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

ІВАЩЕНКО Микола Васильович

Система пошуку загроз на основі Wazuh та хмарної платформи Google / Threat Detection System Based on Wazuh and Google Cloud Platform

спеціальність: 125 – Кібербезпека

освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБм -21
М.В. Іващенко

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

Кваліфікаційну роботу
допущено до захисту:

«____» _____ 2023 р.

Завідувач кафедри
_____ **В.В.Яцків**

ТЕРНОПІЛЬ - 2023

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

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
«____» _____ 2022 року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

ІВАЩЕНКО МИКОЛА ВАСИЛЬОВИЧ
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Система пошуку загроз на основі Wazuh та хмарної платформи Google / Threat Detection System Based on Wazuh and Google Cloud Platform
керівник роботи д.т.н., професор В.В. Яцків

затверджені наказом по університету від 1 грудня 2022 року № _____

2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 р.

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

4. Основні питання, які потрібно розробити:
– провести аналіз платформ пошуку кіберзагроз;
– проаналізувати можливості та переваги платформи Wazuh;
– дослідити ландшафт загроз кібербезпеці;
– дослідити життєвий цикл аналізу загроз;
– інтегрувати Wazuh з управлінням хмарною безпекою;
– розробити мніторинг цілісності файлів на основі Wazuh.

5. Перелік графічного матеріалу у роботі:
- Ланцюг Cyber Kill;
- Високорівневий процес виявлення загроз;
- Процес високого рівня пошуку загроз;
- Життєвий цикл аналізу загроз;
- Події Wazuh MITER ATT&CK;
- Інтеграції Google Cloud Platform із Wazuh.

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз систем пошуку та аналізу кіберзагроз	12.2021 р. – 03.2022 р.	
2	Структура системи пошуку загрози	03.2022 р. – 05.2022 р.	
3	Розробка та дослідження системи пошуку загроз	05.2022 р. – 11.2022 р.	

Студент _____ Іващенко М.В.
(підпис)

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

АНОТАЦІЯ

Кваліфікаційна робота на тему «Система пошуку загроз на основі Wazuh та хмарної платформи Google» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека» освітньо-професійної програми «Кібербезпека» написана обсягом 7 сторінок і містить 41 ілюстрація, 1 додаток та 32 джерела за переліком посилань.

Метою роботи є підвищення ефективності пошуку та аналізу кіберзагроз.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи пошуку кіберзагроз, методи аналізу інформації про загрози, методи захисту цілісності файлів.

Результати дослідження. Удосконалено систему пошуку загроз на основі Wazuh для управління хмарною безпекою.

Розроблено алгоритм моніторингу цілісності файлів з використанням платформи Wazuh, який дозволяє контролювати цілісність файлів в локальних та хмарних платформах.

Результати роботи можуть бути застосовані для пошуку нових загроз та виявлення атак та порушення безпеки.

Ключові слова: ПОШУК КІБЕРЗАГРОЗ, WAZUH, ЛАНДШАФТ КІБЕРЗАГРОЗ, MITER ATT&CK.

ABSTRACT

Qualification work on "Threat Detection System Based on Wazuh and Google Cloud Platform" for the degree of "Master" in the specialty 125 "Cybersecurity" educational and professional program "Cybersecurity" is written in 78 pages and contains 41 illustrations, 1 appendice and 32 sources according to the list of links.

The purpose of the work is to increase the effectiveness of the search and analysis of cyber threats.

Research methods. To solve the tasks in this qualification work, the following methods were used: methods of searching for cyber threats, methods of analysing information about threats, methods of protecting the integrity of files.

Research results. Improved Wazuh-based threat detection system for cloud security management.

An algorithm for monitoring the integrity of files using the Wazuh platform has been developed, which allows you to control the integrity of files in local and cloud platforms.

The results of the work can be applied to search for new threats and detect attacks and security breaches.

Keywords: CYBER THREAT SEARCH, WAZUH, CYBER THREAT LANDSCAPE, MITER ATT&CK.

ЗМІСТ

ВСТУП

Актуальність роботи. Враховуючи зростаючі виклики в кібербезпеці та збільшення обсягу даних, що генеруються в усьому світі, адміністратори мереж і систем безпеки стикаються з дедалі більшими проблемами пов’язаними різноманітними загрозами.

Загроза – будь-яка обставина чи подія, яка потенційно може негативно вплинути на діяльність організації (включаючи місію, функції, імідж або репутацію), активи організації або осіб через інформаційну систему шляхом несанкціонованого доступу, знищення, розкриття, зміни інформації та/або відмови в обслуговування. Крім того, потенціал для джерела загроз успішно використовувати певну вразливість інформаційної системи.

Інтелектуальні дані про загрози – це дані, які збираються, обробляються та аналізуються, щоб зрозуміти мотиви, цілі та поведінку атаки суб’єкта загрози. Інтелектуальні дані про загрози дають змогу приймати швидші й обґрунтованіші рішення щодо безпеки на основі даних і змінювати їхню поведінку з реактивної на проактивну в боротьбі із загрозливими суб’єктами.

Організації все більше визнають цінність пошуку та аналізу загроз. Однак, більшість організацій сьогодні зосереджують свої зусилля лише на найпростіших випадках використання, таких як інтеграція каналів даних про загрози з існуючою мережею, системи попередження загроз, міжмережевими екранами та SIEM, не користуючись повною мірою перевагами інформації, яку може запропонувати розвідка. На даний час існує багато рішень для пошуку загроз та моніторингу безпеки. Одним із інструментів, який допомагає ідентифікувати та виявляти атаки, є Wazuh.

Wazuh – це інструмент, який використовується в різних цілях у всьому світі. Wazuh можна використовувати для тестування рішень, які виявляють атаки всередині створеної приманки.

Мета і завдання дослідження. Метою роботи є підвищення ефективності пошуку та аналізу кіберзагроз.

Досягнення визначеної мети передбачає вирішення таких завдань:

– провести аналіз платформ пошуку кіберзагроз;

– проаналізувати можливості та переваги платформи Wazuh;

– дослідити ландшафт загроз кібербезпеці;

– дослідити життєвий цикл аналізу загроз;

– інтегрувати Wazuh з управлінням хмарною безпекою;

– розробити мніторинг цілісності файлів на основі Wazuh.

Об’єкт дослідження – процеси пошуку та аналізу кіберзагроз;

Предмет дослідження – системи та алгоритми пошуку та аналізу кіберзагроз.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи пошуку кіберзагроз, методи аналізу інформації про загрози, методи захисту цілісності файлів.

Наукова новизна одержаних результатів. Удосконалено систему пошуку загроз на основі Wazuh для управління хмарною безпекою.

Практичне значення отриманих результатів. Розроблено алгоритм моніторингу цілісності файлів з використанням платформи Wazuh, який дозволяє контролювати цілісність файлів в локальних та хмарних платформах.

Публікації та апробація КР.

1. Гарматюк В.Р., Понедєльніков Г.М., Іващенко М.В. Життєвий цикл розвідки загроз. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ - 2023), Тернопіль, 2023. – С. 71–73

2. Іващенко М.В., Кондратюк В.М. Алгоритм впровадження Wazuh у хмарному середовищі. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2023. – С. 74-75.

1 АНАЛІЗ СИСТЕМ ПОШУКУ ТА АНАЛІЗУ КІБЕЗЗАГРОЗ

1.1 Платформи аналізу загроз

Щодня з’являються нові загрози та вразливості, які постійно розвиваються. Аналітики безпеки знають, що ключ до того, щоб випередити ці загрози, полягає в аналізі даних про них, але з такою кількістю різних джерел інформації командам важко ефективно аналізувати великі обсяги даних і отримувати корисну інформацію [1, 2].

Такі інструменти, як антивірус, брандмауери та шлюзи, часто включають власні канали загроз від постачальника; однак клієнти часто відчувають затримку між виявленням індикатора загрози (сигнатури зловмисного програмного забезпечення, зловмисної URL-адреси тощо) та включенням цієї інформації в офіційний канал загроз постачальника. Платформи аналізу загроз доповнюють офіційні канали постачальників різноманітними каналами загроз, щоб скоротити затримки.

Рішення аналізу загроз та інструменти управління інформацією про безпеку та подіями (SIEM) допомагають групам безпеки аналізувати події журналу; однак їхня спрямованість є чіткою. Інструменти SIEM зосереджені на консолідації, пріоритезації та зберіганні внутрішніх журналів подій, тоді як канали розвідки зосереджені на зовнішніх сповіщеннях і можуть не зберігати дані для майбутніх розслідувань.

Для професіоналів безпеки володіння передовими знаннями є вирішальним сприятливим фактором. Перш ніж розглядати преміум-версії, доцільно поекспериментувати з безкоштовними джерелами аналізу загроз, які надають перевірену та своєчасну інформацію.

Численні інструменти CTI (Cyber Threat Intelligence) можуть виявитися корисними на різних етапах циклу розвідки. Хоча ці інструменти не можуть бути комплексними рішеннями, окрім полегшення автоматизованого збору, зберігання, спільного використання й аналізу даних, вони можуть заощадити

значні фінансові інвестиції, які не можуть собі дозволити багато малих і середніх компаній.

1.1.1 Відкритий обмін загрозами AlienVault

AlienVault Open Threat Exchange (OTX) пропонує відкритий доступ до глобальної спільноти дослідників загроз і експертів з безпеки. Він надає дані про загрози, створені спільнотою, сприяє спільним дослідженням і автоматизує процес оновлення інфраструктури безпеки за допомогою даних про загрози з будь-якого джерела (рисунок 1.1) [3].

Ця платформа служить оригінальним краудсорсинговим корпусом аналізу загроз і залишається однією з найкращих, щодня обробляючи понад 19 мільйонів нових записів індикаторів компрометації (IoC). Сервіс є безкоштовним для використання та пропонує інформацію про загрози в різних форматах, включаючи формати STIX, OpenIoC, JSON, MAEC і CSV. Кожен зразок даних називається «імпульсом».

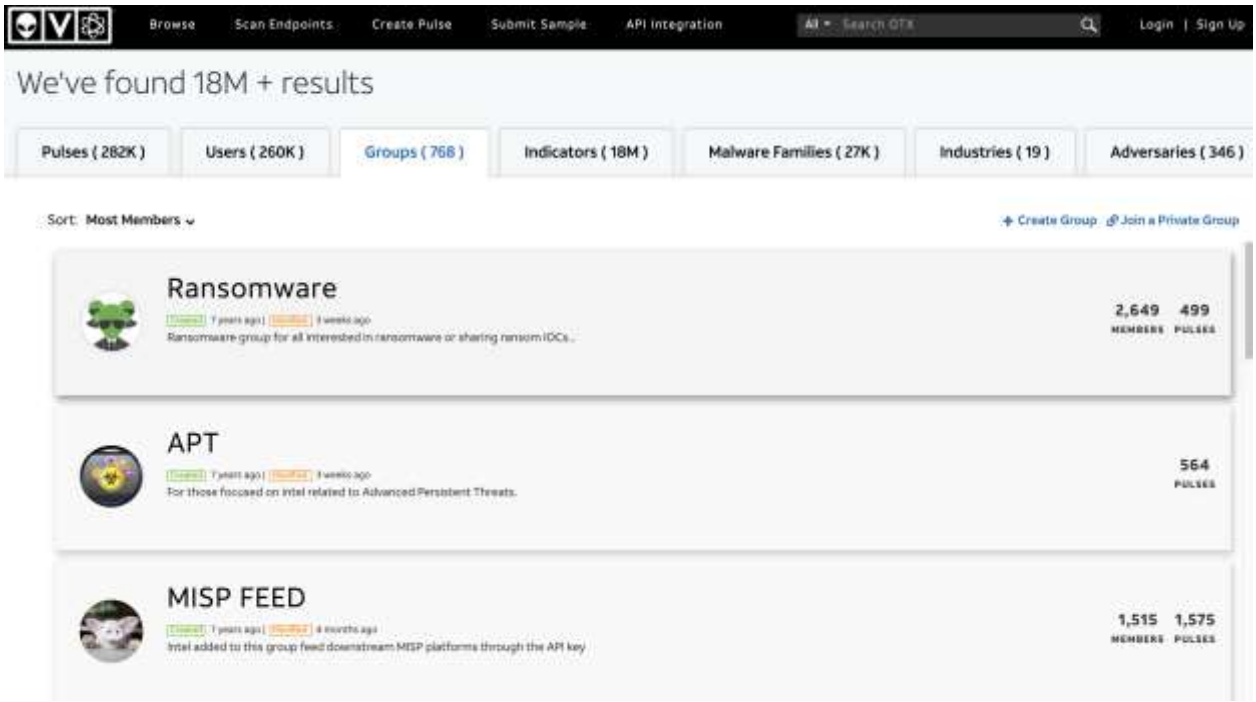

Рисунок 1.1 – Сторінка груп AlienVault

Ви маєте можливість визначати свої конкретні вимоги, отримуючи певні попередньо відфільтровані дані, а також є можливість отримувати канали, адаптовані до типів пристроїв, наприклад кінцевих точок. Якщо відповідні дані виходять за межі параметрів каналу, ці додаткові дані зв’язуються в наданих записах.

1.1.2 Платформа CTI4SOC

Нове автономне рішення CTI від SOC Radar, CTI4SOC – це платформа аналізу загроз наступного покоління, призначена для полегшення роботи аналітиків SOC. Вона служить унікальним помічником для команд SOC завдяки 12 функціональним модулям (рисунок 1.2) [4].

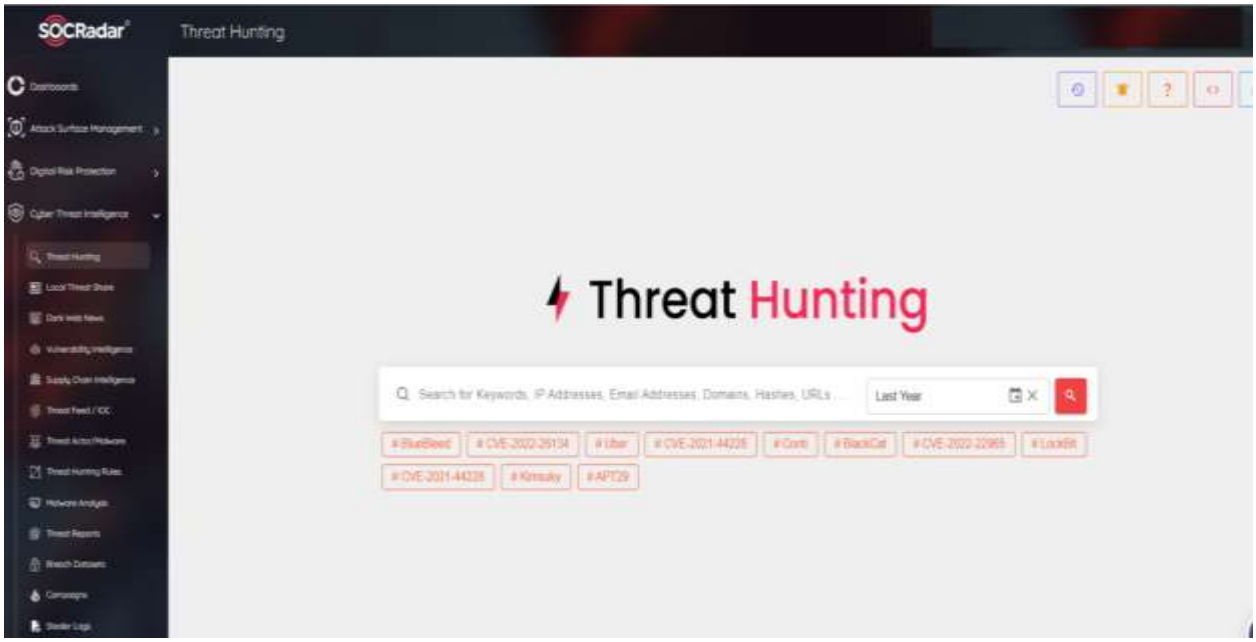

Рисунок 1.2 – Модуль пошуку загроз SOCRadar

На відміну від традиційних платформ аналізу загроз, CTI4SOC працює на основі великих даних і представляє всі дані, які аналітики можуть отримати за допомогою різних інструментів, у організованому та контекстному вигляді.

З CTI4SOC командам SOC не потрібно шукати правдиву та корисну інформацію в різних джерелах інформації. Платформа відбирає та фільтрує

інформацію очима аналітика, надаючи фахівцям правильну гіпотезу для початку дослідження.

Платформа не лише збирає корисну інформацію, але й подає її в контексті, який можна застосувати. Вона пропонує доступ одним натисканням до звітів про загрози, опублікованих аналітиками безпеки SOCRadar та іншими надійними джерелами.

У сучасному ландшафті загроз, що постійно змінюється, деякі суб'єкти загрози можуть націлюватися лише на певні сектори та мати власні відмінні характеристики. Розуміння аналітиком SOC тактики, прийомів, процедур (TTP), мотивації та моделей поведінки цих супротивників безпосередньо сприяє процесу розслідування, допомагаючи їм сформувати добре поінформовану точку зору. За допомогою CTI4SOC ви можете додавати активних акторів загроз до списків спостереження, щоб бути в курсі їхніх дій.

Модуль пошуку загроз SOCRadar є найціннішим інструментом аналітика SOC після етапу розслідування. Звідти співробітники служби безпеки можуть розширити свою роботу, шукаючи критично важливу інформацію, таку як центри управління (C2), зловмисне програмне забезпечення, IP-адреси та домени. CTI4SOC – це готове до API рішення, яке дозволяє всім цим корисним даним бути легкодоступними у разі можливої атаки.

1.1.3 Служба DOCGuard

DOCGuard – це служба аналізу зловмисного програмного забезпечення, яка інтегрується з рішеннями Secure Email Gateways (SEG) і SOAR. Сервіс використовує новий тип статичного аналізу, відомий як структурний аналіз. Цей метод розбиває зловмисне програмне забезпечення на частини та передає їх до основних механізмів на основі компонентів файлової структури. Застосовуючи цей підхід, DOCGuard може однозначно виявляти зловмисне програмне забезпечення, витягувати індикатори компрометації

(IoC) без F/P (без помилкових спрацьовувань) і ідентифікувати обфускацію та шифрування у формі кодування послідовності та шифрування документів. Наразі підтримувані типи файлів включають файли Microsoft Office, PDF, LNK, HTML, HTM, ISO, IMG, JScript, VHD, VCF та архіви (.zip, .rar, .7z тощо). Детальні результати структурного аналізу представлені в зведеному вигляді в графічному інтерфейсі користувача та можуть бути завантажені як звіт у форматі JSON. Ці висновки також можна збирати через API. Революційний аналізатор DOCGuard дозволяє аналізувати файли за лічені секунди та виявляти всі відомі методи атак, не пропускаючи жодної. Крім того, він виконує цей аналіз із дуже низьким використанням системних ресурсів. DOCGuard полегшує автоматизацію перевірки сповіщень із різних джерел, таких як рішення SIEM і SOAR, PhishMe, Cofense тощо. Сервіс пропонує швидкий аналіз зразків і легко інтегрується з екосистемою кібербезпеки за лічені хвилини за допомогою інтерфейсу API. DOCGuard можна легко встановити, розгорнувши контейнер Docker та інтегрувавши його у свою інфраструктуру кібербезпеки (рисунок 1.3) .

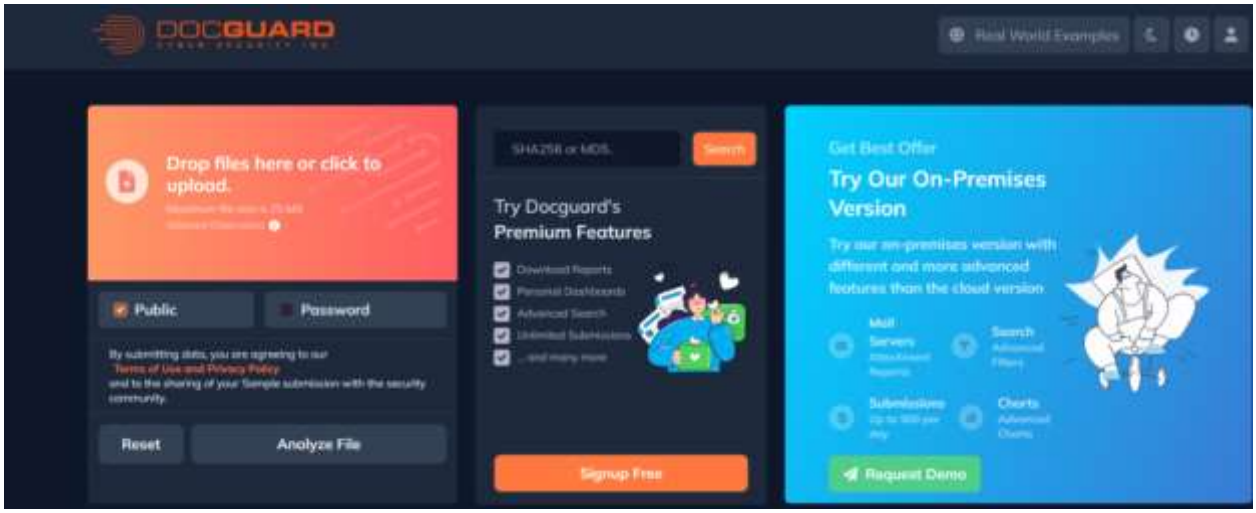

Рисунок 1.3 – Безкоштовна сторінка аналізу файлів DOCGuard

VirusTotal нещодавно оголосив, що співпраця з аналізом документів, інтегрована з DOCGuard, дозволить спільноті по-іншому поглянути на відскановані документи.

1.1.4 Платформа GreyNoise

GreyNoise забезпечує видимість і глибокий контекст для аналітиків і мисливців за загрозами Cyber Threat Intelligence (CTI). Він збирає та аналізує дані про активність веб-перегляду в Інтернеті, допомагаючи зменшити помилкові спрацьовування під час аналізу інформації про загрози. GreyNoise збирає інформацію про безпечні сканери, такі як Shodan, а також про зловмисників, таких як SSH і хробаки Telnet. Крім того, він визначає шумові дані, які може пропустити аналітик SOC (рисунок 1.4).

GreyNoise визначає веб-браузери та загальну бізнес-активність у ваших подіях безпеки, забезпечуючи швидше та безпечніше прийняття рішень. Незалежно від того, використовуєте ви його Viewer, API чи інтегруєте дані GreyNoise у свої інструменти безпеки, ви можете знайти те, що має значення, у своїх журналах безпеки та повернутися до роботи.

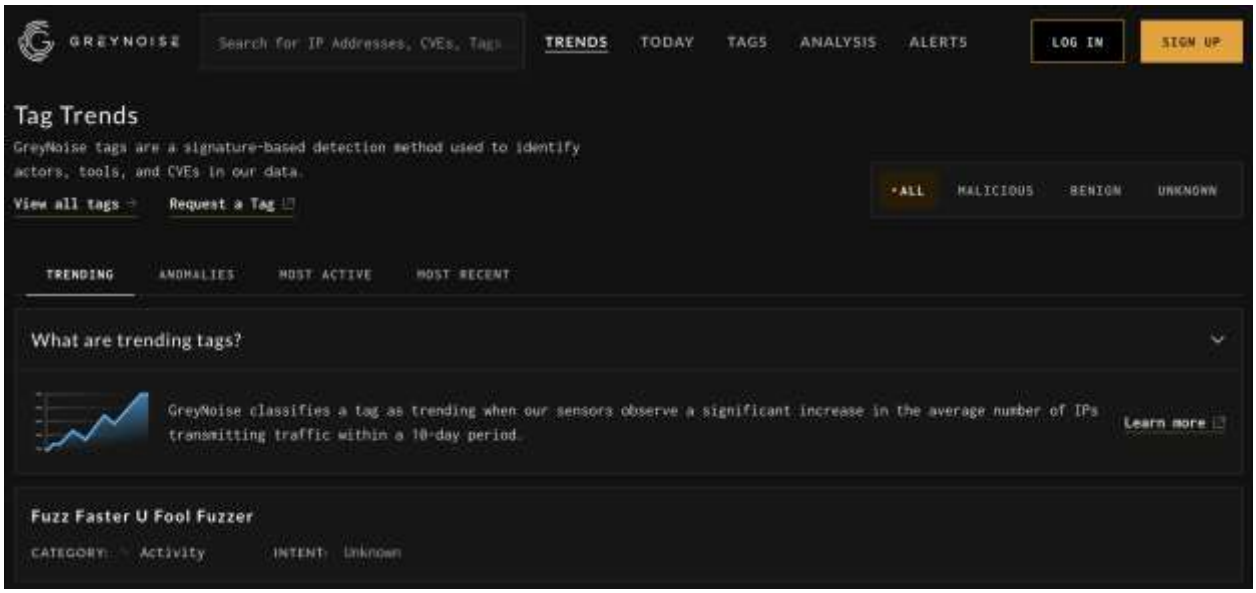

Рисунок 1.4 – Сторінка тенденцій тегів GreyNoise

Інтеграція GreyNoise дозволяє легко збагачувати дані на платформі аналізу загроз (TIP) і допомагає усунути шум і помилкові спрацьовування, з якими команди CTI зазвичай стикаються під час прийому різних джерел розвідувальної інформації. Мисливці за загрозами можуть дозволити

GreyNoise виявляти аномальні шаблони в тактиці, техніці та процедурах (TTP), таким чином виявляючи ворожі кампанії та інфраструктуру. Вони також можуть глибоко зануритися в показники компрометації (IoCs) за допомогою інструменту GreyNoise Analysis, щоб прискорити розслідування.

1.1.5 Платформа Intezer

Intezer – це платформа, призначена для аналізу та дослідження сповіщень, як досвідчений аналітик безпеки та реверс-проектування (рисунок 1.5).

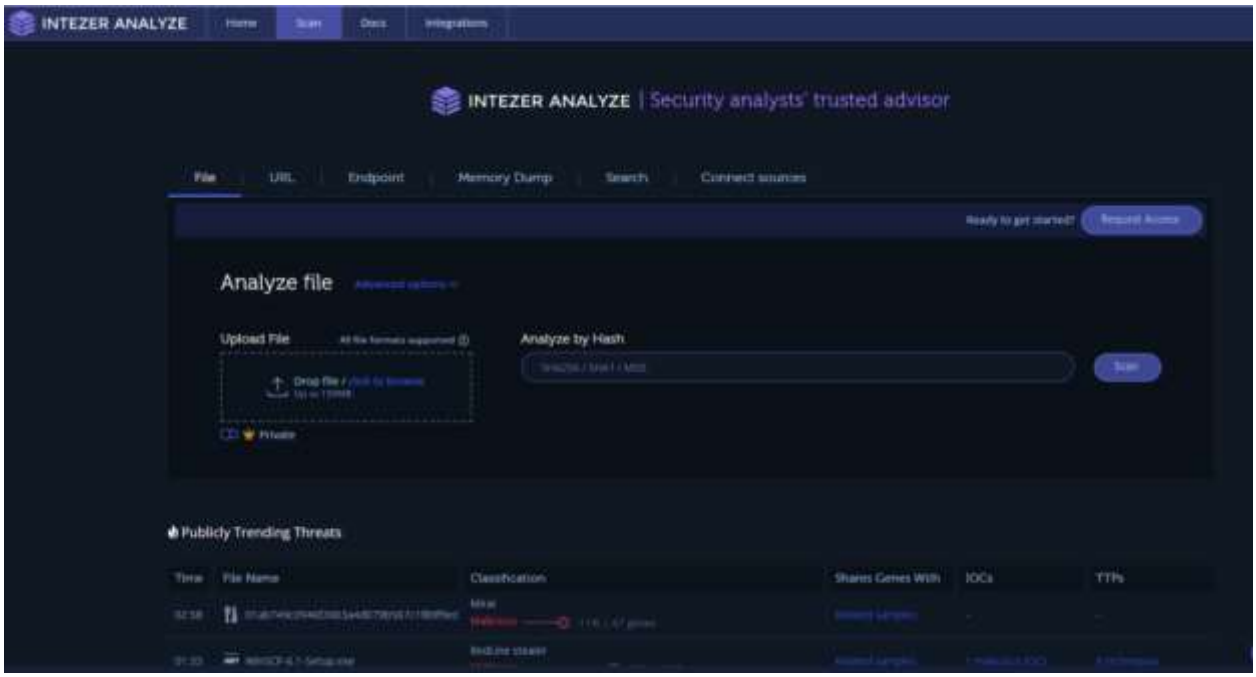

Рисунок 1.5 – Сторінка аналізу Intezer

Протягом багатьох років Intezer вдосконалювала та розширювала можливості свого власного механізму аналізу коду для автоматизації завдань, що потребують все більше часу або повторюються для команд SOC. Це виходить за рамки автоматизованих ігор, ізольованого програмного середовища чи збагачення сповіщень, щоб діяти, приймати розумні рішення та надавати рекомендації команді щодо реагування на інциденти.

Платформа Self-Directed SOC від Intezer визначає пріоритетність сповіщень і розслідує загрози для команди 24/7. Використовуючи автоматичний аналіз, інтелектуальні рекомендації та автоматизоване виправлення, Intezer позбавляє команду від витрачання часу на помилкові спрацьовування, повторювані завдання аналізу та обробку надто великої кількості сповіщень високого рівня, що потребують багато часу.

Intezer Analyze – це комплексна платформа для аналізу зловмисного програмного забезпечення, яка може виконувати статичний, динамічний і генетичний аналіз коду файлів будь-якого типу. Це допомагає реагувати на інциденти та спрощувати командам SOC розслідування будь-якого інциденту, пов’язаного зі шкідливим програмним забезпеченням. Користувачі можуть відстежувати сімейства шкідливих програм, видобувати IoC/MITRE TTP і завантажувати підписи YARA. Існує також версія для спільноти, щоб почати безкоштовно.

За допомогою Intezer Transformations аналітики зловмисного програмного забезпечення та дослідники загроз можуть швидко отримати відповіді щодо будь-якого підозрілого файлу чи кінцевої точки, класифікувати підозрілі файли та машини за лічені секунди, прискорити час відповіді та об’єднати кілька інструментів аналізу зловмисного програмного забезпечення в один.

Intezer забезпечує своєчасне поглиблене звітування та вважається «обов’язковим», щоб мати спеціальний екземпляр для завантаження потенційно конфіденційних даних і автоматичного визначення пріоритетів і дослідження кожного сповіщення. Платформа надає лише підтверджені серйозні загрози.

1.1.6 Платформа MISP

MISP, яка раніше називалася Malware Information Sharing Platform, є безкоштовною платформою аналізу загроз із відкритим кодом і відкритими стандартами для обміну інформацією про загрози. Вона була створена CIRCL

і надає функції для збору, зберігання, розповсюдження та обміну загрозами кібербезпеки, пов'язаними з інцидентами кібербезпеки та аналізом шкідливих програм (рисунок 1.6).

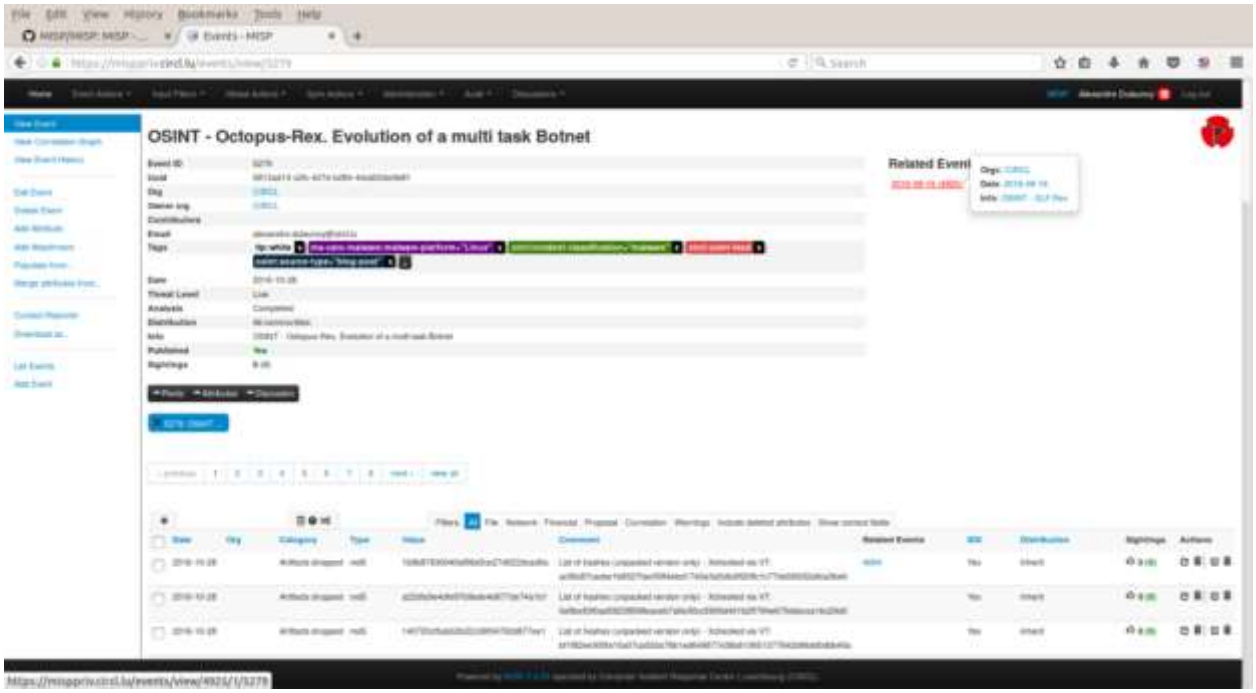

Рисунок 1.6 – Модуль перегляду подій MISP

MISP дозволяє співвідносити індикатори компрометації (IoC) у базі даних з атрибутами та індикаторами зловмисного програмного забезпечення, атак або кампаній. Вона розроблена аналітиками SOC, фахівцями з безпеки та ІКТ, а також розробниками зловмисного програмного забезпечення для підтримки їхніх щоденних операцій і ефективного обміну структурованою інформацією.

У міру розширення проекту MISP вона почала охоплювати не лише індикатори зловмисного програмного забезпечення, але й інформацію про шахрайство та вразливості. Тепер вана називається MISP, яка включає основне програмне забезпечення MISP і безліч інструментів (PyMISP) і форматів (основний формат, таксономії MISP, списки попереджень) для підтримки MISP. MISP тепер є громадським проектом, який очолює команда волонтерів.

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

Основні функції MISP, платформи обміну інформацією про зловмисне програмне забезпечення та обміну інформацією про загрози включають.

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

Автоматизована кореляція для пошуку зв'язків між атрибутами та індикаторами зловмисного програмного забезпечення, кампаній атак або аналізів.

Гнучка модель даних, у якій складні об'єкти можна виражати та зв'язувати разом, щоб виражати дані про загрози, події або пов'язані елементи.

Вбудована функція обміну для полегшення обміну даними за допомогою різних моделей розподілу.

Інтуїтивно зрозумілий інтерфейс користувача для створення, оновлення та спільної роботи над подіями та атрибутами/індикаторами.

Гнучкий API для інтеграції MISP із вашими власними рішеннями. MISP поставляється з PyMISP, гнучкою бібліотекою Python для доступу до платформ MISP через їхній REST API, що дозволяє отримувати події, додавати або оновлювати події/атрибути, додавати або оновлювати зразки зловмисного програмного забезпечення або шукати атрибути.

Регульована таксономія для класифікації та позначення подій відповідно до ваших схем класифікації або існуючої таксономії.

Словники розвідки під назвою галактика MISP, яка включає існуючі загрози, зловмисне програмне забезпечення, RAT, програми-вимагачі або MITER ATT&CK, можна легко пов'язати з подіями та атрибутами в MISP.

1.1.7 Платформа OpenCTI

OpenCTI – відкрита платформа аналізу кіберзагроз. Проект OpenCTI, уніфікована платформа для всіх рівнів Open Cyber Threat Intelligence, є інструментом, призначеним для полегшення обробки та обміну інформацією для цілей аналізу кіберзагроз. Це результат співпраці між Групою реагування на комп'ютерні надзвичайні ситуації (CERT-EU) і Національним агентством кібербезпеки Франції (ANSSI) (рисунок 1.7).

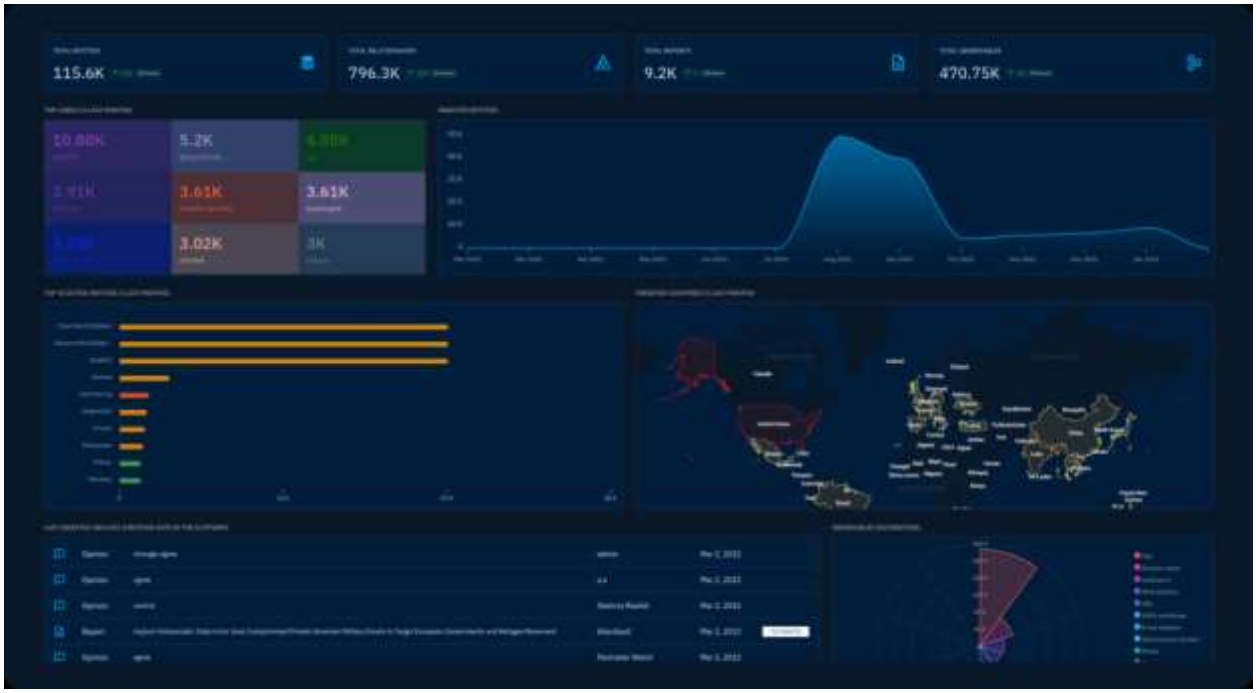

Рисунок 1.7 – Інформаційна панель OpenCTI

OpenCTI – це платформа з відкритим вихідним кодом, яка дозволяє організаціям керувати своєю розвідувальною інформацією про кіберзагрози (CTI) і спостережуваними об'єктами. ЇЇ було створено для зберігання, організації та візуалізації технічної та нетехнічної інформації про кіберзагрози.

Структурування даних здійснюється за допомогою інформаційної схеми на основі стандартів STIX2. Вона розроблена як сучасна веб-програма, яка включає GraphQL API та інтерфейс, орієнтований на взаємодію з

користувачем (UX). ЇЇ також можна інтегрувати з іншими інструментами та програмами, такими як MISP, TheHive, MITRE ATT&CK тощо.

Деякі з ключових елементів, включених до цієї платформи аналізу загроз, такі:

– OpenCTI надає пов’язану оперативну та стратегічну розвідувальну інформацію через єдину модель даних на основі стандартів STIX2;

– автоматизовані робочі процеси: механізм автоматично робить логічні висновки, щоб надати інформацію та підключення в реальному часі;

– інтеграція з екосистемою інформаційних технологій: її дизайн із відкритим вихідним кодом забезпечує просту інтеграцію з будь-якою рідною системою чи системою третьої сторони;

– інтелектуальна візуалізація даних дозволяє аналітикам візуально представляти сутності та їхні зв’язки, включаючи вкладені зв’язки, використовуючи різні параметри відображення;

– інструменти аналізу: кожна інформація та індикатор пов’язані з основним джерелом, з якого вони надійшли, щоб полегшити аналіз, підрахунок балів і виправлення.

OpenCTI – це структура, яка включає інтерфейси API Python або Go та потужний веб-інтерфейс.

1.1.9 Платформа VirusTotal

VirusTotal перевіряє елементи за допомогою понад 70 антивірусних сканерів і служб блокування URL/доменів, а також численні інструменти для вилучення сигналів із аналізованого вмісту. Будь-який користувач може використовувати свій браузер, щоб вибрати файл зі свого комп’ютера та надіслати його до VirusTotal. Платформа пропонує кілька методів надсилання файлів, включаючи основний загальнодоступний веб-інтерфейс, інсталятори для робочого столу, розширення браузера та програмний API. Веб-інтерфейс має найвищий пріоритет серед публічних методів подання. Подання можна робити будь-якою мовою програмування за допомогою публічного API на

основі HTTP. Так само URL-адреси можна надсилати різними способами, включаючи веб-сторінку VirusTotal, розширення браузера та API.

Коли надсилається файл або URL-адреса, відповідні результати передаються відправнику, а також партнерам із перевірки, які використовують результати для покращення власної безпеки. Таким чином, надсилаючи файли, URL-адреси, домени до VirusTotal, ви долучаєтесь до підвищення глобального рівня безпеки (рисунок 1.9).

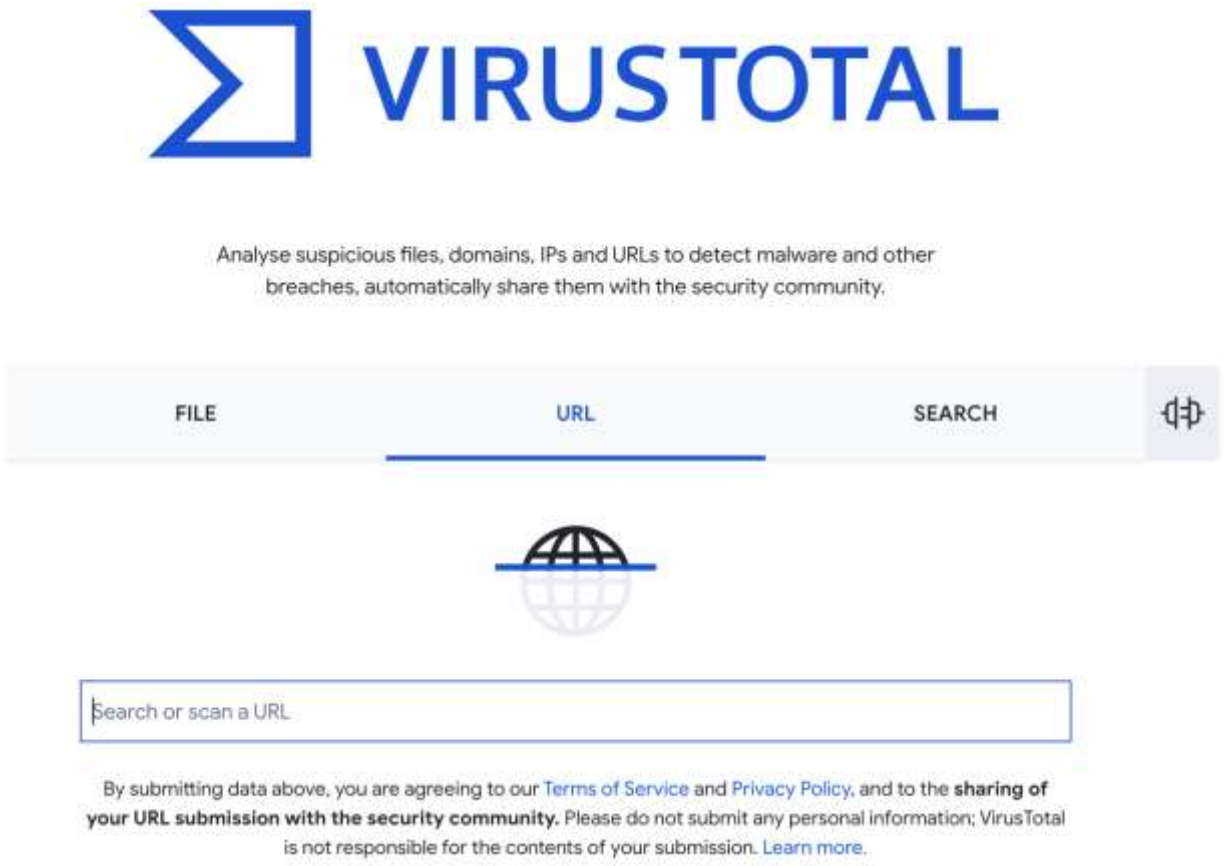

Рисунок 1.8 – Публічна сторінка VirusTotal

Цей базовий аналіз також служить основою для багатьох інших функцій, включаючи мережу, яка дозволяє користувачам коментувати файли та URL-адреси та ділитися нотатками один з одним.

VirusTotal виявився корисним для виявлення шкідливого вмісту та ідентифікації помилкових спрацьовувань. Крім того, VirusTotal сповіщає користувачів, коли антивірусне рішення визначає надісланий файл як

шкідливий і відображає мітку виявлення. Крім того, більшість сканерів URL-адрес розрізняють типи веб-сайтів, зокрема зловмисне програмне забезпечення, фішингові та підозрілі.

1.2 Платформа Wazuh

Wazuh – це безкоштовна платформа з відкритим кодом, яка використовується для запобігання загрозам, їх виявлення та реагування. Вона здатна захищати робочі навантаження в локальних, віртуалізованих, контейнерних та хмарних середовищах.

Рішення Wazuh складається з агента безпеки кінцевої точки, розгорнутого в системах, що контролюються, і сервера керування, який збирає й аналізує дані, зібрані агентами. Крім того, Wazuh був повністю інтегрований з Elastic Stack, забезпечуючи пошукову систему та інструмент візуалізації даних, який дозволяє користувачам переміщатися між своїми сповіщеннями безпеки.

1.3.1 Можливості Wazuh

Проведемо аналіз деяких найбільш поширених випадків використання рішення Wazuh.

Виявлення вторгнень. Агенти Wazuh сканують контрольовані системи на наявність шкідливого програмного забезпечення, руткітів і підозрілих аномалій. Вони можуть виявляти приховані файли, замасковані процеси або незареєстровані мережеві слухачі, а також невідповідності у відповідях на системні виклики.

На додаток до агентських можливостей, серверний компонент використовує підхід до виявлення вторгнень на основі сигнатур, використовуючи механізм регулярних виразів для аналізу зібраних даних журналу та пошуку ознак компрометації.

Аналіз даних журналу. Агенти Wazuh читають журнали операційної системи та програм і безпечно пересилають їх до центрального менеджера для аналізу та зберігання на основі правил. Якщо агент не розгорнуто, сервер також може отримувати дані через системний журнал від мережевих пристроїв або програм.

Правила Wazuh допомагають вам повідомити про помилки програми або системи, неправильні конфігурації, спроби та/або успішні зловмисні дії, порушення політики та низку інших питань безпеки та роботи.

Контроль цілісності файлів. Wazuh відстежує файлову систему, виявляючи зміни у вмісті, дозволах, власності та атрибутах файлів, за якими потрібно стежити. Крім того, він ідентифікує користувачів і програми, які використовуються для створення або зміни файлів.

Можливості моніторингу цілісності файлів можна використовувати в поєднанні з аналізом загроз для виявлення загроз або скомпрометованих хостів. Крім того, цього вимагають деякі нормативні стандарти відповідності, наприклад PCI DSS.

Виявлення вразливостей. Агенти Wazuh збирають дані інвентаризації програмного забезпечення та надсилають цю інформацію на сервер, де вона співвідноситься з постійно оновлюваними базами даних CVE (Common Vulnerabilities and Exposure), щоб ідентифікувати добре відоме вразливе програмне забезпечення.

Автоматизована оцінка вразливості допомагає вам знайти слабкі місця у ваших критично важливих активах і вжити заходів для виправлення, перш ніж зловмисники використають їх для саботування вашого бізнесу або викрадення конфіденційних даних.

Оцінка конфігурації. Wazuh відстежує параметри конфігурації системи та програм, щоб переконатися, що вони відповідають вашим політикам безпеки, стандартам і/або посібникам із захисту. Агенти виконують періодичне сканування, щоб виявити програми, які, як відомо, є вразливими, невиправленими або ненадійно налаштованими.

Крім того, перевірки конфігурації можна налаштувати, адаптуючи їх відповідно до вашої організації. Сповіщення містять рекомендації щодо кращої конфігурації, посилання та зіставлення з нормативною відповідністю.

Реагування на інцидент. Wazuh надає готові активні відповіді для виконання різноманітних заходів протидії активним загрозам, наприклад блокування доступу до системи з джерела загрози, коли виконуються певні критерії.

Крім того, Wazuh можна використовувати для віддаленого запуску команд або системних запитів, ідентифікації індикаторів компрометації (IOC) і допомоги у виконанні інших завдань криміналістики або реагування на інциденти.

Відповідність нормативним вимогам. Wazuh забезпечує деякі необхідні засоби контролю безпеки, щоб відповідати галузевим стандартам і правилам. Ці функції в поєднанні з масштабованістю та підтримкою кількох платформ допомагають організаціям відповідати вимогам технічної відповідності.

Wazuh широко використовується компаніями з обробки платежів і фінансовими установами для відповідності вимогам PCI DSS (Payment Card Industry Data Security Standard). Його веб-інтерфейс користувача надає звіти та інформаційні панелі, які можуть допомогти з цим та іншими правилами (наприклад, GPG13 або GDPR).

Хмарна безпека. Wazuh допомагає контролювати хмарну інфраструктуру на рівні API, використовуючи модулі інтеграції, які можуть отримувати дані безпеки від відомих хмарних провайдерів, таких як Amazon AWS, Azure або Google Cloud. Крім того, Wazuh надає правила для оцінки конфігурації вашого хмарного середовища, легко виявляючи слабкі місця.

Крім того, для моніторингу хмарних середовищ на рівні екземплярів зазвичай використовуються легкі та мультиплатформенні агенти Wazuh.

Безпека контейнерів. Wazuh забезпечує безпекову видимість ваших хостів і контейнерів Docker, відстежуючи їх поведінку та виявляючи загрози, вразливості та аномалії. Агент Wazuh має вбудовану інтеграцію з механізмом

Docker, що дозволяє користувачам контролювати зображення, томи, параметри мережі та запущені контейнери.

Wazuh постійно збирає та аналізує детальну інформацію про час виконання. Наприклад, сповіщення про контейнери, що працюють у привілейованому режимі, уразливі програми, оболонку, що працює в контейнері, зміни постійних томів або зображень та інші можливі загрози.

Wazuh WUI надає потужний інтерфейс користувача для візуалізації та аналізу даних. Цей інтерфейс також можна використовувати для керування конфігурацією Wazuh і моніторингу її стану.

1.3 Полювання на загрози з MITRE ATT&CK і Wazuh

Полювання за загрозами – це процес пошуку зловмисної активності та її артефактів у комп'ютерній системі чи мережі. Полювання за загрозами здійснюється періодично в середовищі незалежно від того, чи були виявлені загрози автоматизованими рішеннями безпеки. Деякі суб'єкти загрози можуть залишатися бездіяльними в інфраструктурі організації, розширюючи свій доступ, чекаючи відповідної нагоди для використання виявлених недоліків [9, 10].

Тому важливо проводити пошук загроз, щоб виявити зловмисників у середовищі та зупинити їх до того, як вони досягнуть своєї кінцевої мети.

Щоб ефективно виконувати полювання на загрози, мисливець за загрозами повинен мати систематичний підхід до імітації можливої поведінки супротивника. Ця суперницька поведінка визначає, які артефакти можна шукати, що вказують на поточну чи минулу зловмисну діяльність.

Протягом багатьох років співтовариство безпеки спостерігало, що зловмисники зазвичай використовують багато тактик, методів і процедур (TTP) для проникнення в мережі та переміщення між ними, підвищення привілеїв і викрадання конфіденційних даних. Це призвело до розробки

різноманітних схем для відображення діяльності та методів суб'єктів загрози. Одним із прикладів є структура MITER ATT&CK [11, 12].

MITER ATT&CK – це добре задокументована база знань про дії та поведінку суб'єктів реальної загрози. Фреймворк MITRE ATT&CK має 14 тактик і багато прийомів, які ідентифікують або вказують на поточну атаку. MITER використовує ідентифікатори для посилання на тактику чи техніку, які використовує супротивник (рисунок 2.5).

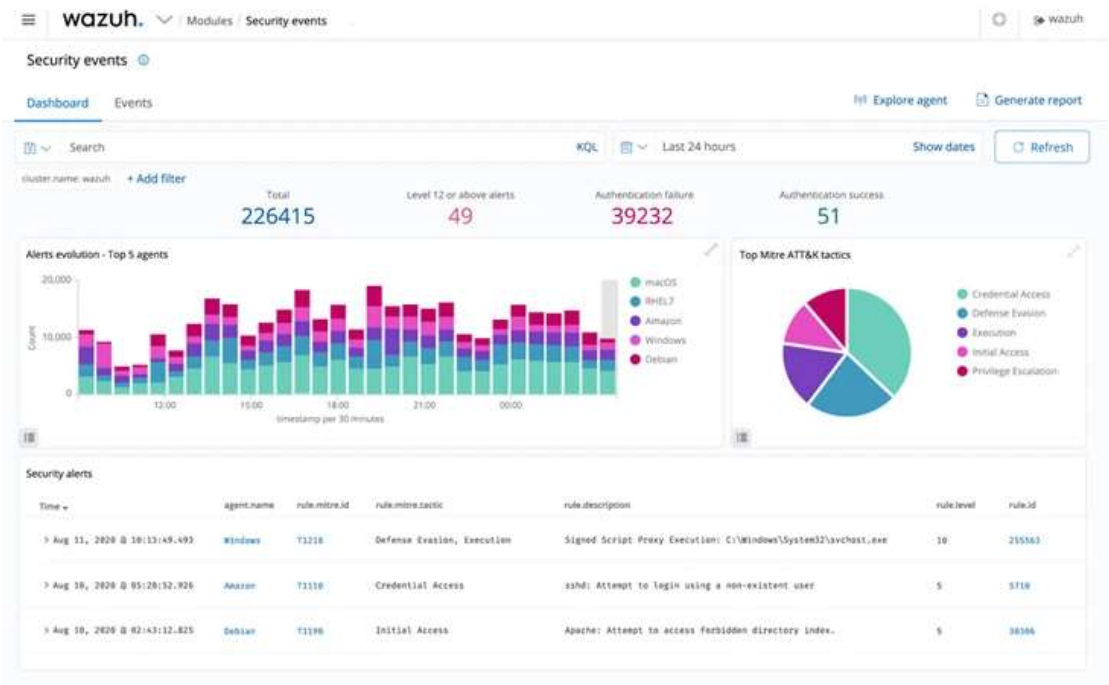

Рисунок 10 – Інформаційна панель подій безпеки Wazuh

Уніфікована платформа Wazuh XDR і SIEM. Wazuh – це уніфікована платформа XDR і SIEM з відкритим кодом. Рішення Wazuh складається з єдиного універсального агента, який розгортається на контрольованих кінцевих точках для виявлення загроз і автоматичного реагування. Він також має центральні компоненти (сервер Wazuh, індексатор і інформаційну панель), які аналізують і візуалізують дані про події безпеки, зібрані агентом Wazuh. Він захищає локальні та хмарні робочі навантаження.

Полювання на загрози з Wazuh. Мисливці за загрозами використовують різні інструменти, процеси та методи для пошуку шкідливих

артефактів у середовищі. Вони включають, але не обмежуються, використання інструментів для моніторингу безпеки, моніторингу цілісності файлів і оцінки конфігурації кінцевої точки.

Wazuh пропонує такі надійні можливості, як моніторинг цілісності файлів, оцінка конфігурації безпеки, виявлення загроз, автоматичне реагування на загрози та інтеграція з рішеннями, які надають дані про загрози.

2 СТРУКТУРА СИСТЕМИ ПОШУКУ ЗАГРОЗ

2.1 Ландшафт загроз кібербезпеці

Кіберзагрози постійно множаться та розвиваються, і хорошого захисту вже недостатньо. Найбезпечніший підхід до кіберзагроз – виявляти їх до того, як вони завдадуть шкоди, а не реактивно чекати, поки їх розкриють.

Сучасний ландшафт кіберзагроз є складним, постійно розвивається та різноманітним. Зловмисники, починаючи від організованих кіберзлочинців і закінчуючи спонсорованими державою групами, активно вдосконалюють існуючі методи та інструменти атак і створюють нові, щоб надійно встановити та швидко просуватися через ланцюг кіберзнищень, починаючи від розвідки до дій по цілях [7].

Ланцюг кіберзнищень, розроблений компанією Lockheed Martin, показаний на рисунку 2.1, описує набір етапів, які противники зазвичай проходять, щоб досягти своєї кінцевої мети. Кіберланцюг вбивств складається з семи етапів.

1. Розвідка: зловмисник оцінює ситуацію, щоб визначити потенційні цілі атаки та тактику. Наприклад, зловмисник збирає акаунти в соціальних мережах або проводить активне сканування вразливостей у загальнодоступних програмах.

2. Озброєння: зловмисник розробляє код для використання вразливостей або слабких місць, які були виявлені на етапі розвідки. Наприклад, підготовка фішингового електронного листа, формулювання коду впровадження SQL або підготовка коду зловмисного програмного забезпечення.

3. Доставка: зловмисник використовує вектори доставки, щоб відправити озброєне корисне навантаження. Наприклад, зловмисник використовує електронну пошту для доставки коду зловмисного програмного забезпечення.

4. Експлуатація: зловмисник виконує код, який він створив на етапі створення зброї.

5. Інсталяція: зловмисник створює канал, який дозволяє йому дістатися до скомпрометованої системи.

6. Командування та управління: зловмисник встановлює командно-контрольний канал (C2) із зовнішнім сервером. Наприклад, зловмисник використовує соціальну мережу *X* як прихований канал командування та контролю для зв'язку зі зламаними системами.

7. Дії щодо досягнення мети: зловмисник виконує ціль атаки. Наприклад, зловмисник шифрує файли на кінцевій точці у випадку зловмисника-вимагача.

Рисунок 2.1 – Ланцюг Cyber Kill

Полювання на загрози дозволяє організаціям застосовувати проактивний підхід, коли вони припускають, що їх зламали, і можуть виявити докази цього.

Ландшафт загроз кібербезпеці постійно змінюється. Через багато нових повідомлень/виявлених порушень, які тривалий час залишалися непоміченими, пошук кіберзагроз став критично важливою проактивною послугою, яку багато IT-директорів, CISO, спеціалістів з кібербезпеки та інших практиків безпеки прагнуть започаткувати або покращити, створивши пошук за кіберзагрозами.

Немає ідеальних кіберзлочинів. Противники залишають підказки та слід доказів під час виконання одного або кількох етапів кіберланцюга вбивств.

Просунуті зловмисники перейшли від використання шумових атак, які запускають сигналізацію безпеки, до більш прихованих, які залишають невеликий слід і викликають мінімальні сповіщення, якщо такі є, залишаючись непоміченими інструментами автоматизованого виявлення. Відповідно до опублікованого звіту SANS, «розвиток загроз, таких як безфайлове зловмисне програмне забезпечення, програмне забезпечення-вимагач, програмне забезпечення з нульовими днями та просунуте зловмисне програмне забезпечення, у поєднанні з обходом інструментів безпеки, створює додаткові ризики для підприємств».

Збільшення досвіду загрозливих суб'єктів у роботі в прихованій природі та їхня здатність запускати атаки з мінімальними шансами на виявлення спонукають організації думати не тільки про стандартні засоби виявлення. Зміни в поведінці супротивника вимагають від захисників створення проактивних можливостей, таких як полювання на загрози та розгортання розширеної аналітики за допомогою статистики та машинного навчання. Наприклад, мисливці можуть регулярно шукати потенційну діяльність з викрадання даних через службу доменних імен (DNS), застосовуючи статистичну аналітику на основі обсягів, не чекаючи та не покладаючись на інструменти безпеки мережі, такі як системи виявлення вторгнень, для створення сповіщень безпеки.

Організації покладаються на навички мисливців за загрозами, щоб виявити зазначені вище загрози під час пошукових операцій, що призводить до скорочення часу перебування та підвищення кіберстійкості. Час перебування – це час між початковим проникненням зловмисника в середовище організації (час успішного виконання першої загрози) і моментом, коли організація виявляє зловмисника (час виявлення загрози).

Окрім скорочення часу перебування, запуск операції пошуку загроз надає організації інші переваги безпеки, серед яких:

− виявлення прогалин у можливостях запобігання та виявлення безпеки;

− налаштування існуючих випадків використання моніторингу безпеки;

− виявлення нових випадків використання моніторингу безпеки;

− виявлення вразливостей, які не були виявлені під час оцінювання;

− виявлення неправильної конфігурації в системах і програмах, яка може вплинути на безпеку, роботу та відповідність.

Щоб отримати наведений вище перелік переваг, організаціям необхідно створити та запровадити надійний процес пошуку загроз, який чітко описує входи та результати експедицій пошуку загроз.

2.2 Структурування пошуку загроз

У пошуках загроз використовується підхід до розслідування на основі гіпотез. Гіпотеза – це пропозиція, яка узгоджується з відомими даними, але не була ані перевірена, ані доведена як хибна. Хороша гіпотеза має відповідати середовищу організації та бути перевіреною з точки зору доступності даних та інструментів. Підхід, заснований на гіпотезах, називається структурованим пошуком загроз [8 - 10.

З іншого боку, неструктуроване полювання на загрози стосується діяльності, під час якої мисливці аналізують наявні у них дані для пошуку аномалій без заздалегідь визначеної гіпотези. Наприклад, мисливець може обробляти та візуалізувати дані, щоб шукати несподівані зміни в шаблонах, наприклад помітні сплески або спади. Виявлення таких змін може спонукати мисливця до подальшого дослідження, щоб виявити непомічені загрози.

Висування гіпотези. Ландшафт загроз, пов’язаний із середовищем, яке необхідно захистити, має керувати тим, яку гіпотезу (наприклад, зловмисник отримав доступ до кінцевих точок організації через PowerShell) створити та виконати. Різні джерела, що стосуються загроз та їхнього значення для середовища, можуть допомогти вам зрозуміти ландшафт загроз. Мисливці за загрозами перетворюють це розуміння на гіпотези.

Перевірка гіпотези. Завдання мисливця за загрозами – перевірити гіпотезу, використовуючи найкращі ресурси, які є в його розпорядженні. Перевірку гіпотези можна розпочати з визначення керованого переліку дій, які можуть виявити перший набір доказів чи індикаторів, що стосуються гіпотези, або спрямувати мисливців до наступних пошуків. Наприклад, наступні дії мають відношення до попередньо висловленої гіпотези.

Полювання на підозрілі дії PowerShell може виявити існування компромісу, підтверджуючи гіпотезу. Успішне виконання наступних дій може виявити докази компромісу.

Полювання на загрозу. Виконання пошуку загроз може тривати годину або тиждень, залежно від багатьох факторів. Нездатність довести гіпотезу не обов’язково означає, що загрози не існує. Це означає, що мисливець не міг виявити загрозу за допомогою наявних навичок, даних та інструментів.

Книга присвячена структурованому полюванню, під час якого мисливець за загрозами, працюючи з іншими членами команди безпеки, щоб визначити та підтвердити гіпотезу, націлюється на тактику, техніку та процедури противника (TTP).

Рівень зрілості полювання на загрози організації з часом має підвищуватися. Є багато уроків, які мисливець отримає від мисливських операцій.

Тепер порівняємо полювання на загрози з виявленням загроз, фундаментальною службою моніторингу безпеки, і виявимо відмінності та підкреслимо схожість.

Різниця між полюванням за загрозами та виявленням загроз. Виявленням керує інструмент, а полюванням керує людина. Під час полювання мисливець займає центральне місце в порівнянні з інструментами, які виконують цю роль у процесі виявлення. Полювання за загрозами значною мірою покладається на досвід мисливця за загрозами для визначення гіпотези, пошуку доказів у величезній кількості даних і постійного перегляду в пошуках доказів компромісу. Пошук загроз не замінює технології виявлення загроз; вони доповнюють один одного.

Виявлення загроз відноситься до реактивного підходу, за якого аналітики Security Operation Center (SOC) реагують на сповіщення безпеки, створені інструментами. Наприклад, аналітики SOC сортували б і досліджували подію безпеки, згенеровану інструментом Endpoint Exposure and Response (EDR), або сповіщення безпеки, створене системою безпеки та керування інформацією (SIEM).

Аналітики SOC звертають увагу на сповіщення безпеки, які виявляються та повідомляються інструментами безпеки, а також проводять сортування та розслідування інцидентів безпеки. На рисунку 2.2 показано процес виявлення загроз на високому рівні, у якому аналітики SOC в першу чергу виконують обробку кіберзагроз. Аналітики SOC зазвичай очікують сповіщень на панелі приладів, щоб сортувати та реагувати на них. З іншого боку, полювання використовує проактивний підхід. Мисливці беруть на себе лідерство, виходячи на поле проведення операцій, споряджені правильним мисленням, досвідом, усвідомленням ситуації та правильним набором інструментів, необхідних для операції.

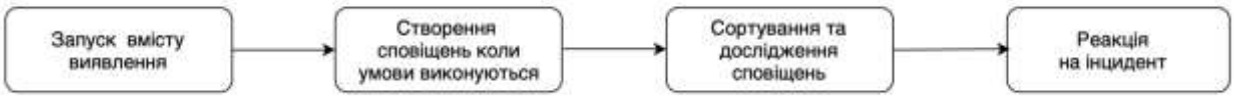

Рисунок 2.2 – Високорівневий процес виявлення загроз

Виявлення є важливою послугою SOC. Усунення недоліків у службі моніторингу безпеки має бути першочерговим завданням під час створення або передачі на аутсорсинг можливостей полювання на загрози. Організаціям не слід розглядати створення програми полювання на загрози, щоб перекласти роботу з групи моніторингу безпеки на мисливців за загрозами.

Виявлення та полювання повинні працювати разом, щоб забезпечити краще покриття ландшафту кіберзагроз. Виявлення та полювання взаємодіють, а в деяких випадках накладаються. Завжди будуть випадки, коли виявлення є входом до пошуку загроз, і навпаки. Наприклад, мисливець за загрозами може побудувати гіпотезу, яка розглядає поширену компрометацію системи на основі небагатьох підозрілих дій, виявлених на одній або кількох кінцевих точках і спостережених командою моніторингу безпеки.

Виявлення та полювання можуть використовувати однакові або різні аналітичні методи для виявлення зловмисних дій або полювання на них. Наприклад, інструменти аналізу поведінки користувачів використовують статистичний аналіз і машинне навчання, щоб виявляти аномальну поведінку користувачів і повідомляти групі моніторингу безпеки. Мисливці можуть використовувати подібні методи для пошуку кіберзагроз. Мисливці повинні розуміти можливості та обмеження різних аналітичних методів.

Описана в гіпотезі атака або загроза не відбулася. Мисливець може ще не мати повної інформації про навколишнє середовище. Наприклад, пошук загроз щодо нещодавно розгорнутого набору систем і програм може виявитися складним завданням під час пошуку.

Мисливець може ще не мати набору навичок, необхідних для розкриття складних атак на технології, з якими мисливець не дуже знайомий. Наприклад, запуск операції пошуку загроз у приватному середовищі Kubernetes, поки шукач не знайомий із контейнерними розгортаннями.

Відсутність даних, необхідних мисливцю для проведення ретельного розслідування. Використання невідповідних методів для розкриття складних

атак. Наприклад, виконання базових пошуків для виявлення розширених постійних загроз (APT).

Успішні мисливці за загрозами витрачають багато часу на дослідження та, у багатьох випадках, на випробування нових тактик, методів і процедур (TTP). Кібербезпека – це динамічний ландшафт, і наявність дорогоцінного часу на дослідження підвищує шанси виявлення передових TTP.

Процес полювання на загрозу. Визначення процесу допомагає мисливцям за загрозами встановлювати, проводити та постійно вдосконалювати загальну практику пошуку загроз та окремі дії пошуку загроз, з часом збільшуючи ймовірність виявлення загроз. Це не тільки допомагає покращити якість пошуків загроз, але й включає інші цінності, які пошук загроз вводить в організацію, наприклад оновлення наявного або розробка нового вмісту виявлення та аналізу загроз.

На рисунку 2.3 показано процес полювання на загрози, який починається з формалізації гіпотези, а потім спроби довести гіпотезу.

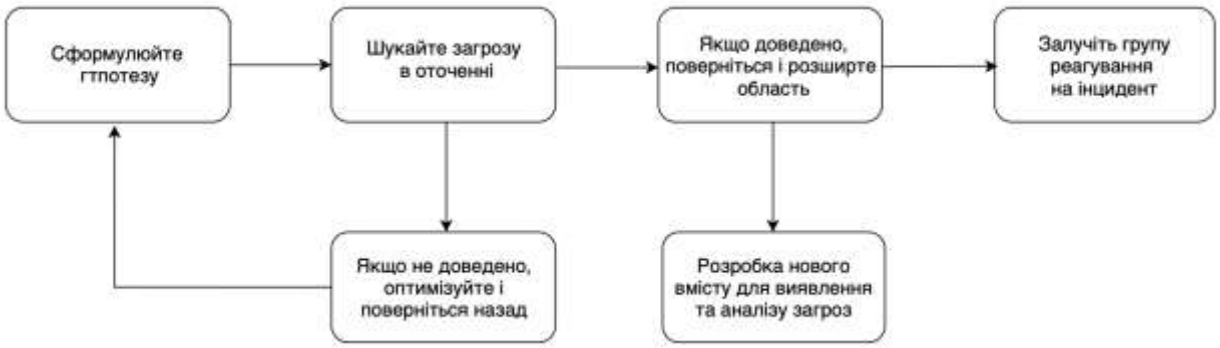

Рисунок 2.3 – Процес високого рівня пошуку загроз

Якщо мисливець не зміг довести гіпотезу, то необхідно її покращити, оновивши деталі гіпотези та знову здійснивши пошук загрози. Якщо гіпотезу доведено, то загрозу виявлено. На цьому мисливець не зупиняється; розширює сферу дії та знайходить індикатори в інших системах, щоб зрозуміти масштаб і поширення атаки. Тоді мисливець залучить групу

реагування на інциденти та задокументує та поширить новий вміст, який буде корисним для моніторингу безпеки та групи розвідки про загрози.

2.3 Життєвий цикл аналізу загроз

Розвідка про загрози базується на аналітичних методах, які протягом кількох десятиліть відточували урядові та військові установи. Традиційна розвідка зосереджується на шести окремих фазах, які складають так званий «цикл розвідки»: спрямування, збір, обробка, аналіз, розповсюдження та зворотний зв’язок (рисунок 2.4) [11, 12].

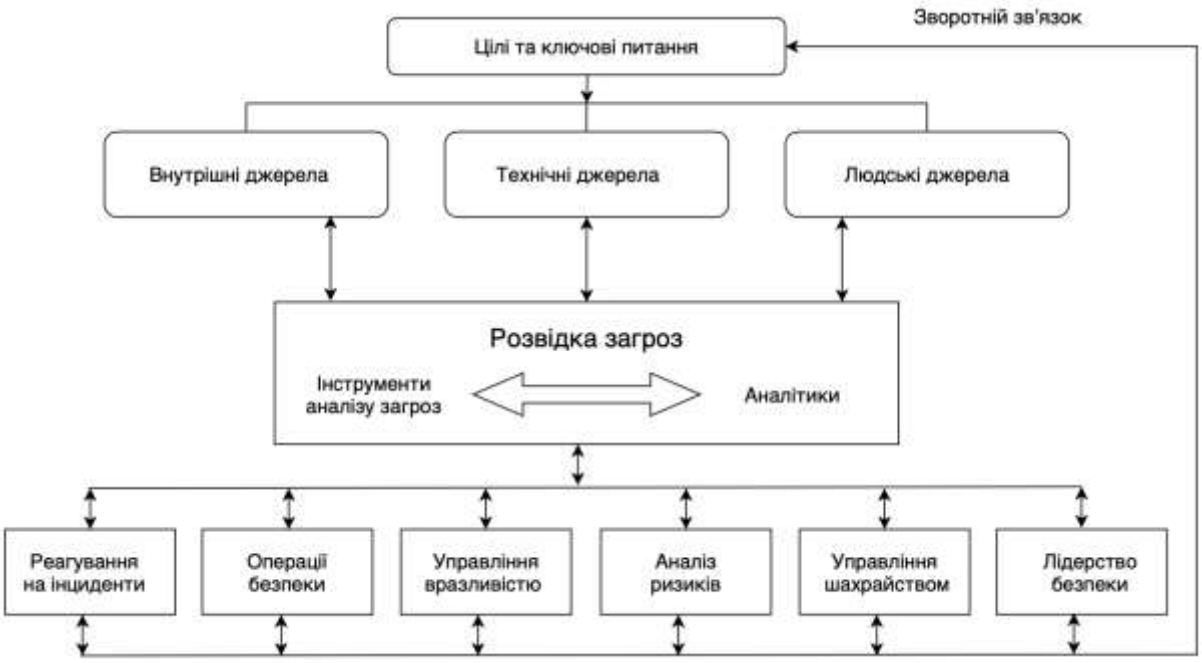

Рисунок 2.4 – Життєвий цикл аналізу загроз

Життєвий цикл розвідки про загрози складається з шести етапів. Розглянемо кожний з етапів детальніше [8 – 10].

1. Спрямування. Фаза спрямування життєвого циклу – це коли фахівець встановлює цілі для програми аналізу загроз. Це передбачає розуміння та формулювання:

− інформаційні активи та бізнес-процеси, які необхідно захистити;

− потенційні наслідки втрати цих активів або переривання цих процесів;

− типи розвідки про загрози, необхідні організації безпеки для захисту активів і реагування на нові загрози;

− пріоритети щодо того, що захищати.

Після того як визначено потреби в розвідці, організація може сформулювати запитання, які направляють потребу в інформації в окремі вимоги. Наприклад, якщо мета полягає в тому, щоб зрозуміти ймовірних супротивників, одним із логічних запитань було б: «Які загрозливі суб'єкти на підпільних форумах активно збирають дані про нашу організацію?»

2. Збір. Збір – це процес збирання інформації для задоволення найважливіших вимог розвідки. Збір інформації може відбуватися органічно різними засобами, зокрема:

− отримання метаданих і журналів із внутрішніх мереж і пристроїв безпеки;

− підписка на канали даних про загрози від галузевих організацій і постачальників засобів кібербезпеки;

− проведення бесід і цільових інтерв'ю з обізнаними джерелами;

− сканування відкритих новин і блогів (звичайна практика OSINT);

− веб-сайти та форуми зі зішкрібання та збору врожаю;

− проникнення в закриті джерела, такі як темні форуми.

Зазвичай зібрані дані являють собою комбінацію готової розвідувальної інформації, як-от звітів розвідки від експертів із кібербезпеки та постачальників, і необроблених даних, як-от підписи зловмисного програмного забезпечення або витік облікових даних на вставленому сайті.

3. Обробка. Обробка – це перетворення зібраної інформації у формат, придатний для використання організацією. Майже всі зібрані необроблені дані мають бути оброблені певним чином, як людьми, так і машинами. Різні

методи збору часто вимагають різних засобів обробки. Людські звіти можуть потребувати кореляції та ранжирування, деконфлікту та перевірки.

Прикладом може бути вилучення IP-адрес зі звіту постачальника безпеки та додавання їх до файлу CSV для імпорту до продукту керування інформацією та подіями безпеки (SIEM). У більш технічній сфері обробка може включати вилучення індикаторів з електронного листа, збагачення їх іншою інформацією, а потім обмін даними з інструментами захисту кінцевої точки для автоматичного блокування.

4. Аналіз. Аналіз – це людський процес, який перетворює оброблену інформацію в розвідку, яка може стати основою для прийняття рішень. Залежно від обставин рішення можуть стосуватися того, чи слід досліджувати потенційні загрози, які виникають, які дії негайно вжити для блокування атаки, як посилити контроль безпеки або скільки інвестицій у додаткові ресурси безпеки виправдано.

Особливо важлива форма, в якій подається інформація. Марно та марнотратно збирати та обробляти інформацію, а потім надавати її у формі, яка не може бути зрозуміла та використана особою, яка приймає рішення. Наприклад, якщо необхідно спілкуватися з нетехнічними фахівцями, звіт повинен:

- бути лаконічним (записка на одній сторінці або декілька слайдів);
- уникайте заплутаних і надто технічних термінів і жаргону;
- сформулюйте проблеми в ділових термінах (наприклад, прямі та непрямі витрати та вплив на репутацію);
- включіть рекомендований план дій.

Успішні групи розвідки про кіберзагрози надають постійні технічні звіти іншим групам безпеки з зовнішнім контекстом щодо IOC, зловмисного програмного забезпечення, учасників загроз, вразливостей і тенденцій загроз.

5. Поширення. Розповсюдження передбачає доставку готової розвідувальної інформації в ті місця, де вона має потрапити. Більшість

організацій з кібербезпеки мають щонайменше шість команд, які можуть отримати вигоду від аналізу загроз.

Для кожної з цих аудиторій потрібно запитати:

1) яка розвідка про загрози їм потрібна і як зовнішня інформація може підтримувати їх діяльність?

2) як слід подавати розвідувальні дані, щоб вони були зрозумілими та придатними для цієї аудиторії?

3) як часто повинні надавати оновлення та іншу інформацію?

4) за допомогою яких засобів масової інформації слід поширювати розвідувальні дані?

6. Зворотній зв'язок. Останній етап життєвого циклу розвідки про загрози включає отримання зворотного зв’язку щодо звіту розвідки, щоб визначити, чи був аналіз своєчасним, релевантним і дієвим. Зацікавлені сторони можуть змінити свої пріоритети або змінити спосіб поширення чи представлення даних. Встановлення показників ефективності для вимірювання ефективності аналізу загроз і визначення можливостей для постійного вдосконалення є важливими аспектами етапу збору зворотного зв’язку.

2.4 Модуль Wazuh MITER ATT&CK

Wazuh поставляється з готовим модулем MITER ATT&CK і правилами виявлення загроз, зіставленими з відповідними ідентифікаторами техніки MITRE. Цей модуль складається з чотирьох компонентів [13, 14]:

1. Компонент розвідки модуля Wazuh MITER ATT&CK: містить детальну інформацію про групи загроз, засоби пом’якшення, програмне забезпечення, тактику та методи, які використовуються під час кібератак. Цей компонент допомагає мисливцям за загрозами ідентифікувати та класифікувати різні TTP, які використовують зловмисники (рисунок 2.6).

2. Компонент каркаса модуля Wazuh MITER ATT&CK: допомагає мисливцям за загрозами звузити коло загроз або скомпрометованих кінцевих точок. Цей компонент використовує певні методи, щоб побачити всі події, пов’язані з цією технікою, і кінцеві точки, де ці події відбулися (рисунок 2.7).

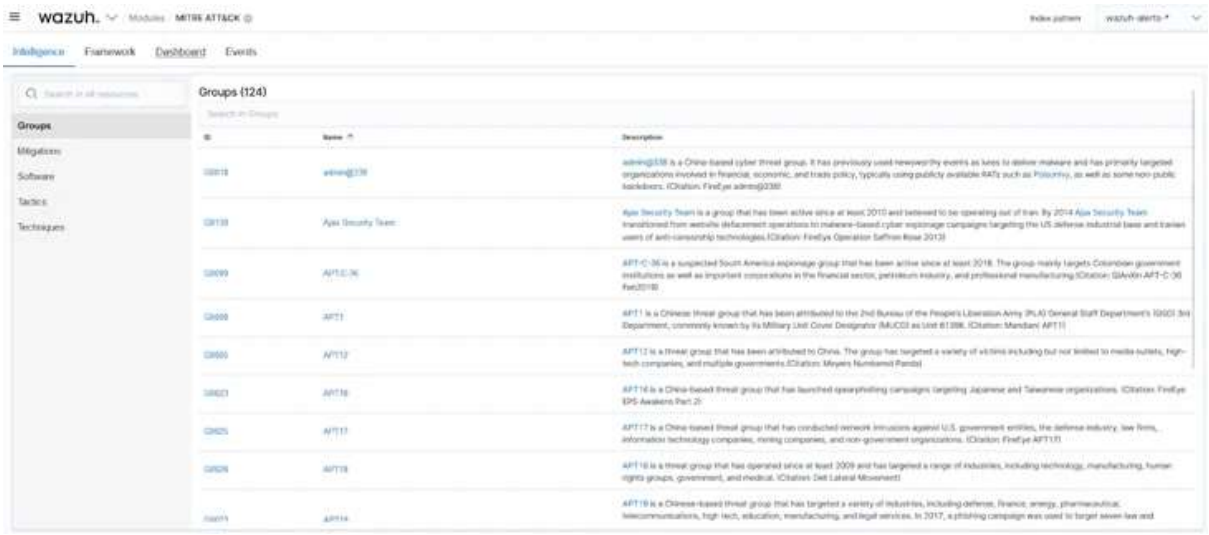

Рисунок 2.6 – Wazuh MITER ATT&CK Intelligence

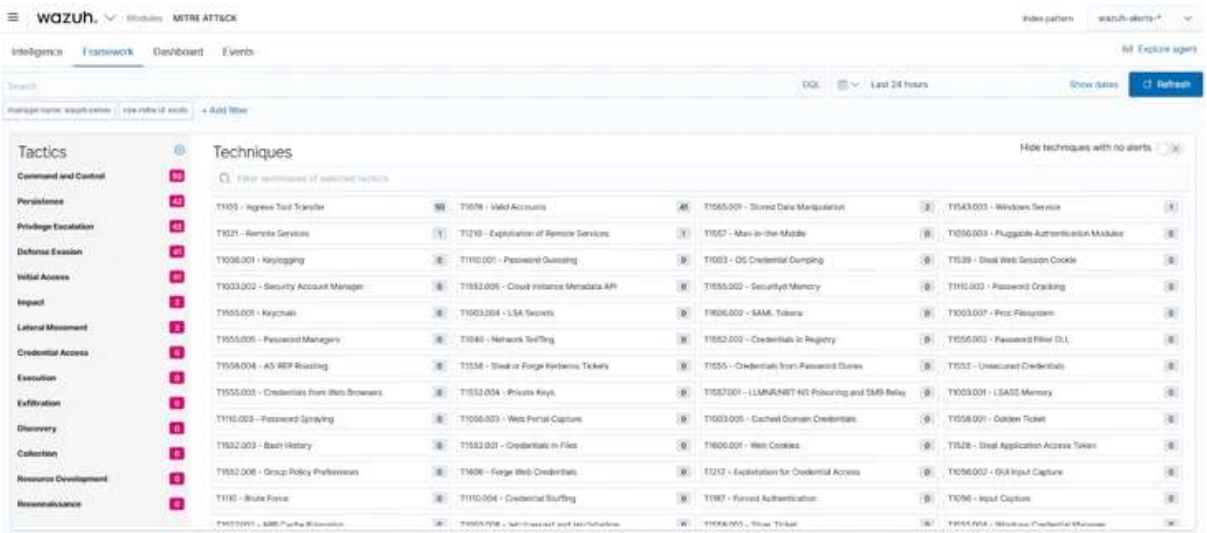

Рисунок 2.7 – Структура Wazuh MITER ATT&CK

3. Компонент інформаційної панелі модуля MITER ATT&CK: допомагає узагальнити всі події в діаграмах, щоб допомогти мисливцям за загрозами отримати швидкий огляд діяльності, пов’язаної з MITER, в інфраструктурі (рисунок 2.8).

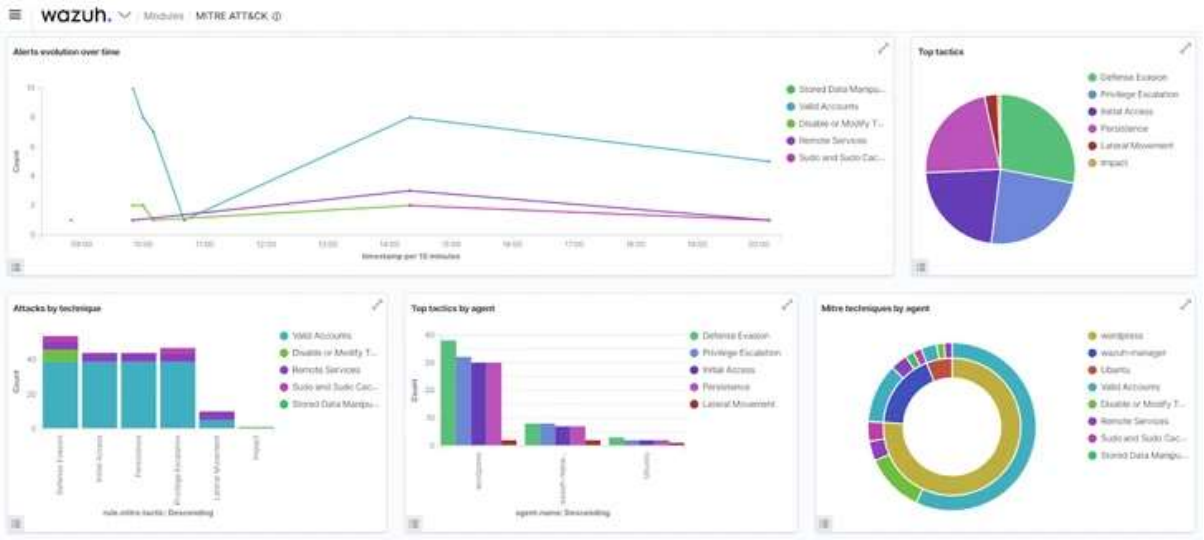

Рисунок 2.8 – Панель приладів Wazuh MITER ATT&CK

4. Компонент подій Wazuh MITER ATT&CK: відображає події в режимі реального часу з відповідними ідентифікаторами MITER, щоб краще зрозуміти кожне сповіщення (рисунок 2.9).

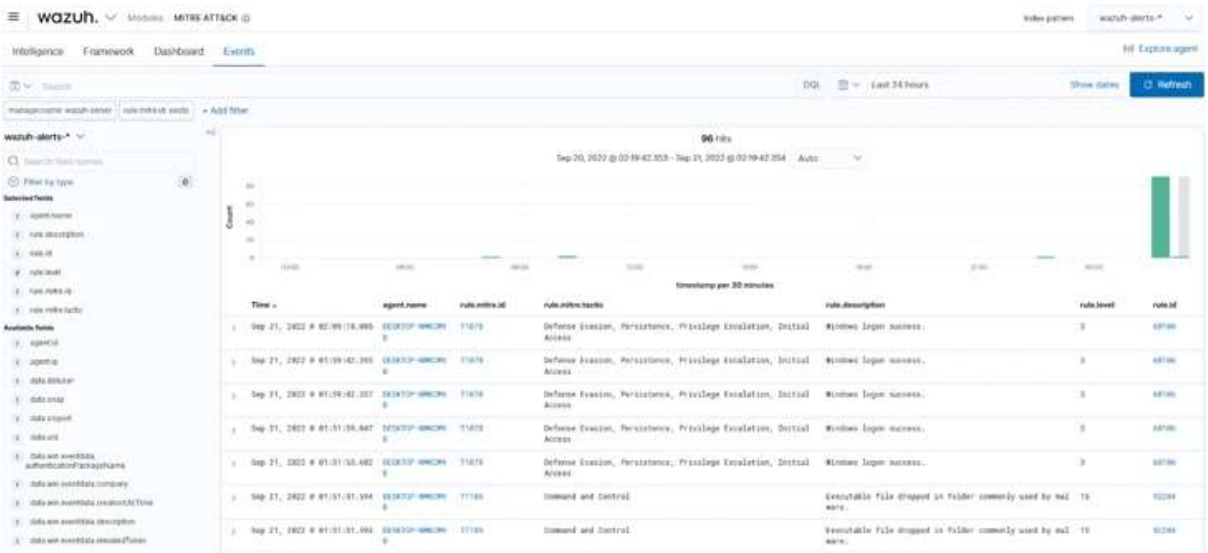

Рисунок 2.10 – Події Wazuh MITER ATT&CK

Правила та декодери Wazuh. У Wazuh є готові правила та декодери для аналізу безпеки та даних виконання, згенерованих із різних джерел. Wazuh

підтримує правила для різних технологій (наприклад, Docker, CISCO, Microsoft Exchange), які зіставлено з відповідними ідентифікаторами MITRE. Користувачі також можуть створювати власні правила та декодери та відображати кожне правило відповідною тактикою чи технікою MITRE. У цій публікації в блозі показано приклад використання спеціальних правил MITRE ATT&CK і Wazuh для виявлення противника [15].

Модуль оцінки конфігурації безпеки (SCA). Модуль Wazuh SCA виконує періодичне сканування в кінцевих точках, щоб виявити неправильну конфігурацію системи та програми. Його також можна використовувати для пошуку індикаторів компрометації, наприклад шкідливих файлів і папок, створених зловмисним програмним забезпеченням. Аналіз інвентаризації програмного забезпечення, служб, неправильних конфігурацій і змін у конфігурації на кінцевій точці може допомогти мисливцям за загрозами виявити поточні атаки (рисунок 2.11).

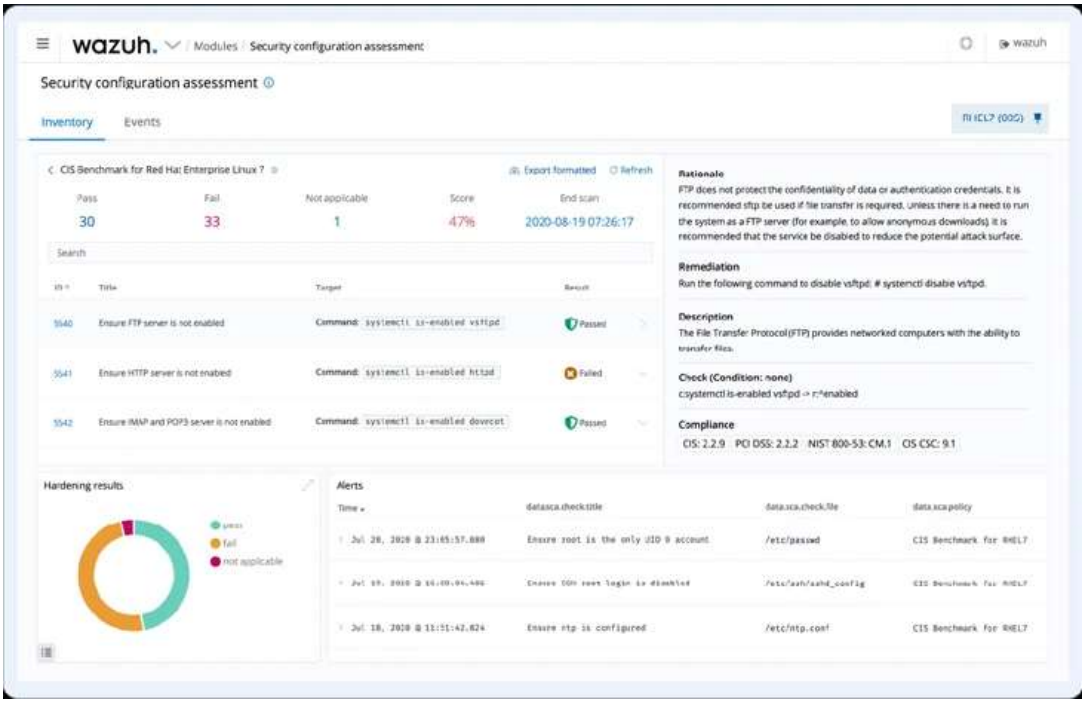

Рисунок 2.11 – Інформаційна панель Wazuh SCA

Інтеграція з рішеннями аналізу загроз. Завдяки своїй природі з відкритим кодом Wazuh надає можливість інтеграції з API аналізу загроз та

іншими рішеннями безпеки. Wazuh інтегрується з відкритими платформами аналізу загроз, такими як Virustotal, URLHaus, MISP і AbuseIPDB, щоб назвати декілька. Залежно від інтеграції відповідні сповіщення з'являються на інформаційній панелі Wazuh. Конкретну інформацію, таку як IP-адреси, хеші файлів і URL-адреси, можна запитувати за допомогою фільтрів на інформаційній панелі Wazuh [16, 17].

Контроль цілісності файлів. Моніторинг цілісності файлів (FIM) використовується для моніторингу та аудиту конфіденційних файлів і папок на кінцевих точках. Wazuh надає модуль FIM, який відстежує та виявляє зміни в указаних каталогах або файлах у файловій системі кінцевої точки. Модуль FIM також може виявляти, коли файли, введені в кінцеві точки, збігаються з хешами відомого шкідливого програмного забезпечення.

Архіви Wazuh. Архіви Wazuh можна ввімкнути для збору та зберігання всіх подій безпеки, отриманих із контрольованих кінцевих точок. Ця функція допомагає мисливцям за загрозами, надаючи їм дані, які можна використовувати для створення правил виявлення та випередження загроз. Архіви Wazuh також корисні для дотримання нормативних вимог, коли потрібна історія журналу аудиту.

3 РОЗРОБКА ТА ДОСЛІДЖЕННЯ СИСТЕМИ ПОШУКУ ЗАГРОЗ

3.1 Інтеграція Wazuh з управлінням хмарною безпекою

Управління хмарною безпекою (Cloud Security Posture Management, CSPM) є важливим для забезпечення безпеки та відповідності хмарних середовищ. У хмарних обчисленнях, де організації можуть швидко та легко надавати, конфігурувати та змінювати хмарні ресурси, потенціал для неправильної конфігурації безпеки зростає. Ці проблеми з безпекою можуть виникати через неправильне керування дозволами, прогалини в конфігураціях мережі та різні інші фактори [18, 19].

Cloud Security Posture Management вирішує цю проблему шляхом постійного моніторингу та оцінки хмарних робочих навантажень для виявлення неправильних конфігурацій, вразливостей і потенційних ризиків. Він також містить кроки щодо усунення потенційних ризиків безпеці, тим самим підвищуючи загальну безпеку хмарного середовища [20-23].

Інфраструктура. Наступні компоненти є необхідні для реалізації проекту, зокрема:

1) попередньо зібраний, готовий до використання Wazuh OVA 4.5.1. Ця віртуальна машина містить центральні компоненти Wazuh (сервер Wazuh, індексатор Wazuh і інформаційну панель Wazuh);

2) обліковий запис GCP з правами адміністратора. Для цієї демонстрації рекомендується використовувати тестовий обліковий запис, який не керує виробничими навантаженнями.

Інтеграція Wazuh з GCP. Wazuh інтегрується з GCP за допомогою служби видавця та передплатника Google Cloud (GCP Pub/Sub). Google Cloud Pub/Sub – це служба обміну повідомленнями, яка допомагає надсилати та отримувати дані журналу між програмами. Wazuh надає модуль інтеграції для GCP, який отримує журнали зі служби Pub/Sub (рисунок 3.1) [20].

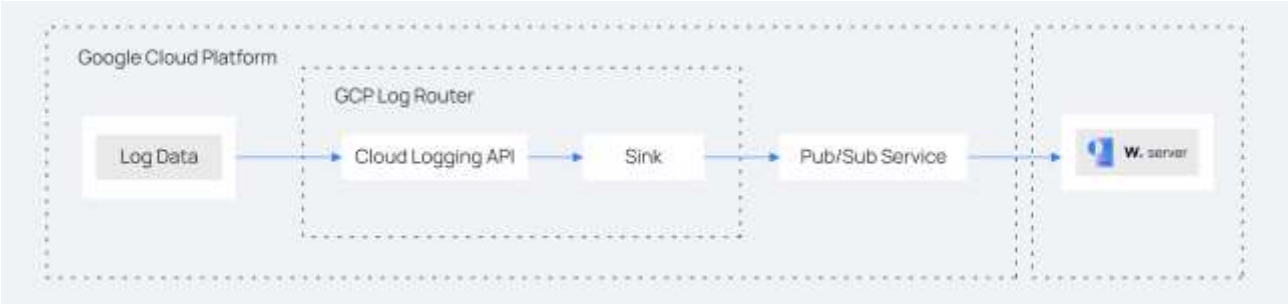

Рисунок 3.1 – Інтеграції Google Cloud Platform із Wazuh

Google Cloud Platform. Налаштування облікового запису GCP. Створюємо новий проект GCP і обліковий запис служби, який дозволяє модулю Wazuh GCP отримувати дані журналу зі служби Google Pub/Sub. Потім налаштовуємо служби Pub/Sub і Sink. Служба приймача направляє журнали стану безпеки в хмарі з центральної служби Cloud Logging GCP до служби Pub/Sub.

Для налаштування, необхідно виконати наведені нижче кроки.

1. Створити новий проект GCP. Зверніть увагу на ідентифікатор проекту (рисунок 3.2).

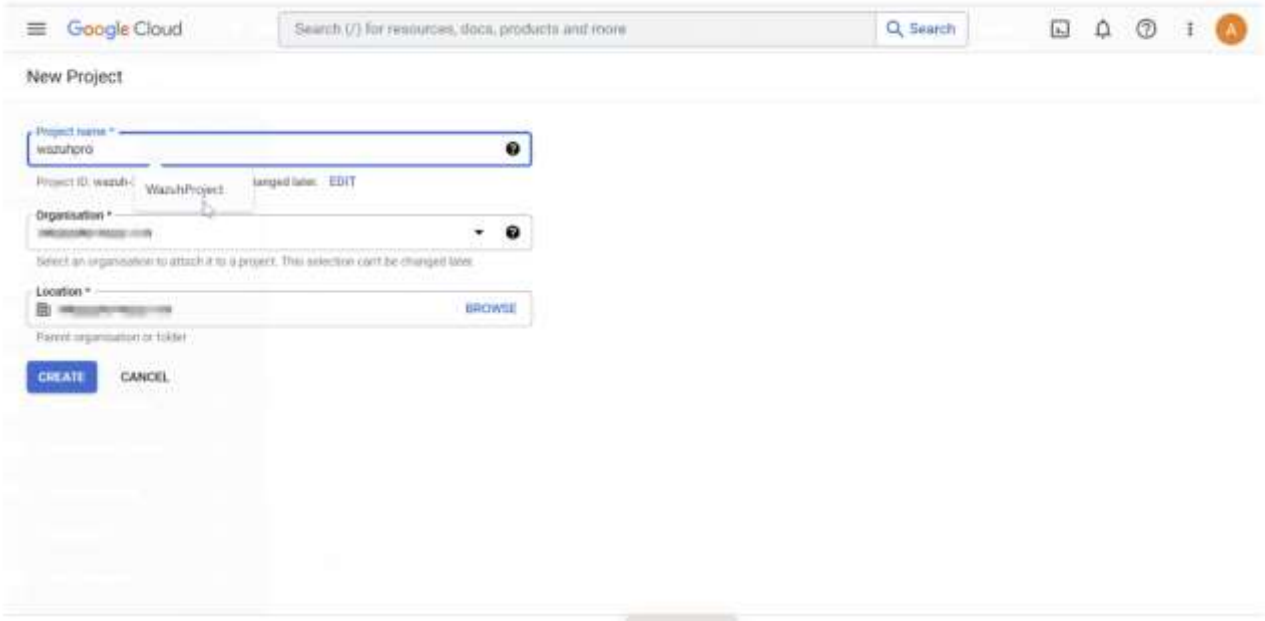

Рисунок 3.2 – Створення нового проекту

де:

«Назва проекту» – це ім’я, дане проекту;

«Організація» – це назва організації GCP.

2. Для створення нового облікового запису служби необхідно перейти до розкривного меню IAM та адміністратора та вибрати «Облікові записи служби». На сторінці створення облікових записів служби додаємо до облікового запису ролі Pub/Sub Publisher і Pub/Sub Subscriber (рисунок 3.3).

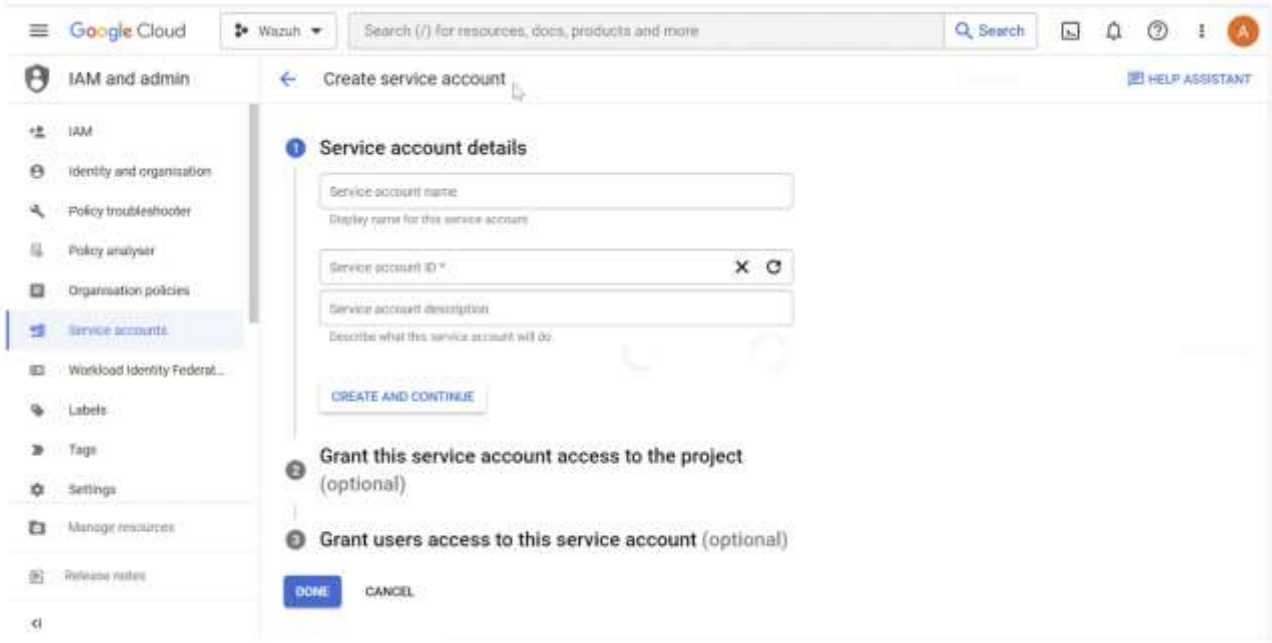

Рисунок 3.3 – Створення облікового запису служби:

де:

«Назва облікового запису служби» – це привілейований обліковий запис, який Wazuh використовує для підключення до GCP.

«Ролі» – це права, надані обліковому запису служби.

3. Відкриваємо щойно створений обліковий запис служби та створюємо закритий ключ у форматі JSON. Браузер автоматично завантажує ключ. Wazuh використовує ключ для автентифікації у проекті GCP (рисунок 3.4).

4. У полі пошуку консолі у верхній частині сторінки вибираємо Pub/Sub. Натискаємо «Створити тему». На сторінці «Створити тему» вводимо ідентифікатор теми та перевіряємо, що встановлено прапорець «Додати підписку за замовчуванням».

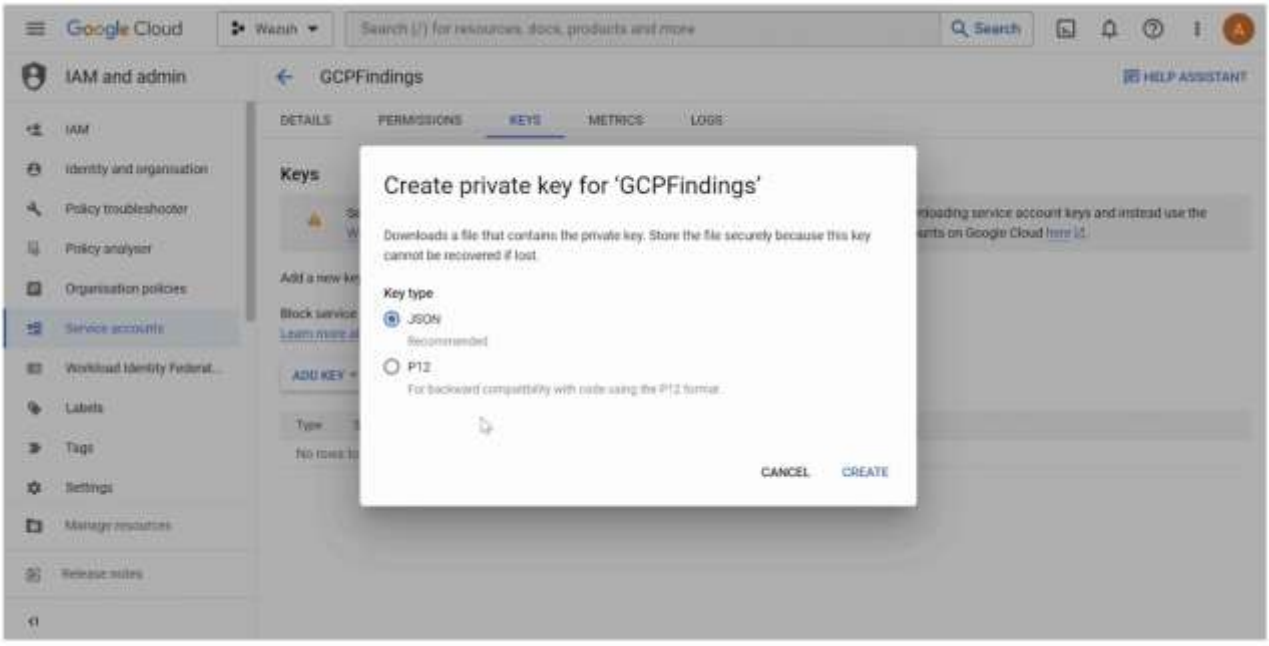

Рисунок 3.4 – Створення ключа облікового запису служби

Потім натискаємо «Створити». Зверніть увагу на ідентифікатор підписки (рисунок 3.5).

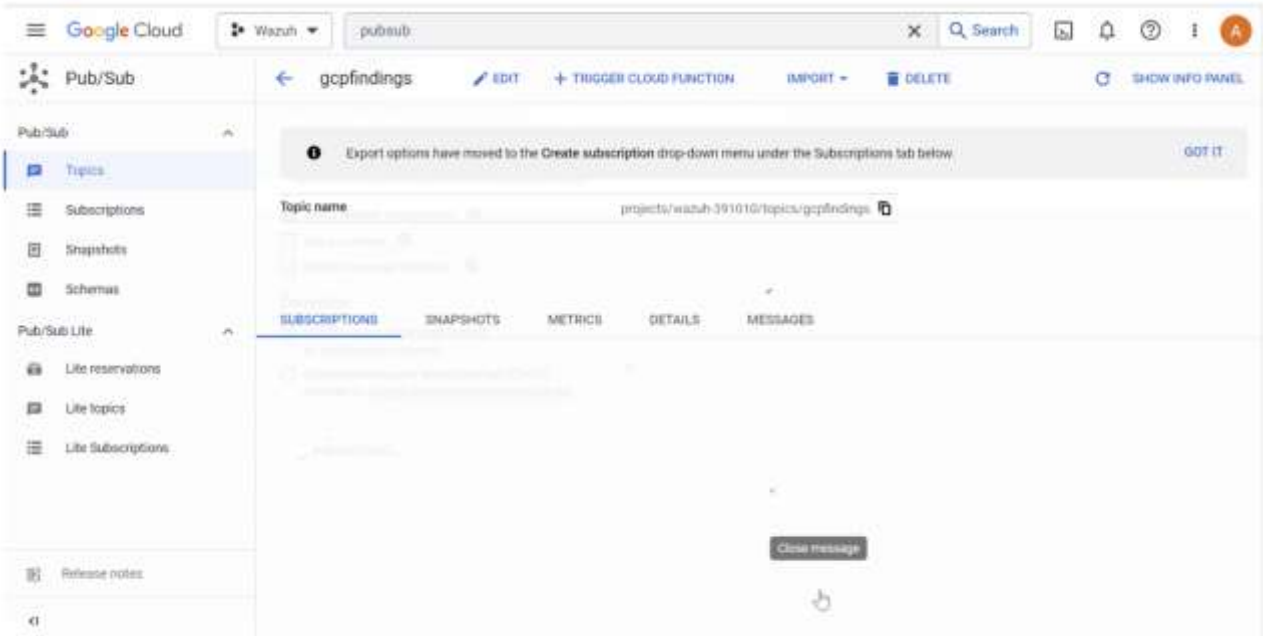

Рисунок 3.5 – Конфігурація Pub/Sub

5. Знаходимо Log Router у консолі GCP і вибираємо його. Натискаємо «Створити приймач ». Називаємо одержувача та натискаємо «Далі». У службі

призначення приймача вибираємо тему Cloud Pub/Sub. Далі вибираємо назву теми, створену раніше. Натискаємо «Створити приймач» (рисунок 3.6).

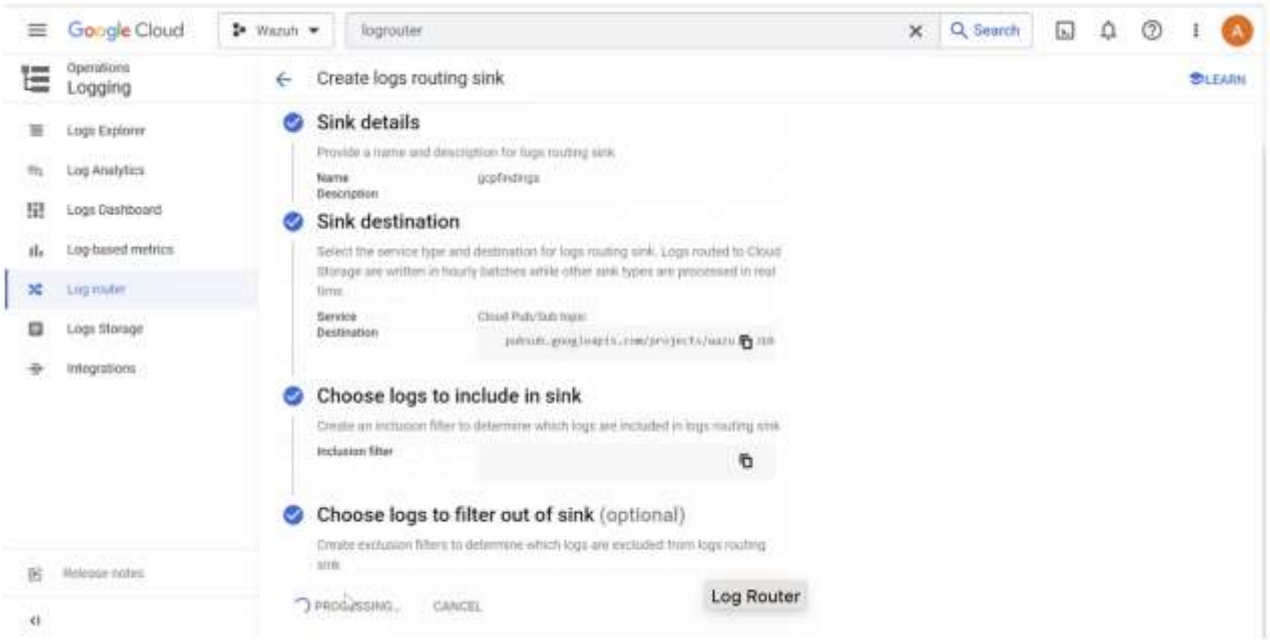

Рисунок 3.6 – Конфігурація приймача

Сервіси Log Router і Sink у проекті GCP відповідають за керування журналами та маршрутизацію призначення журналів відповідно.

6. Налаштування безперервного експорту журналу зі служби GCP Findings до служби GCP Pub/Sub (рисунок 3.7).

Сервер Wazuh. Налаштування серверу Wazuh для отримання журналів від GCP складається з наступних кроків.

1. Створити файл credentials.json у каталозі /var/ossec/wodles/gcloud/:

touch /var/ossec/wodles/gcloud/credentials.json

2. Оновити файл /var/ossec/wodles/gcloud/credentials.json вмістом файлу JSON із закритим ключем, завантаженого раніше. Модуль Wazuh GCP використовує файл ключа для автентифікації вашого облікового запису GCP.

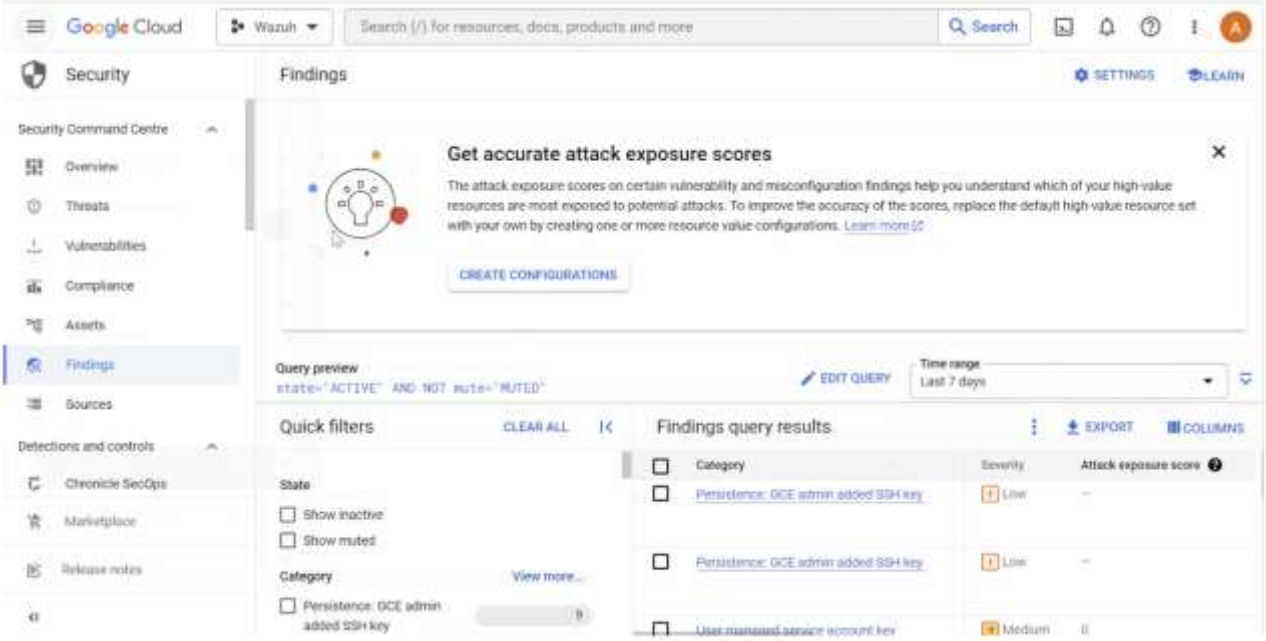

Рисунок 3.7 – Конфігурація безперервного експорту

3. Додати наступний вміст до файлу конфігурації /var/ossec/etc/ossec.conf. Конфігурація вказує, як Wazuh підключається до GCP за допомогою ідентифікатора проекту, ідентифікатора підписки GCP PubSub та облікових даних.

```
<ossec_config>
  <gcp-pubsub>
    <pull_on_start>yes</pull_on_start>
    <interval>5m</interval>
    <project_id><PROJECT_ID></project_id>
    <subscription_name><SUBSCRIPTION_ID></subscription_name>
     <credentials_file>/var/ossec/wodles/gcloud/credentials.json</credentials_file>
  </gcp-pubsub>
</ossec_config>
```

Замінюємо змінні в конфігурації відповідними значеннями:

де:

PROJECT_ID – це ідентифікатор створеного вище проекту.

SUBSCRIPTION_NAME – це ідентифікатор підписки вашого GCP Pub/Sub.

4. Створюємо файл правил gcp_posture.xml у каталозі /var/ossec/etc/rules/ і додайте наступні правила користувача для виявлення результатів положення GCP:

```
<group name="gcp,">
 <!-- Misconfiguration detection -->
  <rule id="100200" level="10">
    <if_sid>65000</if_sid>
    <field name="gcp.finding.findingClass">MISCONFIGURATION</field>
    <description>A $(gcp.finding.findingClass) with $(gcp.finding.severity)
severity has been discovered on the GCP project
$(gcp.resource.projectDisplayName). $(gcp.finding.description)</description>
    <mitre>
     <id>T1562</id>
    </mitre>
  </rule>
```

```
  <!-- Threat detection -->
   <rule id="100201" level="10">
      <if_sid>65000</if_sid>
      <field name="gcp.finding.findingClass">THREAT</field>
      <description>A $(gcp.finding.findingClass) with $(gcp.finding.severity)
 severity has been discovered on the GCP project
 $(gcp.resource.projectDisplayName). $(gcp.finding.category).</description>
      <mitre>
        <id>T1562</id>
      </mitre>
   </rule>
 </group>
```

де:

Ідентифікатор правила 100200 активується, коли Wazuh виявляє неправильну конфігурацію в обліковому записі GCP.

Ідентифікатор правила 100201 активується, коли GCP виявляє загрозу.

5. Перезапускаємо менеджер Wazuh, щоб застосувати конфігурацію:

systemctl restart wazuh-manager

Симуляція управління безпекою в хмарі. Модуль Findings – це служба GCP Security Command Center, яка записує неправильні налаштування безпеки в проекті GCP. Симуляція створює зразки неправильних конфігурацій, які будуть відправлені в Wazuh (рисунок 3.8).

Неправильна конфігурація мережі. Для імітування неправильної конфігурації мережі необхідно виконати наведені нижче дії на консолі GCP.

1. Увімкнути API Compute Engine. Це ввімкне внутрішній брандмауер VPC ().

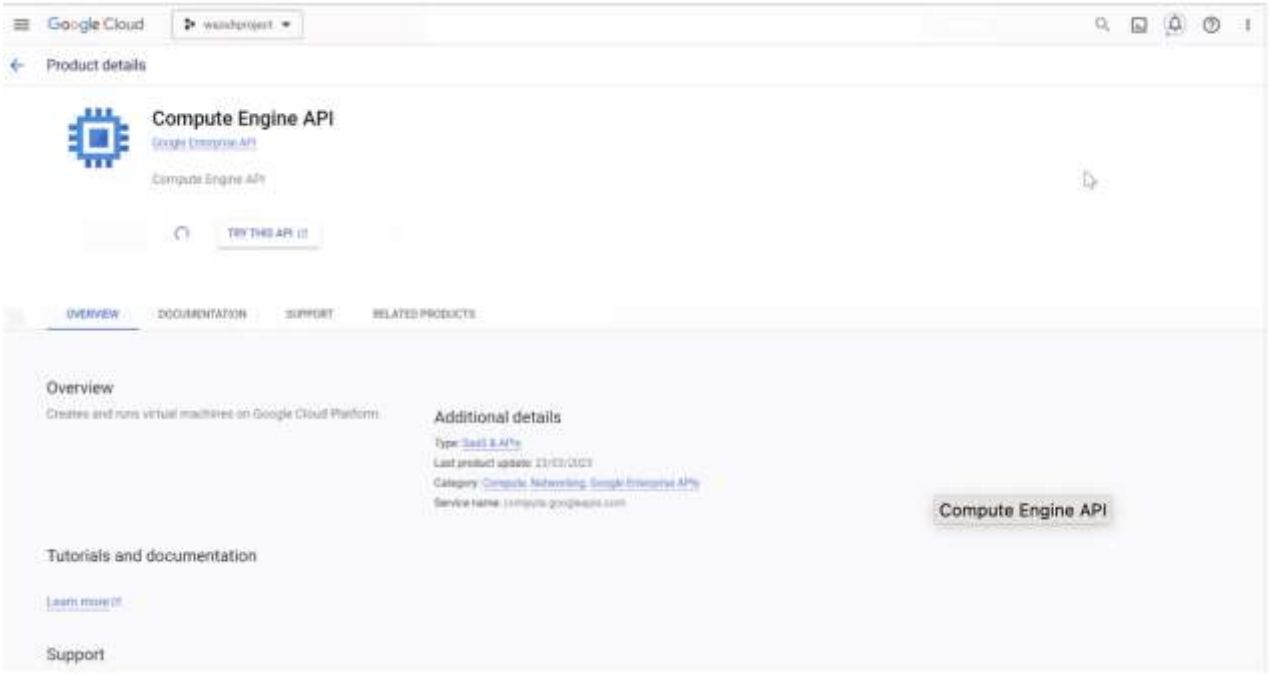

Рисунок 3.8 – API Compute Engine

2. Створюємо правило брандмауера «verybadrule» для безпеки мережі GCP, щоб імітувати кілька неправильних конфігурацій мережі. Правило брандмауера дозволяє підключення з усіх IP-адрес і портів. (рисунок 3.9).

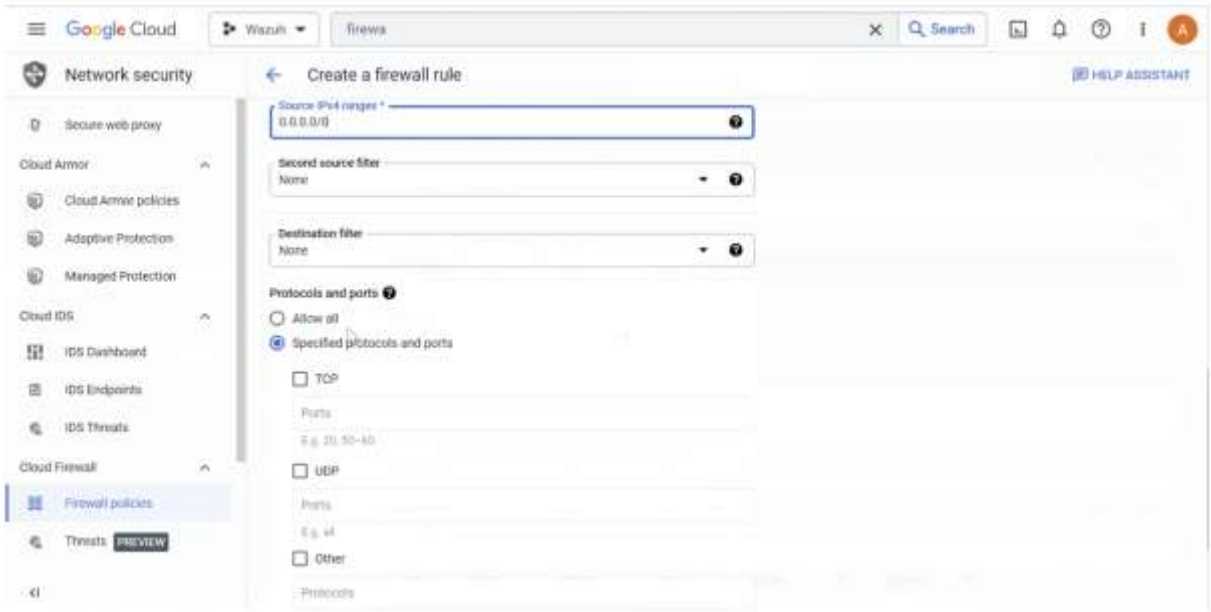

Рисунок 3.9 – Створення правила брандмауера

3. Видалення правила брандмауера «verybadrule» зі списку правил безпеки мережі GCP (рисунок 3.10).

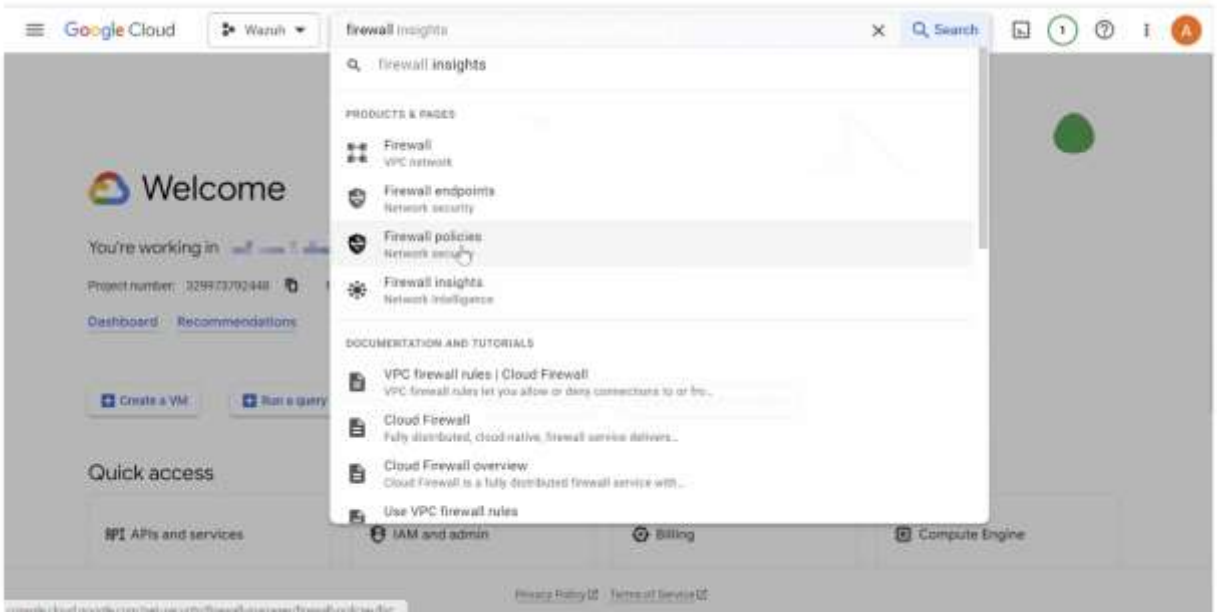

Рисунок 3.10 – Видалення правила брандмауера

Аномальна активність керування ідентифікацією та доступом.

1. Створюємо тестову адресу електронної пошти Gmail, якщо у вас її ще немає.

2. Переходимо до розкривного меню IAM & Admin і вибираємо IAM. Натисніть «Надати доступ». На сторінці надання доступу введіть адресу Gmail тестового користувача як нового. Далі призначте роль «Власник проекту» та натисніть «Зберегти» (3.11).

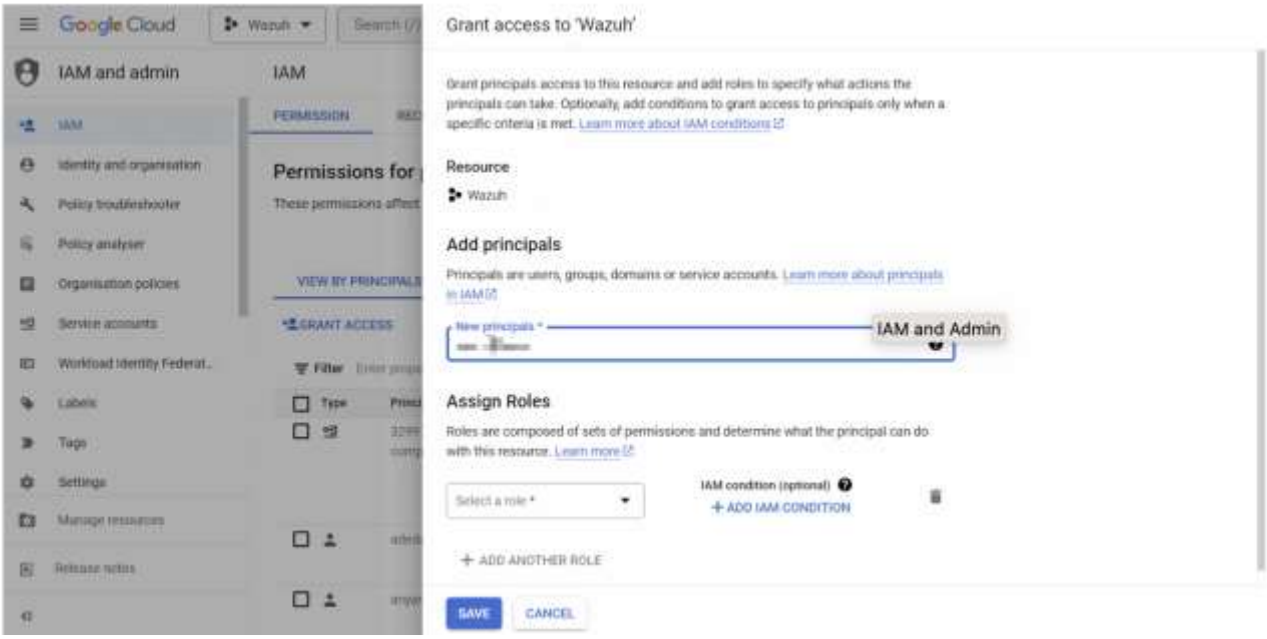

Рисунок 3.11 – Симуляція IAM і адміністратора

Результат інтеграції з фільтром для ідентифікаторів правил 100200 і 100201 приведений на рисунку 3.12.

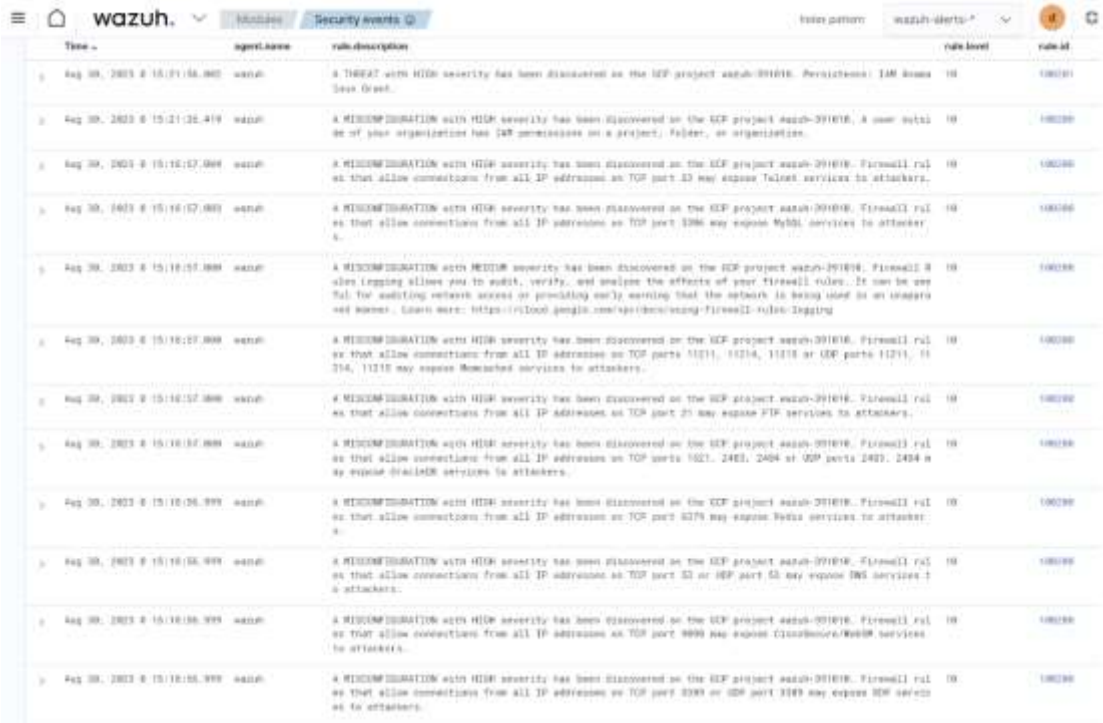

Рисунок 3.12 – Журнал подій безпеки

Результати візуалізації керування положенням GCP, можна побачити перейшовши до подій безпеки модулів.

3.2 Покращення безпеки за допомогою платформи Wazuh

У світі кібербезпеки, що постійно розвивається, організаціям потрібні надійні інструменти для моніторингу та захисту своїх цифрових активів. Платформи безпеки інформації та керування подіями (SIEM) стали ключовим компонентом ефективної стратегії безпеки [24, 25].

Розроблений алгоритм впровадження Wazuh SIEM у хмарному середовищі складається з наступних кроків.

Крок 1. Вибір хмарного постачальника та середовища.

Виберіть постачальника хмарних послуг, який відповідає вимогам і перевагам вашої організації. Серед популярних варіантів – Amazon Web Services (AWS), Microsoft Azure і Google Cloud Platform (GCP). Створіть хмарне середовище, яке відповідає потребам організації, забезпечуючи правильні конфігурації мережі та засоби контролю доступу.

Крок 2. Налаштування серверу Wazuh.

Розгорніть віртуальну машину (VM) у своєму хмарному середовищі, яка буде служити сервером Wazuh. Установіть програмне забезпечення менеджера Wazuh на цю віртуальну машину, яка діє як центральний компонент для збору й аналізу даних про події безпеки. Налаштуйте необхідні параметри мережі, включаючи групи безпеки мережі та правила брандмауера, щоб дозволити зв’язок між сервером Wazuh і контрольованими хостами.

Крок 3. Встановлення і налаштування агентів Wazuh.

На кожному з п’яти хостів, які необхідно контролювати, установлюємо та налаштовуємо агенти Wazuh. Ці легкі програмні компоненти збирають дані про події безпеки та надсилають їх на сервер Wazuh для аналізу. Агенти можна встановити вручну або розгорнути за допомогою автоматизованих методів, таких як групові політики або інструменти керування конфігурацією. Переконайтеся, що агенти правильно налаштовані для встановлення безпечного з’єднання із сервером Wazuh.

Крок 4. Налаштування колекції подій безпеки.

Після встановлення агентів Wazuh необхідно налаштувати сервер Wazuh для збору подій безпеки з контрольованих хостів. Визначте файли журналів і джерелу подій, які ви хочете контролювати, наприклад системні журнали, журнали програм або журнали мережі. Налаштуйте параметри збору подій відповідно до конкретних вимог організації, включаючи шляхи до файлів журналу, параметри ротації журналів і параметри фільтрації подій.

Крок 5. Увімкнення моніторингу і оповіщення в реальному часі.

Налаштуйте сервер Wazuh для моніторингу в реальному часі та попередження на основі попередньо визначених правил і політик. Налаштуйте ці правила відповідно до цілей безпеки вашої організації та вимог відповідності. Налаштуйте параметри сповіщень, щоб забезпечити своєчасне сповіщення про критичні інциденти безпеки. Розгляньте можливість інтеграції Wazuh з іншими системами сповіщень або платформами реагування на інциденти, щоб оптимізувати процес реагування на інциденти.

Крок 6. Виконання регулярного аналізу журналу та розслідування інцидентів.

Необхідно регулярно аналізувати зібрані журнали подій безпеки, використовуючи вбудовані можливості аналізу сервера Wazuh. Швидко розслідувати будь-які виявлені інциденти або аномалії безпеки, щоб зрозуміти їх характер і потенційний вплив. Використовувати багатий набір даних безпеки та візуалізацій, які надає Wazuh, щоб отримати уявлення про стан безпеки вашої мережі.

Крок 7. Постійно підвищувати рівень безпеки.

Відстежуючи мережу та виявляючи потенційні вразливі та слабкі місця, необхідно вживати профілактичних заходів для підвищення рівня безпеки. Необхідно застосовувати відповідні засоби контролю безпеки, такі як системи виявлення та запобігання вторгненням, правила брандмауера або політики контролю доступу. Регулярно оновлювати та виправляти системи,

щоб зменшити відомі вразливості. Використовувати можливості сканування вразливостей Wazuh, щоб визначити та розставити пріоритети для виправлення.

Налаштування основних функцій платформи складається з таких кроків [27]

1. Відповідність стандарту PCI DSS. Відповідність стандарту безпеки даних індустрії платіжних карток (PCI DSS) є надзвичайно важливою для організацій, які обробляють дані власників карток. Wazuh SIEM пропонує спеціальні правила та сповіщення для моніторингу та забезпечення дотримання вимог PCI DSS. Налаштувавши ці правила, можна виявляти й реагувати на потенційні інциденти безпеки, які можуть порушити структуру PCI DSS, забезпечуючи захист конфіденційної інформації платіжної картки.

2. Моніторинг цілісності файлів (МЦФ. Моніторинг цілісності файлів необхідний для виявлення неавторизованих змін або підробки критичних системних файлів. Wazuh SIEM надає надійні можливості МЦФ, що дозволяє визначати та відстежувати певні каталоги чи файли для будь-яких змін. Запровадивши МЦФ, ви зможете швидко виявити будь-які підозрілі або несанкціоновані зміни та вжити відповідних заходів для зменшення потенційних ризиків.

3. Відстеження збоїв автентифікації. Відстеження збоїв автентифікації має вирішальне значення для виявлення спроб неавторизованого доступу та потенційних атак на основі облікових даних. Wazuh SIEM дозволяє відстежувати журнали автентифікації, надаючи сповіщення в режимі реального часу, коли виникають повторні помилки автентифікації. Налаштувавши та ввімкнувши цю функцію, ви зможете швидко виявляти підозрілі спроби входу та реагувати на них, посилюючи загальний захист безпеки.

4. Практика управління вразливістю. Щоб забезпечити стійкість мережі, важливо практикувати ефективне керування вразливістю. Wazuh SIEM містить механізм сканування, який дозволяє регулярно сканувати всі

хости у вашій мережі. Використовуючи цю функцію, ви можете виявити й оцінити вразливі місця в усій інфраструктурі. Звичайне сканування вразливостей дає змогу завчасно виправляти слабкі місця, застосовувати виправлення та впроваджувати необхідні засоби контролю безпеки, щоб захистити ваші системи від потенційних експлойтів.

Впровадження та моніторинг Wazuh SIEM у хмарному середовищі надає організаціям потужний інструмент для підвищення безпеки. Налаштувавши та ввімкнувши такі ключові функції, як відповідність стандарту PCI DSS, моніторинг цілісності файлів і відстеження помилок автентифікації, ви можете посилити захист від потенційних загроз і забезпечити захист критично важливих активів. Крім того, використання механізму сканування Wazuh для керування вразливістю дозволяє проактивно ідентифікувати та усувати вразливості у вашій мережі.

Використання Wazuh SIEM дозволяє організаціям бути на крок попереду кіберзагроз, виявляти інциденти безпеки в режимі реального часу та ефективно реагувати на потенційні ризики. Впроваджуючи та контролюючи Wazuh SIEM, організація займає проактивну позицію щодо захисту цифрової інфраструктури та забезпечення цілісності та конфіденційності цінних даних.

3.3 Моніторинг цілісності файлів з Wazuh

Моніторинг цілісності файлів (МЦФ) – це процес безпеки, який використовується для моніторингу цілісності файлів системи та програм. МЦФ є важливим рівнем захисту безпеки для будь-якої організації, що здійснює моніторинг конфіденційних активів. Він забезпечує захист конфіденційних даних, програм і файлів пристроїв шляхом моніторингу, регулярного сканування та перевірки їх цілісності. Це допомагає організаціям виявляти зміни в критично важливих файлах у їхніх системах,

що знижує ризик викрадення чи зламу даних. Цей процес може заощадити час і гроші через втрату продуктивності, втрачений дохід, шкоду репутації та штрафні санкції за дотримання законодавчих і нормативних вимог [28, 29].

Модуль МЦФ виконує періодичне сканування певних шляхів і відстежує зміни в певних каталогах у режимі реального часу. Адміністратор може встановити, які шляхи відстежувати, у конфігурації агентів і менеджера Wazuh [30 - 32].

МЦФ зберігає контрольні суми файлів та інші атрибути в локальній базі даних МЦФ. Після сканування агент Wazuh повідомляє про будь-які зміни, які модуль МЦФ знаходить у відстежуваних шляхах до сервера Wazuh. Модуль МЦФ шукає модифікації файлу, порівнюючи контрольні суми файлу зі збереженими контрольними сумами та значеннями атрибутів. Він генерує сповіщення, якщо знаходить розбіжності.

Модуль Wazuh МЦФ використовує дві бази даних для збору даних подій МЦФ, таких як дані про створення, модифікацію та видалення файлів. Одна з них – це локальна база даних на основі SQLite на контрольованій кінцевій точці, яка зберігає дані в:

C:\\Program Files (x86) \\ossec–agent\\queue\\ fim\\db у Windows.

/var/ossec/queue /fim/db у Linux.

/Library/Ossec/queue/ fim/db в macOS.

База даних агентів на сервері Wazuh. Wazuh-db daemon створює та керує базою даних для кожного агента на сервері Wazuh. Вона використовує ідентифікатор агента для ідентифікації бази даних. Ця служба зберігає бази даних у каталозі /var/ossec/queue/db.

Модуль МЦФ забезпечує синхронізацію агента Wazuh і баз даних сервера Wazuh між собою. Він завжди оновлює список файлів на сервері Wazuh за допомогою даних, доступних для агента Wazuh. Оновлена база даних сервера Wazuh дозволяє обслуговувати запити API, пов’язані з МЦФ. Механізм синхронізації лише оновлює сервер Wazuh інформацією від агентів Wazuh, як-от контрольні суми та атрибути файлів, які змінилися.

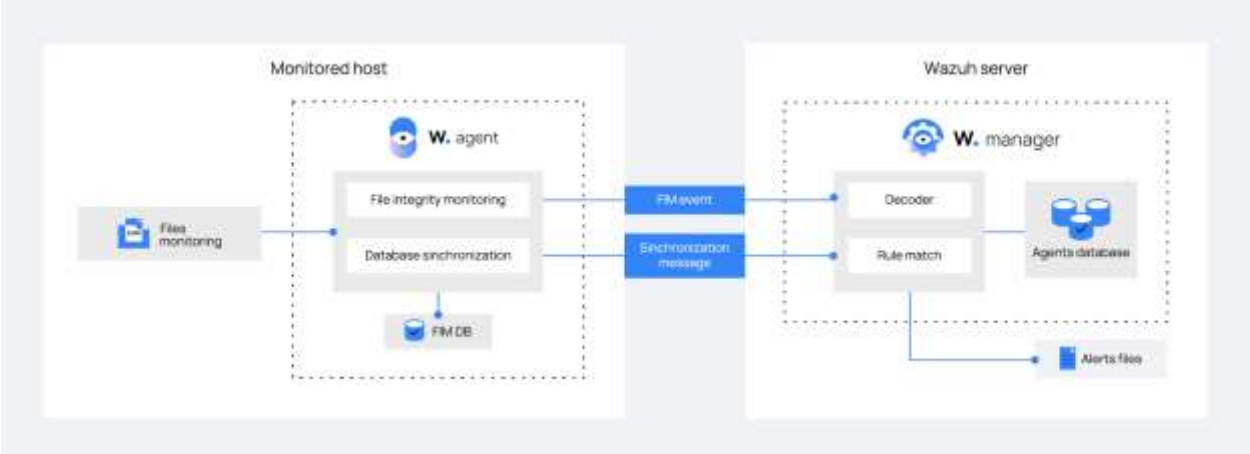

Рисунок 3.13 – Модуль моніторингу цілісності файлів

Управління змінами. Функція Wazuh МЦФ є важливим інструментом для перевірки правильності роботи процесів керування змінами. Ця можливість Wazuh дозволяє перевіряти файли, щоб побачити, чи вони змінюються, як і коли вони змінюються, а також хто або що їх змінює. Модуль Wazuh МЦФ порівнює базову інформацію з інформацією останньої версії файлу. Це порівняння забезпечує видимість змін і оновлень критичних файлів. Наприклад, можна використовувати це для виявлення неправильних оновлень програм або несанкціонованих змін, внесених у файли конфігурації.

Виявлення загроз і реагування. Модуль МЦФ можна поєднати з іншими можливостями Wazuh для виявлення загроз і реагування на них. МЦФ відстежує цілісність файлів, виявляє зміни дозволів і відстежує дії користувачів і файлів. Він надає докладні сповіщення для швидкого реагування на виявлені загрози.

Відповідність нормативним вимогам. Функція МЦФ допомагає організаціям виконувати нормативні вимоги щодо безпеки, конфіденційності та збереження даних. Відстеження змін у критичних файлах є важливою вимогою для таких нормативних актів, як PCI DSS, HIPAA та GDPR.

Wazuh має вбудовану можливість моніторингу цілісності файлів. Модуль Wazuh МЦФ відстежує файли та каталоги та запускає сповіщення, коли користувач або процес створює, змінює та видаляє контрольовані файли. Він запускає базове сканування, зберігаючи криптографічну контрольну суму та інші атрибути контрольованих файлів. Коли користувач або процес змінює файл, модуль порівнює його контрольну суму та атрибути з базовою лінією. Модуль запускає сповіщення, якщо виявляє невідповідність. Модуль МЦФ виконує сканування в реальному часі та за розкладом залежно від конфігурації МЦФ для агентів і менеджера.

Деякі переваги можливості Wazuh МЦФ включають керування змінами, виявлення загроз і реагування на них, а також відповідність нормативним вимогам.

Рішення Wazuh МЦФ, відоме як syscheck, також може відстежувати зміни в реєстрі Windows. Syscheck можна налаштувати для моніторингу різних каталогів або файлів у кількох режимах.

Адміністратор може використовувати моніторинг у реальному часі для каталогів, якими зазвичай зловживають зловмисники, і запланувати перевірку для файлів або каталогів, що містять конфігураційні файли.

За розкладом. Слідкує за змінами через регулярні проміжки часу.

Реальний час. Слідкує за змінами, щойно вони відбуваються.

Визначені дані. Слідкує за змінами, щойно вони відбуваються (мається на увазі в реальному часі).

Інформацію про перевірку користувача, який вносить зміни.

Кожне середовище відрізняється, тому важливо розробити стратегію парадигми МЦФ, яка відповідає потребам.

Налаштування МЦФ. Конфігурації за замовчуванням. МЦФ увімкнено за замовчуванням під час встановлення Wazuh Agent. Існують конфігурації за замовчуванням залежно від операційної системи.

Спеціальні конфігурації. Найпростіший спосіб передати конфігурації syscheck агенту – це централізована конфігурація (або спільна конфігурація).

Основним аспектом централізованої конфігурації є поняття пріоритету, оскільки конфігурації агента у файлі ../shared/agent.conf матимуть пріоритет над будь-чим у файлі ossec.conf за замовчуванням.

Як згадувалося раніше, агенти Wazuh налаштовані зі стандартним набором конфігурацій syscheck у файлі ossec.conf за замовчуванням. Тому все, що треба зберегти з конфігурації за замовчуванням, слід додати до спільної конфігурації.

Розглянемо приклад централізованої конфігурації. Даний приклад конфігурації робить наступне (рисунок 3.14):

Розбиває конфігурації за операційною системою: Linux; Windows.

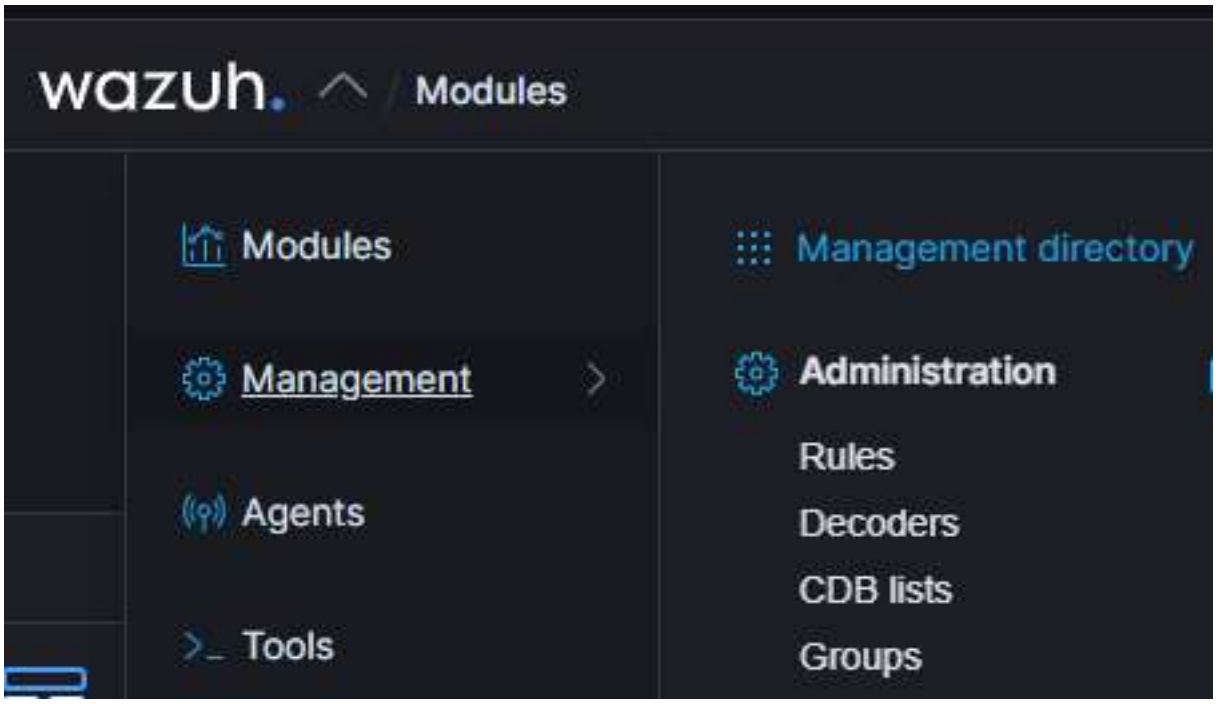

Рисунок 3.14 – Вікно конфігурації

Встановлює моніторинг у реальному часі з check_all='yes' для деяких каталогів, якими зазвичай зловживають зловмисники realtime дозволяє збирати додавання, модифікацію та видалення файлів у міру їх виникнення check_all дозволяє збирати хеші файлів MD5, SHA1 і SHA256 будь-яких нових, змінених або видалених файлів. Зберігає стандартні конфігурації, надіслані командою Wazuh.

Розгортання цієї конфігурації за замовчуванням залежить від вибору групи для її розгортання. Якщо потрібно, щоб ця конфігурація застосовувалася до всіх агентів, відповідно, її необхідно додати до групи за замовчуванням. Щоб вибрати групу за замовчуванням треба натиснути значок олівця поруч із групою за замовчуванням (рисунок 3.15). Вставити конфігурацію в редактор і натисніть зберегти (рисунок 3.16).

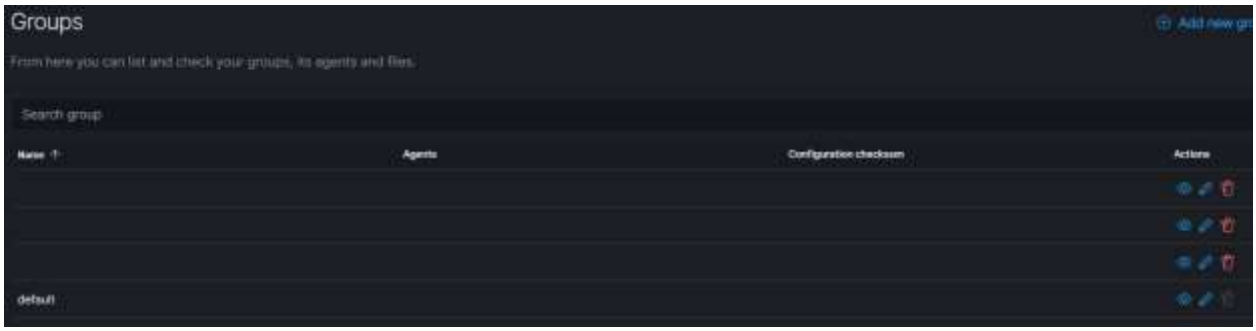

Рисунок 3.15 – Інтерфейс вибору групи

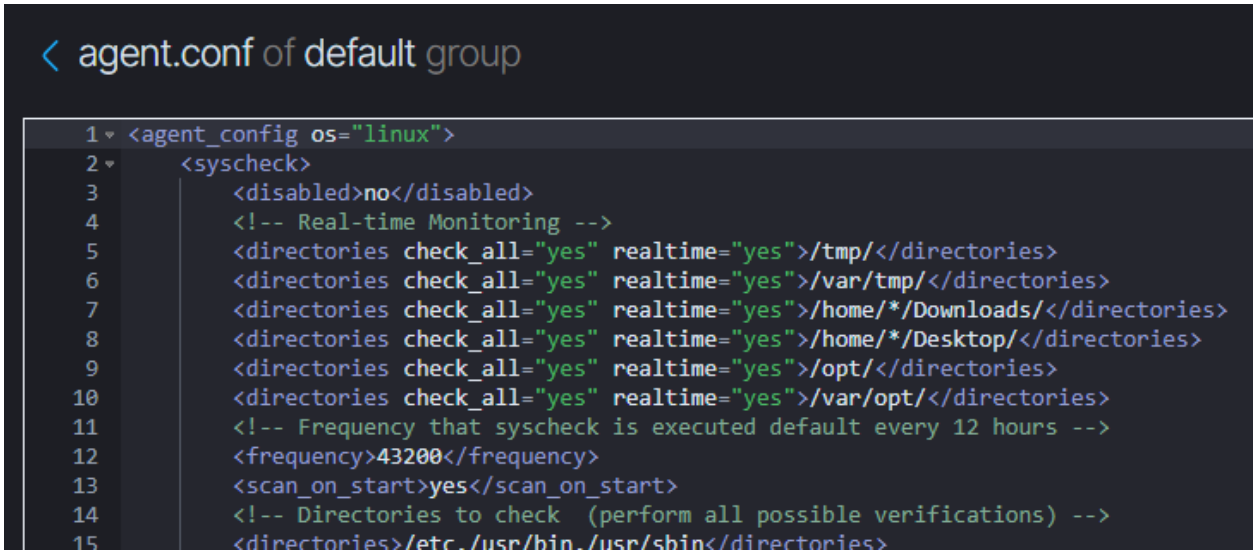

Рисунок 3.16 – Приклад конфігурації агента

Тепер сервер Wazuh Manager надішле конфігурацію зареєстрованим агентам, а агенти перезапустяться та приймуть нову конфігурацію.

Моніторинг сповіщень МЦФ (рисунок 3.17).

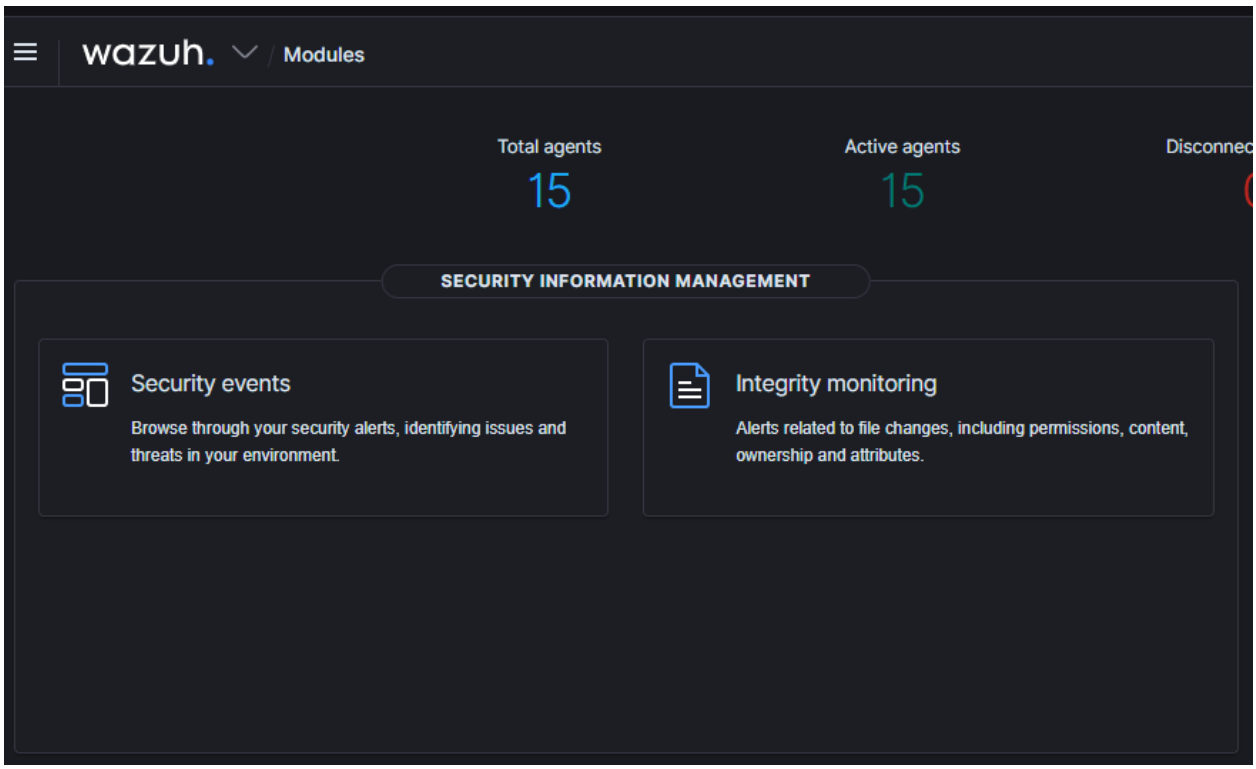

Рисунок 3.17 – Інтерфейс модуля сповіщень

На головному екрані Wazuh Dashboards потрібно вибрати модуль моніторингу цілісності, який буде перенесено на інформаційну панель моніторингу цілісності (рисунок 3.18).

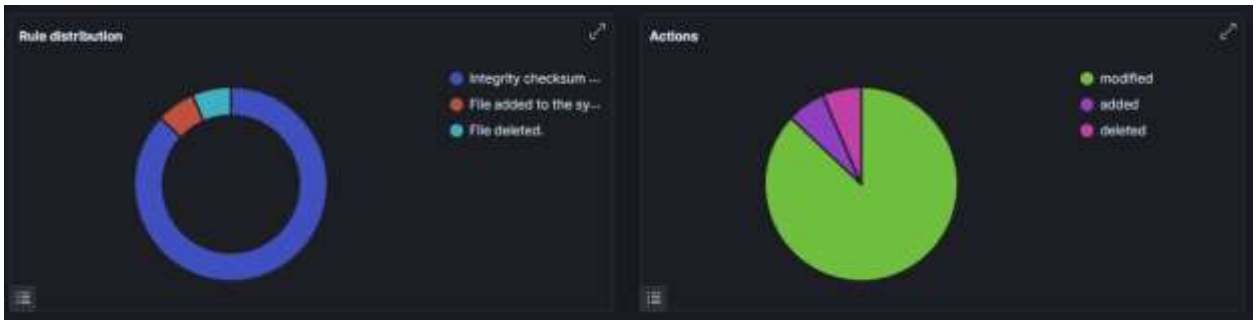

Рисунок 3.18 – Приклад панелі сповіщень

Щоб переглянути фактичні події МЦФ і детально ознайомитись із сповіщеннями переходимо на вкладку «Події» (рисунок 3.19).

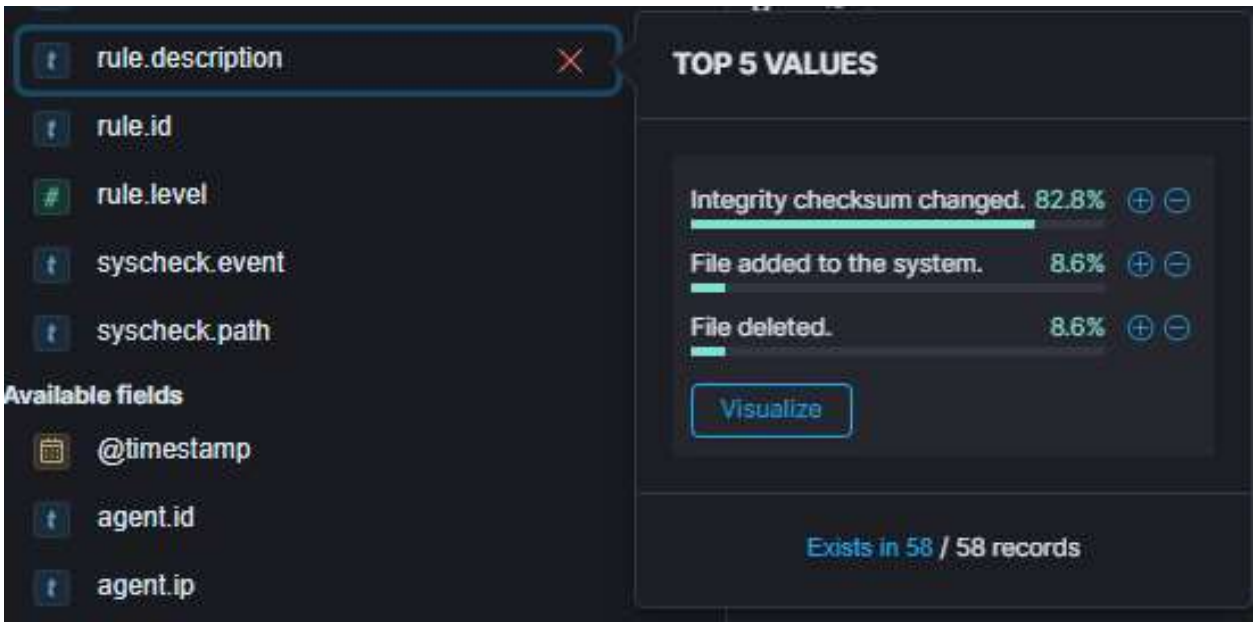

Рисунок 3.19 – Інтерфейс вкладки «Події»

Фільтрування за описом правила може допомогти вибрати певні події (рисунок 3.20).

Рисунок 3.20 – Приклад файлу, доданого до системного сповіщення

Розширення можливостей МЦФ. Одним із очевидних способів доповнити МЦФ є використання хешів файлів, які генерує syscheck. Wazuh є модульним і розширюваним і вже має інтеграцію для YARA та VirusTotal.

Після додавання можна використовувати ці розширення для перевірки хешів файлів на наявність відомих підписів.

ВИСНОВКИ

В кваліфікаційній роботі розв’язано актуальну задачу підвищення ефективності пошуку загроз з використанням платформи Wazuh. При цьому отримано наступні результати.

1. Проведено аналіз функціональних можливостей платформ пошуку загроз, серед який виділено наступні: AlienVault, SOCRadar, DOCGuard, GreyNoise, Intezer, MISP, OpenCTI, VirusTotal, Wazuh.

2. Розкрито можливості та переваги платформи Wazuh, зокрема такі, як виявлення вторгнень, аналізу даних журналів, контроль цілісності файлів, виявлення вразливостей, оцінка конфігурації, реагування на інцидент та хмарної безпеки.

3. Досліджено ландшафт загроз кібербезпеці, який базується на кіберланцюгу вбивств та складається з семи етапів: розвідки, озброєння, доставки, експлуатації, встановлення, командування та управлінн та дії щодо досягнення мети.

4. Інтегровано Wazuh з управлінням хмарною безпекою Google Cloud Platform. Wazuh інтегровано з GCP за допомогою служби видавця та передплатника Google Cloud, яка допомагає надсилати та отримувати дані журналу між програмами. Wazuh надає модуль інтеграції для GCP, який отримує журнали зі служби Pub/Sub.

5. Розроблено алгоритм використання Wazuh для моніторингу цілісності файлів, який відстежує цілісність файлів, виявляє зміни дозволів і відстежує інші дії користувачів файлами. Алгоритм надає докладні сповіщення для швидкого реагування на виявлені загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Top 7 Threat Intelligence Pl. [Електронний ресурс]. – Режим доступу: https://www.esecurityplanet.com/products/threat-intelligence-platforms/
2. Wazuh documentation overview. [Електронний ресурс]. – Режим доступу: https://documentation.wazuh.com/current/
3. Wazuh documentation components. [Електронний ресурс]. – Режим доступу: https://documentation.wazuh.com/current/getting-started/components/index
4. Wazuh documentation, mitre. [Електронний ресурс]. - Режим доступу: https://documentation.wazuh.com/current/user-manual/ruleset/mitre.html
5. Wazuh documentation regulatory compliance. [Електронний ресурс]. - Режим доступу: https://documentation.wazuh.com/current/getting-started/use-cases/regulatory-compliance.html
6. ATT&CK Matrix for Enterprise. [Електронний ресурс]. - Режим доступу: https://attack.mitre.org/
7. The Threat Intelligence Lifecycle: A Definitive Guide for 2023. [Електронний ресурс]. - Режим доступу: https://flare.io/learn/resources/blog/threat-intelligence-lifecycle/
8. Six Stages of the Threat Intelligence Lifecycle. [Електронний ресурс]. - Режим доступу: https://www.noggin.io/blog/six-stages-of-the-threat-intelligence-lifecycle
9. What is cyber threat intelligence? [Електронний ресурс]. - Режим доступу: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/
10. What is threat intelligence? Електронний ресурс]. [Електронний ресурс]. - Режим доступу: https://www.ibm.com/topics/threat-intelligence
11. Що таке SIEM? Інформація про безпеку та управління подіями. [Електронний ресурс]. – Режим доступу: https://gridinsoft.ua/siem

12. Wagner, T. D., Mahbub, K., Palomar, E., Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.

13. Ramsdale, A., Shiaeles, S., & Kolokotronis, N. (2020). A comparative analysis of cyber-threat intelligence sources, formats and languages. Electronics, 9(5), 824.

14. Kaloudi, N., Li, J. (2020). The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34.

15. Hadi, H., Riaz, M., Abbas, Z., Nisa, K. Cyber Threat Intelligence Model: An Evaluation of Taxonomies and Sharing Platforms. In Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence, 2023, pp. 3-33.

16. Tsiknas, K., Taketzis, D., Demertzis, K., Skianis, C. Cyber threats to industrial IoT: a survey on attacks and countermeasures. IoT, 2(1), 2021, 163-186.

17. Mallikarjunaradhya, V., Pothukuchi, A. S., & Kota, L. V. (2023). An Overview of the Strategic Advantages of AI-Powered Threat Intelligence in the Cloud. Journal of Science & Technology, 4(4), 1-12.

18. Wagner, T. D., Mahbub, K., Palomar, E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.

19. Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an industry: A cyber threat intelligence perspective. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 135-154.

20. Mohamed, N. (2022). State-of-the-Art in Chinese APT Attack and Using Threat Intelligence for Detection. A Survey. Journal of Positive School Psychology, 4419-4443.

21. Patel, P. S., Kunwar, R. S., & Thakar, A. (2023). Malware Detection Using Yara Rules in SIEM. In Malware Analysis and Intrusion Detection in Cyber-Physical Systems, pp. 313-330

22. Zahid, H., Hina, S., Hayat, M. F., Shah, G. A. (2023). Agentless approach for security information and event management in industrial IoT. Electronics, 12(8), 1831.

23. Sklavidis, I., Angelidis, C., Babagiannou, R., Liapis, A. Enhancing SIEM Technology for Protecting Electrical Power and Energy Sector. In IEEE International Conference on Cyber Security and Resilience, 2021, pp. 473-478

24. Tariq, A., Manzoor, J., Aziz, M. A. (2022). Open source SIEM solutions for an enterprise. Information & Computer Security, 31(1), 88-107.

25. Alhayani, B., Abbas, S. T., Khutar, D. Z. (2021). Best ways computation intelligent of face cyber attacks. Materials Today: Proceedings, 26-31.

26. Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. Future internet, 11(3), 63.

27. Duggineni, S. (2023). Data Integrity Controls: The Universal basis for Authenticity and Reliability of Data. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY, 7(1), 53-58.

28. Tabrizchi, H., Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

29. Fuentes-García, M., Camacho, J., Maciá-Fernández, G. Present and future of network security monitoring. *IEEE Access*, *9*, 2021, 112744-112760.

30. Sheeraz, M., Paracha, M. A., Haque, M. U., (2023). Effective Security Monitoring Using Efficient SIEM Arc1hitecture. Hum.-Centric Comput. Inf. Sci, 13, 1-18.

31. Гарматюк В.Р., Понедєльніков Г.М., Іващенко М.В. Життєвий цикл розвідки загроз. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2023), Тернопіль, 2023. – С. 71–73

32. Іващенко М.В., Кондратюк В.М. Алгоритм впровадження Wazuh у хмарному середовищі. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2023. – С. 74-75.

ДОДАТОК А

Копії публікацій