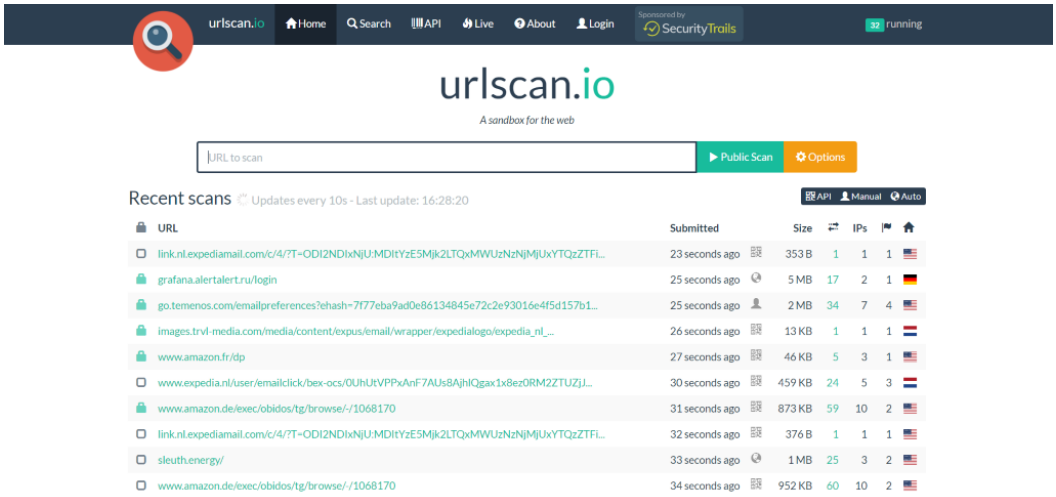


Рисунок 4.31 - Переадресація домену MXToolBox

5) Сканування URL-адрес

Щоб зробити глибоке розслідування, відвідайте https://urlscan.io/, вставте URL у поле пошуку, використовуйте параметри, щоб вибрати приватне сканування, і натисніть Enter. Це розслідування допомагає вивчити технології перенаправлення, які спрямовують відвідувача на фішинг чи зловмисне місце з безпечного сайту (рисунок 4.32).

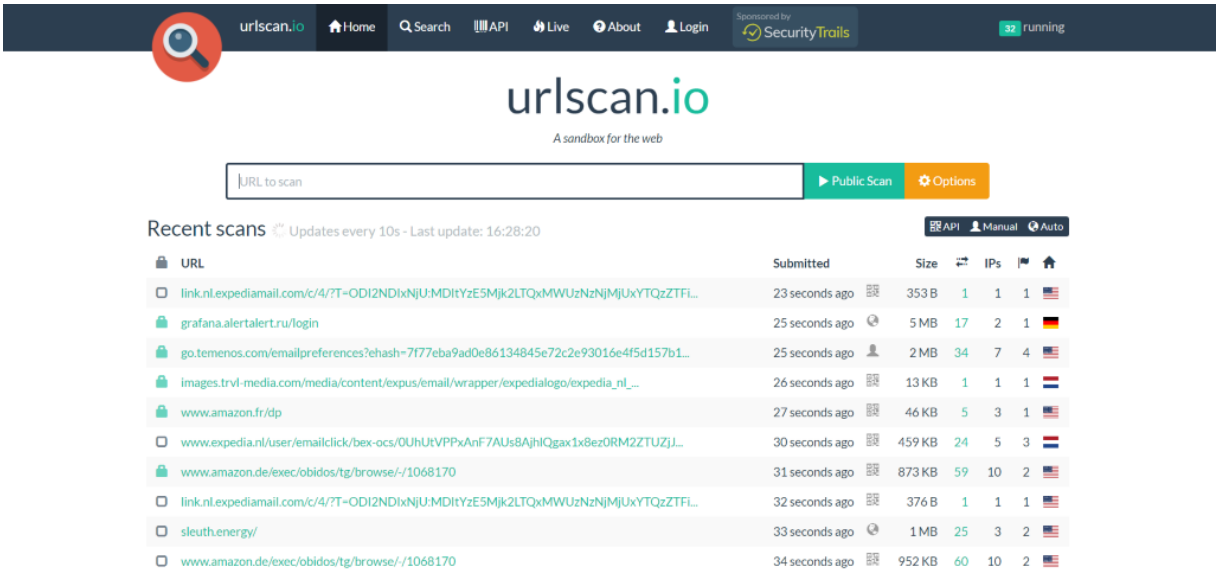


Рисунок 4.32 - Служба Urlscan.io

Потрібно вставити URL-адресу в поле пошуку. Використовуйте опцію приватного сканування. Вікно попереднього перегляду з’явиться під час перегляду. Він покаже веб-сайт, який з’явиться після натискання на посилання (рисунок 4.33).

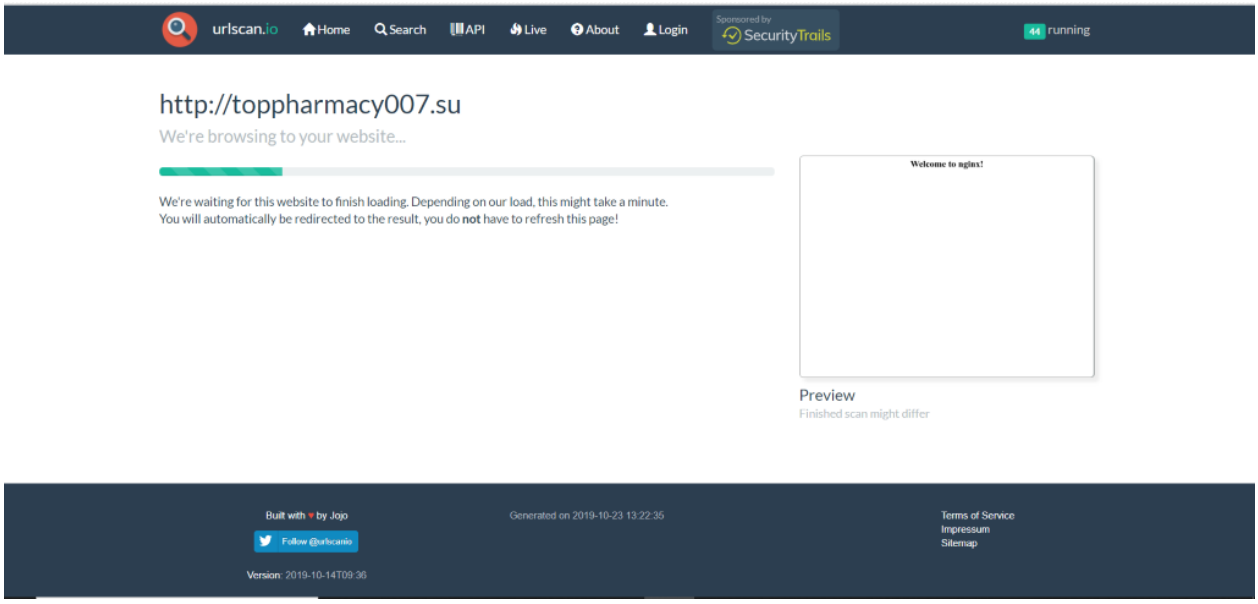


Рисунок 4.33 - Веб-сайт для обробки Urlscan.io

Нарешті, вся інформація про посилання буде доступною (рисунок 4.34).

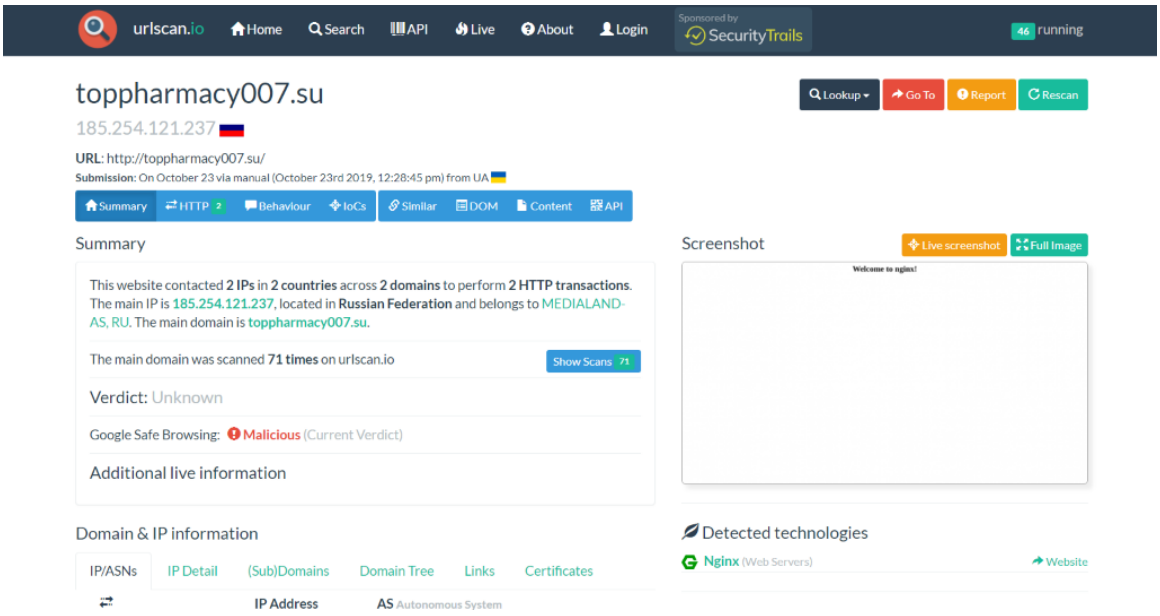


Рисунок 4.34 - Результати перевірки URL-адреси.io

Це повний звіт, що містить кількість IP-адрес, доменів, HTTP-транзакцій, країн IP-реєстрації та реєстрації доменів та поточний вердикт. Також доступні піддомени, дерева доменів, посилання та сертифікати. Система також відображатиме попередні сканування цього веб-сайту (якщо такі є).

Щоб побачити хеш для подальшого аналізу за допомогою Vicheck, перейдіть на вкладку IoC, і ви побачите код в останньому рядку (рисунок 4.35).

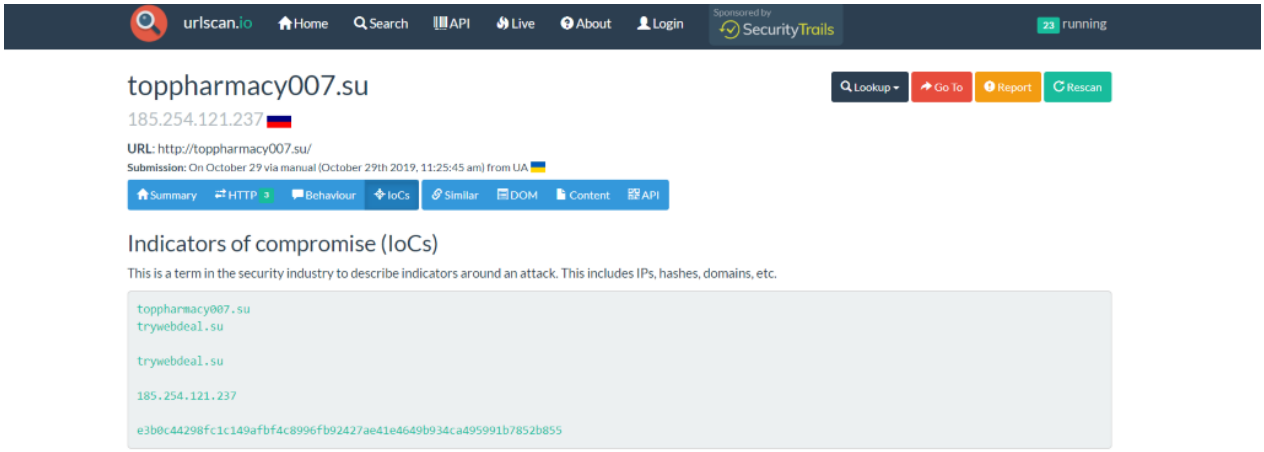


Рисунок 4.35 - Хеш-код

Далі пройдіть повну перевірку фішингу за допомогою https://checkphish.ai/ або https://phishcheck.me/ служби. Перший приклад, наведений нижче, - це https://checkphish.ai/ інспекція. Вставте адресу в поле виявлення та подайте кнопку Сканування (рисунок 4.36).

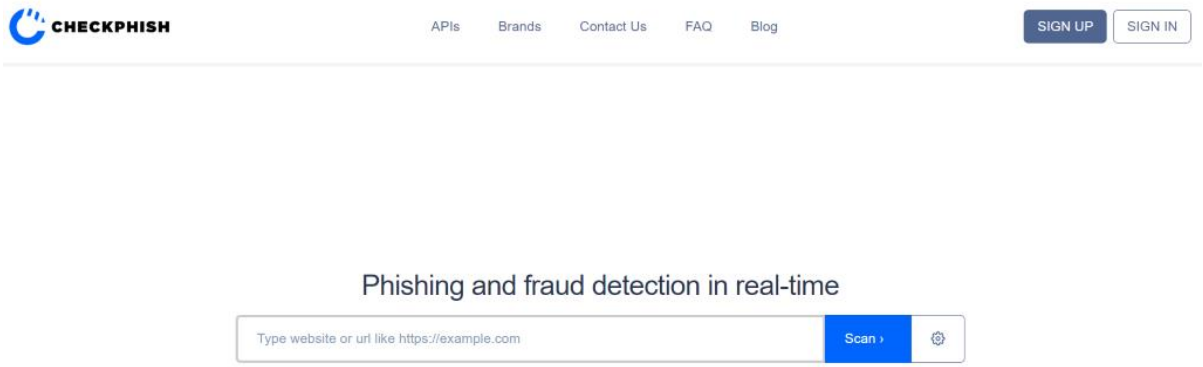


Рисунок 4.36 - Головна сторінка CheckPhish

Система виявить тип посилання, покаже його попередній перегляд та загальну інформацію (рисунок 4.37).

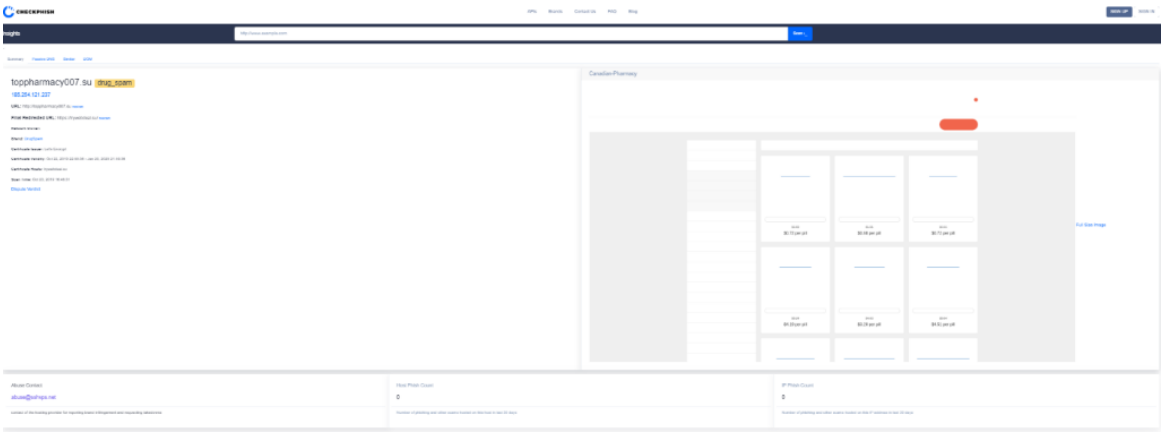


Рисунок 4.37 - Результати перевірки CheckPhish

Крім того, ви можете використовувати https://phishcheck.me/. Він завершує той же аналіз і автоматично створює аналогічний звіт огляду.

Відкрийте послугу у своєму браузері та додайте підозрілу URL-адресу до вікна пошуку та натисніть кнопку Перевірити (рисунок 4.38).

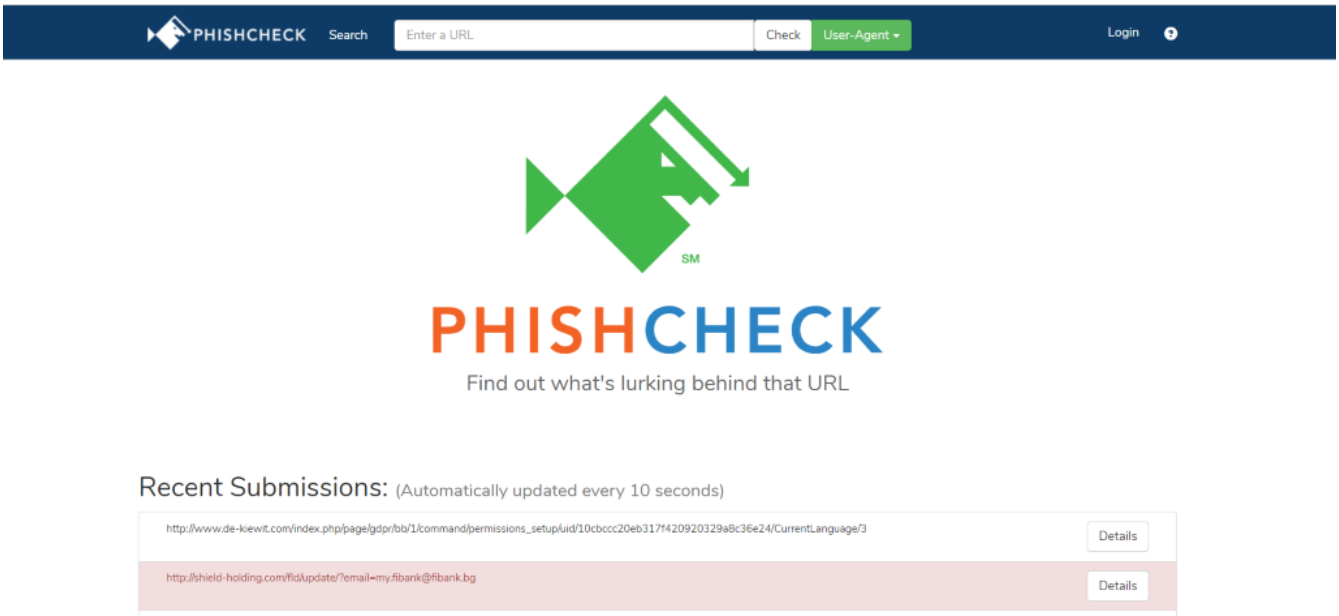


Рисунок 4.38 - Головна сторінка Phish-перевірки

Результати перевірки виглядатимуть наступним чином (рисунок 4.39).

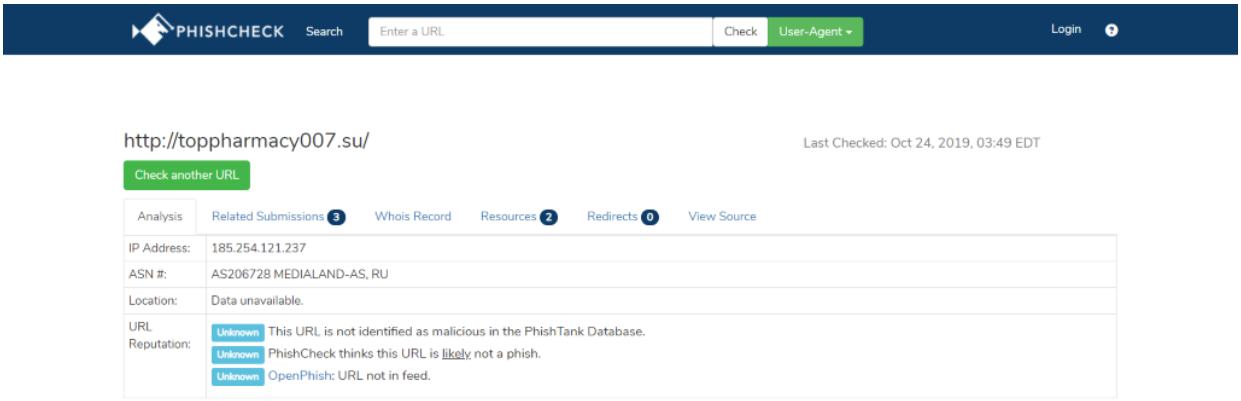


Рисунок 4.39 - Результати перевірки Phishing

4.2 Threat Intelligence.

Ця тематика поширюється на інженерів груп безпеки IT, відповідальних за роботу рішень безпеки, використовуючи канали розвідки про загрози.

Загрозу можна класифікувати за окремими групами відповідно до їх призначення:

- Malware;
- Ransomware;
- Botnet trackers;
- Miners trackers;
- Phishing;
- Fraud;
- Spam;
- Malware email addresses;
- IOCs;
- Miscellaneous custom IP block lists (suspicious).

Trusted Feed Sources - це довірені відкриті джерела які забезпечують постійне оновлення інформації щодо нових векторів нападу та більше можливостей для збору інформації Threat Intelligence. Інтеграція з різними довіреними відкритими джерелами забезпечує швидший огляд, переходячи від нещодавно бачених загроз до Advanced Persistent Threats, для їх аналізу. Деякі з них можуть бути інтегровані з рішеннями безпеки підприємства.

Malware:

- https://threatview.ca/threats/
- http://mirror1.malwaredomains.com/files/domains.txt
- http://osint.bambenekconsulting.com/feeds/
- https://infosec.cert-pa.it/analyze/listdomains.txt
- https://infosec.cert-pa.it/analyze/listip.txt
- https://infosec.cert-pa.it/analyze/listurls.txt

– http://malc0de.com/database/
– https://urlhaus.abuse.ch/browse/
– https://github.com/mitre/cti/blob/master/USAGE.md
– http://data.netlab.360.com/feeds/dga/dga.txt
– https://labs.sucuri.net/?malware
– http://urlvir.com/export-hosts/
– https://malwared.malwaremustdie.org/

Ransomware:

– https://ransomwaretracker.abuse.ch/downloads/RW_DOMBL.txt

Botnet trackers

– https://threatview.ca/threats/;
– https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist;
– https://feodotracker.abuse.ch/;
– http://malwaredomainlist.com/hostslist/zeus.xml ;
– https://palevotracker.abuse.ch;
– https://techhelplist.com/maltlqr/reports/dyreza.txt.

Crypto miners' trackers

– https://github.com/hoshsadiq/adblock-nocoin-list/blob/master/hosts.txt;
– https://gitlab.com/ZeroDot1/CoinBlockerLists/raw/master/list_optional.txt;
– https://notmining.org/export.php.

Phishing

– https://phishtank.com/;
– https://openphish.com/feed.txt;
– https://threatview.ca/threats/;
– http://botscout.com/.

Fraud

– http://voipbl.org/ .

Spam

– https://community.opendns.com/;
– https://www.spamhaus.org/drop/;
– https://threatview.ca/threats/;
– http://www.stopforumspam.com/downloads/listed_ip_1_all.zip.

Malware email addresses

– https://github.com/martenson/disposable-email-domains;
– https://raw.githubusercontent.com/WSTNPHX/scripts-n-tools/master/malware-email-addresses.txt.

IOCs

– https://github.com/MISP/MISP;
– https://github.com/TheHive-Project/TheHive;
– https://circl.lu/doc/misp/feed-osint/;
– http://botvrij.eu;
– http://botvrij.eu/data/ioclist.url;
– http://botvrij.eu/data/ioclist.domain;
– http://botvrij.eu/data/ioclist.ip-dst.

Threat Intelligence pools

– https://threatconnect.com/;
– https://recordedfuture.com;
– https://threatview.ca/threats/;

– https://intel.criticalstack.com/;
– https://c1fapp.com/;
– https://cymon.io/;
– https://threatfeeds.io/;
– https://github.com/maravento/blackweb;
– http://iplists.firehol.org/;
– http://dns-bh.sagadc.org/.

Miscellaneous custom IP block lists (suspicious)

– https://autoshun.org/;
– https://binarydefense.com/banlist.txt;
– http://cinsscore.com/list/ci-badguys.txt;
– http://rules.emergingthreats.net/fwrules/;
– http://iplists.firehol.org/;
– https://iblocklist.com/lists;
– http://lists.blocklist.de/lists/dnsbl/;
– https://report.cs.rutgers.edu/mrtg/drop/dropstat.cgi?start=-86400;
– https://dshield.org/ipsascii.html;
– https://projecthoneypot.org/list_of_ips.php;
– http://blocklist.greensnow.co/greensnow.txt;
– http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt;
– http://danger.rulez.sk/projects/bruteforceblocker/blist.php;
– http://malc0de.com/bl/IP_Blacklist.txt;
– http://hosts-file.net/?s=Browse&f=2019;
– http://labs.snort.org/feeds/ip-filter.blf;
– https://github.com/stamparm/maltrail/blob/master/trails/static/mass_scanner.txt;
– https://myip.ms/files/blacklist/htaccess/latest_blacklist.txt;
– https://badips.com/get/list/any/2?age=7d.

Other (temporary unavailable feed sources)

– https://malwr.com/;
– http://malwaregroup.com/ipaddresses;
– http://malwaredb.malekal.com/;
– http://projecthoneypot.org/list_of_ips.php;
– https://talosintelligence.com/reputation_centerthreatview.

Для перефірки фіда рекомендовано скористатися сервісом VirusTotal (рисунок 4.40).

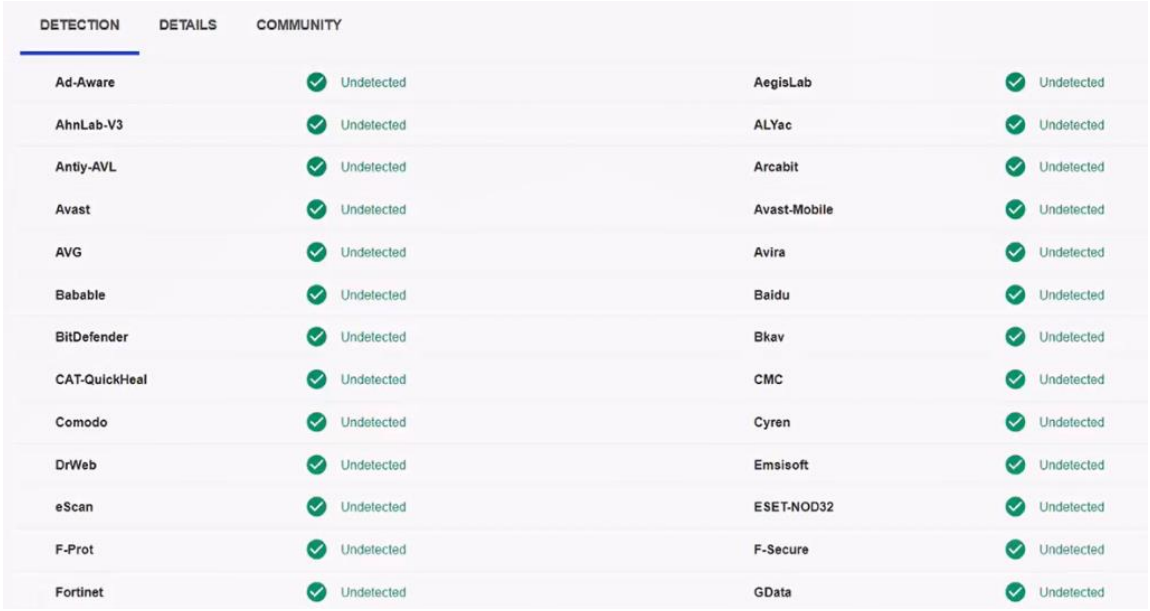


Рисунок 4.40 – Перевірка на сервісе VirusTotal

Серед усіх постачальників VirusTotal, для цілей цієї оцінки, ми вважали таких постачальників надійними:

– CLEANMX;
– Kaspersky;
– BitDefender;
– DrWeb;
– AlienVault;

– Phishtank;
– OpenPhish;
– Spamhaus;
– Sophos;
– ESET;
– Mitre.

Будь-який канал, виявлений цими надійними постачальниками VirusTotal, є потенційним FALSE POSITIVE.

4.3 Software security check.

Програмне забезпечення VPN, P2P з функцією анонімізації не може використовуватися для хакерських дій що потрібно забороняти на підприємствах. Запити щодо використання такого програмного забезпечення потрібно відхиляти.

Перш ніж додавати Програмне забезпечення до затвердженого списку, його слід перевірити на наявність вразливих місць. Щоб виявити вразливості програмного забезпечення та його компонентів, використовуйте наявні сканери вразливості на підприємстві.

Щоб здійснити перевірку безпеки програмного забезпечення, слід переглянути все програмне забезпечення, яке встановлене на хості, та всі його відповідні вразливості. Для цього відфільтруйте інформацію за хостом (за допомогою попередньо встановленого агента). Все програмне забезпечення, встановлене на хості, буде доступне на вкладці Встановлене програмне забезпечення (рисунок 4.41).

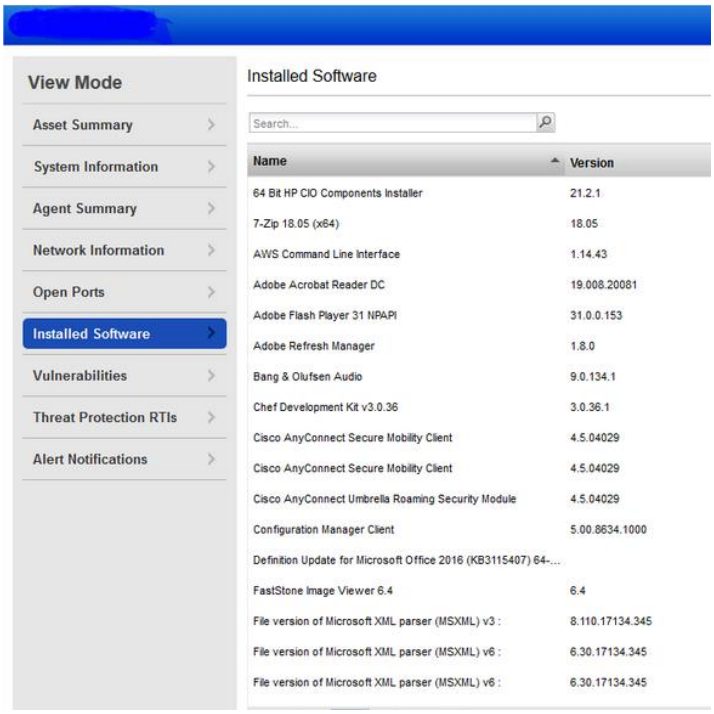


Рисунок 4.41 - Список встановленого програмного забезпечення

Щоб побачити всі вразливості конкретного програмного забезпечення, натисніть Vulnerabilities > View Vulnerabilities (рисунок 4.42).

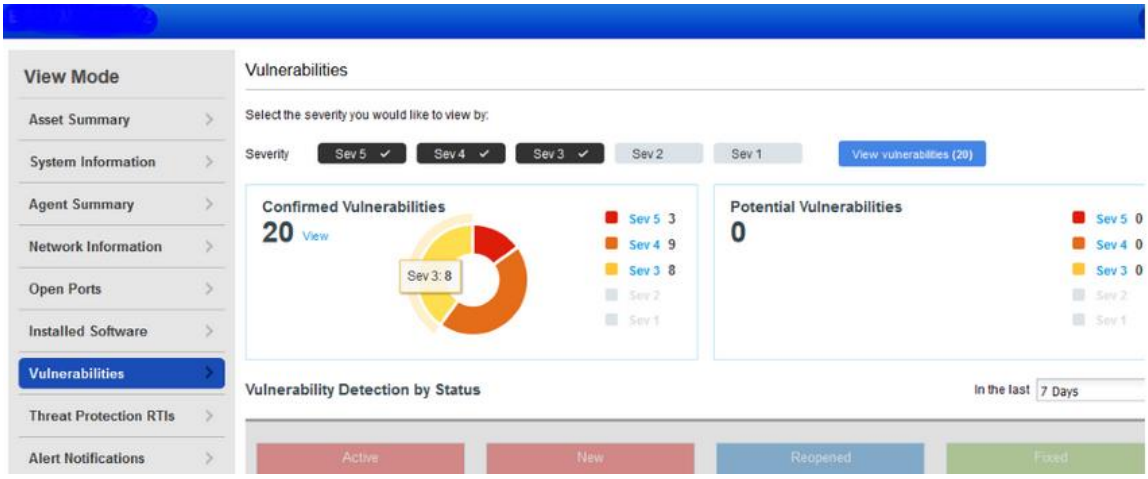


Рисунок 4.42 - Інформація про вразливі місця

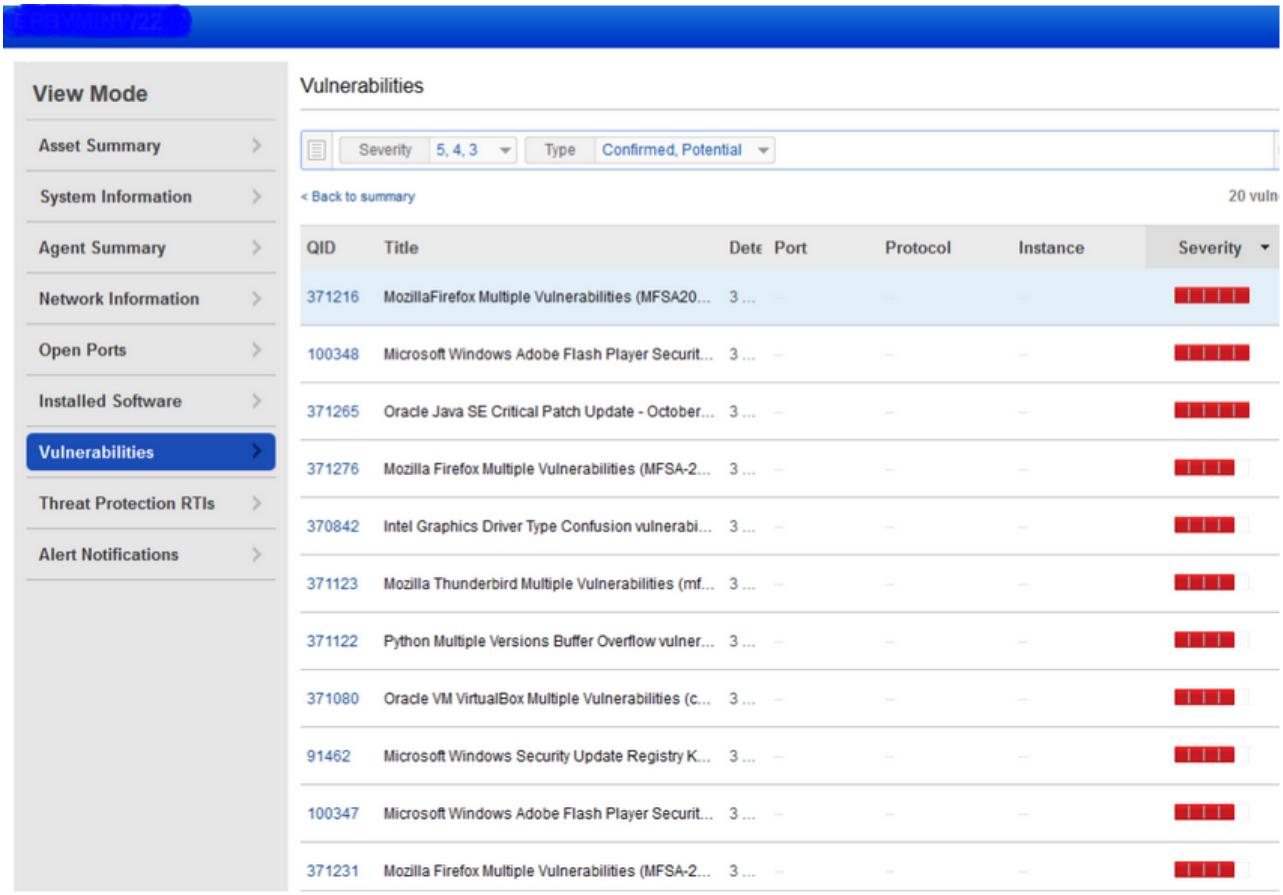


Рисунок 4.43- Список вразливості програмного забезпечення

Якщо рішення Qualys не виявляє вразливості, додаткова перевірка іншими рішеннями наразі не потрібна.

Для аналізу шкідливих показників для файлу можна скористатися сервісом Hybrid Analysis.

Hybrid Analysis - це безкоштовна служба аналізу шкідливих програм для спільноти, яка виявляє та аналізує невідомі загрози за допомогою унікальної технології Hybrid Analysis. Ви можете подавати файли як для глибокого статичного, так і динамічного аналізу.

Гібридний аналіз дозволяє виявити різні шкідливі показники, наприклад, записи реєстру, ін'єкції процесів тощо. Повний список показників див. У підрозділі Показники.

Служба підтримує файли PE, Office, PDF, APK та навіть більше (наприклад, EML). Максимальний розмір завантаження - 100 Мб (рисунок 4.44-4.46).

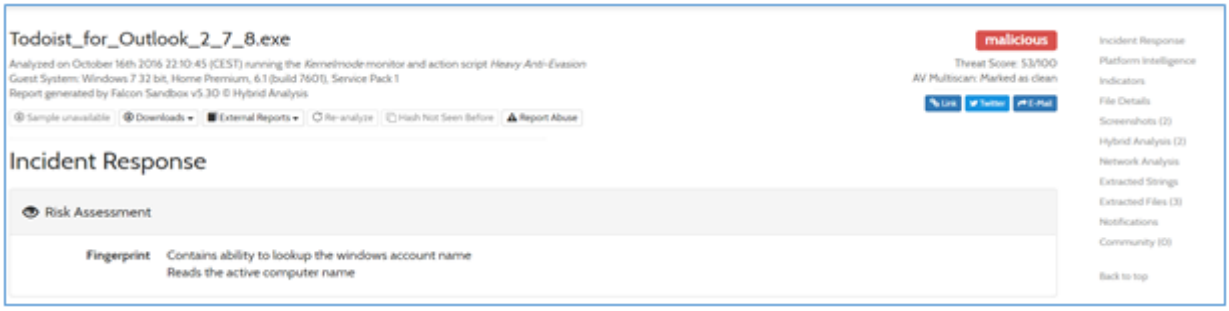


Рисунок 4.44 - Результат тесту: https://www.reverse.it/sample/8cc1d29d4f5e95f4d527158f4ea8460dd0ef7fa79cd508d1c2eec531113240e0?environmentId=100

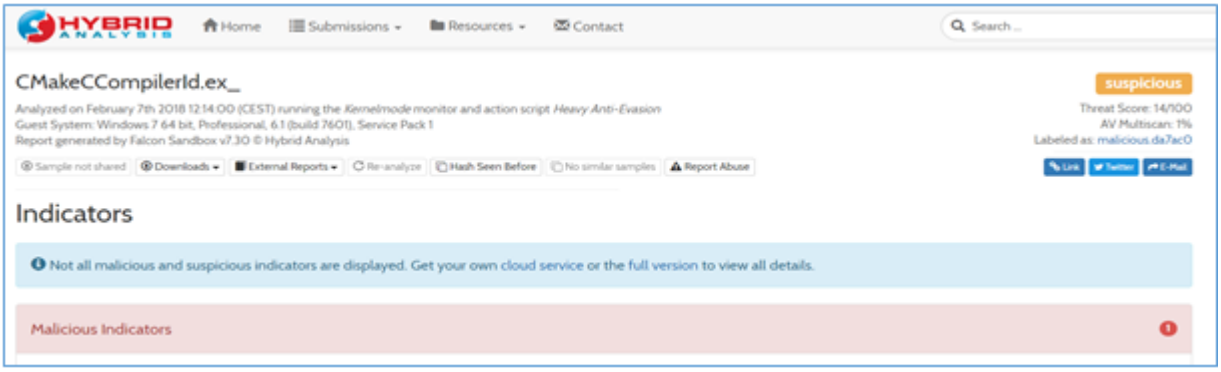


Рисунок 4.45 - Результат тесту: https://www.hybrid-analysis.com/sample/4269a680c35f8f8ecb20f55e3626b2e9dc4bd700e854449dcf599030e8a0be86?environmentId=120

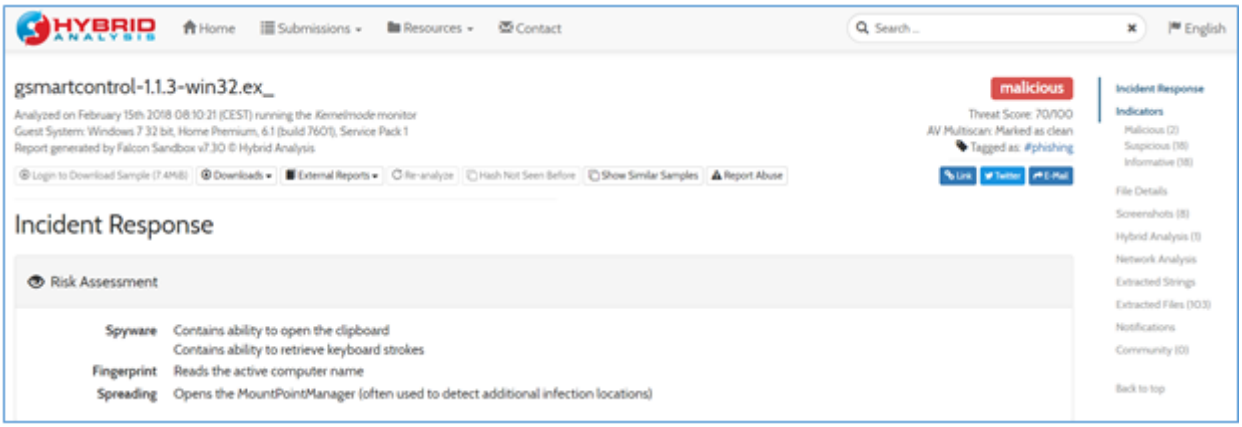


Рисунок 4.46 - Результат тесту:https://www.hybrid-analysis.com/sample/29aa1b4b71677e9e01657325bd214402dcd0724cc5a65f4ff30aab487f990792?environmentId=100

На (рисунок 4.47) нижче представлений інтригуючий фрагмент програмного забезпечення, який було схвалено навіть із тривожними результатами звіту Hybrid Analysis:

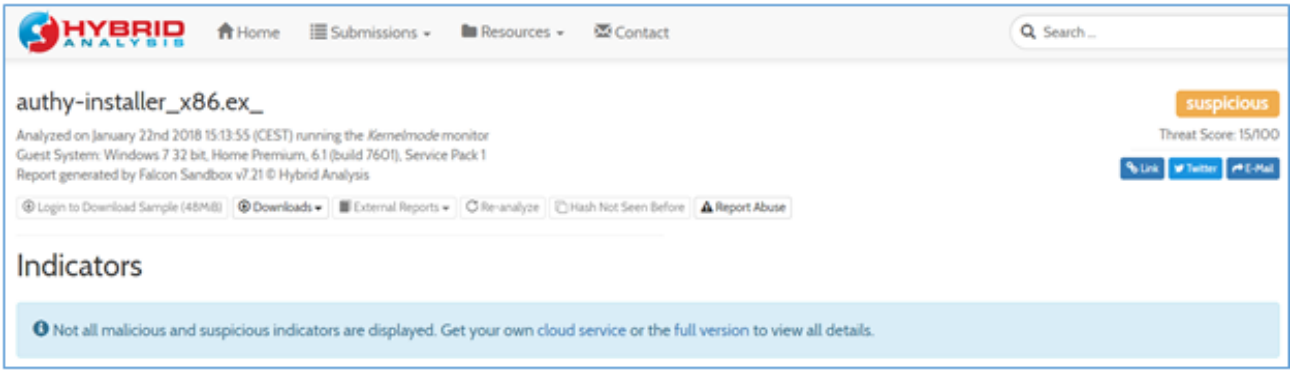


Рисунок 4.47 - Результат тесту: https://www.hybrid-analysis.com/sample/d0e7894f20f42dcf00fb53446c2ecb47063f9b1e2792a567d889a685d3ecad93?environmentId=100

Оригінальний сайт https://authy.com/download/. Це програмне забезпечення використовується для включення 2FA для улюблених сайтів користувача.

Іноді програмне забезпечення може бути дозволене на сервісі аналізу. Наприклад, деякі техніки приховування функцій можна додати до білого списку. Це означає, що ви можете схвалити це програмне забезпечення для використання на підприємстві (рисунок 4.48).

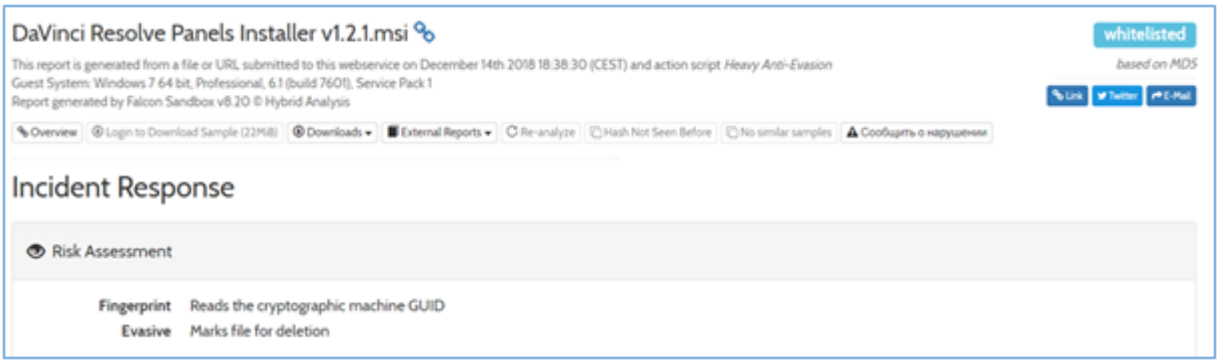


Рисунок 4.48 - Результат тесту: https://www.hybrid-analysis.com/sample/8075501febed956c2af576c8b9ae22e3a3c62e2ea9935df88225a40928bd30e8?environmentId=120

Якщо у вас все ще виникають сумніви щодо білої програми, або програмне забезпечення дійсно популярне, а підозрілий показник Hybrid Analysis не великий (у нашому випадку - 15/100), ми можемо подвоїти його через Symantec https://submit.symantec.com/websubmit/platinum.cgi: (рисунок 4.49)

Рисунок 4.49 - Відповідь безпеки Symantec

Вердикт з гібридного аналізу є дуже цінним, щоб вирішити, чи може цільова безкоштовна програма бути затверджена чи ні, або знайти причину, через яку AV-файли виявляють вбудований файл.

Усі зареєстровані користувачі можуть генерувати безкоштовний публічний ключ API. Крім того, зареєстрований користувач отримує доступ до розширених варіантів пошуку. Ви можете шукати прізвище вірусу, знаходити всі звіти, які зв'язувались з певною IP-адресою, доменом, URL-адресою, мають певний тип файлу, нечіткий хеш, #hashtag, спільний артефакт тощо. Ось вибрані приклади деяких операторів розширеного пошуку:

– host:95.181.53.78

– port:3448
– domain:checkip.dyndns.org
– vxfamily:upatre
– indicatorid:network-6
– filetype:jar
– filetype_tag:hwp
– url:google
– similar-to:hash
– authentihash:hash
– tag:teslacrypt

Щоб зареєструватися в службі Hybrid Analysis, скористайтеся наступним посиланням: https://www.hybrid-analysis.com/signup

InTEZER Analyze

Посилання на інструмент: https://analyze.intezer.com/

На даний момент використовується безкоштовна версія INTEZER Analyse, оскільки функціонал, який вона пропонує, є достатнім для поточних потреб компанії.

Intezer Analyse розбирає двійковий код на тисячі дрібних фрагментів коду (генів) порівнює їх з масовою базою даних, яка містить гени шкідливого програмного забезпечення та законного програмного забезпечення, ефективно забезпечуючи повне відображення ДНК кожного виконуваного файлу.

Підтримувані формати: виконувані файли Windows, такі як .exe, .dll, .sys тощо.

Intezer Analyse не підтримує такі документи, як .pdf, .doc, .ppt, .xls, .odt тощо (рисунок 4.50).

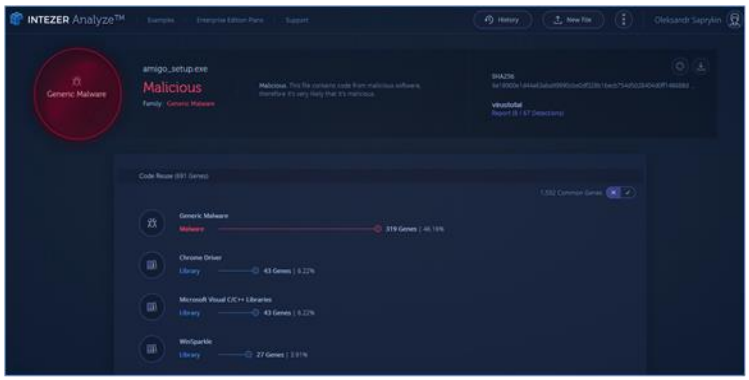


Рисунок 4.50 - Приклад аналізу MailRu Amigo

Показники Intezer є цінними даними при аналізі файлів Windows Executable.

ANY.RUN

Посилання на інструмент: https://app.any.run/.

Any.Run - це інтерактивна онлайн-служба аналізу зловмисного програмного забезпечення для динамічного та статичного дослідження більшості типів загроз з використанням будь-яких середовищ. Він замінює набір інструментів для дослідження.

Він підтримує будь-який тип вмісту, який можна було б відкрити, усі виконувані файли, файли Java, документи Microsoft Office, PDF-файли, сценарії, листи тощо (рисунок 4.51).

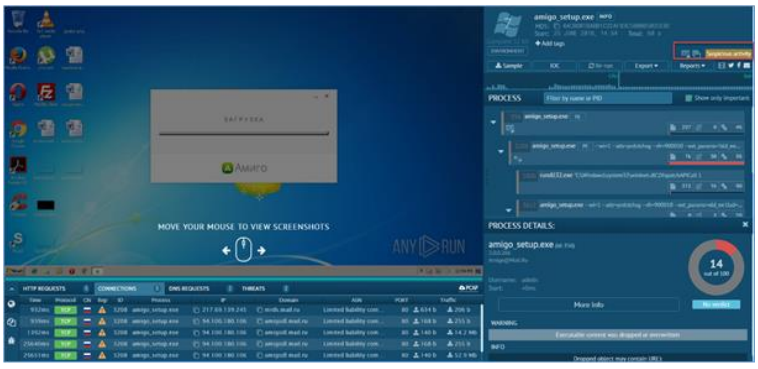


Рисунок 4.51 - Приклад аналізу MailRu Amigo:
https://app.any.run/tasks/59a41675-d5af-44ce-956f-e5e775775d3d

Вердикти Any.Run також можуть бути надіслані одержувачу реквесту як доказовий зв’язок із шкідливими індикаторами для аналізованого файла.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Підчас виконаної атестаційної роботи були проаналізовані моделі та типи архітектур Security Operation Center та фактори що впливають на вибір конкретної моделі Security Operation Center. В результаті були подані рекомендації щодо вибору моделі та архітектури Security Operation Center для підприємства при побудові SOC на підприємстві. Представлено порядок розміщення Security Operation Center на підприємстві.

Було проаналізовано 3 основні компанії що надають SIEM, які можуть впливати на вибір конкретної моделі SOC. На основі цих даних можливо зробити вибір найкращої системи для підприємства. Найбільш привабливим рішенням для підприємства є SIEM Qradar від компанії IBM [11].

Впровадження Security Operation Center на підприємстві дозволяє мінімізувати реалізацію можливих загроз та вирішує такі проблеми як з інформаційної та кібербезпеки:

- контролювати стан інформаційної безпеки:
- моніторити події інформаційної безпеки;
- проводити аудит дій користувачів;
- відстежувати та управляти вразливостями;
- управляти інцидентами з інформаційної безпеки;
- проводити контроль за дотриманням законодавчих вимог, міжнародних та промислових стандартів, внутрішньої політики компанії.

В практичній частині розроблені алгоритми реагування на різні типи інцидентів. Розроблений алгоритм надає можливість прискорити розслідування інцидентів у Security Operation Center підприємства.

Результати виконаної атестаційної роботи на даний час являються актуальними та можуть бути застосовані на підприємствах під час побудови центрів оперативного управління кібербезпекою. Тим самим можуть допомогти при розслідуванні інцидентів з інформаційної та кібербезпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. What is a SOC (Security Operations Center) [Електронний ресурс]. – Режим доступу: http://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html .;

2. Security Information and Event Management [Електронний ресурс]. – Режим доступу: https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem .;

3. S. David. A Practical Application of SIM/SEM/SIEM / Automating Threat Identification. SANS Institute, 2006. p.3. [Електронний ресурс]. – Режим доступу: https://www.sans.org/reading-room/whitepapers/logging/practical-%20application-sim-sem-siem-automating-threat-identification-1781.pdf .;

4. Types of Log Collection Methods (Електрон. ресурс)/Спосіб доступу: URL: https://support.symantec.com/en_US/article.INFO4456.html .;

5. SIEM – Security Information and Event Management [Електронний ресурс]. – Режим доступу: https://amica.ua/siem-security-information-and-event-management/ .;

6. CERT-UA [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/ .;

7. Міжнародний стандарт ISO/IEC 27001:2013 «Система управління інформаційною безпекою. Вимоги» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742 .;

8. Міжнародний стандарт ISO/IEC 27037:2012 «Інформаційні технології. Методи забезпечення безпеки. Настанови щодо ідентифікації, збору, придбання і збереження цифрових даних» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/catalogue_detail?csnumber=4438 .;

9. Корреляція SIEM [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/analytics/431459.php .;

10. HPE ArcSight Marketplace [Електронний ресурс]. – Режим доступу: https://marketplace.microfocus.com/arcsight .;

11. IBM Security App Exchange Marketplace [Електронний ресурс]. –

Режим доступу: https://exchange.xforce.ibmcloud.com/hub .;

12. Міжнародний стандарт ISO/IEC 27005:2011 «Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742 .;

13. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення. [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ru/catalog/doc-page?id_doc=61937 .;

14. Configuring SNMP and using the NetFlow [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/netflow/configuration/12-4t/nf-12-4t-book/cfg-snmp-mib-mon-nf.html .;

15. Kearney, K.T.; Torelli, F. (2011). "The SLA Model". [text] / Wieder, P.; Butler, J.M.; Theilmann, W.; Yahyapour, R. Service Level Agreements for Cloud Computing. Springer Science+Business Media, 2011. – pp. 43–68.;

16. COBIT - Цілі контролю за інформаційними та суміжними технологіями, 2012 р..

17. МАТЕРІАЛИ ПЕРШОГО МІЖНАРОДНОГО НАУКОВО-ПРАКТИЧНОГО ФОРУМУ. GLOBAL CYBER SECURITY FORUM. А. Демидов, В. Караваев. Организация оперативного управления кибербезопасностью на производстве с. 45.